# Prism_GroupIT Scan Report

| | |
|---|---|
| Project Name | Prism_GroupIT |
| Scan Start | Friday, April 25, 2025 1:08:18 PM |
| Preset | Group IT Security |
| Scan Time | 00h:17m:45s |
| Lines Of Code Scanned | 1662427 |
| Files Scanned | 12594 |
| Report Creation Time | Monday, April 28, 2025 7:30:12 AM |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996 |
| Team | Group IT Security |
| Checkmarx Version | 9.7.2.1000 HF1 |
| Scan Type | Full |
| Source Origin | GIT |
| Scanned Branch | /refs/heads/prism_d10_preprod |
| Density | 4/100000 (Vulnerabilities/LOC) |
| Visibility | Public |
| Scan Custom Fields | |

# Filter Settings

**Severity**

Included: Critical, High, Medium, Low

Excluded: Information

**Result State**

Included: Confirmed

Excluded: To Verify, Not Exploitable, Urgent, Proposed Not Exploitable

**Assigned to**

Included: All

**Categories**

Included:

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

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

Excluded:

| | |
|---|---|
| Uncategorized | None |
| Custom | None |
| PCI DSS v3.2.1 | None |
| OWASP Top 10 2013 | None |
| FISMA 2014 | None |
| NIST SP 800-53 | None |
| OWASP Top 10 2017 | None |
| OWASP Mobile Top 10 2016 | None |
| ASD STIG 4.10 | None |
| OWASP Top 10 API | None |
| OWASP Top 10 2010 | None |
| OWASP Top 10 2021 | None |
| CWE top 25 | None |
| MOIS(KISA) Secure Coding 2021 | None |
| OWASP ASVS | None |
| SANS top 25 | None |
| ASA Mobile Premium | None |
| ASA Premium | None |
| Top Tier | None |

| | |
|---|---|
| PCI DSS v4.0 | None |
| Base Preset | None |
| OWASP Top 10 API 2023 | None |
| ASD STIG 6.1 | None |
| OWASP Mobile Top 10 2024 | None |

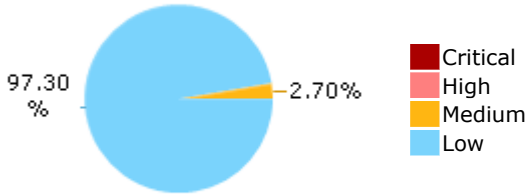
**Results Limit**

Results limit per query was set to 50

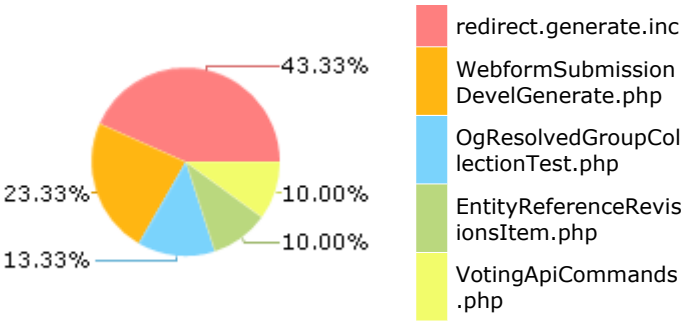
**Selected Queries**

Selected queries are listed in Result Summary

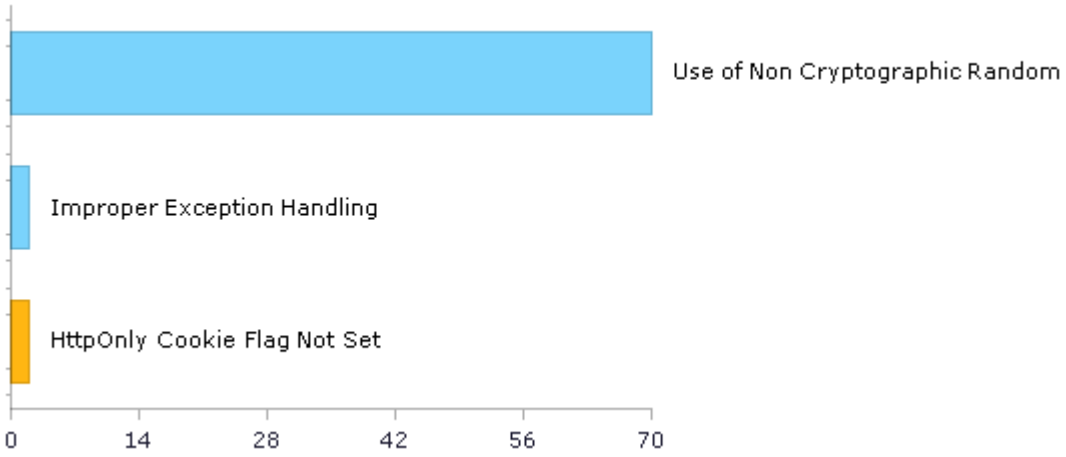
## Result Summary




## Most Vulnerable Files




## Top 5 Vulnerabilities



# Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

| Category | Threat Agent | Exploitability | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations * |
|---|---|---|---|---|---|---|---|---|
| A1-Injection** | App. Specific | EASY | COMMON | EASY | SEVERE | App. Specific | 0 | 0 |
| A2-Broken Authentication** | App. Specific | EASY | COMMON | AVERAGE | SEVERE | App. Specific | 0 | 0 |
| A3-Sensitive Data Exposure** | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | App. Specific | 0 | 0 |
| A4-XML External Entities (XXE) | App. Specific | AVERAGE | COMMON | EASY | SEVERE | App. Specific | 0 | 0 |
| A5-Broken Access Control** | App. Specific | AVERAGE | COMMON | AVERAGE | SEVERE | App. Specific | 0 | 0 |
| A6-Security Misconfiguration ** | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 0 | 0 |
| A7-Cross-Site Scripting (XSS)** | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 0 | 0 |
| A8-Insecure Deserialization | App. Specific | DIFFICULT | COMMON | AVERAGE | SEVERE | App. Specific | 0 | 0 |
| A9-Using Components with Known Vulnerabilities** | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | MODERATE | App. Specific | 70 | 70 |
| A10-Insufficient Logging & Monitoring | App. Specific | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | App. Specific | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - OWASP Top 10 2021

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| A1-Broken Access Control** | 0 | 0 |
| A2-Cryptographic Failures** | 70 | 70 |
| A3-Injection** | 0 | 0 |
| A4-Insecure Design** | 2 | 12 |
| A5-Security Misconfiguration** | 2 | 2 |
| 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

| Category | Threat Agent | Attack Vectors | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations * |
|---|---|---|---|---|---|---|---|---|
| A1-Injection** | EXTERNAL, INTERNAL, ADMIN USERS | EASY | COMMON | AVERAGE | SEVERE | ALL DATA | 0 | 0 |
| A2-Broken Authentication and Session Management** | EXTERNAL, INTERNAL USERS | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | AFFECTED DATA AND FUNCTIONS | 0 | 0 |
| A3-Cross-Site Scripting (XSS)** | EXTERNAL, INTERNAL, ADMIN USERS | AVERAGE | VERY WIDESPREAD | EASY | MODERATE | AFFECTED DATA AND SYSTEM | 0 | 0 |
| A4-Insecure Direct Object References** | SYSTEM USERS | EASY | COMMON | EASY | MODERATE | EXPOSED DATA | 0 | 0 |
| A5-Security Misconfiguration ** | EXTERNAL, INTERNAL, ADMIN USERS | EASY | COMMON | EASY | MODERATE | ALL DATA AND SYSTEM | 0 | 0 |
| A6-Sensitive Data Exposure** | EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS | DIFFICULT | UNCOMMON | AVERAGE | SEVERE | EXPOSED DATA | 0 | 0 |
| A7-Missing Function Level Access Control** | EXTERNAL, INTERNAL USERS | EASY | COMMON | AVERAGE | MODERATE | EXPOSED DATA AND FUNCTIONS | 0 | 0 |
| A8-Cross-Site Request Forgery (CSRF) | USERS BROWSERS | AVERAGE | COMMON | EASY | MODERATE | AFFECTED DATA AND FUNCTIONS | 0 | 0 |
| A9-Using Components with Known Vulnerabilities** | EXTERNAL USERS, AUTOMATED TOOLS | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | AFFECTED DATA AND FUNCTIONS | 0 | 0 |
| A10-Unvalidated Redirects and Forwards** | USERS BROWSERS | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | AFFECTED DATA AND FUNCTIONS | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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 | 70 | 70 |
| PCI DSS (3.2.1) - 6.5.4 - Insecure communications | 0 | 0 |
| PCI DSS (3.2.1) - 6.5.5 - Improper error handling** | 2 | 12 |
| 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - FISMA 2014

| Category | Description | Issues Found | Best Fix Locations* |
|---|---|---|---|
| Access Control** | Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. | 0 | 0 |
| Audit And Accountability** | Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. | 0 | 0 |
| Configuration Management** | Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems. | 0 | 0 |
| Identification And Authentication** | Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | 0 | 0 |
| Media Protection** | Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. | 70 | 70 |
| System And Communications Protection | Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. | 2 | 2 |
| System And Information Integrity** | Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response. | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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)** | 70 | 70 |
| SC-4 Information in Shared Resources (P1) | 0 | 0 |
| SC-5 Denial of Service Protection (P1)** | 2 | 12 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 2 | 2 |
| 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - OWASP Mobile Top 10 2016

| Category | Description | Issues Found | Best Fix Locations* |
|---|---|---|---|
| M1-Improper Platform Usage | This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk. | 0 | 0 |
| M2-Insecure Data Storage | This category covers insecure data storage and unintended data leakage. | 0 | 0 |
| M3-Insecure Communication | This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc. | 0 | 0 |
| M4-Insecure Authentication | This category captures notions of authenticating the end user or bad session management. This can include:<br>-Failing to identify the user at all when that should be required<br>-Failure to maintain the user's identity when it is required<br>-Weaknesses in session management | 0 | 0 |
| M5-Insufficient Cryptography | The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly. | 0 | 0 |
| M6-Insecure Authorization | This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure. | 0 | 0 |
| M7-Client Code Quality | This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device. | 0 | 0 |
| M8-Code Tampering | This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the | 0 | 0 |

| | | | |
|---|---|---|---|
| | application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain. | | |
| M9-Reverse Engineering | This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property. | 0 | 0 |
| M10-Extraneous Functionality | Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing. | 0 | 0 |

***** Best fix location values are absolute values derived from the entire vulnerabilities detected.

# Scan Summary - Custom

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| Must audit | 0 | 0 |
| Check | 0 | 0 |
| Optional | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.

# Scan Summary - PCI DSS v4.0

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development** | 74 | 84 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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 | 0 | 0 |

| | | |
|---|---|---|
| supports on-demand reporting requirements. | | |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| information during preparation for transmission. | | |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| to show how deadlock and recursion issues in web services are being mitigated. | | |
| 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 product will be configured by following available guidance. | 0 | 0 |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| accreditation impact prior to implementation. | | |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| indicating the reliable termination of authenticated communications sessions. | | |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| Information System Security Officers when accounts are modified. | | |
| 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.

# Scan Summary - 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 | 0 | 0 |

| | | |
|---|---|---|
| supports on-demand reporting requirements. | | |
| 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. | 70 | 70 |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| information during preparation for transmission. | | |
| 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.** | 2 | 12 |
| 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 | 0 | 0 |

| | | |
|---|---|---|
| to show how deadlock and recursion issues in web services are being mitigated. | | |
| 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 product will be configured by following available guidance. | 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 | 0 | 0 |

| | | |
|---|---|---|
| storage. | | |
| 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.

# Scan Summary - 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - 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** | 2 | 12 |
| MOIS(KISA) Security Functions** | 70 | 70 |
| MOIS(KISA) Time and status | 0 | 0 |
| MOIS(KISA) Verification and representation of input data** | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - SANS top 25

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| SANS top 25** | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - CWE top 25

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| CWE top 25** | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - Top Tier

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| Top Tier** | 70 | 70 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - OWASP ASVS

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| V01 Architecture, Design and Threat Modeling** | 0 | 0 |
| V02 Authentication** | 70 | 70 |
| V03 Session Management** | 2 | 2 |
| 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** | 2 | 12 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - ASA Mobile Premium

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

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - ASA Premium

| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| ASA Premium** | 72 | 72 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.
** Please note, the report only includes the presets/filters you applied to the scan results.

# Scan Summary - Base Preset

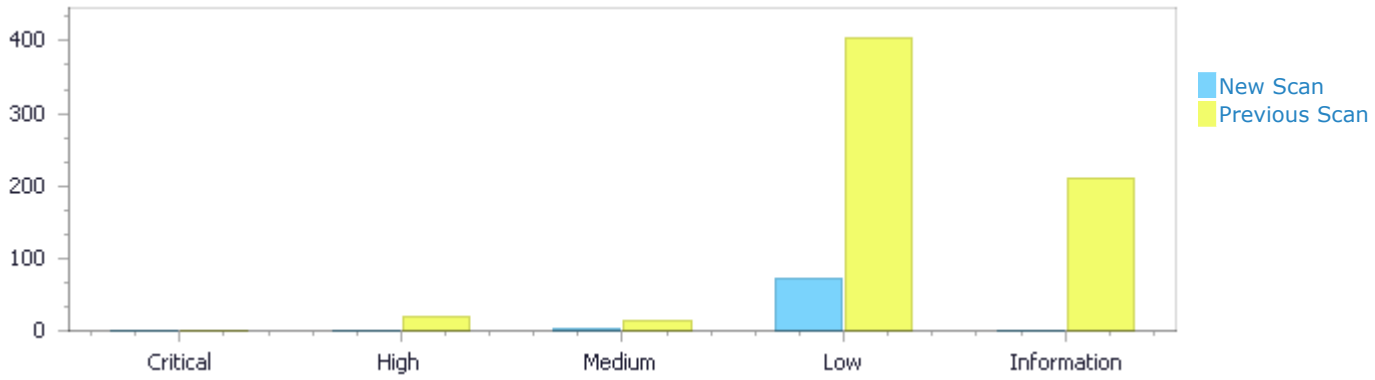
| Category | Issues Found | Best Fix Locations* |
|---|---|---|
| Base Preset | 0 | 0 |

* Best fix location values are absolute values derived from the entire vulnerabilities detected.

## Results Distribution By Status

Compared to project scan from 8/2/2024 1:28 PM

| | Critical | High | Medium | Low | Information | Total |
|---|---|---|---|---|---|---|
| New Issues | 0 | 0 | 2 | 72 | 0 | 74 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 0 | 0 | 2 | 72 | 0 | 74 |
| | | | | | | |
| Fixed Issues | 0 | 20 | 14 | 405 | 211 | 650 |




## Results Distribution By State

| | Critical | High | Medium | Low | Information | Total |
|---|---|---|---|---|---|---|
| To Verify | 0 | 0 | 0 | 0 | 0 | 0 |
| Not Exploitable | 0 | 0 | 0 | 0 | 0 | 0 |
| Confirmed | 0 | 0 | 2 | 72 | 0 | 74 |
| Urgent | 0 | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 0 | 0 | 2 | 72 | 0 | 74 |

## Result Summary

| Vulnerability Type | Occurrences | Severity |
|---|---|---|
| HttpOnly Cookie Flag Not Set | 2 | Medium |
| Use of Non Cryptographic Random | 70 | Low |
| Improper Exception Handling | 2 | Low |

## 10 Most Vulnerable Files

## Critical High and Medium Vulnerabilities

| File Name | Issues Found |
|---|---|
| modules/custom/custom_cart/js/cap-crp.js | 1 |
| themes/custom/capgemini_b5/js/custom.js | 1 |

# Scan Results Details

## HttpOnly Cookie Flag Not Set

Query Path:
JavaScript\Cx\JavaScript Server Side Vulnerabilities\HttpOnly Cookie Flag Not Set Version:4

### Categories

FISMA 2014: System And Communications Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2021: A5-Security Misconfiguration
OWASP ASVS: V03 Session Management
ASA Premium: ASA Premium
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

*Description*

**HttpOnly Cookie Flag Not Set\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=13 |
| Status | New |
| Detection Date | 4/25/2025 1:25:24 PM |

The web application's function method creates a cookie cookie, at line 43 of modules/custom/custom_cart/js/cap-crp.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | modules/custom/custom_cart/js/cap-crp.js | modules/custom/custom_cart/js/cap-crp.js |
| Line | 43 | 43 |
| Object | cookie | cookie |

Code Snippet
File Name modules/custom/custom_cart/js/cap-crp.js
Method (function ($, Drupal, drupalSettings) {

```
....
43.  document.cookie = 'session_local_timezone=' + localeTimezone;
```

**HttpOnly Cookie Flag Not Set\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=14 |
| Status | New |
| Detection Date | 4/25/2025 1:25:24 PM |

The web application's function method creates a cookie cookie, at line 546 of themes/custom/capgemini_b5/js/custom.js, and returns it in the response. However, the

application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | themes/custom/capgemini_b5/js/custom.js | themes/custom/capgemini_b5/js/custom.js |
| Line | 546 | 546 |
| Object | cookie | cookie |

Code Snippet
File Name themes/custom/capgemini_b5/js/custom.js
Method (function ($, Drupal, drupalSettings) {

```
....
546.  document.cookie='session_local_timezone='+localeTimezone;
```

## Use of Non Cryptographic Random

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

### Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage
FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A2-Cryptographic Failures
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V02 Authentication
ASA Premium: ASA Premium
Top Tier: Top Tier
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
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\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=944 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 476 of modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php | modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php |

| | | |
|---|---|---|
| Line | 476 | 476 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition): array {

```
....
476.  $values['timezone'] = $timeZoneList[array_rand($timeZoneList)];
```

**Use of Non Cryptographic Random\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=945 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 477 of modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php | modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php |
| Line | 477 | 477 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/date_recur/src/Plugin/Field/FieldType/DateRecurItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition): array {

```
....
477.  $values['rrule'] = 'FREQ=DAILY;COUNT=' . rand(2, 10);
```

**Use of Non Cryptographic Random\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=946 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 532 of modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php uses a weak method array_rand to produce random values. These values might be

used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php | modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php |
| Line | 532 | 532 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition) {

```
....
532.  $group = array_rand($referenceable);
```

**Use of Non Cryptographic Random\Path 4:**

Severity Low
Result State Confirmed
Online Results https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=947
Status New
Detection Date 4/25/2025 1:25:33 PM

Method generateSampleValue at line 533 of modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php | modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php |
| Line | 533 | 533 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/dynamic_entity_reference/src/Plugin/Field/FieldType/DynamicEntityReferenceItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition) {

```
....
533.  $values['target_id'] = array_rand($referenceable[$group]);
```

**Use of Non Cryptographic Random\Path 5:**

Severity Low

| | |
|---|---|
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=948 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 503 of modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php |
| Line | 503 | 503 |
| Object | array_rand | array_rand |

Code Snippet

File Name modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php

Method public static function generateSampleValue(FieldDefinitionInterface $field_definition) {

```
....
503.  $bundle = array_rand($bundles);
```

**Use of Non Cryptographic Random\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=949 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 509 of modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php |
| Line | 509 | 509 |
| Object | mt_rand | mt_rand |

Code Snippet

File Name modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php

| | |
|---|---|
| Method | public static function generateSampleValue(FieldDefinitionInterface $field_definition) { |

```
....
509.  $label = $random->word(mt_rand(1, 10));
```

**Use of Non Cryptographic Random\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=950 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 528 of modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php |
| Line | 528 | 528 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | modules/contrib/entity_reference_revisions/src/Plugin/Field/FieldType/EntityReferenceRevisionsItem.php |
| Method | public static function generateSampleValue(FieldDefinitionInterface $field_definition) { |

```
....
528.  $max = rand(1, 5);
```

**Use of Non Cryptographic Random\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=951 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 97 of modules/contrib/field_group/tests/src/Functional/EntityDisplayTest.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/field_group/tests/src/Fu | modules/contrib/field_group/tests/src/Fu |

| | | |
|---|---|---|
| | nctional/EntityDisplayTest.php | nctional/EntityDisplayTest.php |
| Line | 97 | 97 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/field_group/tests/src/Functional/EntityDisplayTest.php
Method public function setUp(): void {

```
....
97.  $node_values[$field_name][0]['value'] = mt_rand(1, 127);
```

**Use of Non Cryptographic Random\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=952 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testRelationshipAccess at line 193 of modules/contrib/group/tests/src/Unit/AccessControlTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/group/tests/src/Unit/AccessControlTest.php | modules/contrib/group/tests/src/Unit/AccessControlTest.php |
| Line | 193 | 193 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/group/tests/src/Unit/AccessControlTest.php
Method public function testRelationshipAccess(\Closure $expected, $plugin_id, GroupRelationTypeInterface $definition, $has_admin_permission, $has_permission, $has_own_permission, $permission, $own_permission, $is_owner, $check_chain) {

```
....
193.  $account_id = rand(1, 100);
```

**Use of Non Cryptographic Random\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=953 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testEntityAccess at line 472 of modules/contrib/group/tests/src/Unit/AccessControlTest.php uses a weak method rand to

produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/group/tests/src/Unit/AccessControlTest.php | modules/contrib/group/tests/src/Unit/AccessControlTest.php |
| Line | 472 | 472 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/group/tests/src/Unit/AccessControlTest.php
Method public function testEntityAccess(\Closure $expected, $plugin_id, GroupRelationTypeInterface $definition, $has_admin_permission, $has_permission, $has_own_permission, $permission, $own_permission, $is_grouped, $is_ownable, $is_owner, $is_publishable, $is_published, $operation, $check_chain) {

```
....
472.  $account_id = rand(1, 100);
```

**Use of Non Cryptographic Random\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=954 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method applyEffect at line 44 of modules/contrib/image_effects/src/Plugin/ImageEffect/RotateImageEffect.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/image_effects/src/Plugin/ImageEffect/RotateImageEffect.php | modules/contrib/image_effects/src/Plugin/ImageEffect/RotateImageEffect.php |
| Line | 44 | 44 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/image_effects/src/Plugin/ImageEffect/RotateImageEffect.php
Method public function applyEffect(ImageInterface $image) {

```
....
44.  $degrees = rand(-$max, $max);
```

**Use of Non Cryptographic Random\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |

| | |
|---|---|
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=955 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 28 of modules/contrib/legal/tests/src/Functional/PasswordResetTest.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/legal/tests/src/Functional/PasswordResetTest.php | modules/contrib/legal/tests/src/Functional/PasswordResetTest.php |
| Line | 28 | 28 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/legal/tests/src/Functional/PasswordResetTest.php
Method public function setUp(): void {

```
....
28.  $this->account->login = \Drupal::time()->getRequestTime() -
mt_rand(10, 100000);
```

**Use of Non Cryptographic Random\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=956 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 64 of modules/contrib/message/tests/src/Functional/MessageEntityDelete.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/message/tests/src/Functional/MessageEntityDelete.php | modules/contrib/message/tests/src/Functional/MessageEntityDelete.php |
| Line | 64 | 64 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/message/tests/src/Functional/MessageEntityDelete.php
Method public function setUp():void {

```
....
64.  'weight' => mt_rand(0, 10),
```

**Use of Non Cryptographic Random\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=957 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 49 of modules/contrib/message/tests/src/Kernel/MessageTokenTest.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/message/tests/src/Kernel/MessageTokenTest.php | modules/contrib/message/tests/src/Kernel/MessageTokenTest.php |
| Line | 49 | 49 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/message/tests/src/Kernel/MessageTokenTest.php
Method public function setUp():void {

```
....
49.  'uid' => mt_rand(5, 10),
```

**Use of Non Cryptographic Random\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=958 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testHeaders at line 462 of modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php | modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php |
| Line | 462 | 462 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php
Method public function testHeaders(): void {

```
....
462.  $local = $this->randomMachineName() . $chars[array_rand($chars)] .
$this->randomMachineName();
```

**Use of Non Cryptographic Random\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=959 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testHeaders at line 463 of modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php | modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php |
| Line | 463 | 463 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/mimemail/tests/src/Kernel/MimeMailFormatHelperTest.php
Method public function testHeaders(): void {

```
....
463.  $domain = $this->randomMachineName() . '-' . $this-
>randomMachineName() . '.' . $this->randomMachineName(rand(2, 4));
```

**Use of Non Cryptographic Random\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=960 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testSubscribeAccess at line 278 of modules/contrib/og/tests/src/Functional/GroupSubscribeTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Functional/GroupSubscribeTest.php | modules/contrib/og/tests/src/Functional/GroupSubscribeTest.php |
| Line | 278 | 278 |

| | | |
|---|---|---|
| Object | rand | rand |

Code Snippet
File Name modules/contrib/og/tests/src/Functional/GroupSubscribeTest.php
Method public function testSubscribeAccess() {

```
....
278.  'entity_id' => rand(1000, 2000),
```

**Use of Non Cryptographic Random\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=961 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 135 of modules/contrib/og/tests/src/Unit/GroupCheckTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/GroupCheckTest.php | modules/contrib/og/tests/src/Unit/GroupCheckTest.php |
| Line | 135 | 135 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/GroupCheckTest.php
Method protected function setUp(): void {

```
....
135.  $this->entityId = rand(10, 50);
```

**Use of Non Cryptographic Random\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=962 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 121 of modules/contrib/og/tests/src/Unit/OgAdminRoutesControllerTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/OgAd | modules/contrib/og/tests/src/Unit/OgAd |

| | | |
|---|---|---|
| | minRoutesControllerTest.php | minRoutesControllerTest.php |
| Line | 121 | 121 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/OgAdminRoutesControllerTest.php
Method protected function setUp(): void {

```
....
121.  $this->entityId = rand(20, 30);
```

**Use of Non Cryptographic Random\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=963 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testAddGroup at line 97 of modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php |
| Line | 97 | 97 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php
Method public function testAddGroup() {

```
....
97.  $weight = rand(-100, 100);
```

**Use of Non Cryptographic Random\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=964 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testRemoveGroup at line 174 of modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php |
| Line | 174 | 174 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php
Method public function testRemoveGroup() {

```
....
174.  $group = $this->groups[array_rand($this->groups)];
```

**Use of Non Cryptographic Random\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=965 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testHasGroup at line 210 of modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php |
| Line | 210 | 210 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php
Method public function testHasGroup() {

```
....
210.  $random_selection = array_rand($this->groups, count($this->groups) / 2);
```

**Use of Non Cryptographic Random\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=966 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testVoteWeightDataType at line 294 of modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php | modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php |
| Line | 294 | 294 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/OgResolvedGroupCollectionTest.php
Method public function testVoteWeightDataType($weight) {

```
....
294.  $group = $this->groups[array_rand($this->groups)];
```

**Use of Non Cryptographic Random\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=967 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 117 of modules/contrib/og/tests/src/Unit/SubscriptionControllerTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/og/tests/src/Unit/SubscriptionControllerTest.php | modules/contrib/og/tests/src/Unit/SubscriptionControllerTest.php |
| Line | 117 | 117 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/og/tests/src/Unit/SubscriptionControllerTest.php
Method protected function setUp(): void {

```
....
117.  $this->userId = rand(20, 50);
```

**Use of Non Cryptographic Random\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=968 |
| Status | New |

| Detection Date | 4/25/2025 1:25:33 PM |
|---|---|

Method redirect_generate_batch_generate at line 103 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 103 | 103 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
103.  $rand = mt_rand(0, 100);
```

**Use of Non Cryptographic Random\Path 26:**

| Severity | Low |
|---|---|
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=969 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 112 of modules/contrib/redirect/redirect.generate.inc uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 112 | 112 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
112.  $redirect_target = 'node/' .
array_rand($context['sandbox']['nids']);
```

**Use of Non Cryptographic Random\Path 27:**

| Severity | Low |
|---|---|

| | |
|---|---|
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=970 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 120 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 120 | 120 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
120.  $redirect_options['fragment'] =
DevelGenerateBase::generateWord(mt_rand(4, 8));
```

**Use of Non Cryptographic Random\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=971 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 125 of modules/contrib/redirect/redirect.generate.inc uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 125 | 125 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
125.  $redirect->setStatusCode($types[array_rand($types)]);
```

**Use of Non Cryptographic Random\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=972 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 129 of modules/contrib/redirect/redirect.generate.inc uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 129 | 129 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
129.  $redirect->setLanguage($languages[array_rand($languages)]);
```

**Use of Non Cryptographic Random\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=973 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 142 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 142 | 142 |
| Object | mt_rand | mt_rand |

| | |
|---|---|
| Code Snippet | |
| File Name | modules/contrib/redirect/redirect.generate.inc |
| Method | function redirect_generate_batch_generate($num, array &$context) { |

```
....
142.  if (mt_rand(0, 1)) {
```

**Use of Non Cryptographic Random\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=974 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 146 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 146 | 146 |
| Object | mt_rand | mt_rand |

| | |
|---|---|
| Code Snippet | |
| File Name | modules/contrib/redirect/redirect.generate.inc |
| Method | function redirect_generate_batch_generate($num, array &$context) { |

```
....
146.  'count' => mt_rand(1, 500),
```

**Use of Non Cryptographic Random\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=975 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method redirect_generate_batch_generate at line 147 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 147 | 147 |

| | | |
|---|---|---|
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function redirect_generate_batch_generate($num, array &$context) {

```
....
147.  'access' => mt_rand(Drupal::time()->getRequestTime() - 31536000,
Drupal::time()->getRequestTime()),
```

**Use of Non Cryptographic Random\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=976 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method _redirect_generate_url at line 183 of modules/contrib/redirect/redirect.generate.inc uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 183 | 183 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function _redirect_generate_url($external = FALSE, $max_levels = 2) {

```
....
183.  $url[] = 'http://www.example.'. $tlds[array_rand($tlds)];
```

**Use of Non Cryptographic Random\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=977 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method _redirect_generate_url at line 185 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |

| | | |
|---|---|---|
| Line | 185 | 185 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function _redirect_generate_url($external = FALSE, $max_levels = 2) {

```
....
185.  $max_levels = mt_rand($external ? 0 : 1, $max_levels);
```

**Use of Non Cryptographic Random\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=978 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method _redirect_generate_url at line 187 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 187 | 187 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function _redirect_generate_url($external = FALSE, $max_levels = 2) {

```
....
187.  $url[] = DevelGenerateBase::generateWord(mt_rand(6 / $i, 8));
```

**Use of Non Cryptographic Random\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=979 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method _redirect_generate_querystring at line 193 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 193 | 193 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function _redirect_generate_querystring() {

```
....
193.  $query = [DevelGenerateBase::generateWord(mt_rand(1, 3)) =>
DevelGenerateBase::generateWord(mt_rand(2, 4))];
```

**Use of Non Cryptographic Random\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=980 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method _redirect_generate_querystring at line 193 of modules/contrib/redirect/redirect.generate.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/redirect.generate.inc | modules/contrib/redirect/redirect.generate.inc |
| Line | 193 | 193 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/redirect.generate.inc
Method function _redirect_generate_querystring() {

```
....
193.  $query = [DevelGenerateBase::generateWord(mt_rand(1, 3)) =>
DevelGenerateBase::generateWord(mt_rand(2, 4))];
```

**Use of Non Cryptographic Random\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=981 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 69 of modules/contrib/redirect/src/Plugin/Field/FieldType/RedirectSourceItem.php uses a weak

method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/src/Plugin/Field/FieldType/RedirectSourceItem.php | modules/contrib/redirect/src/Plugin/Field/FieldType/RedirectSourceItem.php |
| Line | 69 | 69 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/src/Plugin/Field/FieldType/RedirectSourceItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition) {

```
....
69.  $domain_length = mt_rand(7, 15);
```

**Use of Non Cryptographic Random\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=982 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method createVocabulary at line 224 of modules/contrib/redirect/tests/src/Functional/RedirectUITest.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/redirect/tests/src/Functional/RedirectUITest.php | modules/contrib/redirect/tests/src/Functional/RedirectUITest.php |
| Line | 224 | 224 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/redirect/tests/src/Functional/RedirectUITest.php
Method public function createVocabulary() {

```
....
224.  'weight' => mt_rand(0, 10),
```

**Use of Non Cryptographic Random\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=983 |
| Status | New |

| Detection Date | 4/25/2025 1:25:33 PM |
|---|---|

Method testMappingCrudForm at line 68 of modules/contrib/salesforce/modules/salesforce_mapping_ui/src/Tests/SalesforceMappingCrudFormTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/salesforce/modules/salesforce_mapping_ui/src/Tests/SalesforceMappingCrudFormTest.php | modules/contrib/salesforce/modules/salesforce_mapping_ui/src/Tests/SalesforceMappingCrudFormTest.php |
| Line | 68 | 68 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/salesforce/modules/salesforce_mapping_ui/src/Tests/SalesforceMappingCrudFormTest.php
Method public function testMappingCrudForm() {

```
....
68.  $mapping_name = 'mapping' . rand(100, 10000);
```

**Use of Non Cryptographic Random\Path 41:**

| Severity | Low |
|---|---|
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=984 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 111 of modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php | modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php |
| Line | 111 | 111 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php
Method protected function setUp(): void {

```
....
111.  for ($i = 0; $i < mt_rand(1, 3); $i++) {
```

**Use of Non Cryptographic Random\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=985 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method setUp at line 146 of modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php | modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php |
| Line | 146 | 146 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/simple_oauth/tests/src/Functional/TokenBearerFunctionalTestBase.php
Method protected function setUp(): void {

```
....
146.  $num_roles = mt_rand(1, count($this->additionalRoles));
```

**Use of Non Cryptographic Random\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=986 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testMigrateSettings at line 42 of modules/contrib/smtp/tests/src/Kernel/MigrateD7SettingsTest.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/smtp/tests/src/Kernel/MigrateD7SettingsTest.php | modules/contrib/smtp/tests/src/Kernel/MigrateD7SettingsTest.php |
| Line | 42 | 42 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/smtp/tests/src/Kernel/MigrateD7SettingsTest.php

| | |
|---|---|
| Method | public function testMigrateSettings() { |

```
....
42.  $port = strval(rand(1, 65535));
```

**Use of Non Cryptographic Random\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=987 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 451 of modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php | modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php |
| Line | 451 | 451 |
| Object | array_rand | array_rand |

| | |
|---|---|
| Code Snippet | |
| File Name | modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php |
| Method | public static function generateSampleValue(FieldDefinitionInterface $field_definition) { |

```
....
451.  $bundle = array_rand($bundle_ids);
```

**Use of Non Cryptographic Random\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=988 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method generateSampleValue at line 479 of modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php | modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php |
| Line | 479 | 479 |

| | | |
|---|---|---|
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/state_machine/src/Plugin/Field/FieldType/StateItem.php
Method public static function generateSampleValue(FieldDefinitionInterface $field_definition) {

```
....
479.  $random_state = array_rand($states);
```

**Use of Non Cryptographic Random\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=989 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testField at line 91 of modules/contrib/state_machine/tests/src/Kernel/StateItemTest.php uses a weak method array_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/state_machine/tests/src/Kernel/StateItemTest.php | modules/contrib/state_machine/tests/src/Kernel/StateItemTest.php |
| Line | 91 | 91 |
| Object | array_rand | array_rand |

Code Snippet
File Name modules/contrib/state_machine/tests/src/Kernel/StateItemTest.php
Method public function testField($initial_state, $allowed_transitions, $invalid_new_state, $valid_transition, $expected_new_state) {

```
....
91.  $random_key = array_rand($invalid_transitions);
```

**Use of Non Cryptographic Random\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=990 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method testGetInvalidTokens at line 98 of modules/contrib/token/tests/src/Kernel/UnitTest.php uses a weak method shuffle to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | modules/contrib/token/tests/src/Kernel/UnitTest.php | modules/contrib/token/tests/src/Kernel/UnitTest.php |
| Line | 98 | 98 |
| Object | shuffle | shuffle |

Code Snippet
File Name modules/contrib/token/tests/src/Kernel/UnitTest.php
Method public function testGetInvalidTokens() {

```
....
98.  shuffle($tokens);
```

**Use of Non Cryptographic Random\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=991 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method token_tokens at line 1174 of modules/contrib/token/token.tokens.inc uses a weak method mt_rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/token/token.tokens.inc | modules/contrib/token/token.tokens.inc |
| Line | 1174 | 1174 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name modules/contrib/token/token.tokens.inc
Method function token_tokens($type, array $tokens, array $data, array $options, BubbleableMetadata $bubbleable_metadata) {

```
....
1174.  $replacements[$original] = mt_rand();
```

**Use of Non Cryptographic Random\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=992 |
| Status | New |
| Detection Date | 4/25/2025 1:25:33 PM |

Method createTestNodes at line 164 of modules/contrib/views_bulk_operations/tests/src/Kernel/ViewsBulkOperationsKernelTestBase.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/views_bulk_operations/tests/src/Kernel/ViewsBulkOperationsKernelTestBase.php | modules/contrib/views_bulk_operations/tests/src/Kernel/ViewsBulkOperationsKernelTestBase.php |
| Line | 164 | 164 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/views_bulk_operations/tests/src/Kernel/ViewsBulkOperationsKernelTestBase.php
Method protected function createTestNodes(array $test_node_data): void {

```
....
164.  $langcode = $type_data['languages'][\rand(0, $count_languages -
1)];
```

**Use of Non Cryptographic Random\Path 50:**

Severity Low
Result State Confirmed
Online Results https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=993
Status New
Detection Date 4/25/2025 1:25:33 PM

Method castVotes at line 179 of modules/contrib/votingapi/src/Commands/VotingApiCommands.php uses a weak method rand to produce random values. These values might be used as personal identifiers, session tokens or cryptographic input; however, due to their insufficient randomness, an attacker may be able to derive their value.

| | Source | Destination |
|---|---|---|
| File | modules/contrib/votingapi/src/Commands/VotingApiCommands.php | modules/contrib/votingapi/src/Commands/VotingApiCommands.php |
| Line | 179 | 179 |
| Object | rand | rand |

Code Snippet
File Name modules/contrib/votingapi/src/Commands/VotingApiCommands.php
Method protected function castVotes($entity_type, $entity_id, $timestamp = 0, array $uids = [], $style = 'percent') {

```
....
179.  $value = $style === 'points' ? rand(0, 1) ? 1 : -1 : mt_rand(1, 5)
* 20;
```

## Improper Exception Handling

Query Path:
PHP\Cx\PHP Low Visibility\Improper Exception Handling Version:3

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2021: A4-Insecure Design
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Error processing
OWASP ASVS: V14 Configuration
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
ASD STIG 6.1: 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.

*Description*

**Improper Exception Handling\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=19 |
| Status | New |
| Detection Date | 4/25/2025 1:25:26 PM |

The method taxonomymigrate at line 100 of modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php | modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php |
| Line | 100 | 100 |
| Object | json_encode | json_encode |

Code Snippet
File Name modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php
Method public function taxonomymigrate() {

```
....
100.  $encoded_data = base64_encode(json_encode($remap_data));
```

**Improper Exception Handling\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.capgemini.com/CxWebClient/ViewerMain.aspx?scanid=1027535&projectid=996&pathid=638 |
| Status | New |
| Detection Date | 4/25/2025 1:25:26 PM |

The method taxonomy_migration_proceed at line 182 of modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php | modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php |

| | | |
|---|---|---|
| Line | 182 | 182 |
| Object | json_decode | json_decode |

Code Snippet
File Name modules/custom/custom_external_scripts/src/Controller/TaxonomyUpdate.php
Method public function taxonomy_migration_proceed($data) {

```
....
182.  $decoded_data = !empty($data) ? json_decode(base64_decode($data),
TRUE) : '';
```

# HttpOnly Cookie Flag Not Set

## Risk

**What might happen**

Cookies that contain the user's session identifier, and other sensitive application cookies, are typically accessible by client-side scripts, such as JavaScript. Unless the web application explicitly prevents this using the "httpOnly" cookie flag, these cookies could be read and accessed by malicious client scripts, such as Cross-Site Scripting (XSS). This flag would mitigate the damage done in case XSS vulnerabilities are discovered, according to Defense in Depth.
Likewise, sensitive cookies could be exposed by being sent over unprotected HTTP protocol, allowing attackers to sniff the users' requests and impersonate them to the application.

---

## Cause

**How does it happen**

The web application framework, by default, does not set the "httpOnly" flag for the application's sessionid cookie and other sensitive application cookies. Likewise, the application does not explicitly use the "httpOnly" cookie flag, thus allowing client scripts to access the cookies by default.
Similarly, cookies that lack the "secure" flag will be automatically sent by the browser to the web server, regardless of the safety of the underlying protocol, such as unprotected HTTP. Cookies that are flagged with the "secure" attribute will only be sent over a secure HTTPS connection.

---

## General Recommendations

**How to avoid it**

- Always set the "httpOnly" flag for any sensitive server-side cookie. - It is highly recommended to implement HTTP Strict Transport Security (HSTS) in order to ensure that the cookie will be sent over a secured channel. - Explicitly set the "httpOnly" flag for each cookie set by the application. - Configure and set all sensitive cookies to be created with the "secure" attribute.

---

## Source Code Examples

**JavaScript**
**Setting Cookie with Express**

```
var express = require('express');
var app = express();

app.use(express.cookieParser());

app.get('/', function(req, res) {
```

```
      res.cookie('DepartmentID', getUserDept());
      res.send(getUserPage());
});

app.listen(SERVER_PORT);
```

**Using Express for Secure Cookies**

```
var express = require('express');
var app = express();

app.use(express.cookieParser());

app.get('/', function(req, res) {
      res.cookie('DepartmentID', getUserDept(),
                {maxAge: 900000,
                 path: APP_ROOT,
                 secure: true,
                 httpOnly: true });

      res.send(getUserPage());
});

app.listen(SERVER_PORT);
```

# Improper Exception Handling

## Risk

**What might happen**

An attacker could maliciously cause an exception that could crash the application, potentially resulting in a denial of service (DoS) or unexpected behavior under certain erroneous conditions. Exceptions may also occur without any malicious intervention, resulting in general instability.

---

## Cause

**How does it happen**

The application performs some operation, such as database or file access, that could throw an exception. Since the application is not designed to properly handle the exception, the application could crash.

---

## General Recommendations

**How to avoid it**

Any method that could cause an exception should be wrapped in a try-catch block that:

- Explicitly handles expected exceptions
- Includes a default solution to explicitly handle unexpected exceptions

---

## Source Code Examples

**CSharp**

**Always catch exceptions explicitly.**

```
try
{
// Database access or other potentially dangerous function
}
catch (SqlException ex)
{
// Handle exception
}
catch (Exception ex)
{
// Default handler for unexpected exceptions
}
```

**Java**

**Always catch exceptions explicitly.**

```
try
{
// Database access or other potentially dangerous function
}
catch (SQLException ex)
{
// Handle exception
}
catch (Exception ex)
{
```

```
// Default handler for unexpected exceptions
}
```

# Use of Non Cryptographic Random

## Risk

### What might happen

Random values are often used as a mechanism to prevent malicious users from knowing or predicting a given value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values, based on sources often used to derive certain randomness; however, while they may seem random, large statistical samples would demonstrate that they are insufficiently random, producing a much smaller space of possible "random" values than a truly random sample would. This could enable an attacker to derive or guess this value, and thus hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

---

## Cause

### How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values, it would be possible for an attacker to calculate past or future values. Specifically, if this pseudo-random value is used in any security context, such as one-time passwords, keys, secret identifiers or salts - an attacker would likely be able to predict the next value generated and steal it, or guess a previously generated value and spoof its original intent.

---

## General Recommendations

### How to avoid it

- Always use a cryptographically secure pseudo-random number generator, instead of basic random methods, particularly when dealing with a security context
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, thus making brute-force attacks unfeasible.

---

## Source Code Examples

### Java

**Use of a weak pseudo-random number generator**

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

**Cryptographically secure random number generator**

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);
```

```
String sessionId = new String(sessBytes);
```

**Objc**
**Use of a weak pseudo-random number generator**

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

**Cryptographically secure random number generator**

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

**Swift**
**Use of a weak pseudo-random number generator**

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

**Cryptographically secure random number generator**

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

## Scanned Languages

| Language | Hash Number | Change Date |
|---|---|---|
| JavaScript | 0368423245887012 | 4/11/2025 |
| VbScript | 0742915089703437 | 4/11/2025 |
| PHP | 0631115642851010 | 4/11/2025 |
| Common | 3281302260691862 | 4/11/2025 |