171632_epf-cms_retail-service-integration_ICG Scan Report

Project Name	171632_epf-cms_retail-service-integration_ICG
Scan Start	Tuesday, February 17, 2026 10:27:46 AM
Preset	AST - Internet
Scan Time	00h:03m:00s
Lines Of Code Scanned	53955
Files Scanned	616
Report Creation Time	Thursday, February 19, 2026 10:30:54 AM
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917
Team	171632
Checkmarx Version	9.7.3.1000 HF3
Scan Type	Full
Source Origin	LocalPath
Density	5/10000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: Critical, High, Medium, Low, Information

Excluded: None

Result State

Included: To Verify, Not Exploitable, Confirmed, Urgent, Proposed Not Exploitable, Fixed, Proposed Urgent, Proposed Confirmed

Excluded: None

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
OWASP Top 10 API	All
ASD STIG 4.10	All
OWASP Top 10 2021	All
OWASP Top 10 2010	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
Base Preset	All
OWASP Top 10 API 2023	All
PCI DSS v4.0	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
OWASP Top 10 API	None
ASD STIG 4.10	None
OWASP Top 10 2021	None
OWASP Top 10 2010	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
Base Preset	None
OWASP Top 10 API 2023	None

PCI DSS v4.0	None
ASD STIG 6.1	None
OWASP Mobile Top 10 2024	None

Results Limit

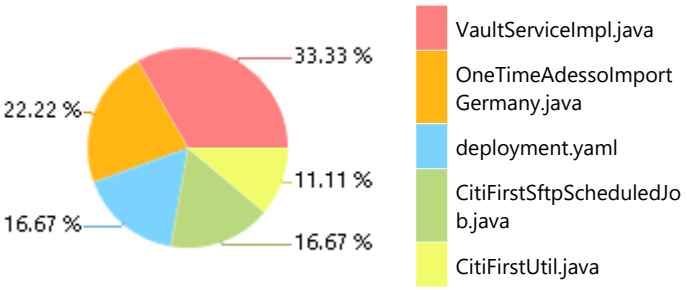
Results limit per query was set to 50

Selected Queries

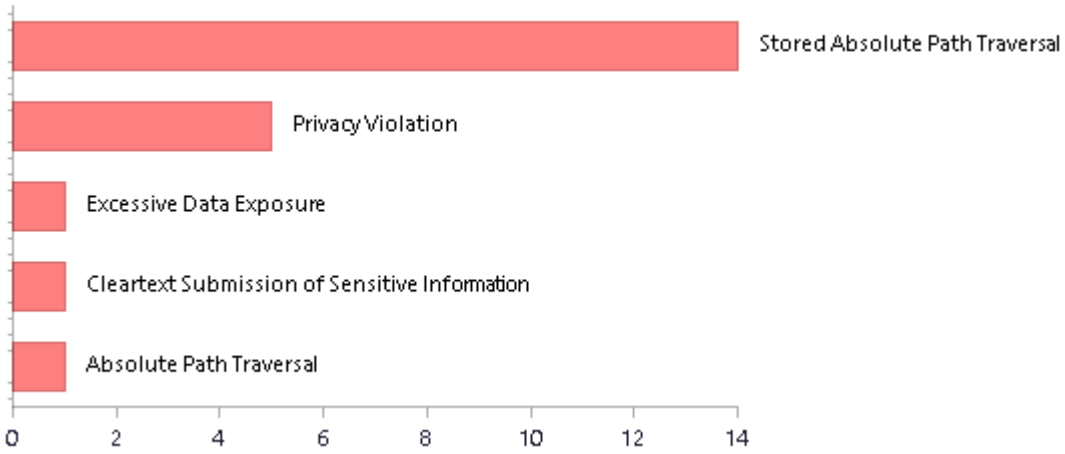
Selected queries are listed in Result Summary

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	0	0
A10-Insufficient Logging & Monitoring*	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* 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*	0	0
A3-Injection*	0	0
A4-Insecure Design*	0	0
A5-Security Misconfiguration*	0	0
A6-Vulnerable and Outdated Components*	0	0
A7-Identification and Authentication Failures*	0	0
A8-Software and Data Integrity Failures*	0	0
A9-Security Logging and Monitoring Failures*	0	0
A10-Server-Side Request Forgery*	0	0

***** 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*	1	1
M2: Inadequate Supply Chain Security*	0	0
M3: Insecure Authentication/Authorization*	0	0
M4: Insufficient Input/Output Validation*	15	9
M5: Insecure Communication*	1	1
M6: Inadequate Privacy Controls*	6	2
M7: Insufficient Binary Protections*	0	0
M8: Security Misconfiguration*	0	0
M9: Insecure Data Storage*	0	0
M10: Insufficient Cryptography*	0	0

* 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

* 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*	0	0
PCI DSS (3.2.1) - 6.5.4 - Insecure communications*	0	0
PCI DSS (3.2.1) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)*	0	0
PCI DSS (3.2.1) - 6.5.8 - Improper access control*	0	0
PCI DSS (3.2.1) - 6.5.9 - Cross-site request forgery*	0	0
PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management*	0	0

***** 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.	0	0
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.	0	0
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

***** 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)*	0	0
SC-4 Information in Shared Resources (P1)*	0	0
SC-5 Denial of Service Protection (P1)*	0	0
SC-8 Transmission Confidentiality and Integrity (P1)*	0	0
SI-10 Information Input Validation (P1)*	0	0
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)*	0	0
SI-16 Memory Protection (P1)*	0	0

***** 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: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -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 application uses, or	0	0

	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

* 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

***** Please note, the report only includes the presets/filters you applied to the scan results.

Scan Summary - Custom

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

Scan Summary - PCI DSS v4.0

Category	Issues Found	Best Fix Locations
PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development*	23	13

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

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

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

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

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

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

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

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

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

***** Please note, the report only includes the presets/filters you applied to the scan results.

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

APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.*	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.*	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.*	1	1
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.*	5	1
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.*	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.*	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0

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

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

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

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

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

***** 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

***** Please note, the report only includes the presets/filters you applied to the scan results.

Scan Summary - OWASP Top 10 API 2023

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization*	0	0
API2-Broken Authentication*	1	1
API3-Broken Object Property Level Authorization*	1	1
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*	1	1

***** 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*	0	0
MOIS(KISA) Security Functions*	6	2
MOIS(KISA) Time and status*	0	0
MOIS(KISA) Verification and representation of input data*	15	9

* 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*	21	11

* 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*	20	10

* 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*	0	0

* 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*	1	1
V03 Session Management*	1	1
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*	1	1
V10 Malicious Code*	5	1
V11 Business Logic*	0	0
V12 Files and Resources*	15	9
V13 API and Web Service*	0	0
V14 Configuration*	0	0

* 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

* 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*	8	4

* Please note, the report only includes the presets/filters you applied to the scan results.

Scan Summary - Base Preset

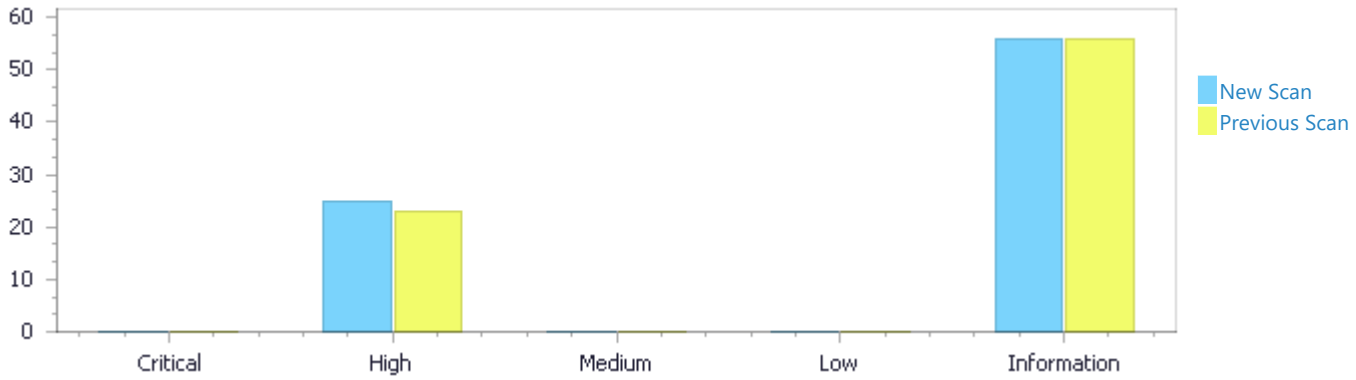
Category	Issues Found	Best Fix Locations
Base Preset*	6	2

* Please note, the report only includes the presets/filters you applied to the scan results.

Results Distribution By Status

Compared to project scan from 2/16/2026 3:11 AM

	Critical	High	Medium	Low	Information	Total
New Issues	0	2	0	0	0	2
Recurrent Issues	0	23	0	0	56	79
Total	0	25	0	0	56	81
Fixed Issues	0	0	0	0	0	0



Results Distribution By State

	Critical	High	Medium	Low	Information	Total
To Verify	0	3	0	0	23	26
Not Exploitable	0	22	0	0	33	55
Confirmed	0	0	0	0	0	0
Urgent	0	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0	0
Fixed	0	0	0	0	0	0
Proposed Urgent	0	0	0	0	0	0
Proposed Confirmed	0	0	0	0	0	0
Total	0	25	0	0	56	81

Result Summary

Vulnerability Type	Occurrences	Severity
Stored Absolute Path Traversal	14	High
Privacy Violation	5	High
Absolute Path Traversal	1	High
Cleartext Submission of Sensitive Information	1	High
Excessive Data Exposure	1	High
Plaintext Storage of a Password	1	High
Plaintext Storage of a Password	1	High
Plaintext Storage of a Password	1	High
Apache Commons Collections Positive	56	Information

10 Most Vulnerable Files

Critical High and Medium Vulnerabilities

File Name	Issues Found
src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	6
src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java	4
helm/templates/deployment.yaml	3
src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java	3
src/main/java/com/citi/rsi/citifirst/util/CitiFirstUtil.java	2
src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java	2
src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java	2
src/main/java/com/citi/rsi/citifirst/service/impl/CsvFileService.java	2
src/main/java/com/citi/rsi/citifirst/job/LegalDocImport.java	1
src/main/java/com/citi/rsd/service/EquityTokenService.java	1

Scan Results Details

Stored Absolute Path Traversal

Query Path:
Java\Corp\Java Medium Threat\Stored Absolute Path Traversal Version:2

Categories

CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V12 Files and Resources
SANS top 25: SANS top 25
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
OWASP Mobile Top 10 2024: M4: Insufficient Input/Output Validation

Description

Stored Absolute Path Traversal\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=6
Status	Recurrent
Detection Date	3/12/2025 5:30:07 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java	src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java
Line	77	77
Object	filePath	readAllBytes

Code Snippet
File Name src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java
Method private List<Map<String, String>> readNavFileFromServer() {

```
....
77.  s3Service.putFileToTargetBucket(bucketName, "NAVUpdate/" +
date_YMD_Str + "/" + fileName.replace(".csv", "_" + date_YMDHMS_Str +
".csv"), java.nio.file.Files.readAllBytes(filePath));
```

Stored Absolute Path Traversal\Path 2:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=7
Status	Recurrent
Detection Date	3/12/2025 5:30:07 AM

	Source	Destination
File	src/main/java/com/citi/srp/controller/SRPConnectController.java	src/main/java/com/citi/srp/controller/SRPConnectController.java
Line	118	118
Object	path	readAllBytes

Code Snippet
File Name src/main/java/com/citi/srp/controller/SRPConnectController.java
Method private String getLastRunDate() throws IOException {

```
....
118.  return new String(Files.readAllBytes(path)).trim();
```

Stored Absolute Path Traversal\Path 3:

Severity	High
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=8
Status	New
Detection Date	2/17/2026 10:30:33 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java
Line	241	244
Object	toFile	delete

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java
Method executorService.submit(() -> {

```
....
241.  File csvFile = filePath.toFile();
....
244.  Files.delete(csvFile.toPath());
```

Stored Absolute Path Traversal\Path 4:

Severity	High
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=9
Status	New
Detection Date	2/17/2026 10:30:33 AM

	Source	Destination

File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java
Line	241	267
Object	toFile	newBufferedReader

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java
Method executorService.submit(() -> {

```
....
241.  File csvFile = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportNetherlands.java
Method private void importToExpiredProductTable(File csvFile, String baseUrl) throws IOException {

```
....
267.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Stored Absolute Path Traversal\Path 5:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=10
Status	Recurrent
Detection Date	12/3/2025 1:09:56 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Line	280	285
Object	toFile	delete

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Method executorService.submit(() -> {

```
....
280.  File csvFile = filePath.toFile();
....
285.  Files.delete(csvFile.toPath());
```

Stored Absolute Path Traversal\Path 6:

Severity	High
Result State	Not Exploitable

Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=11
Status	Recurrent
Detection Date	12/29/2025 6:54:58 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Line	280	428
Object	toFile	newBufferedReader

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Method executorService.submit(() -> {

```
....
280.  File csvFile = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java

Method private void createProductsFromFile(File csvFile, String baseUrl) throws IOException {

```
....
428.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Stored Absolute Path Traversal\Path 7:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=12
Status	Recurrent
Detection Date	12/3/2025 1:09:56 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Line	308	311
Object	toFile	delete

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Method executorService.submit(() -> {

```
....
308.  File csvFile = filePath.toFile();
....
311.  Files.delete(csvFile.toPath());
```

Stored Absolute Path Traversal\Path 8:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=13
Status	Recurrent
Detection Date	12/30/2025 10:25:34 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java
Line	308	334
Object	toFile	newBufferedReader

Code Snippet

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java

Method executorService.submit(() -> {

```
....
308.  File csvFile = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportGermany.java

Method private void importToExpiredProductTable(File csvFile, String baseUrl) throws IOException {

```
....
334.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Stored Absolute Path Traversal\Path 9:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=14
Status	Recurrent
Detection Date	1/12/2026 6:04:44 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java

Line	59	160
Object	toFile	newBufferedReader

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java
Method public void processFiles(@PathVariable String countryCode) {

```
....
59.  File file = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java

Method public StrikeKoHistoryWrapper createStrikeAndKoHistory(File csvFile) throws IOException {

```
....
160.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Stored Absolute Path Traversal\Path 10:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=15
Status	Recurrent
Detection Date	11/25/2025 12:19:07 PM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java
Line	59	112
Object	toFile	delete

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java
Method public void processFiles(@PathVariable String countryCode) {

```
....
59.  File file = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeStrikeImport.java

Method filesToDelete.forEach(file -> {

```
....
112.  Files.delete(file.toPath());
```

Stored Absolute Path Traversal\Path 11:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=16
Status	Recurrent
Detection Date	1/12/2026 6:04:44 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportPortugal.java	src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportPortugal.java
Line	246	285
Object	toFile	newBufferedReader

Code Snippet

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportPortugal.java

Method executorService.submit(() -> {

```
....
246.  File csvFile = filePath.toFile();
```

File Name src/main/java/com/citi/rsi/citifirst/job/OneTimeAdessoImportPortugal.java

Method private List<ExpiredProductsCitiFirst> createProductsFromFile(File csvFile, String baseUrl) throws IOException {

```
....
285.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Stored Absolute Path Traversal\Path 12:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=17
Status	Recurrent
Detection Date	11/25/2025 12:19:07 PM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java	src/main/java/com/citi/rsi/citifirst/util/CitiFirstUtil.java
Line	44	174
Object	toFile	readAllBytes

Code Snippet

File Name src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java
Method public void watchSftpFolder() {

```
....
44.  processFile(filePath.toFile());
```

File Name src/main/java/com/citi/rsi/citifirst/util/CitiFirstUtil.java

Method public byte[] readFileToByteArray(File file) {

```
....
174.  return Files.readAllBytes(file.toPath());
```

Stored Absolute Path Traversal\Path 13:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=18
Status	Recurrent
Detection Date	11/25/2025 12:19:07 PM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java	src/main/java/com/citi/rsi/citifirst/service/impl/CsvFileService.java
Line	44	87
Object	toFile	newBufferedReader

Code Snippet
File Name src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java
Method public void watchSftpFolder() {

```
....
44.  processFile(filePath.toFile());
```

File Name src/main/java/com/citi/rsi/citifirst/service/impl/CsvFileService.java

Method private void handleDelistingAndKO(File file) throws IOException {

```
....
87.  try (Reader reader = Files.newBufferedReader(file.toPath())) {
```

Stored Absolute Path Traversal\Path 14:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=19

Status	Recurrent
Detection Date	1/28/2026 2:30:14 PM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java	src/main/java/com/citi/rsi/citifirst/service/impl/CsvFileService.java
Line	44	186
Object	toFile	newBufferedReader

Code Snippet

File Name src/main/java/com/citi/rsi/citifirst/service/CitiFirstSftpScheduledJob.java

Method public void watchSftpFolder() {

```
....
44.  processFile(filePath.toFile());
```

File Name src/main/java/com/citi/rsi/citifirst/service/impl/CsvFileService.java

Method private List<CitiFirstPrice> createPriceFromFileForTimeSeries(File csvFile) throws IOException {

```
....
186.  try (Reader reader = Files.newBufferedReader(csvFile.toPath())) {
```

Privacy Violation

Query Path:
Java\Corp\Java Medium Threat\Privacy Violation Version:10

Categories

CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V10 Malicious Code
SANS top 25: SANS top 25
ASA Premium: ASA Premium
Base Preset: Base Preset
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
ASD STIG 6.1: 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.
OWASP Mobile Top 10 2024: M6: Inadequate Privacy Controls

Description

Privacy Violation\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=20
Status	Recurrent
Detection Date	4/23/2025 8:46:05 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Line	147	117
Object	secretId	error

Code Snippet
File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Method private String getSecretId() {

```
....
147.  return secretId;
```

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private int getSecretIdLiveDays() {

```
....
117.  log.error("Failed to parse creation_time from response: {}",
responseJson, e);
```

Privacy Violation\Path 2:

Severity High
Result State Not Exploitable
Online Results https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=21
Status Recurrent
Detection Date 4/23/2025 8:46:05 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Line	147	118
Object	secretId	BusinessException

Code Snippet
File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Method private String getSecretId() {

```
....
147.  return secretId;
```

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method	private int getSecretIdLiveDays() {

```
....
118.  throw new BusinessException("Failed to parse creation_time from
response: {}", responseJson, e);
```

Privacy Violation\Path 3:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=22
Status	Recurrent
Detection Date	4/23/2025 8:46:05 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Line	147	90
Object	secretId	write

Code Snippet

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private String getSecretId() {

```
....
147.  return secretId;
```

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private void updateSecretId() {

```
....
90.  Files.write(Paths.get(secretIdPath),
newSecretId.getBytes(StandardCharsets.UTF_8));
```

Privacy Violation\Path 4:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=23
Status	Recurrent
Detection Date	4/23/2025 8:46:05 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Line	128	117
Object	getSecretId	error

Code Snippet

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private String generateAppRoleLoginToken() {

```
....
128.  String secretId = getSecretId();
```

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private int getSecretIdLiveDays() {

```
....
117.  log.error("Failed to parse creation_time from response: {}",
responseJson, e);
```

Privacy Violation\Path 5:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=24
Status	Recurrent
Detection Date	4/23/2025 8:46:05 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Line	128	118
Object	getSecretId	BusinessException

Code Snippet

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private String generateAppRoleLoginToken() {

```
....
128.  String secretId = getSecretId();
```

File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java

Method private int getSecretIdLiveDays() {

```
....
118.  throw new BusinessException("Failed to parse creation_time from
response: {}", responseJson, e);
```

Absolute Path Traversal

Query Path:
Java\Corp\Java High Risk\Absolute Path Traversal Version:1

Categories

CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V12 Files and Resources
SANS top 25: SANS top 25
ASA Premium: ASA Premium
Base Preset: Base Preset
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
ASD STIG 6.1: APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.
OWASP Mobile Top 10 2024: M4: Insufficient Input/Output Validation

Description

Absolute Path Traversal\Path 1:

Severity	High
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=1
Status	Recurrent
Detection Date	2/16/2026 3:13:36 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citifirst/job/LegalDocImport.java	src/main/java/com/citi/rsi/citifirst/util/CitiFirstUtil.java
Line	81	251
Object	countryCode	File

Code Snippet

File Name src/main/java/com/citi/rsi/citifirst/job/LegalDocImport.java

Method public String importLegalDoc(@PathVariable("countryCode") String countryCode, @RequestParam("file") MultipartFile file) {

```
....
81.  public String importLegalDoc(@PathVariable("countryCode") String
countryCode, @RequestParam("file") MultipartFile file) {
```

File Name src/main/java/com/citi/rsi/citifirst/util/CitiFirstUtil.java

Method public void writeRecordsToExcel(List<Map<String, String>> excelRecords, String errorFileName) throws IOException {

```
....
251.  File errorFile = new File(ERROR_DIRECTORY + errorFileName);
```

Plaintext Storage of a Password

Query Path:
Kotlin\Corp\Kotlin Medium Threat\Plaintext Storage of a Password Version:2

Description

Plaintext Storage of a Password\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=2
Status	Recurrent
Detection Date	12/9/2025 1:00:45 PM

	Source	Destination
File	helm/templates/deployment.yaml	helm/templates/deployment.yaml
Line	19	19
Object	secrets:	secrets:

Code Snippet
File Name helm/templates/deployment.yaml
Method ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName }}

```
....
19.  ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName
}}
```

Excessive Data Exposure

Query Path:
Java\Corp\Java Medium Threat\Excessive Data Exposure Version:1

Categories

OWASP ASVS: V03 Session Management
OWASP Top 10 API 2023: API3-Broken Object Property Level Authorization
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
OWASP Mobile Top 10 2024: M6: Inadequate Privacy Controls

Description

Excessive Data Exposure\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=3
Status	Recurrent
Detection Date	4/23/2025 8:46:01 AM

	Source	Destination
File	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java	src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Line	90	90
Object	secretIdPath	secretIdPath

Code Snippet
File Name src/main/java/com/citi/san/vault/service/impl/VaultServiceImpl.java
Method private void updateSecretId() {

```
....
90.  Files.write(Paths.get(secretIdPath),
newSecretId.getBytes(StandardCharsets.UTF_8));
```

Plaintext Storage of a Password

Query Path:
Groovy\Corp\Groovy Medium Threat\Plaintext Storage of a Password Version:2

Description

Plaintext Storage of a Password\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=4
Status	Recurrent
Detection Date	12/7/2025 3:53:51 PM

	Source	Destination
File	helm/templates/deployment.yaml	helm/templates/deployment.yaml
Line	19	19
Object	secrets:	secrets:

Code Snippet
File Name helm/templates/deployment.yaml
Method ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName }}

```
....
19.  ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName
}}
```

Cleartext Submission of Sensitive Information

Query Path:
Java\Corp\Java High Risk\Cleartext Submission of Sensitive Information Version:1

Categories

MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V09 Communication

SANS top 25: SANS top 25
ASA Premium: ASA Premium
OWASP Top 10 API 2023: API10-Unsafe Consumption of APIs
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
ASD STIG 6.1: APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.
OWASP Mobile Top 10 2024: M5: Insecure Communication

Description

Cleartext Submission of Sensitive Information\Path 1:

Severity	High
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=5
Status	Recurrent
Detection Date	3/12/2025 5:30:06 AM

	Source	Destination
File	src/main/java/com/citi/rsd/service/EquityTokenService.java	src/main/java/com/citi/rsd/service/EquityTokenService.java
Line	64	84
Object	secret_key	build

Code Snippet
File Name src/main/java/com/citi/rsd/service/EquityTokenService.java
Method public Token getToken() {

```
....
64.  "&client_secret=" + secret_key +
....
84.  .build();
```

Plaintext Storage of a Password

Query Path:
Java\Corp\Java Medium Threat\Plaintext Storage of a Password Version:20

Categories

OWASP ASVS: V02 Authentication
ASA Premium: ASA Premium
OWASP Top 10 API 2023: API2-Broken Authentication
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
ASD STIG 6.1: APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.
OWASP Mobile Top 10 2024: M1: Improper Credential Usage

Description

Plaintext Storage of a Password\Path 1:

Severity	High
Result State	Not Exploitable

Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=25
Status	Recurrent
Detection Date	3/12/2025 5:30:11 AM

	Source	Destination
File	helm/templates/deployment.yaml	helm/templates/deployment.yaml
Line	19	19
Object	secrets:	secrets:

Code Snippet
File Name helm/templates/deployment.yaml
Method ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName }}

```
....
19.  ecs.o2c/retail-content-service.secrets: {{ .Values.secret.nickName
}}
```

Apache Commons Collections Positive

Query Path:
Java\Corp\Team6 Custom Intel\Apache Commons Collections Positive Version:1

Description

Apache Commons Collections Positive\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=26
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/cma/kafka/handler/AbstractAuditHandler.java	src/main/java/com/citi/cma/kafka/handler/AbstractAuditHandler.java
Line	14	14
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/cma/kafka/handler/AbstractAuditHandler.java
Method import org.apache.commons.collections4.MapUtils;

```
....
14.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 2:

Severity	Information

Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=27
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/common/utils/AkamaiFastPurgeUtil.java	src/main/java/com/citi/common/utils/AkamaiFastPurgeUtil.java
Line	12	12
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/common/utils/AkamaiFastPurgeUtil.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
12.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=28
Status	Recurrent
Detection Date	4/14/2025 4:34:00 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/common/impl/CommonServiceImpl.java	src/main/java/com/citi/dataScan/service/common/impl/CommonServiceImpl.java
Line	13	13
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/common/impl/CommonServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
13.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 4:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=29

Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/dataRemove/impl/AbstractRemoveServiceImpl.java	src/main/java/com/citi/dataScan/service/dataRemove/impl/AbstractRemoveServiceImpl.java
Line	16	16
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/dataRemove/impl/AbstractRemoveServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
16.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 5:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=30
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/dataRemove/impl/ContentRemoveServiceImpl.java	src/main/java/com/citi/dataScan/service/dataRemove/impl/ContentRemoveServiceImpl.java
Line	9	9
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/dataRemove/impl/ContentRemoveServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
9.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=31
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/dataRemove/impl/PageRemoveServiceImpl.java	src/main/java/com/citi/dataScan/service/dataRemove/impl/PageRemoveServiceImpl.java
Line	9	9
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/dataRemove/impl/PageRemoveServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
9.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 7:

Severity Information
Result State To Verify
Online Results https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=32
Status Recurrent
Detection Date 4/14/2025 4:34:00 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/impl/CommonVersionCompareServiceImpl.java	src/main/java/com/citi/dataScan/service/impl/CommonVersionCompareServiceImpl.java
Line	23	23
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/impl/CommonVersionCompareServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
23.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 8:

Severity Information
Result State Not Exploitable
Online Results https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=33
Status Recurrent
Detection Date 3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/impl/	src/main/java/com/citi/dataScan/service/impl/

	VersionCompareServiceImpl.java	VersionCompareServiceImpl.java
Line	20	20
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/impl/VersionCompareServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
20.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 9:

Severity Information
Result State Not Exploitable
Online Results https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=34
Status Recurrent
Detection Date 3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/dataScan/service/impl/VersionCompareServiceImpl.java	src/main/java/com/citi/dataScan/service/impl/VersionCompareServiceImpl.java
Line	21	21
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/dataScan/service/impl/VersionCompareServiceImpl.java
Method import org.apache.commons.collections4.MapUtils;

```
....
21.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 10:

Severity Information
Result State Not Exploitable
Online Results https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=35
Status Recurrent
Detection Date 3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ems/jobs/MarkOverdueQuestionJob.java	src/main/java/com/citi/ems/jobs/MarkOverdueQuestionJob.java
Line	9	9

Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/ems/jobs/MarkOverdueQuestionJob.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
9.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 11:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=36
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ems/jobs/OnboardingReviewReminderJob.java	src/main/java/com/citi/ems/jobs/OnboardingReviewReminderJob.java
Line	9	9
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/ems/jobs/OnboardingReviewReminderJob.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
9.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 12:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=37
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ems/service/email/impl/EmailServiceImpl.java	src/main/java/com/citi/ems/service/email/impl/EmailServiceImpl.java
Line	11	11
Object	collections4	collections4

Code Snippet	
File Name	src/main/java/com/citi/ems/service/email/impl/EmailServiceImpl.java
Method	import org.apache.commons.collections4.CollectionUtils;

```
....
11.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 13:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=38
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ems/service/impl/ApprovalMailServiceImpl.java	src/main/java/com/citi/ems/service/impl/ApprovalMailServiceImpl.java
Line	11	11
Object	collections4	collections4

Code Snippet	
File Name	src/main/java/com/citi/ems/service/impl/ApprovalMailServiceImpl.java
Method	import org.apache.commons.collections4.CollectionUtils;

```
....
11.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 14:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=39
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ems/service/impl/OnboardingMailServiceImpl.java	src/main/java/com/citi/ems/service/impl/OnboardingMailServiceImpl.java
Line	7	7
Object	collections4	collections4

Code Snippet	
File Name	src/main/java/com/citi/ems/service/impl/OnboardingMailServiceImpl.java
Method	import org.apache.commons.collections4.CollectionUtils;

```
....
7.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 15:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=40
Status	Recurrent
Detection Date	5/14/2025 8:30:04 AM

	Source	Destination
File	src/main/java/com/citi/msg/ckcSyncTTS/service/CKCSyncTTSService.java	src/main/java/com/citi/msg/ckcSyncTTS/service/CKCSyncTTSService.java
Line	25	25
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/ckcSyncTTS/service/CKCSyncTTSService.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
25.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 16:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=41
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/elasticsearch/feed/service/impl/ESSearchFeedContentService.java	src/main/java/com/citi/msg/elasticsearch/feed/service/impl/ESSearchFeedContentService.java
Line	31	31
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/elasticsearch/feed/service/impl/ESSearchFeedContentService.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
31.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 17:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=42
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/elasticsearch/retry/service/impl/ESRefreshStatusServiceImpl.java	src/main/java/com/citi/msg/elasticsearch/retry/service/impl/ESRefreshStatusServiceImpl.java
Line	8	8
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/elasticsearch/retry/service/impl/ESRefreshStatusServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
8.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 18:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=43
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/llm/service/impl/TtsFaqPdfGenerationService.java	src/main/java/com/citi/msg/llm/service/impl/TtsFaqPdfGenerationService.java
Line	6	6
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/llm/service/impl/TtsFaqPdfGenerationService.java
Method import org.apache.commons.collections4.MapUtils;

```
....
6.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 19:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=44
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/llm/service/impl/TtsPdfServiceImpl.java	src/main/java/com/citi/msg/llm/service/impl/TtsPdfServiceImpl.java
Line	25	25
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/llm/service/impl/TtsPdfServiceImpl.java
Method import org.apache.commons.collections4.MapUtils;

```
....
25.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 20:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=45
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/llm/service/impl/TtsUserGuidePdfGenerationService.java	src/main/java/com/citi/msg/llm/service/impl/TtsUserGuidePdfGenerationService.java
Line	6	6
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/llm/service/impl/TtsUserGuidePdfGenerationService.java
Method import org.apache.commons.collections4.MapUtils;

```
....
6.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 21:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=46
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/reflinkscheck/consumer/AbstractCheckConsumer.java	src/main/java/com/citi/msg/reflinkscheck/consumer/AbstractCheckConsumer.java
Line	25	25
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/reflinkscheck/consumer/AbstractCheckConsumer.java
Method import org.apache.commons.collections4.MapUtils;

```
....
25.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 22:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=47
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/reflinkscheck/consumer/PageCheckConsumer.java	src/main/java/com/citi/msg/reflinkscheck/consumer/PageCheckConsumer.java
Line	158	158
Object	commons	commons

Code Snippet
File Name src/main/java/com/citi/msg/reflinkscheck/consumer/PageCheckConsumer.java
Method private void getAllPortletIds(List<Row> rows, List<String> portletList) {

```
....
158.  if (org.apache.commons.collections4.CollectionUtils.isEmpty(rows))
{
```

Apache Commons Collections Positive\Path 23:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=48
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/reflinkscheck/service/impl/PortletServiceImpl.java	src/main/java/com/citi/msg/reflinkscheck/service/impl/PortletServiceImpl.java
Line	11	11
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/reflinkscheck/service/impl/PortletServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
11.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 24:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=49
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/CcbFeedContentServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/CcbFeedContentServiceImpl.java
Line	30	30
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/CcbFeedContentServiceImpl.java
Method import org.apache.commons.collections4.MapUtils;

```
....
30.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 25:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=50
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/ContentFilterServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/ContentFilterServiceImpl.java
Line	12	12
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/ContentFilterServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
12.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 26:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=51
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java
Line	8	8
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
8.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 27:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=52
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java
Line	9	9
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/EventServiceImpl.java
Method import org.apache.commons.collections4.MapUtils;

```
....
9.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 28:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=53
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/InsightsServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/InsightsServiceImpl.java
Line	10	10
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/InsightsServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
10.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 29:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=54
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/KXCServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/KXCServiceImpl.java
Line	12	12
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/KXCServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
12.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 30:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=55
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/PublicEventServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/PublicEventServiceImpl.java
Line	10	10
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/PublicEventServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
10.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 31:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=56
Status	Recurrent
Detection Date	4/2/2025 10:24:44 PM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataAssetConverterServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataAssetConverterServiceImpl.java
Line	11	11
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataAssetConverterServiceImpl.java

Method import org.apache.commons.collections4.MapUtils;

```
....
11.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 32:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=57
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataConverterServiceImpl.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataConverterServiceImpl.java
Line	12	12
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SearchDataConverterServiceImpl.java

Method import org.apache.commons.collections4.MapUtils;

```
....
12.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 33:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=58
Status	Recurrent
Detection Date	4/2/2025 10:24:44 PM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedAssetService.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedAssetService.java
Line	26	26
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedAssetService.java
Method import org.apache.commons.collections4.MapUtils;

```
....
26.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 34:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=59
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java
Line	30	30
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
30.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 35:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=60
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java
Line	31	31
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedContentService.java
Method import org.apache.commons.collections4.MapUtils;

```
....
31.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 36:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=61
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedPageService.java	src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedPageService.java
Line	26	26
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/service/impl/SolrSearchFeedPageService.java
Method import org.apache.commons.collections4.MapUtils;

```
....
26.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 37:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=62
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java	src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java
Line	13	13
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
13.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 38:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=63
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java	src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java
Line	14	14
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/msg/solrsearchfeed/utils/SolrDataConvertUtil.java
Method import org.apache.commons.collections4.MapUtils;

```
....
14.  import org.apache.commons.collections4.MapUtils;
```

Apache Commons Collections Positive\Path 39:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=64
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java	src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java
Line	17	17
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/rsi/citiFunds/service/impl/NavServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
17.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 40:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=65
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/rsi/service/impl/KalturaServiceImpl.java	src/main/java/com/citi/rsi/service/impl/KalturaServiceImpl.java
Line	21	21
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/rsi/service/impl/KalturaServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
21.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 41:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=66
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/san/alertNotification/service/impl/RetailMessageStatusServiceImpl.java	src/main/java/com/citi/san/alertNotification/service/impl/RetailMessageStatusServiceImpl.java
Line	13	13
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/san/alertNotification/service/impl/RetailMessageStatusServiceImpl.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
13.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 42:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=67
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/san/alertNotification/service/impl/SSGErrorAlertServiceImpl.java	src/main/java/com/citi/san/alertNotification/service/impl/SSGErrorAlertServiceImpl.java
Line	20	20
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/san/alertNotification/service/impl/SSGErrorAlertServiceImpl.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
20.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 43:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=68
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/san/assetStatusNullScan/scanController.java	src/main/java/com/citi/san/assetStatusNullScan/scanController.java
Line	7	7
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/san/assetStatusNullScan/scanController.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
7.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 44:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=69
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/san/cachecompare/model/CacheCompareResult.java	src/main/java/com/citi/san/cachecompare/model/CacheCompareResult.java
Line	6	6
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/san/cachecompare/model/CacheCompareResult.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
6.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 45:

Severity	Information
Result State	To Verify
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=70
Status	Recurrent
Detection Date	4/28/2025 5:30:15 AM

	Source	Destination
File	src/main/java/com/citi/san/stagingRequest/service/impl/WorkflowConfigurationServiceImpl.java	src/main/java/com/citi/san/stagingRequest/service/impl/WorkflowConfigurationServiceImpl.java
Line	12	12
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/san/stagingRequest/service/impl/WorkflowConfigurationServiceImpl.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
12.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 46:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=71
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ssg/common/kafka/AbstractSsgKafkaConsumer.java	src/main/java/com/citi/ssg/common/kafka/AbstractSsgKafkaConsumer.java
Line	35	35
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/ssg/common/kafka/AbstractSsgKafkaConsumer.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
35.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 47:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=72
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ssg/common/service/refreshstatus/impl/PageRefreshStatusServiceImpl.java	src/main/java/com/citi/ssg/common/service/refreshstatus/impl/PageRefreshStatusServiceImpl.java
Line	14	14
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/ssg/common/service/refreshstatus/impl/PageRefreshStatusServiceImpl.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
14.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 48:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=73
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ssg/common/service/resource/impl/ContentServiceImpl.java	src/main/java/com/citi/ssg/common/service/resource/impl/ContentServiceImpl.java
Line	17	17
Object	collections4	collections4

Code Snippet

File Name src/main/java/com/citi/ssg/common/service/resource/impl/ContentServiceImpl.java

Method import org.apache.commons.collections4.CollectionUtils;

```
....
17.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 49:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=74
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ssg/common/service/resource/impl/PageServiceImpl.java	src/main/java/com/citi/ssg/common/service/resource/impl/PageServiceImpl.java
Line	14	14
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/ssg/common/service/resource/impl/PageServiceImpl.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
14.  import org.apache.commons.collections4.CollectionUtils;
```

Apache Commons Collections Positive\Path 50:

Severity	Information
Result State	Not Exploitable
Online Results	https://securecodeanalysis01.citigroup.net/CxWebClient/ViewerMain.aspx?scanid=8996657&projectid=178917&pathid=75
Status	Recurrent
Detection Date	3/12/2025 5:30:14 AM

	Source	Destination
File	src/main/java/com/citi/ssg/features/purgecache/akamai/AkamaiFastPurgeService.java	src/main/java/com/citi/ssg/features/purgecache/akamai/AkamaiFastPurgeService.java
Line	17	17
Object	collections4	collections4

Code Snippet
File Name src/main/java/com/citi/ssg/features/purgecache/akamai/AkamaiFastPurgeService.java
Method import org.apache.commons.collections4.CollectionUtils;

```
....
17.  import org.apache.commons.collections4.CollectionUtils;
```

Absolute Path Traversal

Weakness ID: 36 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly sanitize absolute path sequences such as "/abs/path" that can resolve to a location that is outside of that directory.

Extended Description

This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

In the example below, the path to a dictionary file is read from a system property and used to initialize a File object.

(Bad Code)

Example Language: **Java**

```
String filename = System.getProperty("com.domain.application.dictionaryFile");
File dictionaryFile = new File(filename);
```

However, the path is not sanitized before creating the File object. This allows anyone who can control the system property to determine what file is used. Ideally, the path should be resolved relative to some kind of application or user home directory.

Potential Mitigations

see "Path Traversal" (CWE-22)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	37	Path Traversal: '/absolute/pathname/here'	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	38	Path Traversal: '\absolute\pathname\here'	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	39	Path Traversal: 'C:dirname'	**Development Concepts**

				(primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	40	Path Traversal: '\\UNC\share\name\' (Windows UNC Share)	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Absolute Path Traversal

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

BACK TO TOP

Plaintext Storage of a Password

Weakness ID: 256 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

Storing a password in plaintext may result in a system compromise.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

All

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following code reads a password from a properties file and uses the password to connect to a database.

(Bad Code)

Example Language: **Java**

```
...
Properties prop = new Properties();
prop.load(new FileInputStream("config.properties"));
String password = prop.getProperty("password");
DriverManager.getConnection(url, usr, password);
...
```

This code will run successfully, but anyone who has access to config.properties can read the value of password. If a devious employee has access to this information, they can use it to break into the system.

Example 2

The following code reads a password from the registry and uses the password to create a new network credential.

(Bad Code)

Example Language: **Java**

```
...
String password = regKey.GetValue(passKey).toString();
NetworkCredential netCred = new NetworkCredential(username,password,domain);
...
```

This code will run successfully, but anyone who has access to the registry key used to store the password can read the value of password. If a devious employee has access to this information, they can use it to break into the system

Potential Mitigations

Avoid storing passwords in easily accessible locations.

Consider storing cryptographic hashes of passwords as an alternative to storing in plaintext.

Other Notes

Password management issues occur when a password is stored in plaintext in an application's properties or configuration file. A programmer can attempt to remedy the password management problem by obscuring the password with an encoding function, such as base 64 encoding, but this effort does not adequately protect the password. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's

job easier. Good password management guidelines require that a password never be stored in plaintext.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	522	Insufficiently Protected Credentials	**Development Concepts (primary)699 Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Password Management

References

J. Viega and G. McGraw. "Building Secure Software: How to Avoid Security Problems the Right Way". 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-01-30	Plaintext Storage		

BACK TO TOP

Information Leak Through Sent Data

Weakness ID: 201 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The accidental leaking of sensitive information through sent data refers to the transmission of data which are either sensitive in and of itself or useful in the further exploitation of the system through standard data channels.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Confidentiality	Data leakage results in the compromise of data confidentiality.

Demonstrative Examples

Example 1

The following is an actual mysql error statement:

(Result)

Example Language: **SQL**

```
Warning: mysql_pconnect(): Access denied for user: 'root@localhost' (Using password: N1nj4) in /usr/local/www/wi-data/includes/database.inc on line 4
```

Potential Mitigations

Requirements specification: Specify data output such that no sensitive data is sent.

Phase: Implementation

Ensure that any possibly sensitive data specified in the requirements is verified with designers to ensure that it is either a calculated risk or mitigated elsewhere. Any information that is not necessary to the functionality should be removed in order to lower both the overhead and the possibility of security sensitive data being sent.

Compartmentalize your system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Setup default error message to handle unexpected errors.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	200	Information Exposure	**Development Concepts (primary)699 Research Concepts (primary)1000**
CanAlsoBe	Weakness Variant	202	Privacy Leak through Data Queries	Research Concepts1000
CanAlsoBe	Weakness Base	209	Information Exposure Through an Error Message	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Accidental leaking of sensitive information through sent data

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
12	Choosing a Message/Channel Identifier on a Public/Multicast Channel	

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes, Potential Mitigations		

BACK TO TOP

Plaintext Storage of a Password

Weakness ID: 256 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

Storing a password in plaintext may result in a system compromise.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

All

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following code reads a password from a properties file and uses the password to connect to a database.

(Bad Code)

Example Language: **Java**

```
...
Properties prop = new Properties();
prop.load(new FileInputStream("config.properties"));
String password = prop.getProperty("password");
DriverManager.getConnection(url, usr, password);
...
```

This code will run successfully, but anyone who has access to config.properties can read the value of password. If a devious employee has access to this information, they can use it to break into the system.

Example 2

The following code reads a password from the registry and uses the password to create a new network credential.

(Bad Code)

Example Language: **Java**

```
...
String password = regKey.GetValue(passKey).toString();
NetworkCredential netCred = new NetworkCredential(username,password,domain);
...
```

This code will run successfully, but anyone who has access to the registry key used to store the password can read the value of password. If a devious employee has access to this information, they can use it to break into the system

Potential Mitigations

Avoid storing passwords in easily accessible locations.

Consider storing cryptographic hashes of passwords as an alternative to storing in plaintext.

Other Notes

Password management issues occur when a password is stored in plaintext in an application's properties or configuration file. A programmer can attempt to remedy the password management problem by obscuring the password with an encoding function, such as base 64 encoding, but this effort does not adequately protect the password. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's

job easier. Good password management guidelines require that a password never be stored in plaintext.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	522	Insufficiently Protected Credentials	**Development Concepts (primary)699 Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Password Management

References

J. Viega and G. McGraw. "Building Secure Software: How to Avoid Security Problems the Right Way". 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-01-30	Plaintext Storage		

BACK TO TOP

Cleartext Transmission of Sensitive Information

Weakness ID: 319 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Extended Description

Many communication channels can be "sniffed" by attackers during data transmission. For example, network traffic can often be sniffed by any attacker who has access to a network interface. This significantly lowers the difficulty of exploitation by attackers.

Time of Introduction

- Architecture and Design
- Operation
- System Configuration

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Confidentiality	Anyone can read the information by gaining access to the channel being used for communication.

Likelihood of Exploit

Medium to High

Observed Examples

Reference	Description
CVE-2002-1949	Passwords transmitted in cleartext.
CVE-2008-4122	Chain: failure to set "secure" flag in HTTPS cookie causes it to be transmitted across unencrypted HTTP.
CVE-2008-3289	Product sends password hash in cleartext in violation of intended policy.
CVE-2008-4390	Remote management feature sends sensitive information including passwords in cleartext.
CVE-2007-5626	Backup routine sends password in cleartext in email.
CVE-2004-1852	Product transmits Blowfish encryption key in cleartext.
CVE-2008-0374	Printer sends configuration information, including administrative password, in cleartext.
CVE-2007-4961	Chain: cleartext transmission of the MD5 hash of password enables attacks against a server that is susceptible to replay (CWE-294).
CVE-2007-4786	Product sends passwords in cleartext to a log server.
CVE-2005-3140	Product sends file with cleartext passwords in e-mail message intended for diagnostic purposes.

Potential Mitigations

Phase: Architecture and Design

Encrypt the data with a reliable encryption scheme before transmitting.

Phase: Implementation

When using web applications with SSL, use SSL for the entire session from login to logout, not just for the initial login page.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process, trigger the feature that sends the data, and look for the presence or absence of common cryptographic functions in the call tree. Monitor the network and determine if the data packets contain readable commands. Tools exist for detecting if certain encodings are in use. If the traffic contains high entropy, this might indicate the usage of encryption.

Phase: Operation

Configure servers to use encrypted channels for communication, which may include SSL or other secure protocols.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	311	Missing Encryption of Sensitive Data	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ParentOf	Weakness Variant	5	J2EE Misconfiguration: Data Transmission Without Encryption	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Plaintext Transmission of Sensitive Information

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
65	Passively Sniff and Capture Application Code Bound for Authorized Client	
102	Session Sidejacking	

References

OWASP. "Top 10 2007-Insecure Communications". <http://www.owasp.org/index.php/Top_10_2007-A9>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 9, "Protecting Secret Data" Page 299. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Observed Examples, Potential Mitigations, References, Relationships		

2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Time of Introduction		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Plaintext Transmission of Sensitive Information

BACK TO TOP

Absolute Path Traversal

Weakness ID: 36 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly sanitize absolute path sequences such as "/abs/path" that can resolve to a location that is outside of that directory.

Extended Description

This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

In the example below, the path to a dictionary file is read from a system property and used to initialize a File object.

(Bad Code)

Example Language: **Java**

```
String filename = System.getProperty("com.domain.application.dictionaryFile");
File dictionaryFile = new File(filename);
```

However, the path is not sanitized before creating the File object. This allows anyone who can control the system property to determine what file is used. Ideally, the path should be resolved relative to some kind of application or user home directory.

Potential Mitigations

see "Path Traversal" (CWE-22)

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	37	Path Traversal: '/absolute/pathname/here'	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	38	Path Traversal: '\absolute\pathname\here'	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	39	Path Traversal: 'C:dirname'	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	40	Path Traversal:	**Development**

			'\\UNC\share\name\' (Windows UNC Share)	**Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Absolute Path Traversal

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

BACK TO TOP

Privacy Violation

Weakness ID: 359 *(Weakness Class)* **Status:** Incomplete

Description

Description Summary

Mishandling private information, such as customer passwords or social security numbers, can compromise user privacy and is often illegal.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code contains a logging statement that tracks the contents of records added to a database by storing them in a log file. Among other values that are stored, the getPassword() function returns the user-supplied plaintext password associated with the account.

(Bad Code)

Example Language: **C#**

```
pass = GetPassword();
...
dbmsLog.WriteLine(id + ":" + pass + ":" + type + ":" + tstamp);
```

The code in the example above logs a plaintext password to the filesystem. Although many developers trust the filesystem as a safe storage location for data, it should not be trusted implicitly, particularly when privacy is a concern.

Other Notes

Privacy violations occur when: 1. Private user information enters the program. 2. The data is written to an external location, such as the console, file system, or network.

Private data can enter a program in a variety of ways:

- Directly from the user in the form of a password or personal information
- Accessed from a database or other data store by the application
- Indirectly from a partner or other third party

Sometimes data that is not labeled as private can have a privacy implication in a different context. For example, student identification numbers are usually not considered private because there is no explicit and publicly-available mapping to an individual student's personal information. However, if a school generates identification numbers based on student social security numbers, then the identification numbers should be considered private.

Security and privacy concerns often seem to compete with each other. From a security perspective, you should record all important operations so that any anomalous activity can later be identified. However, when private data is involved, this practice can in fact create risk. Although there are many ways in which private data can be handled unsafely, a common risk stems from misplaced trust. Programmers often trust the operating environment in which a program runs, and therefore believe that it is acceptable store private information on the file system, in the registry, or in other locally-controlled resources. However, even if access to certain resources is restricted, this does not guarantee that the individuals who do have access can be trusted.

For example, in 2004, an unscrupulous employee at AOL sold approximately 92 million private customer e-mail addresses to a spammer marketing an offshore gambling web site. In response to such high-profile exploits, the collection and management of private data is becoming increasingly regulated. Depending on its location, the type of business it conducts, and the nature of any private data it handles, an organization may be required to comply with one or more of the following federal and state regulations: - Safe Harbor Privacy Framework [REF-2] - Gramm-Leach Bliley Act (GLBA) [REF-3] - Health Insurance Portability and Accountability Act (HIPAA) [REF-4] - California SB-1386 [REF-5]

Relationships

Nature	Type	ID	Name	View(s) this

				relationship pertains to
ChildOf	Weakness Class	200	Information Exposure	**Research Concepts (primary)1000**
ChildOf	Category	254	Security Features	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	202	Privacy Leak through Data Queries	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Privacy Violation

References

J. Oates. "AOL man pleads guilty to selling 92m email addies". The Register. 2005. <http://www.theregister.co.uk/2005/02/07/aol_email_theft/>.

[REF-2] U.S. Department of Commerce. "Safe Harbor Privacy Framework". <http://www.export.gov/safeharbor/>.

[REF-3] Federal Trade Commission. "Financial Privacy: The Gramm-Leach Bliley Act (GLBA)". <http://www.ftc.gov/privacy/glbact/index.html>.

[REF-4] U.S. Department of Human Services. "Health Insurance Portability and Accountability Act (HIPAA)". <http://www.hhs.gov/ocr/hipaa/>.

[REF-5] Government of the State of California. "California SB-1386". 2002. <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Other Notes, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Other Notes, References		

BACK TO TOP

Plaintext Storage of a Password

Weakness ID: 256 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

Storing a password in plaintext may result in a system compromise.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

All

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following code reads a password from a properties file and uses the password to connect to a database.

(Bad Code)

Example Language: **Java**

```
...
Properties prop = new Properties();
prop.load(new FileInputStream("config.properties"));
String password = prop.getProperty("password");
DriverManager.getConnection(url, usr, password);
...
```

This code will run successfully, but anyone who has access to config.properties can read the value of password. If a devious employee has access to this information, they can use it to break into the system.

Example 2

The following code reads a password from the registry and uses the password to create a new network credential.

(Bad Code)

Example Language: **Java**

```
...
String password = regKey.GetValue(passKey).toString();
NetworkCredential netCred = new NetworkCredential(username,password,domain);
...
```

This code will run successfully, but anyone who has access to the registry key used to store the password can read the value of password. If a devious employee has access to this information, they can use it to break into the system

Potential Mitigations

Avoid storing passwords in easily accessible locations.

Consider storing cryptographic hashes of passwords as an alternative to storing in plaintext.

Other Notes

Password management issues occur when a password is stored in plaintext in an application's properties or configuration file. A programmer can attempt to remedy the password management problem by obscuring the password with an encoding function, such as base 64 encoding, but this effort does not adequately protect the password. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's

job easier. Good password management guidelines require that a password never be stored in plaintext.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	522	Insufficiently Protected Credentials	**Development Concepts (primary)699 Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Password Management

References

J. Viega and G. McGraw. "Building Secure Software: How to Avoid Security Problems the Right Way". 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-01-30	Plaintext Storage		

BACK TO TOP

Deserialization of Untrusted Data

Weakness ID: 502 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

Extended Description

It is often convenient to serialize objects for communication or to save them for later use. However, deserialized data or code can often be modified without using the provided accessor functions if it does not use cryptography to protect itself. Furthermore, any cryptography would still be client-side security -- which is a dangerous security assumption.

Data that is untrusted can not be trusted to be well-formed.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	If a function is making an assumption on when to terminate, based on a sentry in a string, it could easily never terminate.
Authorization	Code could potentially make the assumption that information in the deserialized object is valid. Functions which make this dangerous assumption could be exploited.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

(Bad Code)

Example Language: **Java**

```
try {
File file = new File("object.obj");
ObjectInputStream in = new ObjectInputStream(new FileInputStream(file));
javax.swing.JButton button = (javax.swing.JButton) in.readObject();
in.close();
byte[] bytes = getBytesFromFile(file);
in = new ObjectInputStream(new ByteArrayInputStream(bytes));
button = (javax.swing.JButton) in.readObject();
in.close();
}
```

Potential Mitigations

Phase: Requirements

A deserialization library could be used which provides a cryptographic framework to seal serialized data.

Phase: Implementation

Use the signing features of a language to assure that deserialized data has not been tainted.

Phase: Implementation

When deserializing data populate a new object rather than just deserializing, the result is that the data flows through safe input validation and that the functions are safe.

Phase: Implementation

Explicitly define final readObject() to prevent deserialization. An example of this is:

(Good Code)

Example Language: **Java**

```
private final void readObject(ObjectInputStream in) throws java.io.IOException {
throw new java.io.IOException("Cannot be deserialized"); }
```

Phases: Architecture and Design; Implementation

Make fields transient to protect them from deserialization.

An attempt to serialize and then deserialize a class containing transient fields will result in NULLs where the transient data should be. This is an excellent way to prevent time, environment-based, or sensitive variables from being carried over and used improperly.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	485	Insufficient Encapsulation	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Deserialization of untrusted data

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Relationships, Other Notes, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Other Notes, Potential Mitigations		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
Java	0417366009739895	12/6/2025
Groovy	0108265307926968	12/6/2025
Kotlin	0460997576477410	12/6/2025
Common	5315621544857687	12/6/2025