CCMSU UPDATER 05-07-2023 Scan Report

Project Name	CCMSU UPDATER 05-07-2023
Scan Start	Wednesday, July 5, 2023 10:01:44 AM
Preset	Checkmarx Default
Scan Time	00h:18m:34s
Lines Of Code Scanned	67110
Files Scanned	933
Report Creation Time	Wednesday, July 5, 2023 10:21:34 AM
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588
Team	CxServer
Checkmarx Version	9.4.0.2076
Scan Type	Full
Source Origin	LocalPath
Density	6/10000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

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
ASD STIG 4.10	All
OWASP Top 10 API	All
OWASP Top 10 2010	All
OWASP Top 10 2021	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2.1	None
OWASP Top 10 2013	None
FISMA 2014	None
NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None
ASD STIG 4.10	None
OWASP Top 10 API	None
OWASP Top 10 2010	None
OWASP Top 10 2021	None

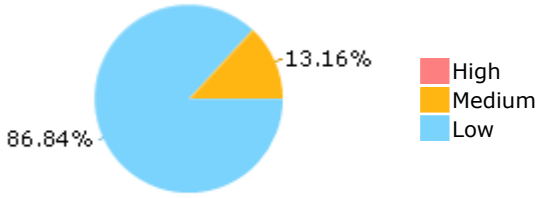
Results Limit

Results limit per query was set to 50

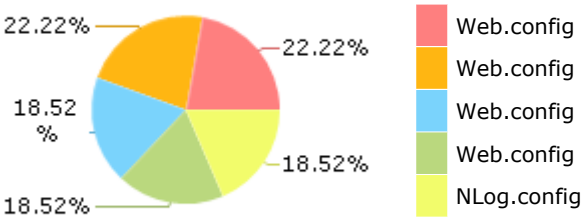
Selected Queries

Selected queries are listed in Result Summary

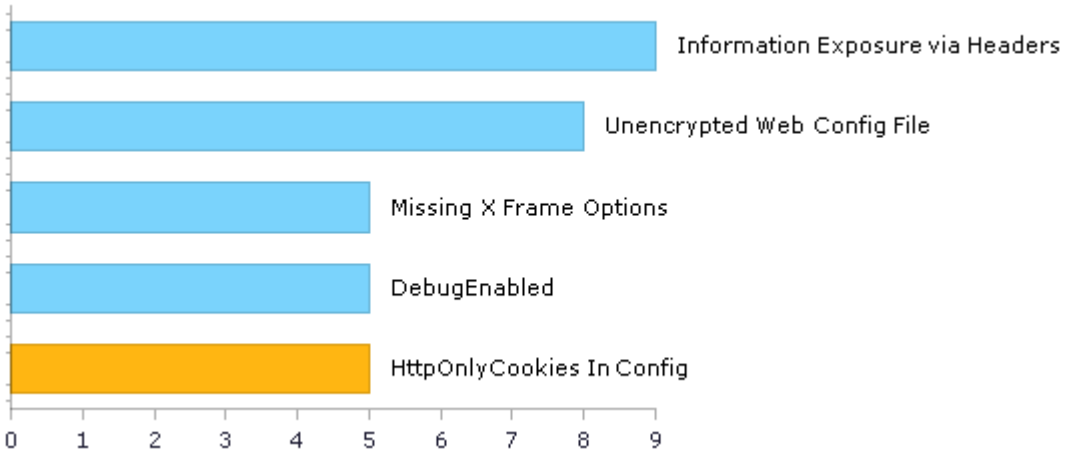
Result Summary



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	5	5
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	5	5
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	5	5
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	1	1
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2021

Category	Issues Found	Best Fix Locations
A1-Broken Access Control*	9	9
A2-Cryptographic Failures*	0	0
A3-Injection*	0	0
A4-Insecure Design*	13	13
A5-Security Misconfiguration*	10	10
A6-Vulnerable and Outdated Components	1	1
A7-Identification and Authentication Failures*	1	1
A8-Software and Data Integrity Failures*	19	19
A9-Security Logging and Monitoring Failures*	2	2
A10-Server-Side Request Forgery	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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	5	5
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	1	1
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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*	9	9
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)*	5	5
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

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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.	5	5
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

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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	0	0

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

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - Custom

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

Scan Summary - ASD STIG 4.10

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

APSC-DV-000870 - CAT II The application must generate audit records for all direct access to the information system.	0	0
APSC-DV-000880 - CAT II The application must generate audit records for all account creations, modifications, disabling, and termination events.	0	0
APSC-DV-000910 - CAT II The application must initiate session auditing upon startup.	0	0
APSC-DV-000940 - CAT II The application must log application shutdown events.	0	0
APSC-DV-000950 - CAT II The application must log destination IP addresses.	0	0
APSC-DV-000960 - CAT II The application must log user actions involving access to data.	0	0
APSC-DV-000970 - CAT II The application must log user actions involving changes to data.	0	0
APSC-DV-000980 - CAT II The application must produce audit records containing information to establish when (date and time) the events occurred.	0	0
APSC-DV-000990 - CAT II The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	0	0
APSC-DV-001000 - CAT II When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	0	0
APSC-DV-001010 - CAT II The application must produce audit records that contain information to establish the outcome of the events.	0	0
APSC-DV-001020 - CAT II The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	0	0
APSC-DV-001030 - CAT II The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	0	0
APSC-DV-001040 - CAT II The application must implement transaction recovery logs when transaction based.	0	0
APSC-DV-001050 - CAT II The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	0	0
APSC-DV-001070 - CAT II The application must off-load audit records onto a different system or media than the system being audited.	0	0
APSC-DV-001080 - CAT II The application must be configured to write application logs to a centralized log repository.	0	0
APSC-DV-001090 - CAT II The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	0	0
APSC-DV-001100 - CAT II Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	0	0
APSC-DV-001110 - CAT II The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	0	0
APSC-DV-001120 - CAT II The application must shut down by default upon audit failure (unless availability is an overriding concern).	0	0
APSC-DV-001130 - CAT II The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	0	0
APSC-DV-001140 - CAT II The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	0	0
APSC-DV-001150 - CAT II The application must provide an audit reduction capability that supports on-demand reporting requirements.	0	0
APSC-DV-001160 - CAT II The application must provide an audit reduction capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001170 - CAT II The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001180 - CAT II The application must provide a report generation capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001190 - CAT II The application must provide a report generation capability that	0	0

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

APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0
APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	5	5
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.	5	5
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.*	4	4
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.	5	5
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0
APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of	0	0

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

to show how deadlock and recursion issues in web services are being mitigated.		
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by following available guidance.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002995 - CAT II The Configuration Management (CM) repository must be properly patched and STIG compliant.	0	0
APSC-DV-003000 - CAT II Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	0	0
APSC-DV-003010 - CAT II A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	0	0
APSC-DV-003020 - CAT II A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	0	0
APSC-DV-003030 - CAT II The application services and interfaces must be compatible with and ready for IPv6 networks.	0	0
APSC-DV-003040 - CAT II The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	0	0
APSC-DV-003050 - CAT II A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	0	0
APSC-DV-003060 - CAT II Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	0	0
APSC-DV-003070 - CAT II Data backup must be performed at required intervals in accordance with DoD policy.	0	0
APSC-DV-003080 - CAT II Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	0	0
APSC-DV-003090 - CAT II Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	0	0
APSC-DV-003100 - CAT II The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	0	0
APSC-DV-003110 - CAT I The application must not contain embedded authentication data.	0	0
APSC-DV-003120 - CAT I The application must have the capability to mark sensitive/classified output when required.	0	0
APSC-DV-003130 - CAT III Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	0	0
APSC-DV-003150 - CAT II At least one tester must be designated to test for security flaws in addition to functional testing.	0	0
APSC-DV-003140 - CAT II Application files must be cryptographically hashed prior to deploying to DoD operational networks.	0	0
APSC-DV-003160 - CAT III Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	0	0
APSC-DV-003170 - CAT II An application code review must be performed on the application.	0	0
APSC-DV-003180 - CAT III Code coverage statistics must be maintained for each release of the application.	0	0
APSC-DV-003190 - CAT II Flaws found during a code review must be tracked in a defect tracking system.	0	0
APSC-DV-003200 - CAT II The changes to the application must be assessed for IA and	0	0

accreditation impact prior to implementation.		
APSC-DV-003210 - CAT II Security flaws must be fixed or addressed in the project plan.	0	0
APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.	0	0
APSC-DV-003220 - CAT III The designer must create and update the Design Document for each release of the application.	0	0
APSC-DV-003230 - CAT II Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	0	0
APSC-DV-003235 - CAT II The application must not be subject to error handling vulnerabilities.*	0	0
APSC-DV-003250 - CAT I The application must be decommissioned when maintenance or support is no longer available.	0	0
APSC-DV-003236 - CAT II The application development team must provide an application incident response plan.	0	0
APSC-DV-003240 - CAT I All products must be supported by the vendor or the development team.	0	0
APSC-DV-003260 - CAT III Procedures must be in place to notify users when an application is decommissioned.	0	0
APSC-DV-003270 - CAT II Unnecessary built-in application accounts must be disabled.	0	0
APSC-DV-003280 - CAT I Default passwords must be changed.	0	0
APSC-DV-003330 - CAT II The system must alert an administrator when low resource conditions are encountered.	0	0
APSC-DV-003285 - CAT II An Application Configuration Guide must be created and included with the application.	0	0
APSC-DV-003290 - CAT II If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	0	0
APSC-DV-003300 - CAT II The designer must ensure uncategorized or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0
APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users	0	0

indicating the reliable termination of authenticated communications sessions.		
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	0	0
APSC-DV-000160 - CAT II The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	0	0
APSC-DV-000170 - CAT II The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	0	0
APSC-DV-000190 - CAT I Messages protected with WS_Security must use time stamps with creation and expiration times.	0	0
APSC-DV-000180 - CAT II Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	0	0
APSC-DV-000200 - CAT I Validity periods must be verified on all application messages using WS-Security or SAML assertions.	0	0
APSC-DV-000210 - CAT II The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	0	0
APSC-DV-000220 - CAT II The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	0	0
APSC-DV-000230 - CAT I The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	0	0
APSC-DV-000240 - CAT I The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	0	0
APSC-DV-000250 - CAT II The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	0	0
APSC-DV-000260 - CAT II The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	0	0
APSC-DV-000290 - CAT II Shared/group account credentials must be terminated when members leave the group.	0	0
APSC-DV-000280 - CAT II The application must provide automated mechanisms for supporting account management functions.	0	0
APSC-DV-000300 - CAT II The application must automatically remove or disable temporary user accounts 72 hours after account creation.	0	0
APSC-DV-000320 - CAT III The application must automatically disable accounts after a 35 day period of account inactivity.	0	0
APSC-DV-000330 - CAT II Unnecessary application accounts must be disabled, or deleted.	0	0
APSC-DV-000420 - CAT II The application must automatically audit account enabling actions.	0	0
APSC-DV-000340 - CAT II The application must automatically audit account creation.	0	0
APSC-DV-000350 - CAT II The application must automatically audit account modification.	0	0
APSC-DV-000360 - CAT II The application must automatically audit account disabling actions.	0	0
APSC-DV-000370 - CAT II The application must automatically audit account removal actions.	0	0
APSC-DV-000380 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are created.	0	0
APSC-DV-000390 - CAT III The application must notify System Administrators and	0	0

Information System Security Officers when accounts are modified.		
APSC-DV-000400 - CAT III The application must notify System Administrators and Information System Security Officers of account disabling actions.	0	0
APSC-DV-000410 - CAT III The application must notify System Administrators and Information System Security Officers of account removal actions.	0	0
APSC-DV-000430 - CAT III The application must notify System Administrators and Information System Security Officers of account enabling actions.	0	0
APSC-DV-000440 - CAT II Application data protection requirements must be identified and documented.	0	0
APSC-DV-000520 - CAT II The application must audit the execution of privileged functions.	0	0
APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	0	0
APSC-DV-000480 - CAT II The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	0	0
APSC-DV-000490 - CAT II The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	0	0
APSC-DV-000500 - CAT II The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	0	0
APSC-DV-000510 - CAT I The application must execute without excessive account permissions.	0	0
APSC-DV-000530 - CAT I The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	0	0
APSC-DV-000560 - CAT III The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	0	0
APSC-DV-000540 - CAT II The application administrator must follow an approved process to unlock locked user accounts.	0	0
APSC-DV-000550 - CAT III The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000570 - CAT III The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000580 - CAT III The application must display the time and date of the users last successful logon.	0	0
APSC-DV-000630 - CAT II The application must provide audit record generation capability for the destruction of session IDs.	0	0
APSC-DV-000590 - CAT II The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	0	0
APSC-DV-000600 - CAT II For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance	0	0
APSC-DV-000610 - CAT II The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	0	0
APSC-DV-000620 - CAT II The application must provide audit record generation capability for the creation of session IDs.	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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	5	5
API8-Injection*	0	0
API9-Improper Assets Management	0	0
API10-Insufficient Logging and Monitoring	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2010

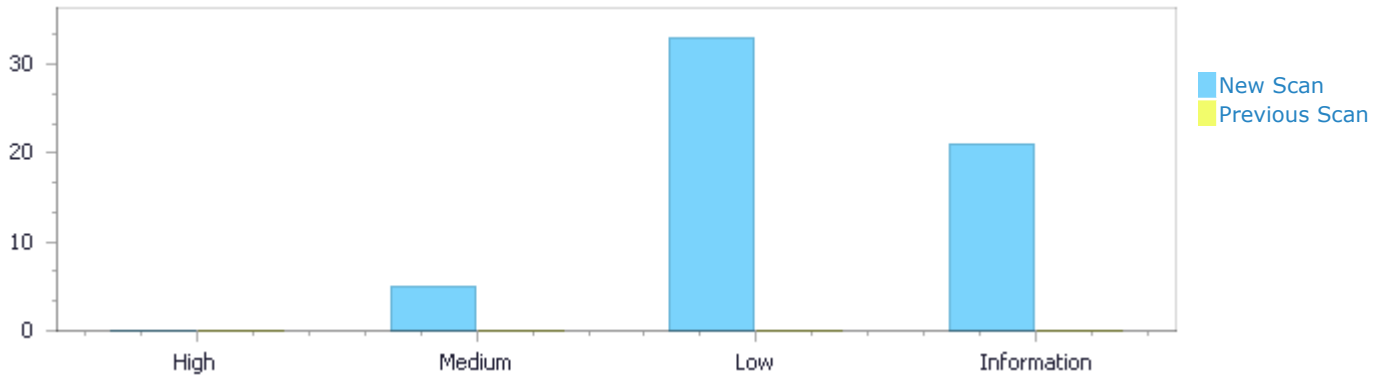
Category	Issues Found	Best Fix Locations
A1-Injection	0	0
A2-Cross-Site Scripting (XSS)*	0	0
A3-Broken Authentication and Session Management*	0	0
A4-Insecure Direct Object References	0	0
A5-Cross-Site Request Forgery (CSRF)	0	0
A6-Security Misconfiguration	0	0
A7-Insecure Cryptographic Storage*	0	0
A8-Failure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

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	5	33	21	59
Recurrent Issues	0	0	0	0	0
Total	0	5	33	21	59
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	0	5	33	21	59
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	5	33	21	59

Result Summary

Vulnerability Type	Occurrences	Severity
HttpOnlyCookies In Config	5	Medium
Information Exposure via Headers	9	Low
Unencrypted Web Config File	8	Low
DebugEnabled	5	Low
Missing X Frame Options	5	Low
Improper Resource Shutdown or Release	4	Low
Client JQuery Deprecated Symbols	1	Low

Missing Content Security Policy	1	Low
Hardcoded Absolute Path	19	Information
Insufficient Logging of Sensitive Operations	2	Information

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	1
CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	1
CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	1
CCMSUpdater_2/Router/Views/Web.config	1
CCMSUpdater_2/Router/Web.config	1

Scan Results Details

HttpOnlyCookies In Config

Query Path:
CSharp\Cx\CSharp WebConfig\HttpOnlyCookies In Config Version:0

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
ASD STIG 4.10: APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.
OWASP Top 10 2021: A5-Security Misconfiguration

Description

HttpOnlyCookies In Config\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=1
Status	New
Detection Date	7/5/2023 10:07:53 AM

The CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass68763cde	CxXmlConfigClass68763cde

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

HttpOnlyCookies In Config\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=2
Status	New

Detection Date	7/5/2023 10:07:53 AM

The CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClassde534cbb	CxXmlConfigClassde534cbb

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

HttpOnlyCookies In Config\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=3
Status	New
Detection Date	7/5/2023 10:07:53 AM

The CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass15ed71e8	CxXmlConfigClass15ed71e8

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

HttpOnlyCookies In Config\Path 4:

Severity	Medium
Result State	To Verify

Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=4
Status	New
Detection Date	7/5/2023 10:07:53 AM

The CCMSUpdater_2/Router/Views/Web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	CCMSUpdater_2/Router/Views/Web.config	CCMSUpdater_2/Router/Views/Web.config
Line	1	1
Object	CxXmlConfigClass94534ebc	CxXmlConfigClass94534ebc

Code Snippet
File Name CCMSUpdater_2/Router/Views/Web.config
Method <?xml version="1.0"?>

```
....
1.  <?xml version="1.0"?>
```

HttpOnlyCookies In Config\Path 5:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=5
Status	New
Detection Date	7/5/2023 10:07:53 AM

The CCMSUpdater_2/Router/Web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config
Line	1	1
Object	CxXmlConfigClassa55c3075	CxXmlConfigClassa55c3075

Code Snippet
File Name CCMSUpdater_2/Router/Web.config
Method

```
....
1.
```

Information Exposure via Headers

Query Path:
CSharp\Cx\CSharp Low Visibility\Information Exposure via Headers Version:1

Categories

OWASP Top 10 2021: A1-Broken Access Control

Description

Information Exposure via Headers\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=11
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config
Line	15	15
Object	HTTPRUNTIME	HTTPRUNTIME

Code Snippet
File Name CCMSUpdater_2/Router/Web.config
Method

```
....
15.      <httpRuntime targetFramework="4.6.1" />
```

Information Exposure via Headers\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=12
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/bin/Router.dll.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/bin/Router.dll.config	CCMSUpdater_2/Router/bin/Router.dll.config
Line	15	15
Object	HTTPRUNTIME	HTTPRUNTIME

Code Snippet
File Name CCMSUpdater_2/Router/bin/Router.dll.config
Method <?xml version="1.0" encoding="utf-8"?>

```
....
15.      <httpRuntime targetFramework="4.6.1" />
```

Information Exposure via Headers\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=13
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/Global.asax.cs, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/Global.asax.cs	CCMSUpdater_2/Router/Global.asax.cs
Line	14	14
Object	Application_Start	Application_Start

Code Snippet
File Name CCMSUpdater_2/Router/Global.asax.cs
Method protected void Application_Start()

```
....
14.          protected void Application_Start()
```

Information Exposure via Headers\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=14
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	35	35
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config

Method

```
....
35.    <system.webServer>
```

Information Exposure via Headers\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=15
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Line	35	35
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Method

```
....
35.    <system.webServer>
```

Information Exposure via Headers\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=16
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Line	35	35
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Method

```
....
35.     <system.webServer>
```

Information Exposure via Headers\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=17
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/Views/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/Views/Web.config	CCMSUpdater_2/Router/Views/Web.config
Line	29	29
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/Router/Views/Web.config
Method <?xml version="1.0"?>

```
....
29.     <system.webServer>
```

Information Exposure via Headers\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=18
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/Web.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config
Line	20	20
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/Router/Web.config

Method

```
....
20.    <system.webServer>
```

Information Exposure via Headers\Path 9:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=19
Status	New
Detection Date	7/5/2023 10:16:17 AM

The application is misconfigured, in CCMSUpdater_2/Router/bin/Router.dll.config, to expose server data in response headers.

	Source	Destination
File	CCMSUpdater_2/Router/bin/Router.dll.config	CCMSUpdater_2/Router/bin/Router.dll.config
Line	20	20
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name CCMSUpdater_2/Router/bin/Router.dll.config
Method <?xml version="1.0" encoding="utf-8"?>

```
....
20.    <system.webServer>
```

Unencrypted Web Config File

Query Path:
CSharp\Cx\CSharp Low Visibility\Unencrypted Web Config File Version:1

Categories

OWASP Top 10 2021: A4-Insecure Design

Description

Unencrypted Web Config File\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=21
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination

File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass68763cde	CxXmlConfigClass68763cde

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

Unencrypted Web Config File\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=22
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClassde534cbb	CxXmlConfigClassde534cbb

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

Unencrypted Web Config File\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=23
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass15ed71e8	CxXmlConfigClass15ed71e8

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

Unencrypted Web Config File\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=24
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/Views/Web.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/Views/Web.config	CCMSUpdater_2/Router/Views/Web.config
Line	1	1
Object	CxXmlConfigClass94534ebc	CxXmlConfigClass94534ebc

Code Snippet
File Name CCMSUpdater_2/Router/Views/Web.config
Method <?xml version="1.0"?>

```
....
1.  <?xml version="1.0"?>
```

Unencrypted Web Config File\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=25
Status	New

Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/Web.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config
Line	1	1
Object	CxXmlConfigClassa55c3075	CxXmlConfigClassa55c3075

Code Snippet
File Name CCMSUpdater_2/Router/Web.config
Method

```
....
1.
```

Unencrypted Web Config File\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=26
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/bin/Router.dll.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/bin/Router.dll.config	CCMSUpdater_2/Router/bin/Router.dll.config
Line	1	1
Object	CxXmlConfigClass3ecaa22c	CxXmlConfigClass3ecaa22c

Code Snippet
File Name CCMSUpdater_2/Router/bin/Router.dll.config
Method <?xml version="1.0" encoding="utf-8"?>

```
....
1.  <?xml version="1.0" encoding="utf-8"?>
```

Unencrypted Web Config File\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=27
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/Web.Debug.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/Web.Debug.config	CCMSUpdater_2/Router/Web.Debug.config
Line	1	1
Object	CxXmlConfigClass49d25ccc	CxXmlConfigClass49d25ccc

Code Snippet
File Name CCMSUpdater_2/Router/Web.Debug.config
Method <?xml version="1.0"?>

```
....
1.  <?xml version="1.0"?>
```

Unencrypted Web Config File\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=28
Status	New
Detection Date	7/5/2023 10:16:17 AM

The web.config file CCMSUpdater_2/Router/Web.Release.config does not encrypt the sensitive element found at line 1. This information can be plainly read by anyone with local file-system access.

	Source	Destination
File	CCMSUpdater_2/Router/Web.Release.config	CCMSUpdater_2/Router/Web.Release.config
Line	1	1
Object	CxXmlConfigClass26a216ac	CxXmlConfigClass26a216ac

Code Snippet
File Name CCMSUpdater_2/Router/Web.Release.config
Method <?xml version="1.0"?>

```
....
1.  <?xml version="1.0"?>
```

DebugEnabled

Query Path:
CSharp\Cx\CSharp WebConfig\DebugEnabled Version:1

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
FISMA 2014: Configuration Management

NIST SP 800-53: SI-11 Error Handling (P2)
OWASP Top 10 2017: A3-Sensitive Data Exposure
ASD STIG 4.10: APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.
OWASP Top 10 API: API7-Security Misconfiguration
OWASP Top 10 2021: A5-Security Misconfiguration

Description

DebugEnabled\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=29
Status	New
Detection Date	7/5/2023 10:16:18 AM

The application source code includes "true", in line 1 of CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Line	28	28
Object	"true"	"true"

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Method

```
....
28.      <compilation debug="true">
```

DebugEnabled\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=30
Status	New
Detection Date	7/5/2023 10:16:18 AM

The application source code includes "true", in line 1 of CCMSUpdater_2/Router/bin/Router.dll.config, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	CCMSUpdater_2/Router/bin/Router.dll.config	CCMSUpdater_2/Router/bin/Router.dll.config
Line	14	14
Object	"true"	"true"

Code Snippet	
File Name	CCMSUpdater_2/Router/bin/Router.dll.config
Method	<?xml version="1.0" encoding="utf-8"?>

```
....
14.      <compilation debug="true" targetFramework="4.6.1" />
```

DebugEnabled\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=31
Status	New
Detection Date	7/5/2023 10:16:18 AM

The application source code includes "true", in line 1 of CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Line	28	28
Object	"true"	"true"

Code Snippet	
File Name	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Method	

```
....
28.      <compilation debug="true">
```

DebugEnabled\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=32
Status	New
Detection Date	7/5/2023 10:16:18 AM

The application source code includes "true", in line 1 of CCMSUpdater_2/Router/Web.config, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config

Line	14	14
Object	"true"	"true"

Code Snippet
File Name CCMSUpdater_2/Router/Web.config
Method

```
....
14.      <compilation debug="true" targetFramework="4.6.1" />
```

DebugEnabled\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=33
Status	New
Detection Date	7/5/2023 10:16:18 AM

The application source code includes "true", in line 1 of CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	28	28
Object	"true"	"true"

Code Snippet
File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Method

```
....
28.      <compilation debug="true">
```

Missing X Frame Options

Query Path:
CSharp\Cx\CSharp WebConfig\Missing X Frame Options Version:1

Categories

NIST SP 800-53: SC-18 Mobile Code (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
ASD STIG 4.10: APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.
OWASP Top 10 2021: A4-Insecure Design

Description

Missing X Frame Options\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=34
Status	New
Detection Date	7/5/2023 10:16:18 AM

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass68763cde	CxXmlConfigClass68763cde

Code Snippet

File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config

Method

```
....
1.
```

Missing X Frame Options\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=35
Status	New
Detection Date	7/5/2023 10:16:18 AM

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClassde534cbb	CxXmlConfigClassde534cbb

Code Snippet

File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.4/Content/Areas/HelpPage/Views/Web.config

Method

```
....
1.
```

Missing X Frame Options\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=36
Status	New
Detection Date	7/5/2023 10:16:18 AM

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass15ed71e8	CxXmlConfigClass15ed71e8

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/Views/Web.config
Method

```
....
1.
```

Missing X Frame Options\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=37
Status	New
Detection Date	7/5/2023 10:16:18 AM

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	CCMSUpdater_2/Router/Views/Web.config	CCMSUpdater_2/Router/Views/Web.config
Line	1	1
Object	CxXmlConfigClass94534ebc	CxXmlConfigClass94534ebc

Code Snippet
File Name CCMSUpdater_2/Router/Views/Web.config
Method <?xml version="1.0"?>

```
....
1.  <?xml version="1.0"?>
```

Missing X Frame Options\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=38
Status	New
Detection Date	7/5/2023 10:16:18 AM

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	CCMSUpdater_2/Router/Web.config	CCMSUpdater_2/Router/Web.config
Line	1	1
Object	CxXmlConfigClassa55c3075	CxXmlConfigClassa55c3075

Code Snippet
File Name CCMSUpdater_2/Router/Web.config
Method

```
....
1.
```

Improper Resource Shutdown or Release

Query Path:
CSharp\Cx\CSharp Low Visibility\Improper Resource Shutdown or Release Version:2

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
ASD STIG 4.10: APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.

Description

Improper Resource Shutdown or Release\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=7
Status	New
Detection Date	7/5/2023 10:16:12 AM

The application's SpoolClosedLog method in CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs defines and initializes the OracleCommand object at 1620. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Line	1632	1635
Object	OracleCommand	ExecuteReader

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Method public CCMSUpdateAudit SpoolClosedLog(CCMSUpdateAudit cCMSUpdateAudit)

```
....
1632.                           OracleCommand cmd = new OracleCommand();
....
1635.                           OracleDataReader dr =
cmd.ExecuteReader();
```

Improper Resource Shutdown or Release\Path 2:

Severity Low
Result State To Verify
Online Results https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=8
Status New
Detection Date 7/5/2023 10:16:12 AM

The application's WriteSampleObjectUsingFormatter method in CCMSUpdater_2/Router/Areas/HelpPage/SampleGeneration/HelpPageSampleGenerator.cs defines and initializes the StreamReader object at 288. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/SampleGeneration/HelpPageSampleGenerator.cs	CCMSUpdater_2/Router/Areas/HelpPage/SampleGeneration/HelpPageSampleGenerator.cs
Line	310	311
Object	StreamReader	ReadToEnd

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/SampleGeneration/HelpPageSampleGenerator.cs
Method public virtual object WriteSampleObjectUsingFormatter(MediaTypeFormatter formatter, object value, Type type, MediaTypeHeaderValue mediaType)

```
....
310.                        StreamReader reader = new StreamReader(ms);
311.                        string serializedSampleString =
reader.ReadToEnd();
```

Improper Resource Shutdown or Release\Path 3:

Severity Low

Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=9
Status	New
Detection Date	7/5/2023 10:16:12 AM

The application's CountIssuesClosed method in CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs defines and initializes the SqlConnection object at 1867. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Line	1878	1882
Object	SqlConnection	Close

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Method public int CountIssuesClosed(int day = 30) //changed int month =1 to day = 20

```
....
1878.               SqlConnection DBConn = new
SqlConnection(ConnectionString);
....
1882.               DBConn.Close();
```

Improper Resource Shutdown or Release\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=10
Status	New
Detection Date	7/5/2023 10:16:12 AM

The application's CountIssues method in CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs defines and initializes the SqlCommand object at 1848. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs	CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Line	1860	1860
Object	SqlCommand	cmd

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/Concrete/grpManager.cs
Method public int CountIssues(int day = 25) //changed int month =1 to day = 25

```
....
1860.               SqlCommand cmd = new SqlCommand(qr, DBConn);
```

Client JQuery Deprecated Symbols

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client JQuery Deprecated Symbols Version:1

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components

Description

Client JQuery Deprecated Symbols\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=6
Status	New
Detection Date	7/5/2023 10:16:10 AM

Method function in CCMSUpdater_2/packages/Microsoft.AspNetCore.Identity.UI.3.1.0/staticwebassets/V4/lib/bootstrap/dist/js/bootstrap.bundle.min.js, at line 304, calls an obsolete API, bind. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNetCore.Identity.UI.3.1.0/staticwebassets/V4/lib/bootstrap/dist/js/bootstrap.bundle.min.js	CCMSUpdater_2/packages/Microsoft.AspNetCore.Identity.UI.3.1.0/staticwebassets/V4/lib/bootstrap/dist/js/bootstrap.bundle.min.js
Line	305	305
Object	bind	bind

Code Snippet

File Name	CCMSUpdater_2/packages/Microsoft.AspNetCore.Identity.UI.3.1.0/staticwebassets/V4/lib/bootstrap/dist/js/bootstrap.bundle.min.js
Method	}, t.cycle = function(t) {

```
....
305.                   t || (this._isPaused = !1), this._interval &&
(clearInterval(this._interval), this._interval = null),
this._config.interval && !this._isPaused && (this._interval =
setInterval((document.visibilityState ? this.nextWhenVisible :
this.next).bind(this), this._config.interval))
```

Missing Content Security Policy

Query Path:
CSharp\Cx\CSharp Low Visibility\Missing Content Security Policy Version:1

Categories

OWASP Top 10 2021: A7-Identification and Authentication Failures

Description

Missing Content Security Policy\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=20
Status	New
Detection Date	7/5/2023 10:16:17 AM

A Content Security Policy is not explicitly defined within the web-application.

	Source	Destination
File	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config	CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config
Line	1	1
Object	CxXmlConfigClass68763cde	CxXmlConfigClass68763cde

Code Snippet

File Name CCMSUpdater_2/packages/Microsoft.AspNet.WebApi.HelpPage.5.2.3/Content/Areas/HelpPage/Views/Web.config

Method

```
....
1.
```

Hardcoded Absolute Path

Query Path:

CSharp\Cx\CSharp Best Coding Practice\Hardcoded Absolute Path Version:1

Categories

OWASP Top 10 2021: A8-Software and Data Integrity Failures

Description

Hardcoded Absolute Path\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=39
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config

Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=40
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Line	13	13
Object	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
13.      <target xsi:type="File" name="Infos"
fileName="C:\logs\CCMS\audits\${date:format=yyyy-MM-dd}-info.log"
```

Hardcoded Absolute Path\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=41
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Line	16	16
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
16.      <target xsi:type="File" name="Warnings"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-warning.log"
```

Hardcoded Absolute Path\Path 4:

Severity Information
Result State To Verify
Online Results https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=42
Status New
Detection Date 7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Line	19	19
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
19.      <target xsi:type="File" name="Errors"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-error.log"
```

Hardcoded Absolute Path\Path 5:

Severity Information
Result State To Verify
Online Results https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=43
Status New

Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Line	22	22
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Debug/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
22.      <target xsi:type="File" name="Fatals"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-fatal.log"
```

Hardcoded Absolute Path\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=44
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 7:

Severity	Information
Result State	To Verify

Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=45
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Line	13	13
Object	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
13.      <target xsi:type="File" name="Infos"
fileName="C:\logs\CCMS\audits\${date:format=yyyy-MM-dd}-info.log"
```

Hardcoded Absolute Path\Path 8:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=47
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Line	16	16
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
16.      <target xsi:type="File" name="Warnings"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-warning.log"
```

Hardcoded Absolute Path\Path 9:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=49
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Line	19	19
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
19.      <target xsi:type="File" name="Errors"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-error.log"
```

Hardcoded Absolute Path\Path 10:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=50
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log" in CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Line	22	22
Object	"C:\\logs\\CCMS\\errors\\${date:format	"C:\\logs\\CCMS\\errors\\${date:format

	=yyyy-MM-dd}-fatal.log"	=yyyy-MM-dd}-fatal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/bin/Release/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
22.      <target xsi:type="File" name="Fatals"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-fatal.log"
```

Hardcoded Absolute Path\Path 11:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=51
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/CCMSUpdater.Domain/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 12:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=52
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log" in CCMSUpdater_2/CCMSUpdater.Domain/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/	CCMSUpdater_2/CCMSUpdater.Domain/

	NLog.config	NLog.config
Line	13	13
Object	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"	"C:\\logs\\CCMS\\audits\\${date:format=yyyy-MM-dd}-info.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
13.      <target xsi:type="File" name="Infos"
fileName="C:\logs\CCMS\audits\${date:format=yyyy-MM-dd}-info.log"
```

Hardcoded Absolute Path\Path 13:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=53
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log" in CCMSUpdater_2/CCMSUpdater.Domain/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Line	16	16
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-warning.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
16.      <target xsi:type="File" name="Warnings"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-warning.log"
```

Hardcoded Absolute Path\Path 14:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=54
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log" in CCMSUpdater_2/CCMSUpdater.Domain/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Line	19	19
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-error.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
19.      <target xsi:type="File" name="Errors"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-error.log"
```

Hardcoded Absolute Path\Path 15:

Severity Information
Result State To Verify
Online Results https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=55
Status New
Detection Date 7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log" in CCMSUpdater_2/CCMSUpdater.Domain/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config	CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Line	22	22
Object	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log"	"C:\\logs\\CCMS\\errors\\${date:format=yyyy-MM-dd}-fatal.log"

Code Snippet
File Name CCMSUpdater_2/CCMSUpdater.Domain/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
22.      <target xsi:type="File" name="Fatals"
fileName="C:\logs\CCMS\errors\${date:format=yyyy-MM-dd}-fatal.log"
```

Hardcoded Absolute Path\Path 16:

Severity Information
Result State To Verify
Online Results https://checkmarx-

	app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=56
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/packages/NLog.Config.4.5.11/contentFiles/any/any/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/packages/NLog.Config.4.5.11/contentFiles/any/any/NLog.config	CCMSUpdater_2/packages/NLog.Config.4.5.11/contentFiles/any/any/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/packages/NLog.Config.4.5.11/contentFiles/any/any/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 17:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=57
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/packages/NLog.Config.4.5.11/content/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/packages/NLog.Config.4.5.11/content/NLog.config	CCMSUpdater_2/packages/NLog.Config.4.5.11/content/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/packages/NLog.Config.4.5.11/content/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 18:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=58
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/packages/NLog.Config.4.6.2/contentFiles/any/any/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/packages/NLog.Config.4.6.2/contentFiles/any/any/NLog.config	CCMSUpdater_2/packages/NLog.Config.4.6.2/contentFiles/any/any/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/packages/NLog.Config.4.6.2/contentFiles/any/any/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Hardcoded Absolute Path\Path 19:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=59
Status	New
Detection Date	7/5/2023 10:16:18 AM

The <?xml version="1.0" encoding="utf-8" ?> method references external files using a hard-coded, absolute path "c:\\temp\\nlog-internal.log" in CCMSUpdater_2/packages/NLog.Config.4.6.2/content/NLog.config at line 1.

	Source	Destination
File	CCMSUpdater_2/packages/NLog.Config.4.6.2/content/NLog.config	CCMSUpdater_2/packages/NLog.Config.4.6.2/content/NLog.config
Line	7	7
Object	"c:\\temp\\nlog-internal.log"	"c:\\temp\\nlog-internal.log"

Code Snippet
File Name CCMSUpdater_2/packages/NLog.Config.4.6.2/content/NLog.config
Method <?xml version="1.0" encoding="utf-8" ?>

```
....
7.        internalLogLevel="Off" internalLogFile="c:\temp\nlog-
internal.log">
```

Insufficient Logging of Sensitive Operations

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Insufficient Logging of Sensitive Operations Version:1

Categories

OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

Description

Insufficient Logging of Sensitive Operations\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=46
Status	New
Detection Date	7/5/2023 10:16:18 AM

In line 389, the sensitive operation LogInvalidSampleAsError is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs	CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs
Line	396	396
Object	LogInvalidSampleAsError	LogInvalidSampleAsError

Code Snippet

File Name	CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs
Method	private static void GenerateSamples(HelpPageApiModel apiModel, HelpPageSampleGenerator sampleGenerator)

```
....
396.                    LogInvalidSampleAsError(apiModel, item.Value);
```

Insufficient Logging of Sensitive Operations\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx-app.ubagroup.com/CxWebClient/ViewerMain.aspx?scanid=1000591&projectid=588&pathid=48
Status	New
Detection Date	7/5/2023 10:16:18 AM

In line 389, the sensitive operation LogInvalidSampleAsError is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination

File	CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs	CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs
Line	402	402
Object	LogInvalidSampleAsError	LogInvalidSampleAsError

Code Snippet
File Name CCMSUpdater_2/Router/Areas/HelpPage/HelpPageConfigurationExtensions.cs
Method private static void GenerateSamples(HelpPageApiModel apiModel, HelpPageSampleGenerator sampleGenerator)

```
....
402.                    LogInvalidSampleAsError(apiModel, item.Value);
```

HttpOnlyCookies In Config

Risk

What might happen

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

Cause

How does it happen

The web application framework, by default, does not set the "httpOnly" flag for the application's sessionid cookie and other sensitive application cookies. Likewise, the application does not explicitly use the "httpOnly" cookie flag, thus allowing client scripts to access the cookies by default.

General Recommendations

How to avoid it

- Always set the "httpOnly" flag for any sensitive server-side cookie. - It is highly recommended to implement HTTP Strict Transport Security (HSTS) in order to ensure that the cookie will be sent over a secured channel. - Configure the application to always use "httpOnly" cookies in the site-wide configuration file. - Set the `httpOnlyCookies` attribute on the `<httpCookies>` element, under `<system.web>` in your application's web.config, to `"true"`.

Source Code Examples

CSharp

ASP.NET web.config file without HttpOnly configured

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
      <system.web>
                ...
            <authentication mode="Forms">
                  <forms loginUrl="~/default.aspx" timeout="2880" />
            </authentication>
```

```
    </system.web>
</configuration>
```

Configuring Secure Cookies with HttpOnly

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.web>
            ...
            <authentication mode="Forms">
                  <forms loginUrl="~/default.aspx" timeout="2880" />
            </authentication>

            <httpCookies domain="MyDomain"
                  httpOnlyCookies="true"
            requireSSL="true" />

    </system.web>
</configuration>
```

Client JQuery Deprecated Symbols

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
However, even if deprecated code is used in a way that is completely secure, its very use and inclusion in the code base would encourage developers to re-use the deprecated element in the future, potentially leaving the application vulnerable to attack, which is why deprecated code should be eliminated from the code-base as a matter of practice.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.
Use of a deprecated API on client code may leave users vulnerable to browser-based attacks; this is exacerbated by the fact client-side code is available to any attacker with client access, who may be able to trivially detect use of this deprecated API.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

JavaScript
jQuery - Using the Deprecated $.parseJSON

```
$.parseJSON(json); // Legacy method for support of older browsers; tends to throw unexpected exceptions with certain control characters
```

Using a Native Call instead of Deprecated jQuery Calls

```
JSON.parse(json); // Native call to replace $.parseJSON(json)
```

Obtain Year via Deprecated JavaScript Method

```
var d = new Date();
```

```
var year = d.getYear(); // getYear() is deprecated and affected by Y2K; for a given year,
20xx, it will return 1xx.
```

Obtain Year via a Supported JavaScript Method

```
var d = new Date();
var year = d.getFullYear();
```

Invoking a Deprecated Function, Denoted Using JSDoc

```
/** @deprecated */
function myOldFunction() {
      /* Code that is deprecated */
}

myOldFunction();
```

Improper Resource Shutdown or Release

Risk

What might happen

Unreleased resources can cause a drain of those available for system use, eventually causing general reliability and availability problems, such as performance degradation, process bloat, and system instability. If a resource leak can be intentionally exploited by an attacker, it may be possible to cause a widespread DoS (Denial of Service) attack. This might even expose sensitive information between unprivileged users, if the resource continues to retain data or user id between subsequent allocations.

Cause

How does it happen

The application code allocates resource objects, but does not ensure these are always closed and released in a timely manner. This can include database connections, file handles, network sockets, or any other resource that needs to be released. In some cases, these might be released - but only if everything works as planned; if there is any runtime exception during the normal course of system operations, resources start to leak.

Note that even in managed-memory languages such as Java, these resources must be explicitly released. Many types of resource are not released even when the Garbage Collector runs; and even if the the object would eventually release the resource, we have no control over when the Garbage Collector does run.

General Recommendations

How to avoid it

- Always close and release all resources.
- Ensure resources are released (along with any other necessary cleanup) in a `finally { }` block. Do not close resources in a `catch { }` block, since this is not ensured to be called.
- Explicitly call .close() on any instance of a class that implements the `Closable` or `AutoClosable` interfaces.
- Alternatively, an even better solution is to use the try-with-resources idiom, in order to automatically close any defined `AutoClosable` instances.

Source Code Examples

Java

Unreleased Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
}
```

Explicit Release of Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
      finally {
            if ((con != null) && (!con.isClosed())) {
            con.close();
         }
     }
}
```

Automatic Implicit Release Using Try-With-Resources

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try (Connection con = DriverManager.getConnection(CONN_STRING)) {
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
}
```

Information Exposure via Headers

Risk

What might happen

Names and version numbers often denote a specific point in the life-cycle of a specific piece of technology. By exposing specific technologies by their names and version numbers to external actors, attackers may learn how to better target the server using known vulnerabilities and available exploits, research these specific technologies and develop new exploits themselves to fit a target of their desire, or document the specific technology at its specific location and wait for a point in time when a new vulnerability is unearthed to attack immediately. While obscurity is by no means security - reducing exposure of internal and system information is advised.

Cause

How does it happen

The application is configured to expose system information in its response headers, allowing attackers to gain valuable information of the underlying system.

General Recommendations

How to avoid it

- Always ensure environments do not leak information pertaining to software, operating systems and other technologies being used, such as their names, versions or settings, to reduce attacker visibility
- Specifically when dealing IIS and .NET Server headers, a web.config is required. If one does not exist, one has to be created for this purpose alone.

Source Code Examples

XML

Removing Server Headers from IIS Express in web.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.webServer>
        <security>
            <requestFiltering removeServerHeader="true" />
        </security>
        <httpProtocol>
            <customHeaders>
                <remove name="X-Powered-By" />
            </customHeaders>
        </httpProtocol>
    </system.webServer>
</configuration>
```

Removing Server Header from IIS in web.config

```
<configuration>
    <system.web>
        <!-- Additional configurations -->
        <httpRuntime targetFramework="4.6.1" enableVersionHeader="false" />
    </system.web>
```

```
</configuration>
```

CSharp
Removing Server Header from Kestrel During HostBuilder Creation

```
public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureWebHostDefaults(webBuilder =>
        {
            webBuilder.UseStartup<Startup>().UseKestrel(options => options.AddServerHeader =
false);
        });
}
```

Missing Content Security Policy

Risk

What might happen

The Content-Security-Policy header enforces that the source of content, such as the origin of a script, embedded (child) frame, embedding (parent) frame or image, are trusted and allowed by the current web-page; if, within the web-page, a content's source does not adhere to a strict Content Security Policy, it is promptly rejected by the browser. Failure to define a policy may leave the application's users exposed to Cross-Site Scripting (XSS) attacks, Clickjacking attacks, content forgery and more.

Cause

How does it happen

The Content-Security-Policy header is used by modern browsers as an indicator for trusted sources of content, including media, images, scripts, frames and more. If these policies are not explicitly defined, default browser behavior would allow untrusted content.

General Recommendations

How to avoid it

Explicitly set the Content-Security-Policy headers for all applicable policy types (frame, script, form, script, media, img etc.) according to business requirements and deployment layout of external file hosting services. Specifically, do not use a wildcard, '*', to specify these policies, as this would allow content from any external resource.
The Content-Security-Policy can be explicitly defined within web-application code, as a header managed by web-server configurations, or within `<meta>` tags in the HTML `<head>` section.

Source Code Examples

PHP

Restricting Content-Security-Policy to Only Obtain Embedded Content from Current Web-Application

```
<?php
      header("Content-Security-Policy: default-src 'none'; script-src 'self'; connect-src
'self'; img-src 'self'; style-src 'self';");
?>
```

Unencrypted Web Config File

Risk

What might happen

In .NET applications, web.config files often contain sensitive information such as service account login credentials or connection strings; this potentially sensitive data must be stored in a secure, encrypted container to prevent attackers with local file-system access from retrieving it.

Cause

How does it happen

The application utilizes a web.config file, which is stored locally on the file-system, and does not encrypt all sensitive elements within it.

General Recommendations

How to avoid it

Ensure sensitive contents of web.config files are encrypted at rest. For a best practice approach, utilize .NET aspnet_regiis.exe's tool to encrypt sensitive elements within web.config, so that they are read by the web-server, but cannot be plainly read from the file.

Source Code Examples

ASP

web.config File with Plain-Text Sensitive Content

```
<configuration>
  <connectionStrings>
      <add name="ServiceName" connectionString="[connection strings]" />
   </connectionStrings>
   <system.web>
     <machineKey validationKey="[validation key]" decryptionKey="[decryption key]" />
   </system.web>
</configuration>
```

web.config File with Encrypted Sensitive Content

```
<configuration>
  <connectionStrings configProtectionProvider="RsaProtectedConfigurationProvider">
      <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
         xmlns="http://www.w3.org/2001/04/xmlenc#">
         <EncryptionMethod Algorithm="[Encryption Algorithm]" />
         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
               <EncryptionMethod Algorithm="[Encryption Algorithm]" />
               <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                  <KeyName>RSA Key
                  </KeyName>
               </KeyInfo>
               <CipherData>[Cipher Value]</CipherValue>
               </CipherData>
            </EncryptedKey>
         </KeyInfo>
         <CipherData>[Cipher Value]</CipherValue>
```

```
        </CipherData>
      </EncryptedData>
   </connectionStrings>
   <system.web>
     <machineKey configProtectionProvider="RsaProtectedConfigurationProvider">
       <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
         <EncryptionMethod Algorithm="[Encryption Algorithm]" />
         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
           <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
             <EncryptionMethod Algorithm="[Encryption Algorithm]" />
             <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
               <KeyName>RSA Key
               </KeyName>
             </KeyInfo>
             <CipherData>
               <CipherValue>[Cipher Value]</CipherValue>
             </CipherData>
           </EncryptedKey>
         </KeyInfo>
         <CipherData>
           <CipherValue>[Cipher Value]</CipherValue>
         </CipherData>
       </EncryptedData>
     </machineKey>
   </system.web>
</configuration>
```

DebugEnabled

Risk

What might happen

Tests and debugging code are not intended to be deployed to the production environment, and can create unintended entry points, thus increasing the application's attack surface. Furthermore, this code is often not properly tested or maintained, and can retain historic vulnerabilities that were fixed in other parts of the codebase. Often, debug code will contain a functional "back door", by enabling the programmer to bypass operational security mechanisms, such as authentication or access controls.

Cause

How does it happen

During application development, it is common for programmers to implement specialized code, in order to ease debugging and testing. Often the programmer will even enable the debug code to bypass security mechanisms, so as to focus the tests on the specific functionality and isolate it from the security architecture.
This debug or test code is not removed from the codebase, and is then included in the software build and deployed to the production environment.

General Recommendations

How to avoid it

- Remove all debug code before deploying or building the application. Ensure the configuration settings are not defined to enable debug mode. - Implement all test code via a dedicated test framework, which can isolate the test case code from the rest of the application. - Avoid implementing special "test code", "debugging-time" functionality, or "secret" interfaces or parameters in the application code itself. - Define and implement a standard and automatic build / deployment process, using dedicated CI / CD tools, that can automatically configure the deployed application, exclude all temporary code, and include only intended application code.

Source Code Examples

Java

Main in Servlet

```
public class AppServlet extends HttpServlet {
      protected void doGet(HttpServletRequest request, HttpServletResponse response)
                              throws ServletException, IOException {
            // handle request
      }

      private static String MODE = "";
      public static void main(String[] args) {
            // initialize app for debugging and testing
            MODE = "DEBUGGING";
      }
}
```

Ruby

Internal Test Method

```
class AppClass
      def run_app
       # Run the app
    end
      def test_app
       # Test and debug the app
    end
end
```

CSharp
Debug Configuration

```
<configuration>
      <system.web>
      <compilation debug="false" />
    </system.web>
</configuration>
```

Missing X Frame Options

Risk

What might happen

Allowing setting of web-pages inside of a frame in an untrusted web-page will leave these web-pages vulnerable to Clickjacking, otherwise known as a redress attack. This may allow an attacker to redress a vulnerable web-page by setting it inside a frame within a malicious web-page. By crafting a convincing malicious web-page, the attacker can then use the overlayed redress to convince the user to click a certain area of the screen, unknowingly clicking inside the frame containing the vulnerable web-page, and thus performing actions within the user's context on the attacker's behalf.

Cause

How does it happen

Failure to utilize the "X-FRAME-OPTIONS" header will likely allow attackers to perform Clickjacking attacks. Properly utilizing the "X-FRAME-OPTIONS" header would indicate to the browser to disallow embedding the web-page within a frame, mitigating this risk, if the browser supports this header. All modern browsers support this header by default.

General Recommendations

How to avoid it

Utilize the "X-FRAME-OPTIONS" header flags according to business requirements to restrict browsers that support this header from allowing embedding web-pages in a frame:
· "X-Frame-Options: DENY" will indicate to the browser to disallow embedding any web-page inside a frame, including the current web-site.
· "X-Frame-Options: SAMEORIGIN" will indicate to the browser to disallow embedding any web-page inside a frame, excluding the current web-site.
· "X-Frame-Options: ALLOW-FROM https://example.com/" will indicate to the browser to disallow embedding any web-page inside a frame, excluding the web-site listed after the ALLOW-FROM parameter.

Source Code Examples

Java

Setting the "DENY" Flag on a Response

```
response.addHeader("X-Frame-Options", "DENY");
```

Hardcoded Absolute Path

Risk

What might happen

Generally, hardcoding absolute paths makes the application brittle, and will prevent the program from operating properly in some environments that do not have the identical file system structure. This will also cause software maintenance problems in future versions of the application, if the design or requirements were to change.

Additionally, if the application uses this path to read or write data, this can cause a breach of confidentiality or allow malicious input into the program. In some situations, this vulnerability might even allow a malicious user to override the expected functionality, and cause the application to run any arbitrary program and execute any code the attacker deploys to the server.

Cause

How does it happen

Hardcoded paths are less flexible, and do not allow the application to account for changes in the environment. For example, the program might be installed in a different directory than the default. Likewise, different system languages and OS architectures can change the names of the system folders; for example, in a Spanish Windows machine there could be "`C:\Archivos de programa (x86)\`" instead of "`C:\Program Files\`".

Moreover, on Windows by default all directories and files created outside of the system folders and outside the user's profile, will be allow full read and write access to any authenticated user. An unauthorized, malicious user could access any sensitive data in these folders, despite the application assuming they are protected. Even worse, an attacker could overwrite existing programs in these unprotected folders and plant malicious code, which will be activated by the application.

General Recommendations

How to avoid it

- Do not hardcode absolute paths into the application.
- Instead, store the absolute paths in an external configuration file, that can be modified as required for each environment.
- Alternatively, use paths relative to the current application, if the target file is in a subdirectory of the application's root.
- Do not assume a specific file system structure, outside of the application's subdirectories. On Windows, use the built-in expandable variables, such as `%WINDIR%`, `%PROGRAMFILES%`, and `%TEMP%`.
- On Linux and other OS where available, implement a system jail (chroot) for the application, and store all programs and data files there only.
- Prefer storing all executables under the protected program directory (under "`C:\Program Files\`" by default on Windows).
- Do not store sensitive data or configuration files in arbitrary folders. Likewise, do not store data files in the program directory. Instead, use the designated folders as intended, i.e. `%PROGRAMDATA%` and `%APPDATA%` on Windows, respectively.
- Configure hardened permissions to the most restricted as possible, according to the Principle of Least Privilege. Consider implementing this automatically in the installation and setup routines.

Source Code Examples

Java

Hardcoded Path to Data File

```
public File getLogFile() {
      String filename = "C:\Logs\myapp.log";
      File logFile = new File(filename);

      return logFile;
}
```

Configured Path for Data File

```
public File getLogFile() {
      Properties props = this.Properties;
      String filename = (String)props.get("logDirectory") + (String)props.get("logFilename");

      File logFile = new File(filename);

      return logFile;
}
```

Insufficient Logging of Sensitive Operations

Risk

What might happen

If sensitive operations executions is not recorded, there will be no trail for forensic analysis and discovering the cause of possible associated problems or the source of attacks may become more difficult or impossible.

Cause

How does it happen

The execution of sensitive operations is not logged.

General Recommendations

How to avoid it

Use a logging mechanism that supports multiple levels of detail. Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks.

Source Code Examples

CSharp

Insufficient Logging of a HttpDelete action

```
[HttpDelete]
[Route("/movie/{id}")]
public ActionResult HandleMovies(int id)
{
    doSomthing();
}
```

Insufficient Logging of Sensitive Operation

```
public void DoSomethingWith1(int id)
{
    var msg = DatabaseInstance.Delete(id);
}
```

Sensitive Operation Logged

```
[HttpPost]
[Route("/login")]
public ActionResult handler1_v2()
{
    doThings();
    logger.Info( "Login of user occurred");
}
```

```

```

Sensitive Operation Logged (case2)

```
public void DoSomethingWith2(int id)
{
    var msg = DatabaseInstance.Delete(id);
    logger.Info( "Delete of something occurred");
}
```

Scanned Languages

Language	Hash Number	Change Date
CSharp	5845120472948080	1/13/2022
JavaScript	9095271965336651	1/13/2022
VbScript	0386000544005133	1/13/2022
PLSQL	4873116881329330	1/13/2022
Common	0318477963775793	1/13/2022