wp-surchargepay-api_prod Scan Report

Project Name	wp-surchargepay-api_prod
Scan Start	Thursday, July 24, 2025 11:47:42 PM
Preset	ASA-Default
Scan Time	00h:00m:31s
Lines Of Code Scanned	25394
Files Scanned	149
Report Creation Time	Friday, July 25, 2025 2:15:08 PM
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290
Team	Paymetric
Checkmarx Version	V 9.4.4 HF27
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: To Verify, Not Exploitable, Confirmed, Critical, Proposed Not Exploitable, Approved Exception, Proposed for Exception, Backlog

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
CVSSv3	All
OWASP Top 10 2021	All
ASD STIG 4.10	All
OWASP Top 10 API	All
OWASP Top 10 2010	All

MOIS(KISA) Secure Coding 2021	All
SANS top 25	All
FIS Policy Vulnerabilities	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
CVSSv3	None
OWASP Top 10 2021	None
ASD STIG 4.10	None
OWASP Top 10 API	None
OWASP Top 10 2010	None
MOIS(KISA) Secure Coding 2021	None
SANS top 25	None
FIS Policy Vulnerabilities	None

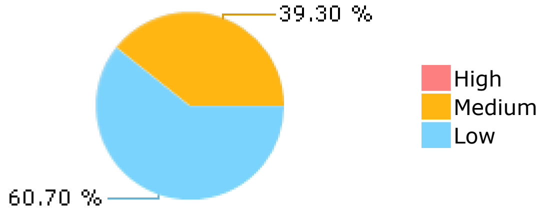
Results Limit

Results limit per query was set to 50

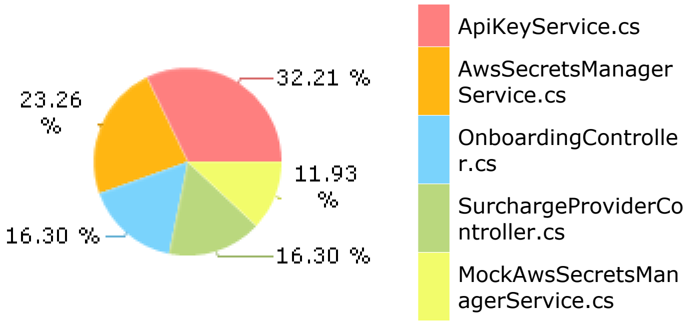
Selected Queries

Selected queries are listed in Result Summary

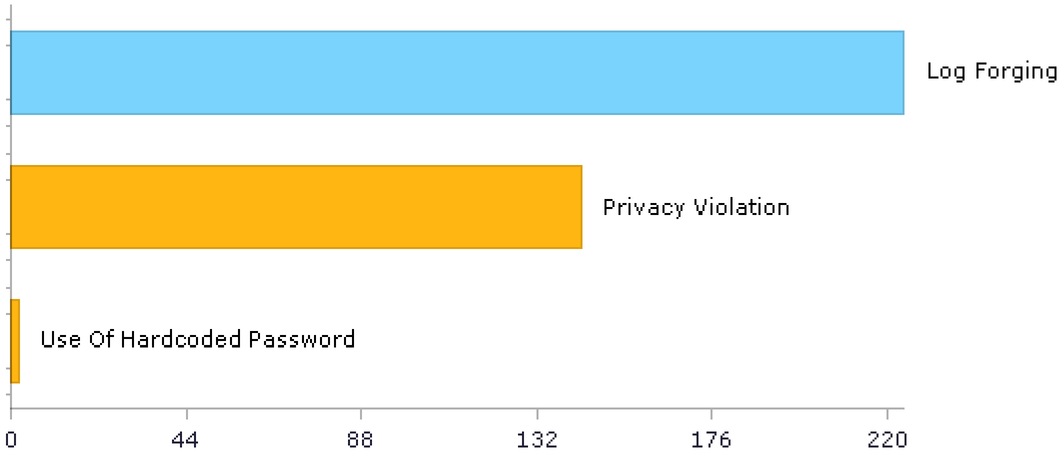
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - FIS Policy Vulnerabilities

Category	Issues Found	Best Fix Locations
High*	0	0
OWASP Medium*	145	15
OWASP Low*	224	35

* 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*	143	13
A2-Cryptographic Failures*	0	0
A3-Injection*	0	0
A4-Insecure Design*	0	0
A5-Security Misconfiguration*	0	0
A6-Vulnerable and Outdated Components*	0	0
A7-Identification and Authentication Failures*	2	2
A8-Software and Data Integrity Failures*	0	0
A9-Security Logging and Monitoring Failures*	224	35
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 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	224	35
A2-Broken Authentication*	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	2	2
A3-Sensitive Data Exposure*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	143	13
A4-XML External Entities (XXE)*	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration *	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization*	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* 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	2	2
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References*	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration *	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure*	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	143	13
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)*	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards*	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

* 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*	367	48
PCI DSS (3.2.1) - 6.5.2 - Buffer overflows*	0	0
PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage*	2	2
PCI DSS (3.2.1) - 6.5.4 - Insecure communications*	0	0
PCI DSS (3.2.1) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)*	0	0
PCI DSS (3.2.1) - 6.5.8 - Improper access control*	0	0
PCI DSS (3.2.1) - 6.5.9 - Cross-site request forgery*	0	0
PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management*	0	0

* 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.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	145	15
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.	224	35

* 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)*	224	35
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)*	0	0
SC-13 Cryptographic Protection (P1)*	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)*	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)*	2	2
SC-4 Information in Shared Resources (P1)*	143	13
SC-5 Denial of Service Protection (P1)*	0	0
SC-8 Transmission Confidentiality and Integrity (P1)*	0	0
SI-10 Information Input Validation (P1)*	0	0
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)*	0	0
SI-16 Memory Protection (P1)*	0	0

***** 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 - CVSSv3

Category	Issues Found	Best Fix Locations
Critical*	0	0
High*	0	0
Medium*	224	35
Low*	0	0
Info*	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 - MOIS(KISA) Secure Coding 2021

Category	Issues Found	Best Fix Locations
MOIS(KISA) API misuse*	0	0
MOIS(KISA) Code error*	0	0
MOIS(KISA) Encapsulation*	0	0
MOIS(KISA) Error processing*	0	0
MOIS(KISA) Security Functions*	145	15
MOIS(KISA) Time and status*	0	0
MOIS(KISA) Verification and representation of input data*	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 - SANS top 25

Category	Issues Found	Best Fix Locations
SANS top 25*	145	15

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

Scan Summary - ASD STIG 4.10

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

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

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

APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0
APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.*	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.*	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.*	2	2
APSC-DV-001850 - CAT I The application must not display passwords/PINs as clear text.	0	0
APSC-DV-001750 - CAT I The application must transmit only cryptographically-protected passwords.	0	0
APSC-DV-001760 - CAT II The application must enforce 24 hours/1 day as the minimum password lifetime.	0	0
APSC-DV-001770 - CAT II The application must enforce a 60-day maximum password lifetime restriction.	0	0
APSC-DV-001780 - CAT II The application must prohibit password reuse for a minimum of five generations.	0	0

APSC-DV-001790 - CAT II The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	0	0
APSC-DV-001795 - CAT II The application password must not be changeable by users other than the administrator or the user with which the password is associated.	0	0
APSC-DV-001800 - CAT II The application must terminate existing user sessions upon account deletion.	0	0
APSC-DV-001820 - CAT I The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	0	0
APSC-DV-001830 - CAT II The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	0	0
APSC-DV-001870 - CAT II The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	0	0
APSC-DV-001810 - CAT I The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	0	0
APSC-DV-001840 - CAT II The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	0	0
APSC-DV-001860 - CAT II The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	0	0
APSC-DV-001880 - CAT II The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-001890 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-002050 - CAT II Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	0	0
APSC-DV-001900 - CAT II The application must accept FICAM-approved third-party credentials.	0	0
APSC-DV-001910 - CAT II The application must conform to FICAM-issued profiles.	0	0
APSC-DV-001930 - CAT II Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	0	0
APSC-DV-000310 - CAT III The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	0	0
APSC-DV-001940 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001950 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001960 - CAT II Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001970 - CAT II The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001980 - CAT II The application must terminate all sessions and network connections when non-local maintenance is completed.	0	0
APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.	0	0
APSC-DV-002000 - CAT II The application must terminate all network connections associated with a communications session at the end of the session.	0	0
APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	0	0
APSC-DV-002020 - CAT II The application must utilize FIPS-validated cryptographic modules when signing application components.	0	0
APSC-DV-002030 - CAT II The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	0	0

APSC-DV-002040 - CAT II The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	0	0
APSC-DV-002150 - CAT II The application user interface must be either physically or logically separated from data storage and management interfaces.	0	0
APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.	0	0
APSC-DV-002220 - CAT II The application must set the secure flag on session cookies.	0	0
APSC-DV-002230 - CAT I The application must not expose session IDs.*	0	0
APSC-DV-002240 - CAT I The application must destroy the session ID value and/or cookie on logoff or browser close.*	0	0
APSC-DV-002250 - CAT II Applications must use system-generated session identifiers that protect against session fixation.*	0	0
APSC-DV-002260 - CAT II Applications must validate session identifiers.*	0	0
APSC-DV-002270 - CAT II Applications must not use URL embedded session IDs.	0	0
APSC-DV-002280 - CAT II The application must not re-use or recycle session IDs.	0	0
APSC-DV-002290 - CAT II The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.*	0	0
APSC-DV-002300 - CAT II The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	0	0
APSC-DV-002310 - CAT I The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	0	0
APSC-DV-002320 - CAT II In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	0	0
APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.*	143	13
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.*	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.*	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0
APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of	0	0

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

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

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

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

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

***** 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*	0	0
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

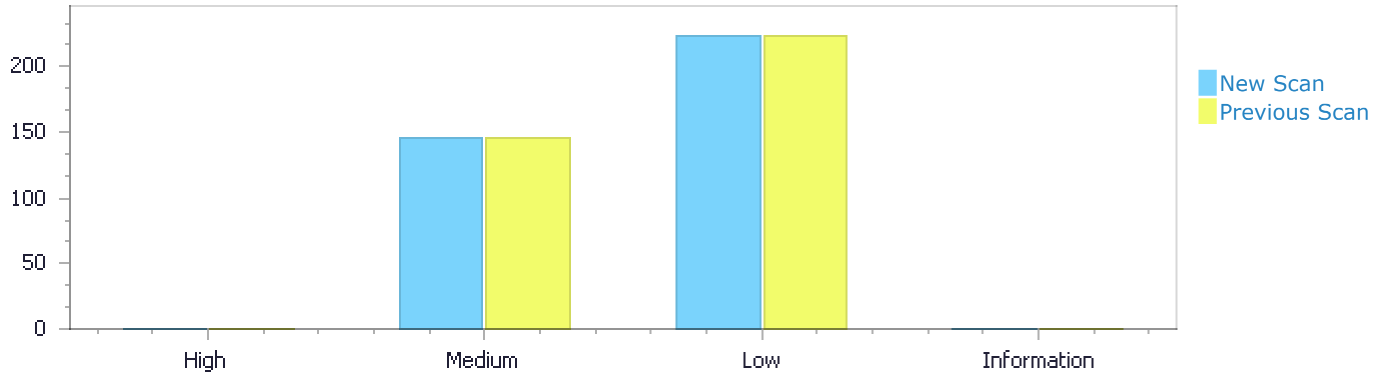
***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Results Distribution By Status

Compared to project scan from 7/24/2025 10:19 PM

	High	Medium	Low	Information	Total
New Issues	0	0	0	0	0
Recurrent Issues	0	145	224	0	369
Total	0	145	224	0	369

Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
To Verify	0	145	224	0	369
Not Exploitable	0	0	0	0	0
Confirmed	0	0	0	0	0
Critical	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Approved Exception	0	0	0	0	0
Proposed for Exception	0	0	0	0	0
Backlog	0	0	0	0	0
Total	0	145	224	0	369

Result Summary

Vulnerability Type	Occurrences	Severity
Privacy Violation	143	Medium

Use Of Hardcoded Password	2	Medium
Log Forging	224	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
Services/ApiKeyService.cs	95
Services/AwsSecretsManagerService.cs	91
Services/MockAwsSecretsManagerService.cs	36
Controllers/V1/AdminController.cs	14
Controllers/V1/SurchargeProviderController.cs	13
Services/SurchargeProviderService.cs	13
Repositories/SurchargeProviderRepository.cs	13
Controllers/MockController.cs	9
Services/RequestSigningService.cs	9
Services/SurchargeProviderConfigService.cs	9

Scan Results Details

Privacy Violation

Query Path:
CSharp\Teams Queries\CxServer\WorldPay\CSharp Medium Threat\Privacy Violation Version:1

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A1-Broken Access Control
ASD STIG 4.10: 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.
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
FIS Policy Vulnerabilities: OWASP Medium

Description

Privacy Violation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=227
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Controllers/V1/AdminController.cs
Line	75	75
Object	secretName	LogInformation

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
75.   _logger.LogInformation("Looking up admin secret: {SecretName}",
secretName);
```

Privacy Violation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=228
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKey at line 33 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/MockAwsSecretsManagerService.cs
Line	66	65
Object	_secretsManager	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GenerateInitialApiKey([FromBody] JsonElement request)

```
....
66.   await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=229
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	784	65
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
784.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=230
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	920	65
Object	_secretsManager	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
920.  await _secretsManager.StoreSecretAsync(merchantSecretName,
JsonSerializer.Serialize(newSecretValue));
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 5:

Severity	Medium
Result State	To Verify

Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=231
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RegenerateSecretAsync at line 943 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	979	65
Object	_secretsManager	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<ApiKeyResponse> RegenerateSecretAsync(string merchantId)

```
....
979.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=232
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKeyAsync at line 1024 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1108	65
Object	_secretsManager	LogError

Code Snippet

File Name	Services/ApiKeyService.cs

Method	public async Task<GenerateInitialApiKeyResponse> GenerateInitialApiKeyAsync(Guid merchantId, GenerateInitialApiKeyRequest request)

```
....
1108.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=233
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateAdminApiKeyAsync at line 1148 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1194	65
Object	_secretsManager	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<GenerateApiKeyResponse> RotateAdminApiKeyAsync(string serviceName)

```
....
1194.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=234
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKey at line 33 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/MockAwsSecretsManagerService.cs
Line	66	65
Object	secretName	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GenerateInitialApiKey([FromBody] JsonElement request)

```
....
66.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=235
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	784	65
Object	adminSecretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
784.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=236
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	920	65
Object	merchantSecretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
920.  await _secretsManager.StoreSecretAsync(merchantSecretName,
JsonSerializer.Serialize(newSecretValue));
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=237
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKeyAsync at line 1024 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1108	65
Object	secretName	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<GenerateInitialApiKeyResponse> GenerateInitialApiKeyAsync(Guid merchantId, GenerateInitialApiKeyRequest request)

```
....
1108.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=238
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateAdminApiKeyAsync at line 1148 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1194	65

Object	adminSecretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> RotateAdminApiKeyAsync(string serviceName)

```
....
1194.  await _secretsManager.StoreSecretAsync(adminSecretName, 
JsonSerializer.Serialize(secretValue));
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.  _logger.LogError(ex, "Error storing secret {SecretName}", 
secretName);
```

Privacy Violation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=239
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	658	65
Object	_secretsManager	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
658.  var secret = await 
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task StoreSecretAsync(string secretName, string secretValue)

```
....
65.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=240
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKey at line 33 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/AwsSecretsManagerService.cs
Line	66	88
Object	_secretsManager	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GenerateInitialApiKey([FromBody] JsonElement request)

```
....
66.   await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=241
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs

Line	784	88
Object	_secretsManager	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
784.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs
Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=242
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	920	88
Object	_secretsManager	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
920.  await _secretsManager.StoreSecretAsync(merchantSecretName,
JsonSerializer.Serialize(newSecretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs
Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=243
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RegenerateSecretAsync at line 943 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	979	88
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyResponse> RegenerateSecretAsync(string merchantId)

```
....
979.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=244
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKeyAsync at line 1024 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1108	88

Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateInitialApiKeyResponse> GenerateInitialApiKeyAsync(Guid merchantId, GenerateInitialApiKeyRequest request)

```
....
1108.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=245
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateAdminApiKeyAsync at line 1148 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1194	88
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> RotateAdminApiKeyAsync(string serviceName)

```
....
1194.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=246
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKey at line 33 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/AwsSecretsManagerService.cs
Line	66	88
Object	secretName	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GenerateInitialApiKey([FromBody] JsonElement request)

```
....
66.   await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=247
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs

Line	784	88
Object	adminSecretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
784.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=248
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	920	88
Object	merchantSecretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
920.  await _secretsManager.StoreSecretAsync(merchantSecretName,
JsonSerializer.Serialize(newSecretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=249
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateInitialApiKeyAsync at line 1024 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1108	88
Object	secretName	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<GenerateInitialApiKeyResponse> GenerateInitialApiKeyAsync(Guid merchantId, GenerateInitialApiKeyRequest request)

```
....
1108.  await _secretsManager.StoreSecretAsync(secretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=250
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateAdminApiKeyAsync at line 1148 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination

File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1194	88
Object	adminSecretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> RotateAdminApiKeyAsync(string serviceName)

```
....
1194.  await _secretsManager.StoreSecretAsync(adminSecretName,
JsonSerializer.Serialize(secretValue));
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.  _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=251
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	658	88
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
658.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task StoreSecretAsync(string secretName, string secretValue)

```
....
88.   _logger.LogError(ex, "Error storing secret {SecretName}",
secretName);
```

Privacy Violation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=252
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	78	34
Object	secretsManager	LogError

Code Snippet

File Name Controllers/V1/AdminController.cs

Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.   var secretJson = await secretsManager.GetSecretAsync(secretName);
```

▾

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=253
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKeyAsync at line 1213 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs

Line	1225	34
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyRevokeResponse> RevokeAdminApiKeyAsync(string serviceName)

```
....
1225.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(adminSecretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=254
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	78	34
Object	secretName	LogError

Code Snippet

File Name Controllers/V1/AdminController.cs

Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.  var secretJson = await secretsManager.GetSecretAsync(secretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=255
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/MockAwsSecretsManagerService.cs
Line	93	34
Object	secretName	LogError

Code Snippet

File Name	Controllers/MockController.cs
Method	public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
93.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=256
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ValidateMerchantApiKeyAsync at line 184 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination

File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	188	34
Object	secretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method private async Task<bool> ValidateMerchantApiKeyAsync(string merchantId, string apiKey, string timestamp, string nonce, string signature, string serviceName)

```
....
188.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=257
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKeyAsync at line 280 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	339	34
Object	secretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyInfo> UpdateApiKeyAsync(UpdateApiKeyRequest request, OnboardingMetadata onboardingMetadata)

```
....
339.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=258
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKeyAsync at line 382 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	418	34
Object	secretName	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<bool> RevokeApiKeyAsync(RevokeApiKeyRequest request)

```
....
418.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=259
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	658	34
Object	secretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
658.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▾

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=260
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKeyAsync at line 1213 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1225	34
Object	adminSecretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyRevokeResponse> RevokeAdminApiKeyAsync(string serviceName)

```
....
1225.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(adminSecretName);
```

▾

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=261
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKeyAsync at line 382 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	424	34
Object	_secretsManager	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<bool> RevokeApiKeyAsync(RevokeApiKeyRequest request)

```
....
424.   await _secretsManager.UpdateSecretAsync(secretName, secret); // <-
- Use update, not create
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=262
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	78	49
Object	secretsManager	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.   var secretJson = await secretsManager.GetSecretAsync(secretName);
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=263
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKeyAsync at line 1213 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1225	49
Object	_secretsManager	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyRevokeResponse> RevokeAdminApiKeyAsync(string serviceName)

```
....
1225.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(adminSecretName);
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=264
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	78	49
Object	secretName	LogError

Code Snippet

File Name	Controllers/V1/AdminController.cs
Method	public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.  var secretJson = await secretsManager.GetSecretAsync(secretName);
```

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task<string?> GetSecretAsync(string secretName)

```
....
49.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=265
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/AwsSecretsManagerService.cs
Line	93	49

Object	secretName	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
93.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 40:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=266
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ValidateMerchantApiKeyAsync at line 184 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	188	49
Object	secretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method private async Task<bool> ValidateMerchantApiKeyAsync(string merchantId, string apiKey, string timestamp, string nonce, string signature, string serviceName)

```
....
188.  var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 41:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=267
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKeyAsync at line 280 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	339	49
Object	secretName	LogError

Code Snippet

File Name	Services/ApiKeyService.cs
Method	public async Task<ApiKeyInfo> UpdateApiKeyAsync(UpdateApiKeyRequest request, OnboardingMetadata onboardingMetadata)

```
....
339.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 42:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=268
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKeyAsync at line 382 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs

Line	418	49
Object	secretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<bool> RevokeApiKeyAsync(RevokeApiKeyRequest request)

```
....
418.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 43:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=269
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	658	49
Object	secretName	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
658.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=270
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKeyAsync at line 1213 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs
Line	1225	49
Object	adminSecretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyRevokeResponse> RevokeAdminApiKeyAsync(string serviceName)

```
....
1225.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(adminSecretName);
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 45:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=271
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKeyAsync at line 382 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/AwsSecretsManagerService.cs

Line	424	49
Object	_secretsManager	LogError

Code Snippet
File Name Services/ApiKeyService.cs
Method public async Task<bool> RevokeApiKeyAsync(RevokeApiKeyRequest request)

```
....
424.  await _secretsManager.UpdateSecretAsync(secretName, secret); // <-
- Use update, not create
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=272
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	78	51
Object	secretsManager	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.  var secretJson = await secretsManager.GetSecretAsync(secretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
51.  _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Privacy Violation\Path 47:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=273
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKeyAsync at line 1213 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	1225	51
Object	_secretsManager	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyRevokeResponse> RevokeAdminApiKeyAsync(string serviceName)

```
....
1225.   var secret = await 
_secretsManager.GetSecretAsync<ApiKeySecret>(adminSecretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
51.  _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Privacy Violation\Path 48:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=274
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination

File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	78	51
Object	secretName	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
78.   var secretJson = await secretsManager.GetSecretAsync(secretName);
```

▼

File Name Services/MockAwsSecretsManagerService.cs
Method public Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
51.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 49:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=275
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Controllers/MockController.cs	Services/MockAwsSecretsManagerService.cs
Line	93	51
Object	secretName	LogError

Code Snippet
File Name Controllers/MockController.cs
Method public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
93.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

▼

File Name Services/MockAwsSecretsManagerService.cs
Method public Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
51.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Privacy Violation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=276
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ValidateMerchantApiKeyAsync at line 184 of Services/ApiKeyService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Services/ApiKeyService.cs	Services/MockAwsSecretsManagerService.cs
Line	188	51
Object	secretName	LogError

Code Snippet

File Name Services/ApiKeyService.cs

Method private async Task<bool> ValidateMerchantApiKeyAsync(string merchantId, string apiKey, string timestamp, string nonce, string signature, string serviceName)

```
....
188.   var secret = await
_secretsManager.GetSecretAsync<ApiKeySecret>(secretName);
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
51.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Use Of Hardcoded Password

Query Path:
CSharp\Teams Queries\SP\CSharp Low Visibility\Use Of Hardcoded Password Version:3

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A2-Broken Authentication and Session Management
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A2-Broken Authentication
OWASP Top 10 2021: A7-Identification and Authentication Failures

ASD STIG 4.10: APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
FIS Policy Vulnerabilities: OWASP Medium

Description

Use Of Hardcoded Password\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=83
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

The application uses the hard-coded password Password for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 3 of appsettings.Development.json appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination
File	appsettings.Development.json	appsettings.Development.json
Line	3	3
Object	Password	Password

Code Snippet
File Name appsettings.Development.json
Method "DefaultConnection": "Host=localhost;Port=5432;Database=surchargepay;Username=svc_surchargepay_api;Password=api_default_password"

```
....
3.   "DefaultConnection": "Host=localhost;Port=5432;Database=surchargepay;Username=svc_surchargepay_api;Password=api_default_password"
```

Use Of Hardcoded Password\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=85
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

The application uses the hard-coded password Password for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 3 of appsettings.json appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination
File	appsettings.json	appsettings.json
Line	3	3
Object	Password	Password

Code Snippet

File Name	appsettings.json
Method	"DefaultConnection": "Host=localhost;Port=5432;Database=surchargepay;Username=svc_surchargepay_api;Password=api_default_password"

```
....
   "DefaultConnection":
"Host=localhost;Port=5432;Database=surchargepay;Username=svc_surchargepa
y_api;Password=api_default_password"
```

Log Forging

Query Path:
CSharp\Teams Queries\CxServer\SP\WorldPay\Paymetric\CSharp Low Visibility\Log Forging Version:2

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: AU-9 Protection of Audit Information (P1)
OWASP Top 10 2017: A1-Injection
CVSSv3: Medium
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
FIS Policy Vulnerabilities: OWASP Low

Description

Log Forging\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=1
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Controllers/V1/SurchargeProviderController.cs
Line	365	585
Object	merchantId	LogInformation

Code Snippet

File Name	Controllers/V1/SurchargeProviderController.cs
Method	public async Task<IActionResult> UpdateProvider(string merchantId, Guid id, [FromBody] SurchargeProviderUpdateRequest request)

```
....
365.  public async Task<IActionResult> UpdateProvider(string merchantId,
Guid id, [FromBody] SurchargeProviderUpdateRequest request)
....
585.  _logger.LogInformation("Successfully updated surcharge provider:
{ProviderId} ({ProviderName}) for merchant: {MerchantId}",
```

Log Forging\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=2
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Controllers/V1/SurchargeProviderController.cs
Line	365	585
Object	request	LogInformation

Code Snippet

File Name	Controllers/V1/SurchargeProviderController.cs
Method	public async Task<IActionResult> UpdateProvider(string merchantId, Guid id, [FromBody] SurchargeProviderUpdateRequest request)

```
....
365.  public async Task<IActionResult> UpdateProvider(string merchantId,
Guid id, [FromBody] SurchargeProviderUpdateRequest request)
....
585.  _logger.LogInformation("Successfully updated surcharge provider:
{ProviderId} ({ProviderName}) for merchant: {MerchantId}",
```

Log Forging\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=3
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method DeleteProvider at line 627 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in SoftDeleteAsync at line 310 of Services/SurchargeProviderService.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderControll	Services/SurchargeProviderService.cs

	er.cs	
Line	627	320
Object	merchantId	LogError

Code Snippet
File Name Controllers/V1/SurchargeProviderController.cs
Method public async Task<IActionResult> DeleteProvider(string merchantId, Guid id)

```
....
627.  public async Task<IActionResult> DeleteProvider(string merchantId,
Guid id)
```

▼

File Name Services/SurchargeProviderService.cs

Method public async Task<bool> SoftDeleteAsync(Guid id, string deletedBy)

```
....
320.  _logger.LogError(ex, "Error soft deleting provider {ProviderId} by
{DeletedBy}", id, deletedBy);
```

Log Forging\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=4
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element req. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	141	69
Object	req	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> RevokeAdminApiKey(

```
....
141.  [FromBody] AdminKeyServiceNameRequest req,
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=5
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKey at line 441 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	441	69
Object	request	LogError

Code Snippet

File Name	Controllers/V1/OnboardingController.cs
Method	public async Task<IActionResult> UpdateApiKey([FromBody] UpdateApiKeyRequest request)

```
....
441.   public async Task<IActionResult> UpdateApiKey([FromBody]
UpdateApiKeyRequest request)
```

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=6
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKey at line 529 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	529	69
Object	request	LogError

Code Snippet
File Name	Controllers/V1/OnboardingController.cs
Method	public async Task<IActionResult> RevokeApiKey([FromBody] RevokeApiKeyRequest request)

```
....
529.  public async Task<IActionResult> RevokeApiKey([FromBody]
RevokeApiKeyRequest request)
```

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=7
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	47	69
Object	request	LogError

Code Snippet
File Name	Controllers/V1/AdminController.cs
Method	public async Task<IActionResult> GenerateAdminApiKey(

```
....
47.   [FromBody] GenerateApiKeyRequest request,
```

File Name	Services/AwsSecretsManagerService.cs

Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=8
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	824	69
Object	request	LogError

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.   public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 9:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=9
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element secretsManager. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	48	69
Object	secretsManager	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
48.   [FromServices] IAwsSecretsManagerService secretsManager,
```

▼

File Name Services/AwsSecretsManagerService.cs
Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 10:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=10
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element apiKeyService. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	142	69
Object	apiKeyService	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> RevokeAdminApiKey(

```
....
142.   [FromServices] IApiKeyService apiKeyService)
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Log Forging\Path 11:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=11
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync<T> at line 54 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/MockController.cs	Services/AwsSecretsManagerService.cs
Line	79	69
Object	request	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
79.   public async Task<IActionResult> GetApiKeySecret([FromBody] 
JsonElement request)
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<T?> GetSecretAsync<T>(string secretName) where T : class

```
....
69.   _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Log Forging\Path 12:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=12
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKey at line 441 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in UpdateApiKeyAsync at line 280 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	441	310
Object	request	LogWarning

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> UpdateApiKey([FromBody] UpdateApiKeyRequest request)

```
....
441.  public async Task<IActionResult> UpdateApiKey([FromBody]
UpdateApiKeyRequest request)
```

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyInfo> UpdateApiKeyAsync(UpdateApiKeyRequest request, OnboardingMetadata onboardingMetadata)

```
....
310.  _logger.LogWarning("API key {ApiKey} is not active (status:
{Status})", request.ApiKey, apiKeyEntity.Status);
```

Log Forging\Path 13:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=13
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ProcessSale at line 96 of Controllers/V1/SurchargeController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in ProcessSale at line 96 of Controllers/V1/SurchargeController.cs.

	Source	Destination
File	Controllers/V1/SurchargeController.cs	Controllers/V1/SurchargeController.cs
Line	96	115
Object	request	LogWarning

Code Snippet

File Name Controllers/V1/SurchargeController.cs

Method public async Task<IActionResult> ProcessSale([FromBody] SurchargeSaleRequest request)

```
....
96.  public async Task<IActionResult> ProcessSale([FromBody]
SurchargeSaleRequest request)
....
115.  _logger.LogWarning("Invalid merchant ID format in claims:
{MerchantId} for transaction: {CorrelationId}",
```

Log Forging\Path 14:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=14
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ProcessRefund at line 159 of Controllers/V1/SurchargeController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in ProcessRefund at line 159 of Controllers/V1/SurchargeController.cs.

	Source	Destination
File	Controllers/V1/SurchargeController.cs	Controllers/V1/SurchargeController.cs
Line	159	177
Object	request	LogWarning

Code Snippet

File Name Controllers/V1/SurchargeController.cs

Method public async Task<IActionResult> ProcessRefund([FromBody] SurchargeRefundRequest request)

```
....
159.  public async Task<IActionResult> ProcessRefund([FromBody]
SurchargeRefundRequest request)
....
177.  _logger.LogWarning("Invalid merchant ID format in claims:
{MerchantId} for transaction: {CorrelationId}",
```

Log Forging\Path 15:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=15
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element secretsManager. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Controllers/V1/AdminController.cs

Line	48	91
Object	secretsManager	LogWarning

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
48.  [FromServices] IAwsSecretsManagerService secretsManager,
....
91.  _logger.LogWarning("Admin Secret (from DB): {StoredSecret} |
Provided: {ProvidedSecret}", Mask(storedSecretStr),
Mask(providedSecretStr));
```

Log Forging\Path 16:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=16
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Controllers/V1/AdminController.cs
Line	47	91
Object	request	LogWarning

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
47.  [FromBody] GenerateApiKeyRequest request,
....
91.  _logger.LogWarning("Admin Secret (from DB): {StoredSecret} |
Provided: {ProvidedSecret}", Mask(storedSecretStr),
Mask(providedSecretStr));
```

Log Forging\Path 17:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=17
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Controllers/V1/OnboardingController.cs
Line	824	923
Object	request	LogWarning

Code Snippet
File Name   Controllers/V1/OnboardingController.cs
Method   public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.  public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
....
923.  _logger.LogWarning(ex, "Invalid operation during API key rotation
for merchant {MerchantId}", request.MerchantId);
```

Log Forging\Path 18:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=18
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/MockAwsSecretsManagerService.cs
Line	824	34
Object	request	LogError

Code Snippet
File Name   Controllers/V1/OnboardingController.cs
Method   public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.  public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
```

File Name   Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Log Forging\Path 19:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=19
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element secretsManager. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	48	34
Object	secretsManager	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
48.   [FromServices] IAwsSecretsManagerService secretsManager,
```

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}", 
secretName);
```

Log Forging\Path 20:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=20
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element apiKeyService. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	142	34
Object	apiKeyService	LogError

Code Snippet

File Name	Controllers/V1/AdminController.cs
Method	public async Task<IActionResult> RevokeAdminApiKey(

```
....
142.   [FromServices] IApiKeyService apiKeyService)
```

▼

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 21:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=21
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/MockController.cs	Services/MockAwsSecretsManagerService.cs
Line	79	34
Object	request	LogError

Code Snippet

File Name	Controllers/MockController.cs
Method	public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
79.  public async Task<IActionResult> GetApiKeySecret([FromBody]
JsonElement request)
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 22:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=22
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element req. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	141	34
Object	req	LogError

Code Snippet

File Name	Controllers/V1/AdminController.cs
Method	public async Task<IActionResult> RevokeAdminApiKey(

```
....
141.   [FromBody] AdminKeyServiceNameRequest req,
```

File Name	Services/MockAwsSecretsManagerService.cs
Method	public Task<string?> GetSecretAsync(string secretName)

```
....
34.  _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 23:

Severity	Low
Result State	To Verify

Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=23
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKey at line 441 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/MockAwsSecretsManagerService.cs
Line	441	34
Object	request	LogError

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> UpdateApiKey([FromBody] UpdateApiKeyRequest request)

```
....
441.  public async Task<IActionResult> UpdateApiKey([FromBody]
UpdateApiKeyRequest request)
```

▼

File Name Services/MockAwsSecretsManagerService.cs

Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 24:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=24
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKey at line 529 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/MockAwsSecretsManagerService.cs
Line	529	34
Object	request	LogError

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> RevokeApiKey([FromBody] RevokeApiKeyRequest request)

```
....
529.   public async Task<IActionResult> RevokeApiKey([FromBody]
RevokeApiKeyRequest request)
```

▼

File Name Services/MockAwsSecretsManagerService.cs
Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 25:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=25
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 22 of Services/MockAwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/MockAwsSecretsManagerService.cs
Line	47	34
Object	request	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
47.   [FromBody] GenerateApiKeyRequest request,
```

▼

File Name Services/MockAwsSecretsManagerService.cs
Method public Task<string?> GetSecretAsync(string secretName)

```
....
34.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 26:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=26
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKey at line 441 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	441	49
Object	request	LogError

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> UpdateApiKey([FromBody] UpdateApiKeyRequest request)

```
....
441.   public async Task<IActionResult> UpdateApiKey([FromBody]
UpdateApiKeyRequest request)
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 27:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=27
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKey at line 529 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	529	49
Object	request	LogError

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> RevokeApiKey([FromBody] RevokeApiKeyRequest request)

```
....
529.  public async Task<IActionResult> RevokeApiKey([FromBody]
RevokeApiKeyRequest request)
```

▼

File Name Services/AwsSecretsManagerService.cs
Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 28:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=28
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	47	49
Object	request	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
47.   [FromBody] GenerateApiKeyRequest request,
```

▼

File Name Services/AwsSecretsManagerService.cs

Method	public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 29:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=29
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/AwsSecretsManagerService.cs
Line	824	49
Object	request	LogError

Code Snippet

File Name	Controllers/V1/OnboardingController.cs
Method	public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.   public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
```

File Name	Services/AwsSecretsManagerService.cs
Method	public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 30:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=30
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element secretsManager. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	48	49
Object	secretsManager	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
48.   [FromServices] IAwsSecretsManagerService secretsManager,
```

File Name Services/AwsSecretsManagerService.cs
Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 31:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=31
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element apiKeyService. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	142	49
Object	apiKeyService	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> RevokeAdminApiKey(

```
....
142.   [FromServices] IApiKeyService apiKeyService)
```

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 32:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=32
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GetApiKeySecret at line 79 of Controllers/MockController.cs gets user input from element request. This element's value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/MockController.cs	Services/AwsSecretsManagerService.cs
Line	79	49
Object	request	LogError

Code Snippet

File Name Controllers/MockController.cs

Method public async Task<IActionResult> GetApiKeySecret([FromBody] JsonElement request)

```
....
79.   public async Task<IActionResult> GetApiKeySecret([FromBody]
JsonElement request)
```

▼

File Name Services/AwsSecretsManagerService.cs

Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 33:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=33
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeAdminApiKey at line 140 of Controllers/V1/AdminController.cs gets user input from element req. This element's value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetSecretAsync at line 35 of Services/AwsSecretsManagerService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/AwsSecretsManagerService.cs
Line	141	49
Object	req	LogError

Code Snippet
File Name Controllers/V1/AdminController.cs
Method public async Task<IActionResult> RevokeAdminApiKey(

```
....
141.   [FromBody] AdminKeyServiceNameRequest req,
```

File Name Services/AwsSecretsManagerService.cs
Method public async Task<string?> GetSecretAsync(string secretName)

```
....
49.   _logger.LogError(ex, "Error retrieving secret {SecretName}",
secretName);
```

Log Forging\Path 34:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=34
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKey at line 529 of Controllers/V1/OnboardingController.cs gets user input from element request. This element's value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in RevokeApiKeyAsync at line 382 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	529	399
Object	request	LogWarning

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> RevokeApiKey([FromBody] RevokeApiKeyRequest request)

```
....
529.   public async Task<IActionResult> RevokeApiKey([FromBody]
RevokeApiKeyRequest request)
```

File Name	Services/ApiKeyService.cs
Method	public async Task<bool> RevokeApiKeyAsync(RevokeApiKeyRequest request)

```
....
399.   _logger.LogWarning("API key {ApiKey} not found during revocation",
request.ApiKey);
```

Log Forging\Path 35:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=35
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method DeleteProvider at line 627 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element's value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in DeleteProvider at line 627 of Controllers/V1/SurchargeProviderController.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Controllers/V1/SurchargeProviderController.cs
Line	627	642
Object	merchantId	LogWarning

Code Snippet

File Name	Controllers/V1/SurchargeProviderController.cs
Method	public async Task<IActionResult> DeleteProvider(string merchantId, Guid id)

```
....
627.   public async Task<IActionResult> DeleteProvider(string merchantId,
Guid id)
....
642.   _logger.LogWarning("Merchant ID mismatch: URL {UrlMerchantId} vs
authenticated {AuthMerchantId}",
```

Log Forging\Path 36:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=36
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method CreateProvider at line 54 of Controllers/V1/SurchargeProviderController.cs gets user input from element request. This element's value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in CreateWithConfigurationAsync at line 215 of Services/SurchargeProviderService.cs.

	Source	Destination

File	Controllers/V1/SurchargeProviderController.cs	Services/SurchargeProviderService.cs
Line	54	251
Object	request	LogInformation

Code Snippet
File Name Controllers/V1/SurchargeProviderController.cs
Method public async Task<IActionResult> CreateProvider(string merchantId, [FromBody] SurchargeProviderRequest request)

```
....
54.   public async Task<IActionResult> CreateProvider(string merchantId,
[FromBody] SurchargeProviderRequest request)
```

File Name Services/SurchargeProviderService.cs
Method public async Task<SurchargeProvider> CreateWithConfigurationAsync(SurchargeProvider provider, ProviderConfigurationRequest configuration, string merchantId)

```
....
251.   _logger.LogInformation("Successfully created provider {ProviderId}
with configuration {ConfigId} for merchant {MerchantId}",
```

Log Forging\Path 37:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=37
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method CreateProvider at line 54 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in CreateWithConfigurationAsync at line 215 of Services/SurchargeProviderService.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Services/SurchargeProviderService.cs
Line	54	251
Object	merchantId	LogInformation

Code Snippet
File Name Controllers/V1/SurchargeProviderController.cs
Method public async Task<IActionResult> CreateProvider(string merchantId, [FromBody] SurchargeProviderRequest request)

```
....
54.  public async Task<IActionResult> CreateProvider(string merchantId,
[FromBody] SurchargeProviderRequest request)
```

File Name Services/SurchargeProviderService.cs

Method public async Task<SurchargeProvider> CreateWithConfigurationAsync(SurchargeProvider provider, ProviderConfigurationRequest configuration, string merchantId)

```
....
251.  _logger.LogInformation("Successfully created provider {ProviderId}
with configuration {ConfigId} for merchant {MerchantId}",
```

Log Forging\Path 38:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=38
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element apiKeyService. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/ApiKeyService.cs
Line	49	890
Object	apiKeyService	LogWarning

Code Snippet

File Name Controllers/V1/AdminController.cs

Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
49.   [FromServices] IApiKeyService apiKeyService)
```

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
890.  _logger.LogWarning("Admin/superuser API key generated for merchant
{MerchantId} by {AdminUserId}", request.MerchantId,
request.OnboardingMetadata?.AdminUserId ?? "admin");
```

Log Forging\Path 39:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=39
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateAdminApiKey at line 46 of Controllers/V1/AdminController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/AdminController.cs	Services/ApiKeyService.cs
Line	47	890
Object	request	LogWarning

Code Snippet

File Name Controllers/V1/AdminController.cs

Method public async Task<IActionResult> GenerateAdminApiKey(

```
....
47.   [FromBody] GenerateApiKeyRequest request,
```

File Name Services/ApiKeyService.cs

Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
890.   _logger.LogWarning("Admin/superuser API key generated for merchant
{MerchantId} by {AdminUserId}", request.MerchantId,
request.OnboardingMetadata?.AdminUserId ?? "admin");
```

Log Forging\Path 40:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=40
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKey at line 251 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateApiKeyAsync at line 739 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	251	890

Object	request	LogWarning

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> GenerateApiKey([FromBody] GenerateApiKeyRequest request)

```
....
251.  public async Task<IActionResult> GenerateApiKey([FromBody]
GenerateApiKeyRequest request)
```

▼

File Name Services/ApiKeyService.cs
Method public async Task<GenerateApiKeyResponse> GenerateApiKeyAsync(GenerateApiKeyRequest request)

```
....
890.  _logger.LogWarning("Admin/superuser API key generated for merchant
{MerchantId} by {AdminUserId}", request.MerchantId,
request.OnboardingMetadata?.AdminUserId ?? "admin");
```

Log Forging\Path 41:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=41
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	824	619
Object	request	LogInformation

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.  public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
```

▼

File Name Services/ApiKeyService.cs
Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
619.   _logger.LogInformation("Getting API key info for key {ApiKey}",
apiKey);
```

Log Forging\Path 42:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=42
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateApiKey at line 441 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	441	619
Object	request	LogInformation

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> UpdateApiKey([FromBody] UpdateApiKeyRequest request)

```
....
441.   public async Task<IActionResult> UpdateApiKey([FromBody]
UpdateApiKeyRequest request)
```

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
619.   _logger.LogInformation("Getting API key info for key {ApiKey}",
apiKey);
```

Log Forging\Path 43:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=43
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RevokeApiKey at line 529 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GetApiKeyInfoAsync at line 617 of Services/ApiKeyService.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Services/ApiKeyService.cs
Line	529	619
Object	request	LogInformation

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method public async Task<IActionResult> RevokeApiKey([FromBody] RevokeApiKeyRequest request)

```
....
529.  public async Task<IActionResult> RevokeApiKey([FromBody]
RevokeApiKeyRequest request)
```

File Name Services/ApiKeyService.cs

Method public async Task<ApiKeyInfo> GetApiKeyInfoAsync(string apiKey)

```
....
619.  _logger.LogInformation("Getting API key info for key {ApiKey}",
apiKey);
```

Log Forging\Path 44:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=44
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Controllers/V1/SurchargeProviderController.cs
Line	365	593
Object	merchantId	LogWarning

Code Snippet

File Name Controllers/V1/SurchargeProviderController.cs

Method public async Task<IActionResult> UpdateProvider(string merchantId, Guid id, [FromBody] SurchargeProviderUpdateRequest request)

```
....
365.  public async Task<IActionResult> UpdateProvider(string merchantId,
Guid id, [FromBody] SurchargeProviderUpdateRequest request)
....
593.  _logger.LogWarning(ex, "Provider not found while updating:
{ProviderId} for merchant {MerchantId}", id, merchantId);
```

Log Forging\Path 45:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=45
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ProcessAuth at line 35 of Controllers/V1/SurchargeController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in ProcessAuth at line 35 of Controllers/V1/SurchargeController.cs.

	Source	Destination
File	Controllers/V1/SurchargeController.cs	Controllers/V1/SurchargeController.cs
Line	35	66
Object	request	LogInformation

Code Snippet
File Name Controllers/V1/SurchargeController.cs
Method public async Task<IActionResult> ProcessAuth([FromBody] SurchargeAuthRequest request)

```
....
35.  public async Task<IActionResult> ProcessAuth([FromBody]
SurchargeAuthRequest request)
....
66.  _logger.LogInformation("Successfully processed surcharge auth for
transaction: {CorrelationId}, surcharge transaction ID:
{SurchargeTransactionId}", request.CorrelationId,
response.SurchargeTransactionId);
```

Log Forging\Path 46:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=46
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method GenerateApiKey at line 251 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in GenerateApiKey at line 251 of Controllers/V1/OnboardingController.cs.

	Source	Destination

File	Controllers/V1/OnboardingController.cs	Controllers/V1/OnboardingController.cs
Line	251	386
Object	request	LogInformation

Code Snippet
File Name Controllers/V1/OnboardingController.cs
Method public async Task<IActionResult> GenerateApiKey([FromBody] GenerateApiKeyRequest request)

```
....
251.  public async Task<IActionResult> GenerateApiKey([FromBody]
GenerateApiKeyRequest request)
....
386.  _logger.LogInformation("Generated API key response for merchant
{MerchantId}: HasApiKey={HasApiKey}, HasSecret={HasSecret},
ExpiresAt={ExpiresAt}",
```

Log Forging\Path 47:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=47
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ProcessRefund at line 159 of Controllers/V1/SurchargeController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in ProcessRefund at line 159 of Controllers/V1/SurchargeController.cs.

	Source	Destination
File	Controllers/V1/SurchargeController.cs	Controllers/V1/SurchargeController.cs
Line	159	185
Object	request	LogInformation

Code Snippet
File Name Controllers/V1/SurchargeController.cs
Method public async Task<IActionResult> ProcessRefund([FromBody] SurchargeRefundRequest request)

```
....
159.  public async Task<IActionResult> ProcessRefund([FromBody]
SurchargeRefundRequest request)
....
185.  _logger.LogInformation("Successfully processed surcharge refund
for transaction: {CorrelationId}, " +
```

Log Forging\Path 48:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=48

Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method UpdateProvider at line 365 of Controllers/V1/SurchargeProviderController.cs gets user input from element merchantId. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in UpdateAsync at line 263 of Services/SurchargeProviderService.cs.

	Source	Destination
File	Controllers/V1/SurchargeProviderController.cs	Services/SurchargeProviderService.cs
Line	365	267
Object	merchantId	LogInformation

Code Snippet

File Name Controllers/V1/SurchargeProviderController.cs

Method public async Task<IActionResult> UpdateProvider(string merchantId, Guid id, [FromBody] SurchargeProviderUpdateRequest request)

```
....
365.   public async Task<IActionResult> UpdateProvider(string merchantId,
Guid id, [FromBody] SurchargeProviderUpdateRequest request)
```

File Name Services/SurchargeProviderService.cs

Method public async Task<SurchargeProvider> UpdateAsync(SurchargeProvider provider)

```
....
267.   _logger.LogInformation("Updating provider {ProviderId} for
merchant {MerchantId}", provider.Id, provider.UpdatedBy);
```

Log Forging\Path 49:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=49
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in RotateApiKey at line 824 of Controllers/V1/OnboardingController.cs.

	Source	Destination
File	Controllers/V1/OnboardingController.cs	Controllers/V1/OnboardingController.cs
Line	824	931
Object	request	LogError

Code Snippet

File Name Controllers/V1/OnboardingController.cs

Method	public async Task<IActionResult> RotateApiKey([FromBody] RotateApiKeyRequest request)

```
....
824.  public async Task<IActionResult> RotateApiKey([FromBody]
RotateApiKeyRequest request)
....
931.  _logger.LogError(ex, "Error rotating API key for merchant
{MerchantId}", request.MerchantId);
```

Log Forging\Path 50:

Severity	Low
Result State	To Verify
Online Results	https://worldpay.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=2330009&projectid=42290&pathid=50
Status	Recurrent
Detection Date	7/23/2025 8:17:04 PM

Method ProcessAuth at line 35 of Controllers/V1/SurchargeController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually used in writing an audit log in ProcessAuth at line 35 of Controllers/V1/SurchargeController.cs.

	Source	Destination
File	Controllers/V1/SurchargeController.cs	Controllers/V1/SurchargeController.cs
Line	35	67
Object	request	LogInformation

Code Snippet

File Name	Controllers/V1/SurchargeController.cs
Method	public async Task<IActionResult> ProcessAuth([FromBody] SurchargeAuthRequest request)

```
....
35.  public async Task<IActionResult> ProcessAuth([FromBody]
SurchargeAuthRequest request)
....
67.  _logger.LogInformation("Auth Response: {@Response}", response);
```

Use Of Hardcoded Password

Risk

What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.

Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

Cause

How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

General Recommendations

How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

Source Code Examples

Java
Hardcoded Admin Password

```
bool isAdmin(String username, String password) {
    bool isMatch = false;

    if (username.equals("admin")) {
        if (password.equals("P@ssw0rd"))
            return isMatch = true;
    }

    return isMatch;
}
```

No Hardcoded Credentials

```
bool isAdmin(String username, String password) {
    bool adminPrivs = false;

    if (authenticateUser(username, password)) {
        UserPrivileges privs = getUserPrivileges(username);

        if (privs.isAdmin)
            adminPrivs = true;
    }

    return adminPrivs;
}
```

Privacy Violation

Risk

What might happen

A user’s personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

Cause

How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

General Recommendations

How to avoid it

1. Personal data should be removed before writing to logs or other files.
2. Review the need and justification of sending personal data to remote web services.

Source Code Examples

CSharp

The user's password is written to the screen

```
class PrivacyViolation
{
        static void CreateUser(string username, string password)
        {
                AddUser(username, password);
                System.Console.WriteLine(password);
        }
}
```

Log Forging

Risk

What might happen

An attacker could engineer audit logs of security-sensitive actions and lay a false audit trail, potentially implicating an innocent user or hiding an incident.

Cause

How does it happen

The application writes audit logs upon security-sensitive actions. Since the audit log includes user input that is neither checked for data type validity nor subsequently sanitized, the input could contain false information made to look like legitimate audit log data,

General Recommendations

How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Validation is not a replacement for encoding. Fully encode all dynamic data, regardless of source, before embedding it in logs.
3. Use a secure logging mechanism.

Source Code Examples

CSharp

Ensure you encode any special delimiter characters before writing to a log file.

```
Log.Write( logDetails.Replace(CRLF, @"\CRLF"));
```

Java

Ensure you encode any special delimiter characters before writing to a log file.

```
Log.Write( logDetails.Replace(CRLF, @"\CRLF"));
```

Objc

Ensure you encode any special delimiter characters before writing to a log file.

```
NSLog(@"%@", [logDetails stringByReplacingOccurrencesOfString:@"\n" withString:@"\\n"]);
```

Swift

Ensure you encode any special delimiter characters before writing to a log file.

```
print(logDetails.stringByReplacingOccurrencesOfString("\n", withString: "\\n"))
```

Scanned Languages

Language	Hash Number	Change Date
CSharp	0510055218487407	8/7/2022
JavaScript	0581226327418505	8/7/2022
Common	6313173566890873	8/7/2022