CICD 掃描報告

專案名稱	CICD
掃描開始	2024年12月12日 上午 10:05:11
預設集合	Checkmarx Default
掃描時間	00h:15m:01s
被掃描的程式行數	405902
被掃描的檔案數	4401
報告建立時間	2024年12月12日 上午 10:21:00
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588
團隊	planning
Checkmarx版本	9.5.5.1007 HF14
掃描類別	完整的
來源	LocalPath
漏洞密度	3/1000 (漏洞/LOC)
可見性	公開

過濾器設置

嚴重程度：

包含在內: 高風險, 中風險, 低風險, 資訊

排除在外: 無

結果狀態：

包含在內: 校驗, 不可利用, 確認, 緊急, 推薦不可用

排除在外: 無

被分配給

包含在內: 全部

類別

包含在內:

未分類	全部
Custom	全部
PCI DSS v3.2.1	全部
OWASP Top 10 2013	全部
FISMA 2014	全部
NIST SP 800-53	全部
OWASP Top 10 2017	全部
OWASP Mobile Top 10 2016	全部
OWASP Top 10 API	全部
ASD STIG 4.10	全部
OWASP Top 10 2010	全部
CWE top 25	全部
MOIS(KISA) Secure Coding 2021	全部

OWASP ASVS	全部
OWASP Top 10 2021	全部
SANS top 25	全部
ASA Mobile Premium	全部
ASA Premium	全部
ASD STIG 5.2	全部
Top Tier	全部

排除在外:

未分類	無
Custom	無
PCI DSS v3.2.1	無
OWASP Top 10 2013	無
FISMA 2014	無
NIST SP 800-53	無
OWASP Top 10 2017	無
OWASP Mobile Top 10 2016	無
OWASP Top 10 API	無
ASD STIG 4.10	無
OWASP Top 10 2010	無
CWE top 25	無
MOIS(KISA) Secure Coding 2021	無
OWASP ASVS	無
OWASP Top 10 2021	無
SANS top 25	無
ASA Mobile Premium	無
ASA Premium	無
ASD STIG 5.2	無
Top Tier	無

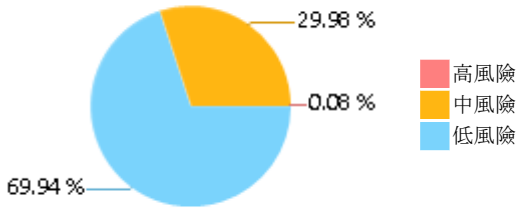
結果限制

每次問詢的結果限制設置為 50

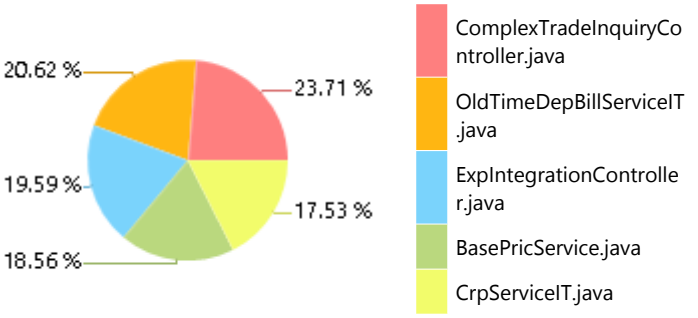
選中的問詢

選中的問詢列出在 掃描結果摘要

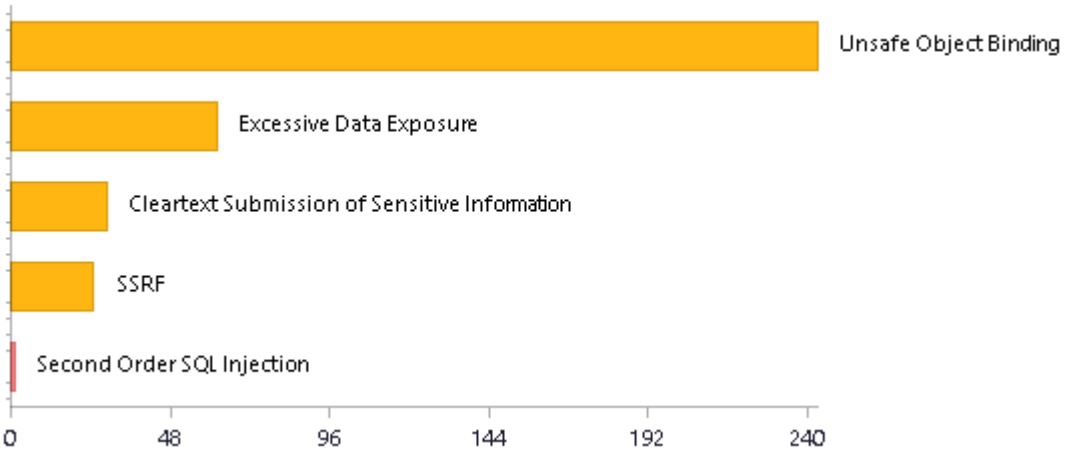
掃描結果摘要



最容易受攻擊的檔案



數量最多的前5類漏洞



掃描總結 - OWASP Top 10 2017

有關可見性和風險的詳細資訊及闡述參見： 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	35	21
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	31	11
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	35	11
A6-Security Misconfiguration *	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	74	74
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

* 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - OWASP Top 10 2021

Category	Issues Found	Best Fix Locations
A1-Broken Access Control*	177	170
A2-Cryptographic Failures	35	15
A3-Injection*	4	3
A4-Insecure Design*	156	156
A5-Security Misconfiguration*	0	0
A6-Vulnerable and Outdated Components*	0	0
A7-Identification and Authentication Failures*	543	543
A8-Software and Data Integrity Failures*	244	108
A9-Security Logging and Monitoring Failures	109	95
A10-Server-Side Request Forgery	25	8

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - OWASP Top 10 2013

有關可見性和風險的詳細資訊及闡述參見： 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	1	1
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	8	1
A5-Security Misconfiguration*	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	58	58
A6-Sensitive Data Exposure*	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	37	17
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

* 專案掃描結果不包括所有相關的查詢。 應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - PCI DSS v3.2.1

Category	Issues Found	Best Fix Locations
PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection	20	7
PCI DSS (3.2.1) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage*	0	0
PCI DSS (3.2.1) - 6.5.4 - Insecure communications*	29	9
PCI DSS (3.2.1) - 6.5.5 - Improper error handling*	136	136
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	2	2

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - 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.	24	17
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.	87	67
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.	109	109
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.	69	36

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)*	133	126
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	34	20
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)	0	0
SC-5 Denial of Service Protection (P1)*	78	78
SC-8 Transmission Confidentiality and Integrity (P1)	29	9
SI-10 Information Input Validation (P1)*	33	14
SI-11 Error Handling (P2)*	58	58
SI-15 Information Output Filtering (P0)*	0	0
SI-16 Memory Protection (P1)*	0	0

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - 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.	25	15
M8-Code Tampering*	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering*	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	2	2
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

* 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - OWASP Top 10 API

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization	8	1
API2-Broken Authentication*	0	0
API3-Excessive Data Exposure	58	58
API4-Lack of Resources and Rate Limiting	3	2
API5-Broken Function Level Authorization	0	0
API6-Mass Assignment	0	0
API7-Security Misconfiguration*	29	9
API8-Injection*	1	1
API9-Improper Assets Management	0	0
API10-Insufficient Logging and Monitoring	0	0

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - Custom

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

掃描總結 - ASD STIG 4.10

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

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

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

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

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

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

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

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

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

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

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

掃描總結 - ASD STIG 5.2

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

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

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

APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.	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.	2	2
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.	6	6
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.*	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0

APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.	29	9
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.	3	2
APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.*	1	1
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.*	11	5
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.*	136	136
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.	7	5
APSC-DV-002630 - CAT II Security-relevant software updates and patches must be kept up to date.	0	0
APSC-DV-002760 - CAT II The application performing organization-defined security functions must verify correct operation of security functions.	0	0
APSC-DV-002900 - CAT II The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	0	0
APSC-DV-002770 - CAT II The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	0	0
APSC-DV-002780 - CAT III The application must notify the ISSO and ISSM of failed security verification tests.	0	0
APSC-DV-002870 - CAT II Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	0	0
APSC-DV-002880 - CAT II The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	0	0
APSC-DV-002890 - CAT I Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	0	0
APSC-DV-002910 - CAT II The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	0	0
APSC-DV-002920 - CAT II The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	0	0
APSC-DV-002930 - CAT II The ISSO must ensure active vulnerability testing is performed.	0	0
APSC-DV-002980 - CAT II New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPS	0	0
APSC-DV-002950 - CAT II Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	0	0
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party	0	0

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

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

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

APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.*	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.*	8	1
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

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - 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

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - 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*	136	136
MOIS(KISA) Security Functions*	160	140
MOIS(KISA) Time and status*	2	2
MOIS(KISA) Verification and representation of input data*	49	21

* 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - SANS top 25

Category	Issues Found	Best Fix Locations
SANS top 25*	240	209

* 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - CWE top 25

Category	Issues Found	Best Fix Locations
CWE top 25*	238	210

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - Top Tier

Category	Issues Found	Best Fix Locations
Top Tier	1	1

掃描總結 - OWASP ASVS

Category	Issues Found	Best Fix Locations
V01 Architecture, Design and Threat Modeling*	534	527
V02 Authentication	6	6
V03 Session Management*	62	62
V04 Access Control	123	123
V05 Validation, Sanitization and Encoding*	284	127
V06 Stored Cryptography*	0	0
V07 Error Handling and Logging*	109	95
V08 Data Protection	6	6
V09 Communication*	31	11
V10 Malicious Code	0	0
V11 Business Logic*	0	0
V12 Files and Resources	0	0
V13 API and Web Service	0	0
V14 Configuration*	673	673

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - ASA Mobile Premium

Category	Issues Found	Best Fix Locations
ASA Mobile Premium*	13	7

* 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描總結 - ASA Premium

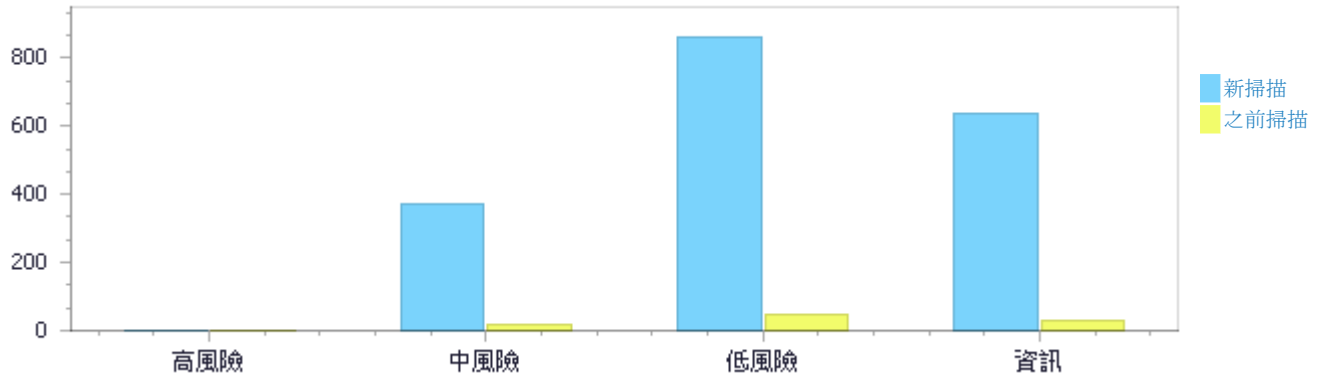
Category	Issues Found	Best Fix Locations
ASA Premium*	328	141

***** 專案掃描結果不包括所有相關的查詢。應該變更預設和/或篩選器以包括所有相關的標準查詢。

掃描結果分佈

與2024/11/18 下午 05:17的專案掃描比較

	高風險	中風險	低風險	資訊	總共
新問題	1	370	863	639	1,873
反覆出現的問題	0	0	0	0	0
總共	1	370	863	639	1,873
已修復的問題	1	16	48	32	97



掃描結果分佈

	高風險	中風險	低風險	資訊	總共
校驗	1	370	863	639	1,873
不可利用	0	0	0	0	0
確認	0	0	0	0	0
緊急	0	0	0	0	0
推薦不可用	0	0	0	0	0
總共	1	370	863	639	1,873

掃描結果摘要

漏洞類別	事件	嚴重程度：
Second Order SQL Injection	1	高風險
Unsafe Object Binding	243	中風險
Excessive Data Exposure	62	中風險
Cleartext Submission of Sensitive Information	29	中風險
SSRF	25	中風險

DB Parameter Tampering	8	中風險
Unchecked Input for Loop Condition	3	中風險
Spring Overly Permissive Cross Origin Resource Sharing Policy	536	低風險
Improper Resource Access Authorization	107	低風險
Improper Exception Handling	78	低風險
Information Exposure Through an Error Message	58	低風險
Stored Log Forging	23	低風險
Incorrect Permission Assignment For Critical Resources	16	低風險
Log Forging	11	低風險
Integer Overflow	7	低風險
Integer Underflow	7	低風險
Heap Inspection	6	低風險
Spring Use Of Hardcoded Password	4	低風險
Portability Flaw Locale Dependent Comparison	2	低風險
Race Condition Format Flaw	2	低風險
Serializable Class Containing Sensitive Data	2	低風險
Use Of Hardcoded Password	2	低風險
Spring Missing Content Security Policy	1	低風險
Spring Missing Expect CT Header	1	低風險
Undocumented API	524	資訊
Insufficient Logging of Exceptions	75	資訊
Portability Flaw In File Separator	40	資訊

10個最容易受攻擊的檔案

高級和中級漏洞

檔案名稱	找到的問題
cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java	36
dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	22
remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java	18
remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	14
dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	13
remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	13
dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java	12
cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java	11
dep/dep-	11

app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java	
dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/FdcSeqService.java	11

掃描結果詳細資料

Second Order SQL Injection

查詢路徑:

Java\Cx\Java High Risk\Second Order SQL Injection 版本:9

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 API: API8-Injection
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
OWASP Top 10 2021: A3-Injection
SANS top 25: SANS top 25
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.
Top Tier: Top Tier

描述

Second Order SQL Injection\路徑 1:

嚴重程度：	高風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1
狀態	新的
Detection Date	12/12/2024 10:17:32 AM

應用程式中的loadDbDataFromFile透過len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java中的45之executeBatch執行SQL 查詢(Query)。此應用程式建構SQL查詢時，在未過濾的的情況下將不受信任的字串嵌入到查詢字串中。串接後的查詢字串被提交到資料庫，在資料庫中進行解析(parse)及執行(executed)。
攻擊者可能能夠事先把惡意資料寫入資料庫，應用程式會在 len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java 中 loadDbDataFromFile 第 45 的 readFileToString 取出這個惡意資料，沒有對其清理就直接在SQL查詢中使用，最終這些未經過濾的惡意資料就會隨成程式流進入資料庫Server。
這可能會造成二階SQL注入攻擊(Second-Order SQL Injection)。

	來源	目的地
檔案	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java
行	48	66
物件	readFileToString	executeBatch

代碼片斷	
檔案名稱	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java
方法	private void loadDbDataFromFile(DataSource ds, String file) throws Exception {

```
....
48.  String sqlList = FileUtils.readFileToString(resource.getFile(),
"UTF-8");
....
66.  stmt.executeBatch();
```

Unsafe Object Binding

查詢路徑:

Java\公司\Java Medium Threat\Unsafe Object Binding 版本:3

類別

OWASP ASVS: V05 Validation, Sanitization and Encoding
OWASP Top 10 2021: A8-Software and Data Integrity Failures
ASA Premium: ASA Premium

描述

Unsafe Object Binding\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1631
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CustomerIntRateUpdateRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CustomerIntRateUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1632
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	49	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<PriceProjectCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<PriceProjectCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 3:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1633
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	49	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<FeeProjectCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<FeeProjectCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 4:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1634
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java 中 62 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	62	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<IntRateStandardUpdateRq>> apiRequest) {

```
....
62.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<IntRateStandardUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 5:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1635
狀態 新的
Detection Date 12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectControll	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

	er.java	
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<PriceProjectDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<PriceProjectDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 6:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1636
狀態 新的
Detection Date 12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<FeeProjectDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<FeeProjectDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 7:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1637
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CustomerFeeUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CustomerFeeUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 8:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1638
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<IntRateProjectUpdateRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<IntRateProjectUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 9:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1639

狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java 中 52 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	52	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<PricExchgRateUpdateRq>> apiRequest) {

```
....
52.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<PricExchgRateUpdateRq>> apiRequest)  {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 10:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1640
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/control	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/serv

	ler/pric/fee/bizfee/BusinessFeeController.java	ice/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BusinessFeeUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<BusinessFeeUpdateRq>> apiRequest)  {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 11:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1641
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	49	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<BusinessFeeCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<BusinessFeeCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 12:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1642
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java 中 71 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	71	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<IntRateProjectDeleteRq>> apiRequest) {

```
....
71.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<IntRateProjectDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 13:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1643
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	49	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<FeeStandardCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<FeeStandardCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 14:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1644
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FeeProjectRelateUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FeeProjectRelateUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 15:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1645
狀態 新的
Detection Date 12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45

物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<FeeStandardDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<FeeStandardDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 16:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1646
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java 中 47 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	47	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateproj/IntRateProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<IntRateProjectCreateRq>> apiRequest) {

```
....
47.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<IntRateProjectCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 17:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1647
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java 中 59 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	59	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<PricExchgRateDeleteRq>> apiRequest) {

```
....
59.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<PricExchgRateDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 18:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1648
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/common/priceproj/PriceProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<PriceProjectUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<PriceProjectUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 19:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1649

狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeproj/FeeProjectController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FeeProjectUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FeeProjectUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 20:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1650
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

行	49	45
物件	apiRequest	save

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<CustomerFeeCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<CustomerFeeCreateRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 21:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1651
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java 中 71 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	71	45
物件	apiRequest	save

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java

方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<IntRateProjectRelateDeleteRq>> apiRequest) {

```
....
71.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<IntRateProjectRelateDeleteRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 22:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1652
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CustomerFeeDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CustomerFeeDeleteRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 23:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1653
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java 中 71 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	71	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BusinessIntRateDeleteRq>> apiRequest) {

```
....
71.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BusinessIntRateDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 24:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1654

狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java 中 45 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	45	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/exchgrate/exchgrate/PricExchgRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<PricExchgRateCreateRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<PricExchgRateCreateRq>> apiRequest)  {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 25:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1655
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java 中 47 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-	cmn/cmn-

	app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java	service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	47	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<IntRateProjectRelateCreateRq>> apiRequest) {

```
....
47.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<IntRateProjectRelateCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 26:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1656
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 中 71 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	71	45
物件	apiRequest	save

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CustomerIntRateDeleteRq>> apiRequest) {

```
....
71.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CustomerIntRateDeleteRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 27:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1657
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java 中 46 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	46	45
物件	apiRequest	save

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<IntRateStandardCreateRq>> apiRequest) {

```
....
46.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<IntRateStandardCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 28:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1658
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intrateprojrel/IntRateProjectRelateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<IntRateProjectRelateUpdateRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<IntRateProjectRelateUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 29:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1659
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/bizfee/BusinessFeeController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BusinessFeeDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BusinessFeeDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 30:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1660
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java 中 47 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地

檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	47	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<BusinessIntRateCreateRq>> apiRequest) {

```
....
47.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<BusinessIntRateCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 31:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1661
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java 中 49 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	49	45
物件	apiRequest	save

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<FeeProjectRelateCreateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<FeeProjectRelateCreateRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 32:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1662
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/bizintrate/BusinessIntRateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BusinessIntRateUpdateRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<BusinessIntRateUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 33:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1663
狀態 新的
Detection Date 12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 中 47 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	47	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<CustomerIntRateCreateRq>> apiRequest) {

```
....
47.  public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody
ApiRequest<ServiceRq<CustomerIntRateCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 34:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1664
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java 中 56 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	56	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feestd/FeeStandardController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FeeStandardUpdateRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FeeStandardUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 35:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1665
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地

檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	63	45
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/feeprojrel/FeeProjectRelateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<FeeProjectRelateDeleteRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<FeeProjectRelateDeleteRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java

方法 protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 36:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1666
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java 中 70 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java 中 33 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
行	70	45
物件	apiRequest	save

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/intratestd/IntRateStandardController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<IntRateStandardDeleteRq>> apiRequest) {

```
....
70.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<IntRateStandardDeleteRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/BasePricService.java
方法	protected void writeToPricLog(String logBeforeEntity, String logAfterEntity, String content) {

```
....
45.  cmnPricRecLogRepository.save(logEntity);
```

Unsafe Object Binding\路徑 37:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1667
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java 中 46 行的 apiRequest 可能意外地允許設置 len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java 中 256 行的 save 的值。

	來源	目的地
檔案	len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java
行	46	295
物件	apiRequest	save

代碼片斷

檔案名稱	len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java
方法	public ApiResponse<ServiceRs<StockLoanRs>> maintainStockLoan(@RequestBody ApiRequest<ServiceRq<StockLoanRq>> apiRequest) {

```
....
46.  public ApiResponse<ServiceRs<StockLoanRs>>
maintainStockLoan(@RequestBody ApiRequest<ServiceRq<StockLoanRq>>
apiRequest) {
```

檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java
方法	private void updateStockLoanEntity(LenStockLoanEntity stockLoanEntity, StockLoanArg stockLoanArg, List<StockCollateralInfo> stockCollateralInfoList, LimitCollateralsResponseBody limitCollateral) {

```
....
295.  stockLoanRepository.save(stockLoanEntity);
```

Unsafe Object Binding\路徑 38:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1668
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 xau/xau-app/src/main/java/com/scsb/ncbs/xau/controller/xau/summary/XauSummaryController.java 中 58 行的 apiRequest 可能意外地允許設置 xau/xau-service/src/main/java/com/scsb/ncbs/xau/service/xau/summary/XauSummaryService.java 中 142 行的 save 的值。

	來源	目的地
檔案	xau/xau-app/src/main/java/com/scsb/ncbs/xau/controller/xau/summary/XauSummaryController.java	xau/xau-service/src/main/java/com/scsb/ncbs/xau/service/xau/summary/XauSummaryService.java
行	58	154
物件	apiRequest	save

代碼片斷

檔案名稱	xau/xau-app/src/main/java/com/scsb/ncbs/xau/controller/xau/summary/XauSummaryController.java
方法	public ApiResponse<ServiceRs<XauSummaryReadReRs>> readRe(@RequestBody ApiRequest<ServiceRq<XauSummaryReadRq>> apiRequest) {

```
....
58.  public ApiResponse<ServiceRs<XauSummaryReadReRs>>
readRe(@RequestBody ApiRequest<ServiceRq<XauSummaryReadRq>> apiRequest)
{
```

檔案名稱	xau/xau-service/src/main/java/com/scsb/ncbs/xau/service/xau/summary/XauSummaryService.java
方法	public ServiceRs<XauSummaryReadReRs> readRe(@NotBlank String functionCode) {

```
....
154.  logRepository.save(logEntity);
```

Unsafe Object Binding\路徑 39:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1669
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java 中 46 行的 apiRequest 可能意外地允許設置 len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java 中 256 行的 save 的值。

	來源	目的地
檔案	len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java
行	46	296
物件	apiRequest	save

代碼片斷	
檔案名稱	len/len-app/src/main/java/com/scsb/ncbs/len/controller/collatertal/StockCollateralController.java
方法	public ApiResponse<ServiceRs<StockLoanRs>> maintainStockLoan(@RequestBody ApiRequest<ServiceRq<StockLoanRq>> apiRequest) {
	`` .... 46. public ApiResponse<ServiceRs<StockLoanRs>> maintainStockLoan(@RequestBody ApiRequest<ServiceRq<StockLoanRq>> apiRequest) { ```
檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/collateral/StockCollateralService.java
方法	private void updateStockLoanEntity(LenStockLoanEntity stockLoanEntity, StockLoanArg stockLoanArg, List<StockCollateralInfo> stockCollateralInfoList, LimitCollateralsResponseBody limitCollateral) {
	`` .... 296. stockLoanHistoryRepository.save(stockLoanHistoryEntity); ```

Unsafe Object Binding\路徑 40:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1670
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crr/CrrController.java 中 46 行的 apiRequest 可能意外地允許設置 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/crr/CrrService.java 中 115 行的 save 的值。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crr/CrrController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/crr/CrrService.java
行	46	128
物件	apiRequest	save

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crr/CrrController.java

方法 public ApiResponse<ServiceRs<CrrRecordsRs>> records(@RequestBody ApiRequest<ServiceRq<CrrRecordsRq>> apiRequest) {

```
....
46.  public ApiResponse<ServiceRs<CrrRecordsRs>> records(@RequestBody
ApiRequest<ServiceRq<CrrRecordsRq>> apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/crr/CrrService.java

方法 public ServiceRs<CrrRecordsRs> createRecords(@NotNull @Valid RecordsArg arg) {

```
....
128.  recordsRepository.save(entity);
```

Unsafe Object Binding\路徑 41:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1671
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java 中 42 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java 中 72 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java
行	42	133
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java

方法 public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<IdocTuneOutUpdateRq>> apiRequest) {

```
....
42.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<IdocTuneOutUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java

方法 public void update(@Valid @NotNull IdocTuneOutUpdateArg arg) {

```
....
133.  cmnIdocBrhReqRepository.save(cmnIdocBrhReqEntity);
```

Unsafe Object Binding\路徑 42:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1672
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java 中 72 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java 中 224 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	72	230
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java

方法 public ApiResponse<?> delete(@RequestBody ApiRequest<ServiceRq<IdocSpvOrderDeleteRq>> apiRequest) {

```
....
72.  public ApiResponse<?> delete(@RequestBody
ApiRequest<ServiceRq<IdocSpvOrderDeleteRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
方法	public void delete(@NotNull @Valid String spvApplyNo) {

```
....
230.  cmnIdocSpvReqRepository.save(entity);
```

Unsafe Object Binding\路徑 43:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1673
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java 中 42 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java 中 72 行的 saveAll 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java
行	42	134
物件	apiRequest	saveAll

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/tuneout/IdocTuneOutController.java
方法	public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<IdocTuneOutUpdateRq>> apiRequest) {

```
....
42.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<IdocTuneOutUpdateRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/tuneout/IdocTuneOutService.java
方法	public void update(@Valid @NotNull IdocTuneOutUpdateArg arg) {

```
....
134.  cmnIdocBrhReqDtlRepository.saveAll(cmnIdocBrhStockEntities);
```

Unsafe Object Binding\路徑 44:

嚴重程度：	中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1674
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java 中 48 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java 中 164 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java
行	48	200
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java

方法 public ApiResponse<ServiceRs<NtfMessageCreateRs>> create(@RequestBody ApiRequest<ServiceRq<NtfMessageCreateRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<NtfMessageCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<NtfMessageCreateRq>>
apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java

方法 private List<NtfMessageSendInfo> outerMessage(CmnNtfMessageEntity messageEntity, NtfMessageCreateArg arg, CmnNtfParmEntity parmEntity) {

```
....
200.  cmnNtfMessageRepository.save(messageEntity);
```

Unsafe Object Binding\路徑 45:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1675
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java 中 51 行的 apiRequest 可能意外地允許設置 cmn/cmn-

service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java 中 164 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java
行	51	200
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java

方法 public ApiResponse<ServiceRs<NtfOtpCreateRs>> create(@RequestBody ApiRequest<ServiceRq<NtfOtpCreateRq>> apiRequest) {

```
....
51.  public ApiResponse<ServiceRs<NtfOtpCreateRs>> create(@RequestBody
ApiRequest<ServiceRq<NtfOtpCreateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java

方法 private List<NtfMessageSendInfo> outerMessage(CmnNtfMessageEntity messageEntity, NtfMessageCreateArg arg, CmnNtfParmEntity parmEntity) {

```
....
200.  cmnNtfMessageRepository.save(messageEntity);
```

Unsafe Object Binding\路徑 46:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1676
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/parm/FdrParmController.java 中 78 行的 apiRequest 可能意外地允許設置 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/parm/FdrRateService.java 中 106 行的 save 的值。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/parm/FdrParmController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/parm/FdrRateService.java
行	78	119
物件	apiRequest	save

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/parm/FdrParmController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> updateSpread(@RequestBody ApiRequest<ServiceRq<FdrSpreadUpdateRq>> apiRequest) {

```
....
78.  public ApiResponse<ServiceRs<EmptyRs>> updateSpread(@RequestBody
ApiRequest<ServiceRq<FdrSpreadUpdateRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/parm/FdrRateService.java
方法	arg.getSpreadInfoList().forEach(info -> {

```
....
119.  rateRepository.save(entity);
```

Unsafe Object Binding\路徑 47:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1677
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java 中 44 行的 apiRequest 可能意外地允許設置 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java 中 32 行的 save 的值。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java
行	44	33
物件	apiRequest	save

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java
方法	public ApiResponse<ServiceRs<FdcReadRs>> readFdcSeq(@RequestBody ApiRequest<ServiceRq<FdcReadRq>> apiRequest) {

```
....
44.  public ApiResponse<ServiceRs<FdcReadRs>> readFdcSeq(@RequestBody
ApiRequest<ServiceRq<FdcReadRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java

方法	public void save(DepFdcSeqParmEntity parmEntity, DepFdcSeqLogEntity logEntity) {

```
....
33.  parmRepository.save(parmEntity);
```

Unsafe Object Binding\路徑 48:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1678
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java 中 56 行的 apiRequest 可能意外地允許設置 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java 中 32 行的 save 的值。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java
行	56	33
物件	apiRequest	save

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdc/FdcSeqController.java
方法	public ApiResponse<ServiceRs<FdcReadRs>> read(@RequestBody ApiRequest<ServiceRq<FdcReadRq>> apiRequest) {

```
....
56.  public ApiResponse<ServiceRs<FdcReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FdcReadRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdc/helper/FdcSeqTransactionalHelper.java
方法	public void save(DepFdcSeqParmEntity parmEntity, DepFdcSeqLogEntity logEntity) {

```
....
33.  parmRepository.save(parmEntity);
```

Unsafe Object Binding\路徑 49:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1679
狀態	新的

Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 中 63 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java 中 121 行的 saveAll 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java
行	63	145
物件	apiRequest	saveAll

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CustomerIntRateUpdateRq>> apiRequest) {

```
....
63.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CustomerIntRateUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java

方法 public ServiceRs<EmptyRs> update(@NotNull @Valid CustomerIntRateUpdateArg arg) {

```
....
145.  cmnPricCustIntRateDtlRepository.saveAll(newCustIntRateDtlList);
```

Unsafe Object Binding\路徑 50:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1680
狀態	新的
Detection Date	12/12/2024 10:20:08 AM

位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvdetail/IdocSpvDetailController.java 中 51 行的 apiRequest 可能意外地允許設置 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvdetail/IdocSpvDetailService.java 中 116 行的 save 的值。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvdetail/IdocSpvDetailController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvdetail/IdocSpvDetailService.java
行	51	158
物件	apiRequest	save

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvdetail/IdocSpvDetailController.java

方法 public ApiResponse<?> updateUsed(@RequestBody ApiRequest<ServiceRq<IdocSpvDetailUpdateUsedRq>> apiRequest) {

```
....
51.  public ApiResponse<?> updateUsed(@RequestBody
ApiRequest<ServiceRq<IdocSpvDetailUpdateUsedRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvdetail/IdocSpvDetailService.java

方法 public void updateUsed(@Valid @NotNull IdocSpvDetailUpdateUsedArg arg) {

```
....
158.  cmnIdocLogRepository.save(cmnIdocLogEntity);
```

Excessive Data Exposure

查詢路徑:

Java\Cx\Java Medium Threat\Excessive Data Exposure 版本:5

類別

OWASP ASVS: V03 Session Management
OWASP Top 10 2021: A1-Broken Access Control

描述

Excessive Data Exposure\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=10
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 的第 66 行中的 updateArg 內的資料可能是敏感的。通過位於 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 的第 66 行中的 updateArg 中的API 來暴露上述敏感資訊。

	來源	目的地

檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
行	68	68
物件	updateArg	updateArg

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<BranchCbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModUpdateRq>> apiRequest) {

```
....
68.  return ApiResponseBuilder.success(service.update(updateArg));
```

Excessive Data Exposure\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=11
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java 的第 66 行中的 updateArg 內的資料可能是敏感的。通過位於 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java 的第 66 行中的 updateArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java
行	68	68
物件	updateArg	updateArg

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {

```
....
68.  return
ApiResponseBuilder.success(branchCoreCbrDataService.update(updateArg));
```

Excessive Data Exposure\路徑 3:

嚴重程度：	中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=12
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 59 行中的createArg 內的資料可能是敏感的。通過位於 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 59 行中的createArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	61	61
物件	createArg	createArg

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModCreateRs>> create(@RequestBody ApiRequest<ServiceRq<CbrDataModCreateRq>> apiRequest) {

```
....
61.  return
ApiResponseBuilder.success(cbrDataModService.create(createArg));
```

Excessive Data Exposure\路徑 4:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=13
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 85 行中的updateArg 內的資料可能是敏感的。通過位於 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 85 行中的updateArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	87	87
物件	updateArg	updateArg

代碼片斷

檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<CbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<CbrDataModUpdateRq>> apiRequest) {

```
....
87.  return
ApiResponseBuilder.success(cbrDataModService.update(updateArg));
```

Excessive Data Exposure\路徑 5:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=14
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 124 行中的amendArg 內的資料可能是敏感的。通過位於 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 的第 124 行中的amendArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	126	126
物件	amendArg	amendArg

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<CbrDataModAmendRs>> amend(@RequestBody ApiRequest<ServiceRq<CbrDataModAmendRq>> apiRequest) {

```
....
126.  return
ApiResponseBuilder.success(cbrDataModService.amend(amendArg));
```

Excessive Data Exposure\路徑 6:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=15
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java 的第 48 行中的 rq 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java 的第 48 行中的rq 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java
行	50	50
物件	rq	rq

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java

方法 public ApiResponse<ServiceRs<NtfMessageCreateRs>> create(@RequestBody ApiRequest<ServiceRq<NtfMessageCreateRq>> apiRequest) {

```
....
50.  return
ApiResponseBuilder.success(service.create(controllerMapper.createRqToCre
ateArg(rq)));
```

Excessive Data Exposure\路徑 7:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=16
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java 的第 64 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java 的第 64 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java
行	66	66
物件	arg	arg

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/otp/NtfOtpController.java

方法 public ApiResponse<ServiceRs<NtfOtpVerifyRs>> verify(@RequestBody ApiRequest<ServiceRq<NtfOtpVerifyRq>> apiRequest) {

```
....
66.  return ApiResponseBuilder.success(ntfOtpService.verify(arg));
```

Excessive Data Exposure\路徑 8:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=17
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 49 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 49 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
行	51	51
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<CustomerFeeCreateRq>> apiRequest) {

```
....
51.  return ApiResponseBuilder.success(customerFeeService.create(arg));
```

Excessive Data Exposure\路徑 9:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=18
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 56 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 56 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
行	58	58

物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CustomerFeeUpdateRq>> apiRequest) {

```
....
58.  return ApiResponseBuilder.success(customerFeeService.update(arg));
```

Excessive Data Exposure\路徑 10:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=19
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 63 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 63 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
行	65	65
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CustomerFeeDeleteRq>> apiRequest) {

```
....
65.  return ApiResponseBuilder.success(customerFeeService.delete(arg));
```

Excessive Data Exposure\路徑 11:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=20

狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 70 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java 的第 70 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
行	72	72
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/fee/custfee/CustomerFeeController.java
方法	public ApiResponse<ServiceRs<CustomerFeeReadRs>> read(@RequestBody ApiRequest<ServiceRq<CustomerFeeReadRq>> apiRequest) {

```
....
72.  return ApiResponseBuilder.success(customerFeeService.read(arg));
```

Excessive Data Exposure\路徑 12:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=21
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 47 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 47 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
行	50	50
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<CustomerIntRateCreateRq>> apiRequest) {

```
....
50.  return
ApiResponseBuilder.success(customerIntRateService.create(arg));
```

Excessive Data Exposure\路徑 13:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=22
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 55 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 55 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
行	58	58
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
方法	public ApiResponse<ServiceRs<CustomerIntRateReadRs>> read(@RequestBody ApiRequest<ServiceRq<CustomerIntRateReadRq>> apiRequest) {

```
....
58.  return
ApiResponseBuilder.success(customerIntRateService.read(arg));
```

Excessive Data Exposure\路徑 14:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=23

狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 63 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 63 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
行	66	66
物件	arg	arg

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CustomerIntRateUpdateRq>> apiRequest) {

```
....
66.  return
ApiResponseBuilder.success(customerIntRateService.update(arg));
```

Excessive Data Exposure\路徑 15:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=24
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 71 行中的 arg 內的資料可能是敏感的。通過位於 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java 的第 71 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java
行	74	74

物件	arg	arg

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/pric/intrate/custintrate/CustomerIntRateController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CustomerIntRateDeleteRq>> apiRequest) {

```
....
74.  return
ApiResponseBuilder.success(customerIntRateService.delete(arg));
```

Excessive Data Exposure\路徑 16:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=25
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 33 行中的 queryKycArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 33 行中的queryKycArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java
行	35	35
物件	queryKycArg	queryKycArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java

方法 public ApiResponse<ServiceRs<QueryKycRs>> query(@RequestBody ApiRequest<ServiceRq<QueryKycRq>> apiRequest) {

```
....
35.  return ApiResponseBuilder.success(kycService.query(queryKycArg));
```

Excessive Data Exposure\路徑 17:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=26
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 57 行中的 queryKycArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 57 行中的queryKycArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java
行	59	59
物件	queryKycArg	queryKycArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java

方法 public ApiResponse<ServiceRs<CheckAmlRs>> checkAml(@RequestBody ApiRequest<ServiceRq<QueryKycRq>> apiRequest) {

```
....
59.  return
ApiResponseBuilder.success(kycService.checkAml(queryKycArg));
```

Excessive Data Exposure\路徑 18:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=27
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 69 行中的 queryKycArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java 的第 69 行中的queryKycArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java
行	71	71
物件	queryKycArg	queryKycArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/aml/KycController.java

方法 public ApiResponse<ServiceRs<UpdateLowRiskReviewRs>> updateLowRiskReviewIncomplete(@RequestBody ApiRequest<ServiceRq<QueryKycRq>> apiRequest) {

```
....
71.  return
ApiResponseBuilder.success(kycService.updateLowRiskReviewToComplete(quer
yKycArg));
```

Excessive Data Exposure\路徑 19:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=28
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java 的第 35 行中的 creditAndDepositConfirmationArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java 的第 35 行中的 creditAndDepositConfirmationArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java
行	37	37
物件	creditAndDepositConfirmationArg	creditAndDepositConfirmationArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java

方法 public ApiResponse<ServiceRs<CreditAndDepositCertRs>> query(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {

```
....
37.  return
ApiResponseBuilder.success(crCertService.query(creditAndDepositConfirmat
ionArg));
```

Excessive Data Exposure\路徑 20:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=29
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java 的第 48 行中的 creditAndDepositConfirmationArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java 的第 48 行中的 creditAndDepositConfirmationArg 中的API 來暴露上述敏感資訊。

	來源	目的地

檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java
行	50	50
物件	creditAndDepositConfirmationArg	creditAndDepositConfirmationArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java

方法 public ApiResponse<ServiceRs<CreditAndDepositCertRs>> print(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {

```
....
50.  return
ApiResponseBuilder.success(crCertService.print(creditAndDepositConfirmat
ionArg));
```

Excessive Data Exposure\路徑 21:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=30
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 28 行中的 depCertArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 28 行中的 depCertArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
行	30	30
物件	depCertArg	depCertArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java

方法 public ApiResponse<ServiceRs<DepQueryCertRs>> queryCustomer(@RequestBody ApiRequest<ServiceRq<DepCertRq>> apiRequest) {

```
....
30.  return
ApiResponseBuilder.success(depCertService.queryCustomer(depCertArg));
```

Excessive Data Exposure\路徑 22:

嚴重程度：	中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=31
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 35 行中的 depCertArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 35 行中的 depCertArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
行	37	37
物件	depCertArg	depCertArg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
方法	public ApiResponse<ServiceRs<DepQueryCertRs>> query(@RequestBody ApiRequest<ServiceRq<DepCertRq>> apiRequest) {

```
....
37.  return
ApiResponseBuilder.success(depCertService.query(depCertArg));
```

Excessive Data Exposure\路徑 23:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=32
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 42 行中的 depCertArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 42 行中的 depCertArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
行	44	44
物件	depCertArg	depCertArg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
方法	public ApiResponse<ServiceRs<DepQueryCertRs>> calculateTotalCertAmount(@RequestBody ApiRequest<ServiceRq<DepCertRq>> apiRequest) {

```
....
44.  return
ApiResponseBuilder.success(depCertService.calculateTotalCertAmount(depCe
rtArg));
```

Excessive Data Exposure\路徑 24:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=33
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 49 行中的 depCertArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java 的第 49 行中的 depCertArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
行	51	51
物件	depCertArg	depCertArg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/DepCertController.java
方法	public ApiResponse<ServiceRs<DepPrintCertRs>> print(@RequestBody ApiRequest<ServiceRq<DepCertRq>> apiRequest) {

```
....
51.  return
ApiResponseBuilder.success(depCertService.print(depCertArg));
```

Excessive Data Exposure\路徑 25:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=34
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crp/CrpController.java 的第 73 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crp/CrpController.java 的第 73 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crp/CrpController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crp/CrpController.java
行	75	75
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/crp/CrpController.java

方法 public ApiResponse<ServiceRs<CrpUpdateReserveRs>> updateReserve(@RequestBody ApiRequest<ServiceRq<CrpUpdateReserveRq>> apiRequest) {

```
....
75.  return ApiResponseBuilder.success(service.updateReserve(arg));
```

Excessive Data Exposure\路徑 26:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=35
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 63 行中的 argList 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 63 行中的argList 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	66	66
物件	argList	argList

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<List<FdrNegotiatedRq>>> apiRequest) {

```
....
66.  return ApiResponseBuilder.success(service.create(argList));
```

Excessive Data Exposure\路徑 27:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=36
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 90 行中的 argList 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 90 行中的argList 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	93	93
物件	argList	argList

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<List<FdrNegotiatedRq>>> apiRequest) {

```
....
93.  return ApiResponseBuilder.success(service.update(argList));
```

Excessive Data Exposure\路徑 28:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=37
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 104 行中的 argList 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 104 行中的argList 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	107	107
物件	argList	argList

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<List<FdrNegotiatedRq>>> apiRequest) {

```
....
107.  return ApiResponseBuilder.success(service.delete(argList));
```

Excessive Data Exposure\路徑 29:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=38
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 118 行中的 argList 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 118 行中的argList 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	121	121
物件	argList	argList

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> approve(@RequestBody ApiRequest<ServiceRq<List<FdrNegotiatedRq>>> apiRequest) {

```
....
121.  return ApiResponseBuilder.success(service.approve(argList));
```

Excessive Data Exposure\路徑 30:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=39
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 172 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 172 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	175	175
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> updateApprovalRecord(@RequestBody ApiRequest<ServiceRq<FdrNegotiatedRq>> apiRequest) {

```
....
175.  return
ApiResponseBuilder.success(service.updateApprovalRecord(arg));
```

Excessive Data Exposure\路徑 31:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=40
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 186 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java 的第 186 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
行	189	189
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> deleteApprovalRecord(@RequestBody ApiRequest<ServiceRq<FdrNegotiatedRq>> apiRequest) {

```
....
189.  return
ApiResponseBuilder.success(service.deleteApprovalRecord(arg));
```

Excessive Data Exposure\路徑 32:

嚴重程度： 中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=41
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/media/MediaIncomeTaxController.java 的第 55 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/media/MediaIncomeTaxController.java 的第 55 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/media/MediaIncomeTaxController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/media/MediaIncomeTaxController.java
行	57	57
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/media/MediaIncomeTaxController.java

方法 public ApiResponse<ServiceRs<MediaIncomeTaxRs>> maintain(@RequestBody ApiRequest<ServiceRq<MediaIncomeTaxRq>> apiRequest) {

```
....
57.  return ApiResponseBuilder.success(service.maintain(arg));
```

Excessive Data Exposure\路徑 33:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=42
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 50 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 50 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
行	52	52
物件	arg	arg

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
方法	public ApiResponse<ServiceRs<XauUpdatePbRs>> updatePassbookWithFee(@RequestBody ApiRequest<ServiceRq<XauUpdatePbWithFeeRq>> apiRequest) {

```
....
52.  return
ApiResponseBuilder.success(service.updatePassbookWithFee(arg));
```

Excessive Data Exposure\路徑 34:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=43
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 58 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 58 行中的arg 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
行	60	60
物件	arg	arg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
方法	public ApiResponse<ServiceRs<XauCustUpdateScrdRs>> updateScrd(@RequestBody ApiRequest<ServiceRq<XauUpdateScrdRq>> apiRequest) {

```
....
60.  return ApiResponseBuilder.success(service.updateScrd(arg));
```

Excessive Data Exposure\路徑 35:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=44
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 65 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-

app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 65 行中的arg 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
行	67	67
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java

方法 public ApiResponse<ServiceRs<XauCustProofPbBalRs>> proofPassbookBal(@RequestBody ApiRequest<ServiceRq<XauProofPbBalRq>> apiRequest) {

```
....
67.  return ApiResponseBuilder.success(service.proofPassbookBal(arg));
```

Excessive Data Exposure\路徑 36:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=45
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 80 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java 的第 80 行中的arg 中的 API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java
行	82	82
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/pbs/cust/PbsXauCustController.java

方法 public ApiResponse<ServiceRs<XauBaseInfoRs>> updateBaseInfo(@RequestBody ApiRequest<ServiceRq<XauBaseInfoUpdateRq>> apiRequest) {

```
....
82.  return ApiResponseBuilder.success(service.updateBaseInfo(arg));
```

Excessive Data Exposure\路徑 37:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=46
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/stampcard/StampCardController.java 的第 45 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/stampcard/StampCardController.java 的第 45 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/stampcard/StampCardController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/stampcard/StampCardController.java
行	47	47
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/stampcard/StampCardController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> create(@RequestBody ApiRequest<ServiceRq<StampCardRq>> apiRequest) {

```
....
47.  return ApiResponseBuilder.success(service.create(arg));
```

Excessive Data Exposure\路徑 38:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=47
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 80 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 80 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
行	82	82

物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
82.  return ApiResponseBuilder.success(service.readAccountDetails(arg));
```

Excessive Data Exposure\路徑 39:

嚴重程度： 中風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=48

狀態 新的

Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 90 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 90 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
行	92	92
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<List<InterestCalculationInfoRs>>> readInterestCalculation(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
92.  return
ApiResponseBuilder.success(service.readInterestCalculation(arg));
```

Excessive Data Exposure\路徑 40:

嚴重程度： 中風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=49

狀態 新的

Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 100 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 100 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
行	102	102
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<List<InterestPaidInfoRs>>> readInterestPaid(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
102.  return ApiResponseBuilder.success(service.readInterestPaid(arg));
```

Excessive Data Exposure\路徑 41:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=50
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 110 行中的 arg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java 的第 110 行中的arg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
行	112	112
物件	arg	arg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<List<RegularSavingInfoRs>>> readRegularSaving(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
112.  return ApiResponseBuilder.success(service.readRegularSaving(arg));
```

Excessive Data Exposure\路徑 42:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=51
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java 的第 38 行中的 allInOneTDArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java 的第 38 行中的 allInOneTDArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java
行	40	40
物件	allInOneTDArg	allInOneTDArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java

方法 public ApiResponse<ServiceRs<AllInOneTDRs>> query(@RequestBody ApiRequest<ServiceRq<AllInOneTDRq>> apiRequest) {

```
....
40.  return
ApiResponseBuilder.success(allInOneTDService.query(allInOneTDArg));
```

Excessive Data Exposure\路徑 43:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=52
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java 的第 46 行中的 allInOneTDArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java 的第 46 行中的 allInOneTDArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-	dep/dep-

	app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java	app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java
行	48	48
物件	allInOneTDArg	allInOneTDArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/timedep/AllInOneTDController.java

方法 public ApiResponse<ServiceRs<AllInOneTDReportRs>> printStatement(@RequestBody ApiRequest<ServiceRq<AllInOneTDRq>> apiRequest) {

```
....
48.  return
ApiResponseBuilder.success(allInOneTDService.printStatement(allInOneTDAr
g));
```

Excessive Data Exposure\路徑 44:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=53
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 43 行中的 accountTxArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 43 行中的 accountTxArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java
行	45	45
物件	accountTxArg	accountTxArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java

方法 public ApiResponse<ServiceRs<AccountTxnRs>> query(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
45.  return
ApiResponseBuilder.success(accountTxnService.query(accountTxArg));
```

Excessive Data Exposure\路徑 45:

嚴重程度： 中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=54
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 55 行中的 accountTxnArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 55 行中的 accountTxnArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java
行	57	57
物件	accountTxnArg	accountTxnArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java

方法 public ApiResponse<ServiceRs<AccountTxnStmtRs>> queryTxStatement(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
57.  return
ApiResponseBuilder.success(accountTxnService.queryStmt(accountTxnArg));
```

Excessive Data Exposure\路徑 46:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=55
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 72 行中的 accountTxnArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java 的第 72 行中的 accountTxnArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java
行	74	74
物件	accountTxnArg	accountTxnArg

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java
方法	public ApiResponse<ServiceRs<DiskReportRs>> printDisk(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
74.  return
ApiResponseBuilder.success(accountTxnService.printDisk(accountTxnArg));
```

Excessive Data Exposure\路徑 47:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=56
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/TellerTxnController.java 的第 42 行中的 tellerTxnArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/TellerTxnController.java 的第 42 行中的tellerTxnArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/TellerTxnController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/TellerTxnController.java
行	44	44
物件	tellerTxnArg	tellerTxnArg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/TellerTxnController.java
方法	public ApiResponse<ServiceRs<TellerTxnRs>> query(@RequestBody ApiRequest<ServiceRq<TellerTxnRq>> apiRequest) {

```
....
44.  return
ApiResponseBuilder.success(tellerTxnService.query(tellerTxnArg));
```

Excessive Data Exposure\路徑 48:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=57
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/VirtualAccountTxnController.java 的第 41 行中的 virtualAccountTxnArg 內的資料可能是敏感的。通過位於 dep/dep-

app/src/main/java/com/scsb/ncbs/dep/controller/txndata/VirtualAccountTxnController.java 的第 41 行中的 virtualAccountTxnArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/VirtualAccountTxnController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/VirtualAccountTxnController.java
行	43	43
物件	virtualAccountTxnArg	virtualAccountTxnArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/VirtualAccountTxnController.java

方法 public ApiResponse<ServiceRs<VirtualAccountTxnRs>> query(@RequestBody ApiRequest<ServiceRq<VirtualAccountTxnRq>> apiRequest) {

```
....
43.  return
ApiResponseBuilder.success(virtualAccountTxnService.query(virtualAccount
TxnArg));
```

Excessive Data Exposure\路徑 49:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=58
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java 的第 36 行中的 withholdingArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java 的第 36 行中的 withholdingArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java
行	38	38
物件	withholdingArg	withholdingArg

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java

方法 public ApiResponse<ServiceRs<QueryWithholdingRs>> query(@RequestBody ApiRequest<ServiceRq<QueryWithholdingRq>> apiRequest) {

```
....
38.  return
ApiResponseBuilder.success(withholdingService.query(withholdingArg));
```

Excessive Data Exposure\路徑 50:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=59
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java 的第 48 行中的 withholdingArg 內的資料可能是敏感的。通過位於 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java 的第 48 行中的 withholdingArg 中的API 來暴露上述敏感資訊。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java
行	50	50
物件	withholdingArg	withholdingArg

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java
方法	public ApiResponse<ServiceRs<PrintWithholdingRs>> print(@RequestBody ApiRequest<ServiceRq<PrintWithholdingRq>> apiRequest) {

```
....
50.  return
ApiResponseBuilder.success(withholdingService.print(withholdingArg));
```

Cleartext Submission of Sensitive Information

查詢路徑:

Java\Cx\Java Medium Threat\Cleartext Submission of Sensitive Information 版本:6

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.4 - Insecure communications
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Configuration Management
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 API: API7-Security Misconfiguration
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V09 Communication
OWASP Top 10 2021: A2-Cryptographic Failures

SANS top 25: SANS top 25
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.

描述

Cleartext Submission of Sensitive Information\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=72
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/multicurrencyaccount/MulticurrencyaccountT24Client.java 第 24 行的潛在敏感個人資料 accountId， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/multicurrencyaccount/MulticurrencyaccountT24Client.java 第 24 行的 getMcySubAccounts 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/multicurrencyaccount/MulticurrencyaccountT24Client.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/multicurrencyaccount/MulticurrencyaccountT24Client.java
行	27	28
物件	accountId	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/multicurrencyaccount/MulticurrencyaccountT24Client.java

方法 public List<McySubAccountsResponseBody> getMcySubAccounts(String accountId) {

```
....
27.   .uriVariable(ACCOUNT_ID, accountId)
28.   .build();
```

Cleartext Submission of Sensitive Information\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=73
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 30 行的潛在敏感個人資料 accountId， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 30 行的 getSimAutoDep 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
行	33	34
物件	accountId	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java

方法 public SimT24AutoDep getSimAutoDep(String accountId) {

```
....
33.   .uriVariable(ACCOUNT_ID, accountId)
34.   .build();
```

Cleartext Submission of Sensitive Information\路徑 3:

嚴重程度： 中風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=74
狀態 新的
Detection Date 12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 55 行的潛在敏感個人資料 accountId， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 55 行的 getT24InterestPayDetails 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
行	58	59
物件	accountId	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java

方法 public List<SimT24InterestPayDetail> getT24InterestPayDetails(String accountId) {

```
....
58.   .uriVariable(ACCOUNT_ID, accountId)
59.   .build();
```

Cleartext Submission of Sensitive Information\路徑 4:

嚴重程度： 中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=75
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 63 行的潛在敏感個人資料 accountId， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 63 行的 getT24ChequeInfo 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
行	66	67
物件	accountId	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java

方法 public SimT24ChequeInfo getT24ChequeInfo(String accountId) {

```
....
66.   .uriVariable(ACCOUNT_ID, accountId)
67.   .build();
```

Cleartext Submission of Sensitive Information\路徑 5:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=76
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 71 行的潛在敏感個人資料 accountId， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java 第 71 行的 getBcoChequeInfo 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
行	74	75
物件	accountId	build

代碼片斷

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
方法	public SimBcoChequeInfo getBcoChequeInfo(String accountId) {

```
....
74.   .uriVariable(ACCOUNT_ID, accountId)
75.   .build();
```

Cleartext Submission of Sensitive Information\路徑 6:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=77
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 327 行的潛在敏感個人資料 setCreditAccountId， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	347	26
物件	setCreditAccountId	build

代碼片斷

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
347.  body.setCreditAccountId(odchOrdertxnEntity.getCurrency() +
"1400500010005");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 7:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=78
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 389 行的潛在敏感個人資料 setCreditAccountId， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	408	26
物件	setCreditAccountId	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
408.  body.setCreditAccountId("PL54307");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 8:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=79
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 505 行的潛在敏感個人資料 setCreditAccountId， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	525	26
物件	setCreditAccountId	build

代碼片斷

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java

方法 rs.getAllConsolidatedOrderTxnEntities().forEach(odchOrdertxnEntity -> {

```
....
525.  body.setCreditAccountId(odchOrdertxnEntity.getCurrency() +
"1400500010005");
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java

方法 public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 9:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=80
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 565 行的潛在敏感個人資料 setCreditAccountId， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	588	26
物件	setCreditAccountId	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getRemSumTxnEntities().forEach(remOdchSumtxnEntity -> {

```
....
588.  body.setCreditAccountId(remOdchSumtxnEntity.getCurrency() +
"1400500010005");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 10:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=81
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 327 行的潛在敏感個人資料 setCreditCurrency， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	346	26
物件	setCreditCurrency	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
346.  body.setCreditCurrency(odchOrdertxnEntity.getCurrency());
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 11:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=82
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 389 行的潛在敏感個人資料 setCreditCurrency， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	407	26
物件	setCreditCurrency	build

代碼片斷

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
407.  body.setCreditCurrency(odchOrdertxnEntity.getCurrency());
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 12:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=83
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 505 行的潛在敏感個人資料 setCreditCurrency， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	524	26
物件	setCreditCurrency	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getAllConsolidatedOrderTxnEntities().forEach(odchOrdertxnEntity -> {

```
....
524.  body.setCreditCurrency(odchOrdertxnEntity.getCurrency());
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 13:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=84
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 565 行的潛在敏感個人資料 setCreditAmount， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	576	26
物件	setCreditAmount	build

代碼片斷

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java

方法 rs.getRemSumTxnEntities().forEach(remOdchSumtxnEntity -> {

```
....
576.  body.setCreditAmount(remOdchSumtxnEntity.getTotalComm());
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java

方法 public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 14:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=85
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 565 行的潛在敏感個人資料 setCreditCurrency， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	575	26
物件	setCreditCurrency	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getRemSumTxnEntities().forEach(remOdchSumtxnEntity -> {

```
....
575.  body.setCreditCurrency(remOdchSumtxnEntity.getCurrency());
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 15:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=86
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 327 行的潛在敏感個人資料 setCreditorAddress， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	349	26
物件	setCreditorAddress	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
349.  addresse.setCreditorAddress("999999");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 16:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=87
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 389 行的潛在敏感個人資料 setCreditorAddress， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	410	26
物件	setCreditorAddress	build

代碼片斷

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
410.   addresse.setCreditorAddress("999999");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 17:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=88
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 505 行的潛在敏感個人資料 setCreditorAddress， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	527	26
物件	setCreditorAddress	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getAllConsolidatedOrderTxnEntities().forEach(odchOrdertxnEntity -> {

```
....
527.  addresse.setCreditorAddress("999999");
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 18:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=89
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 565 行的潛在敏感個人資料 setCreditorAddress， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	590	26
物件	setCreditorAddress	build

代碼片斷

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java

方法 rs.getRemSumTxnEntities().forEach(remOdchSumtxnEntity -> {

```
....
590.  addresse.setCreditorAddress("999999");
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java

方法 public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 19:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=90
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 327 行的潛在敏感個人資料 CreditorAddresses， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	348	26
物件	CreditorAddresses	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
348.  SCSBFTforGLBody.CreditorAddresses addresse = new
SCSBFTforGLBody.CreditorAddresses();
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 20:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=91
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java 第 389 行的潛在敏感個人資料 CreditorAddresses， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	409	26
物件	CreditorAddresses	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/settletxn/OdchSettleTxnService.java
方法	rs.getSavedEntities().forEach(odchOrdertxnEntity -> {

```
....
409.  SCSBFTforGLBody.CreditorAddresses addresse = new
SCSBFTforGLBody.CreditorAddresses();
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 21:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=92
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 505 行的潛在敏感個人資料 CreditorAddresses， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	526	26
物件	CreditorAddresses	build

代碼片斷

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getAllConsolidatedOrderTxnEntities().forEach(odchOrdertxnEntity -> {

```
....
526.  SCSBFTforGLBody.CreditorAddresses addresse = new
SCSBFTforGLBody.CreditorAddresses();
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.   .build();
```

Cleartext Submission of Sensitive Information\路徑 22:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=93
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java 第 565 行的潛在敏感個人資料 CreditorAddresses， 透過非安全通道被傳送到 remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java 第 22 行的 create 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	589	26
物件	CreditorAddresses	build

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/sumtxn/OdchSumTxnService.java
方法	rs.getRemSumTxnEntities().forEach(remOdchSumtxnEntity -> {

```
....
589.  SCSBFTforGLBody.CreditorAddresses addresse = new
SCSBFTforGLBody.CreditorAddresses();
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

Cleartext Submission of Sensitive Information\路徑 23:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=94
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java 第 254 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-

service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java 第 54 行的 getReservedFunds 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java
行	261	59
物件	accountNo	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java

方法 protected static String getAccountCompany(String accountNo) {

```
....
261.  return accountNo.substring(0, 3);
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java

方法 public List<ReservedFundsResponseBody> getReservedFunds(BaseAccountArg arg) {

```
....
59.  .build();
```

Cleartext Submission of Sensitive Information\路徑 24:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=95
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/abi/AbiService.java 第 154 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java 第 54 行的 getReservedFunds 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/abi/AbiService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java
行	157	59
物件	accountNo	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/abi/AbiService.java

方法	List<ReservedFundsResponseBody> getReservedFunds(String accountNo) {

```
....
157.  arg.setAccountId(accountNo);
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java
方法	public List<ReservedFundsResponseBody> getReservedFunds(BaseAccountArg arg) {

```
....
59.  .build();
```

Cleartext Submission of Sensitive Information\路徑 25:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=96
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java 第 254 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java 第 54 行的 getReservedFunds 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java
行	264	59
物件	accountNo	build

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java
方法	protected static String getAccountCompany(String accountNo) {

```
....
264.  return "0".concat(accountNo.substring(0, 2));
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/account/AccountT24Client.java
方法	public List<ReservedFundsResponseBody> getReservedFunds(BaseAccountArg arg) {

```
....
59.  .build();
```

Cleartext Submission of Sensitive Information\路徑 26:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=97
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java 第 254 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java 第 24 行的 getAccountDetailsByArrangementId 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
行	261	29
物件	accountNo	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java

方法 protected static String getAccountCompany(String accountNo) {

```
....
261.  return accountNo.substring(0, 3);
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java

方法 public List<AccountDetailsByArrangementIdResponseBody> getAccountDetailsByArrangementId(BaseDep0005Arg arg) {

```
....
29.  .build();
```

Cleartext Submission of Sensitive Information\路徑 27:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=98
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java 第 254 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java 第 24 行的 getAccountDetailsByArrangementId 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
行	264	29
物件	accountNo	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java

方法 protected static String getAccountCompany(String accountNo) {

```
....
264.  return "0".concat(accountNo.substring(0, 2));
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java

方法 public List<AccountDetailsByArrangementIdResponseBody> getAccountDetailsByArrangementId(BaseDep0005Arg arg) {

```
....
29.  .build();
```

Cleartext Submission of Sensitive Information\路徑 28:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=99
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/neg/FdrNegService.java 第 1038 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java 第 24 行的 getAccountDetailsByArrangementId 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/neg/FdrNegService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
行	1044	29
物件	accountNo	build

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/fdr/neg/FdrNegService.java

方法	private List<CustomerEventCodesByAccountResponseBody> getCustomerEventCodesByAccount(String accountNo, String branchCode) {

```
....
1044.  dep0004Arg.setAccountNo(accountNo);
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
方法	public List<AccountDetailsByArrangementIdResponseBody> getAccountDetailsByArrangementId(BaseDep0005Arg arg) {

```
....
29.  .build();
```

Cleartext Submission of Sensitive Information\路徑 29:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=100
狀態	新的
Detection Date	12/12/2024 10:17:37 AM

len/len-service/src/main/java/com/scsb/ncbs/len/service/trading/InterestReceiptService.java 第 255 行的潛在敏感個人資料 accountNo， 透過非安全通道被傳送到 len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java 第 25 行的 getAccountLoanType 中。這可能暴露這些個人資料並允許其被竊取。

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/service/trading/InterestReceiptService.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java
行	260	30
物件	accountNo	build

代碼片斷	
檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/trading/InterestReceiptService.java
方法	private LendingAccountsResponseBody getLendingAccount(String accountNo) {

```
....
260.  arg.setAccountNo(accountNo);
```

檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java
方法	public List<AccountLoanTypeResponseBody> getAccountLoanType (String arrangementId, String coCode) {

```
....
30.  .build();
```

SSRF

查詢路徑:

Java\Cx\Java Medium Threat\SSRF 版本:3

類別

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A5-Broken Access Control
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
OWASP Top 10 2021: A10-Server-Side Request Forgery
ASA Premium: ASA Premium

描述

SSRF\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=101
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0013/Len0013T24Client.java文件中的第28行的build傳送請求至遠端伺服器，攻擊者能夠透過len/len-app/src/main/java/com/scsb/ncbs/len/controller/query/LendingAccountController.java文件中的第30行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	len/len-app/src/main/java/com/scsb/ncbs/len/controller/query/LendingAccountController.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0013/Len0013T24Client.java
行	30	33
物件	apiRequest	build

代碼片斷

檔案名稱 len/len-app/src/main/java/com/scsb/ncbs/len/controller/query/LendingAccountController.java

方法 public ApiResponse<ServiceRs<LendingAccountRs>> query(@RequestBody ApiRequest<ServiceRq<LendingAccountRq>> apiRequest) {

```
....
30.  public ApiResponse<ServiceRs<LendingAccountRs>> query(@RequestBody
ApiRequest<ServiceRq<LendingAccountRq>> apiRequest) {
```

檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0013/Len0013T24Client.java
方法	public List<OverdueBillsResponseBody> getOverdueBills (String arrangementId, String coCode) {

```
....
33.   .build();
```

SSRF\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=102
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/t24/gpi/GPIT24Client.java文件中的第54行的build傳送請求至遠端伺服器，攻擊者能夠透過rem/rem-app/src/main/java/com/scsb/ncbs/rem/controller/cinq/ComplexTradeInquiryController.java文件中的第324行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	rem/rem-app/src/main/java/com/scsb/ncbs/rem/controller/cinq/ComplexTradeInquiryController.java	rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/t24/gpi/GPIT24Client.java
行	324	58
物件	apiRequest	build

代碼片斷

檔案名稱	rem/rem-app/src/main/java/com/scsb/ncbs/rem/controller/cinq/ComplexTradeInquiryController.java
方法	public ApiResponse<ServiceRs<List<GetGpiRs>>> getGpi(@RequestBody ApiRequest<ServiceRq<GetGpiRq>> apiRequest) {

```
....
324.  public ApiResponse<ServiceRs<List<GetGpiRs>>> getGpi(@RequestBody
ApiRequest<ServiceRq<GetGpiRq>> apiRequest) {
```

檔案名稱	rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/t24/gpi/GPIT24Client.java
方法	public List<FTNumberQueryWithRefnoResponseBody> getFTNumberWithRefno(BaseFTNumberQueryWithRefnoArg arg) {

```
....
58.   .build();
```

SSRF\路徑 3:

嚴重程度：	中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=103
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java文件中的第42行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java文件中的第39行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java
行	39	46
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java

方法 public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){

```
....
39.  public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody
ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/simulation/SimulationClient.java

方法 public SimEcifCustomerInfo getEcifCustomerInfo(String customerId) {

```
....
46.  .build();
```

SSRF\路徑 4:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=104
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第44行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java文件中的第43行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	43	49
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java

方法 public ApiResponse<ServiceRs<AccountTxnRs>> query(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<AccountTxnRs>> query(@RequestBody
ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<ArrangementDetailsResponseBody> getArrangementDetails(BaseArrangementArg arg) {

```
....
49.  .build();
```

SSRF\路徑 5:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=105
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第44行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java文件中的第55行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

行	55	49
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java

方法 public ApiResponse<ServiceRs<AccountTxnStmtRs>> queryTxStatement(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
55.  public ApiResponse<ServiceRs<AccountTxnStmtRs>>
queryTxStatement(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>>
apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<ArrangementDetailsResponseBody> getArrangementDetails(BaseArrangementArg arg) {

```
....
49.  .build();
```

SSRF\路徑 6:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=106
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第44行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java文件中的第72行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	72	49
物件	apiRequest	build

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/txndata/AccountTxnController.java
方法	public ApiResponse<ServiceRs<DiskReportRs>> printDisk(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {

```
....
72.  public ApiResponse<ServiceRs<DiskReportRs>> printDisk(@RequestBody
ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<ArrangementDetailsResponseBody> getArrangementDetails(BaseArrangementArg arg) {

```
....
49.  .build();
```

SSRF\路徑 7:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=107
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第44行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-rpt/src/main/java/com/scsb/ncbs/dep/controller/AccountTxnController.java文件中的第42行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-rpt/src/main/java/com/scsb/ncbs/dep/controller/AccountTxnController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	42	49
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-rpt/src/main/java/com/scsb/ncbs/dep/controller/AccountTxnController.java
方法	public ApiResponse<ServiceRs<ReportDataRs>> queryTxStatement(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>> apiRequest) throws Throwable {

```
....
42.  public ApiResponse<ServiceRs<ReportDataRs>>
queryTxStatement(@RequestBody ApiRequest<ServiceRq<AccountTxnRq>>
apiRequest) throws Throwable {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<ArrangementDetailsResponseBody> getArrangementDetails(BaseArrangementArg arg) {

```
....
49.  .build();
```

SSRF\路徑 8:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=108
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第44行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	80	49
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<ArrangementDetailsResponseBody> getArrangementDetails(BaseArrangementArg arg) {

```
....
49.  .build();
```

SSRF\路徑 9:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=109
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java文件中的第24行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java文件中的第50行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
行	50	29
物件	apiRequest	build

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/fdr/neg/FdrNegController.java
方法	public ApiResponse<ServiceRs<FdrNegReadAccountRs>> readAccountInformation(@RequestBody ApiRequest<ServiceRq<FdrNegReadAccountRq>> apiRequest) {

```
....
50.  public ApiResponse<ServiceRs<FdrNegReadAccountRs>>
readAccountInformation(@RequestBody
ApiRequest<ServiceRq<FdrNegReadAccountRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0005/Dep0005T24Client.java
方法	public List<AccountDetailsByArrangementIdResponseBody> getAccountDetailsByArrangementId(BaseDep0005Arg arg) {

```
....
29.  .build();
```

SSRF\路徑 10:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=110
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java文件中的第38行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/adi/abi/AbiController.java文件中的第34行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/adi/abi/AbiController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java
行	34	43
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/adi/abi/AbiController.java

方法 public ApiResponse<ServiceRs<AccountBalanceRs>> queryActBalance(@RequestBody ApiRequest<ServiceRq<AccountBalanceRq>> apiRequest) {

```
....
34.  public ApiResponse<ServiceRs<AccountBalanceRs>>
queryActBalance(@RequestBody ApiRequest<ServiceRq<AccountBalanceRq>>
apiRequest)  {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java

方法 public CustomerResponseBody getCustomer(BaseCustomerArg arg) {

```
....
43.  .build();
```

SSRF\路徑 11:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=111

狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java文件中的第38行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java
行	80	43
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java

方法 public CustomerResponseBody getCustomer(BaseCustomerArg arg) {

```
....
43.  .build();
```

SSRF\路徑 12:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=112
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java文件中的第38行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java文件中的第39行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地

檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java
行	39	43
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java

方法 public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){

```
....
39.  public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody
ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java

方法 public CustomerResponseBody getCustomer(BaseCustomerArg arg) {

```
....
43.  .build();
```

SSRF\路徑 13:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=113
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java文件中的第38行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfTwdController.java文件中的第33行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfTwdController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java
行	33	43
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfTwdController.java

方法	public ApiResponse<ServiceRs<PtfTwdCreateRs>> create(@RequestBody ApiRequest<ServiceRq<PtfTwdCreateRq>> apiRequest){

```
....
33.  public ApiResponse<ServiceRs<PtfTwdCreateRs>> create(@RequestBody
ApiRequest<ServiceRq<PtfTwdCreateRq>> apiRequest){
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/customer/CustomerT24Client.java
方法	public CustomerResponseBody getCustomer(BaseCustomerArg arg) {

```
....
43.  .build();
```

SSRF\路徑 14:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=114
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java文件中的第24行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java文件中的第35行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java
行	35	29
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java
方法	public ApiResponse<ServiceRs<CreditAndDepositCertRs>> query(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {

```
....
35.  public ApiResponse<ServiceRs<CreditAndDepositCertRs>>
query(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java

方法	public List<SubAccountsResponseBody> getSubAccounts(BaseDep0006Arg arg) {

```
....
29.   .build();
```

SSRF\路徑 15:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=115
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java文件中的第24行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java文件中的第48行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java
行	48	29
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/certification/CrCertController.java
方法	public ApiResponse<ServiceRs<CreditAndDepositCertRs>> print(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<CreditAndDepositCertRs>>
print(@RequestBody ApiRequest<ServiceRq<CrCertRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/dep0006/Dep0006T24Client.java
方法	public List<SubAccountsResponseBody> getSubAccounts(BaseDep0006Arg arg) {

```
....
29.   .build();
```

SSRF\路徑 16:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=116

狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第104行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第110行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	110	109
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<List<RegularSavingInfoRs>>> readRegularSaving(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
110.  public ApiResponse<ServiceRs<List<RegularSavingInfoRs>>>
readRegularSaving(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<ArrangementActivityResponseBody> getArrangementActivity(BaseArrangementArg arg) {

```
....
109.  .build();
```

SSRF\路徑 17:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=117
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第94行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-

app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第100行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	100	99
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<List<InterestPaidInfoRs>>> readInterestPaid(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
100.  public ApiResponse<ServiceRs<List<InterestPaidInfoRs>>>
readInterestPaid(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<InterestPaidResponseBody> getInterestPaid(BaseArrangementArg arg) {

```
....
99.  .build();
```

SSRF\路徑 18:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=118
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第74行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

行	80	79
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
方法	public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<SettlementDetailsResponseBody> getSettlementDetails(BaseArrangementArg arg) {

```
....
79.  .build();
```

SSRF\路徑 19:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=119
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第64行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	80	69
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法	public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<ScheduleDetailsResponseBody> getScheduleDetails(BaseArrangementArg arg) {

```
....
69.  .build();
```

SSRF\路徑 20:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=120
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第34行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	80	39
物件	apiRequest	build

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
方法	public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<InterestDetailsResponseBody> getInterestDetails(BaseArrangementArg arg) {

```
....
39.   .build();
```

SSRF\路徑 21:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=121
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/currency/CurrencyT24Client.java文件中的第25行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java文件中的第39行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/currency/CurrencyT24Client.java
行	39	30
物件	apiRequest	build

代碼片斷

檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/ptf/PtfFxController.java
方法	public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){

```
....
39.  public ApiResponse<ServiceRs<PtfFxCreateRs>> create(@RequestBody
ApiRequest<ServiceRq<PtfFxCreateRq>> apiRequest){
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/currency/CurrencyT24Client.java
方法	public List<CurrenciesResponseBody> getCurrencies(BaseCurrencyArg arg) {

```
....
30.   .build();
```

SSRF\路徑 22:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=122
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第84行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第90行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	90	89
物件	apiRequest	build

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java
方法	public ApiResponse<ServiceRs<List<InterestCalculationInfoRs>>> readInterestCalculation(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
90.  public ApiResponse<ServiceRs<List<InterestCalculationInfoRs>>>
readInterestCalculation(@RequestBody
ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
方法	public List<InterestAccrualsResponseBody> getInterestAccruals(BaseArrangementArg arg) {

```
....
89.  .build();
```

SSRF\路徑 23:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=123
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java文件中的第24行的build傳送請求至遠端伺服器，攻擊者能夠透過dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java文件中的第80行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java
行	80	29
物件	apiRequest	build

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/tdb/TimeDepController.java

方法 public ApiResponse<ServiceRs<TimeDepositDetailRs>> readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<TimeDepositDetailRs>>
readAccountDetail(@RequestBody ApiRequest<ServiceRq<TdbReadDetailsRq>>
apiRequest)  {
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/t24/arrangement/ArrangementT24Client.java

方法 public List<ArrangementDatesResponseBody> getArrangementDates(BaseArrangementArg arg) {

```
....
29.  .build();
```

SSRF\路徑 24:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=124
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java文件中的第25行的build傳送請求至遠端伺服器，攻擊者能夠透過len/len-app/src/main/java/com/scsb/ncbs/len/controller/trading/InterestReceiptController.java文件中的第37行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地

檔案	len/len-app/src/main/java/com/scsb/ncbs/len/controller/trading/InterestReceiptController.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java
行	37	30
物件	apiRequest	build

代碼片斷

檔案名稱 len/len-app/src/main/java/com/scsb/ncbs/len/controller/trading/InterestReceiptController.java

方法 public ApiResponse<ServiceRs<InterestReceiptRs>> query(@RequestBody @Valid ApiRequest<ServiceRq<InterestReceiptRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<InterestReceiptRs>> query(@RequestBody
@Valid ApiRequest<ServiceRq<InterestReceiptRq>> apiRequest) {
```

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/service/t24/len0008/Len0008T24Client.java

方法 public List<AccountLoanTypeResponseBody> getAccountLoanType (String arrangementId, String coCode) {

```
....
30.  .build();
```

SSRF\路徑 25:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=125
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

應用程式使用remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java文件中的第22行的build傳送請求至遠端伺服器，攻擊者能夠透過remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java文件中的第49行的apiRequest來控制該請求傳送URL或其他資料。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
行	49	26
物件	apiRequest	build

代碼片斷

檔案名稱	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java
方法	public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws Throwable {

```
....
49.  public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody
ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws
Throwable {
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/service/odch/t24/sumtxn/FundsTransferGLClient.java
方法	public SCSBFTforGLResponseBody create(SCSBFTforGLBody body) {

```
....
26.  .build();
```

DB Parameter Tampering

查詢路徑:

Java\Cx\Java Medium Threat\DB Parameter Tampering 版本:1

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A4-Insecure Direct Object References
FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A5-Broken Access Control
OWASP Top 10 API: API1-Broken Object Level Authorization
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V01 Architecture, Design and Threat Modeling
OWASP Top 10 2021: A1-Broken Access Control
SANS top 25: SANS top 25
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.

描述

DB Parameter Tampering\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=2
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 第 79 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java
行	79	40
物件	apiRequest	cbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java

方法 void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=3
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 第 79 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地

檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java
行	79	40
物件	apiRequest	cbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java

方法 void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 3:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=4
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 第 79 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java
行	79	40
物件	apiRequest	cbrDataModListId

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java
方法	void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 4:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=5
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 第 79 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java
行	79	40
物件	apiRequest	cbrDataModListId

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java

方法 void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 5:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=6
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 第 98 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java
行	98	40
物件	apiRequest	cbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileARepository.java

方法	void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 6:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=7
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 第 98 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java
行	98	40
物件	apiRequest	cbrDataModListId

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileGRepository.java
方法	void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 7:

嚴重程度：	中風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=8
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 第 98 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java
行	98	40
物件	apiRequest	cbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileBRepository.java

方法 void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

DB Parameter Tampering\路徑 8:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=9
狀態	新的
Detection Date	12/12/2024 10:17:35 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 第 98 行的 delete 方法從 apiRequest 元素接收了使用者輸入變數，這個輸入變數之後在沒有驗證下被應用程式用來過濾敏感性資料庫中個人資料紀錄的資料表，cbr/cbr-

service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java 第 40 行的 delByCbrDataModListId 方法在沒有加入其他額外資料庫過濾的情況下向 cbrDataModListId 資料庫進行查詢，這會讓使用者能夠單純使用不同的 id 選擇到不同資料。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java
行	98	40
物件	apiRequest	cbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/persistence/repository/file/CbrFileFRepository.java

方法 void delByCbrDataModListId(@Param("cbrDataModListId") Long cbrDataModListId);

```
....
40.  void delByCbrDataModListId(@Param("cbrDataModListId") Long
cbrDataModListId);
```

Unchecked Input for Loop Condition

查詢路徑:

Java\Cx\Java Medium Threat\Unchecked Input for Loop Condition 版本:6

類別

OWASP Top 10 API: API4-Lack of Resources and Rate Limiting
OWASP Top 10 2021: A3-Injection
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-002530 - CAT II The application must validate all input.

描述

Unchecked Input for Loop Condition\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=126
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

方法create在cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java 第 38 行，從元素apiRequest 取得使用者輸入。該元素的值流經程式碼沒有被驗證，並最終於cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java 的第472 行 findWeekendDates 方法，用於迴圈條件中。這構成一個未經檢查迴圈條件(Unchecked Input for Loop Condition)。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
行	38	485
物件	apiRequest	endDate

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<?> create(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
38.  public ApiResponse<?> create(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java

方法 public static List<Integer> findWeekendDates(int year, int month) {

```
....
485.  while (!startDate.isAfter(endDate)) {
```

Unchecked Input for Loop Condition\路徑 2:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=127
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

方法create在cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java 第 38 行，從元素apiRequest 取得使用者輸入。該元素的值流經程式碼沒有被驗證，並最終於cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java 的第472 行 findWeekendDates 方法，用於迴圈條件中。這構成一個未經檢查迴圈條件(Unchecked Input for Loop Condition)。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
行	38	485

物件	apiRequest	startDate

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
方法	public ApiResponse<?> create(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
38.  public ApiResponse<?> create(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
方法	public static List<Integer> findWeekendDates(int year, int month) {

```
....
485.  while (!startDate.isAfter(endDate)) {
```

Unchecked Input for Loop Condition\路徑 3:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=128
狀態	新的
Detection Date	12/12/2024 10:17:45 AM

方法create在cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java 第48 行，從元素 apiRequest 取得使用者輸入。該元素的值流經程式碼沒有被驗證，並最終於cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java 的第289 行 custMessageProcess 方法，用於迴圈條件中。這構成一個未經檢查迴圈條件(Unchecked Input for Loop Condition)。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java
行	48	317
物件	apiRequest	matchFormat

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ntf/message/NtfMessageController.java
方法	public ApiResponse<ServiceRs<NtfMessageCreateRs>> create(@RequestBody ApiRequest<ServiceRq<NtfMessageCreateRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<NtfMessageCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<NtfMessageCreateRq>>
apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java
方法	public List<NtfMessageSendInfo> custMessageProcess(CmnNtfMessageEntity messageEntity, TmpNtfMessageCustInfo info) {

```
....
317.  while (matchFormat.find()) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy

查詢路徑:

Java\Cx\Java Spring\Spring Overly Permissive Cross Origin Resource Sharing Policy 版本:2

類別

OWASP ASVS: V14 Configuration
OWASP Top 10 2021: A7-Identification and Authentication Failures

描述

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=452
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 文件第 53 行上的 readRejected 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
行	53	53
物件	readRejected	readRejected

代碼片斷

檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
方法	public ApiResponse<ServiceRs<BranchCbrDataModReadRejectedRs>> readRejected(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModReadRejectedRq>> apiRequest) {

```
....
53.  public ApiResponse<ServiceRs<BranchCbrDataModReadRejectedRs>>
readRejected(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModReadRejectedRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=453
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 文件第 66 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
行	66	66
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<BranchCbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModUpdateRq>> apiRequest) {

```
....
66.  public ApiResponse<ServiceRs<BranchCbrDataModUpdateRs>>
update(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModUpdateRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=454
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java 文件第 79 行上的 delete 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll

	er/branch/BranchCbrDataModController.java	er/branch/BranchCbrDataModController.java
行	79	79
物件	delete	delete

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 4:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=455
狀態 新的
Detection Date 12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java 文件第 53 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java
行	53	53
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>> apiRequest) {

```
....
53.  public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=456

狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java 文件第 66 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java
行	66	66
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {

```
....
66.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=457
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java 文件第 48 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java

方法 public ApiResponse<ServiceRs<BranchDailySettlementReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchDailySettlementReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchDailySettlementReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchDailySettlementReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=458
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java 文件第 48 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java

方法 public ApiResponse<ServiceRs<BranchErrorReportReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchErrorReportReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchErrorReportReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchErrorReportReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=459
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java 文件第 48 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java

行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java

方法 public ApiResponse<ServiceRs<BranchTxnDailyReportReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchTxnDailyReportReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchTxnDailyReportReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchTxnDailyReportReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=460
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java 文件第 48 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java

方法 public ApiResponse<ServiceRs<BranchTxnDetailReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchTxnDetailReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchTxnDetailReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchTxnDetailReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=461

狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java 文件第 54 行上的 readError 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	54	54
物件	readError	readError

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadErrorRs>> readError(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadErrorRq>> apiRequest) {

```
....
54.  public ApiResponse<ServiceRs<CbrDataInquiryReadErrorRs>>
readError(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadErrorRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=462
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java 文件第 67 行上的 readDeclaration 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	67	67
物件	readDeclaration	readDeclaration

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadDeclarationRs>> readDeclaration(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadDeclarationRq>> apiRequest) {

```
....
67.  public ApiResponse<ServiceRs<CbrDataInquiryReadDeclarationRs>>
readDeclaration(@RequestBody
ApiRequest<ServiceRq<CbrDataInquiryReadDeclarationRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 12:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=463
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java 文件第 80 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	80	80
物件	read	read

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
方法	public ApiResponse<ServiceRs<CbrDataInquiryReadRs>> read(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<CbrDataInquiryReadRs>>
read(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=464
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java 文件第 93 行上的 readRejected 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

行	93	93
物件	readRejected	readRejected

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadRejectedRs>> readRejected(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRejectedRq>> apiRequest) {

```
....
93.  public ApiResponse<ServiceRs<CbrDataInquiryReadRejectedRs>>
readRejected(@RequestBody
ApiRequest<ServiceRq<CbrDataInquiryReadRejectedRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 14:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=465
狀態 新的
Detection Date 12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 59 行上的 create 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	59	59
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModCreateRs>> create(@RequestBody ApiRequest<ServiceRq<CbrDataModCreateRq>> apiRequest) {

```
....
59.  public ApiResponse<ServiceRs<CbrDataModCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<CbrDataModCreateRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 15:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=466
狀態 新的

Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 72 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	72	72
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModReadRs>> read(@RequestBody ApiRequest<ServiceRq<CbrDataModReadRq>> apiRequest) {

```
....
72.  public ApiResponse<ServiceRs<CbrDataModReadRs>> read(@RequestBody
ApiRequest<ServiceRq<CbrDataModReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 16:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=467
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 85 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	85	85
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<CbrDataModUpdateRq>> apiRequest) {

```
....
85.  public ApiResponse<ServiceRs<CbrDataModUpdateRs>>
update(@RequestBody ApiRequest<ServiceRq<CbrDataModUpdateRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 17:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=468
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 98 行上的 delete 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	98	98
物件	delete	delete

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 18:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=469
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 111 行上的 reject 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	111	111
物件	reject	reject

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法	public ApiResponse<ServiceRs<EmptyRs>> reject(@RequestBody ApiRequest<ServiceRq<CbrDataModRejectRq>> apiRequest) {

```
....
111.  public ApiResponse<ServiceRs<EmptyRs>> reject(@RequestBody
ApiRequest<ServiceRq<CbrDataModRejectRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 19:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=470
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java 文件第 124 行上的 amend 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	124	124
物件	amend	amend

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<CbrDataModAmendRs>> amend(@RequestBody ApiRequest<ServiceRq<CbrDataModAmendRq>> apiRequest) {

```
....
124.  public ApiResponse<ServiceRs<CbrDataModAmendRs>>
amend(@RequestBody ApiRequest<ServiceRq<CbrDataModAmendRq>> apiRequest)
{
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 20:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=471
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java 文件第 37 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll

	er/file/CbrFileKController.java	er/file/CbrFileKController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java

方法 public ApiResponse<ServiceRs<FileKReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileKReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileKReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileKReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 21:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=472
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java 文件第 49 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java
行	49	49
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileKUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileKUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 22:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=473
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java 文件第 37 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java

方法 public ApiResponse<ServiceRs<FileLReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileLReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileLReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileLReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 23:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=474
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java 文件第 49 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java
行	49	49
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileLUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileLUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 24:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=475
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java 文件第 37 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
行	37	37
物件	read	read

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
方法	public ApiResponse<ServiceRs<FileMReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileMReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileMReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileMReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 25:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=476
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java 文件第 49 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
行	49	49
物件	update	update

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileMUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileMUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 26:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=477
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java 文件第 37 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java

方法 public ApiResponse<ServiceRs<FilePReadRs>> read(@RequestBody ApiRequest<ServiceRq<FilePReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FilePReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FilePReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 27:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=478
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java 文件第 49 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java
行	49	49

物件	update	update

代碼片斷
檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java
方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FilePUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FilePUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 28:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=479
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java 文件第 35 行上的 compileData 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java
行	35	35
物件	compileData	compileData

代碼片斷
檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java
方法 public ApiResponse<ServiceRs<FileSummaryReadRs>> compileData(@RequestBody ApiRequest<ServiceRq<FileSummaryCompileDataRq>> apiRequest) {

```
....
35.  public ApiResponse<ServiceRs<FileSummaryReadRs>>
compileData(@RequestBody ApiRequest<ServiceRq<FileSummaryCompileDataRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 29:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=480
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java 文件第 46 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java
行	46	46
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java

方法 public ApiResponse<ServiceRs<FXSpotReadRs>> read(@RequestBody ApiRequest<ServiceRq<FXSpotReadRq>> apiRequest) {

```
....
46.  public ApiResponse<ServiceRs<FXSpotReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FXSpotReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 30:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=481
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java 文件第 43 行上的 readByType 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	43	43
物件	readByType	readByType

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法 public ApiResponse<ServiceRs<List<CbrOrgKeywordRs>>> readByType(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordReadByTypeRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<List<CbrOrgKeywordRs>>>
readByType(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordReadByTypeRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 31:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=482
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java 文件第 55 行上的 create 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	55	55
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法 public ApiResponse<ServiceRs<String>> create(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordCreateRq>> apiRequest) {

```
....
55.  public ApiResponse<ServiceRs<String>> create(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordCreateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 32:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=483
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java 文件第 68 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	68	68
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordUpdateRq>> apiRequest) {

```
....
68.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordUpdateRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 33:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=484
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java 文件第 81 行上的 delete 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	81	81
物件	delete	delete

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordDeleteRq>> apiRequest) {

```
....
81.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordDeleteRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 34:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=485
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java 文件第 43 行上的 readAll 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll

	er/param/CbrReturnReasonController.java	er/param/CbrReturnReasonController.java
行	43	43
物件	readAll	readAll

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<List<CbrReturnReasonRs>>> readAll(@RequestBody ApiRequest<ServiceRq<EmptyRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<List<CbrReturnReasonRs>>>
readAll(@RequestBody ApiRequest<ServiceRq<EmptyRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 35:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=486
狀態 新的
Detection Date 12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java 文件第 55 行上的 create 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	55	55
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<String>> create(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonCreatedRq>> apiRequest) {

```
....
55.  public ApiResponse<ServiceRs<String>> create(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonCreatedRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 36:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=487

狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java 文件第 67 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	67	67
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonUpdatedRq>> apiRequest) {

```
....
67.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonUpdatedRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 37:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=488
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java 文件第 80 行上的 delete 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	80	80
物件	delete	delete

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonDeletedRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonDeletedRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 38:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=489
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java 文件第 44 行上的 generate 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java
行	44	44
物件	generate	generate

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java

方法 public ApiResponse<ServiceRs<ReportGenerateRs>> generate(@RequestBody ApiRequest<ServiceRq<ReportGenerateRq>> apiRequest) {

```
....
44.  public ApiResponse<ServiceRs<ReportGenerateRs>>
generate(@RequestBody ApiRequest<ServiceRq<ReportGenerateRq>>
apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 39:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=490
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java 文件第 21 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java
行	21	21

物件	read	read

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java

方法 public ApiResponse<ServiceRs<CmnBdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<CmnBdayNextReadRq>> rq);

```
....
21.  public ApiResponse<ServiceRs<CmnBdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<CmnBdayNextReadRq>> rq);
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 40:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=491
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java 文件第 21 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java
行	21	21
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java

方法 public ApiResponse<ServiceRs<RemExchangeRateReadRs>> read(@RequestBody ApiRequest<ServiceRq<RemExchangeRateReadRq>> rq);

```
....
21.  public ApiResponse<ServiceRs<RemExchangeRateReadRs>>
read(@RequestBody ApiRequest<ServiceRq<RemExchangeRateReadRq>> rq);
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 41:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=492
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java 文件第 39 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
行	39	39
物件	read	read

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayInfoReadRq>> apiRequest) {

```
....
39.  public ApiResponse<ServiceRs<BdayInfoReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayInfoReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 42:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=493
狀態 新的
Detection Date 12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java 文件第 45 行上的 readBusDaysBetween 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
行	45	45
物件	readBusDaysBetween	readBusDaysBetween

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 43:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=494
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java 文件第 38 行上的 create 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	38	38
物件	create	create

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<?> create(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
38.  public ApiResponse<?> create(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 44:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=495
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java 文件第 46 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	46	46

物件	update	update

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
46.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 45:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=496

狀態 新的

Detection Date 12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java 文件第 54 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	54	54
物件	read	read

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<ServiceRs<BdayInitReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayInitReadRq>> apiRequest) {

```
....
54.  public ApiResponse<ServiceRs<BdayInitReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayInitReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 46:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=497

狀態 新的

Detection Date 12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java 文件第 36 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java
行	36	36
物件	read	read

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java

方法 public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 47:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=498
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java 文件第 36 行上的 read 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java
行	36	36
物件	read	read

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java

方法 public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 48:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=499
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java 文件第 37 行上的 readJson 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java
行	37	37
物件	readJson	readJson

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java

方法 public ApiResponse<ServiceRs<BdayProvReadJsonListRs>> readJson(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<BdayProvReadJsonListRs>>
readJson(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest)
{
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 49:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=500
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java 文件第 43 行上的 readChar 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java
行	43	43
物件	readChar	readChar

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java

方法	public ApiResponse<ServiceRs<BdayProvReadCharListRs>> readChar(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<BdayProvReadCharListRs>>
readChar(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest)
{
```

Spring Overly Permissive Cross Origin Resource Sharing Policy\路徑 50:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=501
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java 文件第 34 行上的 update 方法設置了過度寬鬆的 CORS 訪問控制來源標頭。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java
行	34	34
物件	update	update

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java
方法	public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<BdaySuspUpdateRq>> apiRequest) {

```
....
34.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<BdaySuspUpdateRq>> apiRequest) {
```

Improper Resource Access Authorization

查詢路徑:

Java\Cx\Java Low Visibility\Improper Resource Access Authorization 版本:11

類別

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V04 Access Control
OWASP Top 10 2021: A1-Broken Access Control
SANS top 25: SANS top 25

描述

Improper Resource Access Authorization\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=213
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java 的第 78 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java
行	80	80
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java

方法 List<DepCondensedTransactionDetailsEntity> getData(String accountNo, LocalDate condensedDate) throws Exception {

```
....
80.  reader.readLine();
```

Improper Resource Access Authorization\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=214
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java 的第 78 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java
行	83	83
物件	readLine	readLine

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java
方法	List<DepCondensedTransactionDetailsEntity> getData(String accountNo, LocalDate condensedDate) throws Exception {

```
....
83.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=215
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 312 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	314	314
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	<T extends ReserveArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
314.  reader.readLine();
```

Improper Resource Access Authorization\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=216
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 312 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

行	318	318
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 <T extends ReserveArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
318.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=217
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 333 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	335	335
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 List<UpdateReserveArg> getCsvDate() throws Exception {

```
....
335.  reader.readLine();
```

Improper Resource Access Authorization\路徑 6:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=218
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 333 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地

檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	338	338
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 List<UpdateReserveArg> getCsvDate() throws Exception {

```
....
338.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=219
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 352 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	354	354
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 List<RemarkArg> getRemarkCsvDate() throws Exception {

```
....
354.  reader.readLine();
```

Improper Resource Access Authorization\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=220
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 的第 352 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	357	357
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 List<RemarkArg> getRemarkCsvDate() throws Exception {

```
....
357.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 9:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=221

狀態 新的

Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java 的第 109 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
行	111	111
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java

方法 <T extends CreateChargeInfoArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
111.  reader.readLine();
```

Improper Resource Access Authorization\路徑 10:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=222

狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java 的第 109 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
行	115	115
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
方法	<T extends CreateChargeInfoArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
115.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=223
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 的第 210 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	212	212
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	<T extends RecordsArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
212.  reader.readLine();
```

Improper Resource Access Authorization\路徑 12:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=224
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 的第 210 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	216	216
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	<T extends RecordsArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
216.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=225
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java 的第 313 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	315	315
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
315.  reader.readLine();
```

Improper Resource Access Authorization\路徑 14:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=226
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java 的第 313 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	318	318
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
318.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 15:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=227
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java 的第 153 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic

	e/exchangecheque/ExchangeUploadServiceIT.java	e/exchangecheque/ExchangeUploadServiceIT.java
行	155	155
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
155.  reader.readLine();
```

Improper Resource Access Authorization\路徑 16:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=228
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java 的第 153 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	158	158
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
158.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 17:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=229
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java 的第 110 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
行	112	112
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
方法	List<TmbRs> getCsvDate() throws Exception {

```
....
112.  reader.readLine();
```

Improper Resource Access Authorization\路徑 18:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=230
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java 的第 110 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
行	115	115
物件	readLine	readLine

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
方法	List<TmbRs> getCsvDate() throws Exception {

```
....
115.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 19:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=231
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 77 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	79	79
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getTimeDepForCustomer(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
79.  reader.readLine();
```

Improper Resource Access Authorization\路徑 20:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=232
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 77 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic

	e/tdb/OldTimeDepBillServiceIT.java	e/tdb/OldTimeDepBillServiceIT.java
行	80	80
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getTimeDepForCustomer(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
80.  reader.readLine();
```

Improper Resource Access Authorization\路徑 21:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=233
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 77 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	85	85
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getTimeDepForCustomer(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
85.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 22:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=234
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 118 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	120	120
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getTimeDepForAccount(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
120.  reader.readLine();
```

Improper Resource Access Authorization\路徑 23:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=235

狀態 新的

Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 118 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	121	121
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getTimeDepForAccount(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
121.  reader.readLine();
```

Improper Resource Access Authorization\路徑 24:

嚴重程度： 低風險

結果狀態： 校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=236
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 118 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	126	126
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getTimeDepForAccount(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
126.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 25:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=237
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 164 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	166	166
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getApplication(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
166.  reader.readLine();
```

Improper Resource Access Authorization\路徑 26:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=238
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 164 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	167	167
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getApplication(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
167.  reader.readLine();
```

Improper Resource Access Authorization\路徑 27:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=239
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 164 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	173	173
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getApplication(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
173.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 28:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=240
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 210 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	212	212
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getBaseInfo(String custId, String arrangementId, String accountId) throws Exception {

```
....
212.  reader.readLine();
```

Improper Resource Access Authorization\路徑 29:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=241
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 210 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic

	e/tdb/OldTimeDepBillServiceIT.java	e/tdb/OldTimeDepBillServiceIT.java
行	213	213
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getBaseInfo(String custId, String arrangementId, String accountId) throws Exception {

```
....
213.  reader.readLine();
```

Improper Resource Access Authorization\路徑 30:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=242
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 210 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	216	216
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getBaseInfo(String custId, String arrangementId, String accountId) throws Exception {

```
....
216.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 31:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=243
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	276	276
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
276.  readerTimeDep.readLine();
```

Improper Resource Access Authorization\路徑 32:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=244
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	277	277
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
277.  readerTimeDep.readLine();
```

Improper Resource Access Authorization\路徑 33:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=245
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	280	280
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
280.  while ((lineTimeDep = readerTimeDep.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 34:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=246
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	295	295
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
295.  readerInterestCalculation.readLine();
```

Improper Resource Access Authorization\路徑 35:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=247
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	296	296
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
296.  readerInterestCalculation.readLine();
```

Improper Resource Access Authorization\路徑 36:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=248
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	300	300
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
300.  while ((lineInterestCalculation =
readerInterestCalculation.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 37:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=249
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	311	311
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
311.  readerInterestPaid.readLine();
```

Improper Resource Access Authorization\路徑 38:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=250
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	312	312
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
312.  readerInterestPaid.readLine();
```

Improper Resource Access Authorization\路徑 39:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=251
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 274 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	318	318
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
318.  while ((lineInterestPaid = readerInterestPaid.readLine()) != null)
{
```

Improper Resource Access Authorization\路徑 40:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=252
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	387	387
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
387.   readerTimeDep.readLine();
```

Improper Resource Access Authorization\路徑 41:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=253
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	388	388
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
388.   readerTimeDep.readLine();
```

Improper Resource Access Authorization\路徑 42:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=254
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	391	391

物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
391.  while ((line = readerTimeDep.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 43:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=255
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	397	397
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
397.  regularSavings.readLine();
```

Improper Resource Access Authorization\路徑 44:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=256
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic	dep/dep-service/src/test/java/com/scsb/ncbs/dep/servic

	e/tdb/OldTimeDepBillServiceIT.java	e/tdb/OldTimeDepBillServiceIT.java
行	398	398
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
398.  regularSavings.readLine();
```

Improper Resource Access Authorization\路徑 45:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=257
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 385 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	402	402
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
402.  while ((lineRegularSavings = regularSavings.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 46:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=258
狀態 新的
Detection Date 12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 408 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	410	410
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getExchangeRate() throws IOException {

```
....
410.   reader.readLine();
```

Improper Resource Access Authorization\路徑 47:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=259
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 408 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	411	411
物件	readLine	readLine

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法 void getExchangeRate() throws IOException {

```
....
411.   reader.readLine();
```

Improper Resource Access Authorization\路徑 48:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=260
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java 的第 408 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	414	414
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getExchangeRate() throws IOException {

```
....
414.  while ((line = reader.readLine()) != null) {
```

Improper Resource Access Authorization\路徑 49:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=261
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java 的第 134 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java
行	136	136
物件	readLine	readLine

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java

方法 List<InterestAccrualsResponseBody> getInterestCalculationCsv(String path) throws Exception {

```
....
136.  reader.readLine();
```

Improper Resource Access Authorization\路徑 50:

嚴重程度：	低風險
結果狀態：	校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=262
狀態	新的
Detection Date	12/12/2024 10:17:56 AM

在檔案 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java 的第 134 行執行了 I/O 操作，卻沒有進行授權檢查。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java
行	137	137
物件	readLine	readLine

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/TimeDepBillServiceIT.java
方法	List<InterestAccrualsResponseBody> getInterestCalculationCsv(String path) throws Exception {

```
....
137.  reader.readLine();
```

Improper Exception Handling

查詢路徑:

Java\Cx\Java Low Visibility\Improper Exception Handling 版本:1

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Error processing
OWASP ASVS: V14 Configuration
OWASP Top 10 2021: A4-Insecure Design
ASD STIG 5.2: 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.

描述

Improper Exception Handling\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=135
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法testGenerate在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/report/CbrReportServiceIT.java第 26 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/report/CbrReportServiceIT.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/report/CbrReportServiceIT.java
行	33	33
物件	getResultList	getResultList

代碼片斷

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/report/CbrReportServiceIT.java

方法 void testGenerate() {

```
....
33.  rs.getContent().getResultList().forEach(r -> {
```

Improper Exception Handling\路徑 2:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=136

狀態 新的

Detection Date 12/12/2024 10:17:55 AM

方法compileData在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第162 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	220	220
物件	updateCbrDateByDataDateBetweenDates	updateCbrDateByDataDateBetweenDates

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 public ServiceRs<FileSummaryReadRs> compileData(@NotNull @Valid FileSummaryCompileDataArg arg) {

```
....
220.  dataModRepo.updateCbrDateByDataDateBetweenDates(nextCbrDate,
maxCompletedCbrDate, nextCbrDate);
```

Improper Exception Handling\路徑 3:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=137

狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法createFileA在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第480 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	483	483
物件	delByCbrFileMasterListId	delByCbrFileMasterListId

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 private List<Long> createFileA(@NotNull final Long cbrFileMasterListId, @NotNull @Valid List<CbrFileA> fileAs) {

```
....
483.  fileARepo.delByCbrFileMasterListId(cbrFileMasterListId);
```

Improper Exception Handling\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=138
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法deleteFileAByCbrDataModListId在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第1921 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	1937	1937
物件	delByCbrDataModListId	delByCbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 public void deleteFileAByCbrDataModListId(long cbrDataModListId) {

```
....
1937.  fileARepo.delByCbrDataModListId(cbrDataModListId);
```

Improper Exception Handling\路徑 5:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=139
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法createFileB在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第506 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	509	509
物件	delByCbrFileMasterListId	delByCbrFileMasterListId

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 private List<Long> createFileB(@NotNull final Long cbrFileMasterListId, @NotNull @Valid List<CbrFileB> fileBs) {

```
....
509.  fileBRepo.delByCbrFileMasterListId(cbrFileMasterListId);
```

Improper Exception Handling\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=140
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法deleteFileBByCbrDataModListId在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第1953 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	1969	1969
物件	delByCbrDataModListId	delByCbrDataModListId

代碼片斷

檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
方法	public void deleteFileBByCbrDataModListId(long cbrDataModListId) {

```
....
1969.  fileBRepo.delByCbrDataModListId(cbrDataModListId);
```

Improper Exception Handling\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=141
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法createFileF在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第532 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	535	535
物件	delByCbrFileMasterListId	delByCbrFileMasterListId

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
方法	private List<Long> createFileF(@NotNull final Long cbrFileMasterListId, @NotNull @Valid List<CbrFileF> fileFs) {

```
....
535.  fileFRepo.delByCbrFileMasterListId(cbrFileMasterListId);
```

Improper Exception Handling\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=142
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法deleteFileFByCbrDataModListId在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第1985 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/servi	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/servi

	ce/file/CbrFileService.java	ce/file/CbrFileService.java
行	2001	2001
物件	delByCbrDataModListId	delByCbrDataModListId

代碼片斷
檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
方法 public void deleteFileFByCbrDataModListId(long cbrDataModListId) {

```
....
2001.  fileFRepo.delByCbrDataModListId(cbrDataModListId);
```

Improper Exception Handling\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=143
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法createFileG在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第558 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	561	561
物件	delByCbrFileMasterListId	delByCbrFileMasterListId

代碼片斷
檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
方法 private List<Long> createFileG(@NotNull final Long cbrFileMasterListId, @NotNull @Valid List<CbrFileG> fileGs) {

```
....
561.  fileGRepo.delByCbrFileMasterListId(cbrFileMasterListId);
```

Improper Exception Handling\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=144
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法deleteFileGByCbrDataModListId在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第2017 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	2033	2033
物件	delByCbrDataModListId	delByCbrDataModListId

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 public void deleteFileGByCbrDataModListId(long cbrDataModListId) {

```
....
2033.   fileGRepo.delByCbrDataModListId(cbrDataModListId);
```

Improper Exception Handling\路徑 11:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=145

狀態 新的

Detection Date 12/12/2024 10:17:55 AM

方法createFileK在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java第584 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java
行	587	587
物件	delByCbrFileMasterListId	delByCbrFileMasterListId

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileService.java

方法 private List<Long> createFileK(@NotNull final Long cbrFileMasterListId, @NotNull @Valid List<CbrFileK> fileKs) {

```
....
587.   fileKRepo.delByCbrFileMasterListId(cbrFileMasterListId);
```

Improper Exception Handling\路徑 12:

嚴重程度： 低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=146
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法getMaxCompletedCbrDate在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileMasterService.java第105 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileMasterService.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileMasterService.java
行	109	109
物件	obtainMaxCbrDate	obtainMaxCbrDate

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/file/CbrFileMasterService.java
方法	public LocalDate getMaxCompletedCbrDate() {

```
....
109.  return masterRepo.obtainMaxCbrDate(statusCodes);
```

Improper Exception Handling\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=147
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readJson在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java第59 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
行	73	73
物件	obtainBusCalListByBusCurrencyIsNull	obtainBusCalListByBusCurrencyIsNull

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
方法	public ServiceRs<BdayProvReadJsonListRs> readJson(@Valid BdayProvReadArg arg) {

```
....
73.
busCalendarDto.addAll(busCalendarRepository.obtainBusCalListByBusCurrenc
yIsNull(busYear));
```

Improper Exception Handling\路徑 14:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=148
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readJson在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java第59 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
行	74	74
物件	obtainByMultipleConditionsGreaterThanBusYear	obtainByMultipleConditionsGreaterThanBusYear

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
方法	public ServiceRs<BdayProvReadJsonListRs> readJson(@Valid BdayProvReadArg arg) {

```
....
74.
busCalendarDto.addAll(busCalendarRepository.obtainByMultipleConditionsGr
eaterThanBusYear(busYear));
```

Improper Exception Handling\路徑 15:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=149
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readChar在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java第133 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-	cmn/cmn-

	service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java	service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
行	147	147
物件	obtainBusCalListByBusCurrencyIsNullChar	obtainBusCalListByBusCurrencyIsNullChar

代碼片斷
檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
方法 public ServiceRs<BdayProvReadCharListRs> readChar(@Valid BdayProvReadArg arg) {

```
....
147.
busCalendarDto.addAll(busCalendarRepository.obtainBusCalListByBusCurrencyIsNullChar(busYear));
```

Improper Exception Handling\路徑 16:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=150
狀態 新的
Detection Date 12/12/2024 10:17:55 AM

方法readChar在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java第133 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
行	149	149
物件	obtainByMultipleConditionsGreaterThanBusYearChar	obtainByMultipleConditionsGreaterThanBusYearChar

代碼片斷
檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/prov/BdayProvService.java
方法 public ServiceRs<BdayProvReadCharListRs> readChar(@Valid BdayProvReadArg arg) {

```
....
149.
busCalendarDto.addAll(busCalendarRepository.obtainByMultipleConditionsGreaterThanBusYearChar(busYear));
```

Improper Exception Handling\路徑 17:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=151

狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java第45 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java
行	59	59
物件	obtainEcifPukkiRelList	obtainEcifPukkiRelList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java
方法	public ServiceRs<EcifPukkiRelReadListRs> readList(@NotNull @Valid String custId) {

```
....
59.  entityList =
cmnEcifPukkiRelRepository.obtainEcifPukkiRelList(custId).stream()
```

Improper Exception Handling\路徑 18:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=152
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java第45 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java
行	66	66
物件	obtainEcifPukkiRelList	obtainEcifPukkiRelList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ecif/pukkirel/EcifPukkiRelService.java
方法	public ServiceRs<EcifPukkiRelReadListRs> readList(@NotNull @Valid String custId) {

```
....
66.  entityList =
cmnEcifPukkiRelRepository.obtainEcifPukkiRelList(newCustId).stream()
```

Improper Exception Handling\路徑 19:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=153
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法read在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java第69 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
行	80	80
物件	obtainIdocBrhReqDtlList	obtainIdocBrhReqDtlList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java

方法 public ServiceRs<IdocRequestRecordReadRs> read(@NotBlank @Valid String applyNo) {

```
....
80.  List<IdocRequestRecordListInfo> list =
cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlList(applyNo).stream()
```

Improper Exception Handling\路徑 20:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=154
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法.flatMap在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java第171 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地

檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
行	176	176
物件	obtainIdocBrhReqDtlList	obtainIdocBrhReqDtlList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java

方法 .flatMap(entity -> {

```
....
176.  return
cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlList(applyNo).stream()
```

Improper Exception Handling\路徑 21:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=155
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法.map在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java第326 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java
行	326	326
物件	obtainIdocBrhReqDtlInfo	obtainIdocBrhReqDtlInfo

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java

方法 .map(entity -> cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlInfo(queryParam2, entity.getApplyNo()))// Map Page<IdocBrhReqDtlInfoDto> to List<IdocBrhReqDtlInfoDto>

```
....
326.  .map(entity ->
cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlInfo(queryParam2,
entity.getApplyNo()))// Map Page<IdocBrhReqDtlInfoDto> to
List<IdocBrhReqDtlInfoDto>
```

Improper Exception Handling\路徑 22:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=156
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法.map在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java第448 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java
行	448	448
物件	obtainIdocBrhReqDtlBetDate	obtainIdocBrhReqDtlBetDate

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/inventory/IdocInventoryService.java
方法	.map(entity -> cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlBetDate(queryParam2, enqDateStart, finalEnqDateEnd, entity.getApplyNo()))

```
....
448.   .map(entity ->
cmnIdocBrhReqDtlRepository.obtainIdocBrhReqDtlBetDate(queryParam2,
enqDateStart, finalEnqDateEnd, entity.getApplyNo()))
```

Improper Exception Handling\路徑 23:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=157
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法.flatMap在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java第149 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
行	155	155

物件	obtainByFixedDateStr	obtainByFixedDateStr

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
方法	.flatMap(sts -> {

```
....
155.  partialList =
cmnIdocBrhReqRepository.obtainByFixedDateStr(queryParam,
applyDateStr).stream()
```

Improper Exception Handling\路徑 24:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=158
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法.flatMap在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java第149 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
行	159	159
物件	obtainBetweenByDateStrAndEnd	obtainBetweenByDateStrAndEnd

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/request/IdocRequestRecordService.java
方法	.flatMap(sts -> {

```
....
159.  partialList =
cmnIdocBrhReqRepository.obtainBetweenByDateStrAndEnd(queryParam,
applyDateStr, applyDateEnd).stream()
```

Improper Exception Handling\路徑 25:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=159
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java第178 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	190	190
物件	obtainIdocSpvOrderListInfo	obtainIdocSpvOrderListInfo

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
方法	public ServiceRs<IdocSpvOrderReadListRs> readList(@NotNull @Valid String enqSts) {

```
....
190.  entityPage =
cmnIdocSpvReqRepository.obtainIdocSpvOrderListInfo(getServiceInfo().getB
ranchCode()).stream().map(mapper::dtoToListRs).collect(Collectors.toList
());
```

Improper Exception Handling\路徑 26:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=160
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java第178 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	184	184
物件	obtainIdocSpvOrderListInfoInBranch	obtainIdocSpvOrderListInfoInBranch

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
方法	public ServiceRs<IdocSpvOrderReadListRs> readList(@NotNull @Valid String enqSts) {

```
....
184.  entityPage =
cmnIdocSpvReqRepository.obtainIdocSpvOrderListInfoInBranch().stream().ma
p(mapper::dtoToListRs).collect(Collectors.toList());
```

Improper Exception Handling\路徑 27:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=161
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java第178 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	192	192
物件	obtainIdocSpvOrderListInfoBySupplyDate	obtainIdocSpvOrderListInfoBySupplyDate

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java

方法 public ServiceRs<IdocSpvOrderReadListRs> readList(@NotNull @Valid String enqSts) {

```
....
192.  entityPage =
cmnIdocSpvReqRepository.obtainIdocSpvOrderListInfoBySupplyDate(getServic
eInfo().getBranchCode(),
spvSupplyDate).stream().map(mapper::dtoToListRs).collect(Collectors.toLi
st());
```

Improper Exception Handling\路徑 28:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=162
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java第178 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地

檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	186	186
物件	obtainIdocSpvOrderListInfoBySupplyDateInBranch	obtainIdocSpvOrderListInfoBySupplyDateInBranch

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java

方法 public ServiceRs<IdocSpvOrderReadListRs> readList(@NotNull @Valid String enqSts) {

```
....
186.  entityPage =
cmnIdocSpvReqRepository.obtainIdocSpvOrderListInfoBySupplyDateInBranch(s
pvSupplyDate).stream().map(mapper::dtoToListRs).collect(Collectors.toLis
t());
```

Improper Exception Handling\路徑 29:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=163
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法uploadBrhData在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java第156 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java
行	184	184
物件	delByNtfChar	delByNtfChar

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java

方法 public ServiceRs<NtfUploadBrhDataRs> uploadBrhData(@NotNull @Valid NtfUploadBrhDataArg arg) {

```
....
184.
cmnNtfBrhMailRepository.delByNtfChar(arg.getNtfChar().getContext());
```

Improper Exception Handling\路徑 30:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=164
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法valid在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/checker/NtfCustReadListChecker.java第31 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/checker/NtfCustReadListChecker.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/checker/NtfCustReadListChecker.java
行	36	36
物件	obtainNtfCustList	obtainNtfCustList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/checker/NtfCustReadListChecker.java

方法 public void valid(CheckerBean checkerBean, Object[] args) {

```
....
36.  List<NtfCustListInfo> dtos =
cmnNtfCustRepository.obtainNtfCustList(ntfButype, ntfCustid).stream()
```

Improper Exception Handling\路徑 31:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=165
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/NtfCustService.java第156 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/NtfCustService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/NtfCustService.java
行	159	159
物件	obtainNtfCustList	obtainNtfCustList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/cust/NtfCustService.java
方法	public ServiceRs<NtfCustListRs> readList(String ntfButype, @NotNull @Valid String ntfCustid) {

```
....
159.  List<NtfCustListInfo> dtos =
cmnNtfCustRepository.obtainNtfCustList(ntfButype, ntfCustid).stream()
```

Improper Exception Handling\路徑 32:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=166
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法valid在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/checker/NtfInternalGrpReadListChecker.java第32行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/checker/NtfInternalGrpReadListChecker.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/checker/NtfInternalGrpReadListChecker.java
行	36	36
物件	obtainNtfInternalGrpList	obtainNtfInternalGrpList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/checker/NtfInternalGrpReadListChecker.java
方法	public void valid(CheckerBean checkerBean, Object[] args) {

```
....
36.  List<NtfInternalGrpListInfo> infoList =
cmnNtfInternalGrpRepository.obtainNtfInternalGrpList(ntfSendGroup).strea
m()
```

Improper Exception Handling\路徑 33:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=167
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java第101 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java
行	103	103
物件	obtainNtfInternalGrpList	obtainNtfInternalGrpList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java

方法 public ServiceRs<NtfInternalGrpListRs> readList(@NotNull @Valid String ntfSendGroup) {

```
....
103.  List<NtfInternalGrpListInfo> infoList =
cmnNtfInternalGrpRepository.obtainNtfInternalGrpList(ntfSendGroup).strea
m()
```

Improper Exception Handling\路徑 34:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=168
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法valid在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/checker/NtfMessageReadListChecker.java第32行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/checker/NtfMessageReadListChecker.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/checker/NtfMessageReadListChecker.java
行	39	39
物件	obtainNtfMessageList	obtainNtfMessageList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/checker/NtfMessageReadListChecker.java

方法 public void valid(CheckerBean checkerBean, Object[] args) {

```
....
39.  List<NtfMessageListInfo> infoList =
cmnNtfMessageRepository.obtainNtfMessageList(ntfSendDateStart,
ntfSendDateEnd, ntfButype, ntfSendObj).stream().map(mapper::dtoToListRs)
```

Improper Exception Handling\路徑 35:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=169
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java第96 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java
行	98	98
物件	obtainNtfMessageList	obtainNtfMessageList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/message/NtfMessageService.java

方法 public ServiceRs<NtfMessageListRs> readList(@NotNull @Valid LocalDate ntfSendDateStart, @NotNull @Valid LocalDate ntfSendDateEnd, String ntfButype, String ntfSendObj) {

```
....
98.  List<NtfMessageListInfo> infoList =
cmnNtfMessageRepository.obtainNtfMessageList(ntfSendDateStart,
ntfSendDateEnd, ntfButype, ntfSendObj).stream().map(mapper::dtoToListRs)
```

Improper Exception Handling\路徑 36:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=170
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/NtfParmService.java第117 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地

檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/NtfParmService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/NtfParmService.java
行	119	119
物件	obtainNtfParmList	obtainNtfParmList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/NtfParmService.java

方法 public ServiceRs<NtfParmReadListRs> readList() {

```
....
119.  List<NtfParmReadListInfo> dtos =
cmnNtfParmRepository.obtainNtfParmList().stream()
```

Improper Exception Handling\路徑 37:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=171

狀態 新的

Detection Date 12/12/2024 10:17:55 AM

方法valid在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/checker/NtfParmReadListChecker.java第31 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/checker/NtfParmReadListChecker.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/checker/NtfParmReadListChecker.java
行	33	33
物件	obtainNtfParmList	obtainNtfParmList

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/parm/checker/NtfParmReadListChecker.java

方法 public void valid(CheckerBean checkerBean, Object[] args) {

```
....
33.  List<NtfParmReadListInfo> dtos =
cmnNtfParmRepository.obtainNtfParmList().stream()
```

Improper Exception Handling\路徑 38:

嚴重程度： 低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=172
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法readList在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/NtfTemplateService.java第116 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/NtfTemplateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/NtfTemplateService.java
行	118	118
物件	obtainNtfTemplateList	obtainNtfTemplateList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/NtfTemplateService.java
方法	public ServiceRs<NtfTemplateListRs> readList(@NotNull @Valid String ntfButype, String ntfMethod, String ntfTempcode) {

```
....
118.  List<NtfTemplateListInfo> infoList =
cmnNtfTemplateRepository.obtainNtfTemplateList(ntfButype, ntfMethod,
ntfTempcode).stream()
```

Improper Exception Handling\路徑 39:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=173
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法valid在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/checker/NtfTemplateReadListChecker.java第31 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/checker/NtfTemplateReadListChecker.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/checker/NtfTemplateReadListChecker.java
行	37	37
物件	obtainNtfTemplateList	obtainNtfTemplateList

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/template/checker/NtfTemplateReadListChecker.java
方法	public void valid(CheckerBean checkerBean, Object[] args) {

```
....
37.  List<NtfTemplateListInfo> infoList =
cmnNtfTemplateRepository.obtainNtfTemplateList(ntfButype, ntfMethod,
ntfTempcode).stream()
```

Improper Exception Handling\路徑 40:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=174
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法update在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java第96 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java
行	114	114
物件	delByBusiness	delByBusiness

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java
方法	public ServiceRs<EmptyRs> update(@NotNull @Valid BusinessFeeUpdateArg arg) {

```
....
114.  cmnPricBizFeeDtlRepository.delByBusiness(arg.getBusiness());
```

Improper Exception Handling\路徑 41:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=175
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法delete在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java第134 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java
行	146	146
物件	delByBusiness	delByBusiness

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/bizfee/BusinessFeeService.java

方法 public ServiceRs<EmptyRs> delete(@NotNull @Valid BusinessFeeDeleteArg arg) {

```
....
146.  cmnPricBizFeeDtlRepository.delByBusiness(arg.getBusiness());
```

Improper Exception Handling\路徑 42:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=176
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法update在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java第132 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java
行	150	150
物件	delByBusiness	delByBusiness

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java

方法 public ServiceRs<EmptyRs> update(@NotNull @Valid BusinessIntRateUpdateArg arg) {

```
....
150.  cmnPricBizIntRateDtlRepository.delByBusiness(business);
```

Improper Exception Handling\路徑 43:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=177
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法delete在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java第170 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java
行	182	182
物件	delByBusiness	delByBusiness

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/bizintrate/BusinessIntRateService.java
方法	public ServiceRs<EmptyRs> delete(@NotNull @Valid BusinessIntRateDeleteArg arg) {

```
....
182.  cmnPricBizIntRateDtlRepository.delByBusiness(business);
```

Improper Exception Handling\路徑 44:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=178
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法removeByCustIdnoAndAccountNoAndOfferBranch在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java第71 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java
行	76	76

物件	delByCustIdnoAndAccountNoAndOfferBranch	delByCustIdnoAndAccountNoAndOfferBranch

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java
方法	default void removeByCustIdnoAndAccountNoAndOfferBranch(String custIdno, String accountNo, String offerBranch){

```
....
76.  this.delByCustIdnoAndAccountNoAndOfferBranch(custIdno, accountNo,
offerBranch);
```

Improper Exception Handling\路徑 45:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=179
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法removeByCustIdnoAndAccountNoAndOfferBranch在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java第71行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java
行	74	74
物件	delByCustIdnoAndOfferBranchAndAccountNoIsNull	delByCustIdnoAndOfferBranchAndAccountNoIsNull

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/persistence/repository/pric/CmnPricCustFeeDtlRepository.java
方法	default void removeByCustIdnoAndAccountNoAndOfferBranch(String custIdno, String accountNo, String offerBranch){

```
....
74.  this.delByCustIdnoAndOfferBranchAndAccountNoIsNull(custIdno,
offerBranch);
```

Improper Exception Handling\路徑 46:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=180
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法update在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java第121行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java
行	142	142
物件	delByCustIdnoAndAccountNoAndOfferBr	delByCustIdnoAndAccountNoAndOfferBr

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java
方法	public ServiceRs<EmptyRs> update(@NotNull @Valid CustomerIntRateUpdateArg arg) {

```
....
142.
cmnPricCustIntRateDtlRepository.delByCustIdnoAndAccountNoAndOfferBr(custIdno, accountNo, offerBr);
```

Improper Exception Handling\路徑 47:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=181
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法delete在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java第162行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java
行	177	177

物件	delByCustIdnoAndAccountNoAndOfferBr	delByCustIdnoAndAccountNoAndOfferBr

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/intrate/custintrate/CustomerIntRateService.java
方法	public ServiceRs<EmptyRs> delete(@NotNull @Valid CustomerIntRateDeleteArg arg) {

```
....
177.
cmnPricCustIntRateDtlRepository.delByCustIdnoAndAccountNoAndOfferBr(custIdno, accountNo, offerBr);
```

Improper Exception Handling\路徑 48:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=182
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法update在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java第89 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java
行	106	106
物件	delByFeeOffer	delByFeeOffer

代碼片斷	
檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java
方法	public ServiceRs<EmptyRs> update(@NotNull @Valid FeeProjectUpdateArg arg) {

```
....
106.  cmnPricFeeProjDtlRepository.delByFeeOffer(arg.getFeeOffer());
```

Improper Exception Handling\路徑 49:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=183
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法delete在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java第126 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java
行	138	138
物件	delByFeeOffer	delByFeeOffer

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeproj/FeeProjectService.java

方法 public ServiceRs<EmptyRs> delete(@NotNull @Valid FeeProjectDeleteArg arg) {

```
....
138.  cmnPricFeeProjDtlRepository.delByFeeOffer(arg.getFeeOffer());
```

Improper Exception Handling\路徑 50:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=184
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

方法update在cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeprojrel/FeeProjectRelateService.java第95 行執行可預期拋出異常的操作，但未正確包裹在try-catch區塊中。這構成不當異常處理(Improper Exception Handling)。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeprojrel/FeeProjectRelateService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeprojrel/FeeProjectRelateService.java
行	106	106
物件	delByBusiness	delByBusiness

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/pric/fee/feeprojrel/FeeProjectRelateService.java

方法 public ServiceRs<EmptyRs> update(@NotNull @Valid FeeProjectRelateUpdateArg arg) {

```
....
106.  cmnPricFeeProjRelRepository.delByBusiness(arg.getBusiness());
```

Information Exposure Through an Error Message

查詢路徑:

Java\Cx\Java Low Visibility\Information Exposure Through an Error Message 版本:5

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
OWASP Top 10 2013: A5-Security Misconfiguration
FISMA 2014: Configuration Management
NIST SP 800-53: SI-11 Error Handling (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 API: API3-Excessive Data Exposure
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Error processing
OWASP ASVS: V14 Configuration
OWASP Top 10 2021: A4-Insecure Design
SANS top 25: SANS top 25
ASD STIG 5.2: 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.

描述

Information Exposure Through an Error Message\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=320
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java 第 29 行的 rLock 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java rLock 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java
行	43	44
物件	e	printStackTrace

代碼片斷	
檔案名稱	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java
方法	public void rLock() {

```
....
43.  } catch (Throwable e) {
44.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=321
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java 第 64 行的 Thread 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java Thread 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java
行	69	70
物件	e	printStackTrace

代碼片斷	
檔案名稱	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java
方法	Thread aThread = new Thread(() -> {

```
....
69.  } catch (Throwable e) {
70.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=322
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java 第 67 行的 filePaths.forEach 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java filePaths.forEach 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/Rece	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/Rece

	ivePersonalDeletionIT.java	ivePersonalDeletionIT.java
行	70	71
物件	e	printStackTrace

代碼片斷
檔案名稱 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java
方法 filePaths.forEach(filePath -> {

```
....
70.  } catch (IOException e) {
71.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 4:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=323
狀態 新的
Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java 第 75 行的 filePaths.forEach 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java filePaths.forEach 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java
行	78	79
物件	e	printStackTrace

代碼片斷
檔案名稱 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java
方法 filePaths.forEach(filePath -> {

```
....
78.  } catch (IOException e) {
79.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=324
狀態 新的
Detection Date 12/12/2024 10:17:58 AM

在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java 第 74 行的 Thread 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java Thread 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java
行	79	80
物件	e	printStackTrace

代碼片斷

檔案名稱 rds/rds-service/src/test/java/com/scsb/ncbs/rds/service/RedisRepositoryIntegrationTest.java

方法 Thread bThread = new Thread(() -> {

```
....
79.  } catch (Throwable e) {
80.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=325
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java 第 76 行的 filePaths.forEach 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java filePaths.forEach 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java
行	79	80
物件	e	printStackTrace

代碼片斷

檔案名稱 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java

方法 filePaths.forEach(filePath -> {

```
....
79.  } catch (IOException e) {
80.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=326
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/TellerTxnServiceIT.java 第 105 行的 getBcoTellerTxnDetails 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/TellerTxnServiceIT.java getBcoTellerTxnDetails 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/TellerTxnServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/TellerTxnServiceIT.java
行	114	115
物件	e	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/TellerTxnServiceIT.java

方法 private List<BcoTellerTxnDetailRs> getBcoTellerTxnDetails() {

```
....
114.  } catch (IOException e) {
115.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=327
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/NextDayChequeServiceIT.java 第 112 行的 getBcoNextDayChequeDetails 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/NextDayChequeServiceIT.java getBcoNextDayChequeDetails 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/NextDayChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/NextDayChequeServiceIT.java
行	121	122
物件	e	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/NextDayChequeServiceIT.java
方法	private BcoNextDayChequeRs getBcoNextDayChequeDetails(BcoNextDayChequeRq rq) {

```
....
121.  } catch (IOException e) {
122.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=328
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/DishonoredActServiceIT.java 第 132 行的 getT24DishonoredActRs 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/DishonoredActServiceIT.java getT24DishonoredActRs 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/DishonoredActServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/DishonoredActServiceIT.java
行	141	142
物件	e	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/DishonoredActServiceIT.java
方法	private T24DishonoredActRs getT24DishonoredActRs(String fileName) {

```
....
141.  } catch (IOException e) {
142.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=329
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/VirtualAccountTxnServiceIT.java 第 140 行的 getT24VirtualAccountByCASA 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-

service/src/test/java/com/scsb/ncbs/dep/service/txndata/VirtualAccountTxnServiceIT.java getT24VirtualAccountByCASA 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/VirtualAccountTxnServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/VirtualAccountTxnServiceIT.java
行	149	150
物件	e	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/txndata/VirtualAccountTxnServiceIT.java

方法 private VirtualAccountLogRs getT24VirtualAccountByCASA() {

```
....
149.  } catch (IOException e) {
150.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=330
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java 第 163 行的 getAccountCompany 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java getAccountCompany 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java
行	169	170
物件	e	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java

方法 public static String getAccountCompany(String accountNo) {

```
....
169.  catch (Exception e) {
170.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 12:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=331
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/creditcard/CcPaymentServiceIT.java 第 211 行的 getBcoPayments 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/creditcard/CcPaymentServiceIT.java getBcoPayments 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/creditcard/CcPaymentServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/creditcard/CcPaymentServiceIT.java
行	220	221
物件	e	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/creditcard/CcPaymentServiceIT.java

方法 private BcoCcPaymentRs getBcoPayments() {

```
....
220.  } catch (IOException e) {
221.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=332
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/StopPaymentServiceIT.java 第 234 行的 getT24StopPayment 方法處理了例外或執行錯誤 e。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/StopPaymentServiceIT.java getT24StopPayment 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/StopPaymentServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/StopPaymentServiceIT.java
行	243	244
物件	e	printStackTrace

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/chequedep/StopPaymentServiceIT.java
方法	private T24StopPaymentRs getT24StopPayment(String fileName) {

```
....
243.  } catch (IOException e) {
244.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 14:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=333
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 54 行的 testCreate 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreate 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	64	65
物件	Exception	printStackTrace

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	void testCreate() throws Exception {

```
....
64.  e = assertThrows(Exception.class, () ->
service.createReserve(argList.get(0)));
65.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 15:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=334
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java 第 61 行的 testRead 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java testRead 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java
行	65	66
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java

方法 void testRead() {

```
....
65.  e = assertThrows(Exception.class, () ->
service.readProof("12345678901234"));
66.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 16:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=335

狀態 新的

Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java 第 60 行的 testReadChequeReport 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java testReadChequeReport 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
行	67	68
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java

方法 void testReadChequeReport() {

```
....
67.  e = assertThrows(Exception.class, () ->
service.readChequeReport("2", MidDateUtils.stringToLocalDate("20240321",
MidDateUtils.YYYYMMDD)));
68.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 17:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=336
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 54 行的 testCreate 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreate 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	69	70
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testCreate() throws Exception {

```
....
69.  e = assertThrows(Exception.class, () ->
service.createReserve(argList.get(1)));
70.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 18:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=337
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 54 行的 testCreate 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreate 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	74	75
物件	Exception	printStackTrace

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	void testCreate() throws Exception {

```
....
74.  e = assertThrows(Exception.class, () ->
service.createReserve(argList.get(2)));
75.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 19:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=338
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	75	76
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	void testCreateCheque() throws Exception {

```
....
75.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(0)));
76.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 20:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=339
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java 第 59 行的 testCreateCharge 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java testCreateCharge 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
行	75	76
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java

方法 void testCreateCharge() throws Exception {

```
....
75.  Throwable e = assertThrows(Exception.class, () ->
service.createCharge(arg));
76.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 21:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=340

狀態 新的

Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java 第 65 行的 testRead 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java testRead 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
行	76	77
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java

方法 void testRead() throws Exception {

```
....
76.  e = assertThrows(Exception.class, () ->
service.read(createHealthArg(2, "12345678901234", "", "20240101",
"20240330")));
77.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 22:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=341
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 54 行的 testCreate 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreate 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	80	81
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testCreate() throws Exception {

```
....
80.  e = assertThrows(Exception.class, () ->
service.createReserve(argList.get(3)));
81.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 23:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=342
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地

檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	83	84
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法 void testCreateCheque() throws Exception {

```
....
83.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(0)));
84.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 24:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=343
狀態 新的
Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java 第 82 行的 testReadChargeStatus 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java testReadChargeStatus 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
行	85	86
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
方法 void testReadChargeStatus() {

```
....
85.  Throwable e = assertThrows(Exception.class, () ->
service.readChargeStatus(arg));
86.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 25:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=344
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java 第 83 行的 testProcessPrint 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java testProcessPrint 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java
行	87	88
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/obu/ObuTermServiceIT.java
方法	void testProcessPrint() throws Throwable {

```
....
87.  e = assertThrows(Exception.class, () ->
service.readProof("12345678901234"));
88.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 26:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=345
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	89	90
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	void testCreateCheque() throws Exception {

```
....
89.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(1)));
90.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 27:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=346
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java 第 84 行的 testPrintChequeReport 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java testPrintChequeReport 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
行	94	95
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java

方法 void testPrintChequeReport() throws Throwable {

```
....
94.  e = assertThrows(Exception.class, () ->
service.printChequeReport("2",
MidDateUtils.stringToLocalDate("20240321", MidDateUtils.YYYYMMDD)));
95.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 28:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=347
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地

檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	97	98
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法 void testCreateCheque() throws Exception {

```
....
97.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(1)));
98.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 29:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=348
狀態 新的
Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 90 行的 testRead 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testRead 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	100	101
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 void testRead() throws Exception {

```
....
100.  e = assertThrows(Exception.class, () ->
service.readReserve(argList.get(0).getChequeAccountNumber(),
argList.get(0).getChequeNumber()));
101.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 30:

嚴重程度： 低風險
結果狀態： 校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=349
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	105	106
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java

方法 void testCreateCheque() throws Exception {

```
....
105.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(2)));
106.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 31:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=350
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java 第 86 行的 testPrint 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java testPrint 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
行	105	106
物件	Exception	printStackTrace

代碼片斷

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
方法	void testPrint() throws Throwable {

```
....
105.  e = assertThrows(Exception.class, () ->
service.print(createHealthArg(2, "12345678901234", "TWD", "20240101",
"20240330")));
106.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 32:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=351
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	114	115
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	void testCreateCheque() throws Exception {

```
....
114.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(3)));
115.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 33:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=352
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 109 行的 testDelete 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-

service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testDelete 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	120	121
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testDelete() throws Exception {

```
....
120.  e = assertThrows(Exception.class, () ->
service.deleteReserve(argList.get(4)));
121.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 34:

嚴重程度： 低風險

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=353

狀態 新的

Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	122	123
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java

方法 void testCreateCheque() throws Exception {

```
....
122.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(2)));
123.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 35:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=354
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 109 行的 testDelete 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testDelete 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	128	129
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	void testDelete() throws Exception {

```
....
128.  e = assertThrows(Exception.class, () ->
service.deleteReserve(argList.get(4)));
129.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 36:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=355
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 70 行的 testCreateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testCreateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	133	134
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法	void testCreateCheque() throws Exception {

```
....
133.  e = assertThrows(Exception.class, () ->
service.createRecords(argList.get(3)));
134.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 37:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=356
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java 第 115 行的 testRecordedFile 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java testRecordedFile 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
行	133	134
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
方法	void testRecordedFile() {

```
....
133.  e = assertThrows(Exception.class, () -> service.recordedFile());
134.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 38:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=357
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 135 行的 testUpdateReserve 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testUpdateReserve 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	149	150
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 void testUpdateReserve() throws Exception {

```
....
149.  e = assertThrows(Exception.class, () ->
service.updateReserve(argList.get(0)));
150.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 39:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=358
狀態 新的
Detection Date 12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java 第 140 行的 testReopen 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java testReopen 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
行	153	154
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrReportServiceIT.java
方法 void testReopen() {

```
....
153.  e = assertThrows(Exception.class, () -> service.reopen());
154.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 40:

嚴重程度： 低風險
結果狀態： 校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=359
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 135 行的 testUpdateReserve 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testUpdateReserve 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	156	157
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	void testUpdateReserve() throws Exception {

```
....
156.  e = assertThrows(Exception.class, () ->
service.updateReserve(argList.get(0)));
157.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 41:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=360
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 147 行的 testUpdateCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testUpdateCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	158	159
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java

方法	void testUpdateCheque() throws Exception {

```
....
158.  e = assertThrows(Exception.class, () ->
service.updateRecords(argList.get(3)));
159.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 42:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=361
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 135 行的 testUpdateReserve 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testUpdateReserve 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	161	162
物件	Exception	printStackTrace

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	void testUpdateReserve() throws Exception {

```
....
161.  e = assertThrows(Exception.class, () ->
service.updateReserve(argList.get(1)));
162.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 43:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=362
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 135 行的 testUpdateReserve 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testUpdateReserve 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地

檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	169	170
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 void testUpdateReserve() throws Exception {

```
....
169.  e = assertThrows(Exception.class, () ->
service.updateReserve(argList.get(2)));
170.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 44:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=363
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java 第 175 行的 testDeleteCheque 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java testDeleteCheque 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	180	181
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
方法 void testDeleteCheque() throws Exception {

```
....
180.  e = assertThrows(Exception.class, () ->
service.deleteRecords(argList.get(3)));
181.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 45:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=364
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 176 行的 testCreateRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreateRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	187	188
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testCreateRemarkForRedemption() throws Exception {

```
....
187.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(0)));
188.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 46:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=365
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 176 行的 testCreateRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreateRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	193	194
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testCreateRemarkForRedemption() throws Exception {

```
....
193.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(0)));
194.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 47:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=366
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 176 行的 testCreateRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreateRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	198	199
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testCreateRemarkForRedemption() throws Exception {

```
....
198.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(1)));
199.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 48:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=367
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 176 行的 testCreateRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreateRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地

檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	203	204
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 void testCreateRemarkForRedemption() throws Exception {

```
....
203.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(2)));
204.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 49:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=368
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 176 行的 testCreateRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testCreateRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	211	212
物件	Exception	printStackTrace

代碼片斷
檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法 void testCreateRemarkForRedemption() throws Exception {

```
....
211.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(3)));
212.  e.printStackTrace();
```

Information Exposure Through an Error Message\路徑 50:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=369
狀態	新的
Detection Date	12/12/2024 10:17:58 AM

在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java 第 220 行的 testDeleteRemarkForRedemption 方法處理了例外或執行錯誤 Exception。 在例外處理期間，應用程式在 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java testDeleteRemarkForRedemption 方法中將例外詳細資訊 printStackTrace 揭露。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	231	232
物件	Exception	printStackTrace

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法 void testDeleteRemarkForRedemption() throws Exception {

```
....
231.  e = assertThrows(Exception.class, () ->
service.processRemark(argList.get(5)));
232.  e.printStackTrace();
```

Stored Log Forging

查詢路徑:

Java\Cx\Java Low Visibility\Stored Log Forging 版本:5

類別

FISMA 2014: System And Information Integrity
NIST SP 800-53: AU-9 Protection of Audit Information (P1)
OWASP Top 10 2017: A1-Injection
OWASP ASVS: V07 Error Handling and Logging
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

描述

Stored Log Forging\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=425
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java的38行的process方法，從元素result中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-

service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java中38行的process方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java
行	53	54
物件	result	info

代碼片斷
檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java
方法 public ServiceRs<String> process(OdchOrderTxnDeleteArg arg) throws Throwable {

```
....
53.  ServiceRs<String> result = activity.delete(arg,
odchOpenTimeReadRs);
54.  ApLogger.getLogger().info("delete service reuslt: {}", result);
```

Stored Log Forging\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=426
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java的57行的update方法，從元素svcRs中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java中57行的update方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java
行	60	61
物件	svcRs	info

代碼片斷
檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java
方法 void update() {

```
....
60.  ServiceRs<BranchCbrDataModUpdateRs> svcRs =
branchCbrDataModService.update(arg);
61.  log.info("svcRs={}", svcRs);
```

Stored Log Forging\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=427
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java的80行的readDistinctReceiveBankSwiftCodeByCurrency方法，從元素list中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java中80行的readDistinctReceiveBankSwiftCodeByCurrency方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java
行	81	82
物件	list	info

代碼片斷	
檔案名稱	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java
方法	void readDistinctReceiveBankSwiftCodeByCurrency() {

```
....
81.  List<String> list =
repository.readDistinctReceiveBankSwiftCodeByCurrency("JPY");
82.  log.info("list:{}", list);
```

Stored Log Forging\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=428
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java的80行的readDistinctReceiveBankSwiftCodeByCurrency方法，從元素list1中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java中80行的readDistinctReceiveBankSwiftCodeByCurrency方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java
行	84	85
物件	list1	info

代碼片斷
檔案名稱 rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/currdenom/OdchCurrDenomServiceIT.java
方法 void readDistinctReceiveBankSwiftCodeByCurrency() {

```
....
84.  List<String> list1 =
repository.readDistinctReceiveBankSwiftCodeByCurrency("CNY");
85.  log.info("list1:{}", list1);
```

Stored Log Forging\路徑 5:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=429
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/opentime/OdchOpenTimeServiceIT.java的140行的delete方法，從元素readResponse中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/opentime/OdchOpenTimeServiceIT.java中140行的delete方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/opentime/OdchOpenTimeServiceIT.java	rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/opentime/OdchOpenTimeServiceIT.java
行	143	146

物件	readResponse	info

代碼片斷

檔案名稱 rems/rems-service/src/test/java/com/scsb/ncbs/rems/service/odch/opentime/OdchOpenTimeServiceIT.java

方法 void delete() {

```
....
143.  ServiceRs<String> readResponse = odchOpenTimeService.delete(arg);
....
146.  log.info("response :{}", rs);
```

Stored Log Forging\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=430
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkService.java的62行的readBySwiftCodeCurrency方法，從元素obtainBySwiftCodeCurrency中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkServiceIT.java中44行的delete方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkService.java	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkServiceIT.java
行	63	54
物件	obtainBySwiftCodeCurrency	info

代碼片斷

檔案名稱 remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkService.java

方法 public ServiceRs<OdchReceiveBkRs> readBySwiftCodeCurrency(String swiftCode, String currency) {

```
....
63.  RemOdchReceiveBkInfoDto remReceiveBkInfoDto =
remOdchReceiveBkInfoRepository.obtainBySwiftCodeCurrency(swiftCode,
currency).orElse(null);
```

檔案名稱	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/receivebk/OdchReceiveBkServiceIT.java
方法	void delete() {

```
....
54.  log.info("delete remReceiveBkInfoId={} ",
receiveBkRs.getRemReceiveBkInfoId());
```

Stored Log Forging\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=431
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java的45行的loadDbDataFromFile方法，從元素readFileToString中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java中45行的loadDbDataFromFile方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java
行	48	60
物件	readFileToString	info

代碼片斷

檔案名稱	len/len-app/src/test/java/com/scsb/ncbs/len/service/TestDbService.java
方法	private void loadDbDataFromFile(DataSource ds, String file) throws Exception {

```
....
48.  String sqlList = FileUtils.readFileToString(resource.getFile(),
"UTF-8");
....
60.  log.info("sql:{}", sql);
```

Stored Log Forging\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=432
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java的61行的readRejected方法，從元素rejectedDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java中44行的readRejected方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java
行	68	49
物件	rejectedDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java

方法 public ServiceRs<BranchCbrDataModReadRejectedRs> readRejected(@NotNull @Valid BranchCbrDataModReadRejectedArg arg) {

```
....
68.  List<CbrDataModRejectedDto> rejectedDtoList =
dataModRepo.obtainCbrDataModRejected(arg.getBank(), rejectDate,
rejectStatus);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java

方法 void readRejected() {

```
....
49.  log.info("svcRs={}", svcRs);
```

Stored Log Forging\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=433
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteService.java的103行的read方法，從元素readByBeneficiaryStartingWith中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteServiceIT.java中79行的assertDoesNotThrow方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteService.java	rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteServiceIT.java
行	105	81
物件	readByBeneficiaryStartingWith	info

代碼片斷

檔案名稱 rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteService.java

方法 public ServiceRs<LcAdvisingCustNoteReadRs> read(@NotNull @Valid LcAdvisingCustNoteReadArg arg) {

```
....
105.  List<LcAdvisingCustNote> datas =
advisingCustNoteRepository.readByBeneficiaryStartingWith(arg.getBenefici
ary())
```

檔案名稱 rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/tfsf/lcadvisingcustnote/LcAdvisingCustNoteServiceIT.java

方法 assertDoesNotThrow(() -> {

```
....
81.  log.info("查詢結果： {}", svrRs.getContent());
```

Stored Log Forging\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=434
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的127行的readRejected方法，從元素rejectedDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中57行的readRejected方法中用於寫入稽核日誌。

這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

行	133	65
物件	rejectedDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java

方法 public ServiceRs<CbrDataInquiryReadRejectedRs> readRejected(@NotNull @Valid CbrDataInquiryReadRejectedArg arg) {

```
....
133.  List<CbrDataModRejectedDto> rejectedDtoList =
dataModRepo.obtainCbrDataModRejected(bank, arg.getRejectDate(),
rejectStatus);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 void readRejected() {

```
....
65.  log.info("svcRs={}", svcRs);
```

Stored Log Forging\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=435
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的153行的readError方法，從元素checkDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中72行的readError方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	160	80
物件	checkDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java

方法 public ServiceRs<CbrDataInquiryReadErrorRs> readError(@NotNull @Valid CbrDataInquiryReadErrorArg arg) {

```
....
160.  List<CbrDataModErrorDto> checkDtoList =
dataModRepo.obtainCbrDataModError(dataChannel, jobCode,
arg.getCbrDate(), checkStatusList);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 void readError() {

```
....
80.  log.info("rs={}", rs);
```

Stored Log Forging\路徑 12:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=436
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的179行的readDeclaration方法，從元素declarationDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中92行的readDeclaration方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	191	100
物件	declarationDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java

方法 public ServiceRs<CbrDataInquiryReadDeclarationRs> readDeclaration(@NotNull @Valid CbrDataInquiryReadDeclarationArg arg) {

```
....
191.  List<CbrDataModDeclarationDto> declarationDtoList =
dataModRepo.obtainCbrDataModDeclaration(dataChannel, jobCode,
arg.getCbrDate());
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 void readDeclaration() {

```
....
100.  log.info("rs={}", rs);
```

Stored Log Forging\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=437
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/rbid/specialexrate/RbidSpecialExRateService.java的83行的read方法，從元素dtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/rbid/specialexrate/readSpecialExRateServiceIT.java中25行的testReadSpecialExRate方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/rbid/specialexrate/RbidSpecialExRateService.java	rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/rbid/specialexrate/readSpecialExRateServiceIT.java
行	89	30
物件	dtoList	info

代碼片斷

檔案名稱 rem/rem-service/src/main/java/com/scsb/ncbs/rem/service/rbid/specialexrate/RbidSpecialExRateService.java

方法 public ServiceRs<SpecialExRateRs> read(@NotNull @Valid RbidReadSpecialExRateArg arg) {

```
....
89.  List<RbidReadSpecialExRateDto> dtoList =
remRbidSpecialExRateRepository.readProvisioningServerInfo(queryDate,
rateType, baseCurrency);
```

檔案名稱 rem/rem-service/src/test/java/com/scsb/ncbs/rem/service/rbid/specialexrate/readSpecialExRateServiceIT.java

方法 void testReadSpecialExRate() {

```
....
30.  log.info(String.valueOf(rs));
```

Stored Log Forging\路徑 14:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=438
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java的55行的insert方法，從元素readLines中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java中62行的lines.forEach方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java
行	58	81
物件	readLines	info

代碼片斷	
檔案名稱	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java
方法	void insert() throws IOException {

```
....
58.  List<String> lines = MidFileUtils.readLines(file);
```

檔案名稱	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java
方法	lines.forEach(l -> {

```
....
81.  log.info("code=[{}]", entity);
```

Stored Log Forging\路徑 15:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=439
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java的61行的readRejected方法，從元素rejectedDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java中51行的svcRs.getContent方法中用於寫入稽核日誌。

這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java
行	68	52
物件	rejectedDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModService.java

方法 public ServiceRs<BranchCbrDataModReadRejectedRs> readRejected(@NotNull @Valid BranchCbrDataModReadRejectedArg arg) {

```
....
68.  List<CbrDataModRejectedDto> rejectedDtoList =
dataModRepo.obtainCbrDataModRejected(arg.getBank(), rejectDate,
rejectStatus);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/branch/BranchCbrDataModServiceIT.java

方法 svcRs.getContent().getDatas().forEach(d -> {

```
....
52.  log.info("rejectedData={}", d);
```

Stored Log Forging\路徑 16:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=440
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的153行的readError方法，從元素checkDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中82行的rs.getContent方法中用於寫入稽核日誌。

這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	160	83
物件	checkDtoList	info

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java
方法	public ServiceRs<CbrDataInquiryReadErrorRs> readError(@NotNull @Valid CbrDataInquiryReadErrorArg arg) {

```
....
160.  List<CbrDataModErrorDto> checkDtoList =
dataModRepo.obtainCbrDataModError(dataChannel, jobCode,
arg.getCbrDate(), checkStatusList);
```

檔案名稱	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
方法	rs.getContent().getDatas().forEach(checkData -> {

```
....
83.  log.info("checkData={}", checkData);
```

Stored Log Forging\路徑 17:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=441
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的179行的readDeclaration方法，從元素declarationDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中102行的rs.getContent方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	191	103
物件	declarationDtoList	info

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java
方法	public ServiceRs<CbrDataInquiryReadDeclarationRs> readDeclaration(@NotNull @Valid CbrDataInquiryReadDeclarationArg arg) {

```
....
191.  List<CbrDataModDeclarationDto> declarationDtoList =
dataModRepo.obtainCbrDataModDeclaration(dataChannel, jobCode,
arg.getCbrDate());
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 rs.getContent().getDatas().forEach(declarationData -> {

```
....
103.  log.info("declarationData={}", declarationData);
```

Stored Log Forging\路徑 18:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=442
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的127行的readRejected方法，從元素rejectedDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中66行的svcRs.getContent方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	133	67
物件	rejectedDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java

方法 public ServiceRs<CbrDataInquiryReadRejectedRs> readRejected(@NotNull @Valid CbrDataInquiryReadRejectedArg arg) {

```
....
133.  List<CbrDataModRejectedDto> rejectedDtoList =
dataModRepo.obtainCbrDataModRejected(bank, arg.getRejectDate(),
rejectStatus);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 svcRs.getContent().getDatas().forEach(data -> {

```
....
67.  log.info("ListId={}, DataNo={}, RejectStatus={}, RejectDate={},
Reason={}", data.getCbrDataModListId(), data.getDataNo(),
data.getRejectStatus(), data.getRejectDate(), data.getReason());
```

Stored Log Forging\路徑 19:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=443
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java的153行的readError方法，從元素checkDtoList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java中84行的checkData.getErrorMessages方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java	cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java
行	160	85
物件	checkDtoList	info

代碼片斷

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryService.java

方法 public ServiceRs<CbrDataInquiryReadErrorRs> readError(@NotNull @Valid CbrDataInquiryReadErrorArg arg) {

```
....
160.  List<CbrDataModErrorDto> checkDtoList =
dataModRepo.obtainCbrDataModError(dataChannel, jobCode,
arg.getCbrDate(), checkStatusList);
```

檔案名稱 cbr/cbr-service/src/test/java/com/scsb/ncbs/cbr/service/data/CbrDataInquiryServiceIT.java

方法 checkData.getErrorMessages().forEach(errorMessage -> {

```
....
85.  log.info("Code={}, Message={}", errorMessage.getCode(),
errorMessage.getMessage());
```

Stored Log Forging\路徑 20:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=444
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java的98行的.map方法，從元素obtainBySumBranchCode中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java中51行的readBySumBranchCode方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
行	98	57
物件	obtainBySumBranchCode	info

代碼片斷

檔案名稱 remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java

方法 .map(branchCode -> remOdchGroupRepository.obtainBySumBranchCode(branchCode).orElse(null))

```
....
98.   .map(branchCode ->
remOdchGroupRepository.obtainBySumBranchCode(branchCode).orElse(null))
```

檔案名稱 remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java

方法 void readBySumBranchCode() {

```
....
57.   log.info("Sum Branch List:{}", rs.getSumBranchList());
```

Stored Log Forging\路徑 21:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=445
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java的90行的readBySumBranchCode方法，從元素allSumBranchCodeList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java中51行的readBySumBranchCode方法中用於寫入稽核日誌。

這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
行	93	57
物件	allSumBranchCodeList	info

代碼片斷

檔案名稱 remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java

方法 public ServiceRs<OdchGroupReadListRs> readBySumBranchCode(String sumBranchCode) {

```
....
93.  List<RemOdchSumBranchCodeReadDto> allSumBranchCodeList =
remOdchGroupRepository.readDistinctSumBranchCode();
```

檔案名稱 remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java

方法 void readBySumBranchCode() {

```
....
57.  log.info("Sum Branch List:{}", rs.getSumBranchList());
```

Stored Log Forging\路徑 22:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=446
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java的98行的.map方法，從元素obtainBySumBranchCode中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java中60行的applyBranchList.stream方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
行	98	60
物件	obtainBySumBranchCode	info

代碼片斷	
檔案名稱	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java
方法	.map(branchCode -> remOdchGroupRepository.obtainBySumBranchCode(branchCode).orElse(null))

```
....
98.   .map(branchCode ->
remOdchGroupRepository.obtainBySumBranchCode(branchCode).orElse(null))
```

檔案名稱	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
方法	applyBranchList.stream().forEach(applyBranch -> log.info("Apply Branch:{}", applyBranch));

```
....
60.   applyBranchList.stream().forEach(applyBranch -> log.info("Apply
Branch:{}", applyBranch));
```

Stored Log Forging\路徑 23:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=447
狀態	新的
Detection Date	12/12/2024 10:18:17 AM

位於remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java的90行的readBySumBranchCode方法，從元素allSumBranchCodeList中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java中60行的applyBranchList.stream方法中用於寫入稽核日誌。
這可能會導致儲存型稽核日誌偽造攻擊(Stored Log Forging)。

	來源	目的地
檔案	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
行	93	60
物件	allSumBranchCodeList	info

代碼片斷	
檔案名稱	remb/remb-service/src/main/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupService.java
方法	public ServiceRs<OdchGroupReadListRs> readBySumBranchCode(String sumBranchCode) {

```
....
93.  List<RemOdchSumBranchCodeReadDto> allSumBranchCodeList =
remOdchGroupRepository.readDistinctSumBranchCode();
```

檔案名稱	remb/remb-service/src/test/java/com/scsb/ncbs/remb/service/odch/group/OdchGroupServiceIT.java
方法	applyBranchList.stream().forEach(applyBranch -> log.info("Apply Branch:{}", applyBranch));

```
....
60.  applyBranchList.stream().forEach(applyBranch -> log.info("Apply
Branch:{}", applyBranch));
```

Incorrect Permission Assignment For Critical Resources

查詢路徑:

Java\Cx\Java Low Visibility\Incorrect Permission Assignment For Critical Resources 版本:6

類別

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A6-Security Misconfiguration
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V04 Access Control
OWASP Top 10 2021: A4-Insecure Design
SANS top 25: SANS top 25

描述

Incorrect Permission Assignment For Critical Resources\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=378
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java 第 17 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java
行	17	17
物件	path	path

代碼片斷

檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/cmn/CmnBdayNextApiClient.java
方法	@MidApiClient(application = "cmn", name = "cmnBdayNextApi", path = "bday/bdayNext")

```
....
17.  @MidApiClient(application = "cmn", name = "cmnBdayNextApi", path =
"bday/bdayNext")
```

Incorrect Permission Assignment For Critical Resources\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=379
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java 第 17 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java
行	17	17
物件	path	path

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/client/rem/RemExchangeRateApiClient.java
方法	@MidApiClient(application = "rem", name = "remExchangeRateApi", path = "specialexrate")

```
....
17.  @MidApiClient(application = "rem", name = "remExchangeRateApi",
path = "specialexrate")
```

Incorrect Permission Assignment For Critical Resources\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=380
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/cmn/BdayNearApi.java 第 18 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	dep/dep-	dep/dep-

	service/src/main/java/com/scsb/ncbs/dep/service/mid/cmn/BdayNearApi.java	service/src/main/java/com/scsb/ncbs/dep/service/mid/cmn/BdayNearApi.java
行	18	18
物件	path	path

代碼片斷
檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/cmn/BdayNearApi.java
方法 @MidApiClient(application = "cmn", name = "BdayNearApi", path = "bday/bdayNear")

```
....
18.  @MidApiClient(application = "cmn", name = "BdayNearApi", path =
"bday/bdayNear")
```

Incorrect Permission Assignment For Critical Resources\路徑 4:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=381
狀態 新的
Detection Date 12/12/2024 10:17:59 AM

檔案系統中由 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/rem/RbidSpecialExRateApi.java 第 15 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/rem/RbidSpecialExRateApi.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/rem/RbidSpecialExRateApi.java
行	15	15
物件	path	path

代碼片斷
檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/mid/rem/RbidSpecialExRateApi.java
方法 @MidApiClient(application = "rem", name = "RbidSpecialExRateApi", path = "specialexrate")

```
....
15.  @MidApiClient(application = "rem", name = "RbidSpecialExRateApi",
path = "specialexrate")
```

Incorrect Permission Assignment For Critical Resources\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=382
狀態 新的
Detection Date 12/12/2024 10:17:59 AM

檔案系統中由 len/len-service/src/main/java/com/scsb/ncbs/len/service/api/RbidSpecialExRateApi.java 第 13 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/service/api/RbidSpecialExRateApi.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/api/RbidSpecialExRateApi.java
行	13	13
物件	path	path

代碼片斷

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/service/api/RbidSpecialExRateApi.java

方法 @MidApiClient(application = "rem", name = "RbidSpecialExRateApi", path = "specialexrate")

```
....
13.  @MidApiClient(application = "rem", name = "RbidSpecialExRateApi",
path = "specialexrate")
```

Incorrect Permission Assignment For Critical Resources\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=383
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCommissionRateApi.java 第 21 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCommissionRateApi.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCommissionRateApi.java
行	21	21
物件	path	path

代碼片斷

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCommissionRateApi.java

方法 @MidApiClient(application = "rems", name = "RemOdchCommissionRateApi", path = "odchCommissionRate")

```
....
21.  @MidApiClient(application = "rems", name =
"RemOdchCommissionRateApi", path = "odchCommissionRate")
```

Incorrect Permission Assignment For Critical Resources\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=384
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCurrDenomApi.java 第 15 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCurrDenomApi.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCurrDenomApi.java
行	15	15
物件	path	path

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchCurrDenomApi.java
方法	@MidApiClient(application = "rems", name = "RemOdchOdchCurrDenomApi", path = "odchcurrdenom")

```
....
15.  @MidApiClient(application = "rems", name =
"RemOdchOdchCurrDenomApi", path = "odchcurrdenom")
```

Incorrect Permission Assignment For Critical Resources\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=385
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOpenTimeApi.java 第 19 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOpenTimeApi.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOpenTimeApi.java
行	19	19
物件	path	path

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOpenTimeApi.java

方法	@MidApiClient(application = "rems", name = "RemOdchOpenTimeApi", path = "odchOpenTime")

```
....
19.  @MidApiClient(application = "rems", name = "RemOdchOpenTimeApi",
path = "odchOpenTime")
```

Incorrect Permission Assignment For Critical Resources\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=386
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOrderGroupApi.java 第 15 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOrderGroupApi.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOrderGroupApi.java
行	15	15
物件	path	path

代碼片斷	
檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchOrderGroupApi.java
方法	@MidApiClient(application = "remb", name = "RemOdchOrderGroupApi", path = "odchOrderGroup")

```
....
15.  @MidApiClient(application = "remb", name = "RemOdchOrderGroupApi",
path = "odchOrderGroup")
```

Incorrect Permission Assignment For Critical Resources\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=387
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchSellBackOpenTimeApi.java 第 22 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	remm/remm-service/src/main/java/com/scsb/ncbs/remm/ap	remm/remm-service/src/main/java/com/scsb/ncbs/remm/ap

	i/RemOdchSellBackOpenTimeApi.java	i/RemOdchSellBackOpenTimeApi.java
行	22	22
物件	path	path

代碼片斷

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/api/RemOdchSellBackOpenTimeApi.java

方法 @MidApiClient(application = "rems", name = "RemOdchSellBackOpenTimeApi", path = "odchSellBackOpenTime")

```
....
22.  @MidApiClient(application = "rems", name =
"RemOdchSellBackOpenTimeApi", path = "odchSellBackOpenTime")
```

Incorrect Permission Assignment For Critical Resources\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=388
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 rems/rems-service/src/main/java/com/scsb/ncbs/rems/api/RemOdchReceiveBkInfoApi.java 第 17 行的 path 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	rems/rems-service/src/main/java/com/scsb/ncbs/rems/api/RemOdchReceiveBkInfoApi.java	rems/rems-service/src/main/java/com/scsb/ncbs/rems/api/RemOdchReceiveBkInfoApi.java
行	17	17
物件	path	path

代碼片斷

檔案名稱 rems/rems-service/src/main/java/com/scsb/ncbs/rems/api/RemOdchReceiveBkInfoApi.java

方法 @MidApiClient(application = "remb", name = "RemOdchReceiveBkInfoApi", path = "odchReceiveBk")

```
....
17.  @MidApiClient(application = "remb", name =
"RemOdchReceiveBkInfoApi", path = "odchReceiveBk")
```

Incorrect Permission Assignment For Critical Resources\路徑 12:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=389
狀態	新的

Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java 第 228 行的 file 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
行	233	233
物件	file	file

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java

方法 private void sendRequest(String request) {

```
....
233.  File file = new File(filePath);
```

Incorrect Permission Assignment For Critical Resources\路徑 13:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=390
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java 第 146 行的 file 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java
行	151	151
物件	file	file

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java

方法 private void sendRequest(String request) {

```
....
151.  File file = new File(filePath);
```

Incorrect Permission Assignment For Critical Resources\路徑 14:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=391
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java 第 134 行的 file 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
行	135	135
物件	file	file

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
方法	private void writeToOutputFile(String header, List<String> bodyList, String tailer) {

```
....
135.  File file = new File("output.txt");
```

Incorrect Permission Assignment For Critical Resources\路徑 15:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=392
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java 第 55 行的 file 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java
行	56	56
物件	file	file

代碼片斷	
檔案名稱	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnBranchRepositoryIT.java
方法	void insert() throws IOException {

```
....
56.  File file =
ResourceUtils.getFile("classpath:com/scsb/ncbs/rds/cache/branch.csv");
```

Incorrect Permission Assignment For Critical Resources\路徑 16:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=393
狀態	新的
Detection Date	12/12/2024 10:17:59 AM

檔案系統中由 rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnCurrencyRepositoryIT.java 第 44 行的 file 建立一個具有潛在危險權限的檔案。

	來源	目的地
檔案	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnCurrencyRepositoryIT.java	rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnCurrencyRepositoryIT.java
行	45	45
物件	file	file

代碼片斷

檔案名稱 rds/rds-service/src/test/java/com/scsb/ncbs/rds/cache/CmnCurrencyRepositoryIT.java

方法 void insert() throws IOException {

```
....
45.  File file =
ResourceUtils.getFile("classpath:com/scsb/ncbs/rds/cache/currency.csv");
```

Log Forging

查詢路徑:

Java\Cx\Java Low Visibility\Log Forging 版本:4

類別

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
OWASP Mobile Top 10 2016: M7-Client Code Quality
OWASP ASVS: V07 Error Handling and Logging
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
ASA Mobile Premium: ASA Mobile Premium
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.

描述

Log Forging\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=401
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java的57行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnCreateWorkflowImpl.java中41行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnCreateWorkflowImpl.java
行	57	51
物件	apiRequest	info

代碼片斷

檔案名稱 remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java

方法 public ApiResponse<ServiceRs<Long>> create(@RequestBody ApiRequest<ServiceRq<OdchOrderTxnCreateRq>> apiRequest) throws Throwable {

```
....
57.  public ApiResponse<ServiceRs<Long>> create(@RequestBody
ApiRequest<ServiceRq<OdchOrderTxnCreateRq>> apiRequest) throws Throwable
{
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnCreateWorkflowImpl.java

方法 public ServiceRs<Long> process(OdchOrderTxnCreateArg arg) throws Throwable {

```
....
51.  ApLogger.getLogger().info("read open time result: {}",
opentimeEntities);
```

Log Forging\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=402
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java的112行的delete方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java中38行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java
行	112	47
物件	apiRequest	info

代碼片斷

檔案名稱 remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java

方法 public ApiResponse<ServiceRs<String>> delete(@RequestBody ApiRequest<ServiceRq<OdchOrderTxnDeleteRq>> apiRequest) throws Throwable {

```
....
112.  public ApiResponse<ServiceRs<String>> delete(@RequestBody
ApiRequest<ServiceRq<OdchOrderTxnDeleteRq>> apiRequest) throws Throwable
{
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnDeleteWorkflowImpl.java

方法 public ServiceRs<String> process(OdchOrderTxnDeleteArg arg) throws Throwable {

```
....
47.  ApLogger.getLogger().info("read open time result: {}",
odchOpenTimeReadRs);
```

Log Forging\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=403
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java的52行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java中39行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
行	52	59
物件	apiRequest	info

代碼片斷

檔案名稱 remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java

方法 public ApiResponse<ServiceRs<OdchSumtxnCreateRs>> create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>> apiRequest) throws Throwable {

```
....
52.  public ApiResponse<ServiceRs<OdchSumtxnCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>>
apiRequest) throws Throwable {
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java

方法 public ServiceRs<OdchSumtxnCreateRs> process(OdchSumTxnCreateArg arg) throws Throwable {

```
....
59.  ApLogger.getLogger().info("creating service result: {}", result);
```

Log Forging\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=404
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java的53行的read方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-

service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java中45行的read方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java
行	53	47
物件	apiRequest	debug

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>> apiRequest) {

```
....
53.  public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>>
apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java

方法 public ServiceRs<BranchCoreCbrDataReadRs> read(@NotNull @Valid BranchCoreCbrDataReadArg readArg) {

```
....
47.  log.debug("readArg={}", readArg);
```

Log Forging\路徑 5:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=405
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java的52行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java中39行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-	remm/remm-

	app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java	service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
行	52	49
物件	apiRequest	info

代碼片斷

檔案名稱 remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java

方法 public ApiResponse<ServiceRs<OdchSumtxnCreateRs>> create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>> apiRequest) throws Throwable {

```
....
52.  public ApiResponse<ServiceRs<OdchSumtxnCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>>
apiRequest) throws Throwable {
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java

方法 public ServiceRs<OdchSumtxnCreateRs> process(OdchSumTxnCreateArg arg) throws Throwable {

```
....
49.  ApLogger.getLogger().info("read group result: {}",
groupReadListRs);
```

Log Forging\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=406
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java的66行的update方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java中65行的update方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java
行	66	67

物件	apiRequest	debug

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {

```
....
66.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {
```

檔案名稱 cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/branch/BranchCoreCbrDataService.java

方法 public ServiceRs<EmptyRs> update(@NotNull @Valid BranchCoreCbrDataUpdateArg updateArg) {

```
....
67.  log.debug("updateArg={}", updateArg);
```

Log Forging\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=407
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java的52行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java中39行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
行	52	71
物件	apiRequest	info

代碼片斷

檔案名稱 remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java

方法	public ApiResponse<ServiceRs<OdchSumtxnCreateRs>> create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>> apiRequest) throws Throwable {

```
....
52.  public ApiResponse<ServiceRs<OdchSumtxnCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>>
apiRequest) throws Throwable {
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
方法	public ServiceRs<OdchSumtxnCreateRs> process(OdchSumTxnCreateArg arg) throws Throwable {

```
....
71.  ApLogger.getLogger().info("creating service call t24 error result:
{}", result);
```

Log Forging\路徑 8:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=408
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java的52行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java中39行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
行	52	61
物件	apiRequest	error

代碼片斷	
檔案名稱	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/sumtxn/OdchSumTxnController.java
方法	public ApiResponse<ServiceRs<OdchSumtxnCreateRs>> create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>> apiRequest) throws Throwable {

```
....
52.  public ApiResponse<ServiceRs<OdchSumtxnCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<OdchSumTxnCreateRq>>
apiRequest) throws Throwable {
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/sumtxn/workflow/impl/OdchSumTxnCreateWorkflowImpl.java
方法	public ServiceRs<OdchSumtxnCreateRs> process(OdchSumTxnCreateArg arg) throws Throwable {

```
....
61.  ApLogger.getLogger().error("creating service error, result: {}
========> {}", result, e);
```

Log Forging\路徑 9:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=409
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java的49行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java中46行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java
行	49	66
物件	apiRequest	info

代碼片斷

檔案名稱	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java
方法	public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws Throwable {

```
....
49.  public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody
ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws
Throwable {
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java
方法	public ServiceRs<List<Long>> process(OdchSettleTxnCreateArg arg) throws Throwable {

```
....
66.  ApLogger.getLogger().info("creating service call t24 error result:
{}", result);
```

Log Forging\路徑 10:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=410
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java的49行的create方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java中46行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java
行	49	55
物件	apiRequest	info

代碼片斷	
檔案名稱	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/settletxn/OdchSettleTxnController.java
方法	public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws Throwable {

```
....
49.  public ApiResponse<ServiceRs<List<Long>>> create(@RequestBody
ApiRequest<ServiceRq<OdchSettleTxnCreateRq>> apiRequest) throws
Throwable {
```

檔案名稱	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/settletxn/workflow/impl/OdchSettleTxnCreateWorkflowImpl.java
方法	public ServiceRs<List<Long>> process(OdchSettleTxnCreateArg arg) throws Throwable {

```
....
55.  ApLogger.getLogger().info("creating service result: {}", result);
```

Log Forging\路徑 11:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=411
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

位於remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java的90行的update方法，從元素apiRequest中獲取了使用者輸入。該元素的值在程式碼中未經適當的消毒或驗證即被傳遞，最終在remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnUpdateWorkflowImpl.java中42行的process方法中用於寫入稽核日誌。
這可能會導致稽核日誌偽造攻擊(Log Forging)。

	來源	目的地
檔案	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java	remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnUpdateWorkflowImpl.java
行	90	51
物件	apiRequest	info

代碼片斷

檔案名稱	remm/remm-app/src/main/java/com/scsb/ncbs/remm/controller/odch/ordertxn/OdchOrderTxnController.java
方法	public ApiResponse<ServiceRs<String>> update(@RequestBody ApiRequest<ServiceRq<OdchOrderTxnUpdateRq>> apiRequest) throws Throwable {

```
....
90.  public ApiResponse<ServiceRs<String>> update(@RequestBody
ApiRequest<ServiceRq<OdchOrderTxnUpdateRq>> apiRequest) throws Throwable
{
```

檔案名稱 remm/remm-service/src/main/java/com/scsb/ncbs/remm/orchestration/odch/ordertxn/workflow/impl/OdchOrderTxnUpdateWorkflowImpl.java

方法 public ServiceRs<String> process(OdchOrderTxnUpdateArg arg) throws Throwable {

```
....
51.  ApLogger.getLogger().info("read open time result: {}",
opentimeEntities);
```

Integer Overflow

查詢路徑:

Java\Cx\Java Low Visibility\Integer Overflow 版本:2

類別

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Mobile Top 10 2016: M7-Client Code Quality
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
SANS top 25: SANS top 25
ASD STIG 5.2: APSC-DV-002590 - CAT I The application must not be vulnerable to overflow attacks.

描述

Integer Overflow\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=394
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java中的第 48行 apiRequest 的值被使用在 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java中的第 101行 parsedYear算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java
行	48	104

物件	apiRequest	parsedYear

代碼片斷	
檔案名稱	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java
方法	public ApiResponse<ServiceRs<PrintWithholdingRs>> print(@RequestBody ApiRequest<ServiceRq<PrintWithholdingRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<PrintWithholdingRs>>
print(@RequestBody ApiRequest<ServiceRq<PrintWithholdingRq>> apiRequest)
{
```

檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java
方法	public ServiceRs<PrintWithholdingRs> print(WithholdingArg withholdingArg) {

```
....
104.  int parsedYear =
MidNumberUtils.parseInteger(withholdingArg.getInterestPaymentYear()) +
1911;
```

Integer Overflow\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=395
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java中的第 52行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java中的第 115行 idocSerial2算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	52	129
物件	apiRequest	idocSerial2

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java
方法	public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<IdocSpvOrderUpdateRq>> apiRequest) {

```
....
52.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<IdocSpvOrderUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java

方法 public void update(@Valid @NotNull IdocSpvOrderUpdateArg arg) {

```
....
129.  int idocSerial2 = parseInteger(idocSerial) +
parseInteger(arg.getSpvActualQty()) - 1; // 計算保管品迄碼
```

Integer Overflow\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=396
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java中的第 45行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java中的第 196行 startDayIndex算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
行	45	219
物件	apiRequest	startDayIndex

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java

方法	private int calculateBusinessDays(int busYear, String busCurr, String busCount, String brhCode, LocalDate startDate, LocalDate endDate) {

```
....
219.  int startDayIndex = 31 * (startDate.getMonthValue() - 1) +
startDate.getDayOfMonth() - 1;
```

Integer Overflow\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=397
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java中的第 114行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java
行	36	138
物件	apiRequest	nextBusinessDay

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java
方法	public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java
方法	private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
138.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Overflow\路徑 5:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=398
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java中的第 115行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java
行	36	135
物件	apiRequest	nextBusinessDay

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java

方法 public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java

方法 private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
135.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Overflow\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=399
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java中的第 115行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java
行	36	148
物件	apiRequest	nextBusinessDay

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java

方法 public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java

方法 private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
148.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Overflow\路徑 7:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=400
狀態	新的
Detection Date	12/12/2024 10:18:04 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java中的第 45行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java中的第 149行 businessDaysCount算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
行	45	169
物件	apiRequest	businessDaysCount

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
方法	public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
方法	public ServiceRs<BdayInfoBusDaysBetweenReadRs> readBusDaysBetween(@NotNull @Valid BdayInfoBusDaysBetweenReadArg arg) {

```
....
169.  int businessDaysCount = businessDaysCountStart +
businessDaysCountEnd;
```

Integer Underflow

查詢路徑:

Java\Cx\Java Low Visibility\Integer Underflow 版本:2

類別

OWASP Mobile Top 10 2016: M7-Client Code Quality
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
SANS top 25: SANS top 25

描述

Integer Underflow\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=412
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java中的第 48行 apiRequest 的值被使用在 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java中的第 101行 parsedYear算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java
行	48	104

物件	apiRequest	parsedYear

代碼片斷

檔案名稱 dep/dep-app/src/main/java/com/scsb/ncbs/dep/controller/witholding/WithholdingController.java

方法 public ApiResponse<ServiceRs<PrintWithholdingRs>> print(@RequestBody ApiRequest<ServiceRq<PrintWithholdingRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<PrintWithholdingRs>>
print(@RequestBody ApiRequest<ServiceRq<PrintWithholdingRq>> apiRequest)
{
```

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/withholding/WithholdingService.java

方法 public ServiceRs<PrintWithholdingRs> print(WithholdingArg withholdingArg) {

```
....
104.  int parsedYear =
MidNumberUtils.parseInteger(withholdingArg.getInterestPaymentYear()) +
1911;
```

Integer Underflow\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=413
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java中的第 52行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java中的第 115行 idocSerial2算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java
行	52	129
物件	apiRequest	idocSerial2

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/idoc/spvorder/IdocSpvOrderController.java

方法 public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<IdocSpvOrderUpdateRq>> apiRequest) {

```
....
52.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<IdocSpvOrderUpdateRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/idoc/spvorder/IdocSpvOrderService.java

方法 public void update(@Valid @NotNull IdocSpvOrderUpdateArg arg) {

```
....
129.  int idocSerial2 = parseInteger(idocSerial) +
parseInteger(arg.getSpvActualQty()) - 1; // 計算保管品迄碼
```

Integer Underflow\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=414
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java中的第 45行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java中的第 196行 startDayIndex算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
行	45	219
物件	apiRequest	startDayIndex

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java

方法	private int calculateBusinessDays(int busYear, String busCurr, String busCount, String brhCode, LocalDate startDate, LocalDate endDate) {

```
....
219.  int startDayIndex = 31 * (startDate.getMonthValue() - 1) +
startDate.getDayOfMonth() - 1;
```

Integer Underflow\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=415
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java中的第 114行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java
行	36	138
物件	apiRequest	nextBusinessDay

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java
方法	public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/near/BdayNearService.java
方法	private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
138.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Underflow\路徑 5:

嚴重程度：	低風險

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=416
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java中的第 115行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java
行	36	135
物件	apiRequest	nextBusinessDay

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java

方法 public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java

方法 private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
135.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Underflow\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=417
狀態	新的
Detection Date	12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java中的第 36行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java中的第 115行 nextBusinessDay算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java
行	36	148
物件	apiRequest	nextBusinessDay

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java

方法 public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/next/BdayNextService.java

方法 private String findNearestBusinessDay(String formatDate, CalendarDataObj calendarData, String busCurr, String busCount) {

```
....
148.  int nextBusinessDay = IntStream.range(day + 1,
getDay.lengthOfMonth() + 1)
```

Integer Underflow\路徑 7:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=418
狀態 新的
Detection Date 12/12/2024 10:18:06 AM

在 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java中的第 45行 apiRequest 的值被使用在 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java中的第 149行 businessDaysCount算數運算沒有經過驗證，可能會導致算術溢出（俗稱 作為"整數溢出"）。

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
行	45	169
物件	apiRequest	businessDaysCount

代碼片斷

檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
方法	public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
方法	public ServiceRs<BdayInfoBusDaysBetweenReadRs> readBusDaysBetween(@NotNull @Valid BdayInfoBusDaysBetweenReadArg arg) {

```
....
169.  int businessDaysCount = businessDaysCountStart +
businessDaysCountEnd;
```

Heap Inspection

查詢路徑:

Java\Cx\Java Low Visibility\Heap Inspection 版本:8

類別

OWASP Top 10 2013: A6-Sensitive Data Exposure
OWASP ASVS: V08 Data Protection
OWASP Top 10 2021: A2-Cryptographic Failures
ASA Premium: ASA Premium
ASD STIG 5.2: 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.

描述

Heap Inspection\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=129
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java第58行的create方法定義了 psw1，其中包含user passwords。雖然plaintext passwords 稍後assign給psw1，但該值永遠不會從memory中清除。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java
行	70	70

物件	psw1	psw1

代碼片斷
檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java
方法 public ServiceRs<NtfOtpCreateRs> create(@NotNull @Valid NtfOtpCreateArg arg) {

```
....
70.  String psw1 = OtpUtils.generateOTP(6);
```

Heap Inspection\路徑 2:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=130
狀態 新的
Detection Date 12/12/2024 10:17:55 AM

cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java第58行的create方法定義了 psw2，其中包含user passwords。雖然plaintext passwords 稍後assign給psw2，但該值永遠不會從memory中清除。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java
行	71	71
物件	psw2	psw2

代碼片斷
檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpService.java
方法 public ServiceRs<NtfOtpCreateRs> create(@NotNull @Valid NtfOtpCreateArg arg) {

```
....
71.  String psw2 = OtpUtils.generateDigitOTP(6);
```

Heap Inspection\路徑 3:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=131
狀態 新的
Detection Date 12/12/2024 10:17:55 AM

len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java第50行的eftPwd;方法定義了 eftPwd，其中包含user passwords。雖然plaintext passwords 稍後assign給eftPwd，但該值永遠不會從memory中清除。

	來源	目的地

檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	50	50
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java

方法 private String eftPwd;

```
....
50.  private String eftPwd;
```

Heap Inspection\路徑 4:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=132
狀態 新的
Detection Date 12/12/2024 10:17:55 AM

len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java第50行的 eftPwd;方法定義了 eftPwd，其中包含user passwords。雖然plaintext passwords 稍後assign給eftPwd，但該值永遠不會從memory中清除。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	50	50
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java

方法 private String eftPwd;

```
....
50.  private String eftPwd;
```

Heap Inspection\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=133
狀態 新的

Detection Date	12/12/2024 10:17:55 AM

len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java第57行的 eftPwd;方法定義了 eftPwd，其中包含user passwords。雖然plaintext passwords 稍後assign給eftPwd，但該值永遠不會從memory中清除。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	57	57
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private String eftPwd;

```
....
57.  private String eftPwd;
```

Heap Inspection\路徑 6:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=134
狀態	新的
Detection Date	12/12/2024 10:17:55 AM

len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java第64行的 eftPwd;方法定義了 eftPwd，其中包含user passwords。雖然plaintext passwords 稍後assign給eftPwd，但該值永遠不會從memory中清除。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	64	64
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java

方法 private String eftPwd;

```
....
64.  private String eftPwd;
```

Spring Use Of Hardcoded Password

查詢路徑:

Java\Cx\Java Spring\Spring Use Of Hardcoded Password 版本:3

類別

CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V02 Authentication
OWASP Top 10 2021: A7-Identification and Authentication Failures
SANS top 25: SANS top 25

描述

Spring Use Of Hardcoded Password\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=988
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

應用程式使用寫死的密碼 eftPwd 來進行身分驗證或存取其他遠端系統。len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java 第 50 行的密碼出現在程式碼中，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	50	50
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java

方法 private String eftPwd;

```
....
50.  private String eftPwd;
```

Spring Use Of Hardcoded Password\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=989
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

應用程式使用寫死的密碼 eftPwd 來進行身分驗證或存取其他遠端系統。len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java 第 50 行的密碼出現在程式碼中，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	50	50
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java

方法 private String eftPwd;

```
....
50.  private String eftPwd;
```

Spring Use Of Hardcoded Password\路徑 3:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=990
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

應用程式使用寫死的密碼 eftPwd 來進行身分驗證或存取其他遠端系統。len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java 第 57 行的密碼出現在程式碼中，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	57	57
物件	eftPwd	eftPwd

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private String eftPwd;

```
....
57.  private String eftPwd;
```

Spring Use Of Hardcoded Password\路徑 4:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=991
狀態	新的
Detection Date	12/12/2024 10:18:29 AM

應用程式使用寫死的密碼 eftPwd 來進行身分驗證或存取其他遠端系統。len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java 第 64 行的密碼出現在程式碼中，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	64	64
物件	eftPwd	eftPwd

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
方法	private String eftPwd;

```
....
64.  private String eftPwd;
```

Portability Flaw Locale Dependent Comparison

查詢路徑:

Java\Cx\Java Low Visibility\Portability Flaw Locale Dependent Comparison 版本:3

描述

Portability Flaw Locale Dependent Comparison\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=419
狀態	新的
Detection Date	12/12/2024 10:18:11 AM

應用程式在處理字串時未指定特定語系。特別是在文件cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java中的第513行的getDateFromDateString方法呼叫toLowerCase時。這個字串經處理後的結果與文件cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java中的第560行的updateHolidaysAndBizdaysForDate方法的contains進行比較。

	來源	目的地
檔案	cmn/cmn-	cmn/cmn-

	service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java	service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
行	514	568
物件	toLowerCase	contains

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java

方法 private static int getDateFromDateString(String date) {

```
....
514.  return parseInteger(date.substring(2, 4).toLowerCase());
```

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java

方法 private void updateHolidaysAndBizdaysForDate(CalendarDataObj.MonthData monthData, int date, String status) {

```
....
568.  if (!bizdays.contains(date)) {
```

Portability Flaw Locale Dependent Comparison\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=420
狀態	新的
Detection Date	12/12/2024 10:18:11 AM

應用程式在處理字串時未指定特定語系。特別是在文件cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java中的第513行的getDateFromDateString方法呼叫toLowerCase時。這個字串經處理後的結果與文件cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java中的第560行的updateHolidaysAndBizdaysForDate方法的contains進行比較。

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
行	514	573
物件	toLowerCase	contains

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java

方法 private static int getDateFromDateString(String date) {

```
....
514.  return parseInteger(date.substring(2, 4).toLowerCase());
```

檔案名稱	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/init/BdayInitService.java
方法	private void updateHolidaysAndBizdaysForDate(CalendarDataObj.MonthData monthData, int date, String status) {

```
....
573.  if (!holidays.contains(date)) {
```

Race Condition Format Flaw

查詢路徑:

Java\Cx\Java Low Visibility\Race Condition Format Flaw 版本:5

類別

FISMA 2014: System And Information Integrity
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A5-Broken Access Control
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Time and status
OWASP ASVS: V01 Architecture, Design and Threat Modeling
OWASP Top 10 2021: A4-Insecure Design
ASD STIG 5.2: APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.

描述

Race Condition Format Flaw\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=421
狀態	新的
Detection Date	12/12/2024 10:18:16 AM

cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/sequence/CbrDataNoGenerator.java 文件中的 generateSeqValue 方法利用了 format，該方法被其他並行功能以非thread-safe的方式訪問，這可能會導致此資源的資源競爭。

	來源	目的地
檔案	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/sequence/CbrDataNoGenerator.java	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/sequence/CbrDataNoGenerator.java
行	70	70
物件	format	format

代碼片斷	
檔案名稱	cbr/cbr-service/src/main/java/com/scsb/ncbs/cbr/service/sequence/CbrDataNoGenerator.java
方法	public String generateSeqValue(SeqContext context, SeqConfig config) {

```
....
70.  String seqNo = seqNoFormat.format(context.getSeqNo());
```

Race Condition Format Flaw\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=422
狀態	新的
Detection Date	12/12/2024 10:18:16 AM

dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/common/enums/EnumsIT.java 文件中的 enum_DEP00253 方法利用了 format，該方法被其他並行功能以非thread-safe的方式訪問，這可能會導致此資源的資源競爭。

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/common/enums/EnumsIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/common/enums/EnumsIT.java
行	37	37
物件	format	format

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/common/enums/EnumsIT.java

方法 void enum_DEP00253(){

```
....
37.  String message = MessageFormat.format(CodeEnum.DEP00253.getDesc(),
"客戶ID", "帳號");
```

Serializable Class Containing Sensitive Data

查詢路徑:

Java\Cx\Java Low Visibility\Serializable Class Containing Sensitive Data 版本:4

類別

OWASP Top 10 2013: A6-Sensitive Data Exposure
OWASP Top 10 2017: A3-Sensitive Data Exposure
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V09 Communication
OWASP Top 10 2021: A4-Insecure Design

描述

Serializable Class Containing Sensitive Data\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=423
狀態	新的

Detection Date	12/12/2024 10:18:16 AM

敏感資訊的欄位 pendingCredit 在 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java 的第 109 行，被插入到可序列化物件 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java 的第 19 行中的 LenLoanDetailEntity 欄位。

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java	len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java
行	109	19
物件	pendingCredit	LenLoanDetailEntity

代碼片斷

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java

方法 private BigDecimal pendingCredit;

```
....
109.  private BigDecimal pendingCredit;
```

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenLoanDetailEntity.java

方法 @Data

```
....
19.  @Data
```

Serializable Class Containing Sensitive Data\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=424
狀態	新的
Detection Date	12/12/2024 10:18:16 AM

敏感資訊的欄位 accountNo 在 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java 的第 37 行，被插入到可序列化物件 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java 的第 19 行中的 LenBillsEntity 欄位。

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java	len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java

行	37	19
物件	accountNo	LenBillsEntity

代碼片斷

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java

方法 private String accountNo;

```
....
37.  private String accountNo;
```

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/persistence/entity/t24/LenBillsEntity.java

方法 @Data

```
....
19.  @Data
```

Use Of Hardcoded Password

查詢路徑:

Java\Cx\Java Low Visibility\Use Of Hardcoded Password 版本:7

類別

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management
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 Mobile Top 10 2016: M9-Reverse Engineering
CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
OWASP ASVS: V02 Authentication
OWASP Top 10 2021: A7-Identification and Authentication Failures
SANS top 25: SANS top 25
ASA Mobile Premium: ASA Mobile Premium
ASA Premium: ASA Premium
ASD STIG 5.2: APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.

描述

Use Of Hardcoded Password\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=448
狀態	新的
Detection Date	12/12/2024 10:18:25 AM

應用程式使用寫死的密碼 psw1 來進行身分驗證或存取其他遠端系統。cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java 第 85 行的密碼出現在程式碼中

，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java	cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java
行	87	87
物件	psw1	psw1

代碼片斷

檔案名稱 cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java

方法 void verify() {

```
....
87.  String psw1 = "5B3920";
```

Use Of Hardcoded Password\路徑 2:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=449
狀態	新的
Detection Date	12/12/2024 10:18:25 AM

應用程式使用寫死的密碼 psw2 來進行身分驗證或存取其他遠端系統。cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java 第 85 行的密碼出現在程式碼中，這意味著任何可以存取原始碼的人都可以輕易的存取這組密碼，而且除非應用程式重建，否則這組密碼會無法進行更改。

	來源	目的地
檔案	cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java	cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java
行	88	88
物件	psw2	psw2

代碼片斷

檔案名稱 cmn/cmn-service/src/test/java/com/scsb/ncbs/cmn/service/ntf/otp/NtfOtpServiceIT.java

方法 void verify() {

```
....
88.  String psw2 = "299450";
```

Spring Missing Content Security Policy

查詢路徑:

Java\Cx\Java Spring\Spring Missing Content Security Policy 版本:3

類別

OWASP ASVS: V14 Configuration
OWASP Top 10 2021: A7-Identification and Authentication Failures

描述

Spring Missing Content Security Policy\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=450
狀態	新的
Detection Date	12/12/2024 10:18:27 AM

Web 應用程式中未明確定義內容安全性原則。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java
行	5	5
物件	boot	boot

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java

方法 import org.springframework.boot.SpringApplication;

```
....
5.  import org.springframework.boot.SpringApplication;
```

Spring Missing Expect CT Header

查詢路徑:

Java\Cx\Java Spring\Spring Missing Expect CT Header 版本:3

類別

CWE top 25: CWE top 25
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
OWASP Top 10 2021: A8-Software and Data Integrity Failures
SANS top 25: SANS top 25

描述

Spring Missing Expect CT Header\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=451
狀態	新的
Detection Date	12/12/2024 10:18:27 AM

Web 應用程式未定義 Expect-CT 標頭，使其更容易受到攻擊。

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java
行	5	5
物件	boot	boot

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/CbrApplication.java

方法 import org.springframework.boot.SpringApplication;

```
....
5.  import org.springframework.boot.SpringApplication;
```

Undocumented API

查詢路徑:

Java\Cx\Java Best Coding Practice\Undocumented API 版本:2

類別

OWASP ASVS: V01 Architecture, Design and Threat Modeling

描述

Undocumented API\路徑 1:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1032
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readRejected method (line 53) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
行	53	53
物件	readRejected	readRejected

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<BranchCbrDataModReadRejectedRs>> readRejected(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModReadRejectedRq>> apiRequest) {

```
....
53.  public ApiResponse<ServiceRs<BranchCbrDataModReadRejectedRs>>
readRejected(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModReadRejectedRq>> apiRequest) {
```

Undocumented API\路徑 2:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1033
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 66) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java
行	66	66
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<BranchCbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModUpdateRq>> apiRequest) {

```
....
66.  public ApiResponse<ServiceRs<BranchCbrDataModUpdateRs>>
update(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModUpdateRq>>
apiRequest) {
```

Undocumented API\路徑 3:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1034
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's delete method (line 79) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

行	79	79
物件	delete	delete

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCbrDataModController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {

```
....
79.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<BranchCbrDataModDeleteRq>> apiRequest) {
```

Undocumented API\路徑 4:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1035
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 53) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java
行	53	53
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>> apiRequest) {

```
....
53.  public ApiResponse<ServiceRs<BranchCoreCbrDataReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataReadRq>>
apiRequest) {
```

Undocumented API\路徑 5:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1036
狀態	新的

Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 66) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java
行	66	66
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchCoreCbrDataController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {

```
....
66.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<BranchCoreCbrDataUpdateRq>> apiRequest) {
```

Undocumented API\路徑 6:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1037
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 48) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchDailySettlementController.java

方法 public ApiResponse<ServiceRs<BranchDailySettlementReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchDailySettlementReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchDailySettlementReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchDailySettlementReadRq>>
apiRequest) {
```

Undocumented API\路徑 7:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1038
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 48) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchErrorReportController.java

方法 public ApiResponse<ServiceRs<BranchErrorReportReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchErrorReportReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchErrorReportReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchErrorReportReadRq>>
apiRequest) {
```

Undocumented API\路徑 8:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1039
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 48) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java

行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDailyReportController.java

方法 public ApiResponse<ServiceRs<BranchTxnDailyReportReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchTxnDailyReportReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchTxnDailyReportReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchTxnDailyReportReadRq>>
apiRequest) {
```

Undocumented API\路徑 9:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1040
狀態 新的
Detection Date 12/12/2024 10:18:34 AM

The application's read method (line 48) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java
行	48	48
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/branch/BranchTxnDetailController.java

方法 public ApiResponse<ServiceRs<BranchTxnDetailReadRs>> read(@RequestBody ApiRequest<ServiceRq<BranchTxnDetailReadRq>> apiRequest) {

```
....
48.  public ApiResponse<ServiceRs<BranchTxnDetailReadRs>>
read(@RequestBody ApiRequest<ServiceRq<BranchTxnDetailReadRq>>
apiRequest) {
```

Undocumented API\路徑 10:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1041

狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readError method (line 54) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	54	54
物件	readError	readError

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadErrorRs>> readError(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadErrorRq>> apiRequest) {

```
....
54.  public ApiResponse<ServiceRs<CbrDataInquiryReadErrorRs>>
readError(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadErrorRq>>
apiRequest) {
```

Undocumented API\路徑 11:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1042
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readDeclaration method (line 67) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	67	67
物件	readDeclaration	readDeclaration

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadDeclarationRs>> readDeclaration(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadDeclarationRq>> apiRequest) {

```
....
67.  public ApiResponse<ServiceRs<CbrDataInquiryReadDeclarationRs>>
readDeclaration(@RequestBody
ApiRequest<ServiceRq<CbrDataInquiryReadDeclarationRq>> apiRequest) {
```

Undocumented API\路徑 12:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1043
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 80) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java
行	80	80
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadRs>> read(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<CbrDataInquiryReadRs>>
read(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRq>>
apiRequest) {
```

Undocumented API\路徑 13:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1044
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readRejected method (line 93) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

行	93	93
物件	readRejected	readRejected

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataInquiryController.java

方法 public ApiResponse<ServiceRs<CbrDataInquiryReadRejectedRs>> readRejected(@RequestBody ApiRequest<ServiceRq<CbrDataInquiryReadRejectedRq>> apiRequest) {

```
....
93.  public ApiResponse<ServiceRs<CbrDataInquiryReadRejectedRs>>
readRejected(@RequestBody
ApiRequest<ServiceRq<CbrDataInquiryReadRejectedRq>> apiRequest) {
```

Undocumented API\路徑 14:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1045
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's create method (line 59) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	59	59
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModCreateRs>> create(@RequestBody ApiRequest<ServiceRq<CbrDataModCreateRq>> apiRequest) {

```
....
59.  public ApiResponse<ServiceRs<CbrDataModCreateRs>>
create(@RequestBody ApiRequest<ServiceRq<CbrDataModCreateRq>>
apiRequest) {
```

Undocumented API\路徑 15:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1046
狀態	新的

Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 72) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	72	72
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModReadRs>> read(@RequestBody ApiRequest<ServiceRq<CbrDataModReadRq>> apiRequest) {

```
....
72.  public ApiResponse<ServiceRs<CbrDataModReadRs>> read(@RequestBody
ApiRequest<ServiceRq<CbrDataModReadRq>> apiRequest) {
```

Undocumented API\路徑 16:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1047
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 85) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	85	85
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法 public ApiResponse<ServiceRs<CbrDataModUpdateRs>> update(@RequestBody ApiRequest<ServiceRq<CbrDataModUpdateRq>> apiRequest) {

```
....
85.  public ApiResponse<ServiceRs<CbrDataModUpdateRs>>
update(@RequestBody ApiRequest<ServiceRq<CbrDataModUpdateRq>>
apiRequest) {
```

Undocumented API\路徑 17:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1048
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's delete method (line 98) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	98	98
物件	delete	delete

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {

```
....
98.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrDataModDeleteRq>> apiRequest) {
```

Undocumented API\路徑 18:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1049
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's reject method (line 111) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	111	111
物件	reject	reject

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java

方法	public ApiResponse<ServiceRs<EmptyRs>> reject(@RequestBody ApiRequest<ServiceRq<CbrDataModRejectRq>> apiRequest) {

```
....
111.  public ApiResponse<ServiceRs<EmptyRs>> reject(@RequestBody
ApiRequest<ServiceRq<CbrDataModRejectRq>> apiRequest) {
```

Undocumented API\路徑 19:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1050
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's amend method (line 124) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
行	124	124
物件	amend	amend

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/data/CbrDataModController.java
方法	public ApiResponse<ServiceRs<CbrDataModAmendRs>> amend(@RequestBody ApiRequest<ServiceRq<CbrDataModAmendRq>> apiRequest) {

```
....
124.  public ApiResponse<ServiceRs<CbrDataModAmendRs>>
amend(@RequestBody ApiRequest<ServiceRq<CbrDataModAmendRq>> apiRequest)
{
```

Undocumented API\路徑 20:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1051
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 37) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll

	er/file/CbrFileKController.java	er/file/CbrFileKController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java

方法 public ApiResponse<ServiceRs<FileKReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileKReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileKReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileKReadRq>> apiRequest) {
```

Undocumented API\路徑 21:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1052
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 49) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java
行	49	49
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileKController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileKUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileKUpdateRq>> apiRequest) {
```

Undocumented API\路徑 22:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1053
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 37) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java

方法 public ApiResponse<ServiceRs<FileLReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileLReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileLReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileLReadRq>> apiRequest) {
```

Undocumented API\路徑 23:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1054
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 49) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java
行	49	49
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileLController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileLUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileLUpdateRq>> apiRequest) {
```

Undocumented API\路徑 24:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1055
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 37) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
行	37	37
物件	read	read

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
方法	public ApiResponse<ServiceRs<FileMReadRs>> read(@RequestBody ApiRequest<ServiceRq<FileMReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FileMReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FileMReadRq>> apiRequest) {
```

Undocumented API\路徑 25:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1056
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 49) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
行	49	49
物件	update	update

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileMController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FileMUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FileMUpdateRq>> apiRequest) {
```

Undocumented API\路徑 26:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1057
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 37) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java
行	37	37
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java

方法 public ApiResponse<ServiceRs<FilePReadRs>> read(@RequestBody ApiRequest<ServiceRq<FilePReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<FilePReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FilePReadRq>> apiRequest) {
```

Undocumented API\路徑 27:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1058
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 49) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java
行	49	49

物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFilePController.java

方法 public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<FilePUpdateRq>> apiRequest) {

```
....
49.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<FilePUpdateRq>> apiRequest) {
```

Undocumented API\路徑 28:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1059

狀態 新的

Detection Date 12/12/2024 10:18:34 AM

The application's compileData method (line 35) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java
行	35	35
物件	compileData	compileData

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFileSummaryController.java

方法 public ApiResponse<ServiceRs<FileSummaryReadRs>> compileData(@RequestBody ApiRequest<ServiceRq<FileSummaryCompileDataRq>> apiRequest) {

```
....
35.  public ApiResponse<ServiceRs<FileSummaryReadRs>>
compileData(@RequestBody ApiRequest<ServiceRq<FileSummaryCompileDataRq>>
apiRequest) {
```

Undocumented API\路徑 29:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1060

狀態 新的

Detection Date 12/12/2024 10:18:34 AM

The application's read method (line 46) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java
行	46	46
物件	read	read

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/file/CbrFXSpotInquiryController.java

方法 public ApiResponse<ServiceRs<FXSpotReadRs>> read(@RequestBody ApiRequest<ServiceRq<FXSpotReadRq>> apiRequest) {

```
....
46.  public ApiResponse<ServiceRs<FXSpotReadRs>> read(@RequestBody
ApiRequest<ServiceRq<FXSpotReadRq>> apiRequest) {
```

Undocumented API\路徑 30:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1061
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readByType method (line 43) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	43	43
物件	readByType	readByType

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法 public ApiResponse<ServiceRs<List<CbrOrgKeywordRs>>> readByType(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordReadByTypeRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<List<CbrOrgKeywordRs>>>
readByType(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordReadByTypeRq>>
apiRequest) {
```

Undocumented API\路徑 31:

嚴重程度：	資訊

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1062
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's create method (line 55) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	55	55
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法 public ApiResponse<ServiceRs<String>> create(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordCreateRq>> apiRequest) {

```
....
55.  public ApiResponse<ServiceRs<String>> create(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordCreateRq>> apiRequest) {
```

Undocumented API\路徑 32:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1063
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 68) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	68	68
物件	update	update

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java

方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordUpdateRq>> apiRequest) {

```
....
68.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordUpdateRq>> apiRequest) {
```

Undocumented API\路徑 33:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1064
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's delete method (line 81) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
行	81	81
物件	delete	delete

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrOrgKeywordController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrOrgKeywordDeleteRq>> apiRequest) {

```
....
81.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrOrgKeywordDeleteRq>> apiRequest) {
```

Undocumented API\路徑 34:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1065
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readAll method (line 43) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controll

	er/param/CbrReturnReasonController.java	er/param/CbrReturnReasonController.java
行	43	43
物件	readAll	readAll

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<List<CbrReturnReasonRs>>> readAll(@RequestBody ApiRequest<ServiceRq<EmptyRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<List<CbrReturnReasonRs>>>
readAll(@RequestBody ApiRequest<ServiceRq<EmptyRq>> apiRequest) {
```

Undocumented API\路徑 35:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1066
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's create method (line 55) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	55	55
物件	create	create

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java

方法 public ApiResponse<ServiceRs<String>> create(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonCreatedRq>> apiRequest) {

```
....
55.  public ApiResponse<ServiceRs<String>> create(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonCreatedRq>> apiRequest) {
```

Undocumented API\路徑 36:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1067

狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 67) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	67	67
物件	update	update

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonUpdatedRq>> apiRequest) {

```
....
67.  public ApiResponse<ServiceRs<EmptyRs>> update(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonUpdatedRq>> apiRequest) {
```

Undocumented API\路徑 37:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1068
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's delete method (line 80) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
行	80	80
物件	delete	delete

代碼片斷	
檔案名稱	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/param/CbrReturnReasonController.java
方法	public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody ApiRequest<ServiceRq<CbrReturnReasonDeletedRq>> apiRequest) {

```
....
80.  public ApiResponse<ServiceRs<EmptyRs>> delete(@RequestBody
ApiRequest<ServiceRq<CbrReturnReasonDeletedRq>> apiRequest) {
```

Undocumented API\路徑 38:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1069
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's generate method (line 44) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java	cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java
行	44	44
物件	generate	generate

代碼片斷

檔案名稱 cbr/cbr-app/src/main/java/com/scsb/ncbs/cbr/controller/report/CbrReportController.java

方法 public ApiResponse<ServiceRs<ReportGenerateRs>> generate(@RequestBody ApiRequest<ServiceRq<ReportGenerateRq>> apiRequest) {

```
....
44.  public ApiResponse<ServiceRs<ReportGenerateRs>>
generate(@RequestBody ApiRequest<ServiceRq<ReportGenerateRq>>
apiRequest) {
```

Undocumented API\路徑 39:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1070
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 39) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
行	39	39

物件	read	read

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayInfoReadRq>> apiRequest) {

```
....
39.  public ApiResponse<ServiceRs<BdayInfoReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayInfoReadRq>> apiRequest) {
```

Undocumented API\路徑 40:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1071
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readBusDaysBetween method (line 45) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java
行	45	45
物件	readBusDaysBetween	readBusDaysBetween

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/info/BdayInfoController.java

方法 public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>> readBusDaysBetween(@RequestBody ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {

```
....
45.  public ApiResponse<ServiceRs<BdayInfoBusDaysBetweenReadRs>>
readBusDaysBetween(@RequestBody
ApiRequest<ServiceRq<BdayInfoBusDaysBetweenReadRq>> apiRequest) {
```

Undocumented API\路徑 41:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1072
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's create method (line 38) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	38	38
物件	create	create

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<?> create(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
38.  public ApiResponse<?> create(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

Undocumented API\路徑 42:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1073
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 46) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	46	46
物件	update	update

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java

方法 public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {

```
....
46.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<BdayInitRq>> apiRequest) {
```

Undocumented API\路徑 43:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1074
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 54) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
行	54	54
物件	read	read

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/init/BdayInitController.java
方法	public ApiResponse<ServiceRs<BdayInitReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayInitReadRq>> apiRequest) {

```
....
54.  public ApiResponse<ServiceRs<BdayInitReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayInitReadRq>> apiRequest) {
```

Undocumented API\路徑 44:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1075
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 36) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java
行	36	36
物件	read	read

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/near/BdayNearController.java

方法	public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNearReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNearReadRq>> apiRequest) {
```

Undocumented API\路徑 45:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1076
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's read method (line 36) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java
行	36	36
物件	read	read

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/next/BdayNextController.java
方法	public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {

```
....
36.  public ApiResponse<ServiceRs<BdayNextReadRs>> read(@RequestBody
ApiRequest<ServiceRq<BdayNextReadRq>> apiRequest) {
```

Undocumented API\路徑 46:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1077
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readJson method (line 37) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/control	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/control

	ler/bday/prov/BdayProvController.java	ler/bday/prov/BdayProvController.java
行	37	37
物件	readJson	readJson

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java

方法 public ApiResponse<ServiceRs<BdayProvReadJsonListRs>> readJson(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest) {

```
....
37.  public ApiResponse<ServiceRs<BdayProvReadJsonListRs>>
readJson(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest)
{
```

Undocumented API\路徑 47:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1078
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readChar method (line 43) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java
行	43	43
物件	readChar	readChar

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/prov/BdayProvController.java

方法 public ApiResponse<ServiceRs<BdayProvReadCharListRs>> readChar(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest) {

```
....
43.  public ApiResponse<ServiceRs<BdayProvReadCharListRs>>
readChar(@RequestBody ApiRequest<ServiceRq<BdayProvReadRq>> apiRequest)
{
```

Undocumented API\路徑 48:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=1079
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's update method (line 34) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java
行	34	34
物件	update	update

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/bday/susp/BdaySuspController.java
方法	public ApiResponse<?> update(@RequestBody ApiRequest<ServiceRq<BdaySuspUpdateRq>> apiRequest) {

```
....
34.  public ApiResponse<?> update(@RequestBody
ApiRequest<ServiceRq<BdaySuspUpdateRq>> apiRequest) {
```

Undocumented API\路徑 49:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1080
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's getCustomerT24Id method (line 50) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/enquiry/CifEnquiryController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/enquiry/CifEnquiryController.java
行	50	50
物件	getCustomerT24Id	getCustomerT24Id

代碼片斷	
檔案名稱	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/enquiry/CifEnquiryController.java
方法	public ApiResponse<ServiceRs<List<GetCustomerT24IdRs>>> getCustomerT24Id(

```
....
50.  public ApiResponse<ServiceRs<List<GetCustomerT24IdRs>>>
getCustomerT24Id(
```

Undocumented API\路徑 50:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1081
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

The application's readList method (line 44) is an undocumented API endpoint. This is not a best practice and may lead to unintended behavior.

	來源	目的地
檔案	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/interactive/EcifInteractiveController.java	cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/interactive/EcifInteractiveController.java
行	44	44
物件	readList	readList

代碼片斷

檔案名稱 cmn/cmn-app/src/main/java/com/scsb/ncbs/cmn/controller/ecif/interactive/EcifInteractiveController.java

方法 public ApiResponse<ServiceRs<EcifInteractiveReadListRs>> readList(@RequestBody ApiRequest<ServiceRq<EcifInteractiveReadListRq>> apiRequest) {

```
....
44.  public ApiResponse<ServiceRs<EcifInteractiveReadListRs>>
readList(@RequestBody ApiRequest<ServiceRq<EcifInteractiveReadListRq>>
apiRequest) {
```

Insufficient Logging of Exceptions

查詢路徑:

Java\Cx\Java Best Coding Practice\Insufficient Logging of Exceptions 版本:2

類別

OWASP ASVS: V07 Error Handling and Logging
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures

描述

Insufficient Logging of Exceptions\路徑 1:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1556
狀態	新的

Detection Date	12/12/2024 10:18:34 AM

In line 129, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java
行	134	134
物件	catch	catch

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/bday/info/BdayInfoService.java

方法 .forEach(i -> {

```
....
134.  } catch (NoSuchMethodException | IllegalAccessException |
InvocationTargetException e) {
```

Insufficient Logging of Exceptions\路徑 2:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1557
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 161, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java	cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java
行	174	174
物件	catch	catch

代碼片斷

檔案名稱 cmn/cmn-service/src/main/java/com/scsb/ncbs/cmn/service/ntf/group/NtfInternalGrpService.java

方法 .map(data -> {

```
....
174.  } catch (EmptyResultDataAccessException e) {
```

Insufficient Logging of Exceptions\路徑 3:

嚴重程度：	資訊

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1558
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 122, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
行	136	136
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
方法	deletionList.forEach(deletion -> {

```
....
136.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 4:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1559
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 150, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
行	166	166
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
方法	deletionList.forEach(deletion -> {

```
....
166.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 5:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1560
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 228, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
行	236	236
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java

方法 private void sendRequest(String request) {

```
....
236.  } catch (IOException e) {
```

Insufficient Logging of Exceptions\路徑 6:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1561
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 237, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
行	244	244
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private List<PersonalDeletionRequestDto> parseFileToDto(String filePath) {

```
....
244.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 7:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1562
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 237, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
行	265	265
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private List<PersonalDeletionRequestDto> parseFileToDto(String filePath) {

```
....
265.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 8:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1563
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 280, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/j	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/j

	ob/aml/ReceivePersonalDeletionTasklet.java	ob/aml/ReceivePersonalDeletionTasklet.java
行	291	291
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java

方法 private LineIterator parseFile(String filePath) {

```
....
291.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 9:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1564
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 146, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java
行	154	154
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java

方法 private void sendRequest(String request) {

```
....
154.  } catch (IOException e) {
```

Insufficient Logging of Exceptions\路徑 10:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1565
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 49, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java
行	56	56
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ConfirmPersonalDeletionIT.java

方法 public void testTaskletJob() throws JobExecutionException {

```
....
56.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 11:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1566

狀態 新的

Detection Date 12/12/2024 10:18:34 AM

In line 47, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java
行	56	56
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/ReceivePersonalDeletionIT.java

方法 public void testTaskletJob() throws JobExecutionException {

```
....
56.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 12:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1567

狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 47, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java
行	55	55
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-bat/src/test/java/com/scsb/ncbs/dep/aml/RequestPersonalDeletionIT.java
方法	public void testTaskletJob() throws JobExecutionException {

```
....
55.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 13:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1568
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 61, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/BaseAdiService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/BaseAdiService.java
行	67	67
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/adi/BaseAdiService.java
方法	protected SimEcifCustomerInfo getCustomerInfoById(String customerNo) {

```
....
67.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 14:

嚴重程度：	資訊

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1569
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 232, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/aml/PersonalInfoServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/aml/PersonalInfoServiceIT.java
行	242	242
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/aml/PersonalInfoServiceIT.java
方法	void testQueryDeletionDetail() {

```
....
242.  catch(TxnException te) {
```

Insufficient Logging of Exceptions\路徑 15:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1570
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 272, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java
行	278	278
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java
方法	protected static String getBranchCodeFromAccount(String accountNo) {

```
....
278.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 16:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1571
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 289, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java
行	295	295
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/BaseDepService.java
方法	protected SimEcifCustomerInfo getCustomerInfoById(String customerNo) {

```
....
295.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 17:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1572
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 266, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java
行	287	287
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java
方法	.filter(entity -> {

```
....
287.   } catch (TxnException e) {
```

Insufficient Logging of Exceptions\路徑 18:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1573
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 539, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java
行	544	544
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/certification/DepCertService.java

方法 private void checkComment(String comment) {

```
....
544.   } catch (TxnException e) {
```

Insufficient Logging of Exceptions\路徑 19:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1574
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 690, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeService.java
行	699	699
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeService.java
方法	private ServiceRs<ReportDataRs> print(String reportId, Map<String, Object> dataSet) throws Throwable{

```
....
699.  catch (Exception ex) {
```

Insufficient Logging of Exceptions\路徑 20:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1575
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 120, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeUploadService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeUploadService.java
行	142	142
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeUploadService.java
方法	public ServiceRs<ReportDataRs> print(@Valid @NotNull(message = "交換票據提回上傳票查詢/列印(1551) arg 不可為空") ExchangeUploadArg arg) throws Throwable {

```
....
142.  catch (Exception ex) {
```

Insufficient Logging of Exceptions\路徑 21:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1576
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 351, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/media/MediaIncomeTaxService.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/media/MediaIncomeTaxService.java
行	360	360
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-service/src/main/java/com/scsb/ncbs/dep/service/media/MediaIncomeTaxService.java

方法 private CustomerResponseBody getCustomer(String customerNo) {

```
....
360.  catch (T24Exception t24Exception) {
```

Insufficient Logging of Exceptions\路徑 22:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1577

狀態 新的

Detection Date 12/12/2024 10:18:34 AM

In line 59, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java
行	72	72
物件	catch	catch

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java

方法 void testTakeSequenceForBranch3() throws InterruptedException {

```
....
72.  } catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 23:

嚴重程度： 資訊

結果狀態： 校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1578
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 100, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java
行	110	110
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/withholding/WithholdingSeqServiceIT.java
方法	void testTakeSequenceForBranch4() throws InterruptedException {

```
....
110.  } catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 24:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1579
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 126, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java	dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java
行	150	150
物件	catch	catch

代碼片斷	
檔案名稱	dep/dep-service/src/main/java/com/scsb/ncbs/dep/utils/common/CheckUtils.java
方法	public static <T> boolean checkSameObject(T object1, T object2) {

```
....
150.  } catch (IllegalAccessException e) {
```

Insufficient Logging of Exceptions\路徑 25:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1580
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 95, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	147	147
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java

方法 private void importToBondInfo(List<BondInfoInputDTO> dtoList) {

```
....
147.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 26:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1581
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 157, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	176	176
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java

方法	private List<BondInfoInputDTO> parseFileToDto() {

```
....
176.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 27:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1582
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 190, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	207	207
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
方法	private LineIterator parseFile() {

```
....
207.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 28:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1583
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 85, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	111	111
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
方法	private void importToBondPrice(List<BondPriceInputDTO> dtoList) {

```
....
111.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 29:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1584
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 121, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	140	140
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
方法	private List<BondPriceInputDTO> parseFileToDto() {

```
....
140.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 30:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1585
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 154, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-	len/len-

	bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	171	171
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java

方法 private LineIterator parseFile() {

```
....
171.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 31:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1586
狀態 新的
Detection Date 12/12/2024 10:18:34 AM

In line 106, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	184	184
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private void importTrustFundData(List<TrustFundInfoInputDTO> trustFundDTOList) {

```
....
184.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 32:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1587
狀態 新的
Detection Date 12/12/2024 10:18:34 AM

In line 201, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	255	255
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private void importForeignFundData(List<ForeignFundInfoInputDTO> foreignFundDTOList) {

```
....
255.  catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 33:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1588
狀態 新的
Detection Date 12/12/2024 10:18:34 AM

In line 266, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	293	293
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private List<ForeignFundInfoInputDTO> parseFileToForeignFundDto() {

```
....
293.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 34:

嚴重程度： 資訊
結果狀態： 校驗

線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1589
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 351, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	373	373
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
方法	private List<TrustFundInfoInputDTO> parseTrustFundFile(String filePath, String investorType) {

```
....
373.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 35:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1590
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 394, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	409	409
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
方法	private LineIterator parseFile(String filePath) {

```
....
409.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 36:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1591
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 114, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	153	153
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java

方法 private void updateStockInfo(List<LenStockHistoryEntity> filterHistoryEntities) {

```
....
153.  } catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 37:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1592
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 198, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	235	235
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
方法	private List<LenStockHistoryEntity> importToStockHistory(List<StockInfoInputDTO> dtoList) {

```
....
235.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 38:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1593
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 247, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	271	271
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
方法	private List<StockInfoInputDTO> parseFileToDto() {

```
....
271.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 39:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1594
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 288, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/jo	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/jo

	b/collatertal/ImportStockInfoTasklet.java	b/collatertal/ImportStockInfoTasklet.java
行	305	305
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java

方法 private LineIterator parseFile() {

```
....
305.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 40:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1595
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 76, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java
行	87	87
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java

方法 private void write080FileContent(Jcic080HeaderBean header, List<Jcic080BodyBean> bodyList, Jcic080TailerBean tailer) {

```
....
87.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 41:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1596
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 110, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java
行	157	157
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic080Tasklet.java

方法 private List<Jcic080BodyBean> prepare080BodyData(List<MvMidFdbuLimitEntity> limits) {

```
....
157.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 42:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1597

狀態 新的

Detection Date 12/12/2024 10:18:34 AM

In line 106, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java
行	132	132
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java

方法 private void write085FileContent(Jcic085HeaderBean headerBean, List<Jcic085BodyBean> bodyList, Jcic085TailerBean tailerBean) {

```
....
132.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 43:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=1598
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 210, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java
行	243	243
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java
方法	private List<Jcic085BodyBean> processSituationB() {

```
....
243.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 44:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1599
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 256, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java
行	290	290
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic085Tasklet.java
方法	private List<Jcic085BodyBean> processSituationA() {

```
....
290.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 45:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1600
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 95, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
行	120	120
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
方法	private void write207FileContent(Jcic207HeaderBean headerBean, List<Jcic207BodyBean> bodyBeanList, Jcic207TailerBean tailerBean) {

```
....
120.  catch(Exception e) {
```

Insufficient Logging of Exceptions\路徑 46:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1601
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 141, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
行	145	145
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
方法	bodyList.forEach(body -> {

```
....
145.   } catch (IOException e) {
```

Insufficient Logging of Exceptions\路徑 47:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1602
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 134, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
行	152	152
物件	catch	catch

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java

方法 private void writeToOutputFile(String header, List<String> bodyList, String tailer) {

```
....
152.   } catch (IOException e) {
```

Insufficient Logging of Exceptions\路徑 48:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1603
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 190, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
行	307	307
物件	catch	catch

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/jcic/SubmitJcic207Tasklet.java
方法	private void assignValueToBody(Jcic207BodyBean body, QueryPidBasicInfoRs basicInfoRs, EloanRs eloanRs) {

```
....
307.  } catch (UnsupportedEncodingException e) {
```

Insufficient Logging of Exceptions\路徑 49:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1604
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 92, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/service/query/LoanBalCertService.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/query/LoanBalCertService.java
行	105	105
物件	catch	catch

代碼片斷	
檔案名稱	len/len-service/src/main/java/com/scsb/ncbs/len/service/query/LoanBalCertService.java
方法	public ServiceRs<LoanBalCertRs> query(@NotNull LoanBalCertArg loanBalCertArg) {

```
....
105.  } catch (Exception e) {
```

Insufficient Logging of Exceptions\路徑 50:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1605
狀態	新的
Detection Date	12/12/2024 10:18:34 AM

In line 153, the security-critical event is not logged properly and, therefore,the error message has some important details omitted.

	來源	目的地
檔案	len/len-service/src/main/java/com/scsb/ncbs/len/service/query/PaymentCalculationService.java	len/len-service/src/main/java/com/scsb/ncbs/len/service/query/PaymentCalculationService.java

行	173	173
物件	catch	catch

代碼片斷

檔案名稱 len/len-service/src/main/java/com/scsb/ncbs/len/service/query/PaymentCalculationService.java

方法 public ServiceRs<PaymentCalculationRs> calculateLoanPayment(@NotNull PaymentCalculationArg paymentCalculationArg) {

```
....
173.  } catch (Exception e) {
```

Portability Flaw In File Separator

查詢路徑:

Java\Cx\Java Best Coding Practice\Portability Flaw In File Separator 版本:8

描述

Portability Flaw In File Separator\路徑 1:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=992

狀態 新的

Detection Date 12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	78	78
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getTimeDepForCustomer(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
78.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 2:

嚴重程度： 資訊

結果狀態： 校驗

線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=993

狀態 新的

Detection Date 12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java
行	79	79
物件	""./src/test/resources/csv/condensed/testData.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/condensed/CondensedServiceIT.java

方法 List<DepCondensedTransactionDetailsEntity> getData(String accountNo, LocalDate condensedDate) throws Exception {

```
....
79.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/condensed/testData.csv"));
```

Portability Flaw In File Separator\路徑 3:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=994
狀態 新的
Detection Date 12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java
行	110	110
物件	""./src/test/resources/csv/crr/testCharge.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrChargeServiceIT.java

方法 <T extends CreateChargeInfoArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
110.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/crr/testCharge.csv"));
```

Portability Flaw In File Separator\路徑 4:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=995
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
行	111	111
物件	""./src/test/resources/csv/rpt/testDataFor1038.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/healthinsurance/HealthInsuranceServiceIT.java
方法	List<TmbRs> getCsvDate() throws Exception {

```
....
111.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/rpt/testDataFor1038.csv"));
```

Portability Flaw In File Separator\路徑 5:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=996
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	119	119
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getTimeDepForAccount(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
119.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 6:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=997
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	165	165
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getApplication(String customerMnemonic, String altAcctNo, String productGroup, String currency) throws Exception {

```
....
165.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 7:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=998
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java
行	211	211
物件	""./src/test/resources/csv/crr/testRecords.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crr/CrrRecordsServiceIT.java

方法 <T extends RecordsArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
211.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/crr/testRecords.csv"));
```

Portability Flaw In File Separator\路徑 8:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=999
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	211	211
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getBaseInfo(String custId, String arrangementId, String accountId) throws Exception {

```
....
211.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 9:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1000
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	275	275
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
275.  BufferedReader readerTimeDep = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 10:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1001
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	289	289
物件	""./src/test/resources/csv/tdb/interestCalculation_0.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法 void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
289.  BufferedReader readerInterestCalculation = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/interestCalculation_0.csv"));
```

Portability Flaw In File Separator\路徑 11:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1002
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	307	307
物件	""./src/test/resources/csv/tdb/interestPaid.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法	void getInterestCalculation(ReadDetailsArg arg) throws IOException {

```
....
307.  BufferedReader readerInterestPaid = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/interestPaid.csv"));
```

Portability Flaw In File Separator\路徑 12:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1003
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	313	313
物件	""./src/test/resources/csv/crp/test_1504.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	<T extends ReserveArg> List<T> getCsvDate(Class<T> clazz) throws Exception {

```
....
313.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/crp/test_1504.csv"));
```

Portability Flaw In File Separator\路徑 13:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1004
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	334	334
物件	""./src/test/resources/csv/crp/test_1505.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java

方法	List<UpdateReserveArg> getCsvDate() throws Exception {

```
....
334.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/crp/test_1505.csv"));
```

Portability Flaw In File Separator\路徑 14:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1005
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
行	353	353
物件	""./src/test/resources/csv/crp/test_1501.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/crp/CrpServiceIT.java
方法	List<RemarkArg> getRemarkCsvDate() throws Exception {

```
....
353.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/crp/test_1501.csv"));
```

Portability Flaw In File Separator\路徑 15:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1006
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	386	386
物件	""./src/test/resources/csv/tdb/timeDep.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java

方法	void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
386.  BufferedReader readerTimeDep = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/timeDep.csv"));
```

Portability Flaw In File Separator\路徑 16:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1007
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	396	396
物件	""./src/test/resources/csv/tdb/regularSaving.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getRegularSaving(ReadDetailsArg arg) throws IOException {

```
....
396.  BufferedReader regularSavings = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/regularSaving.csv"));
```

Portability Flaw In File Separator\路徑 17:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1008
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
行	409	409
物件	""./src/test/resources/csv/tdb/exchangeRate.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/tdb/OldTimeDepBillServiceIT.java
方法	void getExchangeRate() throws IOException {

```
....
409.  BufferedReader reader = new BufferedReader(new
FileReader("./src/test/resources/csv/tdb/exchangeRate.csv"));
```

Portability Flaw In File Separator\路徑 18:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1009
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	72	154
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	void testRead() throws Exception {

```
....
72.  List<ChequePaymentRs> unPaidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnPa
id.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
154.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 19:

嚴重程度：	資訊

結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1010
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	73	154
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法 void testRead() throws Exception {

```
....
73.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
154.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 20:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1011
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.j	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.j

	ava	ava
行	81	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	void RCALX001() throws Throwable {

```
....
81.  List<ChequePaymentRs> testDataList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 21:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1012
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	98	154
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法	void testPrint() throws Throwable {

```
....
98.  List<ChequePaymentRs> unPaidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnPa
id.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
154.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 22:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1013
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	99	154
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	void testPrint() throws Throwable {

```
....
99.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java

方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
154.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 23:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1014
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
行	134	154
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	void testRecorded() throws Exception {

```
....
134.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeUploadServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
154.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 24:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1015

狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	140	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 void RCALX002() throws Throwable {

```
....
140.  List<ChequePaymentRs> unpaidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnpa
id.csv");
```

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 25:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1016
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java
行	150	151
物件	""src/test/resources/data/personal_deletion_re	File

	quest.txt""	

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/RequestPersonalDeletionTasklet.java
方法	private void sendRequest(String request) {

```
....
150.  String filePath =
"src/test/resources/data/personal_deletion_request.txt";
151.  File file = new File(filePath);
```

Portability Flaw In File Separator\路徑 26:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1017
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	163	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	void RCALX002() throws Throwable {

```
....
163.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 27:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1018
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	218	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 void RCALX004() throws Throwable {

```
....
218.  List<ChequePaymentRs> unpaidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv");
```

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 28:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1019
狀態	新的

Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	219	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 void RCALX004() throws Throwable {

```
....
219.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱 dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java

方法 List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 29:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1020
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
行	232	233
物件	""src/test/resources/data/personal_deletion_confirmation.txt""	File

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ConfirmPersonalDeletionTasklet.java
方法	private void sendRequest(String request) {

```
....
232.  String filePath =
"src/test/resources/data/personal_deletion_confirmation.txt";
233.  File file = new File(filePath);
```

Portability Flaw In File Separator\路徑 30:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1021
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	280	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	void deleteEntity() throws Exception {

```
....
280.  List<ChequePaymentRs> unpaidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForUnpaid.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 31:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1022
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
行	302	314
物件	""./src/test/resources/csv/exchangecheque/chequePaymentForPaid.csv""	FileReader

代碼片斷	
檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	void deleteEntity() throws Exception {

```
....
302.  List<ChequePaymentRs> paidList =
getCsvDate("./src/test/resources/csv/exchangecheque/chequePaymentForPaid
.csv");
```

檔案名稱	dep/dep-service/src/test/java/com/scsb/ncbs/dep/service/exchangecheque/ExchangeChequeServiceIT.java
方法	List<ChequePaymentRs> getCsvDate(String path) throws Exception {

```
....
314.  BufferedReader reader = new BufferedReader(new FileReader(path));
```

Portability Flaw In File Separator\路徑 32:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1023
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-	len/len-

	bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java	bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java
行	161	169
物件	""/BOND_PRICE_""	lineIterator

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondPriceTasklet.java

方法 private LineIterator parseFile() {

```
....
161.  filePath = eftFilepath + "/BOND_PRICE_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
....
169.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 33:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1024
狀態 新的
Detection Date 12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java
行	197	205
物件	""/BOND_INFO_""	lineIterator

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportBondInfoTasklet.java

方法 private LineIterator parseFile() {

```
....
197.  filePath = eftFilepath + "/BOND_INFO_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
....
205.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 34:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathi

	d=1025
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
行	295	303
物件	""/STOCK_INFO_""	lineIterator

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportStockInfoTasklet.java
方法	private LineIterator parseFile() {

```
....
295.  filePath = eftFilepath + "/STOCK_INFO_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
....
303.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 35:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1026
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	273	407
物件	""/FUND_FUNI_""	lineIterator

代碼片斷	
檔案名稱	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
方法	private List<ForeignFundInfoInputDTO> parseFileToForeignFundDto() {

```
....
273.  filePath = eftFilepath + "/FUND_FUNI_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
```

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private LineIterator parseFile(String filePath) {

```
....
407.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 36:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1027
狀態 新的
Detection Date 12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	322	407
物件	""/FUND_ETF_""	lineIterator

代碼片斷
檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
方法 private List<TrustFundInfoInputDTO> parseFileToTrustFundDto() {

```
....
322.  filePath = eftFilepath + "/FUND_ETF_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
```

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private LineIterator parseFile(String filePath) {

```
....
407.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 37:

嚴重程度： 資訊
結果狀態： 校驗
線上結果 http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1028

狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java	len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java
行	335	407
物件	""/FUND_ETX_""	lineIterator

代碼片斷

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private List<TrustFundInfoInputDTO> parseFileToTrustFundDto() {

```
....
335.  filePath = eftFilepath + "/FUND_ETX_" +
MidDateUtils.localDateToString(LocalDate.now(),
DateTimeFormatter.BASIC_ISO_DATE) + ".dat";
```

檔案名稱 len/len-bat/src/main/java/com/scsb/ncbs/len/batch/job/collatertal/ImportFundInfoTasklet.java

方法 private LineIterator parseFile(String filePath) {

```
....
407.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 38:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1029
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
行	229	289
物件	""/data/FQAUT2_DCS.txt""	lineIterator

代碼片斷

檔案名稱 dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java

方法	private List<String> getFilePathList() {

```
....
229.  return Arrays.asList("/data/FQAUT2_DCS.txt",
"/data/FQAUT2_IBS.txt", "/data/FQAUT2_CCS.txt");
```

檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private LineIterator parseFile(String filePath) {

```
....
289.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 39:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1030
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
行	229	289
物件	""/data/FQAUT2_IBS.txt""	lineIterator

代碼片斷

檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private List<String> getFilePathList() {

```
....
229.  return Arrays.asList("/data/FQAUT2_DCS.txt",
"/data/FQAUT2_IBS.txt", "/data/FQAUT2_CCS.txt");
```

檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private LineIterator parseFile(String filePath) {

```
....
289.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Portability Flaw In File Separator\路徑 40:

嚴重程度：	資訊
結果狀態：	校驗
線上結果	http://10.10.2.164/CxWebClient/ViewerMain.aspx?scanid=96597&projectid=31588&pathid=1031
狀態	新的
Detection Date	12/12/2024 10:18:32 AM

	來源	目的地
檔案	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
行	229	289
物件	""/data/FQAUT2_CCS.txt""	lineIterator

代碼片斷	
檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private List<String> getFilePathList() {

```
....
229.  return Arrays.asList("/data/FQAUT2_DCS.txt",
"/data/FQAUT2_IBS.txt", "/data/FQAUT2_CCS.txt");
```

檔案名稱	dep/dep-bat/src/main/java/com/scsb/ncbs/dep/batch/job/aml/ReceivePersonalDeletionTasklet.java
方法	private LineIterator parseFile(String filePath) {

```
....
289.  return MidFileUtils.lineIterator(fileResource.getFile(), "MS950");
```

Second Order SQL Injection

風險

可能發生什麼問題

攻擊者可以直接存取系統內的所有資料、竊取敏感資訊，包含私人使用者資訊，信用卡明細，商業機密，以及其他秘密資料。同樣的，攻擊者可能會修改或刪除已經存在的資料，或者甚至加入假資料。在有些情境下，甚至可能可以在資料庫上執行程式碼。

除了直接揭露及更改機密資訊以外，此漏洞還可以用來做其他應用，像是繞過身分驗證，越過安全驗證機制，或者偽造資料追蹤紀錄。

攻擊者輕易的找到程式的缺陷，進一步增加被漏洞利用的可能性。

原因

如何發生

應用程式利用SQL查詢語句來與資料庫引擎溝通，利用資料庫來儲存及管理資料。應用程式建構SQL查詢語句時，只是簡單的把字串相加，並插入不受信任的資料。而且資料與語句之間沒有分隔；此外，插入資料時，既沒檢查資料格式的正確性

也沒有對其進行過濾。因此，不受信任的資料可能會包含在SQL查詢語句中，或者修改預期的SQL查詢語句。對資料庫而言，這是來自應用程式的SQL查詢，因此會如實的執行這些已被竄改過的查詢。
為了能利用這個漏洞，攻擊者可能會先把惡意的payload想辦法存入資料庫，典型的狀況是透過網頁上的表單(forms)格式。之後應用程式會從資料庫中讀取包含這個payload的資料，接著將其作為SQL指令，插入SQL查詢語句中。

一般建議

如何避免

- 無論來源為何，都要驗證所有不受信任的資料。驗證方式應採用白名單：僅接受符合指定結構的資料。不要建議採用黑名單的方式：僅拒絕非法字元。
- 尤其是要確認：
    - 資料格式(Data type)
    - 資料大小(Size)
    - 資料間距(Range)
    - 資料格式(Format)
    - 資料預期的值(Expected values)
- 根據最小權限原則，限制存取資料庫的物件及功能。
- 不要使用動態的字串串接來建立SQL查詢語句
- 最好使用DB Stored Procedures(預存程序)來存取資料，而非動態的組合查詢語句
- 建議使用安全的資料庫元件，像是參數化查詢及物件綁定(object bindings，例如：指令(commands)及參數(parameters))
- 或者，更好的解法是使用ORM的library，可以把應用程式上允許執行的指令預先定義及封裝起來，代替直接動態存取資料庫。如果使用這個方法就可以把指令部分與資料部分彼此隔離。
- 想要有效的執行資料驗證，可以使用安全函式庫，像是OWASP的Encoder或者ESAPI 函式庫。
- 建議使用 `PreparedStatement` 或更好的 `CallableStatement`來做參數化查詢。正確的使用.set*()方法來加入動態資料，而非字串串接，否則就失去參數化查詢的目的了。
- 考慮使用ORM的package，像是Hibernate、myBatisc等等。

程式碼範例

Java

Create SQL Query Using String Concatenation Based on Arbitrary Data

```
public String getActiveContact_Unsafe(HttpServletRequest request)
            throws ServletException, IOException {
      String userNameFromDB;
      String contact;

      try {
            Connection conn = getConnection();

            CallableStatement readNameStmt = conn.prepareCall("{call getActiveUser (?)}");
            readNameStmt.registerOutParameter(1, java.sql.Types.VARCHAR);
            readNameStmt.execute();
            userNameFromDB = readNameStmt.getString(1);

            String sql = "SELECT [Contact] FROM [AppUsers] WHERE [UserName] = '" +
```

```
userNameFromDB + "' " ;
            Statement readDetailsStmt = conn.createStatement();
            ResultSet data = readDetailsStmt.executeQuery(sql);

            contact = data.getString(1);
      } catch (SQLException ex) {
            handleExceptions(ex);
      }
      finally {
            closeQuietly(data);
            closeQuietly(readNameStmt);
            closeQuietly(readDetailsStmt);
            closeQuietly(conn);
      }

      return contact;
}
```

Build PreparedStatement to Call Stored Procedure and Set Data to Parameters

```
public String getActiveContact_SafeParameterizedQuery(HttpServletRequest request)
            throws ServletException, IOException {
      String userNameFromDB;
      String contact;

      String sqlStoredProc = "{call getUserId (?, ?)}";

      try {
            Connection conn = getConnection();

            CallableStatement readNameStmt = conn.prepareCall("{call getActiveUser (?)}");
            readNameStmt.registerOutParameter(1, java.sql.Types.VARCHAR);
            readNameStmt.execute();
            userNameFromDB = readNameStmt.getString(1);

            CallableStatement readDetailsStmt = conn.prepareCall(sqlStoredProc);

            readDetailsStmt.setString(1, userNameFromDB);
            readDetailsStmt.registerOutParameter(2, java.sql.Types.VARCHAR);

            readDetailsStmt.execute();
            contact = readDetailsStmt.getString(2);
      } catch (SQLException ex) {
            handleExceptions(ex);
      }
      finally {
            closeQuietly(readNameStmt);
            closeQuietly(readDetailsStmt);
            closeQuietly(conn);
      }

      return contact;
}
```

DB Parameter Tampering

風險

可能發生什麼問題

惡意使用者可以透過簡單地更改發送到伺服器的引用參數來訪問其他用戶的個人訊息，因此，惡意的使用者可以繞過訪問控制權限並訪問未經授權的記錄，例如其他用戶的帳號，竊取機密或受限制的訊息。

原因

如何發生

應用程式訪問使用者訊息時不以使用者的 ID 過濾，例如，它可能僅透過提交的帳戶 ID， 該應用程式以使用者的輸入從資料庫表中過濾特定記錄，其中可能包含敏感的個人訊息（例如使用者帳號或付款明細）。 由於應用程式不會根據任何使用者識別碼過濾記錄，也不會將其限制為預先計算的可接受值，因此惡意的使用者可以輕鬆修改提交的識別碼，從而訪問未經授權的記錄。

一般建議

如何避免

通用指南：

- 在提供對敏感性資料（包括特定物件引用）的任何存取權限之前執行授權檢查。
- 明確阻止對任何未經授權的訪問資料，尤其是其他使用者的資料。
- 如果可能，避免允許使用者通過簡單地發送記錄 ID 來請求任意資料。 例如，應用程式不應讓使用者發送帳號 ID，而應查找當前經過身份驗證的使用者會話的帳號 ID。

具體緩解措施：

- 根據使用者特定的識別字（例如客戶編號）過濾資料庫查詢。
- 將使用者輸入映射到間接引用，例如通過準備好的允許值列表。

程式碼範例

Java

Unfiltered Direct Object Reference

```
public ResultSet getAccountInfo(request req){
    int accountId = Integer.parseInt(req.getParameter("accountId"));
    PreparedStatement stmt = connection.PreparedStatement("SELECT * from Accounts where
AccountId = ?");
    stmt.setInt(1, accountId);
    ResultSet accountRS = stmt.executeQuery();
    return accountRS;
}
```

Record References are Now Filtered and Indirect

```
public ResultSet getAccountInfo(request req){
    int accountIndex = Integer.parseInt(req.getParameter("accountId"));
    int realAccountId = userAccountList.get(accountIndex);
    int userId = req.getSession().getAttribute("userId");
    PreparedStatement stmt = connection.PreparedStatement("SELECT * from Accounts where
AccountId = ? AND UserId = ?");
```

```
    stmt.setInt(1, realAccountId);
    stmt.setInt(2, userId);
    ResultSet accountRS = stmt.executeQuery();
    return accountRS;
}
```

Excessive Data Exposure

風險

可能發生什麼問題

API 通常在回應時向客戶端提供物件，供其使用。有時，這些物件可能包含的訊息超過客戶端需要或打算使用的訊息。如果返回給客戶端的物件有這些多餘數據並且該數據是敏感資訊，它就會暴露給 API 的潛在惡意客戶端。

原因

如何發生

API 返回一個具有潛在敏感資訊字段的物件，而沒有排除、過濾或取消所述敏感資訊 - 就會在 API 回應中將其暴露。

一般建議

如何避免

- 從 API 返回保存數據的物件時，請始終考慮返回數據的類型和上下文 - 例如 API 的使用者是否需要它，以及它是否敏感
- 選擇將允許的數據列入白名單從而控制數據流並去除多餘數據

程式碼範例

Java

Exposing a Sensitive Field in a Spring REST API Response

```
// POJO with Sensitive Data
@Entity
public class User {
    @Id
    @GeneratedValue
    private Long id;
    private String username;
    // Field will be exposed if User object is returned as-is from API:
    private String encryptedPassword;
    // ... public constructors getters and setters ... //
}

// Spring REST Controller Mapped Method
@GetMapping("/users/{id}")
User findOne(@PathVariable Long id) {
    User user = repository.findById(id).orElseThrow(() -> new UserNotFoundException(id));
    return user;
}
```

Using a DTO and ModelMapper To Whitelist Desired Output Fields in a Spring REST API

```
// POJO with Sensitive Data
@Entity
public class User {
    @Id
    @GeneratedValue
    private Long id;
```

```
    private String username;
    private String encryptedPassword;
    // ... public constructors getters and setters ... //
}

// DTO without Sensitive Data
public class UserDTO {
    private Long id;
    private String username;
    // ... public constructors getters and setters ... //
}

// Spring REST Controller Mapped Method
@GetMapping("/users/{id}")
User findOne(@PathVariable Long id) {
    User user = repository.findById(id).orElseThrow(() -> new UserNotFoundException(id));
    UserDTO userDTO = modelMapper.map(user, UserDTO.class);
    return userDTO;
}
```

Spring Annotation Used to Exclude A Field from JSON Entirely - Can Also Be Set on Getter Individually to Allow Setting a Value While Preventing Exposure

```
// POJO with Sensitive Data
@Entity
public class User {
    @Id
    @GeneratedValue
    private Long id;
    private String username;
    @JsonIgnore
    private String encryptedPassword;
    // ... public constructors getters and setters ... //
}
```

Cleartext Submission of Sensitive Information

風險

可能發生什麼問題

當敏感且個人的詳細資訊（如密碼、社會安全號碼、信用卡資料以及其他形式的PII（個人身份可識別資訊））在網路上傳輸時，必須始終受到保護。在未加密的通道上發送這些隱私資料，例如未使用SSL/TLS或其他形式的加密，可能會揭露使用者的機密資訊並使其面臨冒充、身份竊取和金融詐欺的風險。

如果SSL/TLS通道在前端網頁伺服器、反向代理或類似伺服器上終止，則可以忽略此問題。

原因

如何發生

應用程式以多種方式處理敏感和隱私資訊。在某一點上，這些機密資料被傳送到網路上，但是應用程式沒有使用SSL/TLS或任何其他安全協議，並且在將其發送到不受保護的通道之前沒有確保資料被加密。

一般建議

如何避免

- 每次透過網路傳輸資料時，皆需保護所有PII和其他敏感資料。
- 在傳輸敏感資料時使用SSL/TLS。或者，還可以使用其他加密協議，如IPsec或SSH。
- 重新考慮應用程式是否需要這些個人詳細資訊。
- 在Web應用程式中，不要在無法確保通道安全的情況下，將個人資料輸出。
- 不要直接將個人資料寫入Standard Socket。取而代之的是，請使用SSLSocket確保通道使用SSL/TLS。

程式碼範例

Java

Using Standard Socket (No Encryption) for a Basic Authentication Server

```
public void runServer() {
    ServerSocket server = new ServerSocket(PORT);
    Socket client;

    while (true) {
        client = server.accept();
        MyUser user = handleRequest(client.getInputStream());

        PrintWriter output = new PrintWriter(server.getOutputStream());
        output.println(user.AccountId);
        output.flush();
    }
}
```

Using Encrypted SSLSocket for a Basic Authentication Server

```
public void runServer() {
    try {
        SSLServerSocketFactory factory =
            (SSLServerSocketFactory) SSLServerSocketFactory.getDefault();
```

```
        ServerSocket server = factory.createServerSocket(PORT);
        Socket client;

        while (true) {
            client = server.accept();
            MyUser user = handleRequest(client.getInputStream());

            PrintWriter output = new PrintWriter(server.getOutputStream());
            output.println(user.AccountId);
            output.flush();
        }
    }
    catch (IOException ex) {
        handleException(ex);
    }
    finally {
        if (output != null) output.close();
        if (client != null)
            if (!client.isClosed()) client.close();
        if (server != null)
            if (!server.isClosed()) server.close();
    }
}
```

Authenticating Server to Server via HTTP

```
public static boolean authenticateServerToServer(String username, String password) throws
IOException {
    String stringUrl = "http://" + HOSTNAME + "/" + URI_PATH;
    URL url = new URL(stringUrl);
    HttpURLConnection conn = (HttpURLConnection)url.openConnection();
    conn.setRequestMethod("POST");
    conn.setDoOutput(true);

    String postParameters  = "username=" + username + "&password=" + password;
    byte[] postRequestBytes = postParameters.getBytes();
    OutputStream os = conn.getOutputStream();
    os.write(postRequestBytes);
    os.flush();
    os.close();
    return conn.getResponseCode() == HttpURLConnection.HTTP_OK;
}
```

Authenticating Server to Server via HTTPS

```
public static boolean authenticateServerToServer(String username, String password)  throws
IOException {
    String stringUrl = "https://" + HOSTNAME + "/" + URI_PATH;
    URL url = new URL(stringUrl);
    HttpsURLConnection conn = (HttpsURLConnection)url.openConnection();
    conn.setRequestMethod("POST");
    conn.setDoOutput(true);

    String postParameters  = "username=" + username + "&password=" + password;
    byte[] postRequestBytes = postParameters.getBytes();
    OutputStream os = conn.getOutputStream();
    os.write(postRequestBytes);
    os.flush();
    os.close();
    return conn.getResponseCode() == HttpURLConnection.HTTP_OK;
```

```
}
```

SSRF

風險

可能發生什麼問題

攻擊者可以利用此漏洞發出任何來源為應用伺服器的請求。這可以被利用來掃描內部服務、代理攻擊受保護的網路、繞過網路控制、下載未經授權的文件、訪問內部服務及管理介面以及可能控制請求內容甚至竊取伺服器憑證。

原因

如何發生

應用程式接收從使用者端傳來的URL，然後將此當作請求傳送給另一個遠端伺服器。
然而，攻擊者可以在請求中注入任意的URL，造成應用程式連線至任意一個攻擊者想要的伺服器。所以，攻擊者可以濫用該應用程式來訪問本來無法訪問的服務，而表面上這個請求來自應用伺服器。

一般建議

如何避免

- 不直接利用使用者輸入對任意服務進行連線。
- 如果可以，應用程式應該讓使用者的瀏覽器直接檢索所需的資訊。
- 如果應用程式需要在伺服器上代理請求，明確地將允許的URL列入白名單，並且不包括任何敏感的伺服器資訊。

程式碼範例

Java

Retrieve and Display Contents of URL

```
protected void doGet(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {
  if (request.getParameterMap().containsKey("url")) {
    String url = request.getParameter("url");
    PrintWriter out = response.getWriter();
    URL u = new URL(url);
    InputStreamReader sr = new InputStreamReader(u.openConnection().getInputStream());
    BufferedReader reader = new BufferedReader(sr);
    String line = reader.readLine();
    while (line != null) {
      out.write(line);
      line = reader.readLine();
    }
  }
}
```

Validate and Redirect User's Browser

```
protected void doGet(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {
  if (request.getParameterMap().containsKey("url")) {
    String url = request.getParameter("url");
    if (url.startsWith("/") && !url.startsWith("//")) {
      response.sendRedirect(url);
    } else {
```

```
        response.sendRedirect("/");
      }
    }
  }
```

Unchecked Input for Loop Condition

風險

可能發生什麼問題

攻擊者可能會輸入非常高的值，從而可能導致阻斷式服務攻擊 (DoS)。

原因

如何發生

應用程式在執行一些重複的任務時，根據使用者的輸入來定義循環次數。一個非常高的值可能會導致應用程式陷入循環，將無法繼續進行其他操作。

一般建議

如何避免

理想情況下，不使用使用者提供的循環設定。如果有必要的話，使用者輸入必須先驗證且應限制其範圍。

程式碼範例

Java

Loop Condition Is Not Bounded By Any Value

```
protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {

    int loopCount = 0;
    try{
        loopCount = Integer.parseInt(request.getParameter("loopCount"));
    } catch(NumberFormatException e){
        return DEFAULT_VAL;
    }
    for(int i=0; i < loopCount; i++){
        //Do Something
    }
}
```

Loop Condition is Bounded With MAX_LOOPS

```
protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {

    int loopCount = 0;
    try{
        loopCount = Integer.parseInt(request.getParameter("loopCount"));
    } catch(NumberFormatException e){
        return DEFAULT_VAL;
    }
    if(loopCount > MAX_LOOPS){
        loopCount = MAX_LOOPS;
    }
    for(int i=0; i < loopCount; i++){
        //Do Something
```

```
        }
    }
```

Unsafe Object Binding

風險

可能發生什麼問題

不安全地將物件綁定到request可能會使未預期的設定器暴露給遠程攻擊者，使其能夠通過將設定器廣泛綁定到傳入的request來直接訪問物件、屬性甚至物件中的物件。

原因

如何發生

使用內建於MVC控制器中的物件綁定方法，會將所有公開的設定器暴露出來，以便輕鬆地將使用者在表單中提交的值與它們所要創建或修改的物件和屬性進行連接。這種方法使應用程式能夠跳過為了解析使用者輸入值而必須逐個手動設定的樣板程式碼。

然而，這也可能對應用程式的邏輯和流程構成重大風險 - 當以這種方式盲目地批量綁定物件時，也可能意外地暴露出未預期的物件或屬性，從而被攻擊者篡改。

一般建議

如何避免

- 審查所有大量指定的物件，以確保這種方法不會無意間暴露出意外的公開設定器或建構函式。
- 確保必要時，應用程式程式碼正確限制對屬性和物件的訪問權限。
- 考慮從物件綁定方法轉向更細緻的方法，只有明確設定值，以防止意外地將未預期的值暴露出來並受到暗中修改。

程式碼範例

Java

Unsafe Object Binding via Spring ModelAttribute

```
//Item Bean:
public class Item {
      private String id;
    private String itemName;
    private String price;
    private String shippingAddress;
    private User buyer;
      //Public setters/getters:
    [..]
}
//User Bean:
public class User {
      private String id;
    private String userName;
    private String password;
      //Public setters/getters:
    [..]
}

//Item Controller:
@Controller
public class ItemController {
      @RequestMapping(value="saveItem", method = RequestMethod.POST)
      public String saveItem(@ModelAttribute("item") Item item, ModelMap model) {
            db.save(item); //If the parameter "user.password=hacked!!" is added, the password
for the user is changed to "hacked!!".
```

```
            return "saveItemView";
        }
    }
```

Heap Inspection

風險

可能發生什麼問題

應用程式在未加密的memory中存儲的所有變數都可能被主機特權User(privileged access)未經授權的檢索。例如，特權攻擊者可以對正在執行的process掛上debugger，也可能從swapfile或crash dump file中檢索process's memory。
一旦攻擊者在Memory中找到User的密碼，就可以輕鬆的假冒User進入系統。

原因

如何發生

字串變數是不變的(immutable) - 換句話說，一旦分配了字串變數，就無法更改或刪除其值。因此，這些字串可能會無限期的留存在memory中，而且可能分散在多個位置中，直到垃圾收集器(garbage collector)將其刪除。敏感資訊，例如密碼，將作為明文在memory中暴露，無法控制其生命週期。

一般建議

如何避免

- 不要將敏感資訊(如password或encryption key)以明文形式存儲在memory中，時間再短都不要。
- 建議使用專為store encrypted memory設計的Class。
- 或者，將機敏資訊存在可變類型中(如byte array)，使用完立即將array中每個byte位歸零。

- 在Java中，不要將密碼儲存在不可變的string中 - 建議使用encrypted memory object，例如SealedObject。

程式碼範例

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private String password;

  public void setPassword(String password)
 {
      this.password = password;
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
```

```
  private SealedObject password;

  public void setPassword(Character[] input)
 {
     Key key = getKeyFromConfiguration();
            Cipher c = Cipher.getInstance(CIPHER_NAME);
            c.init(Cipher.ENCRYPT_MODE, key);
            List<Character> characterList = Arrays.asList(input);
            password = new SealedObject((Serializable) characterList, c);
            Arrays.fill(input, '\0'); // Zero out input. Will also overwrite the values in
characterList by reference.
   }
}
```

Improper Exception Handling

風險

可能發生什麼問題

●攻擊者可能會導致應用程式異常的崩潰，且造成拒絕服務(DoS)攻擊。 ●應用程式可能發生偶發性的崩潰。

原因

如何發生

'應用程式執行如資料庫或文件存取，這可能會引發一些異常狀況。若應用程式未妥善處理異常狀況，可能會當機。

一般建議

如何避免

可能導致異常的任何方法應包裝在一個try-catch區塊: ● 明確地處理預期的異常 ●包含一個預設的解決方案，以處理突發異常

程式碼範例

Java

Loading a Library without Catching

```
public static void loadLib() {
      System.loadLibrary(LIB_NAME); // If LIB_NAME does not exist, an unhandled exception will
be thrown
}
```

Handle All Possible Exceptions within the Error-Prone Method

```
public static void loadLib() {
      try {
            System.loadLibrary(LIB_NAME);
    } catch (SecurityException se) {
                  // Handle SecurityException
      } catch (UnsatisfiedLinkError sle) {
                  // Handle UnsatisfiedLinkError
      } catch (NullPointerException npe) {
                  // Handle NullPointerException
      }
}
```

Aggregate Potential Exceptions to Calling Code

```
public static void loadLib() throws UnsatisfiedLinkError, NullPointerException,
SecurityException {
      System.loadLibrary(LIB_NAME);
}
```

Improper Resource Access Authorization

風險

可能發生什麼問題

未經授權的操作可能允許攻擊者將惡意內容或程式碼寫入檔案、資料庫和其他輸入/輸出，或讀取敏感的輸入/輸出內容。此問題的影響因實作方式而異，但可能造成以下情況：

- 遠端程式碼執行：若攻擊者能夠將惡意資料注入可寫入的輸入/輸出，該資料可能會被編譯為程式碼，從而執行惡意程式碼
- 覆寫或洩漏設定檔案
- 危害儲存數據的機密性或完整性

原因

如何發生

程式碼中的邏輯流程觸發了I/O 操作，但未經授權。如果攻擊者能夠觸發它，則容易遭受攻擊。

一般建議

如何避免

確認邏輯流程是會受到使用者輸入或行為的影響時，請始終確保使用者有授權觸發它們。

程式碼範例

Java

Writing to File Without Any Authorization Checks

```
Part filePart = request.getPart("file");
if (filePart != null) {
      InputStream filecontent = null;
      filecontent = filePart.getInputStream();
      Path path = Paths.get(filename);
      byte[] contentByteArray = new byte[filecontent.available()];
      filecontent.read(contentByteArray);
      Files.write(path, contentByteArray);
}
```

Using a Basic Authorization Check Based on Session Variables

```
HttpSession session = request.getSession();
String role = (String)session.getAttribute("role");
if (role.equals(ADMIN)) {
      Part filePart = request.getPart("file");
      if (filePart != null) {
            InputStream filecontent = null;
            filecontent = filePart.getInputStream();
            Path path = Paths.get(filename);
            byte[] contentByteArray = new byte[filecontent.available()];
            filecontent.read(contentByteArray);
            Files.write(path, contentByteArray);
      }
```

```
}
```

Information Exposure Through an Error Message

風險

可能發生什麼問題

透露關於程式的環境、使用者或相關資訊 (例如：stack trace) 將會讓攻擊者找到其他的缺失也幫助攻擊者來發起攻擊。這也可能會使機密資料洩露，例如：密碼或資料庫欄位。

原因

如何發生

應用程式以不安全的方式處理例外(exception)，包括直接在 error message 中顯示完整的原始詳細訊息。這在幾個狀況下都可能會發生：不處理 exception；直接將 exception 輸出到頁面或檔案中；顯式return exception 物件；設定檔設定不嚴謹。這些 exception 細節可能包含機密資訊，並隨著 Runtime Error 而流出。

一般建議

如何避免

- 不將 excecption 資訊直接輸出或是透露給使用者，建議回傳一個制式化的錯誤訊息。Exception細節則應記錄於Log機制內。
- 任何會拋出 exception 的函式都應該要被包在處理 exception 的區塊內，而處理的方式有:
  - 明確的處理預期內的exception。
  - 包含了一個預設的解決方式來處理無預期的exceptions。
- 設定一個全域處理器來避免無處理的錯誤被送至使用者端。

程式碼範例

Java

Handle Exception by Printing To Output

```
private void wrapCallToDB_Unsafe(HttpServletRequest request)
            throws ServletException, IOException {
      String paramValue = request.getParameter("Param");

      try {
            callDbProc(paramValue);
      } catch (SQLException ex) {
            ex.printStackTrace();
      }
}
```

Write Exception Details to Log, Send Generic Error Message

```
private void wrapCallToDB_SafePrintToLog(HttpServletRequest request)
            throws ServletException, IOException {
      String paramValue = request.getParameter("Param");

      try {
```

```
            callDbProc(paramValue);
        } catch (SQLException ex) {
            writeExceptionToLog(ex);
            System.err.println("Database Error, see log for details");
        }
    }
```

Incorrect Permission Assignment For Critical Resources

風險

可能發生什麼問題

具有危險權限的檔案可能允許攻擊者從這些檔案的內容中擷取敏感資訊、篡改其內容或潛在地執行它們。

原因

如何發生

檔案或目錄被創建時具有危險的權限，可能是有設置這些權限，不然就是依賴於不安全的默認權限。

一般建議

如何避免

- 請始終明確設定檔案的權限
- 請勿將危險權限設定在檔案上
    - 當決定使用者可以讀取、寫入或執行哪些檔案時，請始終考慮最小權限原則，並且只在必要時授予這些權限

程式碼範例

Java

Writing A File with Implicit Permissions

```
File tempFile = File.createTempFile(TEMP_FILE_PREFIX,TEMP_FILE_SUFFIX, new
File(TEMP_FOLDER));
FileWriter fw = new FileWriter(tempFile);
fw.write(CONTENT);
```

Writing A File with Explicit Permissions

```
File tempFile = File.createTempFile(TEMP_FILE_PREFIX,TEMP_FILE_SUFFIX, new
File(TEMP_FOLDER));
FileWriter fw = new FileWriter(tempFile);
tempFile.setExecutable(false);
tempFile.setReadable(true);
tempFile.setWritable(true);
fw.write(CONTENT);
```

Integer Overflow

風險

可能發生什麼問題

算術溢出將導致未定義的行為和意外影響，例如資料損壞（例如值環繞，其中最大值變為最小值）；系統崩潰；無限迴圈；邏輯錯誤，例如繞過安全機制；資料截斷或遺失；當使用溢出的數值執行記憶體操作時，甚至緩衝區溢位導致任意程式碼執行。

原因

如何發生

所有數字資料類型都有按位元表示。 如果在算數運算之後，一個值超過了它的位元表示的位數，那麼被添加的最高有效數字將被簡單地截斷，截斷後保留的值是環繞操作的剩餘部分 - 這被稱為"算術溢出"或其常見的誤稱 - "整數溢出"，這是誤導性的，因為這適用於許多其他類型。 如果可以溢出的資料類型低於它們的最小值，它們將在通常稱為下溢的情況下反向回繞。

例如，如果一個無符號的 32 位元整數設置為 4,294,967,295 並且 1 是 如果它是一個帶符號的 32 位元整數，值為 2,147,483,647 並且添加 1，它將溢出並返回到 0。

為了確保程式碼正確性，檢查必須使值在預期範圍內，以便算數運算的結果不會溢出或下溢。

一般建議

如何避免

- 在對可能包含任何值的資料執行算數運算時，考慮添加檢查以確保此資料在這些運算的乘積不會導致上溢或下溢的範圍內。
- 考慮為所有算數運算創建包裝器，以便對異常情況進行特定處理；例如，如果檢查顯示已經或將要發生溢出，則拋出異常。

程式碼範例

Java

Addition Vulnerable to Overflow and Underflow

```
public static int vuln_addition1(int a, int b)
{
  return a + b;
}
```

Incorrect Check - Vulnerable to Underflow, and Incorrect Negative Value Handling

```
public static int vuln_addition2(int a, int b)
{
  if(a+b < 0)
   throw new RuntimeException ("Integer overflow!");
  return a + b;
}
```

```
```

Addition That will Throw Exception in Case of Overflow or Underflow

```
public static int safe_addition1(int a, int b)
{
   if (a > 0 && b > 0 && a + b < 0)
     throw new RuntimeException ("Integer overflow!");

   if (a < 0 && b < 0 && a + b > 0)
     throw new RuntimeException ("Integer underflow!");

   return a+b;
}
```

Using a bigger data type to hold all the possible result values

```
public static short safe_addition2(short a, short b)
{
  int tot = a+b;
  if(tot > Short.MAX_VALUE)
   return Short.MAX_VALUE;

  if(tot < Short.MIN_VALUE)
   return Short.MIN_VALUE;

  return (short)tot;
}
```

Log Forging

風險

可能發生什麼問題

攻擊者可以偽造安全敏感動作的稽核記錄，並留下虛假的稽核軌跡，可能會牽連無辜的使用者或隱藏事件。

原因

如何發生

當應用程式執行安全與敏感性的動作時，會記錄稽核日誌(audit log)。由於稽核日誌中包含使用者輸入的內容，這些內容既沒有經過驗證資料類型，也沒有經過適當的處理，因此該輸入可能包含假資訊，假裝成合法的稽核日誌資料。

一般建議

如何避免

1. 不管來源為何所有輸入都要進行驗證，且驗證要根據白名單：只接受符合指定格式的資料，而不是使用黑名單。請檢查：
    - 資料型態(Data type)
    - 資料大小(Size)
    - 資料範圍(Range)
    - 資料格式(Format)
2. 驗證不能取代 encode。不論來源為何要將所有的外部資料進行 encode 後才能寫進 Log。
3. 使用安全的 Logging 機制。

程式碼範例

Java

User Input Affects Logging

```
protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {

    String color = request.getParameter("color");
    logger.info("{} was picked", color);
      if colorList.contains(color){
      // Handle Response
    }else{
      // Handle Response
    }
}
```

User Input Encoded Prior Logging

```
protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {

    String color = request.getParameter("color");
      cleanColor = color.replace('\t', '_').replace('\n', '_').replace('\r', '_');
    logger.info("{} was picked", cleanColor);
```

```
      if colorList.contains(cleanColor){
       // Handle Response
     }else{
       // Handle Response
     }
 }
```

Integer Underflow

風險

可能發生什麼問題

算術溢出將導致未定義的行為和意外影響，例如資料損壞（例如值環繞，其中最大值變為最小值）；系統崩潰；無限迴圈；邏輯錯誤，例如繞過安全機制；資料截斷或遺失；當使用溢出的數值執行記憶體操作時，甚至緩衝區溢位導致任意程式碼執行。

原因

如何發生

所有數字資料類型都有按位元表示。 如果在算數運算之後，一個值超過了它的位元表示的位數，那麼被添加的最高有效數字將被簡單地截斷，截斷後保留的值是環繞操作的剩餘部分 - 這被稱為"算術溢出"或其常見的誤稱 - "整數溢出"，這是誤導性的，因為這適用於許多其他類型。 如果可以溢出的資料類型低於它們的最小值，它們將在通常稱為下溢的情況下反向回繞。

例如，如果一個無符號的 32 位元整數設置為 4,294,967,295 並且 1 是 如果它是一個帶符號的 32 位元整數，值為 2,147,483,647 並且添加 1，它將溢出並返回到 0。

為了確保程式碼正確性，檢查必須使值在預期範圍內，以便算數運算的結果不會溢出或下溢。

一般建議

如何避免

- 在對可能包含任何值的資料執行算數運算時，考慮添加檢查以確保此資料在這些運算的乘積不會導致上溢或下溢的範圍內。
- 考慮為所有算數運算創建包裝器，以便對異常情況進行特定處理；例如，如果檢查顯示已經或將要發生溢出，則拋出異常。

程式碼範例

Portability Flaw Locale Dependent Comparison

風險

可能發生什麼問題

對字串型態的變數進行處理時沒有指定語系，會導致非預期的結果。造成驗證繞過攻擊、格式化字串攻擊。
以及其他可能的，以字串為攻擊基礎的漏洞：XSS、SQL Injection、DoS

原因

如何發生

不同語系的符號、字元、日期或數字，其排列方式、寫法不盡相同。但有許多的方法在使用時，不會強制開發者設定語系，而使用預設的語系設定。
然而，依賴預設設定，可能會導致非預期的結果。例如大小寫轉換：

```
public String tagProcessor(String tag){
      if (tag.toUpperCase().equals("SCRIPT")){
            return null;
      }
      //...
}
```

若語系為Turkish(土耳其語)，則小寫英文字母'i'將會被轉換為"上方帶點的大寫拉丁字母 İ"(Unicode編號 0130)，顯然與預期的結果'I'不同，因而發生預期外的結果。

一般建議

如何避免

- 永遠使用locale-sensitive功能來處理特定字串。
- 在Java中，推薦使用Locale.ROOT進行語系設定。

程式碼範例

Java

Locale Ignorant String Comparison

```
private bool validateInput(String input) {
    if (input.toUpperCase().indexOf("SCRIPT") < 0)
        return true;    // Input string does not contain any form of SCRIPT
    else
        return false;
}
```

Locale-Neutral String Comparison

```
private bool validateInput(String input) {
    if (input.toUpperCase(Locale.ROOT).indexOf("SCRIPT") < 0)
        return true;    // Input string does not contain any form of SCRIPT
    else
        return false;
}
```

Race Condition Format Flaw

風險

可能發生什麼問題

資源競爭可能導致錯誤，無效的值或意外行為可能導致拒絕服務。最糟糕的情況是，它可能允許攻擊者通過重新執行可控制的資源競爭來檢索資料或繞過安全管控，直到它對其有利為止。

原因

如何發生

當多個並行邏輯處理使用一個公共的、單一的資源實例時，就會發生資源競爭。如果這些邏輯處理試圖在沒有及時管理系統 (如鎖) 的情況下檢索和更新資源，則會發生資源競爭。
發生資源競爭的一個例子是，可能會將某個值返回流程以進行進一步編輯的資源，然後由第二個更新，從而導致原始流程的資料不再有效。一旦原始流程將不正確的值編輯並更新回資源中，第二個流程的更新將被覆蓋並丟失。

一般建議

如何避免

當跨應用程式在並行流程之間共享資源時，確保這些資源是thread-safe的，或者實現鎖定機制以確保預期的並行活動。

程式碼範例

Java

Testing Static Int Concurrency - Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
	}

	public static class decrementCounter extends Thread {
	    public void run() {
		counter--;
	    }
	}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
	public static int counter = 0;
	public static Object lock = new Object();

	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) { // because of proper locking, this condition is never false
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); // Never reached
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		synchronized (lock) {
			counter++;
		}
	    }
	}

	public static class decrementCounter extends Thread {
	    public void run() {
		synchronized (lock) {
			counter--;
		}
	    }
	}
```

Testing Formatter Race Condition - Java Formatters are Not Thread Safe

```
	static Locale defaultLocale = new Locale("en", "US", "USD");
	static NumberFormat numberFormatter = NumberFormat.getCurrencyInstance(defaultLocale);

	public static class CurrencyFormatRunnable implements Runnable {

		double money;
		public CurrencyFormatRunnable(Object parameter) {
		    this.money = (double)parameter;
		}

		// Format a double as a USD string; if formatter result does not match a known value (100.0 -> $100.00, 50.0 -> $50.00),
		// as expected with a Race Condition, a warning is printed and the application closes.
		public void run() {
			String formattedMoney;
			formattedMoney = numberFormatter.format(money);
			if (!formattedMoney.equals("$"+money+"0")) {
				System.out.println("Formatted number was $" + money + ", but the result was " + formattedMoney +"!");
				System.exit(1);
		/*	Potential outputs:
	*	Formatted number was $50.0, but the result was $100.00!
```

```
             *       Formatted number was $50.0, but the result was 100.00!
                                    *       Formatted number was $100.0, but the result was $50.00!
             *       Formatted number was $100.0, but the result was $$50.00!
             *       Note the erroneous behavior with completely incorrect values, like $$50.00, which
occurs
             *       because the string is read as a new value is written
             */

                        }
                    }
                }

      public static void start() throws InterruptedException {
             Runnable m1;
             Runnable m2;
             Thread t1;
             Thread t2;
             while(true) {
                    m1 = new CurrencyFormatRunnable((double)100.00);
                    m2 = new CurrencyFormatRunnable((double)50.00);
                    t1 = new Thread(m1);
                    t2 = new Thread(m2);
                    // Attempt to concurrently use the formatter
                    t1.start();
                    t2.start();

                    t1.join();
                    t2.join();
             }
      }
```

Formatter Race Condition Mitigated, with Each Thread Using Its Own Instance of Java Formatter

```
      public static class CurrencyFormatRunnable implements Runnable {
                double money;
                public CurrencyFormatRunnable(Object parameter) {
                    this.money = (double)parameter;
                }

                public void run() {
                       String formattedMoney;
                    Locale defaultLocale = new Locale("en", "US", "USD");
                    NumberFormat numberFormatter =
NumberFormat.getCurrencyInstance(defaultLocale);
                       formattedMoney = numberFormatter.format(money);
                       if (!formattedMoney.equals("$"+money+"0")) {
                                System.out.println("Formatted number was $" + money + ", but
the result was " + formattedMoney +"!");
                       // This is never reached
                                System.exit(1);
                       }
                }
             }

      public static void start() throws InterruptedException {
             Runnable m1;
             Runnable m2;
             Thread t1;
             Thread t2;
             while(true) {
                    m1 = new CurrencyFormatRunnable((double)100.00);
                    m2 = new CurrencyFormatRunnable((double)50.00);
                    t1 = new Thread(m1);
                    t2 = new Thread(m2);
                    // Attempt to concurrently use the formatter
```

```
                t1.start();
                t2.start();

                t1.join();
                t2.join();
            }
        }
```

Serializable Class Containing Sensitive Data

風險

可能發生什麼問題

敏感資訊可能透過可序列化物件洩漏。

原因

如何發生

序列化是將記憶體中的物件轉換為序列化形式的過程，例如位元串、XML、JSON等。它通常用於傳輸或儲存資料，這可能會在某些時候暴露其內容。不建議將任何敏感資訊保存在序列化物件中，因為根據其定義，它們能以可復原且可讀的格式儲存或傳輸這些資料。

一般建議

如何避免

- 不要將敏感資訊存放在序列化物件中。
- 如果絕對需要儲存或傳輸包含敏感資訊的序列化物件，請確保不會危及內容的方式進行。在處理包含敏感資訊的序列化物件時，請始終考慮資料靜態與資料傳輸的原則。

程式碼範例

Java

"Purchase" Class Contains Credit Card Information, and Implements Serializable, Implying Credit Card will be Transmitted or Stored

```
public class Purchase implements Serializable {
      private String creditCard;
    private Date expDate;
      private int CCV;
      // .. //
}
```

Stored Log Forging

風險

可能發生什麼問題

攻擊者可以偽造安全敏感動作的稽核記錄，並留下虛假的稽核軌跡，可能會牽連無辜的使用者或隱藏事件。

原因

如何發生

當應用程式執行安全與敏感性的動作時，會記錄稽核日誌(audit log)。由於稽核日誌中包含使用者輸入的內容，這些內容既沒有經過驗證資料類型，也沒有經過適當的處理，因此該輸入可能包含假資訊，假裝成合法的稽核日誌資料。

一般建議

如何避免

1. 不管來源為何所有輸入都要進行驗證，且驗證要根據白名單：只接受符合指定格式的資料，而不是使用黑名單。請檢查：
    - 資料型態(Data type)
    - 資料大小(Size)
    - 資料範圍(Range)
    - 資料格式(Format)
2. 驗證不能取代 encode。不論來源為何要將所有的外部資料進行 encode 後才能寫進 Log。
3. 使用安全的 Logging 機制。

程式碼範例

Java

Logging Untrusted Data

```
private int readUserId(ResultSet rs) {
    String dbValue = rs.getString("UserId");
    int userId = 0;

    try {
        userId = Integer.parseInt(dbValue);
    } catch (NumberFormatException nfe) {
        log.error("User Id: " + userId + " raised an error: " + nfe.getMessage());
    }
    return userId;
}
```

Logging Only Sanitized Data

```
private int readUserId(ResultSet rs) {
    String dbValue = rs.getString("UserId");
    int userId = 0;

    try {
        userId = Integer.parseInt(dbValue);
```

```
    } catch (NumberFormatException nfe) {
        log.error("User Id: " + userId.replace('\r', '').replace('\n', '') +
                  " raised an error: " + nfe.getMessage());
    }
    return userId;
}
```

Use Of Hardcoded Password

風險

可能發生什麼問題

直接寫入的密碼會造成密碼的洩漏。如果攻擊者可以取得程式原始碼，他便可取得密碼，並利用它們來冒充合法使用者。攻擊者可以冒充自己是應用程式的末端使用者，或假裝應用程式登入遠端系統，例如資料庫或網路服務。 一旦攻擊者成功冒充使用者或應用程式，他便可取得完整的控制權，並做到任何能做的事。

原因

如何發生

應用程式程式庫含有嵌入在原始碼內的字串型態的密碼。這個直接寫入的值被直接使用或是用來和使用者輸入做驗證比對。或驗證末端程式連線到遠端系統（如資料庫或網路服務）。 攻擊者只需要取得原始碼即可揭露被直接寫入的密碼。同樣的，攻擊者也可以進行逆向工程反編譯應用程式的二進位程式碼，並簡單的取得寫入的密碼。一旦被發現，攻擊者可以很容易的使用這個密碼進行假冒攻擊，無論是對應用程式或遠端系統。 此外，一旦被偷取，將無法簡單的更改來預防更進一步的濫用，除非應用程式重新編譯過。此外，這個應用程式如果被分配到多個系統，從一個系統竊取的密碼可以自動允許在所有被部屬的系統上使用。

一般建議

如何避免

不要將機密資料直接寫入程式碼內。 特別是，用戶的密碼應該儲存在資料庫或是目錄服務，並使用夠強的雜湊演算法進行加密保護。(如 bcrypt, scrypt, PBKDF2, or Argon2)。不要用直接寫入的值進行比對。 系統密碼應該儲存在配置文件或資料庫，並以強大的加密方法保護（例如AES-256）。加密金鑰應該被安全的保護。

程式碼範例

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;
}
```

Spring Missing Content Security Policy

風險

可能發生什麼問題

Content-Security-Policy header 強制內容的來源，例如腳本的來源、嵌入（子）框架、嵌入（父）框架或圖像，被當前網頁信任和允許；如果在網頁中，內容的來源不遵守嚴格的內容安全性原則，瀏覽器會立即拒絕該內容。 未定義策略可能會使應用程式的使用者暴露於跨網站腳本 (XSS) 攻擊、點擊劫持攻擊、內容偽造等。

原因

如何發生

Content-Security-Policy header被現代瀏覽器用作可信內容來源的指示器，包括媒體、圖像、腳本、框架等。 如果未明確定義這些策略，則默認瀏覽器行為將允許不受信任的內容。

應用程式創建 Web response，但未正確設置 Content-Security-Policy 標頭。

一般建議

如何避免

建議根據業務需求和外部檔案託管服務的部署，明確地設定合適的CSP標頭(框架、腳本、表單、腳本、媒體、圖片等...)，具體來說，不要使用萬用字元"*"來指定這些策略，因為這將允許來自外部的任何資源內容。

CSP可以在網頁應用程序代碼中明確定義，作為由web-server 配置所管理的標頭，或在HTML<head>下的 <meta>標籤中定義。

程式碼範例

Java

Adding CSP Header Using Spring Security Java Configuration

```
@Configuration
public class SpringSecurityConfig extends WebSecurityConfigurerAdapter {

    @Override
    protected void configure(HttpSecurity http) throws Exception {
        // Add CSP headers
        http.headers()
            .contentSecurityPolicy("script-src 'self' https://example.com; object-src
https://example.com; report-uri /csp-report-endpoint/");
    }
}
```

XML

Adding CSP Header Using Spring Security XML Configuration

```
<http>
   <!-- ... -->

    <headers>
```

```
    <content-security-policy policy-directives="script-src 'self' https://apis.example.com">
        </content-security-policy>
    </headers>
</http>
```

Spring Missing Expect CT Header

風險

可能發生什麼問題

如果未能設置 Expect-CT 標頭並向其提供 "enforce" 參數和至少為一年的合理 "max-age" 值，可能會讓用戶容易受到"中間人"攻擊。

原因

如何發生

使用 SSL/TLS 時，瀏覽器會根據客戶端的已識別 CA（證書頒發機構）列表來驗證伺服器在連接握手期間發送的證書。該模型的安全功能將信任從伺服器轉移到 CA。
聲明 Expect-CT 標頭將使受支持的瀏覽器使用證書透明度來檢測 CA 完整性是否受到危害，並根據標頭參數中的定義來報告和/或強制執行安全連接。
使用帶有 Expect-CT 的證書透明度和正確參數，可避免中間人攻擊。

一般建議

如何避免

- 在設置 Expect-CT 標頭之前 - 考慮其可能產生的影響：
  - 強制執行 Expect-CT 將阻止未來使用 HTTP，這可能會阻礙某些測試
  - 禁用 Expect-CT 並非易事，因為一旦在網站上將其禁用，也必須在瀏覽器上將其禁用
- 通過設置沒有 'enforce' 標誌的 Expect-CT 標頭來測試您的環境以檢查是否存在證書問題 - 然後使用 'enforce' 標誌
- 在應用程式程式碼中顯式設置 Expect-CT 標頭，或使用 Web 伺服器配置。
- 確保 Expect-CT 標頭的 "max-age" 值設置為 31536000 以確保證書透明度的使用嚴格執行至少一年。
- 如果通過配置添加此標頭，請確保此配置適用於整個應用程式。

默認情況下，Spring Security 不會添加此標頭。

程式碼範例

XML

Adding Expect_CT Header Using Spring Security's XML Configuration

```
<http>
        <headers>
               <header name="Expect-CT" value="max-age=3600, enforce"/>
        </headers>
</http>
```

Java

Adding Expect_CT Header Using Spring Security's Java Configuration

```
@EnableWebSecurity
```

```
public class WebSecurityConfig extends
WebSecurityConfigurerAdapter {

@Override
protected void configure(HttpSecurity http) throws Exception {
      http
        // ...
        .headers()
             .addHeaderWriter(new StaticHeadersWriter("Expect-CT","max-age=3600, enforce"));
}
}
```

Spring Overly Permissive Cross Origin Resource Sharing Policy

風險

可能發生什麼問題

過於寬鬆的跨域資源共享 (CORS) 標頭 "Access-Control-Allow-Origin" 可能會使其他網站的腳本可以訪問、甚至篡改受影響的 web 應用程式上的資源。這些資源包括頁面內容、Token 等，因此可能受到跨站點請求偽造 (CSRF) 或跨站點腳本 (XSS) 攻擊、假冒用戶執行操作，如更改密碼或違反用戶隱私。

原因

如何發生

程式碼中的 Access-Control-Allow-Origin 被錯誤地設置為不安全的值。
默認情況下，現代瀏覽器會根據同源策略 (SOP) 禁止不同域之間的資源共享訪問彼此的 DOM 內容、cookie jar 和其他資源，這是為了避免惡意 Web 應用程序攻擊合法的 Web 應用程式及其用戶。例如——網站 A 默認無法檢索網站 B 的內容，因為這違反了 SOP。使用具體標頭定義的跨域資源共享 (CORS) 策略可以放鬆這個嚴格的默認行為，允許跨站點通信。但是，如果使用不當，CORS 可能會允許過度地廣泛信任 Web 應用程式，使其能夠提交請求並獲得 Web 應用程式的回應，從而執行意外的或潛在惡意的行為。

一般建議

如何避免

如果沒有顯示需求，請不要設置任何 CORS 標頭。如果有需要，請考慮設置這些標頭的業務需求，然後選擇最嚴格的配置，例如可信任的白名單、安全和允許的域訪問，同時使用其他 CORS 標頭嚴格地提供所需的和預期的功能。
Spring Security 具有內置機制，可使用 @CrossOrigin 註釋來配置 CORS 標頭。
Spring 的默認允許來源過於寬鬆，建議手動指定允許的來源。

程式碼範例

Java

Default 'origins' Parameter Allowing All Origins in a Specific Endpoint

```
@RestController
@RequestMapping("/resource")
public class ResourceController {

      @CrossOrigin
      @GetMapping("/{id}")
      public Resource retrieve(@PathVariable Long id) {
            //  ...
      }
}
```

Setting an 'origins' Parameter on a Specific Controller

```
@CrossOrigin(origins = "https://example.com", maxAge = 3600)
@RestController
```

```
@RequestMapping("/resource")
public class ResourceController {

	@GetMapping("/{id}")
	public Resource retrieve(@PathVariable Long id) {
		//  ...
	}
}
```

Applying the CORS Header to Every Endpoint Using Spring Security's Java Configuration

```
@EnableWebSecurity
public class WebSecurityConfig extends WebSecurityConfigurerAdapter {

	@Override
	protected void configure(HttpSecurity http) throws Exception {
		http
			// by default uses a Bean by the name of corsConfigurationSource
			.cors();
	}

	@Bean
	CorsConfigurationSource corsConfigurationSource() {
		CorsConfiguration configuration = new CorsConfiguration();
		configuration.setAllowedOrigins(Arrays.asList("https://example.com"));
		configuration.setAllowedMethods(Arrays.asList("GET","POST"));
		UrlBasedCorsConfigurationSource source = new UrlBasedCorsConfigurationSource();
	  // Applying the CORS to all endpoints
	  source.registerCorsConfiguration("/**", configuration);
		return source;
	}
}
```

XML

Applying Spring Security's Default CORS with an Overly Permissive Configuration

```
<http>
	<cors />
</http>
```

Spring Use Of Hardcoded Password

風險

可能發生什麼問題

寫死的密碼容易使應用程式洩露密碼。如果攻擊者可以存取原始碼，攻擊者就能竊取嵌入的密碼，然後用其偽裝成有效的用戶身份。這可能包括偽裝成應用程式的管理者身份，或偽裝成應用程式訪問遠端系統，如資料庫或 Web 服務。
一旦攻擊者成功偽裝成用戶或應用程式，攻擊者就可以獲得系統的全部存取權限，執行所偽裝身份可以執行的任何操作。

原因

如何發生

應用程式代碼庫中存在嵌入到原始碼中的字串密碼。該被寫死的值會被用於比較用戶提供的憑證，或用於為下游的遠端系統（例如資料庫或 Web 服務）提供身份驗證。
攻擊者只需訪問源代碼即可存取到這些寫死的密碼。同樣，攻擊者也可以對編譯的應用程式二進製文件進行反向工程，即可輕鬆獲得嵌入的密碼。找到後，攻擊者即可使用密碼輕鬆地直接對應用程式或遠端系統進行假冒身份攻擊。
此外，被盜後很難輕易更改密碼以避免被繼續濫用，除非編譯新版本的應用程式。此外，如果將此應用程式分發到多個系統，則竊取了一個系統的密碼就等於破解了所有已部署的系統。

一般建議

如何避免

- 不要在原始碼中寫死任何秘密數據，特別是密碼。
- 特別是用戶密碼應儲存在資料庫或目錄服務中，並使用強密碼 hash（例如 bcrypt、scrypt、PBKDF2 或 Argon2）進行保護時。不要將用戶密碼與寫死的值進行對比。
- 系統密碼應保存在配置文件或資料庫中，並使用強加密（例如 AES-256）進行保護。要安全地管理加密密鑰，不能寫死。

程式碼範例

Java

Hardcoded Passwords Using the @Value Annotation

```
@Value("Password123!")
private String password;

@Value("${ADMIN_PASSWORD:Benfica123}")
private String springEnvPasswordWithDefault;
```

Use of an Environment Variable as Password

```
@Value("${ADMIN_PASSWORD}")
private String password;
```

In-memory Authentication Using a Plain-text Password

```
auth.inMemoryAuthentication()
    .withUser("admin").password("{noop}password").roles("USER", "ADMIN");
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Undocumented API

風險

可能發生什麼問題

Undocumented or outdated documentation on API endpoints make it more difficult to find and/or fix vulnerabilities.

原因

如何發生

No automatic documentation is being used or if the documentation is being manually specified, some methods are not being correctly documented.

一般建議

如何避免

Generate documentation automatically by adopting open standards. Include the documentation build in your CI/CD pipeline.Document all aspects of your API such as authentication, errors, redirects, rate limiting, cross-origin resource sharing (CORS) policy and endpoints, including their parameters, requests, and responses.

程式碼範例

Java

API Endpoint correctly documented in separate file

```
@Controller
@RequestMapping("/pet")
public class DeferredResultController {

      @GetMapping("/id")
      public @ResponseBody Pet getPetNameById(int id) {
             return context.getPetNameById(id);
    }
}

// OpenAPI specification (openapi.json)
{
  "openapi" : "3.0.1",
  "paths" : {
    "/pet/id" : {
      "get" : {
        "summary" : "Get an existing pet",
        "requestBody" : {
          "description" : "Pet object that needs to be added to the store",
        },
        "responses" : {
          "400" : {
            "description" : "Invalid ID supplied",
            "content" : { }
          }
        }
      }
    }
  }
}
```

API Endpoint not documented

```
@Controller
@RequestMapping("/pet")
public class DeferredResultController {

    @GetMapping("/id")
      public @ResponseBody Pet getPetNameById(int id) {
             return context.getPetNameById(id);
    }

    // This method is not listed on the OpenApi specification file (see below)
    @DeleteMapping("/id")
      public @ResponseBody String deletePetNameById(int id) {
             return context.deletePetNameById(id);
    }
}

// OpenAPI specification (openapi.json)
{
  "openapi" : "3.0.1",
  "paths" : {
    "/pet/id" : {
      "get" : {
        "summary" : "Get an existing pet",
        "requestBody" : {
          "description" : "Pet object that needs to be added to the store",
        },
        "responses" : {
          "400" : {
            "description" : "Invalid ID supplied",
            "content" : { }
          }
        }
      }
    }
  }
}
```

Documentation being automatically generated

```
@Configuration
@EnableSwagger2
public class SpringFoxConfig {
    @Bean
    public Docket api() {
        return new Docket(DocumentationType.SWAGGER_2)
          .select()
          .apis(RequestHandlerSelectors.any())
          .paths(PathSelectors.any())
          .build();
    }
}
```

Insufficient Logging of Exceptions

風險

可能發生什麼問題

If security-critical information is not recorded, there will be no trail for forensic analysis and discovering the cause of problems or the source of attacks may become more difficult or impossible.

原因

如何發生

Error's stack trace is not fully printed.

一般建議

如何避免

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

程式碼範例

Java

Print Stack Trace

```
public class Example1{
	public String login(Model model, String username, String password) {
		try {
			// attempt to login user
			userService.login(username, password);
		} catch (Exception ex) {
			ex.printStackTrace();
		}
		return "login";
	}
}
```

Log Error

```
public class Example{
	public String login(Model model, String username, String password) {
		try {
			// attempt to login user
			userService.login(username, password);
		} catch (Exception ex) {
			log.error("Exception looking up customer by name: " + ex.getMessage());
		}
		return "login";
	}
}
```

Log Error

```
public class Example{
      public String login(Model model, String username, String password) {
            try {
                  userService.login(username, password);
            } catch (Exception ex) {
                  log.error("Exception looking up customer by name: " + ex.getMessage(), ex);
            }
            return "login";
      }
}
```

檢測的語言

語言	HASH值	變更的日期
Java	5683964027843638	2024/6/11
JavaScript	5693733879119650	2024/6/11
VbScript	0386000544005133	2023/4/6
PLSQL	0342189457118079	2024/6/11
Common	1330881790325397	2024/6/11