

townpass 掃描報告

專案名稱	townpass
掃描開始	2025年1月16日 下午 04:41:49
預設集合	OWASP TOP 10 - 2021
掃描時間	00h:01m:30s
被掃描的程式行數	11259
被掃描的檔案數	149
報告建立時間	2025年1月16日 下午 04:44:34
團隊	數位創新中心
Checkmarx版本	9.5.5.1007 HF18
掃描類別	完整的
來源	LocalPath
漏洞密度	1/1000 (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
OWASP Top 10 2021	全部
CWE top 25	全部
MOIS(KISA) Secure Coding 2021	全部

OWASP ASVS	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
OWASP Top 10 2021	無
CWE top 25	無
MOIS(KISA) Secure Coding 2021	無
OWASP ASVS	無
SANS top 25	無
ASA Mobile Premium	無
ASA Premium	無
ASD STIG 5.2	無
Top Tier	無

結果限制

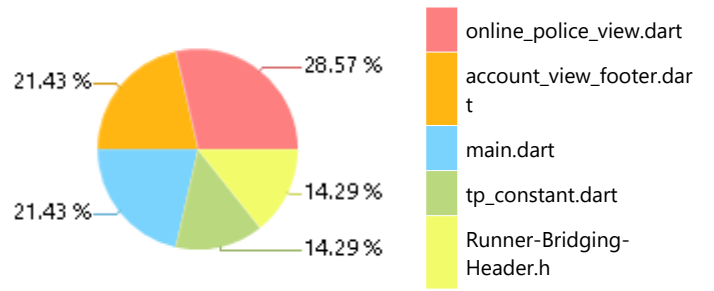
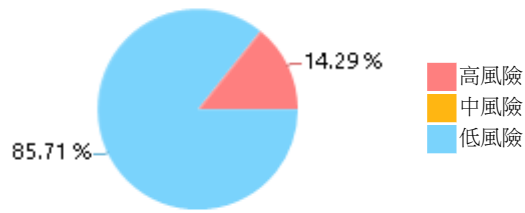
未定義限值

選中的問詢

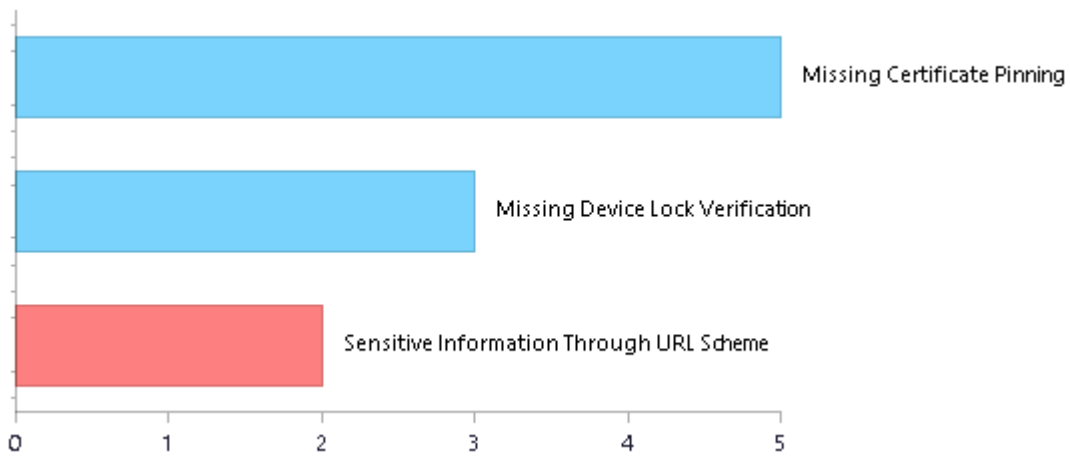
選中的問詢列出在 [掃描結果摘要](#)

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	0	0
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* 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	0	0
A2-Cryptographic Failures	2	1
A3-Injection*	0	0
A4-Insecure Design	4	4
A5-Security Misconfiguration	0	0
A6-Vulnerable and Outdated Components	0	0
A7-Identification and Authentication Failures*	5	5
A8-Software and Data Integrity Failures	7	7
A9-Security Logging and Monitoring Failures	0	0
A10-Server-Side Request Forgery	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 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	0	0
A2-Broken Authentication and Session Management*	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

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

* 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)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)	0	0
SC-28 Protection of Information at Rest (P1)*	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)	0	0
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	0	0
SI-11 Error Handling (P2)	0	0
SI-15 Information Output Filtering (P0)*	0	0
SI-16 Memory Protection (P1)	0	0

* 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 wasn't done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality*	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering*	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

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

* 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	0	0
API2-Broken Authentication	0	0
API3-Excessive Data Exposure	0	0
API4-Lack of Resources and Rate Limiting	0	0
API5-Broken Function Level Authorization	0	0
API6-Mass Assignment	0	0
API7-Security Misconfiguration	0	0
API8-Injection	0	0
API9-Improper Assets Management	0	0
API10-Insufficient Logging and Monitoring	0	0

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.	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-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 unclassified or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0
APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	0	0
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	0	0

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

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

* 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

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	0	0
MOIS(KISA) Security Functions	7	6
MOIS(KISA) Time and status	0	0
MOIS(KISA) Verification and representation of input data*	8	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 - SANS top 25

Category	Issues Found	Best Fix Locations
SANS top 25*	15	14

* 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*	8	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 - Top Tier

Category	Issues Found	Best Fix Locations
Top Tier*	2	1

* 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 ASVS

Category	Issues Found	Best Fix Locations
V01 Architecture, Design and Threat Modeling	4	4
V02 Authentication	0	0
V03 Session Management	0	0
V04 Access Control	0	0
V05 Validation, Sanitization and Encoding*	7	7
V06 Stored Cryptography	0	0
V07 Error Handling and Logging	0	0
V08 Data Protection*	0	0
V09 Communication	7	6
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*	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 - ASA Mobile Premium

Category	Issues Found	Best Fix Locations
ASA Mobile Premium*	5	4

* 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

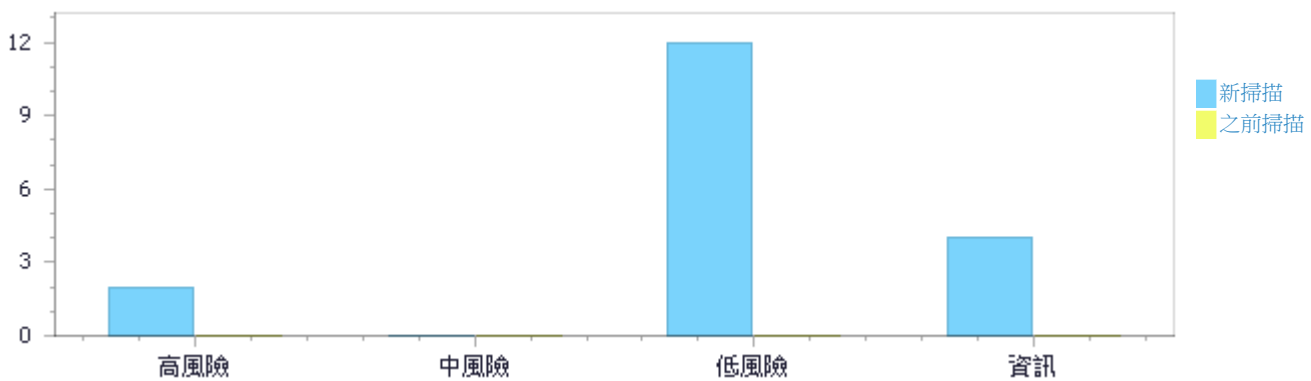
Category	Issues Found	Best Fix Locations
ASA Premium*	0	0

* 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。

掃描結果分佈 專案的首次掃描

	高風險	中風險	低風險	資訊	總共
新問題	2	0	12	4	18
反覆出現的問題	0	0	0	0	0
總共	2	0	12	4	18

已修復的問題	0	0	0	0	0
--------	---	---	---	---	---



掃描結果分佈

	高風險	中風險	低風險	資訊	總共
校驗	2	0	12	4	18
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	2	0	12	4	18

掃描結果摘要

漏洞類別	事件	嚴重程度：
Sensitive Information Through URL Scheme	2	高風險
Missing Certificate Pinning	5	低風險
Missing Device Lock Verification	1	低風險
Missing Device Lock Verification	1	低風險
Missing Device Lock Verification	1	低風險

Missing Jailbreak Check	1	低風險
Missing Jailbreak Check	1	低風險
Missing Root Or Jailbreak Check	1	低風險
No Installer Verification Implemented	1	低風險
Unused Permission	3	資訊
Third Party Keyboard Enabled	1	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
TownPass-main/lib/util/tp_constant.dart	2
TownPass-main/lib/page/account/widget/account_view_footer.dart	2

掃描結果詳細資料

Sensitive Information Through URL Scheme

查詢路徑:

Dart\Cx\Dart Mobile High Risk\Sensitive Information Through URL Scheme 版本:1

類別

- OWASP Top 10 2021: A2-Cryptographic Failures
- MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
- OWASP ASVS: V09 Communication
- SANS top 25: SANS top 25
- ASA Mobile Premium: ASA Mobile Premium
- Top Tier: Top Tier

描述

Sensitive Information Through URL Scheme\路徑 1:

嚴重程度： 高風險

結果狀態： 校驗

結果評論

狀態 新的

Detection Date 1/16/2025 4:43:18 PM

	來源	目的地
檔案	TownPass-main/lib/util/tp_constant.dart	TownPass-main/lib/page/account/widget/account_view_footer.dart
行	9	45
物件	tpMailAddress	launchUrl

代碼片斷

檔案名稱

TownPass-main/lib/util/tp_constant.dart

方法

const String tpMailAddress = 'CodeFestTaipei@gov.taipei';

```
.....
9.  const String tpMailAddress = 'CodeFestTaipei@gov.taipei';
```

檔案名稱

TownPass-main/lib/page/account/widget/account_view_footer.dart

方法

onTap: () async {

```
.....
40.  path: tpMailAddress,
.....
38.  final Uri url = Uri(
.....
45.  await launchUrl(url);
```

Sensitive Information Through URL Scheme\路徑 2:

嚴重程度： 高風險
 結果狀態： 校驗
 結果評論
 狀態： 新的
 Detection Date 1/16/2025 4:43:18 PM

	來源	目的地
檔案	TownPass-main/lib/util/tp_constant.dart	TownPass-main/lib/page/account/widget/account_view_footer.dart
行	9	45
物件	tpMailAddress	launchUrl

代碼片斷

檔案名稱
方法

TownPass-main/lib/util/tp_constant.dart
 const String tpMailAddress = 'CodeFestTaipei@gov.taipei';

```
.....
9.  const String tpMailAddress = 'CodeFestTaipei@gov.taipei';
```

檔案名稱
方法

TownPass-main/lib/page/account/widget/account_view_footer.dart
 onTap: () async {

```
.....
40.  path: tpMailAddress,
.....
38.  final Uri url = Uri(
.....
45.  await launchUrl(url);
```

Missing Certificate Pinning

查詢路徑:

Dart\Cx\Dart Mobile Low Visibility\Missing Certificate Pinning 版本:1

類別

OWASP Top 10 2021: A7-Identification and Authentication Failures
 MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
 OWASP ASVS: V09 Communication
 SANS top 25: SANS top 25

描述

Missing Certificate Pinning\路徑 1:

嚴重程度： 低風險
 結果狀態： 校驗
 結果評論
 狀態： 新的

Detection Date 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/page/account/widget/account_view_footer.dart	TownPass-main/lib/page/account/widget/account_view_footer.dart
行	45	45
物件	launchUrl	launchUrl

代碼片斷

檔案名稱

TownPass-main/lib/page/account/widget/account_view_footer.dart

方法

onTap: () async {

```

.....
45.   await launchUrl(url);

```

Missing Certificate Pinning\路徑 2:

嚴重程度： 低風險

結果狀態： 校驗

結果評論

狀態 新的

Detection Date 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/page/online_police/online_police_view.dart	TownPass-main/lib/page/online_police/online_police_view.dart
行	76	76
物件	launchUrl	launchUrl

代碼片斷

檔案名稱

TownPass-main/lib/page/online_police/online_police_view.dart

方法

onTap: () async => await launchUrl(Uri.parse('tel://110')),

```

.....
76.   onTap: () async => await launchUrl(Uri.parse('tel://110')),

```

Missing Certificate Pinning\路徑 3:

嚴重程度： 低風險

結果狀態： 校驗

結果評論

狀態 新的

Detection Date 1/16/2025 4:43:19 PM

來源	目的地
----	-----

檔案	TownPass-main/lib/page/online_police/online_police_view.dart	TownPass-main/lib/page/online_police/online_police_view.dart
行	90	90
物件	launchUrl	launchUrl

代碼片斷
檔案名稱
方法

TownPass-main/lib/page/online_police/online_police_view.dart
onTap: () async => await launchUrl(Uri.parse('tel://119')),

```
.....
90.  onTap: () async => await launchUrl(Uri.parse('tel://119')),
```

Missing Certificate Pinning\路徑 4:

嚴重程度： 低風險
結果狀態： 校驗
結果評論
狀態 新的

Detection Date 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/page/online_police/online_police_view.dart	TownPass-main/lib/page/online_police/online_police_view.dart
行	110	110
物件	launchUrl	launchUrl

代碼片斷
檔案名稱
方法

TownPass-main/lib/page/online_police/online_police_view.dart
onTap: () async => await launchUrl(Uri.parse('tel://165')),

```
.....
110. onTap: () async => await launchUrl(Uri.parse('tel://165')),
```

Missing Certificate Pinning\路徑 5:

嚴重程度： 低風險
結果狀態： 校驗
結果評論
狀態 新的

Detection Date 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/page/online_police/online_police_view.dart	TownPass-main/lib/page/online_police/online_police_view.dart

行	124	124
物件	launchUrl	launchUrl

代碼片斷
檔案名稱
方法

TownPass-main/lib/page/online_police/online_police_view.dart
onTap: () async => await launchUrl(Uri.parse('tel://113')),

```
.....
124.  onTap: () async => await launchUrl(Uri.parse('tel://113')),
```

Missing Device Lock Verification

查詢路徑:

Obj\Cx\ObjectiveC Low Visibility\Missing Device Lock Verification 版本:1

類別

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

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

Missing Device Lock Verification\路徑 1:

嚴重程度: 低風險

結果狀態: 校驗

結果評論

狀態: 新的

Detection Date: 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/ios/Runner/Runner-Bridging-Header.h	TownPass-main/ios/Runner/Runner-Bridging-Header.h
行	1	1
物件	INCLUDEREPLACE	INCLUDEREPLACE

代碼片斷
檔案名稱
方法

TownPass-main/ios/Runner/Runner-Bridging-Header.h
#import "GeneratedPluginRegistrant.h"

```
.....
1.  #import "GeneratedPluginRegistrant.h"
```

Missing Device Lock Verification

查詢路徑:

Dart\Cx\Dart Mobile Low Visibility\Missing Device Lock Verification 版本:1

類別

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

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](#)

Missing Device Lock Verification\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
結果評論	
狀態	新的
Detection Date	1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/main.dart	TownPass-main/lib/main.dart
行	15	15
物件	main	main

代碼片斷

檔案名稱 TownPass-main/lib/main.dart

方法 void main() async {

```

    ...
    15. void main() async {

```

Missing Device Lock Verification

[查詢路徑:](#)

Swift\Cx\Swift Low Visibility\Missing Device Lock Verification 版本:1

[類別](#)

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

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](#)

Missing Device Lock Verification\路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
結果評論	
狀態	新的
Detection Date	1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-	TownPass-

	main/ios/RunnerTests/RunnerTests.swift	main/ios/RunnerTests/RunnerTests.swift
行	7	7
物件	testExample	testExample

代碼片斷

檔案名稱

TownPass-main/ios/RunnerTests/RunnerTests.swift

方法

func testExample() {

```

.....
7.  func testExample() {

```

Missing Root Or Jailbreak Check

查詢路徑:

Dart\Cx\Dart Mobile Low Visibility\Missing Root Or Jailbreak Check 版本:1

類別

OWASP Top 10 2021: A4-Insecure Design

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

SANS top 25: SANS top 25

ASA Mobile Premium: ASA Mobile Premium

描述

Missing Root Or Jailbreak Check\路徑 1:

嚴重程度: 低風險

結果狀態: 校驗

結果評論

狀態: 新的

Detection Date: 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/lib/main.dart	TownPass-main/lib/main.dart
行	15	15
物件	main	main

代碼片斷

檔案名稱

TownPass-main/lib/main.dart

方法

void main() async {

```

.....
15. void main() async {

```

No Installer Verification Implemented

查詢路徑:

Dart\Cx\Dart Mobile Low Visibility\No Installer Verification Implemented 版本:1

類別

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

No Installer Verification Implemented \路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
結果評論	
狀態	新的
Detection Date	1/16/2025 4:43:20 PM

	來源	目的地
檔案	TownPass-main/lib/main.dart	TownPass-main/lib/main.dart
行	15	15
物件	main	main

代碼片斷

檔案名稱 TownPass-main/lib/main.dart

方法 void main() async {

```

    .....
    15. void main() async {
  
```

Missing Jailbreak Check

查詢路徑:
 Objc\Cx\ObjectiveC Low Visibility\Missing Jailbreak Check 版本:3

類別

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

描述

Missing Jailbreak Check \路徑 1:

嚴重程度：	低風險
結果狀態：	校驗
結果評論	
狀態	新的
Detection Date	1/16/2025 4:43:20 PM

來源	目的地
----	-----

檔案	TownPass-main/ios/Runner/Runner-Bridging-Header.h	TownPass-main/ios/Runner/Runner-Bridging-Header.h
行	1	1
物件	INCLUDEREPLACE	INCLUDEREPLACE

代碼片斷

檔案名稱 TownPass-main/ios/Runner/Runner-Bridging-Header.h
 方法 #import "GeneratedPluginRegistrant.h"

```
.....
1. #import "GeneratedPluginRegistrant.h"
```

Missing Jailbreak Check

查詢路徑:

Swift\Cx\Swift Low Visibility\Missing Jailbreak Check 版本:1

類別

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

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

ASA Mobile Premium: ASA Mobile Premium

描述

Missing Jailbreak Check 路徑 1:

嚴重程度: 低風險

結果狀態: 校驗

結果評論

狀態: 新的

Detection Date: 1/16/2025 4:43:19 PM

	來源	目的地
檔案	TownPass-main/ios/RunnerTests/RunnerTests.swift	TownPass-main/ios/RunnerTests/RunnerTests.swift
行	7	7
物件	testExample	testExample

代碼片斷

檔案名稱 TownPass-main/ios/RunnerTests/RunnerTests.swift
 方法 func testExample() {

```
.....
7. func testExample() {
```

Unused Permission

查詢路徑:

Dart\Cx\Dart Mobile Best Coding Practice\Unused Permission 版本:1

類別

OWASP Top 10 2021: A4-Insecure Design

OWASP ASVS: V01 Architecture, Design and Threat Modeling

[描述](#)

Unused Permission\路徑 1:

嚴重程度： 資訊
 結果狀態： 校驗
 結果評論
 狀態 新的
 Detection Date 1/16/2025 4:43:20 PM

	來源	目的地
檔案	TownPass-main/android/app/src/debug/AndroidManifest.xml	TownPass-main/android/app/src/debug/AndroidManifest.xml
行	6	6
物件	uses-permission	uses-permission

代碼片斷

檔案名稱 TownPass-main/android/app/src/debug/AndroidManifest.xml
 方法 <uses-permission android:name="android.permission.INTERNET"/>

```
.....
6. <uses-permission android:name="android.permission.INTERNET"/>
```

Unused Permission\路徑 2:

嚴重程度： 資訊
 結果狀態： 校驗
 結果評論
 狀態 新的
 Detection Date 1/16/2025 4:43:20 PM

	來源	目的地
檔案	TownPass-main/android/app/src/profile/AndroidManifest.xml	TownPass-main/android/app/src/profile/AndroidManifest.xml
行	6	6
物件	uses-permission	uses-permission

代碼片斷

檔案名稱 TownPass-main/android/app/src/profile/AndroidManifest.xml
 方法 <uses-permission android:name="android.permission.INTERNET"/>

```
.....
6. <uses-permission android:name="android.permission.INTERNET"/>
```

Unused Permission\路徑 3:

嚴重程度： 資訊
 結果狀態： 校驗
 結果評論
 狀態 新的
 Detection Date 1/16/2025 4:43:20 PM

	來源	目的地
檔案	TownPass-main/android/app/src/main/AndroidManifest.xml	TownPass-main/android/app/src/main/AndroidManifest.xml
行	2	2
物件	uses-permission	uses-permission

代碼片斷

檔案名稱 TownPass-main/android/app/src/main/AndroidManifest.xml
 方法 <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />

```
.....
2. <uses-permission
    android:name="android.permission.ACCESS_FINE_LOCATION" />
```

Third Party Keyboard Enabled

查詢路徑:

Swift\Cx\Swift Best Coding Practices\Third Party Keyboard Enabled 版本:2

類別

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

Third Party Keyboard Enabled\路徑 1:

嚴重程度： 資訊
 結果狀態： 校驗
 結果評論
 狀態 新的
 Detection Date 1/16/2025 4:43:20 PM

	來源	目的地
檔案	TownPass-main/ios/Runner/AppDelegate.swift	TownPass-main/ios/Runner/AppDelegate.swift

行	6	6
物件	AppDelegate	AppDelegate

代碼片斷

檔案名稱

TownPass-main/ios/Runner/AppDelegate.swift

方法

@objc class AppDelegate: FlutterAppDelegate {

```
.....
6. @objc class AppDelegate: FlutterAppDelegate {
```

Sensitive Information Through URL Scheme

風險

可能發生什麼問題

在使用深層連結 (Deep Link) 進行傳輸時，務必要針對使用者的個人或機敏資訊，例如：密碼、身份證字號、信用卡資訊和其他的個人識別資訊 (Personally Identifiable Information, 簡稱 PII) 進行保護。因為所有應用程式都能夠藉由註冊一個 URL 來劫持這些傳輸的資訊。如果沒有對機敏資訊加密就直接使用 Deep Link 來進行傳遞，將可能導致這些機敏資訊被暴露而面臨到身分偽造、竊取和金融詐騙等風險。

原因

如何發生

深層連結 (Deep Link) 是一種跨應用程式進行共用資料或呼叫其他應用程式的機制。它是藉由在應用程式中註冊一個唯一的 URL 來達到此一目的。但如果一個惡意的應用程式註冊了與其他應用程式相同的 URL，那應用程式發送時的資訊將有可能被這個惡意的應用程式劫取而導致資料洩漏。

一般建議

如何避免

- 考慮是否需要與其他應用程式共享敏感資訊
- 重新考慮應用程式是否絕對需要這些個人詳細資訊。未收到的資料不能被洩漏。
- 盡可能使用通用連結而不是深層連結來驗證連結接收者
- 在使用深層與其他應用程式共享資訊之前對其進行加密連結

程式碼範例

Dart

Send Login Information Through URL Scheme

```
String password = ${textController.password};
String email = ${textController.email};
Future<HttpResponse> externalLogin(String email, String password) async {
  Uri url = Uri.parse("appscheme://randomapp.link.com/login?e=$email&p=$password");
  final response = await http.get(url);
  var responseData = json.decode(response.body);
  return responseData;
}
```



Missing Device Lock Verification

風險

可能發生什麼問題

可以選擇的情況下，許多User不會用鎖定來保護他們的Device。若應用程式沒有強制要求鎖定驗證功能，萬一Device被攻擊者冒用，則應用程式中儲存的information就會受到威脅。

原因

如何發生

應用程式沒有進行任何device lock verification的檢查

一般建議

如何避免

在應用程式啟動時執行嚴格的device lock檢查，以確保User的Device不會輕易的被冒用。

程式碼範例

Objc

Checking for Device Lock with LAContext (iOS 8.0+)

```
LAContext *context = [[LAContext alloc] init];
NSError *err = nil;

if ([context canEvaluatePolicy:LAPolicyDeviceOwnerAuthentication error:&err])
{
    // Device has, at least, a passcode (could also have TouchId)
}
else
{
    // Device does not lock with a passcode
}
```

Missing Device Lock Verification

風險

可能發生什麼問題

可以選擇的情況下，許多User不會用鎖定來保護他們的Device。若應用程式沒有強制要求鎖定驗證功能，萬一Device被攻擊者冒用，則應用程式中儲存的information就會受到威脅。

原因

如何發生

應用程式沒有進行任何device lock verification的檢查

一般建議

如何避免

在應用程式啟動時執行嚴格的device lock檢查，以確保User的Device不會輕易的被冒用。

程式碼範例

Dart

Checking for Device Lock with Local Authentication

```
import 'package:local_auth/local_auth.dart';

void deviceLockingCheck() async{
  final LocalAuthentication auth = LocalAuthentication();

  //Check for Biometric Authentication
  final bool canAuthenticateWithBiometrics = await auth.canCheckBiometrics;
  //Check for non Biometric Authentication
  final bool canAuthenticate = canAuthenticateWithBiometrics || await
  auth.isDeviceSupported();

  if(canAuthenticate){
    // Device has, at least, a passcode (could also have TouchId)
  }
  else{
    // Device does not lock with a passcode
  }
}
```

Missing Certificate Pinning

風險

可能發生什麼問題

如果攻擊者能夠騙取使用者安裝攻擊者的憑證，就可以破壞與應用程式伺服器之間的連線機密性，並進行中間人攻擊。

原因

如何發生

當應用程式建立一個 SSL 連線時，它會自動驗證對方的憑證是否正確。這個機制旨在防止攻擊者進行中間人攻擊，從而違反安全連線的機密性。

驗證是通過所謂的信任鏈（Trust Chain）來實現的。信任鏈是一系列的憑證，每個憑證都保證下一個憑證是可信的。因此，如果應用程式信任鏈中的第一個憑證，它可能會信任最後一個憑證（即葉子憑證），這正是要驗證的憑證，也就是 SSL 連線對方的憑證。信任鏈中的第一個憑證稱為根憑證，無法通過此方式驗證。為了解決這個問題，大多數包括 Android 操作系統在內的 SSL 實現都會將幾個受信任的中央機構（CA）的憑證儲存在所謂的信任庫中，並將它們用作信任鏈的根憑證。

為了克服這種保護機制，攻擊者可以欺騙使用者將攻擊者自己的憑證添加到信任庫中。這可以通過使用社交工程技術來實現。例如，如果攻擊者通過自己的路由器提供免費的 Wi-Fi 接入，他可能會建議使用者允許安裝攻擊者的憑證。大多數使用者對資訊安全威脅不太熟悉，因此他們會給予許可。這將使攻擊者可以訪問傳輸的數據。

為了保護應用程式數據免受這種攻擊，應用程式應該使用憑證固定（Certificate Pinning）。在這種情況下，應用程式不會信任信任庫中的所有憑證，而只會信任開發人員指定的憑證。實際上，應用程式實現了自己的不可修改的信任庫。因此，即使攻擊者設法安裝他的憑證，資料也不會被破壞。

一般建議

如何避免

只要建立 SSL 連線（例如 HTTPS 請求），就使用憑證綁定。

1. 發送請求時，請確保是否已綁定憑證。
2. 盡可能綁定到根CA（根憑證頒發機構）憑證。
3. 不要綁定到終端憑證，因為它會頻繁更改。
4. 綁定到多個憑證以便制定備份計劃，預防主要計劃出現問題（例如私鑰遺失）。

程式碼範例

Dart

Sending HTTP Request Using Dart's Trusted Root Certificates

```
Future<String> sendHttpRequest(Uri url) async{
  HttpClient client = HttpClient();
  var req = await client.getUrl(url);
  var res = await (await req.close()).transform(utf8.decoder).join();
  // ...
}
```

Using Empty `SecurityContext` to Pin and Verify Certificates

```
Future<String> sendHttpRequest(Uri url) async{
```

```
String certPath = await getCertificatePath();
SecurityContext sc = SecurityContext(withTrustedRoots: false); // `withTrustedRoots: false`
means no other certificate is permitted
sc.setTrustedCertificates(certPath);
HttpClient client = HttpClient(context: sc); // client is initiated with the empty
SecurityContext
client.badCertificateCallback = (X509Certificate cert, String host, int port) => false; //
Hard fail - if the certificate is different from the pinned one

var req = await client.getUrl(url); // safe request
var res = await (await req.close()).transform(utf8.decoder).join();
// ...
}
```

Missing Device Lock Verification

風險

可能發生什麼問題

可以選擇的情況下，許多User不會用鎖定來保護他們的Device。若應用程式沒有強制要求鎖定驗證功能，萬一Device被攻擊者冒用，則應用程式中儲存的information就會受到威脅。

原因

如何發生

應用程式沒有進行任何device lock verification的檢查

一般建議

如何避免

在應用程式啟動時執行嚴格的device lock檢查，以確保User的Device不會輕易的被冒用。

程式碼範例

Missing Root Or Jailbreak Check

風險

可能發生什麼問題

已經取得 root 或越獄的裝置可能會受到多種攻擊形式的威脅，因為應用程式、服務等可能具有對裝置操作的重大存取權限。這些操作包括直接讀寫記憶體、完全存取檔案系統等。

雖然檢查篡改裝置的方法並不是絕對可靠，因為惡意應用程式幾乎可以抑制這類檢查，但建議進行多層防禦，以保護應用程式使用者免受在已被入侵的裝置上使用，例如當裝置已經被取得 root，但尚未被入侵時。

原因

如何發生

若應用程式未進行適當的 root 檢查，表示該應用程式在經過篡改的裝置上仍可正常運作。

一般建議

如何避免

請在應用程式啟動時進行檢查，以確保裝置未取得 root 或越獄。如果發現裝置已被篡改，請警告使用者並考慮禁止他們使用應用程式，以防止敏感資訊在應用程式中受到破壞。

程式碼範例

Dart

Function to Detect a Rooted Android Device

```
bool rootDetection() async{
  bool rooted = await io.File("/sbin/su").exists();
  if(rooted){
    return true;
  }
  return false;
}
```

No Installer Verification Implemented

風險

可能發生什麼問題

可能允許惡意用戶重新編寫原始碼，並在無起疑情況下使用竊取用戶的資料、憑證、信用卡等。

原因

如何發生

缺乏篡改檢測，在開發者沒有起疑的狀況下，攻擊者可以改變原始碼來為所欲為。

一般建議

如何避免

強烈建議使用篡改檢測，以防止篡改的應用程式釋放出來。

程式碼範例

Dart

Installer Verification using a Hashing function

```
void verifyInstall() async{

  // File path to the target application
  final File file = File('data/app/com.random.app/base.apk');

  // Determine the file hash
  String contents = await file.readAsString();
  var digest = sha1.convert(utf8.encode(contents));

  // Perform install verification
  if(digest==SavedHashedValue){
    ...
  }else{
    ...
  }
}
```

Missing Jailbreak Check

風險

可能發生什麼問題

被JB的設備容易受到許多形式的攻擊，因為應用程式、服務等可能取得過高的權限來進行特權操作。例如直接讀寫記憶體、完整的 file system 存取權等等。

雖然檢測JB的程式不一定有效，因為惡意應用程式會想出各種方式抑止這類檢查。但仍然可以建議使用者不要在被污染的設備上使用應用程式，避免使用者的裝置被JB但不知情。

原因

如何發生

沒有進行適當的JB檢查，導致應用程式會在已JB的設備上運行。

一般建議

如何避免

最好在應用程式啟動時進行檢查，確保設備沒有被root。如果設備已經被root，請警告用戶並考慮阻止使用者繼續使用這個應用程式，防止應用程式內的機敏資訊遭受損害。

程式碼範例

Objc

Multiple Methods of Checking If Device is Jailbroken

```
BOOL hasBeenJailBroken()
{
    //Check common Jailbreak files
    if (
        [[NSFileManager defaultManager] fileExistsAtPath:@"Applications/Cydia.app"] ||
        [[NSFileManager defaultManager] fileExistsAtPath:@"Library/MobileSubstrate/MobileSubstrate.dylib"] ||
        [[NSFileManager defaultManager] fileExistsAtPath:@"bin/bash"] ||
        [[NSFileManager defaultManager] fileExistsAtPath:@"usr/sbin/sshd"] ||
        [[NSFileManager defaultManager] fileExistsAtPath:@"etc/apt"] ||
        [[NSFileManager defaultManager] fileExistsAtPath:@"private/var/lib/apt/"]
    ) {
        return YES;
    }
    if ( //Check Cydia AppStore (Exclusive to Jailbroken Devices) URI Scheme
        [[UIApplication sharedApplication] canOpenURL:[NSURL URLWithString:@"cydia://package/com.example.package"]]
    ) {
        return YES;
    }

    NSError *error;
    //Check write permissions, by writing an arbitrary file to /private/ folder
    NSString *stringToBeWritten = @"If written successfully, device is jailbroken.";
    [stringToBeWritten writeToFile:@"private/WriteTestJailbreak.txt" atomically:YES
    encoding:NSUTF8StringEncoding error:&error];
    [[NSFileManager defaultManager] removeItemAtPath:@"private/WriteTestJailbreak.txt"
    error:nil];
    if(error == nil)
    {
        return YES;
    }
}
```

```
}  
  return NO;  
}
```

Missing Jailbreak Check

風險

可能發生什麼問題

被JB的設備容易受到許多形式的攻擊，因為應用程式、服務等可能取得過高的權限來進行特權操作。例如直接讀寫記憶體、完整的 file system 存取權等等。

雖然檢測JB的程式不一定有效，因為惡意應用程式會想出各種方式抑止這類檢查。但仍然可以建議使用者不要在被污染的設備上使用應用程式，避免使用者的裝置被JB但不知情。

原因

如何發生

沒有進行適當的JB檢查，導致應用程式會在已JB的設備上運行。

一般建議

如何避免

最好在應用程式啟動時進行檢查，確保設備沒有被root。如果設備已經被root，請警告用戶並考慮阻止使用者繼續使用這個應用程式，防止應用程式內的機敏資訊遭受損害。

程式碼範例

Unused Permission

風險

可能發生什麼問題

應用程式要求了多餘的特權，不僅在程式中毫無作用，還有可能在特權服務及應用程式上提供額外的攻擊面。

原因

如何發生

根據最小權限原則：對於任何服務、函式庫、或者應用程式 - 它們所獲得的權限都不應超出預期運行所需的最低要求。而此應用程式所請求的權限，並沒有在程式碼中主動使用，這意味著APP向系統請求超過實際所需的權限。

在Android應用程式中，欲請求的權限，需在AndroidManifest.xml檔案之中利用<uses-permission> 標籤來做指定。

一般建議

如何避免

重新檢視應用程式所請求的權限，確保它們在應用程式執行時都有被利用到。以及去除非必要的權限。

程式碼範例

Java

Write to External Storage in AndroidManifest.xml is Requested, But Never Used In Code

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

Third Party Keyboard Enabled

風險

可能發生什麼問題

一個有惡意的第三方鍵盤有可能會紀錄鍵盤輸入歷程，並將記錄檔傳送到攻擊者的伺服器中。所有的 UITextField 和 UITextView 物件如果將 secureTextEntry 屬性設定為 YES 的話預設是會阻擋所有第三方鍵盤的使用。然而，如果為了隱藏的字元將 secureTextEntry 設定為 NO，那麼第三方鍵盤就有可能竊取敏感性資料。

原因

如何發生

使用者安裝了一個看起來沒問題的惡意第三方鍵盤，接著在應用程式介面中點擊一個 UITextField 來輸入他的身分證字號。為了要看得輸入的字元所以 UITextField 的 secureTextEntry 屬性是設定為 NO，這樣的話第三方鍵盤是可以使用的，而且使用者選擇使用這個惡意鍵盤，這個鍵盤記錄了身分證字號並傳送到攻擊者的伺服器。

一般建議

如何避免

1. 透過將包函敏感性資料之 UITextView 及 UITextField 元素的 secureTextEntry 屬性設定為 YES 來提升安全性。詳見範例 "將 UITextField 設定為安全保護的"。

-或是-
2. 在你的應用程式中完全關閉第三方鍵盤，要注意的是這可能會降低應用程式的使用者體驗。詳見範例 "將以下程式加入你的 UIApplicationDelegate 來關閉第三方鍵盤"。

程式碼範例

Objc

Marking a UITextField as secure

```
UITextField* textField = [[UITextField alloc] init];
textField.secureTextEntry = YES;
```

To disabling third party keyboards, add the following code to your UIApplicationDelegate

```
-(BOOL)application:(UIApplication *)application shouldAllowExtensionPointIdentifier:(NSString *)extensionPointIdentifier
{
    if (extensionPointIdentifier == UIApplicationKeyboardExtensionPointIdentifier)
    {
        return NO;
    }
    return YES;
}
```

Swift

Marking a UITextField as secure

```
let textField = UITextField()
textField.secureTextEntry = true
```

To disabling third party keyboards, add the following code to your UIApplicationDelegate

```
func application(application: UIApplication, shouldAllowExtensionPointIdentifier
extensionPointIdentifier: String) -> Bool
{
    if (extensionPointIdentifier == UIApplicationKeyboardExtensionPointIdentifier)
    {
        return false
    }
    return true
}
```

檢測的語言

語言	HASH值	變更的日期
JavaScript	5693733879119650	2024/5/29
Objc	8084807123196146	2022/11/15
Kotlin	0443405911293625	2024/5/29
Swift	0135400581388578	2024/5/29
Dart	0458641660523603	2024/5/29
Common	1330881790325397	2024/5/29