

ios App Audit Report

App Information

MD5	d41d8cd98f00b204e9800998ecf8427e
sha256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Scan time	Mon, 01 May 2023 01:15:34 GMT
App name	
App version	
Average CVSS	0
Build	
Bundle id	jp.mufg.bk.applisp.01
Filename	
Minimum OS require	
SDK name	iphoneos13.3.1

Scan Report

Result	Rule
--------	------

lab_1 - SSL connection check

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.4.1 - The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.

4.1.2.1.2 - The mobile application shall provide users with the right to refuse the collection of sensitive data.

MSTG:

MSTG-STORAGE 4

MSTG-NETWORK-1

MSTG-NETWORK-2

✓ Passed

OWASP MOBILE:

M3

Description:

URL with http found, please check if this URL need to be protected with SSL or not ,Keyword: NSURL with http / NSURL startswith(http://)

詳細資訊:

· NSURL with HTTPs https://idmsa.apple.com.cn/appleauth/auth/authorize/signin
NSURL with HTTPs https://idmsa.apple.com.cn/appleauth/auth/authorize/signin
NSURL with HTTPs https://appleid.apple.com/auth/authorize NSURL with HTTPs
https://appleid.apple.com/auth/authorize NSURL with HTTPs
https://idmsa.apple.com/appleauth/auth/authorize/signin NSURL with HTTPs
https://idmsa.apple.com/appleauth/auth/authorize/signin

lab_2 - Make use of security method

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.6 - Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.

MSTG:

MSTG-STORAGE-14

MSTG CRYPTO

✓ Passed

Description:

Cipher function found. Ensure no weak cipher function used in this application.
Message digest function found. Ensure no weak message digest function used in this application. Signature function found. Ensure no weak signature function used in this application. MAC function found. Ensure no weak MAC function used in this application.

詳細資訊:

.

lab_3 - Make use of security class

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.6 - Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.

MSTG:

MSTG-STORAGE-14

MSTG CRYPTO

✓ Passed

Description:

Cipher function found. Ensure no weak cipher function used in this application. Message digest function found. Ensure no weak message digest function used in this application. Signature function found. Ensure no weak signature function used in this application. MAC function found. Ensure no weak MAC function used in this application.

詳細資訊:

.

lab_4 - Master Key Vulnerability checking

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.5.1.2 - The mobile application shall avoid information security vulnerabilities.

MSTG:

MSTG-CRYPTO-2

MSTG-CRYPTO-4

✓ Passed

詳細資訊:

.

lab_5 - Network access

MSTG:

MSTG-NETWORK-3

✓ Passed

詳細資訊:

.

lab_6 - Make use of SQLite deprecated functions

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.5.3.1 - When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.

MSTG:

MSTG-NETWORK-6

MSTG-CODE-5

✓ Passed

Description:

sqlite3_aggregate_count', 'sqlite3_expired', 'sqlite3_global_recover', 'sqlite3_memory_alarm', 'sqlite3_soft_heap_limit', 'sqlite3_thread_cleanup', 'sqlite3_transfer_bindings' These functions are deprecated. In order to maintain backwards compatibility with older code, these functions continue to be supported. However, new applications should avoid the use of these functions. Keyword: libsqlite3.dylib

詳細資訊:

.

lab_7 - List all native method

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.2.2.1.2 - When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.

✓ Passed

MSTG:

MSTG-PLATFORM-6

詳細資訊:

.

lab_8 - Clipboard manipulation check

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.13 - The user interface in the mobile application shall avoid the leakage of sensitive data.

MSTG:

MSTG-STORAGE-7

OWASP MOBILE:

M4

✓ Passed

Description:

Any app on an iOS device can access the most recent thing copied to your clipboard. Theoretically, a malicious app can read what's on your iOS clipboard and then feed that information back to a remote server. That remote server can be easily accessed by someone stealing your personal and sensitive information.

Keyword: Foundation, copy: ,cut: ,paste:

詳細資訊:

.

lab_9 - Make use of SMS related code

OWASP MOBILE:

M3

✓ Passed

Description:

This application sends SMS message. One of the most common vulnerabilities of SMS verification codes is weak security protocols. Many SMS verification codes are sent over unencrypted channels, making them vulnerable to interception. Make sure it do this action with user permission. Keyword:

MFMessageComposeViewController,canSendText

詳細資訊:

.

lab_10 - Certificate check

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.5.1.2 - The mobile application shall avoid information security vulnerabilities.

MSTG:

MSTG-NETWORK-3

MSTG-NETWORK-4

Description:

Check the SSL Certificate information. We use SSLlab to check your cert, more information <https://www.ssllabs.com/ssltest/> Keyword: NSURL startswith https://

詳細資訊:

```
· {"valid": True, "detail": {"url":  
"https://idmsa.apple.com.cn/appleauth/auth/authorize/signin", "issuer": , "not  
valid after": "2023-05-05 16:21:14", "not valid before": "2022-04-05 16:21:15", "serial  
number": 80668450533936069632275799911989147556, "signature algorithm":  
"sha256", "subject": , "x509 version": , "key size": 2048}} {"valid": True, "detail":  
{"url": "https://idmsa.apple.com.cn/appleauth/auth/authorize/signin", "issuer": ,  
"not valid after": "2023-05-05 16:21:14", "not valid before": "2022-04-05 16:21:15",  
"serial number": 80668450533936069632275799911989147556, "signature  
algorithm": "sha256", "subject": , "x509 version": , "key size": 2048}} {"valid": True,  
"detail": {"url": "https://appleid.apple.com/auth/authorize", "issuer": , "not valid  
after": "2023-08-23 10:56:39", "not valid before": "2023-02-24 10:46:39", "serial  
number": 146223595521062323404235309789466801942, "signature algorithm":  
"sha256", "subject": , "x509 version": , "key size": 2048}} {"valid": True, "detail":  
{"url": "https://appleid.apple.com/auth/authorize", "issuer": , "not valid after":  
"2023-08-23 10:56:39", "not valid before": "2023-02-24 10:46:39", "serial number":  
146223595521062323404235309789466801942, "signature algorithm": "sha256",  
"subject": , "x509 version": , "key size": 2048}} {"valid": True, "detail": {"url":  
"https://idmsa.apple.com/appleauth/auth/authorize/signin", "issuer": , "not valid  
after": "2023-08-07 21:08:10", "not valid before": "2023-02-08 20:58:10", "serial  
number": 65216082230534759689535399055666655046, "signature algorithm":  
"sha256", "subject": , "x509 version": , "key size": 2048}} {"valid": True, "detail":  
{"url": "https://idmsa.apple.com/appleauth/auth/authorize/signin", "issuer": , "not  
valid after": "2023-08-07 21:08:10", "not valid before": "2023-02-08 20:58:10", "serial  
number": 65216082230534759689535399055666655046, "signature algorithm":  
"sha256", "subject": , "x509 version": , "key size": 2048}}
```

⚠ Detected

lab_11 - Base64 String decoding

MSTG:

MSTG-CRYPTO-1
MSTG-CRYPTO-2
MSTG-CRYPTO-3

OWASP MOBILE:

M3

✓ Passed

Description:

Base64-encoded or base64-decoded string found Applications may Base64-encode parameters to conceal them from users or to ease the transfer of binary data. The existence of Base64-encoded data might suggest security-sensitive information or functionality that should be investigated further. Keyword: Base64

詳細資訊:

.

lab_12 - Make use of javascript in webview

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.2.2.1.2 - When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.

MSTG:

MSTG-ARCH-2
MSTG-NETWORK-4
MSTG-PLATFORM-5
MSTG-PLATFORM-6
MSTG-PLATFORM-7

✓ Passed

Description:

Webview JavaScript Enabled, the webview use setJavaScriptEnabled to allow javascript. It is potentially dangerous because it may allow the external website to do XSS attack in the webview. Keyword: UIWebView - stringByEvaluatingJavaScriptFromString in webview

詳細資訊:

.

lab_13 - Screenshot detection

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.9 - The mobile application shall actively alert the user when non-user-initiated screenshots are taken.

MSTG:

MSTG-STORAGE-12

✓ Passed

OWASP MOBILE:

M10

Description:

This application allows users to take screenshots. Please check screenshots function and turn it off. Keyword: UIApplication - _handleScreenshot to detect screenshot

詳細資訊:

.

lab_14 - HTTPS ALLOW_ALL_HOSTNAME_VERIFIER check

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.4.2.3 - The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.

4.1.4.2.4 - mas.4.1.4.2.4

4.1.5.1.2 - The mobile application shall avoid information security vulnerabilities.

MSTG:

MSTG-NETWORK-3

✓ Passed

OWASP MOBILE:

M5

Description:

This application use ALLOW_ALL_HOSTNAME_VERIFIER to verify all the CN. It is dangerous and may cause man-in-the-middle attack.

詳細資訊:

.

<p>✓ Passed</p>	<p>lab_15 - SSL Certificate check</p> <p>Standard Testing Guide of Industrial Development Board, R.O.C.: 4.1.5.1.2 - The mobile application shall avoid information security vulnerabilities.</p> <p>MSTG: MSTG-CODE-5 MSTG-PLATFORM-8 MSTG-PLATFORM-9</p> <p>OWASP MOBILE: M5</p> <p>Description: Check the SSL Certificate information.</p> <p>詳細資訊: .</p>
<p>✓ Passed</p>	<p>lab_16 - Potential XSS in webview</p> <p>Standard Testing Guide of Industrial Development Board, R.O.C.: 4.1.5.4.2 - The mobile application shall provide protection mechanism(s) relevant to injection attacks.</p> <p>MSTG: MSTG-PLATFORM-2</p> <p>OWASP MOBILE:</p> <p>詳細資訊: .</p>
<p>✓ Passed</p>	<p>lab_17 - Use SQLite database</p> <p>Standard Testing Guide of Industrial Development Board, R.O.C.: 4.1.5.1.1 - The mobile application shall avoid containing malicious code.</p> <p>MSTG: MSTG-STORAGE-1 MSTG-STORAGE-2</p> <p>詳細資訊: .</p>

lab_18 - WebView setAllowFileAccess

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.7 - In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.

4.1.2.5.3 - Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.

✓ Passed

MSTG:

MSTG-STORAGE 4

MSTG-PLATFORM-3

MSTG-PLATFORM-4

OWASP MOBILE:

M3

Description:

Allow local file access with webview. Please ensure your code not to allow path traversal.

詳細資訊:

.

lab_19 - SSL Verification Fail

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.4.2.2 - The mobile application shall verify the validity of the server certificate.

4.1.4.2.3 - The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.

✓ Passed

MSTG:

MSTG-NETWORK-3

MSTG-NETWORK-4

OWASP MOBILE:

M3

Description:

Check the SSL Certificate information.

詳細資訊:

.

✓ Passed	<p>lab_20 - Possible hardcoded information</p> <p>Description: The use of a hard-coded password increases the possibility of password guessing tremendously. Keyword: CCCrypt, CCAAlgorithm</p> <p>詳細資訊: .</p>
✓ Passed	<p>lab_21 - USE URL</p> <p>Description: URL found during analysis, check if there are some suspicious URL. Keyword:Use URL schemes with</p> <p>詳細資訊: · Use URL schemes with jp.mufig.bk.applisp.01:// Use URL schemes with krt-e8fce022c2473be3329d807108d13b10:// Use URL schemes with jp.mufig.bk.applisp.app.af:// Use URL schemes with krt-a316f49cff803b6a8e7d868fbff8e831:// Use URL schemes with krt-7ff85aabff1e67c5c266e1fab8b4e479://</p>
✓ Passed	<p>lab_22 - ENCRYPTION_AES/DES/MD5 Cipher&Degist; Method found</p> <p>Standard Testing Guide of Industrial Development Board, R.O.C.: 4.1.2.3.6 - Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.</p> <p>MSTG: MSTG-STORAGE-14 MSTG-CRYPTO</p> <p>OWASP MOBILE:</p> <p>詳細資訊: .</p>

lab_23 - Keychain dump

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.10 - The mobile application shall use system credential storage facilities appropriately to store sensitive data.

MSTG:

MSTG-STORAGE-1

MSTG-STORAGE-2

✓ Passed

Description:

While it can improve the efficiency and availability of the application, it also carries risks. To protect the security of sensitive user information, a better approach is to store the keychain in iOS's secure storage areas, such as the Secure Enclave or iCloud Keychain. Keyword: PrivateFrameworks

詳細資訊:

.

lab_24 - Make use of log function

Standard Testing Guide of Industrial Development Board, R.O.C.:

4.1.2.3.4 - The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.

4.1.2.3.5 - The mobile application shall avoid storing sensitive data in redundant files or log files.

MSTG:

MSTG-STORAGE-3

MSTG-STORAGE-13

⚠ Detected

OWASP MOBILE:

M10

Description:

Log function in this application, you should notice is there sensitive information in these logs. Keyword: Foundation, NSLog

詳細資訊:

· Make use of log function NSLog with ["Can't find keyplane that supports type %ld for keyboard %@; using %@"]

URL in the App

No URL detected in app