



機密

臺藝大智慧行動 行動應用 APP 基本資安檢測報告

檢測報告編號	A0173-2608006-Yi0
送檢單位名稱	國立臺灣藝術大學
報告郵寄地址	220 新北市板橋區浮洲里大觀路一段 59 號
作業系統版本	iPhone (iOS 13.0 以上)
檢測安全等級	☐ L1 ☒ L2 ☐ L3 ☐ L1+F ☐ L2+F ☐ L3+F
檢測報告版別	☒ 初測 ☐ 複測
檢測物件版號	V 1.0.1
檢測物件收件日期	2026 年 07 月 22 日
檢測期間	2026 年 08 月 18 日~2026 年 08 月 24 日
報告製作日期	2026 年 08 月 24 日

行動檢測服務股份有限公司-智能物聯網資安檢測實驗室

實驗室地址：新北市中和區建一路 150 號 9F-4

聯絡電話：(02) 8226-3279

傳真電話：(02) 8221-5288

備註：

1. 本檢測結果報告，僅適用於送檢測樣本，如對檢測結果有疑問，請於七日內向本實驗室查詢。
2. 本報告書僅為參考，不得以任何方式作為商業廣告及其他宣傳之用途。

行動應用 App 基本資安檢測結果摘要

國立臺灣藝術大學 本次送檢測之行動應用 APP 共為 1 支，依據 **行動應用資安聯盟行動應用 App 基本資安檢測基準 V4.0**，共檢測 31 項目，檢測結果有 27 項符合基準要求，3 項不符合基準要求，1 項不適用。詳細檢測結果報告，請詳見內文。

符合要求/不符合要求/不適用事項摘要表

項次	技術要求	結果
1	4.1.1.1.2. 行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途 (L1、L2、L3)	符合基準
2	4.1.1.3.1. 行動應用程式開發者應提供回報安全性問題之管道 (L2、L3)	符合基準
3	4.1.2.1.1. 行動應用程式應於蒐集敏感性資料前，取得使用者同意 (L1、L2、L3)	符合基準
4	4.1.2.1.2. 行動應用程式應提供使用者拒絕蒐集敏感性資料之權利 (L1、L2、L3)	符合基準
5	4.1.2.3.1. 行動應用程式應於儲存敏感性資料前，取得使用者同意 (L1、L2、L3)	符合基準
6	4.1.2.3.2. 行動應用程式應提供使用者拒絕儲存敏感性資料之權利 (L1、L2、L3)	符合基準
7	4.1.2.3.4. 行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中 (L1、L2)	符合基準
8	4.1.2.3.6. 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存 (L1、L2、L3)	符合基準
9	4.1.2.3.7. 敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取 (L1、L2、L3)	符合基準
10	4.1.2.3.8. 敏感性資料應避免出現於行動應用程式之程式碼 (L1、L2、L3)	符合基準
11	4.1.2.3.11. 行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉 (L2、L3)	符合基準
12	4.1.2.3.12. 行動應用程式應避免在 IPC 機制中洩漏敏感性資料 (L1、L2、L3)	符合基準
13	4.1.2.3.13. 行動應用程式中的使用者介面應避免洩漏敏感性資料 (L2、L3)	不符合基準
14	4.1.2.3.16. 行動應用程式應避免將敏感性資料儲存或輸出於系統日誌 (L1、L2、L3)	符合基準
15	4.1.2.4.1. 行動應用程式透過網路傳輸資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密 (L1、L2、L3)	符合基準

本文件著作權屬行動檢測服務股份有限公司所有，未經本公司許可不准引用或翻印。

A0173-2608006-Yi0-臺藝大智慧行動-V1.0.1

項次	技術要求	結果
16	4.1.2.5.1. 行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意 (L1、L2、L3)	符合基準
17	4.1.2.5.2. 行動應用程式應提供使用者拒絕分享敏感性資料之權利 (L1、L2、L3)	符合基準
18	4.1.2.5.3. 行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取 (L1、L2、L3)	符合基準
19	4.1.4.1.1. 行動應用程式應有適當之身分鑑別機制，確認使用者身分 (L2、L3)	符合基準
20	4.1.4.1.2. 行動應用程式應依使用者身分授權 (L2、L3)	符合基準
21	4.1.4.2.1. 行動應用程式應避免使用具有規則性之交談識別碼 (L2、L3)	符合基準
22	4.1.4.2.2. 行動應用程式應確認伺服器憑證之有效性 (L1、L2、L3)	符合基準
23	4.1.4.2.3. 行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發 (L1、L2、L3)	符合基準
24	4.1.4.2.4. 行動應用程式封包流向應與所宣告的內容一致 (L1、L2、L3)	不符合基準
25	4.1.5.1.1. 行動應用程式應避免含有惡意程式碼 (L1、L2、L3)	符合基準
26	4.1.5.1.2. 行動應用程式應避免資訊安全漏洞 (L1、L2、L3)	符合基準
27	4.1.5.1.3. 行動應用程式應針對螢幕覆蓋攻擊進行防護 (L1、L2、L3)	不適用
28	4.1.5.3.1. 行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全 (L1、L2、L3)	符合基準
29	4.1.5.4.1. 行動應用程式應針對使用者於輸入階段之字串，進行安全檢查 (L1、L2、L3)	符合基準
30	4.1.5.4.2. 行動應用程式應提供相關注入攻擊防護機制 (L1、L2、L3)	符合基準
31	4.2.2.1.2. 行動應用程式於 Webview 呈現功能時，所連線之網域應為安全網域 (L1、L2、L3)	不符合基準

檢測人	報告簽署人
鄒興彥	

1. 前言

本報告為行動檢測服務股份有限公司（以下簡稱本公司）下之智能物聯網資安檢測實驗室（以下簡稱本實驗室），針對國立臺灣藝術大學送檢測之行動應用 APP 程式進行安全檢測，並於 08 月 24 日產生檢測結果報告。

2. 行動應用程式之屬性分類

依據行動應用資安聯盟行動應用 App 基本資安檢測基準 V4.0，本次送檢測之行動應用 APP 程式，其分類為「L2」。

行動應用程式屬性分類之定義

「L1」檢測項目	無須使用者身分鑑別之應用程式，須檢測之項目共 25 項。
「L2」檢測項目	須使用者身分鑑別之應用程式，須檢測之項目共 31 項。
「L3」檢測項目	含有交易行為之應用程式，須檢測之項目共 39 項。
F 檢測項目	屬於安全性需求較高之應用程式，為加測項目，須檢測之項目共 9 項。

3. 檢測範圍

本次接受行動應用 APP 程式共 1 支，其檢測範圍與資訊如下：

3.1. 行動應用 APP 程式名稱：

通用名稱	臺藝大智慧行動
唯一識別名稱	tw.edu.ntua.app
APP 版本	V 1.0.1
App 程式檔案 Hash 值	☒ SHA256：(須與申請書相同) 70a2300ccadab58629634260424e418096c54df84eb53fe076ae16f3bf9f3f3a
封包流向國家 (所有)	國內、美國

3.2. 檢測工具:

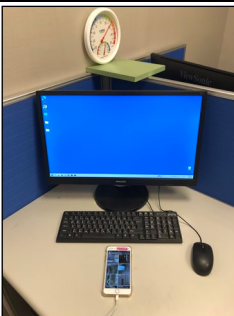
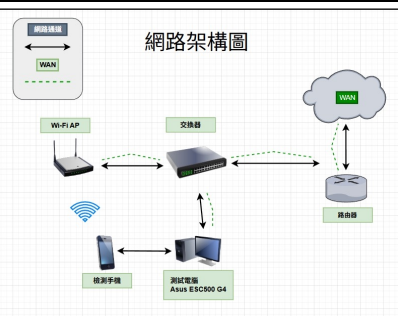
3.2.1 檢測軟體工具

工具名稱	使用說明	版本
Burp Suite	攔截封包，驗證憑證	2025.11.6
Wireshark	攔截封包	4.6.2
ATOM	檔案內容閱讀	1.59.0
iFunbox	iOS 權限偵測	4.0
plist Editor	檔案內容閱讀	2.5.0
OpenSSH	iOS 多功能指令列	8.4-2
Hopper Disassembler	iOS 反編譯	4.5.13
Mob SF	APK.IPA 靜態分析	4.4.0
SSL Kill Switch 3	iOS 繞憑證綁定	1.51
OWASP ZAP	網站弱掃工具	2.17.0
Charles	攔截封包，驗證憑證	4.6.2
Sublime Text	檔案內容閱讀	4126
Introspect	iOS 側錄	0.5.1
Microsoft Visual Studio Community 2022	行動裝置 Log 讀取	17.3.3

3.2.2. 檢測硬體工具

工具名稱	型號
電腦	Asus ESC500 G4
手機	iPhone 8+

3.3. 測試活動記錄：

測試場域	待測物架設
	 

本文件著作權屬行動檢測服務股份有限公司所有，未經本公司許可不准引用或翻印。

A0173-2608006-Yi0-臺藝大智慧行動-V1.0.1

3.4.實驗室聲明：

- 一、本實驗室依據「行動應用 App 基本資安自主檢測推動制度」公告之最新版「行動應用 App 基本資安檢測基準」，及申請機構與實驗室所約定之行動應用 App 檢測項目(包括但不限於：敏感性資料蒐集、敏感性資料儲存、敏感性資料傳輸、付費資源使用、付費資源控管、連線管理機制，執行本服務)。
- 二、申請機構所提供之各項文件與資料，應擔保皆與現況、事實相符，且內容均屬一致，並保證無侵害他人任何權利或其他利益，否則願自負一切責任與相關損失，本實驗室不對前述資料的真實性進行驗證，同時亦不保證前述資料之完整性及正確性。
- 三、本服務係在一定範圍、時間及技術條件下執行，實驗室不保證本服務即可檢測出本服務檢測標的之所有弱點。
- 四、本報告內容僅依申請機構所提供之檢測標的進行檢測及報告之撰寫，不對檢測標的以外的物件進行結果驗證，故本實驗室不保證檢測標的以外的物件之可靠性。
- 五、申請機構未取得實驗室於本服務之檢測合格報告，不得宣稱本機構已通過檢測或其他類似之表示，本報告為申請本檢測相關之標章外亦不得作為其他用途。對於任何人因違反前述規定任意傳閱複製或使用本份報告所引發之任何損失，本公司不負任何義務及責任。
- 六、本報告的測試範圍屬資安領域的定性測試，不涉及量測不確定度。根據『行動應用 APP 基本資安檢測基準』，測試結果判定遵循此標準故無額外自訂決定規則。因此，不適用量測不確定度決定規則，不需進行評估。

4. 檢測方法與結果

本章節說明本次送檢之行動應用程式 符合/不符合事項，行動應用 App 基本資安檢測基準 V4.0 的要求說明，並檢附相關佐證資料。

● 4.1.1.1.2 行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途 (L1、L2、L3)

1. 檢測基準：

- 若行動應用程式已發布，檢查行動應用程式是否於應用程式商店，依實際需要說明欲存取之敏感性資料、行動裝置資源及宣告權限用途。
 - 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供欲存取之敏感性資料、行動裝置資源及宣告權限用途之說明。
- 如為「是」則符合檢測基準；「否」則不符合檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(不公開發布)

經過實驗室檢測，行動應用程式已發布於可信任之應用程式商店 App Store 內(圖一)，應用程式商店依實際需要說明欲存取之敏感性資料、行動裝置資源及宣告權限用途之說明(圖二)，檢測結果符合基準。



圖一

圖二

檢測結果圖示

● 4.1.1.3.1 行動應用 App 開發者應提供回報安全性問題之管道 (L2、L3)

1. 檢測基準：

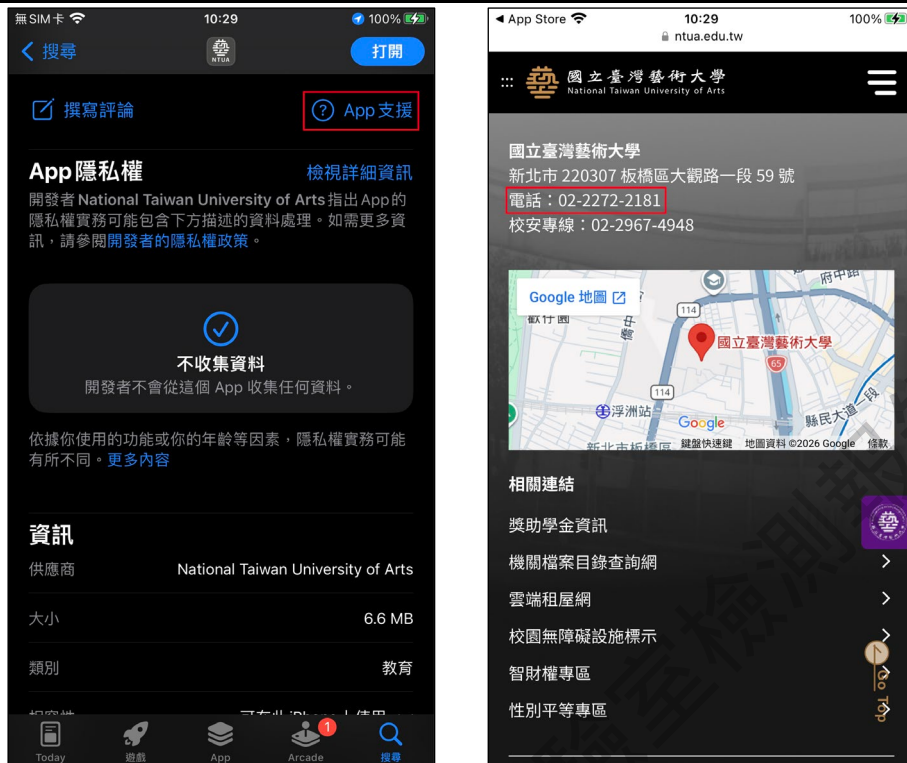
- 若行動應用程式已發布，檢查行動應用程式是否於應用程式商店或行動應用程式內，提供聯絡網頁、留言板、電子郵件、電話或其他類型聯絡方式，並經測試可實際聯絡成功。
 - 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供回報安全性問題之管道與聯絡方式，並經測試可實際聯絡成功。
- 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(不公開發布)

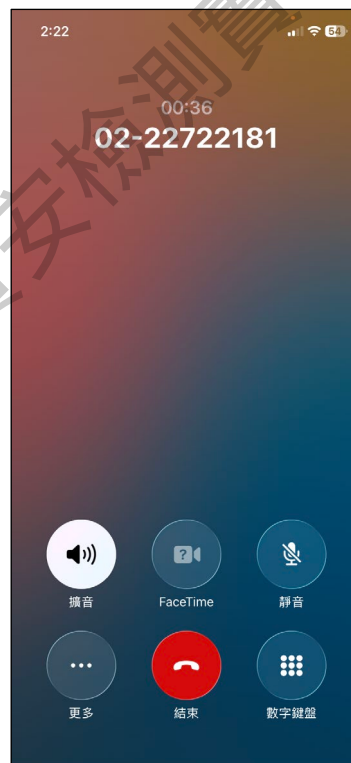
經過實驗室檢測，行動應用程式已發布於 App Store(圖一)，行動應用程式於應用程式商店提供電話的聯絡方式連結(圖二)，並經測試可實際聯絡成功(圖三)，檢測結果符合基準。



圖一



圖二



圖三

檢測結果圖示

● 4.1.2.1.1 行動應用程式應於蒐集敏感性資料前，取得使用者同意 (L1、L2、L3)

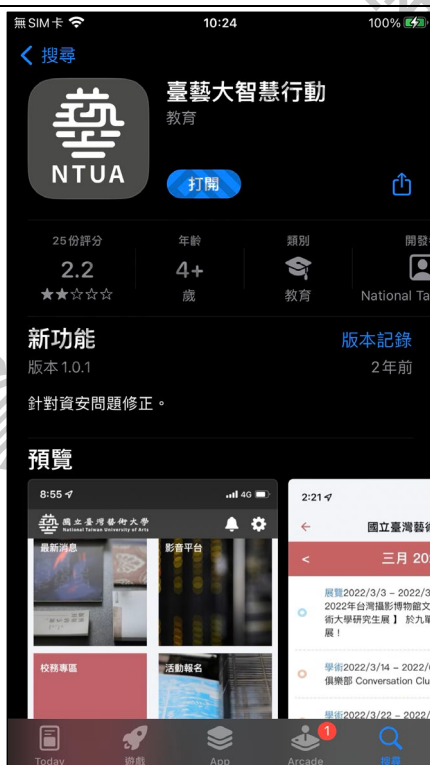
1. 檢測基準：

- 若行動應用程式已發布，檢查行動應用程式所有蒐集之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。
- 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。
- 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。

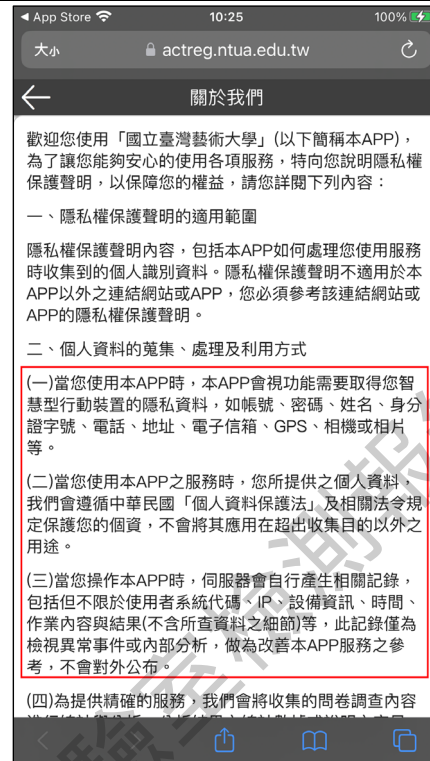
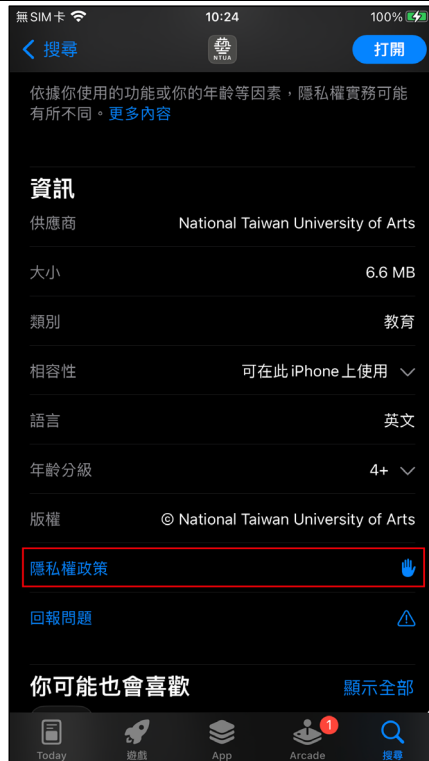
如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

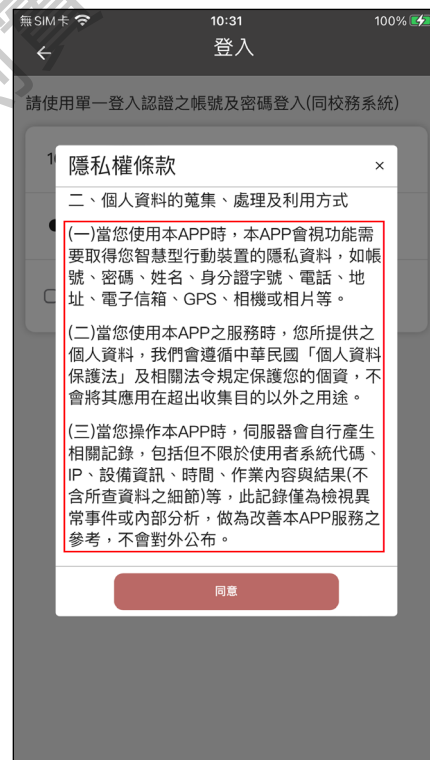
經過實驗室檢測，行動應用程式已發布於 App Store(圖一)，行動應用程式所有蒐集之敏感性資料於應用程式商店內聲明(圖二)，且於行動應用程式內聲明及取得使用者同意(圖三)，檢測結果符合基準。



圖一



圖二



圖三

檢測結果圖示

● 4.1.2.1.2 行動應用程式應提供使用者拒絕蒐集敏感性資料之權利 (L1、L2、L3)

1. 檢測基準：

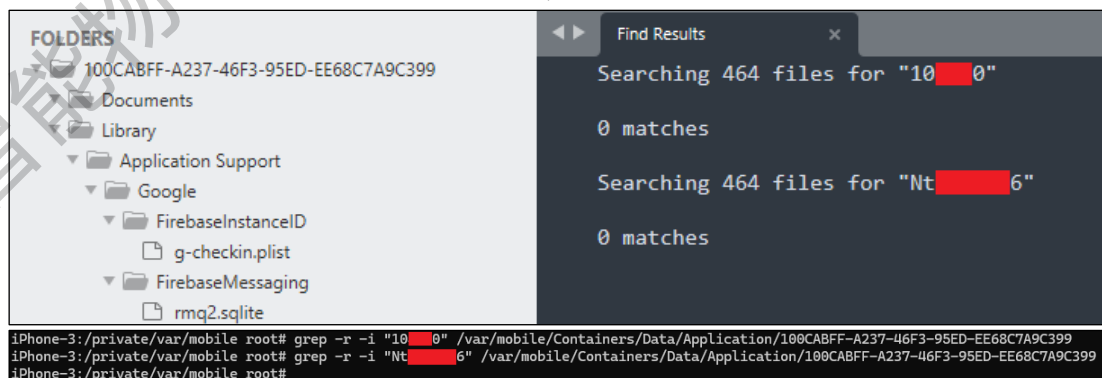
- (1) 檢查行動應用程式是否提供使用者拒絕蒐集敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查在使用者拒絕敏感性資料蒐集的情況下，行動應用程式是否未檢出蒐集敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，基準(1)行動應用程式有提供使用者拒絕蒐集敏感性資料之功能(圖一)；基準(2)在使用者拒絕敏感性資料蒐集的情況下，使用 Sublime Text、OpenSSH 搜尋行動應用程式未檢出蒐集敏感性資料(圖二)，檢測結果符合基準。



圖一



圖二

檢測結果圖示

● 4.1.2.3.1 行動應用程式應於儲存敏感性資料前，取得使用者同意 (L1、L2、L3)

1. 檢測基準：

- 若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。
- 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。
- 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。

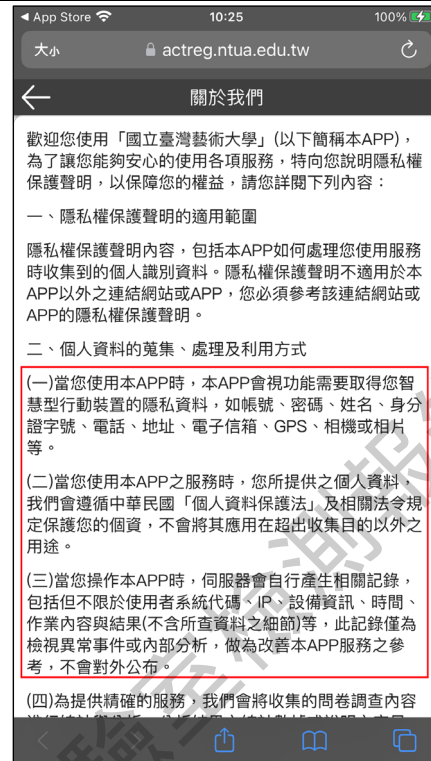
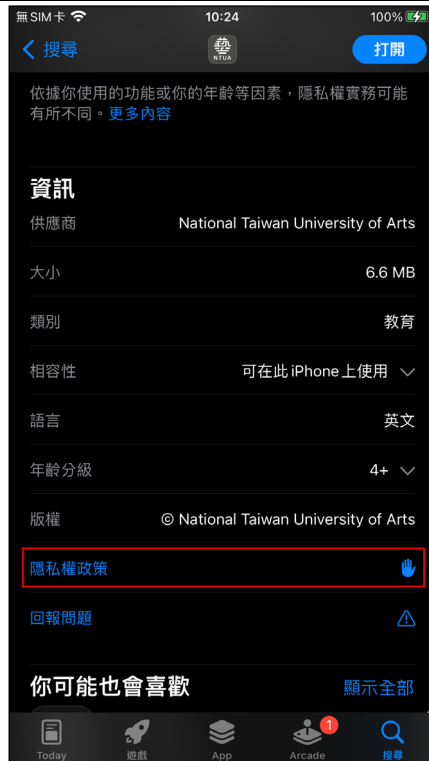
如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

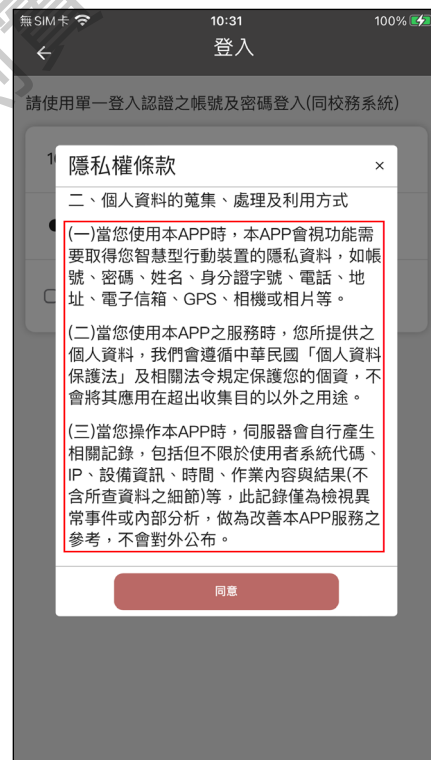
經過實驗室檢測，行動應用程式已發布於App Store(圖一)，行動應用程式所有儲存之敏感性資料於應用程式商店內聲明(圖二)，且於行動應用程式內聲明及取得使用者同意(圖三)，使用Sublime Text、OpenSSH搜尋行動應用程式未檢出蒐集敏感性資料(圖四)，檢測結果符合基準。



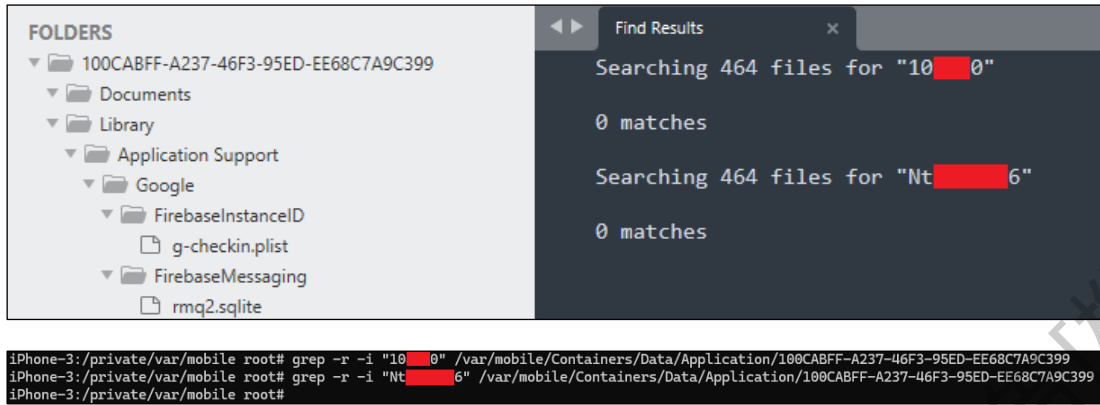
圖一



圖二



圖三



圖四

檢測結果圖示

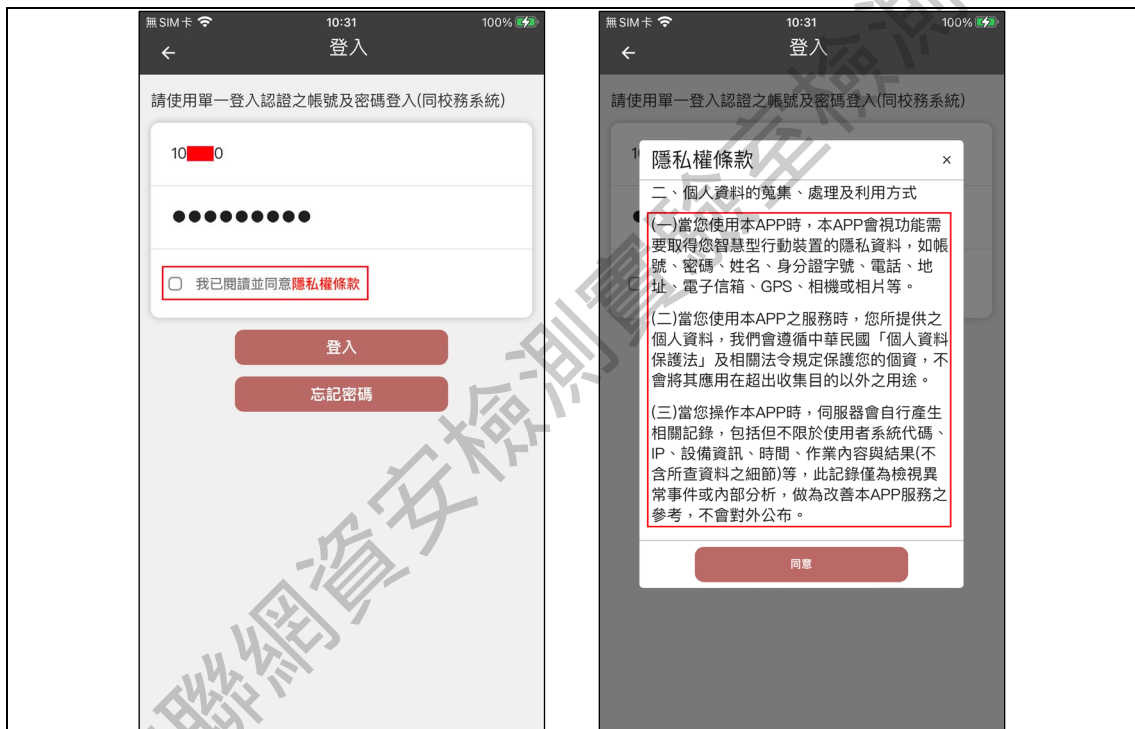
● 4.1.2.3.2 行動應用程式應提供使用者拒絕儲存敏感性資料之權利 (L1、L2、L3)

1. 檢測基準：

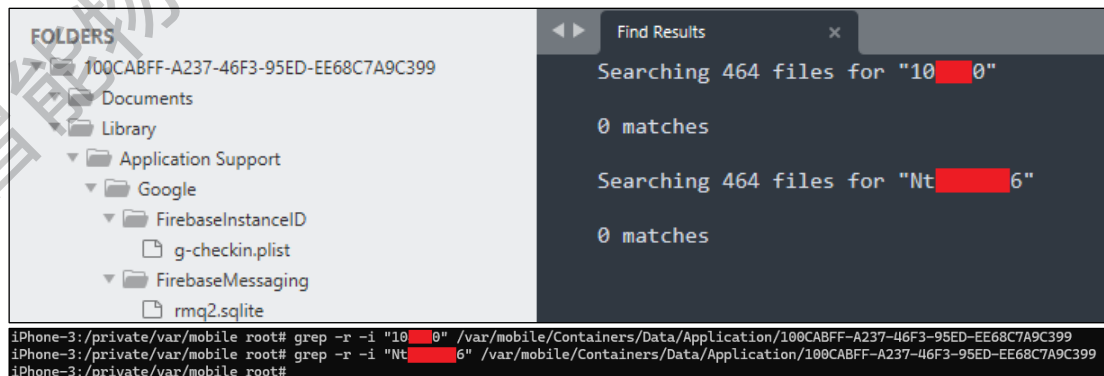
- (1) 檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查在使用者拒絕敏感性資料儲存的情況下，行動應用程式是否未儲存敏感性資料於行動裝置。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，基準(1)行動應用程式有提供使用者拒絕儲存敏感性資料之功能(圖一)；基準(2)在使用者拒絕敏感性資料儲存的情況下，使用 Sublime Text、OpenSSH 搜尋行動應用程式未檢出儲存敏感性資料(圖二)，檢測結果符合基準。



圖一



圖二

檢測結果圖示

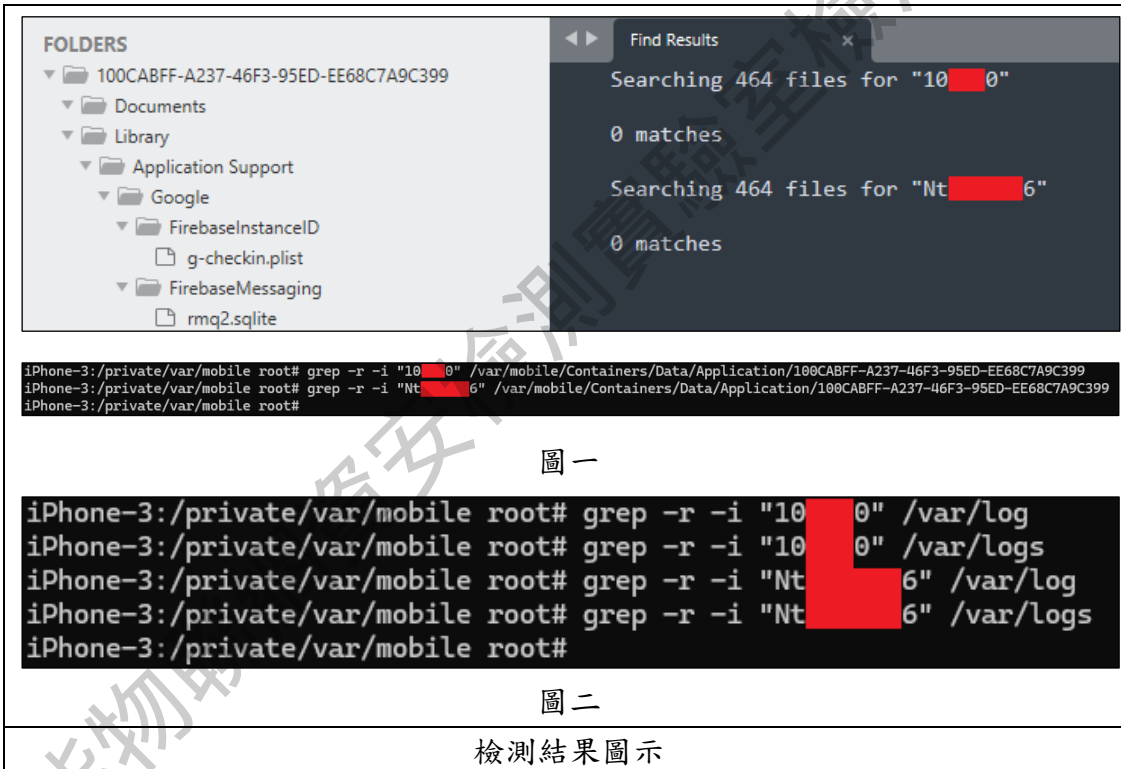
● 4.1.2.3.4.行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中 (L1、L2)

1.檢測基準：

- (1) 檢查行動應用程式是否於關閉及登出後未檢出將敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式是否於關閉及登出後未檢出將敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2.檢測結果： ☒符合 ☐不符合

經過實驗室檢測，使用 Sublime Text、OpenSSH 連線搜尋，基準(1)行動應用程式於關閉及登出後未檢出將敏感性資料儲存於冗餘檔案(圖一)；基準(2)行動應用程式於關閉及登出後未檢出將敏感性資料儲存於日誌檔案(圖二)，檢測結果符合基準。



檢測結果圖示

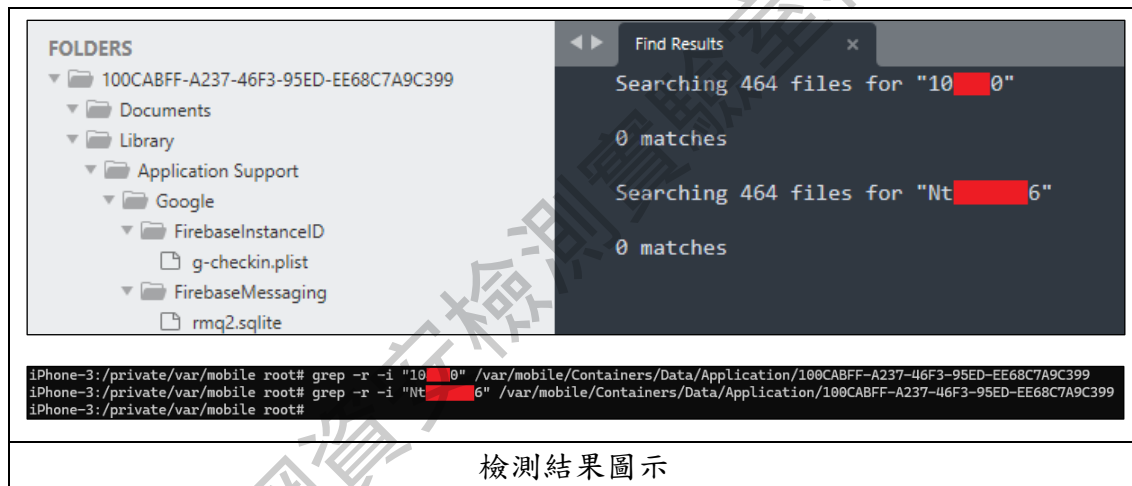
● 4.1.2.3.6 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存 (L1、L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式之非冗餘檔案及非日誌檔案內之敏感性資料是否僅採用金鑰有效長度為128位元（含）以上之先進加密標準（AES），或使用 ChaCha20。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式所使用之加密函式之金鑰是否僅採用符合ANSI X9.17、FIPS 140-3、NIST SP 800-22及SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，使用 Sublime Text、OpenSSH 搜尋行動應用程式未檢出儲存敏感性資料，檢測結果符合基準。



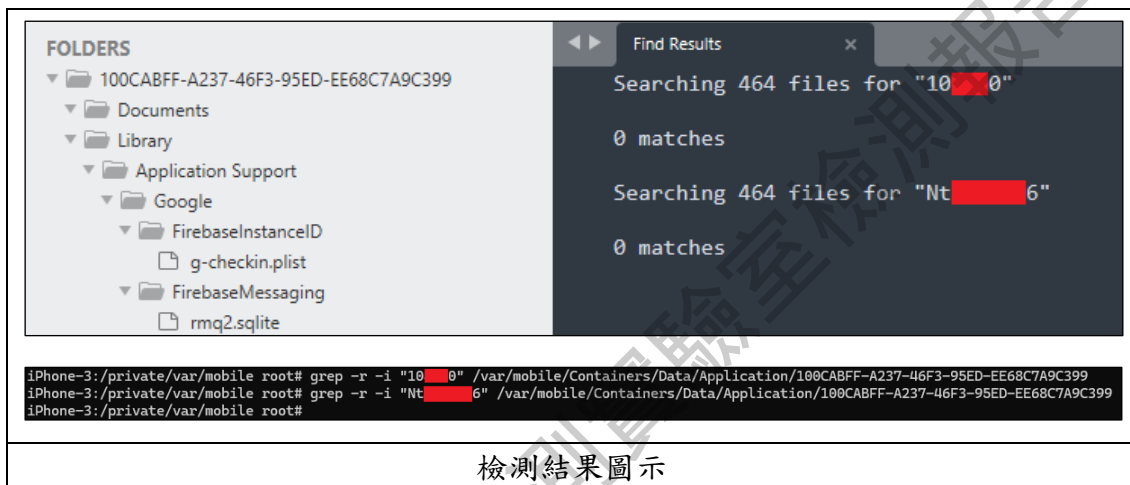
- 4.1.2.3.7 敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式是否儲存敏感性資料於其他行動應用程式預設無法存取之區域。如為「是」則符合檢測基準；「否」則不符合檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(4.1.2.3.4 不符合)

經過實驗室檢測，使用 Sublime Text、OpenSSH 搜尋行動應用程式未檢出儲存敏感性資料，檢測結果符合基準。



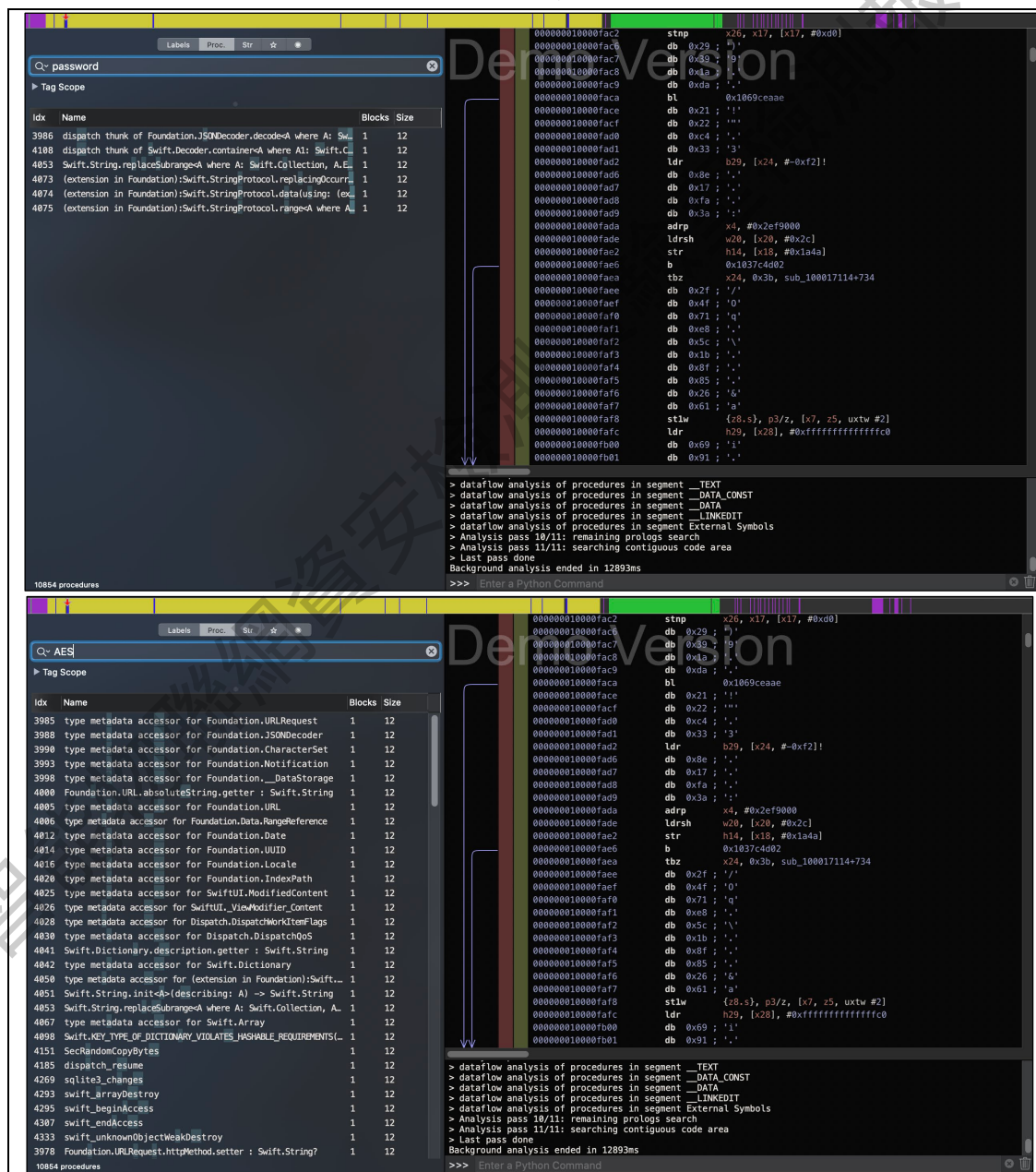
● 4.1.2.3.8 敏感性資料應避免出現於行動應用程式之程式碼 (L1、L2、L3)

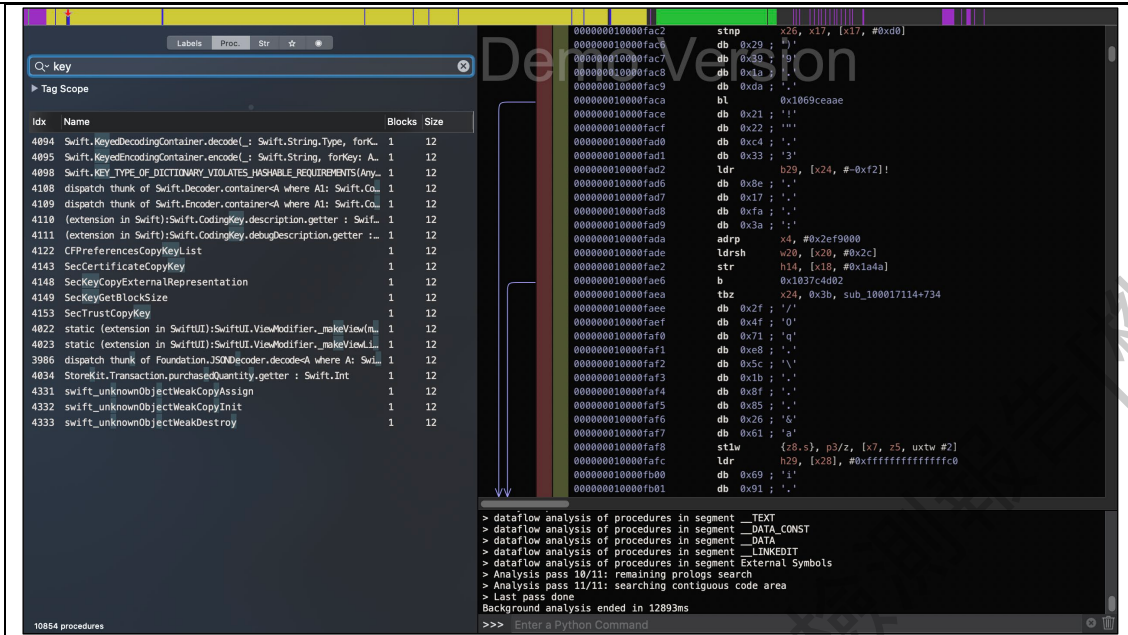
1. 檢測基準：

檢查行動應用程式之程式碼與行動應用程式安裝檔內其他檔案，是否未檢出密碼、身分認證資訊或對稱式加解密演算法之金鑰。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，使用 Hopper Disassembler 工具將測試樣本打開，找出與登入、儲存、加解密、付費相關的單元，並針對每個 procedure 去檢查，則未檢出有密碼或金鑰相關之 hard code，檢測結果符合基準。





檢測結果圖示

● 4.1.2.3.11 行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉 (L2、L3)

1. 檢測基準：

- 檢查行動應用程式是否在輸入敏感性資料欄位中將鍵盤快取機制關閉。
- 檢查行動應用程式於使用者輸入敏感性資料時，是否未自動修正且未帶入可能字串。

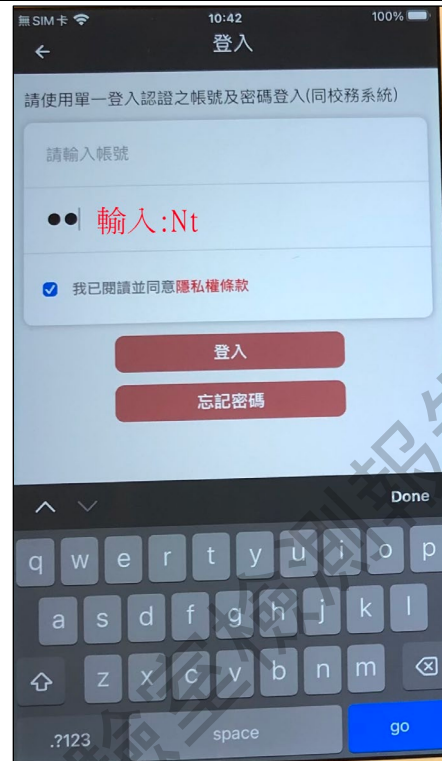
如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式在登入欄位輸入敏感性資料(帳號：10***0、密碼：Nt*****6)後且成功登入(圖一)；登出後於相同欄位輸入身分證號「10」、密碼「Nt」時，未自動修正且未帶入可能字串(圖二)；使用 OpenSSH 連線搜尋行動應用程式未檢出將敏感性資料儲存在鍵盤快取檔案中(圖三)，檢測結果符合基準。



圖一



圖二

```
iPhone-3:/private/var/mobile root# grep -r -i "10" /private/var/mobile/Library/Keyboard
iPhone-3:/private/var/mobile root# grep -r -i "Nt" /private/var/mobile/Library/Keyboard
iPhone-3:/private/var/mobile root#
```

圖三

檢測結果圖示

● 4.1.2.3.12 行動應用程式應避免在 IPC 機制中洩漏敏感性資料 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式是否未於 IPC 機制中洩漏敏感性資料給不特定來源，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(未使用 IPC 機制)

經過實驗室檢測，iOS 環境提供較少選項給不同行動應用程式之間通訊，且都採間接方式通訊，檢視"Custom URL Schemes"方式，使用 MobSF 搜尋 Info.plist 檔案，搜尋"CFBundleURLSchemes"有發現(圖一)；檢視 Binary Analysis 並未發現 IPC 相關訊息(圖二)；行動應用程式介面未提供與其他 App 共享機制(圖三)，參考 4.1.2.5.1、4.1.2.5.2、4.1.2.5.3；使用 OpenSSH 搜尋行動應用程式未檢出蒐集敏感性資料(圖四)，檢測結果符合基準。



圖一

IPA BINARY ANALYSIS

Search:

PROTECTION	STATUS	SEVERITY	DESCRIPTION
ARC	True	Info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
CODE SIGNATURE	True	Info	This binary has a code signature.
ENCRYPTED	True	Info	This binary is encrypted.
NX	True	Info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
PIE	True	Info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
RPATH	True	Warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
STACK CANARY	True	Info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
SYMBOLS STRIPPED	True	Info	Debug Symbols are stripped

圖二



圖三

```

iPhone-3:/private/var/mobile root# grep -r -i "10" /var/mobile/Containers/Data/Application/100CABFF-A237-46F3-95ED-EE68C7A9C399
iPhone-3:/private/var/mobile root# grep -r -i "Nt" /var/mobile/Containers/Data/Application/100CABFF-A237-46F3-95ED-EE68C7A9C399
iPhone-3:/private/var/mobile root#
  
```

圖四

檢測結果圖示

本文件著作權屬行動檢測服務股份有限公司所有，未經本公司許可不准引用或翻印。

A0173-2608006-Yi0-臺藝大智慧行動-V1.0.1

● 4.1.2.3.13 行動應用程式中的使用者介面應避免洩漏敏感性資料 (L2、L3)

1. 檢測基準：

檢查行動應用程式執行時，是否對於敏感性資料進行防護，顯示於使用者介面之敏感性資料(至少包含密碼與信用卡卡號)應有遮蔽設計。若有敏感性資料項不進行遮蔽，應敘明原因。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☐ 符合 ☒ 不符合

經過實驗室檢測，行動應用程式執行時，顯示於使用者介面之「密碼」有遮蔽設計；「帳號」不進行遮蔽(圖一)，廠商未敘明不進行遮蔽之原因(圖二)，檢測結果不符合基準。



圖一

2 7.	備註	請輸入備註
---------	----	-------

圖二

檢測結果圖示

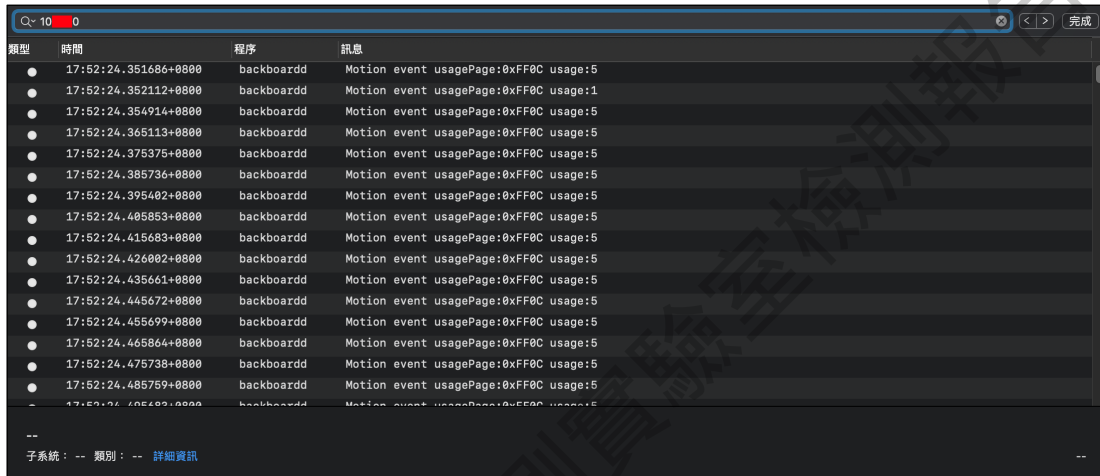
● 4.1.2.3.16 行動應用程式應避免將敏感性資料儲存或輸出於系統日誌 (L1、L2、L3)

1. 檢測基準：

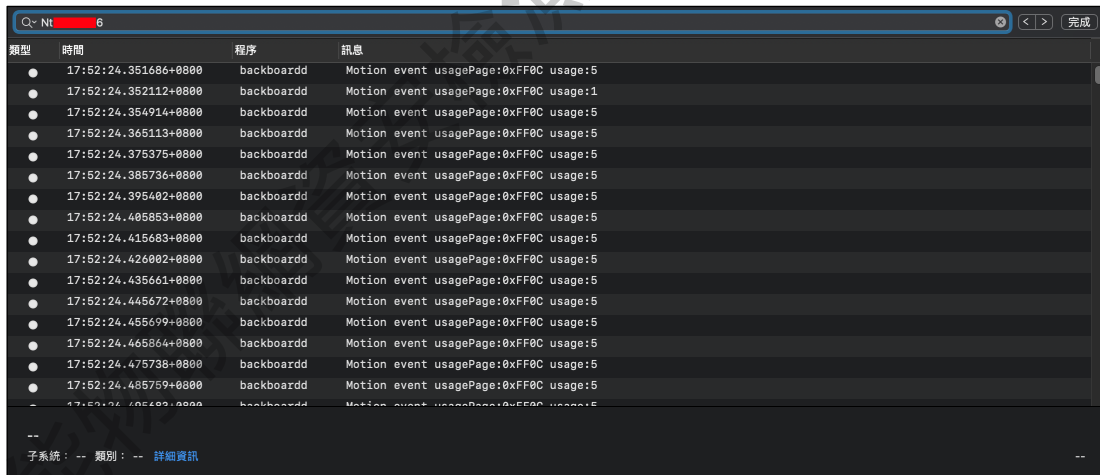
檢查行動應用是否將敏感性資料儲存或輸出於系統日誌中，如為「是」則不符合本項檢測基準；「否」則符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式未將敏感性資料輸出於系統日誌中，檢測結果符合基準。



類型	時間	程序	訊息
●	17:52:24.351686+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.352112+0800	backboardd	Motion event usagePage:0xFF0C usage:1
●	17:52:24.354914+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.365113+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.375375+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.385736+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.395402+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.405853+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.415683+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.426002+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.435661+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.445672+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.455699+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.465864+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.475738+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.485759+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.495402+0800	backboardd	Motion event usagePage:0xFF0C usage:5



類型	時間	程序	訊息
●	17:52:24.351686+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.352112+0800	backboardd	Motion event usagePage:0xFF0C usage:1
●	17:52:24.354914+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.365113+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.375375+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.385736+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.395402+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.405853+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.415683+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.426002+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.435661+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.445672+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.455699+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.465864+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.475738+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.485759+0800	backboardd	Motion event usagePage:0xFF0C usage:5
●	17:52:24.495402+0800	backboardd	Motion event usagePage:0xFF0C usage:5

檢測結果圖示

● 4.1.2.4.1 行動應用程式透過網路傳輸資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密 (L1、L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式是否僅採用 TLS 1.2 (含) 以上版本加密協定傳輸資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式是否僅採用金鑰有效長度為 2048 位元 (含) 以上之 RSA 加密演算法，或採用金鑰有效長度為 224 位元 (含) 以上之橢圓曲線加密演算法 (Elliptic Curve Cryptography)。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (3) 檢查行動應用程式是否僅採用金鑰有效長度為 128 位元 (含) 以上之進階加密標準 (AES)，或使用 TLS 1.2 所支援的加密演算法 (含 ChaCha20)。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，使用 Wireshark 檢視封包，基準(1)行動應用程式採用 TLS 1.2 以上版本加密協定傳輸敏感性資料；基準(3)採用金鑰有效長度 128 位元以上之進階加密標準(AES)(圖一)；基準(2)數位憑證採用金鑰有效長度 2048 位元以上之 RSA 加密演算法(圖二)，檢測結果符合基準。

No.	Time	Source	Destination	Protocol	Length	Info
373	41.945551700	192.168.137.86	120.97.121.132	TLSv1.2	738	Application Data
374	41.945552100	192.168.137.86	120.97.121.132	TCP	66	62798 → 443 [ACK] Seq=1 Ack=1 Win=131104 L...
375	41.945554200	192.168.137.86	120.97.121.132	TLSv1.2	583	Client Hello (SNI=appweb.ntua.edu.tw)
376	41.946741800	192.168.137.86	120.97.121.132	TCP	66	62799 → 443 [ACK] Seq=1 Ack=1 Win=131104 L...
377	41.946743500	192.168.137.86	120.97.121.132	TLSv1.2	583	Client Hello (SNI=appweb.ntua.edu.tw)
378	41.946837900	120.97.121.132	192.168.137.86	TLSv1.2	1404	Server Hello
379	41.946979200	120.97.121.132	192.168.137.86	TCP	1404	443 → 62795 [ACK] Seq=1339 Ack=518 Win=140...
380	41.947116300	120.97.121.132	192.168.137.86	TLSv1.2	1056	Certificate, Server Key Exchange, Server H...
381	41.948870900	120.97.121.132	192.168.137.86	TCP	66	443 → 62797 [ACK] Seq=1 Ack=518 Win=14017 ...
382	41.948894300	120.97.121.132	192.168.137.86	TCP	66	443 → 62796 [ACK] Seq=1 Ack=518 Win=14017 ...
383	41.948956300	192.168.137.86	120.97.121.132	TCP	66	62795 → 443 [ACK] Seq=518 Ack=2677 Win=128...

> Frame 378: 1404 bytes on wire (11232 bits), 1404 bytes captured (11232 bits) on interface \Device\NPF_{9B8CD2EA-C51E-4732-9F69-517}

> Ethernet II, Src: CenturyXinya_d5:da:2a (90:de:80:d5:da:2a), Dst: 1e:64:a0:b2:74:b8 (1e:64:a0:b2:74:b8)

> Internet Protocol Version 4, Src: 120.97.121.132, Dst: 192.168.137.86

> Transmission Control Protocol, Src Port: 443, Dst Port: 62795, Seq: 1, Ack: 518, Len: 1338

✓ Transport Layer Security

 TLSv1.2 Record Layer: Handshake Protocol: Server Hello

 Content Type: Handshake (22)

 Version: TLS 1.2 (0x0303)

 Length: 91

 Handshake Protocol: Server Hello

 Handshake Type: Server Hello (2)

 Length: 87

 Version: TLS 1.2 (0x0303)

 Random: ceef7617056ce0b3bcd8060a00eb7d80e185c008f2151b63025620397ff9a283

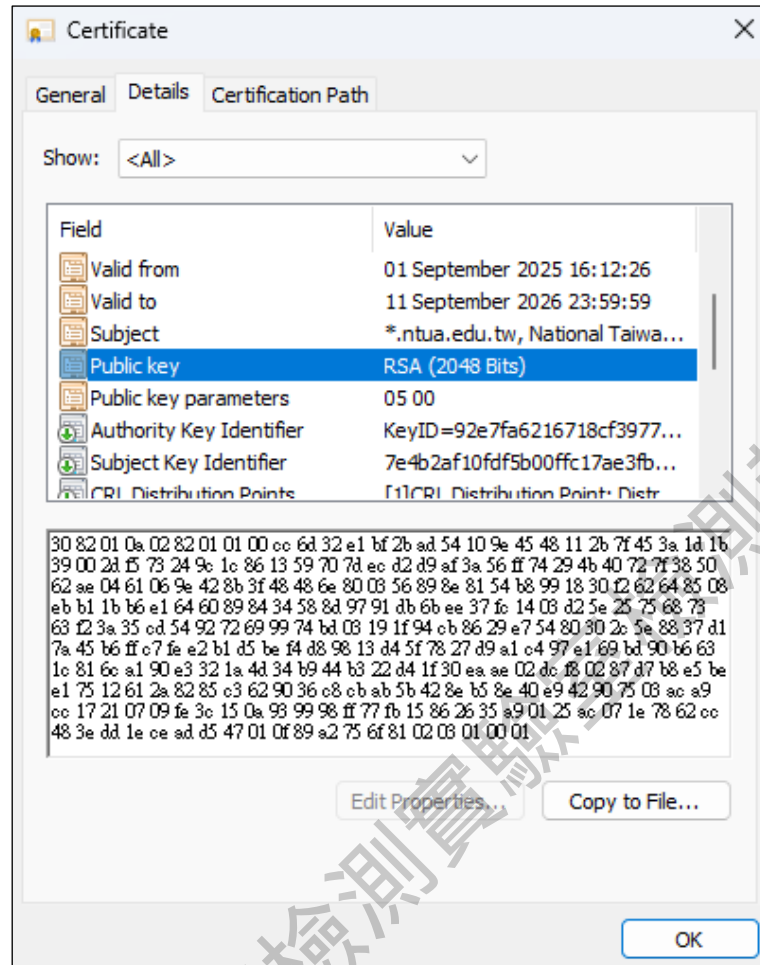
 Session ID Length: 32

 Session ID: 0f2219a4b3765c18960ab83ebadea5c102c6f4eb64285d7264cdf976cbac3510

 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

 Compression Method: null (0)

圖一



圖二

檢測結果圖示

● 4.1.2.5.1 行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意 (L1、L2、L3)

1. 檢測基準：

- 若行動應用程式已發布，檢查行動裝置內之不同行動應用程式間，分享敏感性資料前，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。
- 若行動應用程式尚未發布，檢查調查表內是否有填寫「行動應用程式分享敏感性資料之預計分享內容、用途說明及如何取得使用者同意、分享之應用程式（已發布不須填寫）」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。
- 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。

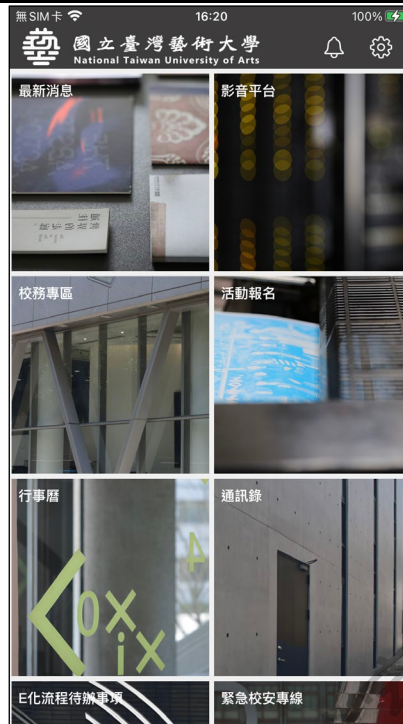
如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

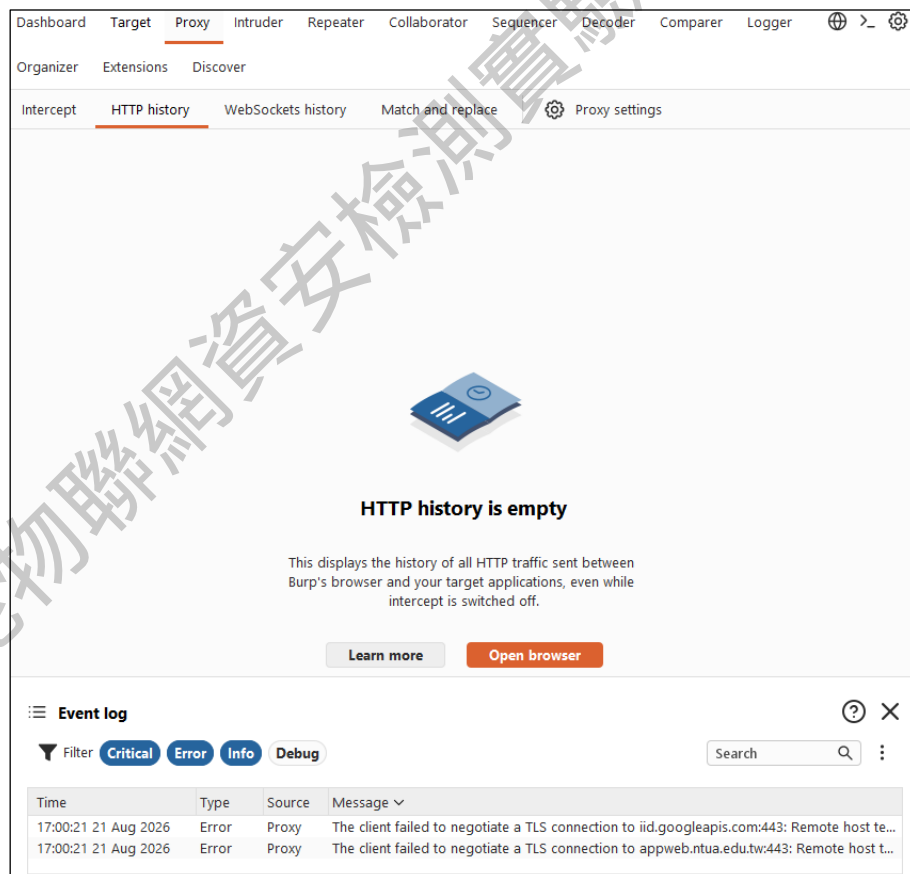
經過實驗室檢測，行動應用程式已發布(圖一)，行動應用程式並未與其他應用程式分享敏感性資料(圖二)；使用 Burp Suite 也無法攔截到相關資訊(圖三)，檢測結果符合基準。



圖一



圖二



圖三

檢測結果圖示

● 4.1.2.5.2 行動應用程式應提供使用者拒絕分享敏感性資料之權利 (L1、L2、L3)

1. 檢測基準：

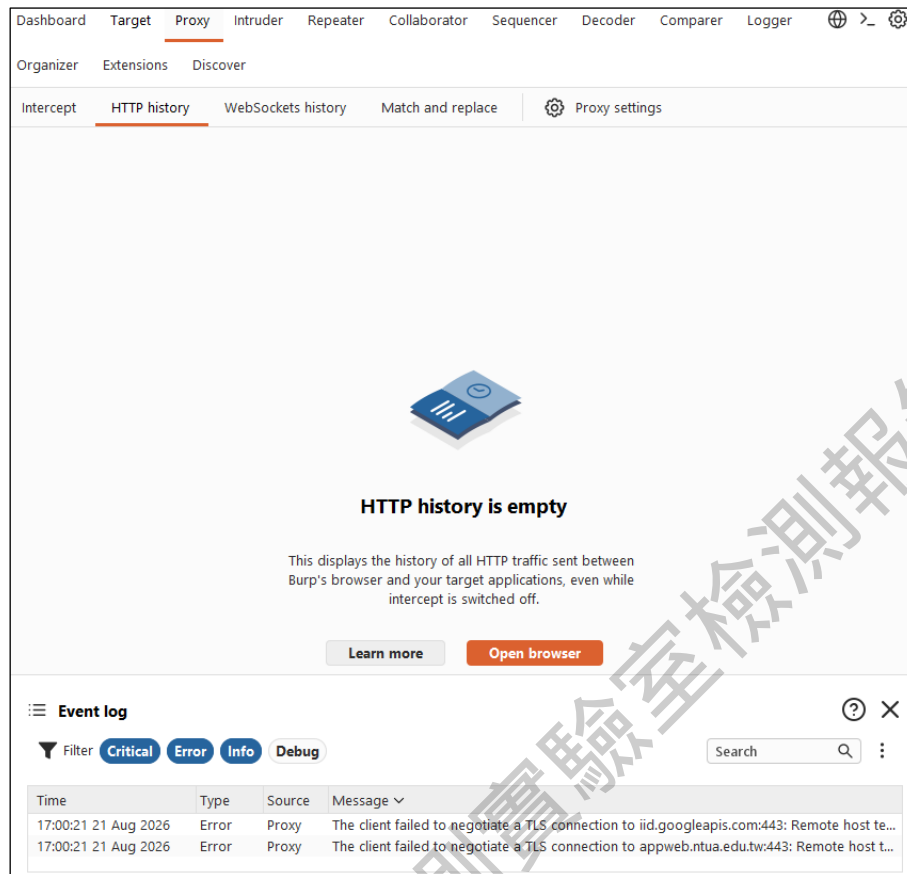
- (1) 檢查行動應用程式是否提供使用者拒絕分享敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查在使用者拒絕敏感性資料分享的情況下，行動應用程式是否未分享敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式並未與其他應用程式分享敏感性資料(圖一)；使用 Burp Suite 也無法攔截到相關資訊(圖二)，檢測結果符合基準。



圖一



圖二

檢測結果圖示

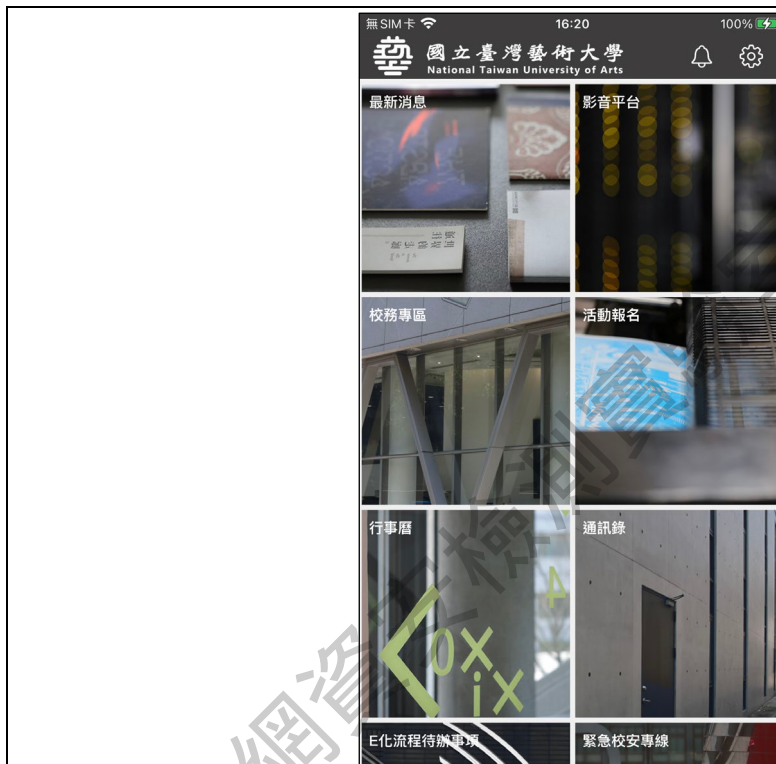
● 4.1.2.5.3 行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取 (L1、L2、L3)

1. 檢測基準：

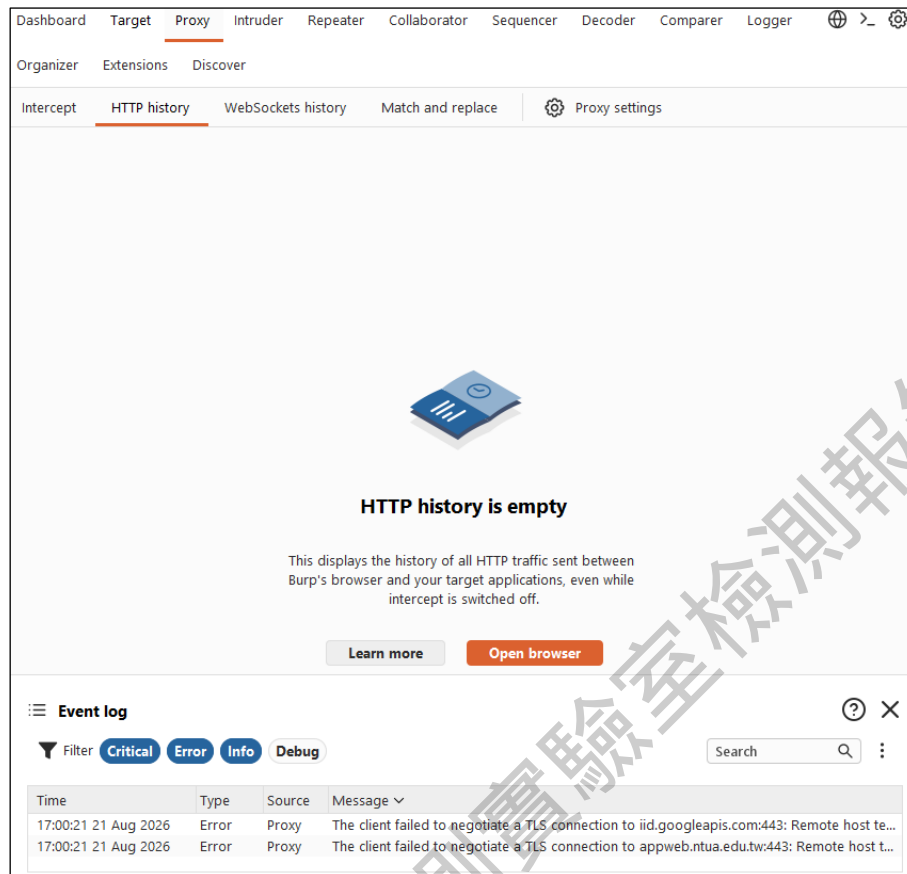
檢查分享敏感性資料之行動應用程式，是否限定特定行動應用程式可存取敏感性資料。如為「是」則符合檢測基準；「否」則不符合檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式並未與其他應用程式分享敏感性資料(圖一)；使用 Burp Suite 也無法攔截到相關資訊(圖二)，檢測結果符合基準。



圖一



圖二

檢測結果圖示

● 4.1.4.1.1 行動應用程式應有適當之身分鑑別機制，確認使用者身分 (L2、L3)

1. 檢測基準：

如行動應用程式存取與個人資料相關之敏感性資料，檢查行動應用程式是否提供鑑別機制。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(經過主管機關同意免身分鑑別與授權)

經過實驗室檢測，行動應用程式存取與個人資料相關之敏感性資料有提供身分鑑別機制(帳號、密碼)，檢測結果符合基準。



檢測結果圖示

● 4.1.4.1.2 行動應用程式應依使用者身分授權 (L2、L3)

1. 檢測基準：

如行動應用程式存取與個人資料相關之敏感性資料，檢查行動應用程式是否提供身分授權機制。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合 ☐ 不適用(經過主管機關同意免身分鑑別與授權)

經過實驗室檢測，行動應用程式以帳號、密碼作為身分鑑別機制(圖一)，依照個別帳號只會授權看到屬於自己的資料(圖二)，檢測結果符合基準。



● 4.1.4.2.1 行動應用程式應避免使用具有規則性之交談識別碼 (L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式是否採用長度為128位元（含）以上之交談識別碼。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式使用之交談識別碼是否未與時間、使用者提交資料、具規則性之數字或字串有直接關聯或難以偽造。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (3) 檢查行動應用程式使用之交談識別碼是否具備登出失效機制。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

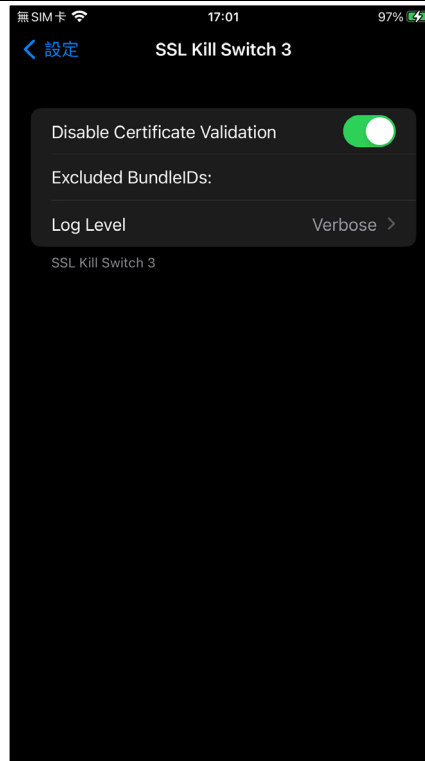
2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式因憑證綁定完整，利用 Burp Suite 進行伺服器之中間人代理無法攔截封包及檢出交談識別碼(圖一)，利用繞過憑證綁定工具 SSL Kill Switch 3 亦失敗無法攔截封包(圖二)，行動應用程式因使用憑證綁定無法取得交談識別碼並難以偽造，符合(1)(2)(3)項目要求，檢測結果符合基準。

依據上述檢測結果與聯盟一致性會議之結論，故判定為符合。



圖一



圖二
檢測結果圖示

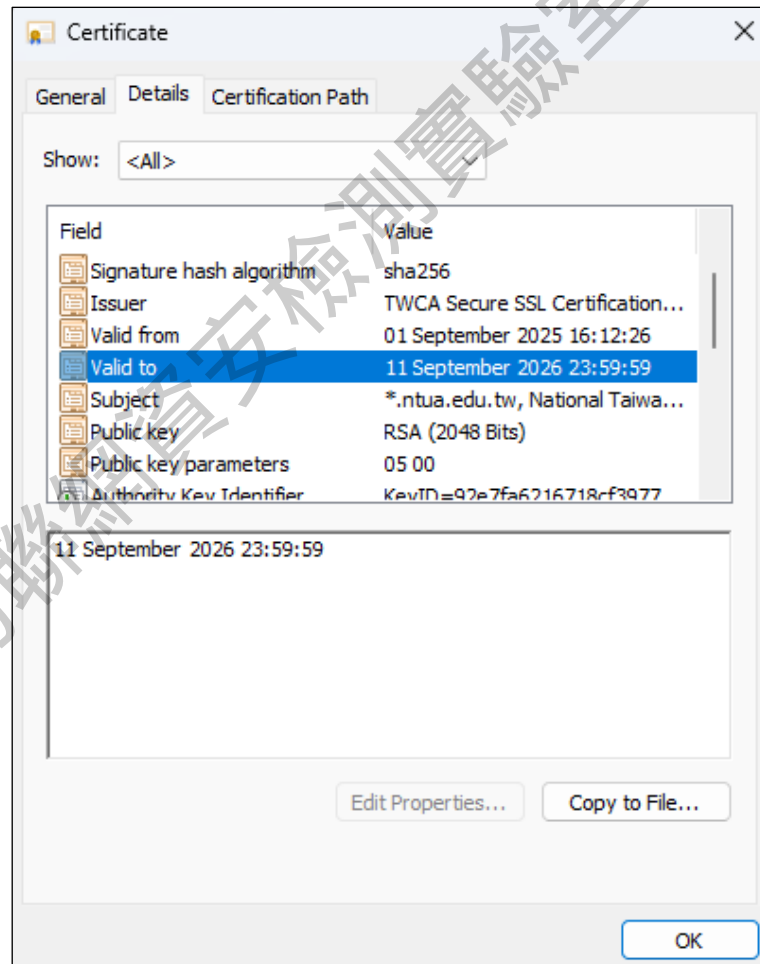
● 4.1.4.2.2 行動應用程式應確認伺服器憑證之有效性 (L1、L2、L3)

1. 檢測基準：

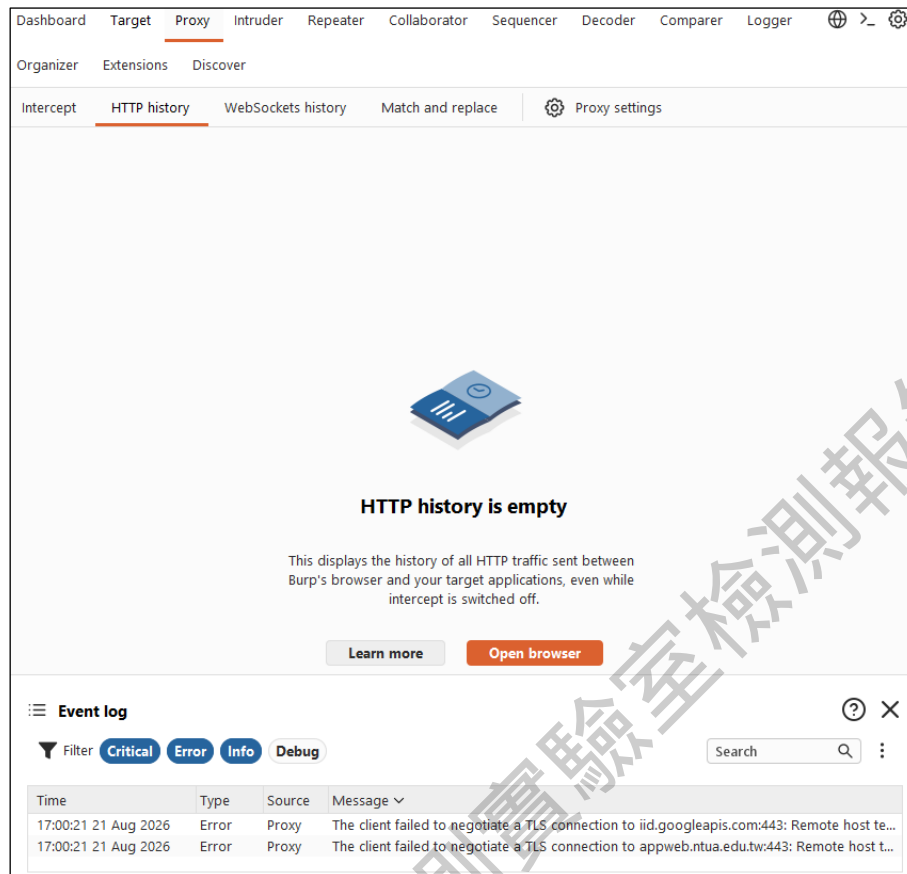
- (1) 檢查行動應用程式使用之伺服器憑證是否仍於有效期間內、未被註銷 (Revoke)，且憑證之主體名稱與主體別名包含連線之伺服器網域名稱。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式是否使用憑證綁定 (Certificate Pinning) 方式驗證，以確保連線之伺服器為行動應用App開發者所指定。若無法預期使用者所連線之網站，則應提示連線目標有變更並有提醒使用者即將連線至其他網站之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，基準(1)行動應用程式使用伺服器憑證仍於有效期間內、未被註銷 (Revoke)，且憑證之主體名稱與主體別名包含連線之伺服器網域名稱(圖一)；基準(2)行動應用程式使用憑證綁定方式驗證，使用 Burp Suite 進行伺服器之中間人代理無法攔截封包(圖二)，檢測結果符合基準。



圖一



圖二

檢測結果圖示

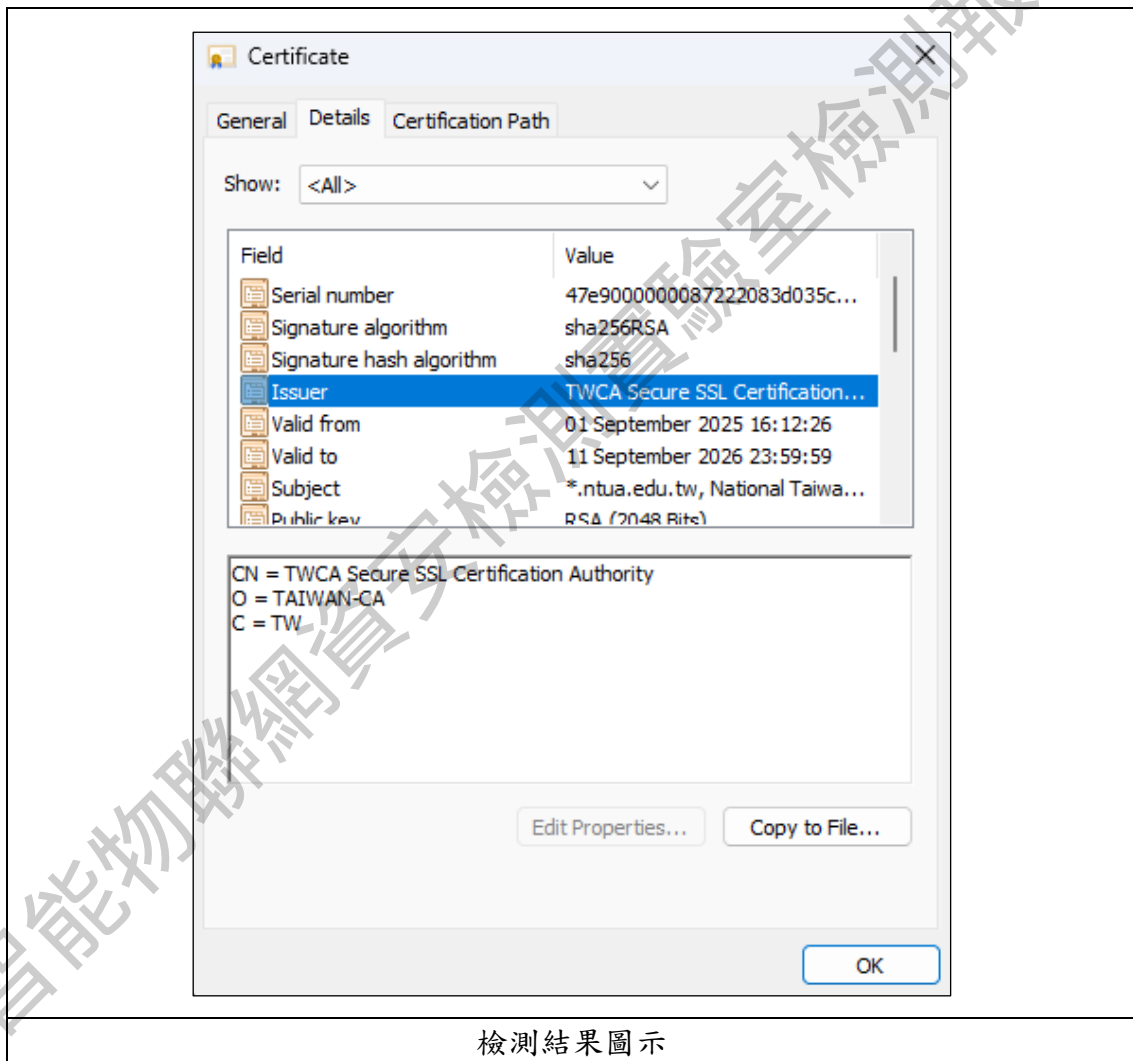
● 4.1.4.2.3 行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式是否驗證並確保伺服器憑證為行動作業系統內建可信任之憑證機構所簽發。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式與伺服器連線使用之伺服器憑證為 TWCA Secure SSL Certification Authority 所簽發，仍在有效期間內、未被註銷，檢測結果符合基準。



● 4.1.4.2.4 行動應用程式封包流向應與所宣告的內容一致 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式封包流向是否與「行動應用APP基本資安檢測資料調查表上」宣告的封包流向一致。如為「是」則符合檢測基準；「否」則不符合檢測基準。

2. 檢測結果： ☐ 符合 ☒ 不符合

經過實驗室檢測，使用 Charles 攔截封包，根據所攔截到的封包查詢所在國家(圖一)，行動應用程式封包流向與「行動應用 APP 基本資安檢測資料調查表上」宣告的封包流向不一致(圖二)，檢測結果不符合基準。



appweb.ntua.edu.tw/120.97.121.132	台灣
iid.googleapis.com/172.217.119.4	美國
www.ntua.edu.tw/120.97.123.119	台灣
www.youtube.com/142.251.155.4	美國
i.ytimg.com/172.253.115.119	美國
googleads.g.doubleclick.net/142.250.31.156	美國
static.doubleclick.net/142.250.188.6	美國
fonts.gstatic.com/142.251.40.227	美國
www.gstatic.com/142.251.211.131	美國
www.google.com/142.251.154.119	美國
jnn-pa.googleapis.com/172.217.112.4	美國
code.jquery.com/151.101.65.155	美國
dsms0mj1bbhn4.cloudfront.net/52.85.31.73	美國
cdn.openshareweb.com/172.67.74.24	美國
yarpp.com/107.20.140.231	美國
jatoflow.ntua.edu.tw/140.131.21.76	台灣
app-analytics-services.com/172.253.115.102	美國

圖一

21	封包流向國家宣告	■ 國內 ■ 其他國家，包括：美國、日本、香港、印度 (如：日本、英國等國家名稱)
22	封包流向網域名稱	google.com (如：apple.com, google.com)

圖二

檢測結果圖示

● 4.1.5.1.1 行動應用程式應避免含有惡意程式碼 (L1、L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式是否未針對其他行動應用程式或行動作業系統之檔案，在未授權情況下，嘗試進行查詢、新增、修改、刪除、存取遠端服務、提權等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準。
- (2) 檢查行動應用程式是否未包括可導致行動作業系統，發生未預期錯誤、資源明顯耗損、重新啟動或關閉等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準。

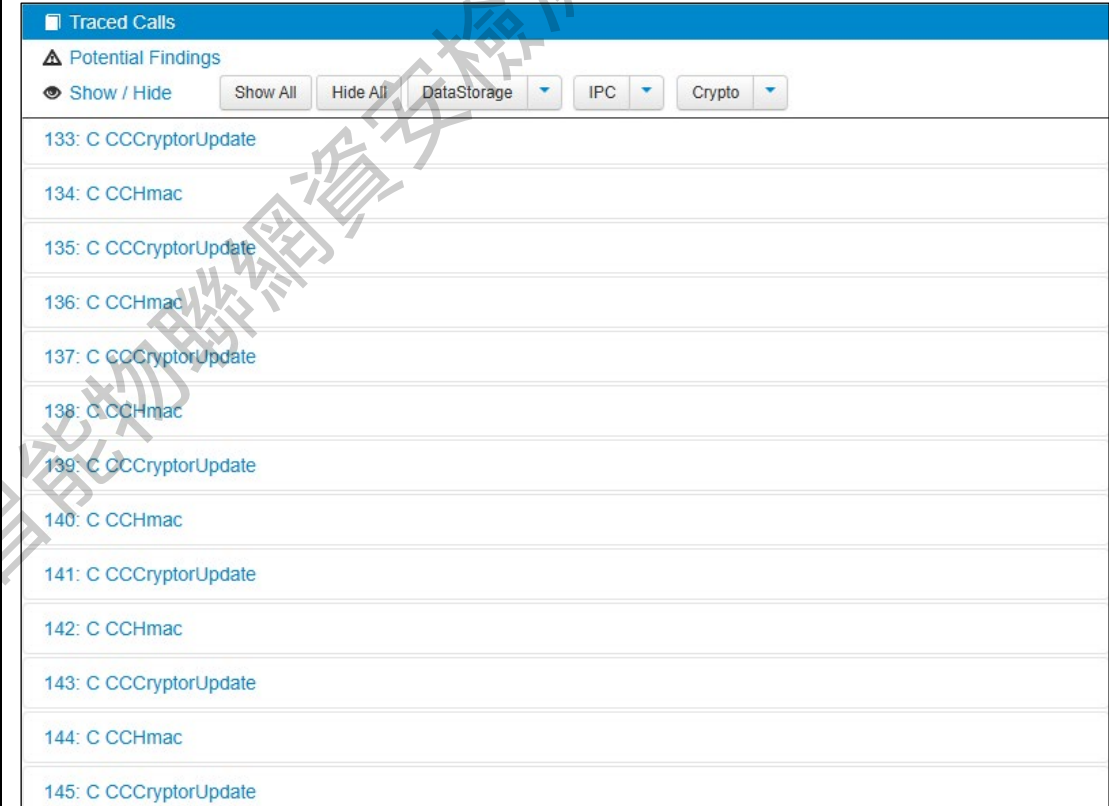
2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，

基準(1)使用 Introspect 工具側錄，行動應用程式未針對其他行動應用程式或行動作業系統之檔案，在未授權情況下，嘗試進行查詢、新增、修改、刪除，行動應用程式未存取位於其他行動應用程式的檔案(圖一)、存取遠端服務(4.1.4.2.2 行動應用程式有使用憑證綁定，防止連向未經授權的遠端服務)、提權(使用 iFunBox 連線手機安裝後未發現 root/JB 行為)(圖二)。

基準(2)使用 OpenSSH 連線 top 指令 CPU 無明顯耗損(圖三)、使用 Microsoft Visual Studio Community 2022 連線執行檢測過程中行動應用程式均未發生未預期錯誤、重新啟動或關閉(圖四)，

檢測結果符合基準。



Traced Calls	
Potential Findings	
Show / Hide Show All Hide All DataStorage IPC Crypto	
133:	C CCCryptorUpdate
134:	C CCHmac
135:	C CCCryptorUpdate
136:	C CCHmac
137:	C CCCryptorUpdate
138:	C CCHmac
139:	C CCCryptorUpdate
140:	C CCHmac
141:	C CCCryptorUpdate
142:	C CCHmac
143:	C CCCryptorUpdate
144:	C CCHmac
145:	C CCCryptorUpdate

圖一

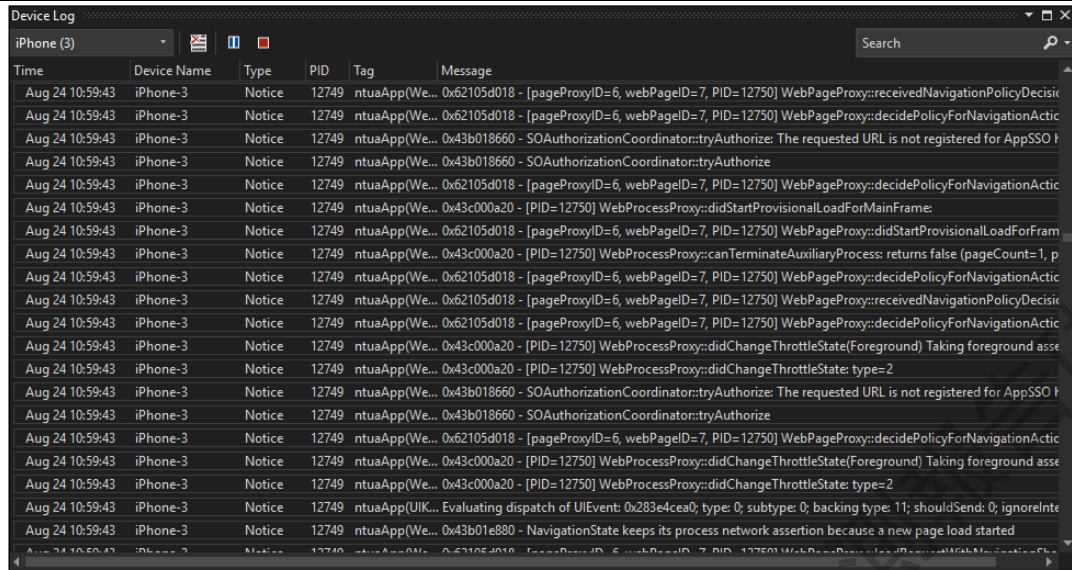


圖二

```
Processes: 431 total, 1 running, 430 sleeping, 1331 threads 10:58:18
Load Avg: 2.04, 1.80, 1.76 CPU usage: 14.83% user, 0.0% sys, 85.16% idle
SharedLibs: 459M resident, 113M data, 26M linkedit. MemRegions: 52544 total, 806M resident, 103M private, 405M shared.
PhysMem: 2781M used (493M wired), 39M unused.
VM: 180T vsize, 15G framework vsize, 232576(0) swapins, 250178(0) swapouts.
Networks: packets: 21718675/11G in, 19564690/9524M out. Disks: 13120977/725G read, 5800768/88G written.
```

PID	COMMAND	%CPU	TIME	#TH	#WQ	#PORT	RSHR	RSIZ	PRGP	PPID	STATE	BOOSTS	%CPU_ME	%CPU_OTHR
68*	backboardd	32.4	07:59:21	18	7	1777	N/A	N/A	68	1	sleeping	*0[1]	0.40775	0.42640
12749*	ntuaApp	16.8	00:04:47	6	2	270	N/A	N/A	12749	1	sleeping	*0[1]	0.63479	0.00000
12750*	com.apple.We	8.0	00:02:71	13	3	78	N/A	N/A	12750	1	sleeping	*0[1]	0.00000	0.00000
12748*	top	7.1	00:03:85	1/1	0	23	N/A	N/A	12748	12747	running	*0[1]	0.00000	0.00000
153*	Accessibilit	6.0	05:43:59	11	5	214	N/A	N/A	153	1	sleeping	*0[1]	0.00000	0.17498
37*	SpringBoard	2.1	69:52:58	12	4	1489	N/A	N/A	37	1	sleeping	*0[1]	0.05177	0.60334
73*	locationd	1.0	01:46:57	11	7	808	N/A	N/A	73	1	sleeping	*0[1]	0.38269	0.00000
12752*	com.apple.We	0.6	00:00:50	5	2	76	N/A	N/A	12752	1	sleeping	*0[1]	0.00000	0.00000
110*	com.apple.Dr	0.5	02:24:36	7	5	1276	N/A	N/A	110	1	sleeping	*0[1]	0.00000	0.00000
79*	dasd	0.4	46:07:65	4	3	287	N/A	N/A	79	1	sleeping	*0[28390]	0.00000	0.00000
99*	CommCenter	0.4	29:42:47	12	5	539	N/A	N/A	99	1	sleeping	*0[1]	1.16943	0.00000
50*	WirelessRadi	0.3	23:26:66	4	3	95	N/A	N/A	50	1	sleeping	*0[104595+]	0.00000	0.36389
52*	wifid	0.3	01:40:26	9	8	406	N/A	N/A	52	1	sleeping	*0[1]	0.00000	0.29211
168*	analyticsd	0.3	54:45:66	3	2	449	N/A	N/A	168	1	sleeping	*0[46247+]	0.00000	0.29063
71*	sharingd	0.2	05:26:67	4	2	307	N/A	N/A	71	1	sleeping	*0[1]	0.01361	0.14301
39*	assistantd	0.2	17:14:45	4	2	589	N/A	N/A	39	1	sleeping	*0[14931+]	0.00000	0.03456
771*	promotedcont	0.1	00:30:50	5	3	88+	N/A	N/A	771	1	sleeping	*0[4141+]	0.00000	0.05236
34*	logd	0.1	36:47:52	4	3	1351	N/A	N/A	34	1	sleeping	*0[1]	0.00000	0.00000
67*	contextstore	0.1	12:48:43	5	4	330	N/A	N/A	67	1	sleeping	*0[65802]	0.00000	0.04317
116*	callservices	0.1	06:51:56	2	1	397	N/A	N/A	116	1	sleeping	*0[8082]	0.00000	0.00000
4571*	symptomsd	0.0	12:07:37	5	3	390	N/A	N/A	4571	1	sleeping	*4743+[18399]	0.00000	0.07284
38*	mediaserverd	0.0	37:15:78	20	3	881	N/A	N/A	38	1	sleeping	*0[1]	0.00547	0.00000

圖三



Time	Device Name	Type	PID	Tag	Message
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::receivedNavigationPolicyDecisio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::decidePolicyForNavigationActio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43b018660 - SOAuthorizationCoordinator::tryAuthorize: The requested URL is not registered for AppSSO f
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43b018660 - SOAuthorizationCoordinator::tryAuthorize
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::decidePolicyForNavigationActio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::didStartProvisionalLoadForMainFrame:
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::didStartProvisionalLoadForFram
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::canTerminateAuxiliaryProcess: returns false (pageCount=1, p
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::decidePolicyForNavigationActio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::receivedNavigationPolicyDecisio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::decidePolicyForNavigationActio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::didChangeThrottleState(Foreground) Taking foreground asse
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::didChangeThrottleState: type=2
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43b018660 - SOAuthorizationCoordinator::tryAuthorize: The requested URL is not registered for AppSSO f
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43b018660 - SOAuthorizationCoordinator::tryAuthorize
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x62105d018 - [pageProxyID=6, webPageID=7, PID=12750] WebPageProxy::decidePolicyForNavigationActio
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::didChangeThrottleState(Foreground) Taking foreground asse
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43c000a20 - [PID=12750] WebProcessProxy::didChangeThrottleState: type=2
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(UIK...	Evaluating dispatch of UIEvent: 0x283e4cea0; type: 0; subtype: 0; backing type: 11; shouldSend: 0; ignoreInte
Aug 24 10:59:43	iPhone-3	Notice	12749	ntuaApp(We...	0x43b01e880 - NavigationState keeps its process network assertion because a new page load started

圖四

檢測結果圖示

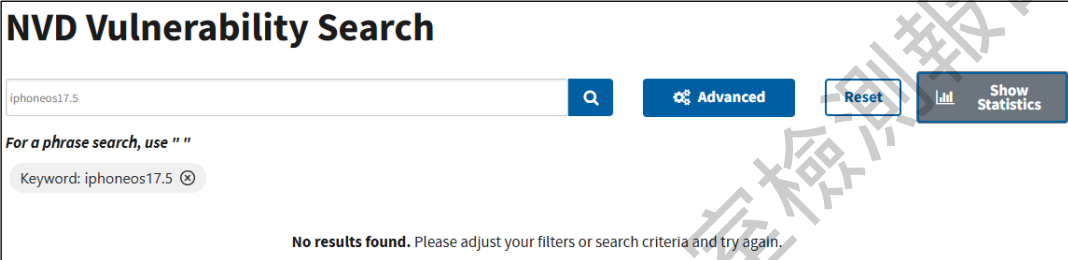
● 4.1.5.1.2 行動應用程式應避免資訊安全漏洞 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式是否不存在已知安全性漏洞。如為「是」則符合檢測基準；「否」則不符合檢測基準。

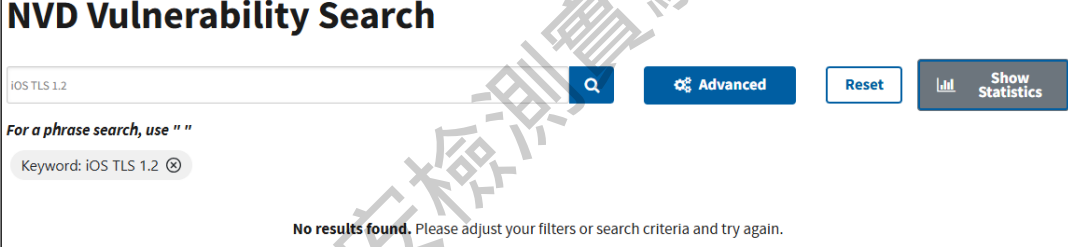
2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，透過 NVD 網站查詢，行動應用程式引用之第三方函式庫(請參照 4.1.5.3.1 測項)、平台 SDK 版本(圖一)及傳輸協定 TLS 1.2(圖二)，均不存在已知安全性漏洞，檢測結果符合基準。



The screenshot shows the NVD Vulnerability Search interface. The search term 'iphoneos17.5' is entered in the search bar. Below the search bar, it says 'For a phrase search, use ""'. The keyword 'iphoneos17.5' is displayed. The result is 'No results found. Please adjust your filters or search criteria and try again.' There are buttons for 'Advanced', 'Reset', and 'Show Statistics'.

圖一



The screenshot shows the NVD Vulnerability Search interface. The search term 'iOS TLS 1.2' is entered in the search bar. Below the search bar, it says 'For a phrase search, use ""'. The keyword 'iOS TLS 1.2' is displayed. The result is 'No results found. Please adjust your filters or search criteria and try again.' There are buttons for 'Advanced', 'Reset', and 'Show Statistics'.

圖二

檢測結果圖示

● 4.1.5.1.3 行動應用程式應針對螢幕覆蓋攻擊進行防護 (L1、L2、L3)

1. 檢測基準：

檢查行動應用程式是否針對螢幕覆蓋攻擊 (Screen Overlay Attack) 進行防護或主動警示使用者，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☐ 符合 ☐ 不符合 ☒ 不適用(iOS 作業系統)

經過實驗室檢測，行動應用程式為 iOS 作業系統，檢測結果不適用。

行動應用程式為 iOS 作業系統
檢測結果圖示

- 4.1.5.3.1 行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全 (L1、L2、L3)

1.檢測基準：

檢查行動應用程式引用之函式庫是否不存在已知安全性漏洞。如為「是」則符合檢測基準；「否」則不符合檢測基準。

2.檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，行動應用程式調查表所列與 MobSF 分析，Hopper Disassembler 工具查詢後未發現第三方函式庫，引用之函式庫未發現已存在之安全性漏洞，檢測結果符合基準

LIBRARIES

▼ Showing all 57 libraries

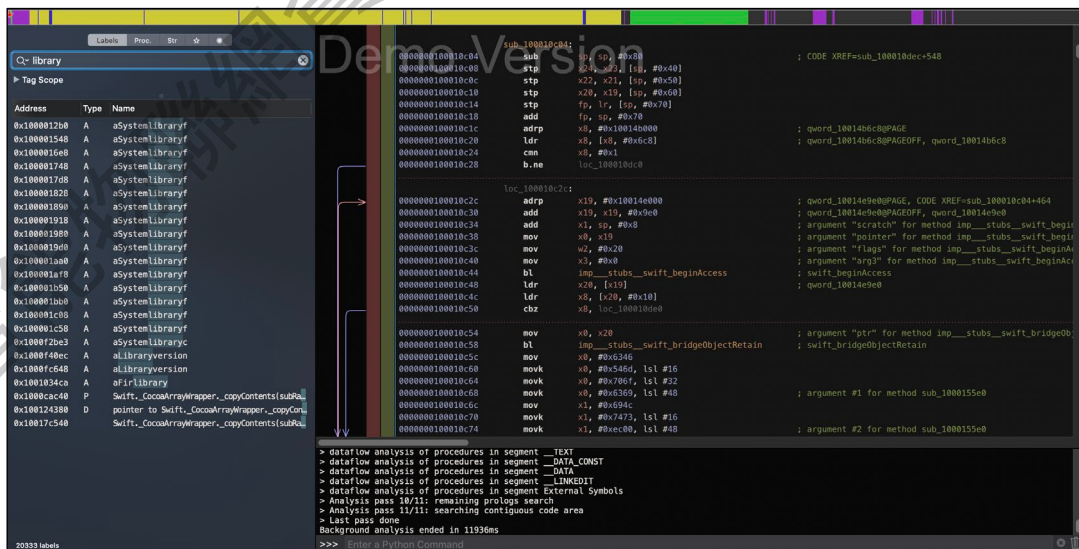
```

/usr/lib/libc++.1.dylib (compatibility version: 1.0.0, current version: 1700.255.0)
/usr/lib/libsqlite3.dylib (compatibility version: 9.0.0, current version: 351.4.0)
/usr/lib/swift/libswiftCoreGraphics.dylib (compatibility version: 1.0.0, current version: 15.0.0)
/usr/lib/libz.1.dylib (compatibility version: 1.0.0, current version: 1.2.12)
/System/Library/Frameworks/CoreTelephony.framework/CoreTelephony (compatibility version: 1.0.0, current version: 0.0.0)
@rpath/FBLPromises.framework/FBLPromises (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseAppCheckInterop.framework/FirebaseAppCheckInterop (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseAuth.framework/FirebaseAuth (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseCore.framework/FirebaseCore (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseCoreInternal.framework/FirebaseCoreInternal (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseInstallations.framework/FirebaseInstallations (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/FirebaseMessaging.framework/FirebaseMessaging (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/Foundation.framework/Foundation (compatibility version: 300.0.0, current version: 2503.1.0)
@rpath/GTMSessionFetcher.framework/GTMSessionFetcher (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/GoogleDataTransport.framework/GoogleDataTransport (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/GoogleUtilities.framework/GoogleUtilities (compatibility version: 1.0.0, current version: 1.0.0)
@rpath/RecaptchaInterop.framework/RecaptchaInterop (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/SafariServices.framework/SafariServices (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/Security.framework/Security (compatibility version: 1.0.0, current version: 61123.120.34)
@rpath/SnapKit.framework/SnapKit (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/StoreKit.framework/StoreKit (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration (compatibility version: 1.0.0, current version: 1300.120.2)
/System/Library/Frameworks/UIKit.framework/UIKit (compatibility version: 1.0.0, current version: 7511.1.104)
@rpath/nanopb.framework/nanopb (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/UserNotifications.framework/UserNotifications (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/WebKit.framework/WebKit (compatibility version: 1.0.0, current version: 618.2.12)
/System/Library/Frameworks/NetworkExtension.framework/NetworkExtension (compatibility version: 1.0.0, current version: 1.0.0)
/usr/lib/libobjc.A.dylib (compatibility version: 1.0.0, current version: 228.0.0)
/usr/lib/libSystem.B.dylib (compatibility version: 1.0.0, current version: 1345.120.2)
  
```

```
/System/Library/Frameworks/AVFoundation.framework/AVFoundation (compatibility version: 1.0.0, current version: 2.0.0)
/System/Library/Frameworks/AudioToolbox.framework/AudioToolbox (compatibility version: 1.0.0, current version: 1000.0.0)
/System/Library/Frameworks/CoreFoundation.framework/CoreFoundation (compatibility version: 150.0.0, current version: 2503.1.0)
/System/Library/Frameworks/CoreGraphics.framework/CoreGraphics (compatibility version: 64.0.0, current version: 1774.5.3)
/System/Library/Frameworks/CoreNFC.framework/CoreNFC (compatibility version: 1.0.0, current version: 1.0.0)
/System/Library/Frameworks/SwiftUI.framework/SwiftUI (compatibility version: 1.0.0, current version: 5.5.8)
/usr/lib/swift/libswiftAVFoundation.dylib (compatibility version: 1.0.0, current version: 2240.7.2)
/usr/lib/swift/libswiftCore.dylib (compatibility version: 1.0.0, current version: 0.0.0)
/usr/lib/swift/libswiftCoreAudio.dylib (compatibility version: 1.0.0, current version: 6.0.0)
/usr/lib/swift/libswiftCoreFoundation.dylib (compatibility version: 1.0.0, current version: 120.100.0)
/usr/lib/swift/libswiftCoreImage.dylib (compatibility version: 1.0.0, current version: 2.0.0)
/usr/lib/swift/libswiftCoreMIDI.dylib (compatibility version: 1.0.0, current version: 6.0.0)
/usr/lib/swift/libswiftCoreMedia.dylib (compatibility version: 1.0.0, current version: 3110.8.2)
/usr/lib/swift/libswiftDarwin.dylib (compatibility version: 1.0.0, current version: 0.0.0)
/usr/lib/swift/libswiftDataDetection.dylib (compatibility version: 1.0.0, current version: 758.7.0)
/usr/lib/swift/libswiftDispatch.dylib (compatibility version: 1.0.0, current version: 41.0.0)
/usr/lib/swift/libswiftFileProvider.dylib (compatibility version: 1.0.0, current version: 1835.120.53)
/usr/lib/swift/libswiftMetal.dylib (compatibility version: 1.0.0, current version: 343.19.0)
/usr/lib/swift/libswiftOSLog.dylib (compatibility version: 1.0.0, current version: 4.0.0)
/usr/lib/swift/libswiftObjectiveC.dylib (compatibility version: 1.0.0, current version: 8.0.0)
/usr/lib/swift/libswiftQuartzCore.dylib (compatibility version: 1.0.0, current version: 3.0.0)
/usr/lib/swift/libswiftUniformTypeIdentifiers.dylib (compatibility version: 1.0.0, current version: 794.2.3)
/usr/lib/swift/libswiftWebKit.dylib (compatibility version: 1.0.0, current version: 0.0.0)
/usr/lib/swift/libswiftXPC.dylib (compatibility version: 1.0.0, current version: 36.100.8)
/usr/lib/swift/libswiftos.dylib (compatibility version: 1.0.0, current version: 1049.100.4)
/usr/lib/swift/libswiftsimd.dylib (compatibility version: 1.0.0, current version: 18.0.0)
/usr/lib/swift/libswiftFoundation.dylib (compatibility version: 1.0.0, current version: 1.0.0)
/usr/lib/swift/libswiftUIKit.dylib (compatibility version: 1.0.0, current version: 1.0.0)
```

17 引用函式庫說明
(包含作業系統內建及第三方函式庫)

格式：函式庫名稱 / 版本 / 來源
範例：webkit / 534.30 / 作業系統內建
請說明：請依以上範例格式提供
WebView / 作業系統內建



檢測結果圖示

● 4.1.5.4.1 行動應用程式應針對使用者於輸入階段之字串，進行安全檢查 (L1、L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式是否針對預期使用者輸入之字串驗證型別，如欄位本身需要接受特殊字元，亦屬於可預期的輸入字串型別。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式是否針對使用者輸入字串驗證長度。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，登入欄位之帳號不接受輸入符號與特殊符號(圖一)、限制輸入50字元；密碼限制輸入255字元(圖二)，檢測結果符合基準。



圖一



圖二
檢測結果圖示

● 4.1.5.4.2 行動應用程式應提供相關注入攻擊防護機制 (L1、L2、L3)

1. 檢測基準：

- (1) 檢查行動應用程式是否防護使用者輸入SQL Injection字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (2) 檢查行動應用程式是否防護使用者輸入JavaScript Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (3) 檢查行動應用程式是否防護使用者輸入Command Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (4) 檢查行動應用程式是否防護使用者輸入Local File Inclusion 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (5) 檢查行動應用程式是否防護使用者輸入XML Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (6) 檢查行動應用程式是否防護使用者輸入Format String Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- (7) 檢查行動應用程式是否防護使用者輸入IPC (Inter-process communication) Injection字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2. 檢測結果： ☒ 符合 ☐ 不符合

經過實驗室檢測，

基準(1)於登入欄位輸入 SQL Injection 測試字串後，防護有效未發生錯誤(圖一)；

基準(2)輸入 JavaScript Injection 測試字串後，畫面未出現預期的彈出式對話框(圖二)；

基準(3)輸入 Command Injection 測試字串後，系統未產生預期的檔案創建行為(圖三)；

基準(4)輸入 Local File Inclusion 測試字串後，應用程式並未開啟相關檔案(圖四)；

基準(5)輸入 XML Injection 測試字串後，系統並未回傳錯誤或異常回應(圖五)；

基準(6)輸入 Format String Injection 測試字串後，系統並未出現緩衝區溢位或 crash 狀況(圖六)；

基準(7) 使用 MobSF 搜尋 Info.plist 檔案，搜尋"CFBundleURLSchemes"有發現(圖七)；檢視 Binary Analysis 並未發現 IPC 相關訊息(圖八)；

檢測結果符合基準。



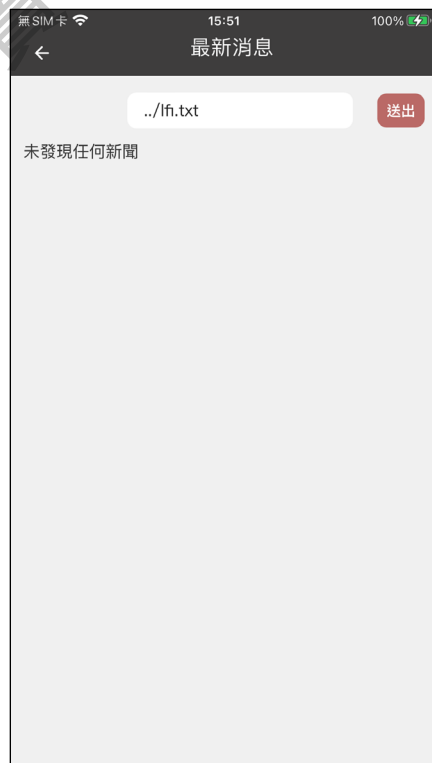
圖一



圖二



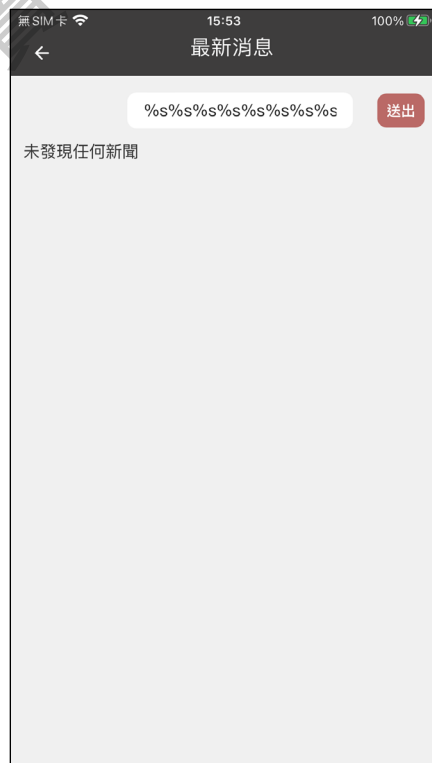
圖三



圖四



圖五



圖六

CFBundleURLSchemes

2/2

```

</dict>
<key>CFBundleIdentifier</key>
<string>tw.edu.ntua.app</string>
<key>CFBundleInfoDictionaryVersion</key>
<string>6.0</string>
<key>CFBundleName</key>
<string>ntuaApp</string>
<key>CFBundlePackageType</key>
<string>APPL</string>
<key>CFBundleShortVersionString</key>
<string>1.0.1</string>
<key>CFBundleSupportedPlatforms</key>
<array>
  <string>iPhoneOS</string>
</array>
<key>CFBundleURLTypes</key>
<array>
  <dict>
    <key>CFBundleTypeRole</key>
    <string>Editor</string>
    <key>CFBundleURLSchemes</key>
    <array>
      <string>com.googleusercontent.apps.706
    </array>
  </dict>
</array>

```

圖七

IPA BINARY ANALYSIS

Search:

PROTECTION	STATUS	SEVERITY	DESCRIPTION
ARC	True	Info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
CODE SIGNATURE	True	Info	This binary has a code signature.
ENCRYPTED	True	Info	This binary is encrypted.
NX	True	Info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
PIE	True	Info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
RPATH	True	Warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
STACK CANARY	True	Info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
SYMBOLS STRIPPED	True	Info	Debug Symbols are stripped

圖八

檢測結果圖示

本文件著作權屬行動檢測服務股份有限公司所有，未經本公司許可不准引用或翻印。

A0173-2608006-Yi0-臺藝大智慧行動-V1.0.1

● 4.2.2.1.2 行動應用程式於 Webview 呈現功能時，所連線之網域應為執行安全檢測 (L1、L2、L3)

1. 檢測基準：

- 檢查行動應用程式使用Webview呈現功能時，其網頁伺服器弱點掃描須驗證 Injection Flaws檢查是否全數通過。如為「是」則符合檢測基準；「否」則不符合檢測基準。
- 若所連線之網域為安全網域且與行動應用App開發者於資料調查表中宣稱實際所連線之網域一致，該網域不需進行網頁伺服器弱點掃描。

2. 檢測結果：☐符合 ☒不符合 ☐不適用(無使用 Webview 呈現功能)

經過實驗室檢測，申請機構應自行檢附之弱點掃描報告，迄今尚未提供，檢測結果不符合基準。

是否使用 Webview	☒ 是，網域/子網域名稱： http://www.ntua.edu.tw (如：https://www.moeaidb.gov.tw, https://www.moeaidb.gov.tw/sub/) 若使用Webview，App對應後台網域的網頁應用程式須進行弱點掃描，(對以上填寫的URL作弱點掃描即可)，請選擇弱點掃描報告的提供者： ☐ 實驗室(依網域/子網域範圍另外收費) 請提供可掃描時段：<u>請輸入可掃描時段</u> ☒ 本申請機構自行檢附 (須為申請日期前後3個月內之用印/簽名弱掃報告) ☐ 否
--------------	---

檢測結果圖示