機密

國立空中大學行動 APP
行動應用 APP 基本資安檢測報告

檢測報告編號	A0189-2607005-Ya0
送檢單位名稱	國立空中大學
報告郵寄地址	247404 新北市蘆洲區中正路 172 號 資訊科技處
作業系統版本	Android 手機 （ 5.0 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 5.2.2
檢測物件收件日期	2026 年 07 月 28 日
檢測期間	2026 年 08 月 18 日～2026 年 08 月 21 日
報告製作日期	2026 年 08 月 21 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

國立空中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 26 項符合基準要求，5 項不符合基準要求，0 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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	不符合要求
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）	符合要求
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）	符合要求

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）	符合要求
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）	符合要求
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）	符合要求
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）	符合要求
20	4.1.4.1.2. 行動應用程式應依使用者身分授權（L2、L3）	符合要求
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）	符合要求
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）	不符合要求
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）	符合要求
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）	不符合要求
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）	符合要求
26	4.1.5.1.2. 行動應用程式應避免資訊安全漏洞（L1、L2、L3）	符合要求
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）	不符合要求
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）	符合要求
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）	符合要求
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）	符合要求
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）	不符合要求

檢測人	報告簽署人
黃政偉	劉家祥

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），針對國立空中大學送檢測之行動應用 APP 程式進行安全檢測，並於 08 月 21 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	國立空中大學 APP
唯一識別名稱	tw.edu.nouapp
APP 版本	V 5.2.2
App 程式檔案 Hash 值	☒ SHA256： 5f29c45bd2564f58a9a2e8d582b5c68ae41fd722b9fbf8884d16e88ac0a3e7b0
封包流向國家(所有)	國內、美國

3.2.檢測工具:

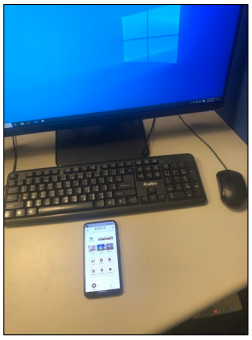
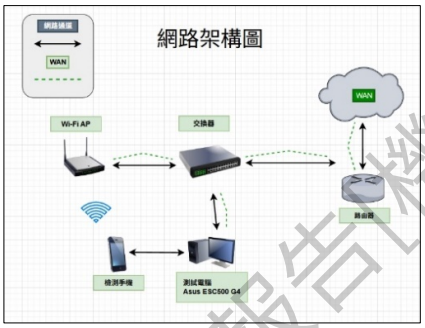
3.2.1. 檢測軟體工具

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
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
Root Checker	Android 權限偵測	6.5.0
MobSF	靜態分析	4.4.0
Android Debug Bridge	Android 多功能指令列	1.0
SSLUnpinning	Android 繞憑證綁定	2.0
jadx	APK 反編譯	1.3.2

3.2.2. 檢測硬體工具

工具名稱	型號
電腦	Asus ESC500 G4
手機	Google Pixel 4a

3.3.測試活動紀錄：

測試場域	待測物架設
	 

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：

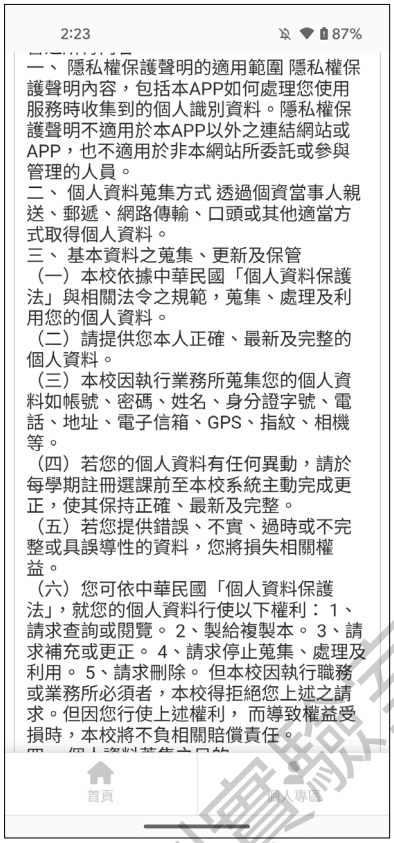
■ 若行動應用程式已發布，檢查行動應用程式是否於應用程式商店，依實際需要說明欲存取之敏感性資料、行動裝置資源及宣告權限用途。

■ 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(已於 Google Play 商店發布)，於可信任之應用程式商店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，檢測結果符合基準。



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）

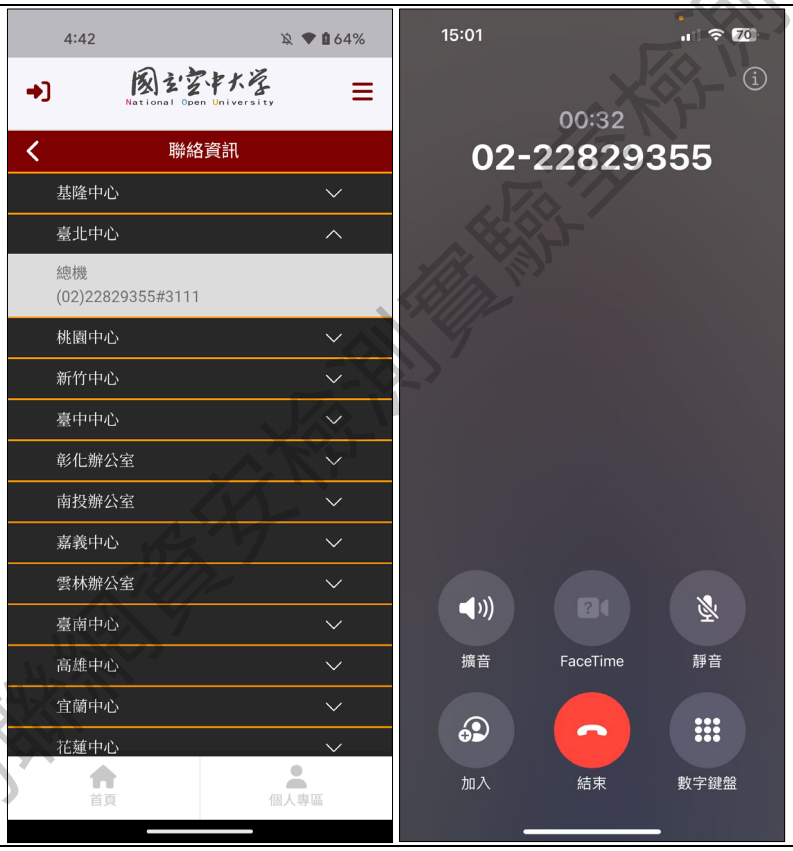
1.檢測基準：

- ■ 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(已於 Google Play 商店發布)，於行動應用程式內提供電話，並經測試可實際聯絡成功，檢測結果符合基準。



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）

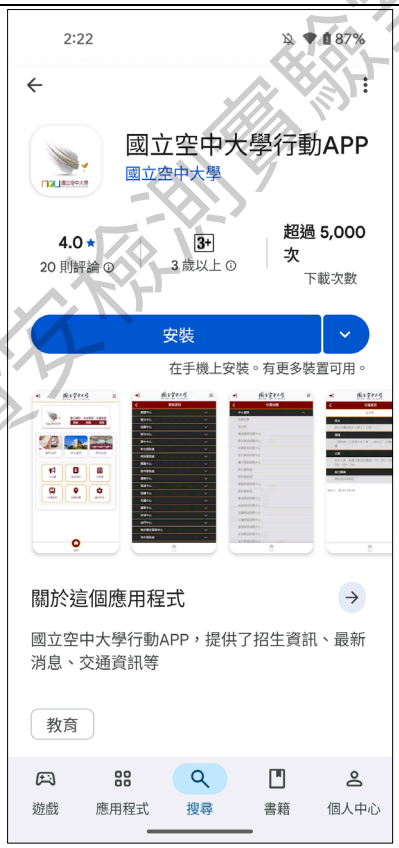
1.檢測基準：

- ■ 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。

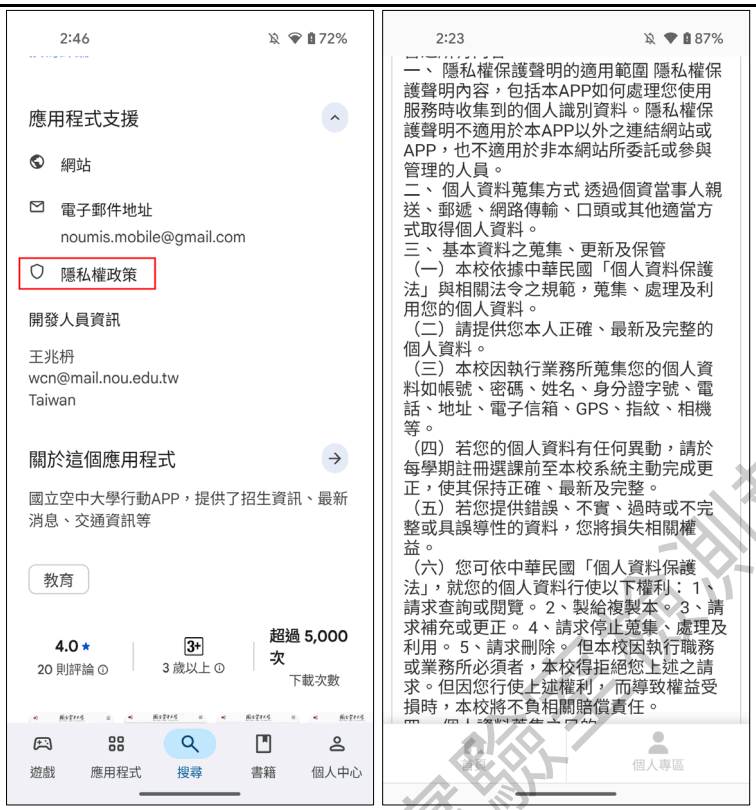
如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

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(圖一)，行動應用程式所有蒐集之敏感性資料於行動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）

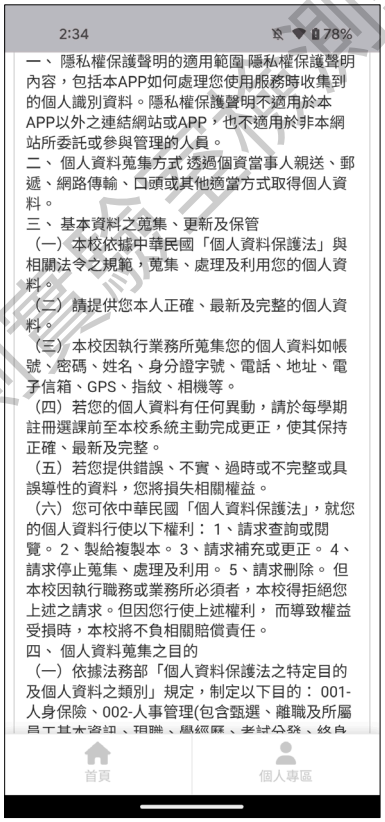
1.檢測基準：

（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，行動應用程式有提供使用者拒絕蒐集敏感性資料之選項，需要使用者自行勾選同意才能使用，使用 ADB 搜尋未檢出蒐集敏感性資料，檢測結果符合基準。




```
sunfish:/ # grep -r -i "no    6" /data/data/tw.edu.nouapp
1|sunfish:/ # grep -r -i "no        7" /data/data/tw.edu.nouapp
1|sunfish:/ #
```

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：

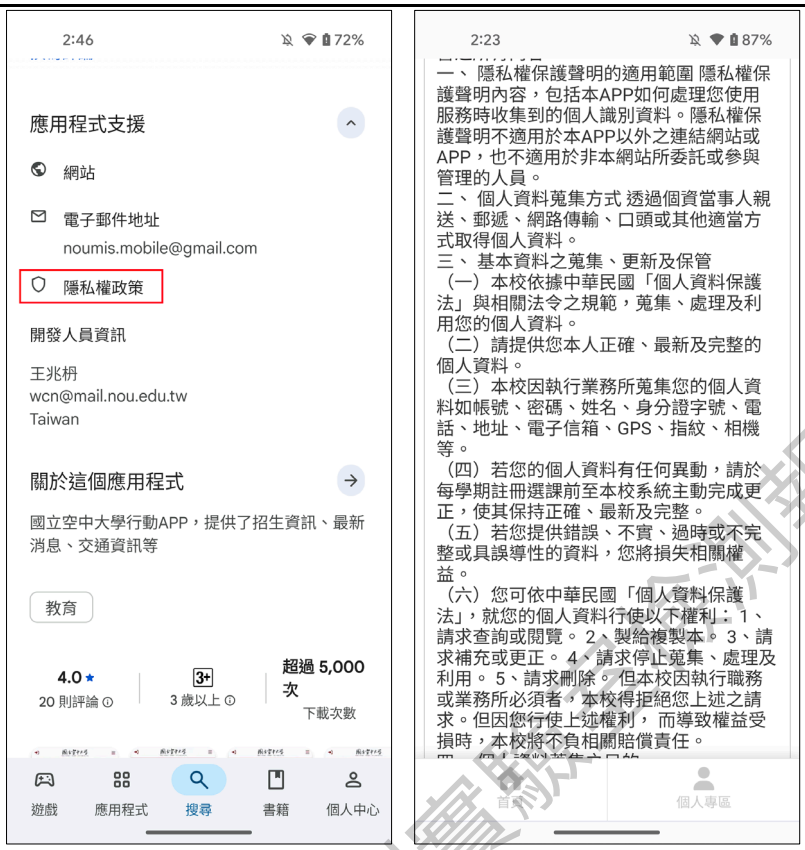
- ■ 若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。
- ■ 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。
- ■ 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。

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

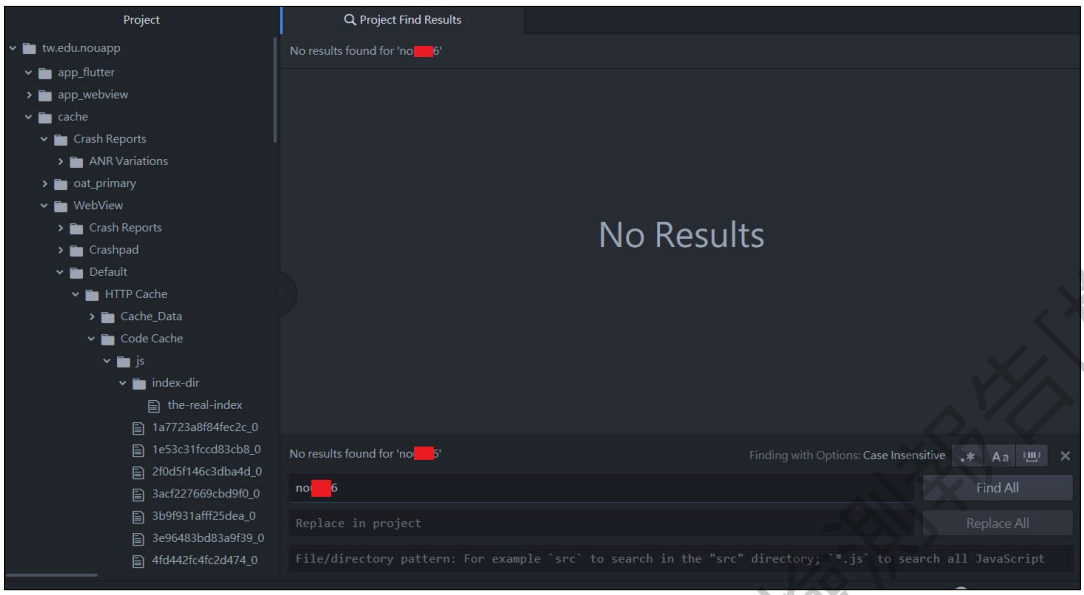
經過實驗室檢測，行動應用程式已發布(圖一)，行動應用程式所有儲存之敏感性資料於行動應用程式商店內聲明(圖二)，且於行動應用程式內聲明及取得使用者同意(圖三) ，使用 Atom、ADB 搜尋未檢出儲存敏感性資料(圖四)，檢測結果符合基準。

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：

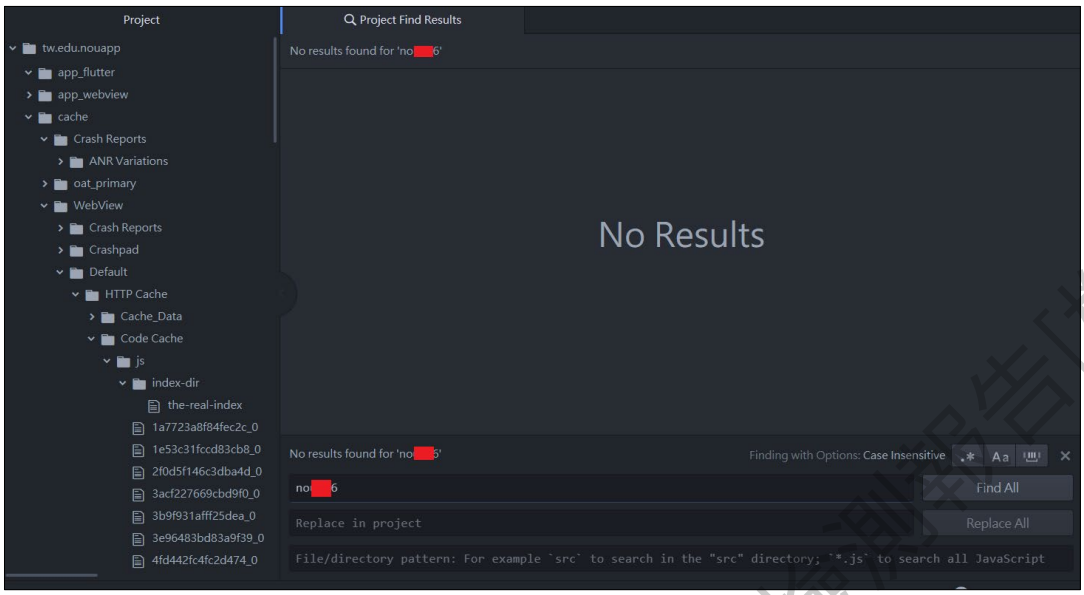
（1）檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

（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，行動應用程式有提供使用者拒絕儲存敏感性資料之選項(圖一)，在使用者拒絕敏感性資料儲存的情況下，使用 Atom、ADB 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）

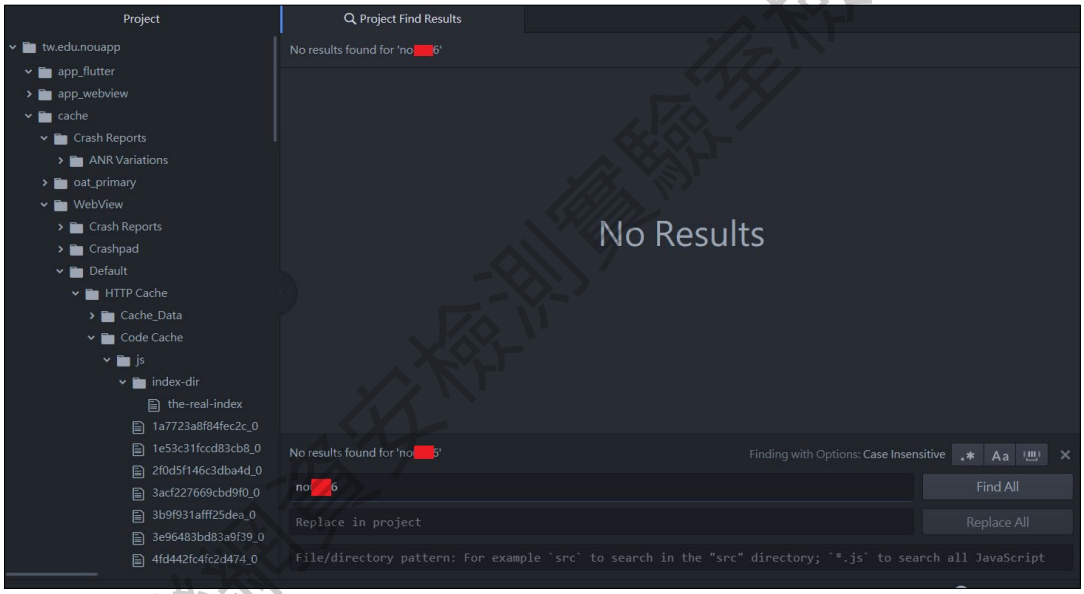
1.檢測基準：

（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，使用工具 Atom、ADB 連線搜尋行動應用程式；(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)；(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。




```
sunfish:/ # grep -r -i "no[redacted]6" /data/data/tw.edu.nouapp
1|sunfish:/ # grep -r -i "no[redacted]7" /data/data/tw.edu.nouapp
1|sunfish:/ #
```

圖一

圖二

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）

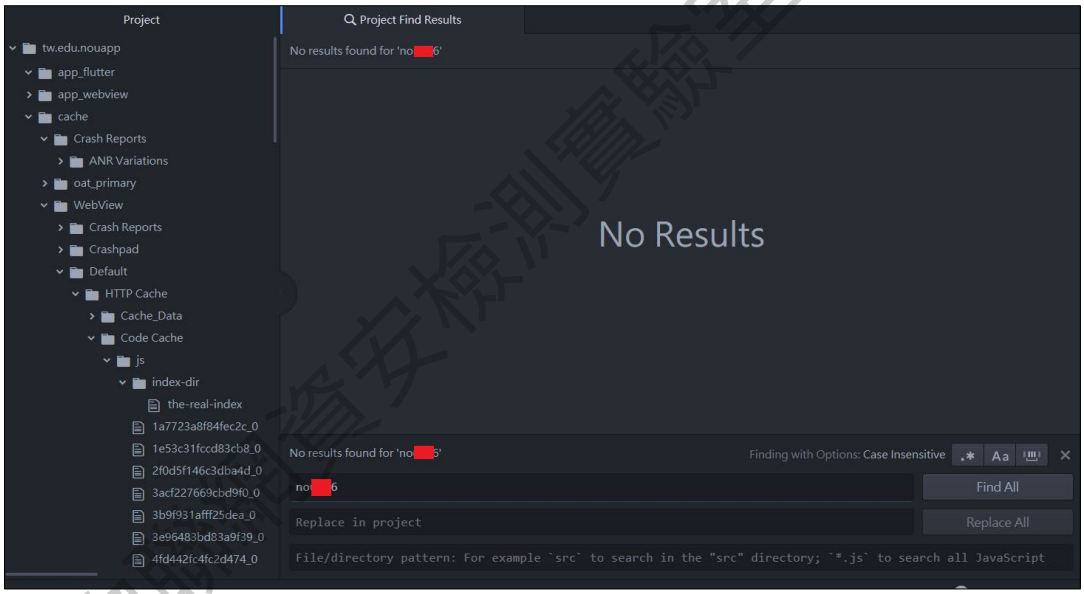
1.檢測基準：

（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 Atom、ADB 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。



檢測結果圖示

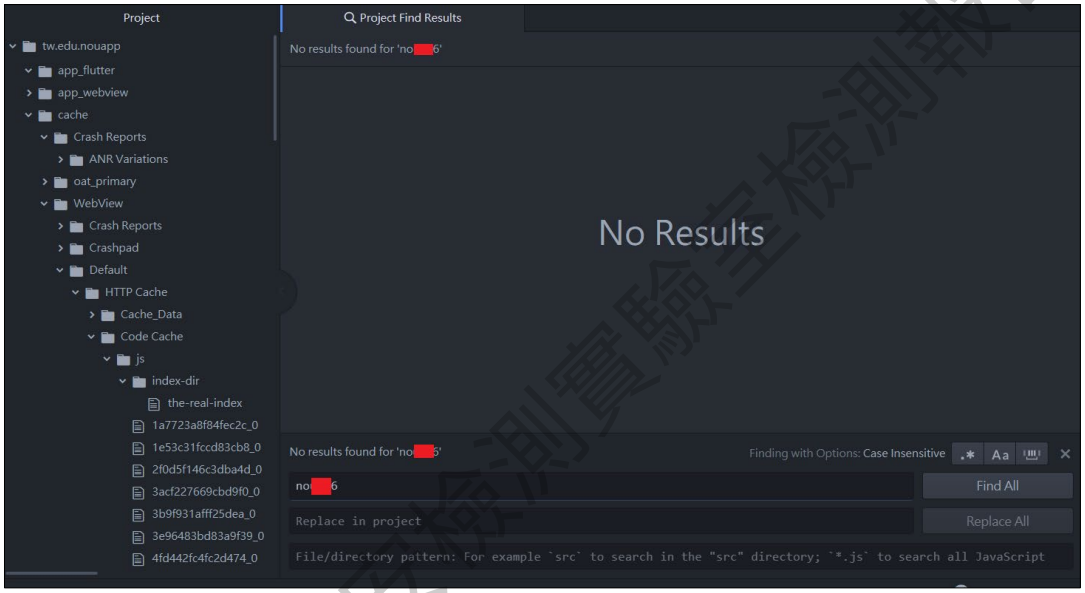
- 4.1.2.3.7 敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取（L1、L2、L3）

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 Atom、ADB 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。



檢測結果圖示

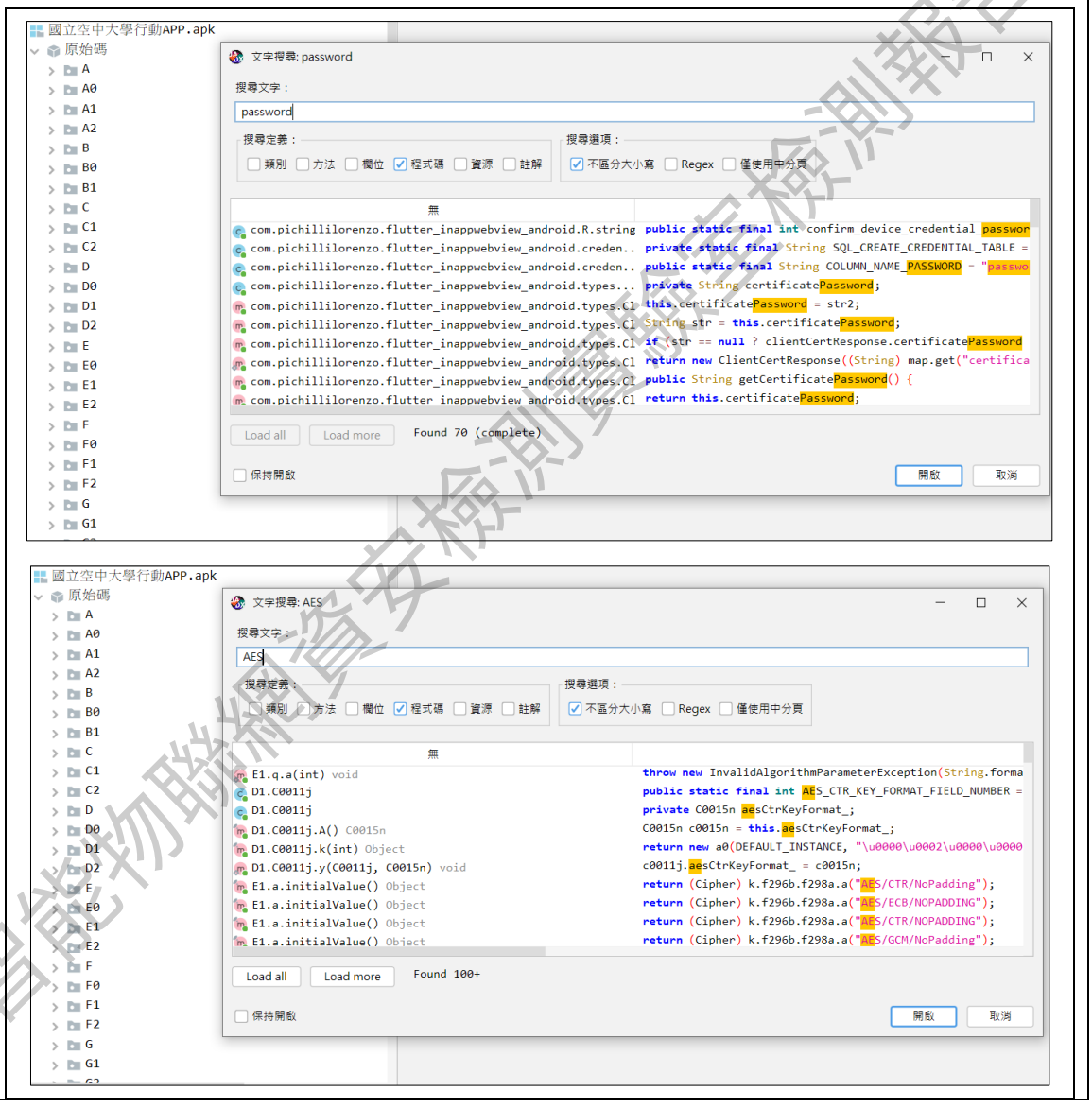
- 4.1.2.3.8 敏感性資料應避免出現於行動應用程式之程式碼（L1、L2、L3）

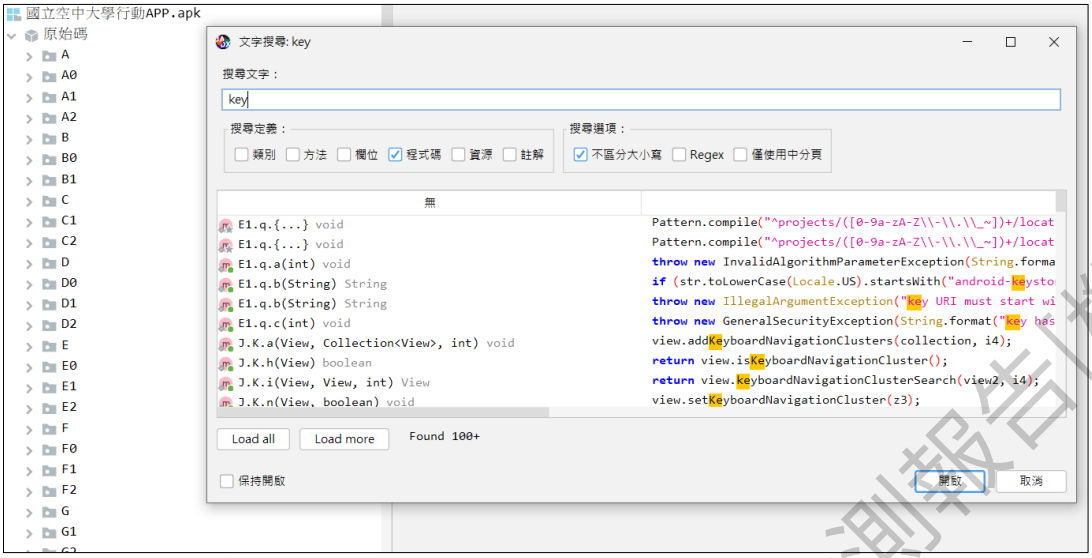
1.檢測基準：

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 jadx 反組譯工具將測試樣本打開，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 no****6 於登入成功後再登出(圖一)，在相同欄位輸入部份敏感性資料 no 未帶入可能字串(圖二)，使用 ADB 連線搜尋檔案未檢出儲存敏感性資料(圖三)，檢測結果符合基準。

圖一

圖二

圖三

檢測結果圖示

- 4.1.2.3.12 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，檢視行動應用程式 AndroidManifest.xml 檔案，搜尋<provider> tag，發現 android:exported 設定為 false(圖一)，IPC 機制未洩漏敏感性資料；使用 ADB 連線搜尋行動應用程式也未檢出蒐集敏感性資料(圖二)，檢測結果符合基準。

```
<provider android:name="com.crazecoder.openfile.FileProvider" android:exported="false"
    <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xm
</provider>
<activity android:theme="@android:style/Theme.NoTitleBar.Fullscreen" android:name="io.f
<service android:name="io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingBa
<service android:name="io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingSe
    <intent-filter>
        <action android:name="com.google.firebase.MESSAGING_EVENT" />
    </intent-filter>
</service>
```

```
<provider android:name="io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingInitProvider" android:exported="false"
<uses-library android:name="androidx.window.extensions" android:required="false" />
<uses-library android:name="androidx.window.sidecar" android:required="false" />
<provider android:name="androidx.startup.InitializationProvider" android:exported="false" android:authorities="tw.edu.nouapp
    <meta-data android:name="androidx.emoji2.text.EmojiCompatInitializer" android:value="androidx.startup" />
    <meta-data android:name="androidx.lifecycle.ProcessLifecycleInitializer" android:value="androidx.startup" />
    <meta-data android:name="androidx.profileinstaller.ProfileInstallerInitializer" android:value="androidx.startup" />
</provider>
```

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider" android:exported="false"
<activity android:theme="@android:style/Theme.Translucent.NoTitleBar" android:name="com.google.andro
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_service
<receiver android:name="androidx.profileinstaller.ProfileInstallReceiver" android:permission="androi
```

圖一

```
sunfish:/ # grep -r -i "no[redacted]6" /data/data/tw.edu.nouapp
1|sunfish:/ # grep -r -i "no[redacted]7" /data/data/tw.edu.nouapp
1|sunfish:/ #
```

圖二

檢測結果圖示

- 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）

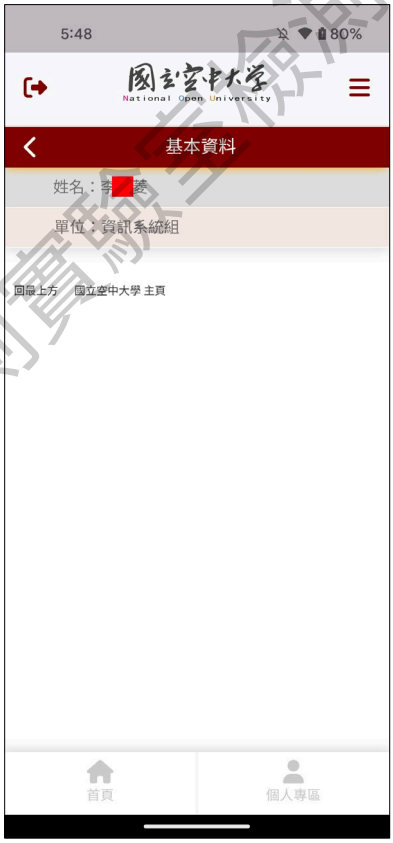
1.檢測基準：

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敏感性資料(帳號, 密碼. 圖一)有遮蔽設計，部分未遮蔽的敏感性資料(姓名. 圖二)未敘明原因(圖三)，檢測結果不符合基準。

圖一



圖二

27.	備註	請輸入備註

圖三

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，檢測結果符合基準。

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：

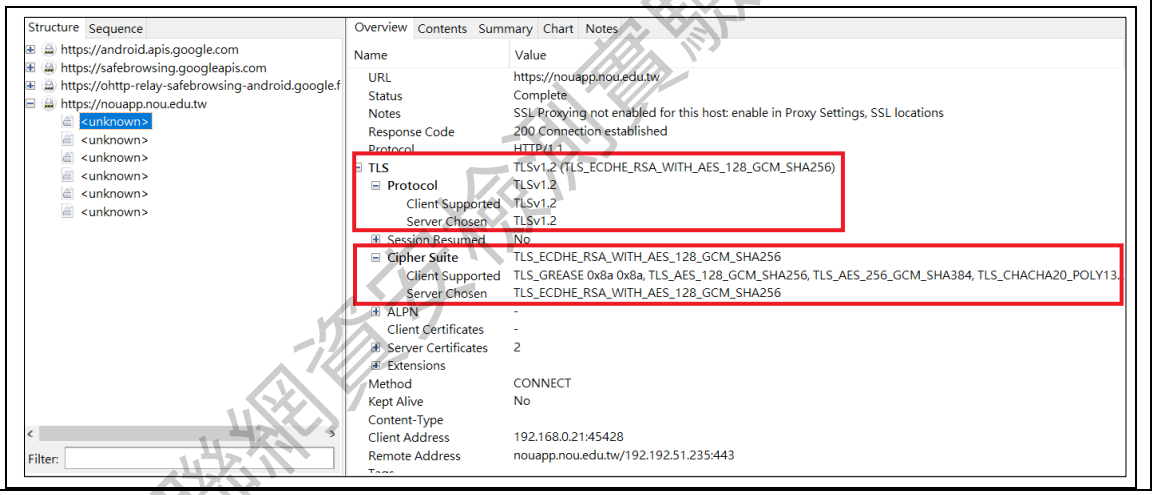
（1）檢查行動應用程式是否僅採用TLS 1.2（含）以上版本加密協定傳輸資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

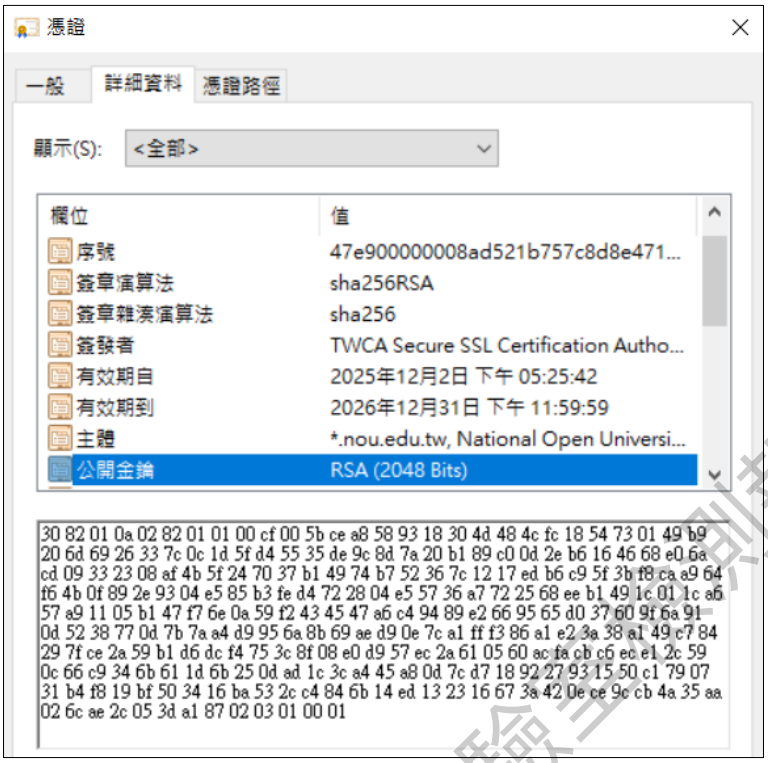
（2）檢查行動應用程式是否僅採用金鑰有效長度為2048位元（含）以上之RSA加密演算法，或採用金鑰有效長度為224位元（含）以上之橢圓曲線加密演算法（Elliptic Curve Cryptography）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

（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TLS1.2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 Charles 攔截封包行動應用程式採用 TLS 1.2 版本以上加密協定傳輸敏感性資料；採用金鑰有效長度 2048 位元之 RSA 加密演算法；採用金鑰有效長度 128 位元以上之進階加密標準(AES)，檢測結果符合基準。





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，行動應用程式未分享敏感性資料，檢測結果符合基準。

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，行動應用程式未分享敏感性資料，檢測結果符合基準。

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，行動應用程式未分享敏感性資料，檢測結果符合基準。

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，行動應用程式有身分鑑別機制，確認使用者身分，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，行動應用程式存取與個人資料相關之敏感性資料，有提供身分授權。才能看到自己的相關個人資料，檢測結果符合基準。

檢測結果圖示

- 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：

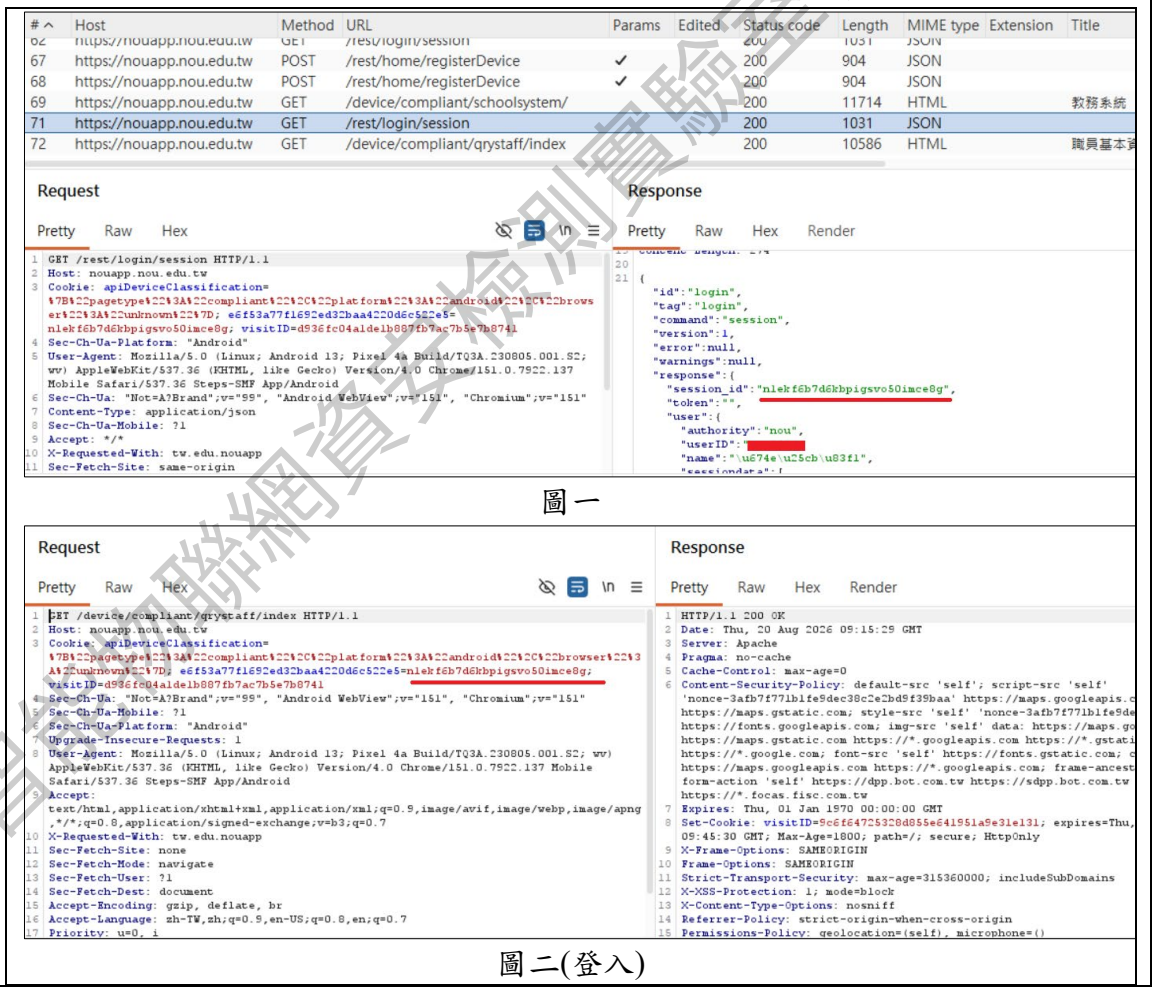
（1）檢查行動應用程式是否採用長度為128位元（含）以上之交談識別碼。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

（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。

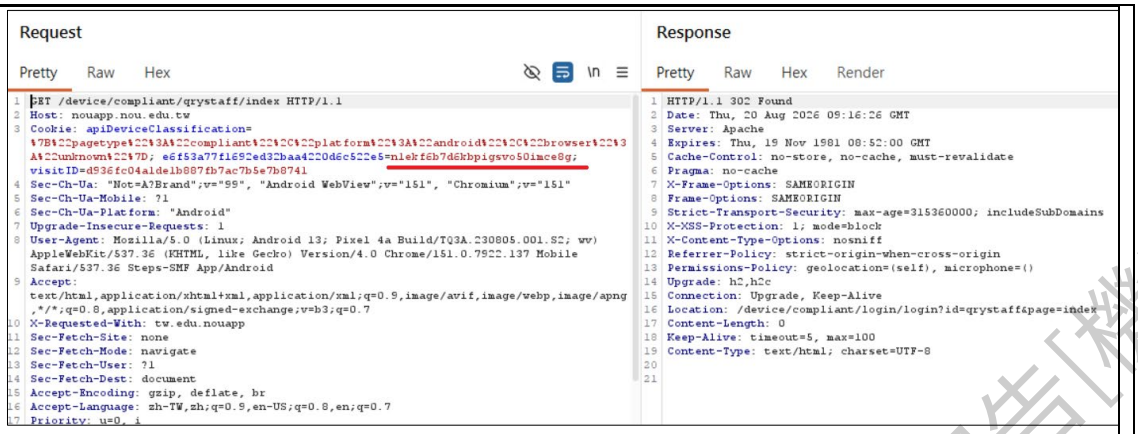
2.檢測結果： ■符合 □不符合

經過實驗室檢測，行動應用程式交談識別碼長度為 128 位元（含）以上且未與時間、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(圖一)，且具備登出失效機制，登出後交談識別碼無法使用(圖二為登入時，圖三為登出後封包重新傳送結果失敗)，檢測結果符合基準。



圖一

圖二(登入)



圖三(登出)

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）

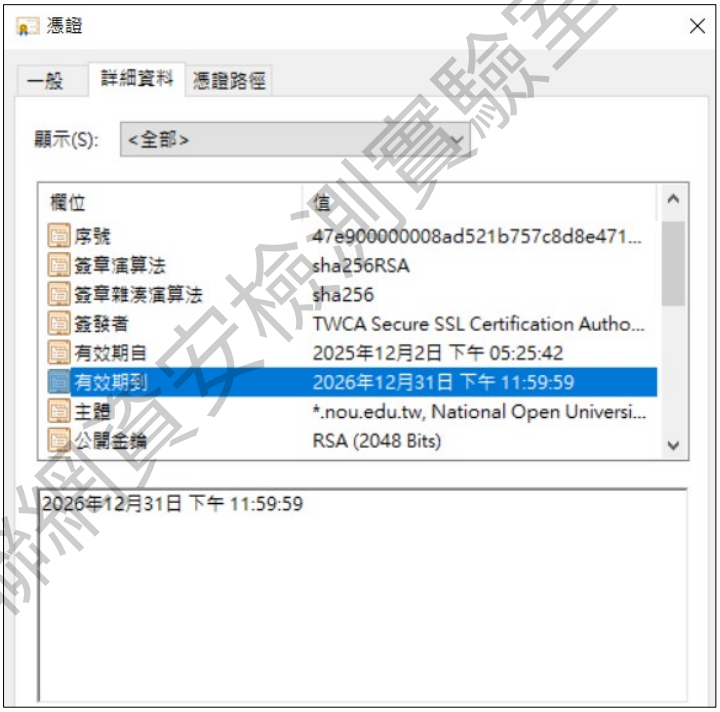
1.檢測基準：

（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。

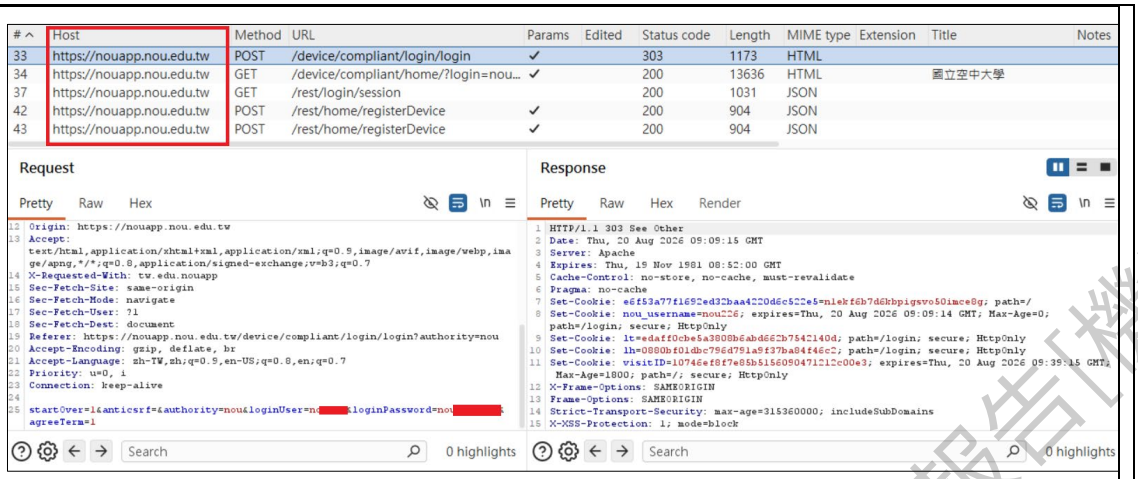
（2）檢查行動應用程式是否使用憑證綁定（Certificate Pinning）方式驗證，以確保連線之伺服器為行動應用App開發者所指定。若無法預期使用者所連線之網站，則應提示連線目標有變更並有提醒使用者即將連線至其他網站之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

2.檢測結果： □符合 ■不符合

經過實驗室檢測，(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)。(2).行動應用程式未使用憑證綁定方式驗證，使用 Burp 進行伺服器之中間人代理可以攔截封包(圖二)，因基準要求(2)不符合，檢測結果不符合基準。



圖一



圖二

檢測結果圖示

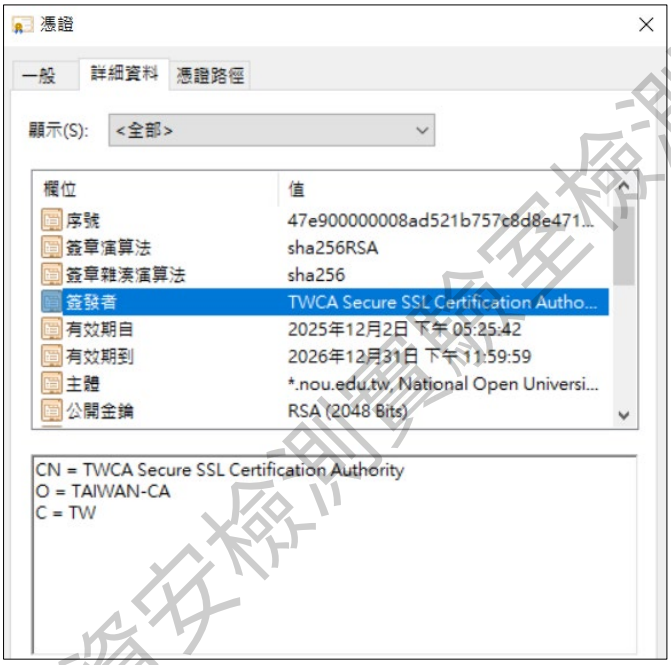
- 4.1.4.2.3 行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發（L1、L2、L3）

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，行動應用程式有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、政府機關、企業簽發，檢測結果符合基準。



檢測結果圖示

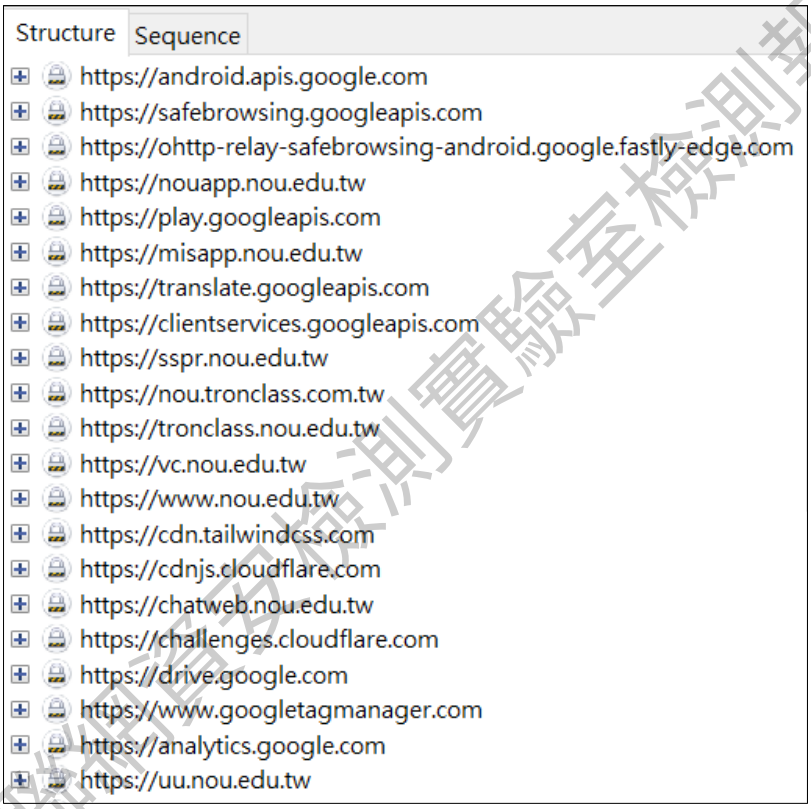
- 4.1.4.2.4 行動應用程式封包流向應與所宣告的內容一致（L1、L2、L3）

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。



android.apis.google.com/64.233.189.138:443	美國
safebrowsing.googleapis.com/142.250.157.95:443	美國
ohttp-relay-safebrowsing-android.google.fastly-edge.com/151.101.65.91:443	美國
nouapp.nou.edu.tw/192.192.51.235:443	台灣
play.googleapis.com/172.217.114.4:443	美國
misapp.nou.edu.tw/192.192.51.231:443	台灣
translate.googleapis.com/142.251.8.95:443	美國
clientservices.googleapis.com/142.250.204.46:443	美國
sspr.nou.edu.tw/192.192.51.10:443	台灣
nou.tronclass.com.tw/34.80.209.33:443	台灣
tronclass.nou.edu.tw/192.192.52.95:443	台灣
vc.nou.edu.tw/211.76.247.80:443	台灣
www.nou.edu.tw/211.76.247.73:443	台灣
cdn.tailwindcss.com/172.67.68.11:443	美國
cdnjs.cloudflare.com/104.17.24.14:443	美國
chatweb.nou.edu.tw/192.192.51.145:443	台灣
challenges.cloudflare.com/104.18.95.41:443	美國
drive.google.com/74.125.204.113:443	美國
www.googletagmanager.com/142.250.66.72:443	美國
analytics.google.com/216.239.36.181:443	美國

uu.nou.edu.tw/211.76.247.67:443	台灣
content-autofill.googleapis.com/172.217.113.4:443	美國
mail.nou.edu.tw/192.192.52.101:443	台灣
personnel.nou.edu.tw/192.192.51.10:443	台灣
ag.nou.edu.tw/211.76.247.74:443	台灣
ids.nou.edu.tw/192.192.51.10:443	台灣
www.facebook.com/31.13.87.36:443	台灣
www.fbsbx.com/31.13.87.1:443	台灣
kaios-d.facebook.com/31.13.87.12:443	台灣
scontent-tpe1-1.xx.fbcdn.net/31.13.87.5:443	台灣
googleads.g.doubleclick.net/142.250.196.194:443	美國
scontent.ftpe7-3.fna.fbcdn.net/203.74.65.145:443	台灣
external.ftpe7-3.fna.fbcdn.net/203.74.65.145:443	台灣
help-n.nou.edu.tw/192.192.51.198:443	台灣
growth-pa.googleapis.com/172.217.118.4:443	美國
pay-users-pa.googleapis.com/64.233.188.92:443	美國
androidpay-users-pa.googleapis.com/74.125.204.92:443	美國
notifications-pa.googleapis.com/172.217.112.4:443	美國
app-measurement.com/142.250.77.206:443	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。

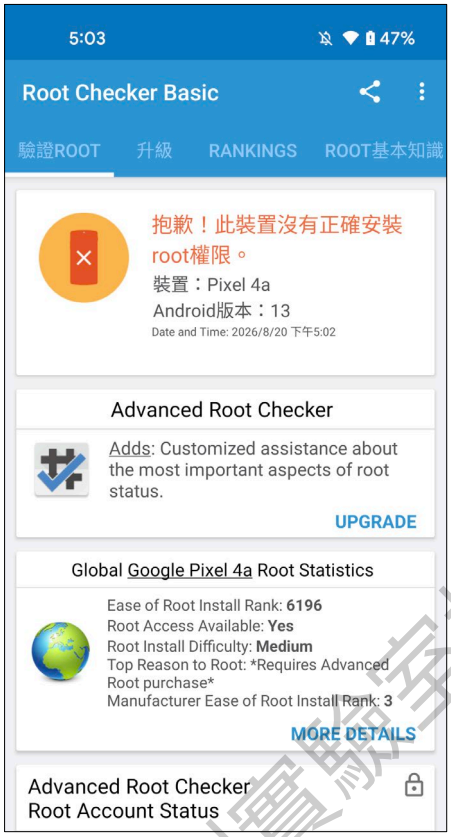
（2）檢查行動應用程式是否未包括可導致行動作業系統，發生未預期錯誤、資源明顯耗損、重新啟動或關閉等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準。

2.檢測結果： ■符合 □不符合

經過實驗室檢測，(1)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(圖一.使用 ADB 搜尋行動應用程式未存取位於其他行動應用程式的檔案)，防止連向未經授權的遠端服務)、提權(圖二.Root Check 驗證安裝後未發現 root/JB 行為)等行為，(2)行動應用程式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，(圖三.使用 ADB top 指令 CPU 無明顯耗損、圖四.圖五.使用 ADB fuzzing 測試未發生未預期錯誤、重新啟動或關閉)，檢測結果符合基準。

```
l!sunfish:/ # ps -A | grep tw.edu.nouapp
u0_a16       31878  1261 45540172 257072 SyS_epoll_wait     0 S tw.edu.nouapp
sunfish:/ # lsof | grep -i -E '31878.*/data/data'
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41   5186052     173659 /data/data/com.google.android.gms/
files/fonts/opentype/Noto_COLR_Emoji_Compat-400-100_0-0_0.ttf
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41   5186052     173659 /data/data/com.google.android.gms/
files/fonts/opentype/Noto_COLR_Emoji_Compat-400-100_0-0_0.ttf
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41     49152      44500 /data/data/tw.edu.nouapp/app_webvi
ew/Default/Shared Dictionary/db
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41     36864     177672 /data/data/tw.edu.nouapp/app_webvi
ew/Default/declarative_performance_observer.db
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41     24576     140547 /data/data/tw.edu.nouapp/app_webvi
ew/Default/Cookies
tw.edu.nouapp 31878     u0_a16  mem       REG             253,41     24576     140547 /data/data/tw.edu.nouapp/app_webvi
ew/Default/Cookies
tw.edu.nouapp 31878     u0_a16   91r      DIR             253,41      3488      53449 /data/data/tw.edu.nouapp/code_cach
e
tw.edu.nouapp 31878     u0_a16  101r      DIR             253,41      3488      53631 /data/data/tw.edu.nouapp/code_cach
e/flutter_engine/dd93de6fb1776398bf586cbd477deade1391c7e4/skia/1f39b47bf067193e98f92a75f7ae824129c18d03
tw.edu.nouapp 31878     u0_a16  103r      DIR             253,41      3488     176159 /data/data/tw.edu.nouapp/code_cach
e/flutter_engine/dd93de6fb1776398bf586cbd477deade1391c7e4/skia/1f39b47bf067193e98f92a75f7ae824129c18d03/sksl
tw.edu.nouapp 31878     u0_a16  138r      DIR             253,41      3488      53449 /data/data/tw.edu.nouapp/code_cach
e
tw.edu.nouapp 31878     u0_a16  147r      REG             253,41       142      55106 /data/data/tw.edu.nouapp/app_webvi
ew/Default/shared_proto_db/metadata/000055.ldb
tw.edu.nouapp 31878     u0_a16  149u      REG             253,41     24576     140547 /data/data/tw.edu.nouapp/app_webvi
ew/Default/Cookies
tw.edu.nouapp 31878     u0_a16  164u      REG             253,41        19      36034 /data/data/tw.edu.nouapp/app_webvi
ew/webview_data.lock
tw.edu.nouapp 31878     u0_a16  191w      REG             253,41        19     180389 /data/data/tw.edu.nouapp/app_webvi
```

圖一



圖二

```
sunfish:/ # top | grep tw.edu.nouapp
31878 u0_a16       10 -10  43G 251M 173M S  3.4   4.4   0:07.83 tw.edu.nouapp
  610 root         20   0  10G 2.9M 2.3M S  0.0   0.0   0:00.00 grep tw.edu.nouapp
31878 u0_a16       10 -10  43G 251M 173M S 10.3   4.4   0:07.84 tw.edu.nouapp
31878 u0_a16       10 -10  43G 253M 174M S  4.3   4.5   0:08.15 tw.edu.nouapp
 [H [JTasks: 833 total,   1 running, 832 sleeping,   0 stopped,   0 zombieu.nouapp
31878 u0_a16       10 -10  43G 253M 174M S 11.3   4.5   0:08.28 tw.edu.nouapp
31878 u0_a16       10 -10  43G 252M 174M S  0.3   4.5   0:08.62 tw.edu.nouapp
 [H [JTasks: 833 total,   1 running, 832 sleeping,   0 stopped,   0 zombieu.nouapp
31878 u0_a16       10 -10  43G 251M 173M S  1.0   4.4   0:08.63 tw.edu.nouapp
  610 root         20   0  10G 2.9M 2.2M S  0.0   0.0   0:00.00 grep tw.edu.nouapp
  610 root         20   0  10G 2.9M 2.2M S  0.0   0.0   0:00.00 grep tw.edu.nouapp
  610 root         20   0  10G 2.9M 2.2M S  0.0   0.0   0:00.00 grep tw.edu.nouapp
31878 u0_a16       10 -10  43G 247M 169M S  2.3   4.4   0:08.66 tw.edu.nouapp
31878 u0_a16       10 -10  43G 247M 169M S 17.3   4.4   0:08.73 tw.edu.nouapp
31878 u0_a16       10 -10  43G 246M 169M S 17.0   4.3   0:09.25 tw.edu.nouapp
31878 u0_a16       10 -10  43G 247M 169M S 20.6   4.4   0:09.76 tw.edu.nouapp
31878 u0_a16       10 -10  43G 258M 179M S  7.0   4.6   0:10.38 tw.edu.nouapp
31878 u0_a16       10 -10  43G 253M 174M S 12.3   4.5   0:10.59 tw.edu.nouapp
31878 u0_a16       10 -10  43G 255M 175M S 16.6   4.5   0:10.96 tw.edu.nouapp
31878 u0_a16       10 -10  43G 259M 180M S 15.6   4.6   0:11.46 tw.edu.nouapp
31878 u0_a16       10 -10  43G 260M 180M S 14.0   4.6   0:11.93 tw.edu.nouapp
 [mm31878 u0_a16       10 -10  43G 258M 180M R  8.6   4.6   0:12.35 tw.edu.nouapp
31878 u0_a16       10 -10  43G 250M 171M S 12.0   4.4   0:12.61 tw.edu.nouapp
31878 u0_a16       10 -10  43G 248M 170M S 18.0   4.4   0:12.97 tw.edu.nouapp
31878 u0_a16       10 -10  43G 254M 175M S 12.0   4.5   0:13.51 tw.edu.nouapp
31878 u0_a16       10 -10  43G 273M 187M S 27.6   4.8   0:13.87 tw.edu.nouapp
31878 u0_a16       10 -10  43G 278M 193M S 17.6   4.9   0:14.70 tw.edu.nouapp
31878 u0_a16       10 -10  43G 277M 193M S 29.6   4.9   0:15.23 tw.edu.nouapp
```

圖三

```
sunfish:/ # monkey -p tw.edu.nouapp -v 500
  bash arg: -p
  bash arg: tw.edu.nouapp
  bash arg: -v
  bash arg: 500
args: [-p, tw.edu.nouapp, -v, 500]
 arg: "-p"
 arg: "tw.edu.nouapp"
 arg: "-v"
 arg: "500"
data="tw.edu.nouapp"
:Monkey: seed=1787444139401 count=500
:AllowPackage: tw.edu.nouapp
:IncludeCategory: android.intent.category.LAUNCHER
:IncludeCategory: android.intent.category.MONKEY
// Event percentages:
//   0: 15.0%
//   1: 10.0%
//   2: 2.0%
//   3: 15.0%
//   4: -0.0%
//   5: -0.0%
//   6: 25.0%
//   7: 15.0%
//   8: 2.0%
//   9: 2.0%
//   10: 1.0%
//   11: 13.0%
:Switch: #Intent;action=android.intent.action.MAIN;category=android.intent.category.LAUNCHER;launchFlags=0
onent=tw.edu.nouapp/.MainActivity;end
```

圖四

```
:Sending Touch (ACTION_DOWN): 0:(324.0,1443.0)
:Sending Touch (ACTION_UP): 0:(202.39392,1489.0844)
:Sending Touch (ACTION_DOWN): 0:(727.0,2036.0)
:Sending Touch (ACTION_UP): 0:(720.7854,2039.8707)
:Sending Trackball (ACTION_MOVE): 0:(-1.0,2.0)
:Sending Trackball (ACTION_MOVE): 0:(-2.0,-5.0)
    //[calendar_time:2026-08-20 17:52:50.515  system_uptime:1483199713]
    // Sending event #400
:Sending Touch (ACTION_DOWN): 0:(465.0,1456.0)
:Sending Touch (ACTION_UP): 0:(465.83044,1451.56)
:Sending Touch (ACTION_DOWN): 0:(187.0,1361.0)
:Sending Touch (ACTION_UP): 0:(289.42566,1349.9642)
:Sending Trackball (ACTION_MOVE): 0:(1.0,-5.0)
:Sending Trackball (ACTION_UP): 0:(0.0,0.0)
:Sending Touch (ACTION_DOWN): 0:(988.0,708.0)
:Sending Touch (ACTION_UP): 0:(1080.0,619.5695)
:Sending Trackball (ACTION_MOVE): 0:(-3.0,4.0)
:Sending Trackball (ACTION_UP): 0:(0.0,0.0)
:Sending Trackball (ACTION_MOVE): 0:(-2.0,-3.0)
:Sending Trackball (ACTION_MOVE): 0:(3.0,-3.0)
:Sending Touch (ACTION_DOWN): 0:(321.0,562.0)
:Sending Touch (ACTION_UP): 0:(337.52805,577.8023)
:Sending Touch (ACTION_DOWN): 0:(337.0,1408.0)
:Sending Touch (ACTION_UP): 0:(374.37698,1423.4415)
:Sending Trackball (ACTION_MOVE): 0:(3.0,4.0)
Events injected: 500
:Sending rotation degree=0, persist=false
:Dropped: keys=0 pointers=0 trackballs=0 flips=0 rotations=0
## Network stats: elapsed time=1410ms (0ms mobile, 0ms wifi, 1410ms not connected)
// Monkey finished
```

圖五

檢測結果圖示

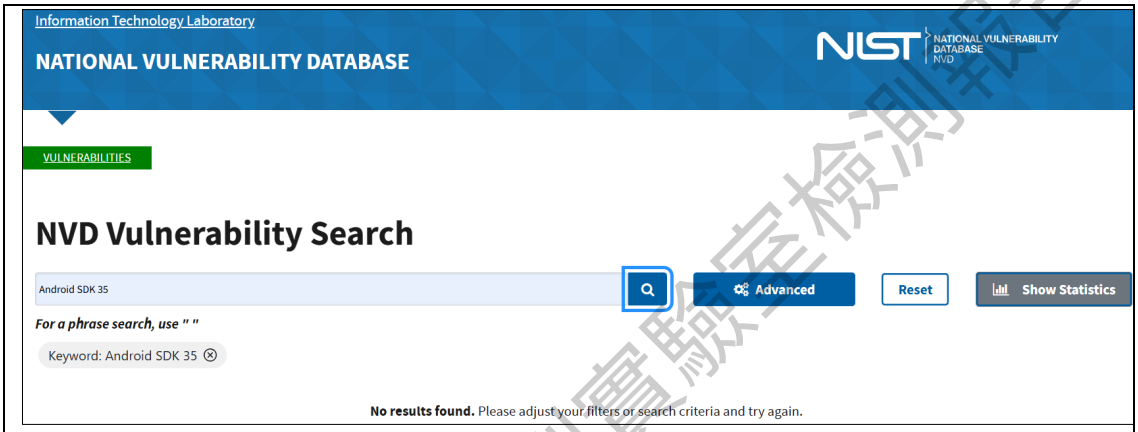
- 4.1.5.1.2 行動應用程式應避免資訊安全漏洞（L1、L2、L3）

1.檢測基準：

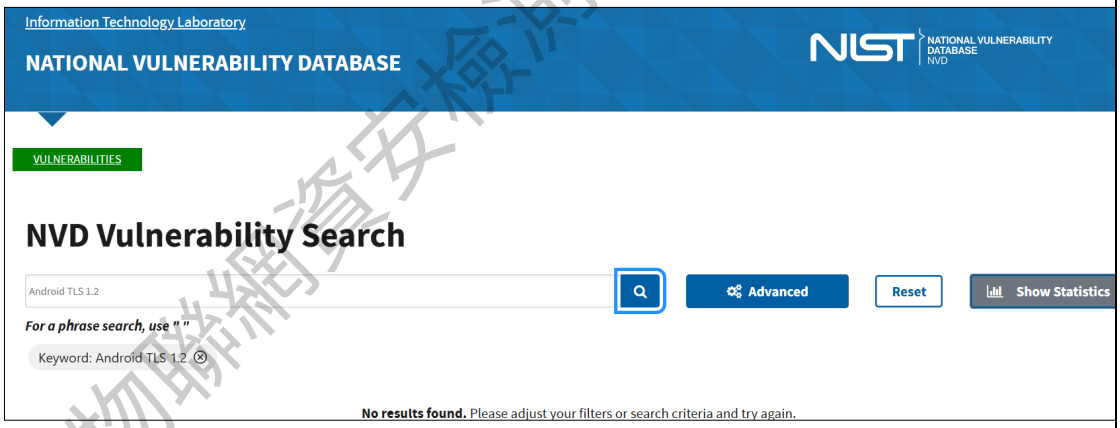
檢查行動應用程式是否不存在已知安全性漏洞。如為「是」則符合檢測基準；「否」則不符合檢測基準。

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)、平台 SDK 版本(圖一)及傳輸協定 TLS1.2(圖二)，均不存在已知的安全性漏洞，檢測結果符合基準。



圖一



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，行動應用程式未針對螢幕覆蓋攻擊進行防護或主動警示使用者，檢測結果不符合基準。

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）

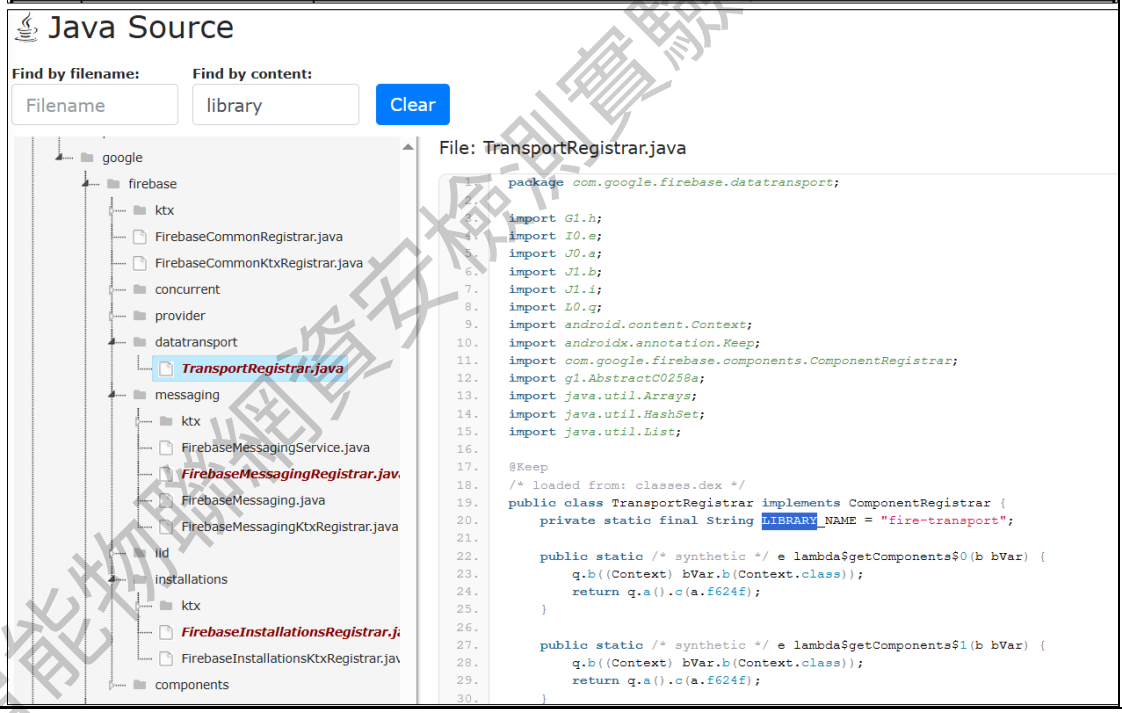
1.檢測基準：

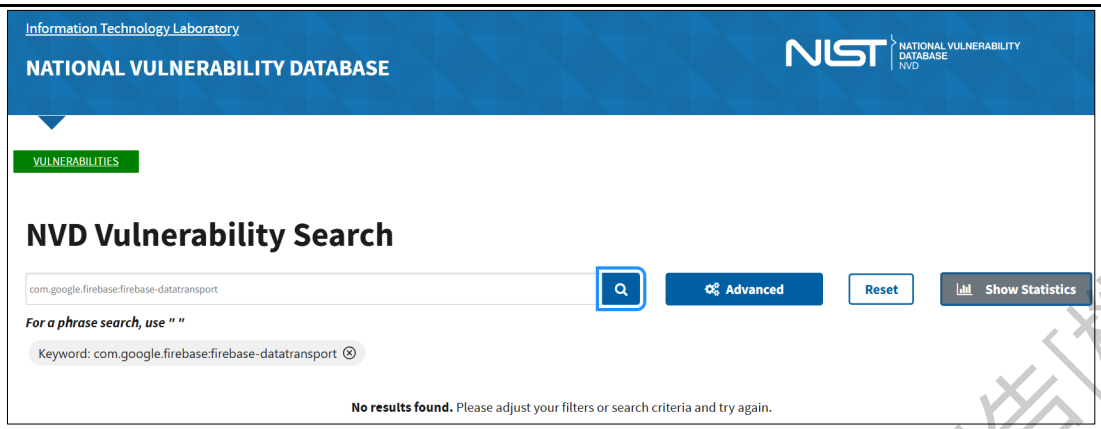
檢查行動應用程式引用之函式庫是否不存在已知安全性漏洞。如為「是」則符合檢測基準；「否」則不符合檢測基準。

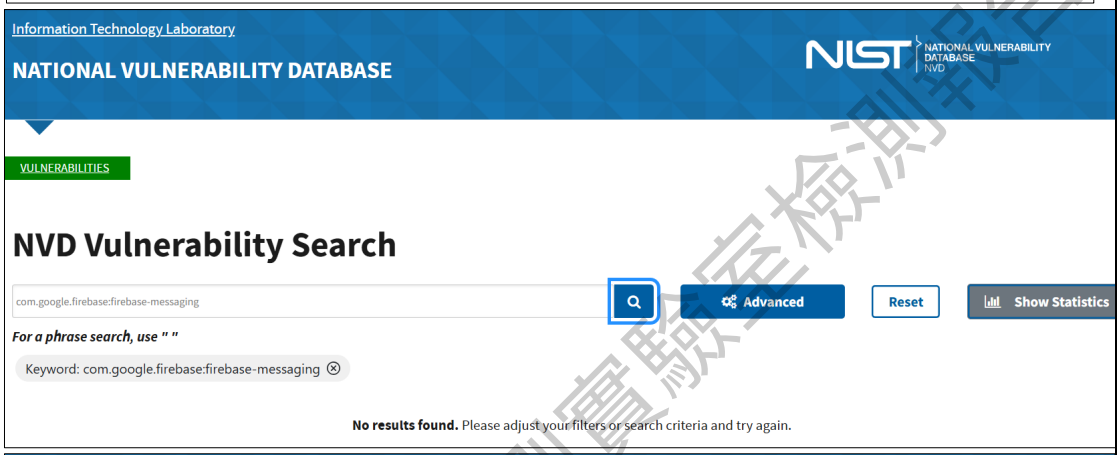
2.檢測結果： ■符合 □不符合

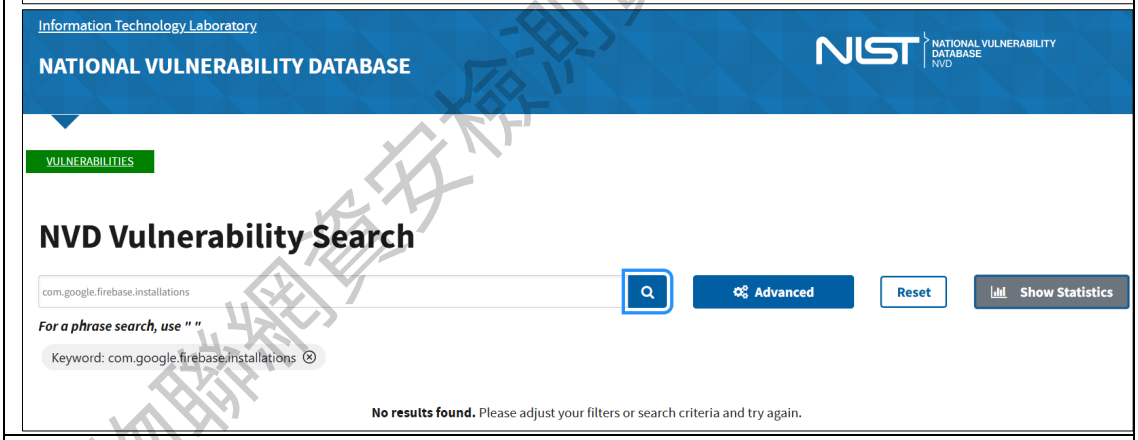
經過實驗室檢測，行動應用程式調查表所列和 MobSF 反組譯，透過 NVD 網站查詢引用之函式庫未發現已存在之安全性漏洞，檢測結果符合基準。

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）

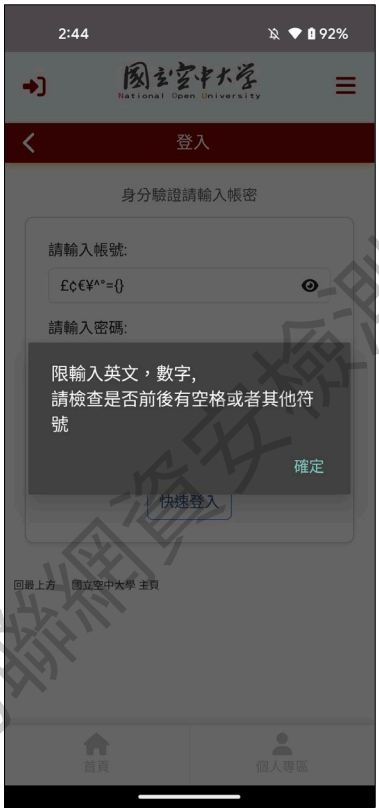
1.檢測基準：

（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。

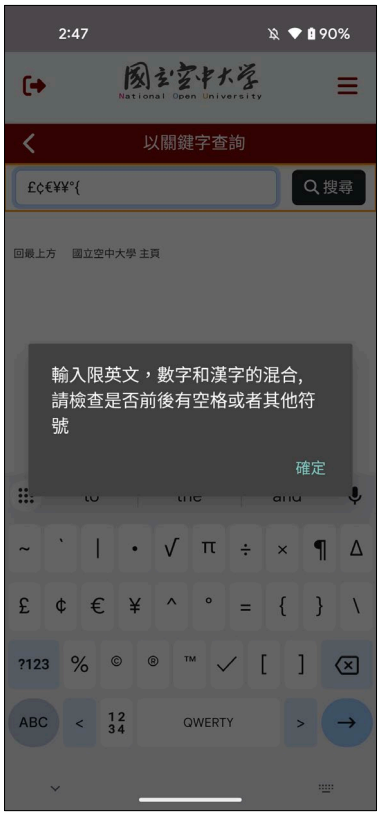
2.檢測結果： ■符合 □不符合

經實驗室檢測，行動應用程式有針對帳號做驗證(限制輸入英文.數字.圖一;限制長度 30 字元.圖二)，密碼(限制 30 字元.圖二)，查詢(限制輸入英文.數字.漢字.圖三;限制長度 50 字元.圖四)，檢測結果符合基準。

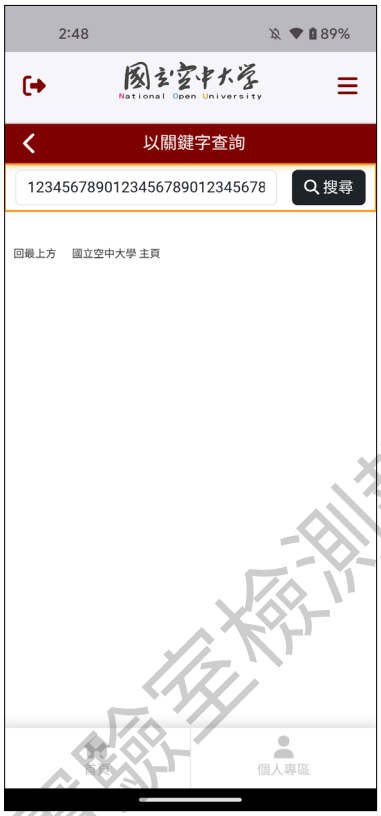


圖一

圖二



圖三



圖四

檢測結果圖示

- 4.1.5.4.2 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。

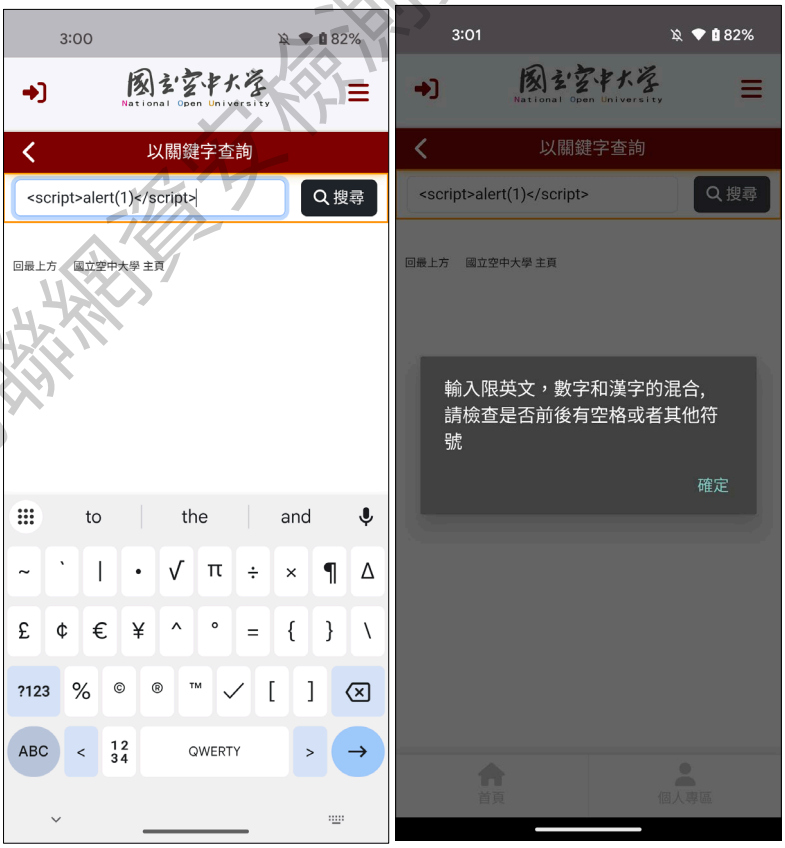
（6）檢查行動應用程式是否防護使用者輸入Format String Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

（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。

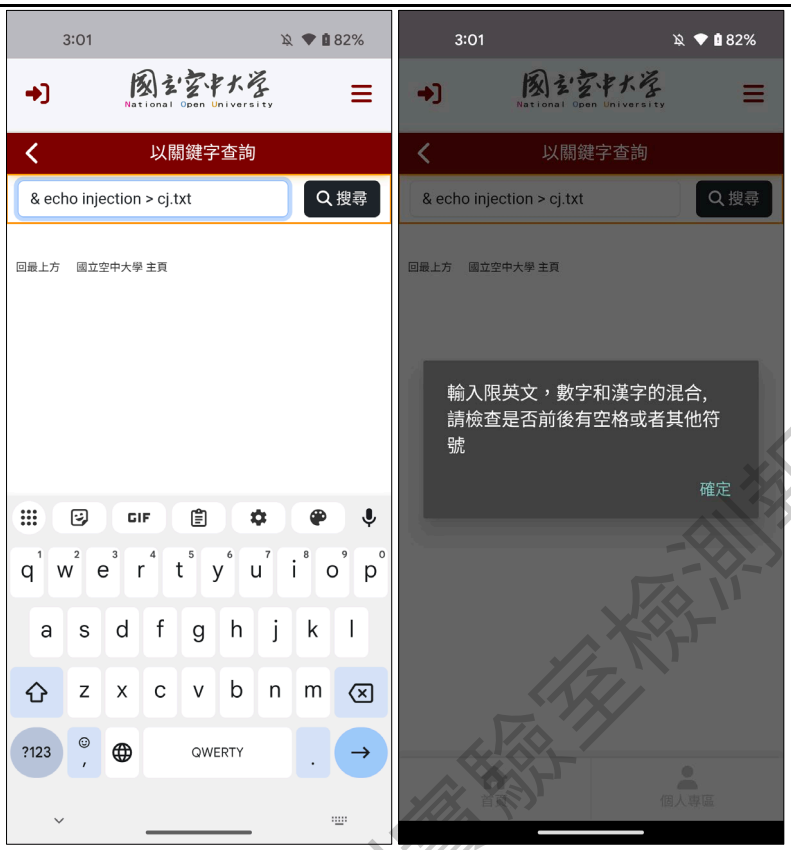
2.檢測結果： ■符合 □不符合

經過實驗室檢測，行動應用程式在設計上都有做輸入的符號格式設定，防護機制完善，輸入 SQL Injection 未發生未知的錯誤(圖一)；輸入 JavaScript Injection 字串未發現預期彈出式對話框(圖二);輸入 Command Injection 字串未發現預期創建檔案(圖三)；輸入 Local File Inclusion 字串未發現行動應用程式開啟該檔案(圖四)；輸入 XML Injection 字串未發生預期錯誤(圖五);輸入 Format String Injection 字串未發生緩衝區溢位或 crash 狀況(圖六)；Intent Injection 字串僅能以注入之 intent 啟動特定 activity (圖七)。在輸入欄位時，以上的測項皆有防護機制設定，檢測結果符合基準。

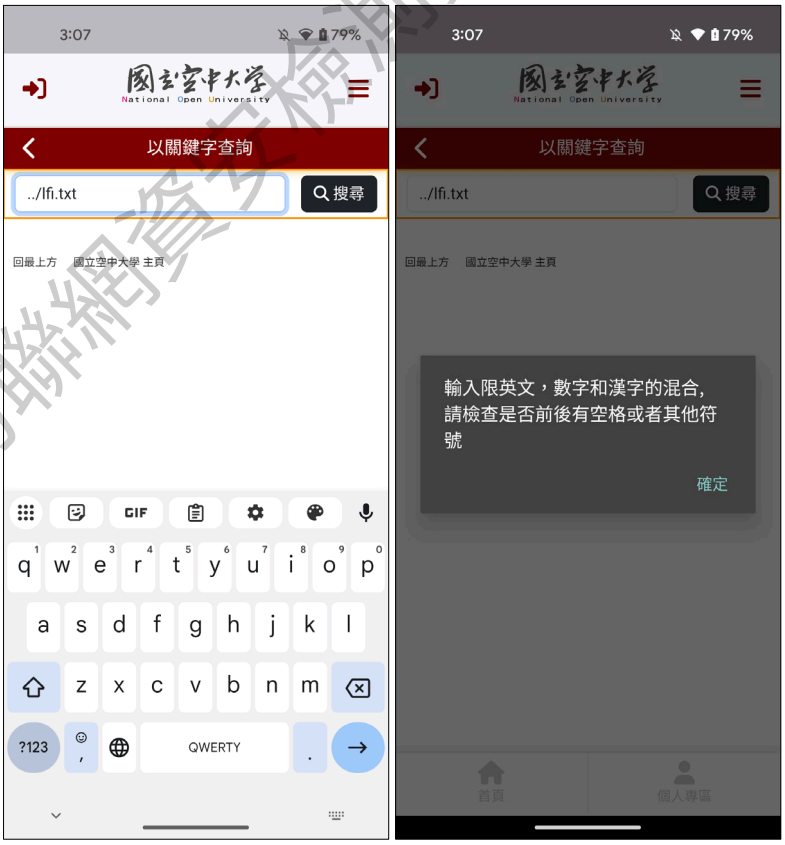
圖一



圖二



圖三



圖四

圖五

圖六

```
sunfish:/ # dumpsys activity activities | grep ResumedActivity
    topResumedActivity=ActivityRecord{9da6471 u0 tw.edu.nouapp/.MainActivity} t1
27}
  ResumedActivity: ActivityRecord{9da6471 u0 tw.edu.nouapp/.MainActivity} t127}
w.edu.nouapp/.MainActivity -a android.intent.action.VIEW                    <
Starting: Intent { act=android.intent.action.VIEW cmp=tw.edu.nouapp/.MainActivit
y }
Warning: Activity not started, its current task has been brought to the front
```

圖七

檢測結果圖示

- 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，網頁伺服器弱點掃描尚未提供，檢測結果不符合基準。

20.	是否使用WebView	■是，網域/子網域名稱： http://www.nou.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， ，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：請輸入可掃描時段 ■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