行動應用App基本資安檢測參考步驟

（Android版）V1.0

中華民國 105 年 10 月 6 日

目　次

表　目　次

1. 編修目的

為使既有及有意加入行動應用 App 檢測之資安實驗室（以下稱檢測實驗室），對於「行動應用 App 基本資安檢測基準」（以下稱基本資安檢測基準）各檢測項目可採用之檢測工具與步驟有更進一步的了解，爰編修此文件提供檢測實驗室參考，以期達成：

- 對於既有檢測實驗室，提供聚焦效果，強化不同實驗室檢測結果之一致性。
- 對於有意加入檢測行列之實驗室提供入門指引，以減少摸索學習時間。

2. 適用對象

本文件主要提供既有及有意加入行動應用 App 檢測之資安實驗室參考，以幫助檢測實驗室發展符合「行動應用 App 基本資安檢測基準」檢測需要之自有檢測方法。

3. 建議事項

以下所列為檢測實驗室於進行檢測工作時，建議應注意之事項。

- 進行靜態分析之程式碼，可由檢測實驗室與送測單位協商提供原始碼進行白箱測試；若使用逆向工程進行程式碼檢測，建議應於檢測前取得送測單位書面同意。
- 使用封包側錄工具檢視行動應用程式所傳輸之資料時，應盡可能檢視所有封包傳送內容。若行動應用程式以 SSL/TLS 加密方式傳輸資料，且進行憑證綁定，應嘗試找出憑證綁定方法，或使用可繞過憑證綁定機制之檢測環境，解除憑證綁定效果進行檢測；亦可經授權取得伺服器私鑰後將加密封包解密進行檢測。
- 「行動應用 App 基本資安檢測資料調查表」可參考「行動應用 App 基本資安檢測基準」中「附錄二、行動應用 App 基本資安檢測資料調查表」所列

內容由檢測實驗室自行增訂檢測所需資訊。

- 可信任之應用程式商店依照「行動應用 App 基本資安檢測基準」中「附錄四、行動應用 App 基本資安參考項目」參考編號 REF-1.之參考說明所述，主要為：
  - 行動作業系統業者之行動應用程式商店。
  - 行動裝置製造業者之行動應用程式商店。
  - 行動通信業者提供之行動應用程式商店。
- 所有需「取得使用者同意」之檢測項目，可於信任之行動應用程式商店以「使用者下載安裝使用即視為同意」之聲明方式或行動應用程式至少於第一次執行時，以「主動提供說明及同意與不同意選項」方式，取得使用者同意，當送檢之行動應用程式同時提供上述兩種取得使用者同意之方式時，以行動應用程式內取得使用者同意之方式為檢測判定是否符合之依據。

4. 檢測步驟

本章節針對 Android 作業系統之行動應用程式檢測，依「行動應用 App 基本資安檢測基準」技術要求與各檢測項目所須檢測之檢查事項，針對每一檢測項目以表列方式分別增加檢測要點、參考工具、前置作業、檢測步驟等欄位，以提供檢測工作中應注意或應依循的事項、檢測可使用之工具、檢測前應完成之程序、檢測環境準備或其他應先完成之檢測項目及檢測進行之程序步驟等參考。檢測步驟表欄位說明請參閱表 1。

表1　檢測步驟表欄位說明

欄位名稱	欄位說明
檢測編號	依據「行動應用 App 基本資安規範」之「4.技術要求」編號項次，檢測編號由 5 碼組成，分別為 4.1.x.y.z，「4.1.」表示為「行動應用程式基本資安檢測基準」，「x.y.z」分別為其向下所展開之次編號項目
檢測項目	參照「行動應用 App 基本資安規範」之「4.技術要求」內容，訂定檢測摘要簡稱
技術要求	依據「行動應用 App 基本資安規範」之「4.技術要求」相對應之行動應用程式資訊安全技術要求事項「內容」
檢測要點	檢測應注意或應依循的事項
參考工具	檢測可使用之工具
前置作業	檢測前應完成之程序、檢測環境準備或其他應先完成之檢測項目
檢測步驟	檢測進行之程序步驟
備註	其他說明事項

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

檢測編號	4.1.1.1.2
檢測項目	行動應用程式發布說明
技術要求	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
檢測要點	應從行動裝置內安裝之可信任應用程式商店 App 介面檢視
參考工具	行動裝置內安裝之可信任應用程式商店 App
前置作業	確認待測行動應用程式發布之可信任應用程式商店
檢測步驟	步驟 1：執行可信任應用程式商店 App 步驟 2：搜尋待測行動應用程式 步驟 3：檢視待測行動應用程式基本資訊中，欲存取之敏感性資料，記錄檢視結果並作為檢測報告附件 步驟 4：檢視待測行動應用程式基本資訊中，欲存取之行動裝置資源，記錄檢視結果並作為檢測報告附件 步驟 5：檢視待測行動應用程式基本資訊中，宣告之權限與用途，記錄檢視結果並作為檢測報告附件
備註	須於「行動應用 App 基本資安檢測資料調查表」自我宣告發布來源 應用程式商店之宣告以行動裝置之商店介面為主

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

檢測編號	4.1.1.3.1
檢測項目	行動應用程式問題回報
技術要求	行動應用程式開發者應提供回報安全性問題之管道
檢測要點	應從行動裝置內安裝之可信任應用程式商店 App 介面檢視
參考工具	手機內安裝之可信任應用程式商店 App
前置作業	確認待測行動應用程式發布之可信任應用程式商店
檢測步驟	步驟 1：執行可信任應用程式商店 App 步驟 2：搜尋待測行動應用程式 步驟 3：檢視待測行動應用程式基本資訊中，欲存取之敏感性資料，記錄檢視結果並作為檢測報告附件 步驟 4：檢視待測行動應用程式基本資訊中，欲存取之行動裝置資源，記錄檢視結果並作為檢測報告附件 步驟 5：檢視待測行動應用程式基本資訊中，宣告之權限與用途，記錄檢視結果並作為檢測報告附件
備註	須於「行動應用 App 基本資安檢測資料調查表」自我宣告發布來源 應用程式商店之宣告以行動裝置之商店介面為主

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

檢測編號	4.1.2.1.1
檢測項目	行動應用程式敏感性資料蒐集聲明
技術要求	行動應用程式應於蒐集敏感性資料前，取得使用者同意
檢測要點	須先盡可能找出待測行動應用程式實際會透過網路傳送之敏感性資料，再進行檢測基準符合性判定
參考工具	Hook 類型檢測工具、wireshark 或其他封包側錄工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行並操作所有待測行動應用程式之功能，檢視所有使用者可輸入資料之欄位位置、預期使用者輸入資料之內容格式是否為敏感性資料，並記錄所有資料欄位位置、內容與結果，並作為檢測報告附件 步驟 3：執行並操作所有待測行動應用程式之功能，包含資料輸入動作，並選擇「同意」待測行動應用程式蒐集，記錄所有待測行動應用程式實際存取與輸入之敏感性資料，並作為檢測報告附件 步驟 4：檢查待測行動應用程式透過網路傳送之敏感性資料，將檢出之敏感性資料作為檢測報告附件 步驟 5：若「步驟 3」未檢出敏感性資料，則待測行動應用程式未發現蒐集敏感性資料，將檢查結果作為檢測報告附件，則本檢測項目檢測結束 步驟 6：若「步驟 3」有檢出敏感性資料，檢查該敏感性資料是否於行動應用程式內聲明，將檢查結果作為檢測報告附件 步驟 7：檢查該敏感性資料於第 1 次執行待測行動應用程式時，是

	否有「使用待測行動應用程式即視為同意蒐集敏感性資料」之相關宣告內容，將檢查結果作為檢測報告附件。若有，則本檢測項目檢測結束 步驟 8：檢查該敏感性資料是否於待測行動應用程式，蒐集該敏感性資料前取得使用者同意，將檢查結果作為檢測報告附件
備註	應明確取得使用者同意

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

檢測編號	4.1.2.1.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料蒐集機制
技術要求	行動應用程式應提供使用者拒絕蒐集敏感性資料之權利
檢測要點	須先盡可能找出待測行動應用程式實際會透過網路傳送之敏感性資料，再進行檢測基準符合性判定
參考工具	Hook 類型檢測工具、wireshark 或其他封包側錄工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：檢查該敏感性資料於第 1 次執行待測行動應用程式時，是否有「若不同意蒐集敏感性資料請勿使用待測行動應用程式」之相關聲明內容與提供不同意的權利，將檢查結果記錄，作為檢測報告附件 步驟 3：執行並操作所有待測行動應用程式功能，包括資料輸入動作，記錄操作過程中待測行動應用程式所有聲明欲蒐集敏感性資料之相關資訊，包括聲明時機、欲蒐集之敏感性資料及是否提供不同意的權利，記錄相關資訊，作為檢測報告附件後，選擇「不同意」蒐集 步驟 4：檢查待測行動應用程式於「步驟 2」中透過網路傳送之敏感性資料，記錄檢出之敏感性資料，作為檢測報告附件
備註	此項適用經由行動應用程式蒐集敏感性資料之管道 於檢測基準 4.1.2.1.1 之檢測結果因未聲明所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

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

檢測編號	4.1.2.3.1
檢測項目	行動應用程式敏感性資料儲存聲明
技術要求	行動應用程式應於儲存敏感性資料前，取得使用者同意
檢測要點	須先找出所有待測行動應用程式會儲存之敏感性資料，再進行檢測基準符合性判定 敏感性資料應容易識別、搜尋且來源應包含所有輸入之敏感性資料、已存在系統內經權限授予而可取得之敏感性資料與登入帳號後由伺服端下載之敏感性資料
參考工具	檔案瀏覽器、SQLite 工具或 Hook 類型檢測工具、Log 檢視工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：檢查待測行動應用程式於可信任之應用程式商店，是否有「使用待測行動應用程式即視為同意儲存敏感性資料」與「若不同意儲存敏感性資料請勿安裝待測行動應用程式」等相關聲明內容，記錄檢查結果作為檢測報告附件 步驟 2：於行動裝置安裝待測行動應用程式 步驟 3：執行並操作所有待測行動應用程式功能，包括資料輸入動作，記錄操作過程中待測行動應用程式所有聲明欲儲存敏感性資料之相關資訊，包括聲明時機、欲儲存之敏感性資料及是否取得使用者同意，記錄相關資訊作為檢測報告附件 步驟 4：關閉待測行動應用程式 步驟 5：使用 SQLite 工具查看行動裝置內，檢查待測行動應用程式執行後所產生之 SQLite 資料庫，尋找待測行動應用程式

	經「步驟2」取得之所有敏感性資料。記錄檢查結果作為檢測報告附件 步驟6：檢查行動裝置內其他檔案中，待測行動應用程式經「步驟2」取得之所有敏感性資料。記錄檢測結果作為檢測報告附件 步驟7：若「步驟5」及「步驟6」未檢出敏感性資料，則待測行動應用程式未發現儲存敏感性資料，記錄檢查結果作為檢測報告附件，則本檢測項目檢測結束 步驟8：若「步驟5」及「步驟6」有檢出敏感性資料，檢查該敏感性資料是否於可信任之應用程式商店內聲明，記錄檢查結果作為檢測報告附件 步驟9：若「步驟5」及「步驟6」有檢出敏感性資料，檢查該敏感性資料是否於待測行動應用程式內聲明，記錄檢查結果作為檢測報告附件
備註	應用程式商店之宣告以行動裝置之商店介面為主

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

檢測編號	4.1.2.3.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料儲存機制
技術要求	行動應用程式應提供使用者拒絕儲存敏感性資料之權利
檢測要點	輸入之敏感性資料應容易識別、搜尋
參考工具	檔案瀏覽器、文字編輯器、解碼工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行並操作所有待測行動應用程式功能，包括敏感性資料輸入 步驟 3：使用檔案瀏覽器檢查待測行動應用程式於行動裝置產生之所有檔案，詳列檢出之敏感性資料作為檢測報告附件，若無檢出敏感性資料，則本檢測項目檢測結束。 步驟 4：若「步驟 3」有檢出敏感性資料，檢視該應用程式是否提供使用者拒絕儲存敏感性資料選項，記錄檢查結果作為檢測報告附件，若無提供拒絕敏感性資料儲存選項，則本檢測項目檢測結束 步驟 5：「步驟 4」有提供使用者拒絕儲存敏感性資料選項，且使用者選擇同意或拒絕儲存敏感性資料，記錄檢查結果作為檢測報告附件
備註	於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

4.1.2.3.4. 行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中

檢測編號	4.1.2.3.4
檢測項目	行動應用程式敏感性資料儲存限制
技術要求	行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中
檢測要點	敏感性資料應容易識別、搜尋且來源應包含所有輸入之敏感性資料、已存在系統內經權限授予而可取得之敏感性資料與登入帳號後由伺服端下載之敏感性資料
參考工具	檔案瀏覽器、文字編輯器、解碼工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：若檢測基準 4.1.2.3.1 有檢出儲存敏感性資料，刪除儲存敏感性資料之檔案後，重新執行並觀察待測行動應用程式運作狀態，記錄檢查結果作為檢測報告附件 步驟 2：若「步驟 1」中刪除之檔案不影響待測行動應用程式重新執行後之所有功能，請與送檢單位確認該檔案之用途，並記錄確認結果作為檢測報告附件。
備註	受作業系統保護之區域亦不可檢出

4.1.2.3.5. 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

檢測編號	4.1.2.3.5
檢測項目	行動應用程式敏感性資料儲存保護
技術要求	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
檢測要點	對於加密演算法常用的關鍵字收集
參考工具	Java 程式碼編輯器、文字編輯器（如：notepad++）, jd-gui, jd-cli, apktool, dex2jar, jadx, find 等
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整 取得待測行動應用程式安裝檔
檢測步驟	步驟 1：對待測行動應用程式安裝檔，進行逆向工程以取得程式碼 步驟 2：搜尋程式碼目錄中有關加密函式之相關字串，記錄具相關字串之程式碼內容、檔案路徑與檔案名稱，作為檢測報告附件 步驟 3：比對是否為 AES，記錄比對結果，作為檢測報告附件 步驟 4：比對是否為 Triple DES，記錄比對結果，作為檢測報告附件 步驟 5：比對是否為 SHA-256，記錄比對結果，作為檢測報告附件
備註	符合檢測基準 4.1.2.3.4 之形成條件為「不得檢出」儲存敏感性資料，故無敏感性資料加密處理後再儲存議題

4.1.2.3.6. 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

檢測編號	4.1.2.3.6
檢測項目	行動應用程式敏感性資料儲存控管
技術要求	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
檢測要點	敏感性資料應容易識別、搜尋且來源應包含所有輸入之敏感性資料、已存在系統內經權限授予而可取得之敏感性資料與登入帳號後由伺服端下載之敏感性資料
參考工具	檔案瀏覽器、文字編輯器
前置作業	將待測行動應用程式執行完畢後，取出執行後的相關檔案進行分析
檢測步驟	步驟 1：若檢測基準 4.1.2.3.1 未檢出儲存敏感性資料，則本檢測項目檢測結束 步驟 2：若檢測基準 4.1.2.3.1 有檢出儲存敏感性資料，檢視所有儲存敏感性資料檔案之路徑，記錄檢視結果，作為檢測報告附件
備註	符合檢測基準 4.1.2.3.4 之形成條件為「不得檢出」儲存敏感性資料，故無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議題

4.1.2.3.7. 敏感性資料應避免出現於行動應用程式之程式碼

檢測編號	4.1.2.3.7
檢測項目	行動應用程式敏感性資料硬碼（Hard Code）
技術要求	敏感性資料應避免出現於行動應用程式之程式碼
檢測要點	檢查標的為待測行動應用程式安裝檔內使用硬碼（Hard Code）方式之敏感性資料
參考工具	逆向工程工具、Hook 類型檢測工具、記憶體分析工具等
前置作業	取得待測行動應用程式安裝檔
檢測步驟	步驟 1：對待測行動應用程式安裝檔，進行逆向工程以取得程式碼及其他安裝檔內封裝之檔案 步驟 2：檢查程式碼及其他安裝檔內封裝之檔案中，有關密碼之相關字串，記錄相關檔案路徑與檔案名稱，作為檢測報告附件 步驟 3：檢查程式碼及其他安裝檔內封裝之檔案中，有關身分驗證資訊之相關字串，記錄相關檔案路徑與檔案名稱，作為檢測報告附件 步驟 4：檢查程式碼及其他安裝檔內封裝之檔案中，有關對稱式加解密演算法金鑰之相關字串，記錄相關檔案路徑與檔案名稱，作為檢測報告附件
備註	參考 CWE 揭露之 Hard code 弱點類型（如：CWE-259、CWE-321、CWE-798）

4.1.2.4.1. 行動應用程式透過網路傳輸敏感性資料，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

檢測編號	4.1.2.4.1
檢測項目	行動應用程式敏感性資料傳輸
技術要求	行動應用程式透過網路傳輸敏感性資料，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
檢測要點	須使用動態檢測方式進行，側錄所有待測行動應用程式產生之網路連線行為，以待測行動應用程式執行時與伺服端實際連線所使用之加密協定為檢測標的
參考工具	wireshark 或其他封包側錄工具
前置作業	準備檢測用行動裝置之網路連線封包側錄環境
檢測步驟	步驟 1：啟動封包側錄作業 步驟 2：於行動裝置安裝待測行動應用程式 步驟 3：執行及操作待測行動應用程式所有功能，並依「檢測報告附件」所記錄之輸入資料資訊，再次完整輸入相同資料 步驟 4：關閉待測行動應用程式 步驟 5：停止封包側錄作業 步驟 6：查看所有側錄封包，檢查待測行動應用程式所有使用 SSL 與 TLS 加密協定之網路連線，記錄連線目的地 IP 位址或網域名稱及其使用之加密協定版本，作為檢測報告附件 步驟 7：查看所有側錄封包，檢查待測行動應用程式所有使用 SSL 與 TLS 加密協定之網路連線，記錄所有伺服端回傳給待測行動應用程式之憑證資訊、金鑰演算法與金鑰長度，作為檢測報告附件 步驟 8：查看所有側錄封包，檢查待測行動應用程式所有使用 SSL 與 TLS 加密協定之網路連線，記錄所有伺服端回應給待測行動應用程式之加密套件資訊與資料加密演算法，作為檢測報告附件
備註	無

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

檢測編號	4.1.2.5.1
檢測項目	行動應用程式敏感性資料分享聲明
技術要求	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
檢測要點	對於分享相關常用的關鍵字收集
參考工具	notepad++, jd-gui, jd-cli, apktool, dex2jar
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整 取得待測行動應用程式安裝檔
檢測步驟	靜態分析方式： 步驟 1：對待測行動應用程式安裝檔，進行逆向工程以取得程式碼 步驟 2：搜尋程式碼目錄中有關分享內容之相關字串，並記錄具相關字串之程式碼內容、檔案路徑與檔案名稱作為檢測報告附件 步驟 3：找出所有可分享之內容，並記錄作為檢測報告附件 步驟 4：檢查是否檢出敏感性資料，記錄結果作為檢測報告附件 動態分析方式： 步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行並操作所有待測行動應用程式分享功能，並記錄作為檢測報告附件 步驟 3：找出所有可分享之內容，並記錄作為檢測報告附件 步驟 4：檢查是否檢出敏感性資料，並記錄作為檢測報告附件
備註	無

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。

檢測編號	4.1.2.5.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料分享機制
技術要求	行動應用程式應提供使用者拒絕分享敏感性資料之權利
檢測要點	對於分享相關常用的關鍵字收集
參考工具	notepad++, jd-gui, jd-cli, apktool, dex2jar
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整 取得待測行動應用程式安裝檔
檢測步驟	靜態分析方式： 步驟 1：對待測行動應用程式安裝檔，進行逆向工程以取得程式碼 步驟 2：搜尋程式碼目錄中有關分享內容之相關字串，並記錄具相關字串之程式碼內容、檔案路徑與檔案名稱作為檢測報告附件 步驟 3：找出所有可分享之內容，並記錄作為檢測報告附件 步驟 4：檢查分享內容是否為敏感性資料，記錄結果作為檢測報告附件 步驟 5：檢查分享內容是否有提供使用者拒絕分享敏感性資料的權利，記錄結果作為檢測報告附件 動態分析方式： 步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行並操作所有待測行動應用程式分享功能，並記錄作為檢測報告附件 步驟 3：找出所有可分享之內容，並記錄作為檢測報告附件 步驟 4：檢查分享內容是否為敏感性資料，並記錄作為檢測報告附件 步驟 5：檢查分享內容是否有提供使用者拒絕分享敏感性資料的權利，並記錄作為檢測報告附件

備註	無

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

檢測編號	4.1.2.5.3
檢測項目	行動應用程式敏感性資料分享權限控管
技術要求	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
檢測要點	使用檔案分享敏感性資料時，檢測是否使用 FileProvider 類別
參考工具	notepad++, apktool
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整 取得待測行動應用程式安裝檔
檢測步驟	靜態分析方式： 步驟 1:對待測行動應用程式安裝檔,進行逆向工程以取得 Android Manifest.xml 步驟 2：若 AndroidManifest.xml 中存在 provider 元素的 android:authorities 的 package name，記錄名稱作為檢測報告附件 步驟 3：找出 res/xml/filepaths.xml 中 files-path 的值，並記錄作為檢測報告附件 步驟 4：判斷 files-path 中分享的資料夾是否檢出敏感性資料，記錄結果作為檢測報告附件 動態分析方式： 步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行並操作所有待測行動應用程式功能，並記錄作為檢測報告附件 步驟 3：找出所有寫入外部儲存空間的檔案，並記錄作為檢測報告附件 步驟 4：判斷是否檢出敏感性資料，並記錄作為檢測報告附件

備註	無

4.1.3.1.1. 行動應用程式應於使用付費資源前主動通知使用者

檢測編號	4.1.3.1.1
檢測項目	行動應用程式付費資源使用聲明
技術要求	行動應用程式應於使用付費資源前主動通知使用者
檢測要點	執行待測行動應用程式後，檢測行動應用程式付費機制中，於付費前是否提供訂單確認功能
參考工具	無
前置作業	檢查待測行動應用程式所有付費方式，準備相關付款所需資料
檢測步驟	步驟 1：執行待測行動應用程式付費功能進行付款程序，記錄所有可使用之付費方式作為檢測報告附件 步驟 2：使用所有付費方式，並觀察於付費前是否主動顯示基準要求之資訊提供使用者確認，作為檢測報告附件
備註	規範中所述之「使用付費資源前」於基準定義為「付費前」，即檢查行動應用程式於付費前是否主動通知使用者

4.1.3.1.2. 行動應用程式應提供使用者拒絕使用付費資源之權利

檢測編號	4.1.3.1.2
檢測項目	行動應用程式拒絕付費資源使用機制
技術要求	行動應用程式應提供使用者拒絕使用付費資源之權利
檢測要點	執行待測行動應用程式後，檢測行動應用程式付費機制中，於實際付費行為發生前是否可終止付款
參考工具	無
前置作業	檢查待測行動應用程式所有付費方式，準備相關付款所需資料
檢測步驟	步驟 1：執行待測行動應用程式付費功能進行付款程序，記錄所有可使用之付費方式，作為檢測報告附件 步驟 2：使用所有付費方式，並觀察於實際付費行為發生前是否主動顯示拒絕付費功能，作為檢測報告附件 步驟 3：選擇拒絕付費功能後，查看交易紀錄，紀錄交易結果作為檢測報告附件
備註	規範中所述之「使用付費資源前」於基準定義為「付費時」，即檢查行動應用程式於付費前是否主動提供使用者拒絕付費選項

4.1.3.2.1. 行動應用程式應於使用付費資源前進行使用者認證

檢測編號	4.1.3.2.1
檢測項目	行動應用程式付費資源使用者認證
技術要求	行動應用程式應於使用付費資源前進行使用者認證
檢測要點	使用者開啟待測行動應用程式付費功能項目後，行動應用程式於付款過程中應有確認使用者認證機制
參考工具	無
前置作業	檢查待測行動應用程式所有付費方式，準備相關付款所需資料
檢測步驟	步驟 1：執行待測行動應用程式付費功能進行付款程序，記錄所有可使用之付費方式，作為檢測報告附件 步驟 2：使用所有付費方式，並觀察於實際付費行為發生前是否有使用者認證機制，作為檢測報告附件 步驟 3：於步驟 2 結束後立即再次使用所有付費功能，並觀察於實際付費行為發生前是否仍有使用者認證機制，作為檢測報告附件
備註	規範中所述之「使用付費資源前」於基準定義為「付費時」，即檢查行動應用程式於付費前是否進行使用者認證 每次交易付費前均須進行身分認證

4.1.3.2.2. 行動應用程式應記錄使用之付費資源與時間

檢測編號	4.1.3.2.2
檢測項目	行動應用程式付費資源紀錄
技術要求	行動應用程式應記錄使用之付費資源與時間
檢測要點	檢視待測行動應用程式付費後之交易紀錄
參考工具	無
前置作業	使用者完成待測行動應用程式付費功能 檢查待測行動應用程式所有付費方式，準備相關付款所需資料
檢測步驟	步驟 1：開啟待測行動應用程式並執行所有功能，檢查是否有須付費之功能。若無，則本檢測項目檢測結束。 步驟 2：執行待測行動應用程式，進行付費程序並確認交易成功，結束待測行動應用程式 步驟 3：依付費方式所提供之交易查詢管道進行查詢，並將查詢結果之內容作為檢測報告附件 步驟 4：待測行動應用程式應提供交易紀錄功能，記錄結果作為檢測報告附件
備註	規範中所述之「付費資源與時間」於基準定義為「交易記錄」，即檢查行動應用程式是否提供交易記錄及記錄之內容

4.1.4.1.1. 行動應用程式應有適當之身分認證機制，確認使用者身分

檢測編號	4.1.4.1.1
檢測項目	行動應用程式使用者身分認證機制
技術要求	行動應用程式應有適當之身分認證機制，確認使用者身分
檢測要點	針對待測行動應用程式進行使用者認證機制檢查
參考工具	無
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：安裝並執行待測行動應用程式所有功能 步驟 2：檢查待測行動應用程式內所有可存取個人資料相關之敏感性資料路徑，是否皆須通過認證機制確認身分 步驟 3：記錄結果含認證方式，作為檢測報告附件
備註	無

4.1.4.1.2. 行動應用程式應依使用者身分授權

檢測編號	4.1.4.1.2
檢測項目	行動應用程式使用者身分授權
技術要求	行動應用程式應依使用者身分授權
檢測要點	確認待測行動應用程式讀取使用者資料時，其確認使用者身分機制
參考工具	無
前置作業	待測行動應用程式進行使用者資料異動時，應有相關的認證機制
檢測步驟	步驟 1：檢查待測行動應用程式使用者相關之身分類別，並記錄作為檢測報告附件 步驟 2：進行滲透測試，進行不同身分權限之越權與提權嘗試
備註	無

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

檢測編號	4.1.4.2.1
檢測項目	行動應用程式交談識別碼規則性
技術要求	行動應用程式應避免使用具有規則性之交談識別碼
檢測要點	使用可觀察交談識別碼之檢測方法進行檢測
參考工具	Burp、逆向工程工具、Hook 類型檢測工具、記憶體分析工具等
前置作業	準備檢測環境
檢測步驟	步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行及操作待測行動應用程式所有功能，並依「檢測基準 4.1.2.1.1」所記錄之輸入資料資訊，再次完整輸入相同資料 步驟 3：找出待測行動應用程式於使用者身分認證後所使用之所有交談識別碼機制（該交談識別碼以下稱認證後交談識別碼），辯識所有交談識別碼機制為程式框架（如：J2EE, ASP .NET, PHP 等）內建或自行設計，記錄結果作為檢測報告附件 步驟 4：檢查認證後交談識別碼之長度及亂度（Entropy），記錄結果作為檢測報告附件 步驟 5：檢查認證後交談識別碼之結構及內容，如果內容部分或整個為亂碼，請將該內容與 Base64、ASCII 及 Unicode 等編碼方式進行解碼或 MD5、SHA-1 及 SHA-256 等雜湊方法進行彩虹表（Rainbow Table）查詢，記錄解碼與查詢結果作為檢測報告附件 步驟 6：分別執行及操作待測行動應用程式所有登入動作，並於登入後不執行任何功能，靜置待測行動應用程式，找出逾時失效時間，最長測試時間至少需 30 分鐘以上，記錄結果作為檢測報告附件
備註	本項檢測基準所述之交談識別碼為使用者身分認證後所使用

4.1.4.2.2. 行動應用程式應確認伺服器憑證之有效性

檢測編號	4.1.4.2.2
檢測項目	行動應用程式伺服器憑證有效性
技術要求	行動應用程式應確認伺服器憑證之有效性
檢測要點	找出所有 SSL/TLS 加密連線並檢查
參考工具	Burp、逆向工程工具、Hook 類型檢測工具、記憶體分析工具等
前置作業	準備檢測用行動裝置之網路連線封包側錄環境，準備 MiTM 檢測環境
檢測步驟	步驟 1：於檢測基準 4.1.2.4.1 所側錄封包中，取出所有 SSL 與 TLS 網路連線之伺服端回傳給待測行動應用程式之憑證，將憑證 MD5、SHA1 或 SHA256 指紋檔，記錄結果作為檢測報告附件 步驟 2：檢查所有憑證有效期及註銷狀態，記錄結果作為檢測報告附件 步驟 3：檢查「檢測報告附件」中於檢測基準 4.1.2.4.1 所記錄之所有使用 SSL 與 TLS 加密協定之網路連線目的地 IP 位址與網域名稱與憑證之主體名稱與主體別名相符情況，記錄結果作為檢測報告附件 步驟 4：關閉待測行動應用程式 步驟 5：於 MiTM 檢測環境中，執行及操作待測行動應用程式所有功能，檢查所有 SSL 與 TLS 加密協定網路連線狀態，記錄結果作為檢測報告附件 步驟 6：將待測行動應用程式進行逆向工程，檢查有關憑證綁定之程式碼，記錄結果作為檢測報告附件
備註	無

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、政府機關或企業簽發

檢測編號	4.1.4.2.3
檢測項目	行動應用程式伺服器憑證簽發來源
技術要求	行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發
檢測要點	須使用動態檢測方式進行，找出所有待測行動應用程式產生之 SSL/TLS 網路加密連線並檢查，以待測行動應用程式執行時與伺服端實際連線所使用之加密協定為檢測標的
參考工具	wireshark 或其他封包側錄工具
前置作業	準備檢測用行動裝置之網路連線封包側錄環境
檢測步驟	步驟 1：於檢測基準 4.1.2.4.1 所側錄封包中，取出所有 SSL 與 TLS 網路連線之伺服端回傳給待測行動應用程式之憑證，記錄憑證鏈中之所有憑證簽發單位，作為檢測報告附件 步驟 2：由憑證簽發單位網站取得步驟 1 記錄中，所有憑證鏈中所有簽發單位之憑證 步驟 3：使用步驟 2 中各憑證鏈所有簽發單位之憑證，檢驗檢測基準 4.1.4.2.4 記錄之所有待測行動應用程式使用之憑證，記錄結果作為檢測報告附件
備註	憑證簽發單位說明如下： 1. 行動作業系統內建之可信任憑證機構：為行動作業系統廠商所安裝受信任之憑證簽發單位 2. 政府機關：為政府單位成立之憑證簽發單位 3. 企業：企業自行成立之憑證簽發單位

4.1.4.2.4. 行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料

檢測編號	4.1.4.2.4
檢測項目	行動應用程式連線安全
技術要求	行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料
檢測要點	找出所有 SSL/TLS 加密連線並檢查
參考工具	Burp、逆向工程工具、Hook 類型檢測工具、記憶體分析工具等
前置作業	準備檢測用行動裝置之網路連線封包側錄環境，準備 MiTM 檢測環境
檢測步驟	檢視檢測基準 4.1.2.1.1.之檢測結果，如有傳輸敏感性資料，檢查檢測基準 4.1.4.2.2 或檢測基準 4.1.4.2.3 之檢測結果，記錄結果作為檢測報告附件
備註	無

4.1.5.1.1. 行動應用程式應避免含有惡意程式碼

檢測編號	4.1.5.1.1
檢測項目	行動應用程式惡意程式碼
技術要求	行動應用程式應避免含有惡意程式碼
檢測要點	檢測待測行動應用程式是否有未經使用者同意，私下存取使用者敏感資料，以造成個資外洩或使裝置設備產生安全漏洞，造成損害影響
參考工具	使用防毒軟體、逆向工程工具、封包側錄工具
前置作業	無
檢測步驟	步驟 1：檢視本檢測基準中所列檢測編號之檢測結果是否有不符合 步驟 2：以逆向工程檢視待測行動應用程式之權限（permission）是否有非必要存取使用者權限功能，記錄檢視結果作為檢測報告附件 步驟 3：以逆向工程檢視待測行動應用程式程式碼，是否有已知的惡意程式碼或經檢測驗證的惡意程式碼，記錄檢視結果作為檢測報告附件 步驟 4：實際執行檢測待測行動應用程式活動行為，記錄檢視結果作為檢測報告附件 步驟 5：實際側錄待測行動應用程式所有對外連線，針對所有對外連線之伺服端進行確認並記錄結果，作為檢測報告附件 步驟 6：觀察待測行動應用程式於檢測過程中，是否發生未預期錯誤、資源明顯耗損、重新啟動或關閉等行為，並記錄檢視結果作為檢測報告附件
備註	無

4.1.5.1.2. 行動應用程式應避免資訊安全漏洞

檢測編號	4.1.5.1.2
檢測項目	行動應用程式資訊安全漏洞
技術要求	行動應用程式應避免資訊安全漏洞
檢測要點	待測行動應用程式開發環境應避免有資安漏洞的函式庫或版本
參考工具	無
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整開發環境與系統版本
檢測步驟	步驟 1：檢視本檢測基準中所列檢測編號之檢測結果是否有不符合 步驟 2：檢查待測行動應用程式是否具 CVE 或 CWE/SANS TOP 25 編號之漏洞與不安全之撰寫方式，並記錄檢查結果作為檢測報告附件
備註	無

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

檢測編號	4.1.5.3.1
檢測項目	行動應用程式函式庫引用安全
技術要求	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
檢測要點	待測行動應用程式內含函式庫版本過舊或有資安疑慮時，應更新至修補後的版本或最新版本
參考工具	無
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整開發環境與系統版本
檢測步驟	步驟 1：檢查待測行動應用程式中引用函式庫的名稱與版本資料項目，並記錄檢查結果作為檢測報告附件 步驟 2：檢查記錄之函式庫版本是否具 CVE 或 CWE/SANS TOP 25 編號之漏洞，並記錄檢查結果作為檢測報告附件
備註	須於「行動應用 App 基本資安檢測資料調查表」自我宣告引用函式庫名稱及版本資訊

4.1.5.4.1. 行動應用程式應針對使用者輸入之字串，進行安全檢查

檢測編號	4.1.5.4.1
檢測項目	行動應用程式使用者輸入檢查
技術要求	行動應用程式應針對使用者輸入之字串，進行安全檢查
檢測要點	找出所有使用者可輸入之欄位並檢查
參考工具	無
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整
檢測步驟	步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：執行及操作待測行動應用程式所有功能，並依檢測基準 4.1.2.1.1 記錄所有使用者可輸入資料之欄位，輸入非該欄位預期輸入之內容與格式等資料，並記錄執行結果作為檢測報告附件 步驟 3：執行及操作待測行動應用程式所有功能，並依檢測基準 4.1.2.1.1 記錄所有可輸入資料之欄位，輸入各種長度之資料，並記錄執行結果作為檢測報告附件
備註	無

4.1.5.4.2. 行動應用程式應提供相關注入攻擊防護機制

檢測編號	4.1.5.4.2
檢測項目	行動應用程式注入攻擊防護機制
技術要求	行動應用程式應提供相關注入攻擊防護機制
檢測要點	對於程式碼中取得輸入內容之函式關鍵字收集、擷取 App 傳送參數之方法
參考工具	notepad++, jd-gui, jd-cli, apktool, dex2jar, hook 工具, MiTM 工具
前置作業	送檢單位所檢附之「行動應用 App 基本資安檢測資料調查表」應填具完整 取得待測行動應用程式安裝檔
檢測步驟	靜態分析方式： 步驟 1：對待測行動應用程式安裝檔，進行逆向工程以取得程式碼 步驟 2：搜尋程式碼目錄中有關取得輸入內容之相關字串，觀察搜尋到的相關字串程式碼片段，並記錄該檔案路徑與行數作為檢測報告附件 步驟 3：檢查程式碼片段，是否在輸入內容送出前進行注入攻擊防護處理，記錄檢查結果作為檢測報告附件 動態分析方式： 步驟 1：於行動裝置安裝待測行動應用程式 步驟 2：於所有待測行動應用程式可輸入資料之欄位輸入相關注入攻擊酬載（payload），檢查待測行動應用程式送出之字串是否進行注入攻擊防護處理，記錄攻擊成功過程作為檢測報告附件
備註	無