**第3次行動應用App基本資安檢測能力試驗活動**

結果摘要表

填寫日期：　年　月　日

各基準項目之檢測結果如為「是」或「不適用」，則可免填檢出問題摘要說明及檢測報告佐證頁次內容，但仍應於該等欄位中填入「無」或「N/A」。

| 項次 | 基準項目 | 檢測結果 | 檢出問題摘要說明 | 檢測報告佐證頁次 |
| --- | --- | --- | --- | --- |
| 1 | 4.1.1.1.2.檢查行動應用程式是否於可信任之應用程式商店，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。 | □ 是  □ 否  □ 不適用 |  |  |
| 2 | 4.1.1.3.1.檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內，提供聯絡網頁、電子郵件、電話或其他類型聯絡方式，並可實際聯絡成功。 | □ 是  □ 否  □ 不適用 |  |  |
| 3 | 4.1.2.1.1.檢查行動應用程式所有蒐集之敏感性資料，是否皆已於可信任之應用程式商店或行動應用程式內聲明，並取得使用者同意。 | □ 是  □ 否  □ 不適用 |  |  |
| 4 | 4.1.2.1.2.(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選項。 | □ 是  □ 否  □ 不適用 |  |  |
| 5 | 4.1.2.1.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 6 | 4.1.2.3.1.(1)檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內聲明。 | □ 是  □ 否  □ 不適用 |  |  |
| 7 | 4.1.2.3.1.(2)檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內取得使用者同意。 | □ 是  □ 否  □ 不適用 |  |  |
| 8 | 4.1.2.3.2.(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選項。 | □ 是  □ 否  □ 不適用 |  |  |
| 9 | 4.1.2.3.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 10 | 4.1.2.3.4.(1)檢查行動應用程式是否未檢出將敏感性資料儲存於冗餘檔案。 | □ 是  □ 否  □ 不適用 |  |  |
| 11 | 4.1.2.3.4.(2)檢查行動應用程式是否未檢出將敏感性資料儲存於系統日誌。 | □ 是  □ 否  □ 不適用 |  |  |
| 12 | 4.1.2.3.5.(1)檢查行動應用程式是否採用金鑰有效長度為 128 位元(含)以上之先進加密標準(AES)。 | □ 是  □ 否  □ 不適用 |  |  |
| 13 | 4.1.2.3.5.(2)檢查行動應用程式是否採用三重資料加密演算法(Triple DES)。 | □ 是  □ 否  □ 不適用 |  |  |
| 14 | 4.1.2.3.6.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。 | □ 是  □ 否  □ 不適用 |  |  |
| 15 | 4.1.2.3.7.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、身分驗證資訊或對稱式加解密演算法之金鑰。 | □ 是  □ 否  □ 不適用 |  |  |
| 16 | 4.1.2.4.1.(1)檢查行動應用程式是否採用 TLS 1.1(含)以上版本加密協定傳輸敏感性資料。 | □ 是  □ 否  □ 不適用 |  |  |
| 17 | 4.1.2.4.1.(2)檢查行動應用程式是否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)。 | □ 是  □ 否  □ 不適用 |  |  |
| 18 | 4.1.2.4.1.(3)檢查行動應用程式是否採用金鑰有效長度為128位元(含)以上之進階加密標準(AES)，或採用三重資料加密演算法(Triple DES)。 | □ 是  □ 否  □ 不適用 |  |  |
| 19 | 4.1.2.5.1.(1)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，是否於行動應用程式內或可信任之應用程式商店聲明。 | □ 是  □ 否  □ 不適用 |  |  |
| 20 | 4.1.2.5.1.(2)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，是否於行動應用程式內或可信任之應用程式商店取得使用者同意。 | □ 是  □ 否  □ 不適用 |  |  |
| 21 | 4.1.2.5.2.(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選項。 | □ 是  □ 否  □ 不適用 |  |  |
| 22 | 4.1.2.5.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 23 | 4.1.2.5.3.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。 | □ 是  □ 否  □ 不適用 |  |  |
| 24 | 4.1.3.1.1.檢查行動應用程式內於付費前，是否主動通知使用者，且資訊至少包含付費資源名稱、數量、金額及付費方式。 | □ 是  □ 否  □ 不適用 |  |  |
| 25 | 4.1.3.1.2.(1)檢查行動應用程式內於付費時，是否提供使用者拒絕付費之選項。 | □ 是  □ 否  □ 不適用 |  |  |
| 26 | 4.1.3.1.2.(2)檢查在使用者拒絕付費的情況下，行動應用程式是否未進行付費。 | □ 是  □ 否  □ 不適用 |  |  |
| 27 | 4.1.3.2.1.檢查行動應用程式於付費時，是否提供身分認證機制。 | □ 是  □ 否  □ 不適用 |  |  |
| 28 | 4.1.3.2.2.檢查行動應用程式於付費後，是否提供查詢交易紀錄之管道，且交易紀錄至少包含付費資源名稱、付費時間及付費金額之記錄。 | □ 是  □ 否  □ 不適用 |  |  |
| 29 | 4.1.4.1.1.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認證機制。 | □ 是  □ 否  □ 不適用 |  |  |
| 30 | 4.1.4.1.2.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。 | □ 是  □ 否  □ 不適用 |  |  |
| 31 | 4.1.4.2.1.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 32 | 4.1.4.2.1.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 33 | 4.1.4.2.1.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 34 | 4.1.4.2.2.(1)檢查行動應用程式是否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。 | □ 是  □ 否  □ 不適用 |  |  |
| 35 | 4.1.4.2.2.(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程式開發者所指定。 | □ 是  □ 否  □ 不適用 |  |  |
| 36 | 4.1.4.2.3.如行動應用程式使用安全加密傳輸協定，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、政府機關、企業簽發。 | □ 是  □ 否  □ 不適用 |  |  |
| 37 | 4.1.4.2.4.(1)如不符合檢測編號4.1.4.2.2.或 4.1.4.2.3.之技術要求，檢查行動應用程式是否未與伺服器進行連線與傳輸敏感性資料。 | □ 是  □ 否  □ 不適用 |  |  |
| 38 | 4.1.4.2.4.(2)檢查行動應用程式是否使用符合檢測編號4.1.4.2.2.與4.1.4.2.3.之憑證與伺服器進行連線與傳輸敏感性資料。 | □ 是  □ 否  □ 不適用 |  |  |
| 39 | 4.1.5.1.1.(5)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。 | □ 是  □ 否  □ 不適用 |  |  |
| 40 | 4.1.5.1.1.(6)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。 | □ 是  □ 否  □ 不適用 |  |  |
| 41 | 4.1.5.1.2.(11)檢查行動應用程式是否不存在已知安全性漏洞。 | □ 是  □ 否  □ 不適用 |  |  |
| 42 | 4.1.5.3.1.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。 | □ 是  □ 否  □ 不適用 |  |  |
| 43 | 4.1.5.4.1.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 44 | 4.1.5.4.1.(2)檢查行動應用程式是否針對使用者輸入字串驗證長度。 | □ 是  □ 否  □ 不適用 |  |  |
| 45 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 46 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 47 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 48 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 49 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 50 | 4.1.5.4.2.(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。 | □ 是  □ 否  □ 不適用 |  |  |
| 51 | 4.1.5.4.2.(7)檢查行動應用程式是否防護使用者輸入Intent Injection字串之設計。 | □ 是  □ 否  □ 不適用 |  |  |