經濟部工業局
行動應用App基本資安檢測基準V2.1(草案)
修訂說明

財團法人資訊工業策進會
資安科技研究所
2016年10月6日

修訂性質

- 「行動應用App 基本資安自主檢測制度」正式實施後，參酌各類活動辦理過程中，檢測實驗室、技術專家與業界回饋意見與建議，所進行之滾動式修正
  - 「能力試驗活動與檢測技術分享」 說明會(105/2/18)
  - 第 1 梯次能力試驗活動(105/3-105/5)
  - 台灣認證基金會(TAF)現場評鑑實作(105/5-105/8)
  - 「行動應用App基本資安自主檢測制度」推廣說明會(105/8/11)
  - 『行動應用App檢測基準V2.1初稿』專家座談會(105/9/26)
- 本次相關增修文件
  - 修訂文件
    - 行動應用App基本資安規範1.1（草案）
    - 行動應用App基本資安檢測基準V2.1（草案）
  - 新增參考文件
    - 行動應用App基本資安檢測參考步驟（Android版）V1.0

行動應用App基本資安規範1.1（草案）

修訂說明

行動應用App基本資安規範1.1（草案）
本次修訂範圍

1. 前言

3. 用語及定義

2. 適用範圍

非特定領域之行動應用程式

共通性行動應用程式

開發

4. 技術要求

4.1.1. 行動應用程式發布安全

4.1.2. 敏感性資料保護

4.1.3. 付費資源控管安全

4.1.4. 身分認證、授權與連線管理安全

4.1.5. 行動應用程式碼安全

使用

目標

用者雙贏局面

創造行動應用程式開發者與使

促進行動應用程式產業發展

提升行動應用程式安全與品質

5. 安全分類

參考資料

附錄

行動應用App基本資安規範1.1（草案）修訂概述

- 微調「用語及定義」
  - 於「 3 .3.敏感性資料」增加傳輸態樣，並配合修訂描述
  - 於「3.5.通行碼」原定義之語意較難理解，故修訂調整之
- 技術要求事項
  - 將同一段技術要求敘述中，含有2個不同之技術要求，修訂為不同技術要求
    - 「4.1.1.1. 行動應用程式發布」、「4.1.2.3.敏感性資料儲存」、「4.1.3.2.付費資源控管」、「4.1.4.2.連線管理機制」
    - 以「4.1.1.1. 行動應用程式發布」技術要求事項為例
      - 1.0版技術要求為單一敘述

        行動應用程式應於可信任來源之行動應用程式商店發布，且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
      - 1.1版(草案)修訂為2個不同之技術要求

        行動應用程式應於可信任來源之行動應用程式商店發布

        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
  - 技術要求事項總數於1.0版為29項，於1.1版(草案)增加為33項

行動應用App基本資安檢測基準V2.1（草案）

增修說明

行動應用App基本資安檢測基準V2.1（草案）本次修訂範圍

1.前言

3.用語及定義

2. 適用範圍

非特定領域之行動應用程式

「行動應用App基本資安規範」中所有類別

4.基本資安檢測基準

4.1.1 行動應用程式發布安全

4.1.2 敏感性資料保護

4.1.3 付費資源控管安全

4.1.4 身分認證、授權與連線管理安全

4.1.5 行動應用程式碼安全

5.檢測方式

目標

驗室檢測結果判定依據

提供行動應用App資安檢測實

遵循「行動應用App基本資安規範」

協助行動應用App開發者妥適

6.檢測結果與產出

參考資料、附錄

行動應用App基本資安檢測基準V2.1（草案）增修概述(1/3)

- 增修目標
  - 期使檢測基準更為具體、一致、明確
  - 降低因檢測基準內容訂定不明確，而造成不同檢測實驗室各自解讀，所產生檢測結果不一致之可能性
- 增修基本原則-**穩定**
  - 在V2.0文件架構下，進行小幅必要增修
  - 文字與格式勘誤
- 增訂部份
  - 用語及定義
    - 於檢測基準V2.1（草案）中，共新增7項
  - 檢測基準項目
    - 針對2項檢測基準，增訂檢測結果不適用之形成條件
    - 針對6項檢測基準，於備註欄新增相關解釋與說明

行動應用App基本資安檢測基準V2.1（草案）增修概述(2/3)

- 修訂部份
  - 用語及定義
    - 刪除「包括但不限於」中「但不限於」用語，避免於基準中使用開放性描述
    - 共修訂檢測基準V2.0中11項用語之定義
  - 「4.基本資安檢測基準」內文
    - 明確說明參考項目不要求進行實際檢測
    - 因「初級」檢測項目於檢測實務中仍需人工介入，故修訂此級別檢測方式與相關內容
  - 「4.1.行動應用程式基本資安檢測基準」檢測項目
    - 共計5項檢測項目，更具體修訂檢測結果之形成條件
    - 共計10項檢測項目，微幅修訂檢查事項內容
  - 格式及內容誤植
- 刪除部份
  - 「4.1.行動應用程式基本資安檢測基準」檢測項目
    - 共計2項檢測項目，由於檢查事項存在重複檢查情形，故刪除重複之檢查事項

行動應用App基本資安檢測基準V2.1（草案）增修概述(3/3)

- V2.1（草案）**檢測項目**與**總數**與V2.0**完全相同**

各檢測分級必要檢測項目 / 檢測分級 / 技術要求(規範)	初級	中級	高級
4.1.1. 行動應用程式發布安全	0	2	2
4.1.2. 敏感性資料保護	3	11	11
4.1.3. 付費資源控管安全	0	0	4
4.1.4. 身分認證、授權與連線管理安全	0	6	6
4.1.5. 行動應用程式碼安全	3	6	6
檢測項目總數	6	25	29

註：「規範」為「行動應用App基本資安規範」之簡稱

行動應用App基本資安檢測參考步驟（Android版）V1.0
新增說明

行動應用App基本資安檢測參考步驟（Android版）V1.0

- 本次新增提供Android版檢測參考步驟
- 編修目的主要提供檢測實驗室參考
  - 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，以期減少摸索學習時間
- 主要內容
  - 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
    - 檢測前須完成之程序、檢測環境準備或其他須先完成之檢測項目
  - 檢測步驟
    - 檢測進行之程序步驟

THANK YOU

行動應用App基本資安制度推動委員會網址：http://www.mas.org.tw
聯絡方式： appsecurity@iii.org.tw

行動應用App基本資安檢測基準V2.1（草案）檢查事項重要修訂內容說明(1/3)

- 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
  - 修訂說明

    對於開發者自行定義使用之檔案，因檢測實驗室難以自行判斷是否為暫存檔或自定義日誌檔，故將「暫存檔」或「自定義日誌檔」相關用語修訂為「冗餘檔案」
  - 修訂前檢查事項（V2.0）

    (1)檢查行動應用程式是否未檢出將敏感性資料儲存於網頁暫存檔或自定義暫存檔

    (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或自定義日誌
  - 修訂後檢查事項（V2.1草案初稿）

    (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

    (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

行動應用App基本資安檢測基準V2.1（草案）檢查事項重要修訂內容說明(2/3)

- 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(Session)
  - 修訂說明
    - 逾時之定義較籠統無一定標準，經工作團隊內部討論後，決議以檢查交談識別碼必須失效之時機為修訂方向，故修訂為登出失效
  - 修訂前檢查事項（V2.0）

    (3)檢查行動應用程式使用之交談識別碼是否具備逾時失效機制
  - 修訂後檢查事項（V2.1草案）

    (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

行動應用App基本資安檢測基準V2.1（草案）檢查事項重要修訂內容說明(3/3)

- 4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制
  - 修訂說明

    因「過濾」僅為前端注入攻擊防護機制之一種，故於檢查事項(1)至(7)修訂為檢查防護使用者輸入各種注入攻擊字串之設計
  - 修訂前檢查事項（V2.0）

    檢查行動應用程式是否過濾導致SQL Injection、JavaScript Injection、Command Injection、Local File Inclusion、XML Injection、Format String Injection及Intent Injection之字串
  - 修訂後檢查事項（V2.1草案初稿）

    檢查行動應用程式是否防護使用者輸入SQL Injection 、JavaScript Injection、Command Injection、Local File Inclusion、XML Injection、Format String Injection及Intent Injection字串之設計