

課程名稱：18696_行動應用 App 資安標章全攻略#3 - 基準說明篇 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- 適合族群：
 - 公部門與採購需求單位：需明確掌握驗收標準，確保外包開發 App 的資安合規性並降低專案風險。
 - App 開發商：適合開發團隊在交付前審視資安風險、內化合規標準，大幅降低重測與修正成本。
 - 檢測實驗室人員：協助提升檢測一致性與專業度，理解基準的防護精神。
- 能力門檻：[入門]~[普通]，適合對移動應用程式（Android / iOS）開發流程或軟體採購驗收有基本概念者。

2. 課程核心大綱與架構圖

- 章節架構：
 - 單元一：檢測基準與安全開發設計邏輯 — 介紹檢測基準分類（Level 1~3 及 F 選測類別）、等級防護目標與實驗室靜/動態檢測原理。
 - 單元二：常見開發缺點與防護對策剖析 — 剖析 8 大常見開發資安缺失（如硬編碼、明文儲存、Log 洩漏、不安全傳輸等）與對應修復範例。
 - 單元三：送測前自我評估 CheckList 與實務內化 — 拆解 7 大領域置評重點清單，將外部檢測基準轉化為前期開發規格。

3. 必備前置知識清單

- App 開發基礎：具備 Android（Java/Kotlin）或 iOS（Swift/Objective-C）基本開發與設定檔（Manifest, Info.plist）概念。
- 基礎資安與網路概念：瞭解基本 API 呼叫、HTTP/HTTPS 傳輸、憑證概念及常見攻擊（如注入攻擊、中間人攻擊）機制。

4. 專有名詞與概念辭典

- **靜態分析 (Static Analysis)**：針對 App 的 Binary Code 進行逆向工程，還原程式碼以檢查設定檔漏洞、硬編碼 Key 及第三方函式庫已知漏洞。
- **動態分析 (Dynamic Analysis)**：透過動態輸入、引數傳遞及 Proxy 攔截封包，檢視 App 在執行期間的真實行為（如日誌洩漏、TLS 加密與憑證繫結）。
- **憑證繫結 (Certificate Pinning)**：在 App 內配置伺服器公開金鑰或雜湊值，連線時比對目標伺服器身份，以有效抵禦中間人攻擊 (MITM)。
- **螢幕覆蓋攻擊 (Overlay Attack)**：攻擊者利用懸浮視窗權限在合法 App 上覆蓋偽造視窗以誘騙用戶操作，需透過觸控事件檢查（如 filterTouchesWhenObscured）防範。

5. 課程學習職能對照

- **對應職能名稱**：行動應用程式資安工程師 / 安全開發者 (DevSecOps) / 資安系統審查員
- **主要工作任務/能力指標**：
 - **安全架構規劃能力**：能在開發前期將資安基準導入規格書，依據功能劃分合規等級 (Level 1~3 及 F 類)。
 - **程式碼安全防護與修復能力**：能防範硬編碼、落實強加密儲存 (Keystore/Keychain)、Session 失效管理及防範注入攻擊。
 - **合規審查與自我檢測能力**：能運用 CheckList 於送測前進行靜/動態自評，提升首次送測通過率。