行動應用APP基本資安自主檢測制度推廣說明會

行動應用App安全開發指引簡介

報告人：協同計畫主持人 陳亮宏 專案顧問

中華民國資訊軟體協會

民國105年１０月６日

簡報大綱

- 指引編寫重點原則
- 指引章節架構介紹
- 問題與討論

行動應用App安全開發指引編目的

- 配合工業局「行動應用App基本資安規範」，從App開發安全設計角度切入，發展Android與iOS作業系統的行動應用App安全開發指引

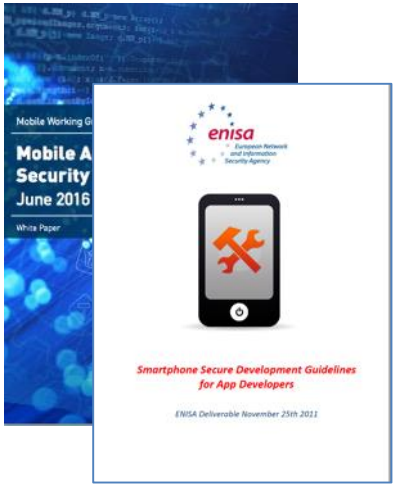
- 目的
  - 建立行動應用App開發人員可參考運用之安全開發指引及流程，說明Android與iOS開發常見之資安風險及安全設計開發實務，並透過各種檢測工具及方法，預防並及早發現安全漏洞，以符合「行動應用 App 基本資安規範」標準
  - 為了扶植新創 App 開發業者，特針對 App 開發人員辦理培訓課程，以提升 App 安全開發品質與產品競爭力

編寫重點原則

- 以經濟部工業局「行動應用App基本資安規範」為基礎架構
- 分析、比較及歸納各國行動應用App開發要點
- 界接「行動應用App基本資安規範」與「行動應用App基本資安檢測基準」
- 優先考慮Android與iOS內建安全規格與官方安全開發原則
- 廣泛參考開發社群、安全專家、學術論文有關安全實務
- 先定實務準則，再尋求技術解決方案

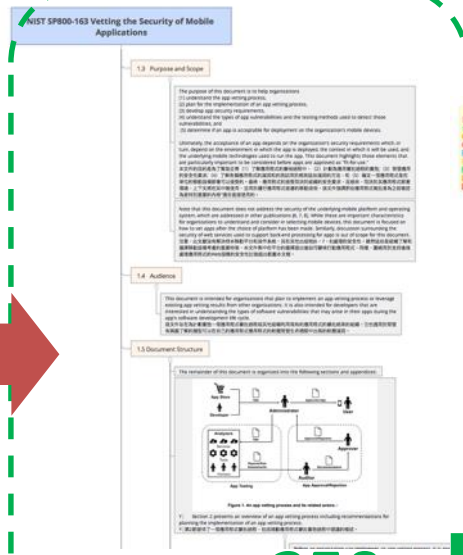
實務編製歷程

基本資安規範
基本資安檢測基準

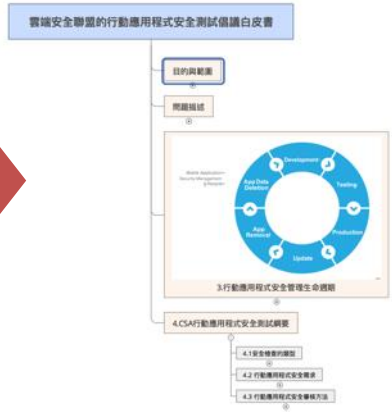


各國安全開發實務

萃取要點



250+



歸納要點

128

參考實務

Android/iOS
官方開發網

開發社群
/BLOG

行動應用App
安全開發指引

不安全 / 安全程式碼範例

行動應用APP安全開發指引架構簡介

國際最佳實務
- NIST
- CSA
- ENISA

行動應用App基本資安規範

行動應用APP安全開發指引

行動應用App基本檢測基準

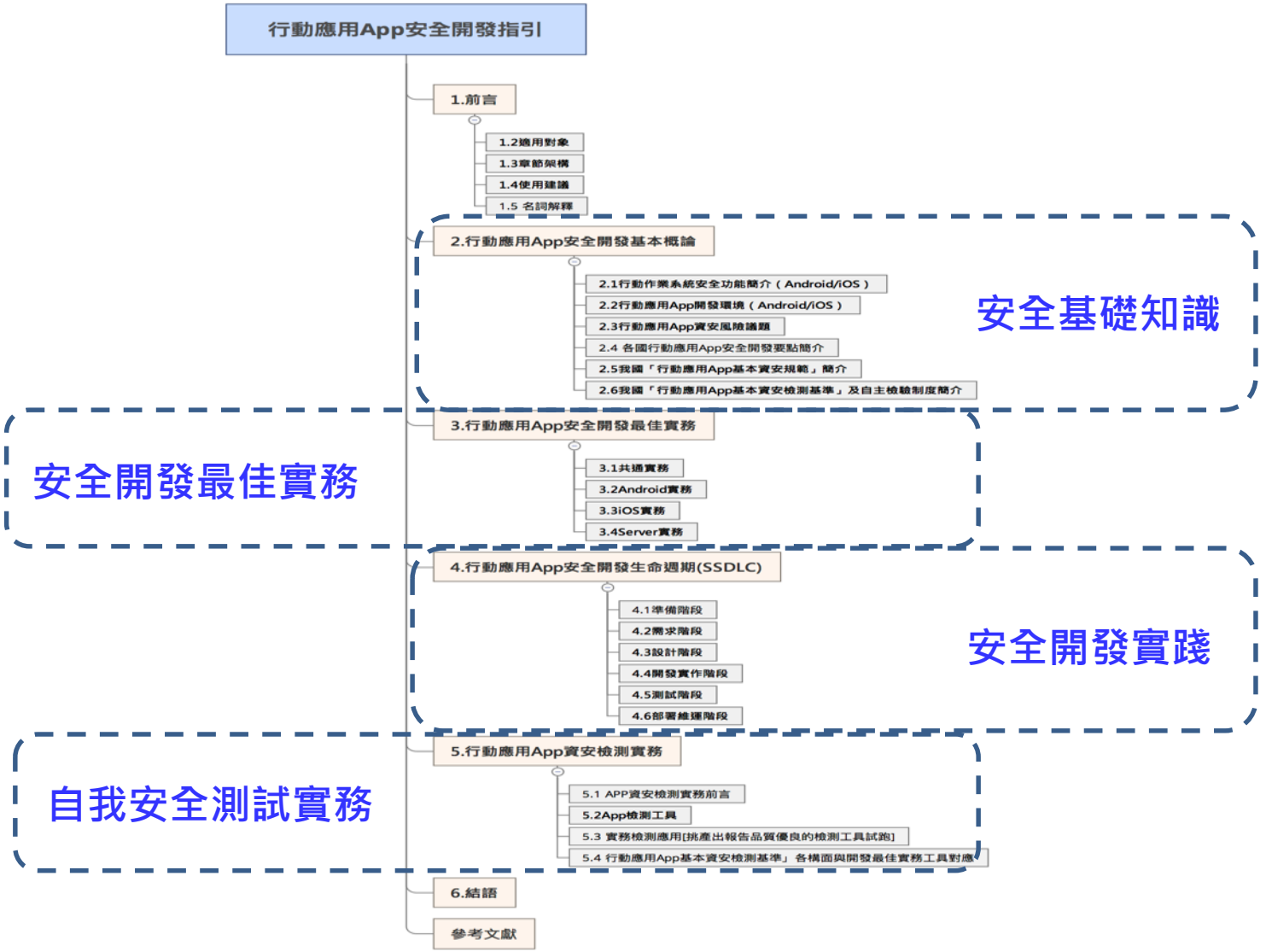
行動應用App基本資安自主檢測推動制度

第1章 前言

第2章 行動應用App安全開發概論	第3章 安全行動應用App開發最佳實務	第4章 行動應用App安全開發生命週期	第5章 行動應用App安全檢測實務
針對行動作業系統及安全功能進行簡介，使讀者在進入軟體開發安全主題前，能對相關議題有一定之知識基礎	說明安全開發實務上須注意之事項，並輔以不安全與安全程式碼範例，使能實際運用於相關開發作業	說明行動應用App安全開發生命週期(SSDLC)各階段之安全需求，包含需求、設計、開發實作、測試及部署維運	以檢測基準為基礎，提出免費或低成本檢測工具，以增強安全性。另可獲取第三方檢測認證標章MAS，更多一層保障

第6章 結語

章節架構


行動應用App安全開發指引
1.前言
1.2適用對象
1.3章節架構
1.4使用建議
1.5 名詞解釋
2.行動應用App安全開發基本概論
2.1行動作業系統安全功能簡介（Android/iOS）
2.2行動應用App開發環境（Android/iOS）
2.3行動應用App資安風險議題
2.4 各國行動應用App安全開發要點簡介
2.5我國「行動應用App基本資安規範」簡介
2.6我國「行動應用App基本資安檢測基準」及自主檢驗制度簡介
安全基礎知識
3.行動應用App安全開發最佳實務
3.1共通實務
3.2Android實務
3.3iOS實務
3.4Server實務
安全開發最佳實務
4.行動應用App安全開發生命週期(SSDLC)
4.1準備階段
4.2需求階段
4.3設計階段
4.4開發實作階段
4.5測試階段
4.6部署維運階段
安全開發實踐
5.行動應用App資安檢測實務
5.1 APP資安檢測實務前言
5.2App檢測工具
5.3 實務檢測應用[挑產出報告品質優良的檢測工具試跑]
5.4 行動應用App基本資安檢測基準」各構面與開發最佳實務工具對應
自我安全測試實務
6.結語
參考文獻

使用建議說明（1/2）

- 「專案經理」、「系統分析/設計人員」、「開發人員」、「測試/品管人員」、「系統管理員」及「資安人員」各角色閱讀本指引文字說明。

角色 章節	PM	SA	SD	Android PG	iOS PG	TEST/QA	MIS	IS
SSDLC	全程	需求	設計	開發實作	開發實作	測試	部署維運	全程
Ch.1	★	★	★	★	★	★	★	★
2.1	★	★	★	★	★	☆	☆	★
2.2	★	★	★	☆	☆	☆	★	★☆
2.3	★	★	★	★	★	☆	★	★
2.4	★	☆	☆	☆	☆	☆	☆	★☆
2.5	★	☆	☆	☆	☆	☆	☆	★
2.6	★	☆	☆	☆	☆	★	☆	★
3.1	★☆	★☆	★☆	★☆	★☆	★☆	☆	★☆
3.2	★☆	★☆	★	★	☆	★☆	☆	★☆
3.3	★☆	★☆	★	☆	★	★☆	☆	★☆
3.4	★☆	★☆	★	☆	☆	★☆	★	★☆

圖例：★：必要 ★☆：部份必要 ☆：選擇性

使用建議說明（2/2）

角色 章節	PM	SA	SD	Android PG	iOS PG	TEST/QA	MIS	IS
SSDLC	全程	需求	設計	開發實作	開發實作	測試	部署維運	全程
4.1	★	★	★	★	★	★	★	★
4.2	★	★	☆	☆	☆	☆	☆	★
4.3	★	☆	★	☆	☆	☆	☆	★
4.4	★	☆	☆	★	★	☆	☆	★
4.5	★	☆	☆	☆	☆	★	☆	★
4.6	★	☆	☆	☆	☆	☆	★	★
5.1	★☆	☆	☆	☆	☆	★	☆	☆
5.2	★☆	☆	☆	☆	☆	★	☆	☆
5.3	★☆	☆	☆	☆	☆	★	☆	☆
5.4	★☆	☆	☆	☆	☆	★	☆	☆
Ch.6	★	★	★	★	★	★	★	★

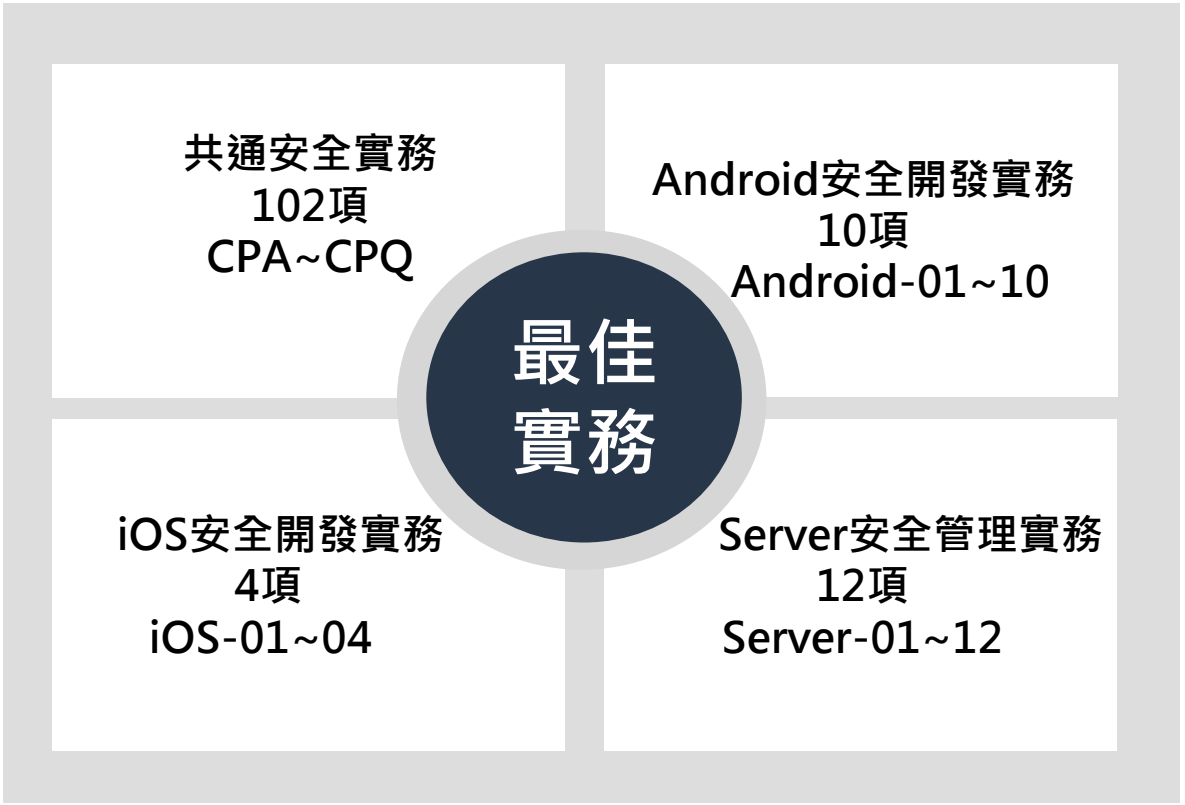
圖例：★：必要 ★☆：部份必要 ☆：選擇性

行動應用App安全開發最佳實務

依據我國經濟部工業局「行動應用App基本資安規範」及「行動應用App基本資安檢測基準」及了中國大陸、歐盟、日本、美國及CSA行動應用App安全開發實務要點。

4
個實務類別

128
項實務準則



App安全開發實務分類

節編號	資訊安全技術要求事項（基本資安規範編號）	安全分類			安全開發實務(編碼)	合計項次
		一	二	三		
3.1.1	A.行動應用程式發布(4.1.1.1.)	V	V	V	CPA-01~CPA-05	5
3.1.2	B.行動應用程式更新(4.1.1.2.)	V	V	V	CPB-01~CPB-03	3
3.1.3	C.行動應用程式安全性問題回報(4.1.1.3.)	V	V	V	CPC-01~CPC-02	2
3.1.4	D.敏感性資料蒐集(4.1.2.1.)	V	V	V	CPD-01~CPD-06	6
3.1.5	E.敏感性資料利用(4.1.2.2.)	V	V	V	CPE-01~CPE-07	7
3.1.6 3.3	F.敏感性資料儲存(4.1.2.3.)	V	V	V	CPF-01~CPF-18 iOS-01~ iOS-02	20
3.1.7 3.3	G.敏感性資料傳輸 (4.1.2.4.)		V	V	CPG-01~CPG-03 iOS-04	4
3.1.8	H.敏感性資料分享(4.1.2.5.)	V	V	V	CPH-01~CPH03	3
3.1.9	I.敏感性資料刪除(4.1.2.6.)	V	V	V	CPI-01~CPI06	6
3.1.10	J.付費資源使用(4.1.3.1.)			V	CPJ-01~CPJ-03	3
3.1.11	K.付費資源控管(4.1.3.2.)			V	CPK-01~CPK-06	6
3.1.12	L.使用者身分認證與授權(4.1.4.1.)		V	V	CPL-01~CPL-08	8
3.1.13	M.連線管理機制(4.1.4.2.)		V	V	CPM-01~CPM-08	8
3.1.14 3.2 3.3	N.防範惡意程式碼與避免資訊安全漏洞(4.1.5.1.)	V	V	V	CPN-01~CPN-07 Android-01~Android-08 iOS-03	16
3.1.15	O.行動應用程式完整性(4.1.5.2.)			V	CPO-01~CPO-05	5
3.1.16	P.函式庫引用安全(4.1.5.3.)	V	V	V	CPP-01~CPP-02	2
3.1.17 3.2	Q.使用者輸入驗證(4.1.5.4.)	V	V	V	CPQ-01~CPQ-10 Android-09~Android-10	12
3.4	作業系統強化與記錄留存	V	V	V	Server-01~Server-02	2
3.4	網頁服務安全	V	V	V	Server-03~Server-08	6
3.4	網路安全防護	V	V	V	Server-09~Server-12	4
					合計(項)	128

通過MAS必要實務
(共37項)

節編號	基本資安檢要求事項 (基本資安規範編號)	安全分類			安全開發實務(編碼)	合計 項次
		一	二	三		
3.1.1	A.行動應用程式發布(4.1.1.1.)	V	V	V	CPA-01	1
3.1.2	B.行動應用程式更新(4.1.1.2.)	V	V	V	N/A	0
3.1.3	C.行動應用程式安全性問題回報(4.1.1.3.)	V	V	V	CPC-01	1
3.1.4	D.敏感性資料蒐集(4.1.2.1.)	V	V	V	CPD-05,CPD-06	2
3.1.5	E.敏感性資料利用(4.1.2.2.)	V	V	V	N/A	0
3.1.6 3.3	F.敏感性資料儲存(4.1.2.3.)	V	V	V	CPF-01,CPF-02,CPF-05,CPF-07, CPF-09,CPF-10,CPF-12	7
3.1.7	G.敏感性資料傳輸 (4.1.2.4.)		V	V	N/A	0
3.1.8	H.敏感性資料分享(4.1.2.5.)	V	V	V	CPH-01,CPH02	2
3.1.9	I.敏感性資料刪除(4.1.2.6.)	V	V	V	N/A	0
3.1.10	J.付費資源使用(4.1.3.1.)			V	CPJ-01	1
3.1.11	K.付費資源控管(4.1.3.2.)			V	CPK-01,CPK-03	2
3.1.12	L.使用者身分認證與授權(4.1.4.1.)		V	V	CPL-01	1
3.1.13	M.連線管理機制(4.1.4.2.)		V	V	CPM-01,CPM-02,CPM-03,CPM-04, CPM-05,CPM-06,CPM-07	7
3.1.14	N.防範惡意程式碼與避免資訊安全漏洞 (4.1.5.1.)	V	V	V	CPN-01,CPN-02,CPN-03,CPN-04	4
3.1.15	O.行動應用程式完整性(4.1.5.2.)			V	N/A	0
3.1.16	P.函式庫引用安全(4.1.5.3.)	V	V	V	CPP-01	1
3.1.17 3.2	Q.使用者輸入驗證(4.1.5.4.)	V	V	V	CPQ-01,CPQ-05,CPQ-06,CPQ-07, CPQ-08,CPQ-09 Android-09,Android-10	8
3.4	作業系統強化與記錄留存	V	V	V	N/A	0
3.4	網頁服務安全	V	V	V	N/A	0
3.4	網路安全防護	V	V	V	N/A	0
					合計	37

實務案例1 - 行動應用程式發布(A)

CPA-01 於行動應用程式商店提供及應用程式內實作提供隱私權政策說明連結，說明欲存取之敏感性資料、行動裝置資源及宣告權限用途。

簡介

- 使用者下載安裝行動應用App時，除了功能及價格因素，還會考量隱私的議題。
- 事前規劃並撰寫此行動應用App的隱私權政策。
- 可參考Center for Democracy & Technology (CDT)的行動應用程式開發最佳實務的隱私權宣告範本(https://www.cdt.org/files/pdfs/Apps%20Best%20Practices%20v%20beta.pdf) 。

隱私權政策的參考範本如下：

- 隱私權保護政策的適用範圍
- 個人資料的蒐集、處理及利用方式
- 資料之保護
- 網站對外的相關連結
- 與第三人共用個人資料之政策
- Cookie之使用
- 隱私權保護政策之修正

開發生命週期	需求階段、開發實作階段、部署維運階段		
不安全程式碼範例	N/A	安全程式碼範例	N/A
行動應用App基本資安規範	4.1.1.1	行動應用App基本資安檢測基準	4.1.1.1.2

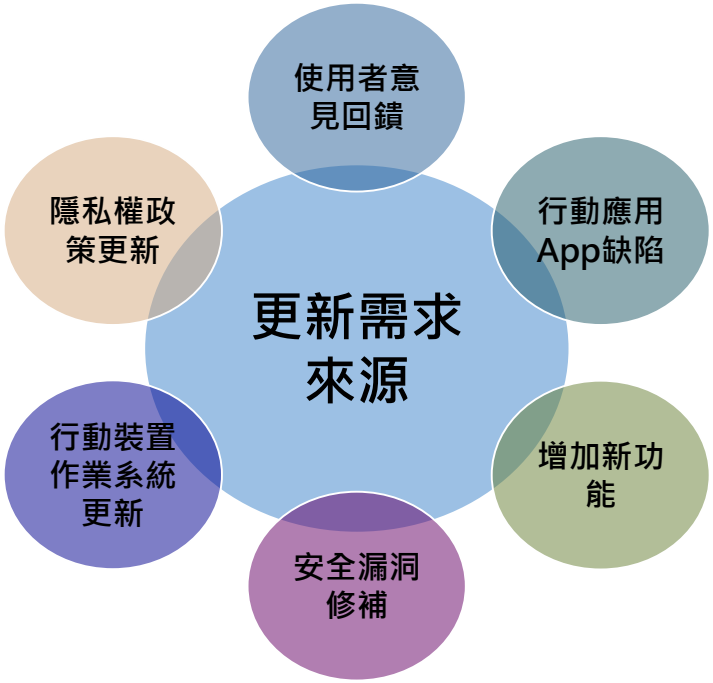
實務案例2 - 行動應用程式更新(B)

CPB-01 行動應用App應提供功能性與安全性更新，以因應新功能加入、發現漏洞及平台安全性提升之需求。

簡介

使用者自平台付費或免費取得行動應用APP後，在其持續使用的過程中，行動應用App可能會因為一些因素有更新需求。

- 可使用電子郵件或App的提示功能告知使用者更新資訊。
- 開發人員應隨時注意重大更新事項，尤其與安全或隱私有關之議題。



開發生命週期	部署維運階段		
不安全程式碼範例	N/A	安全程式碼範例	N/A
行動應用App基本資安規範	4.1.1.2	行動應用App基本資安檢測基準	N/A

實務案例3 - 敏感性資料利用(E)

CPE-01 不要使用設備或與其他App共享持久性敏感資料作為使用者識別碼，如設備ID，最好採用隨機產生識別碼(參考CPM-02)，並採用相同的資料最小化權限原則應用在行動應用App的Session ID及HTTP Session ID/cookies等。

簡介

- 為保持使用者良好體驗，使用者不需持續的進行身分認證，通常以儲存Session ID/Cookies在使用者端用來讓Server端識別使用者身分用，故攻擊者只要獲取使用者Session ID/Cookies就可以使用者身分進入伺服器竊取。

  常用的攻擊為猜測(Session Prediction)、連線劫持(Session Hijacking)及詐取固定(Session Fixation)。

- 系統設計及開發人員在Server端實作網頁應用程式時，最好在每次登入時更換隨機產生或是可變量的Session ID(參考CPM-02)，並設定逾時就清除session ID。

- 在行動應用App的本地端的Session ID也要限制被其他App存取，以最小化權限原則設計實作，傳送至伺服器端應使用TLS連線加密，或將Session ID加密傳送，至server端再解密，不要將 Session ID 使用 URL (GET) 以明文方式來傳遞。

開發生命週期	設計階段、開發實作階段		
不安全程式碼範例	N/A	安全程式碼範例	N/A
行動應用App基本資安規範	4.1.2.2	行動應用App基本資安檢測基準	N/A

實務案例4 - 敏感性資料儲存(F)

CPF-01 行動應用App如需要儲存敏感性資料需依CPD-02規劃於可信任之應用程式商店或行動應用程式內聲明。

簡介

- 行動應用App如需要儲存”敏感性資料”參考CPA-01將行動應用App需要儲存敏感性資料於Google Play及App Store及行動應用App的隱私權政策中聲明。

敏感性資料(Sensitive Data)
指依使用者行為或行動App之運作，建立或儲存於行動裝置及其附屬 儲存媒介之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限 於個人資料、通行碼、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。

開發生命週期	設計階段		
不安全程式碼範例	N/A	安全程式碼範例	N/A
行動應用App基本資安規範	4.1.2.3	行動應用App基本資安檢測基準	4.1.2.3.1

實務案例5 - 敏感性資料傳輸(G)

CPG-01 行動應用App傳輸敏感性資料應規劃並實作傳輸全程全時使用TLS 1.1以上加密，維護敏感性資料機密性及完整性。

簡介

- 新的Web應用協定HTTP/2和SPDY並不支援SSL，只支援TLS。
- Google所有公共服務的加密都是使用TLS，故如果要整合Google的一些功能，只能使用TLS。
- PCI DSS規範SSL在2016年6月30日之後不得繼續使用。

Apple將在2017年1月強制所有iOS App開始使用ATS(App Transport Security, 支援TLS v1.2)，參考iOS-04。

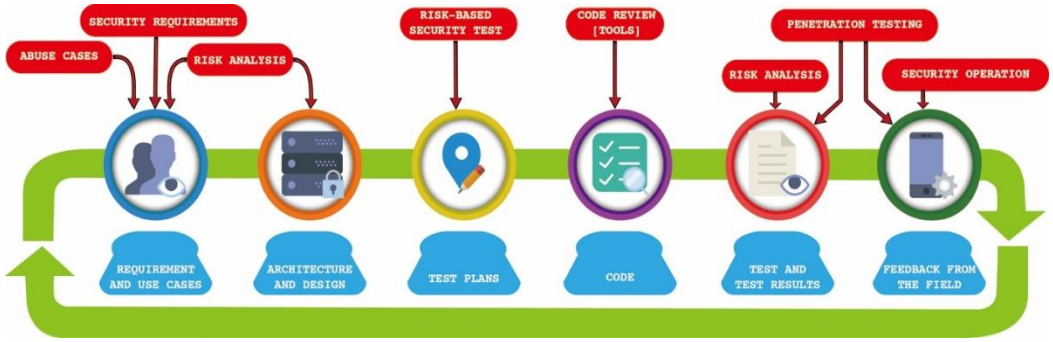
Android支援標準TLS實作，在官方開發人員網站有完整的概念及實作介紹，並包含實例及常見問題。

開發生命週期	設計階段		
不安全程式碼範例	N/A	安全程式碼範例	N/A
行動應用App基本資安規範	4.1.2.3	行動應用App基本資安檢測基準	4.1.2.3.1

行動應用App安全開發生命週期

- 常見安全開發生命週期(Secure Software Development Lifecycle, SSDLC)方法論
  - Cigital的Touchpoint
  - Microsoft的Security Development Lifecycle(SDL)
  - OWASP的Security Assurance Maturity Model(SAMM)

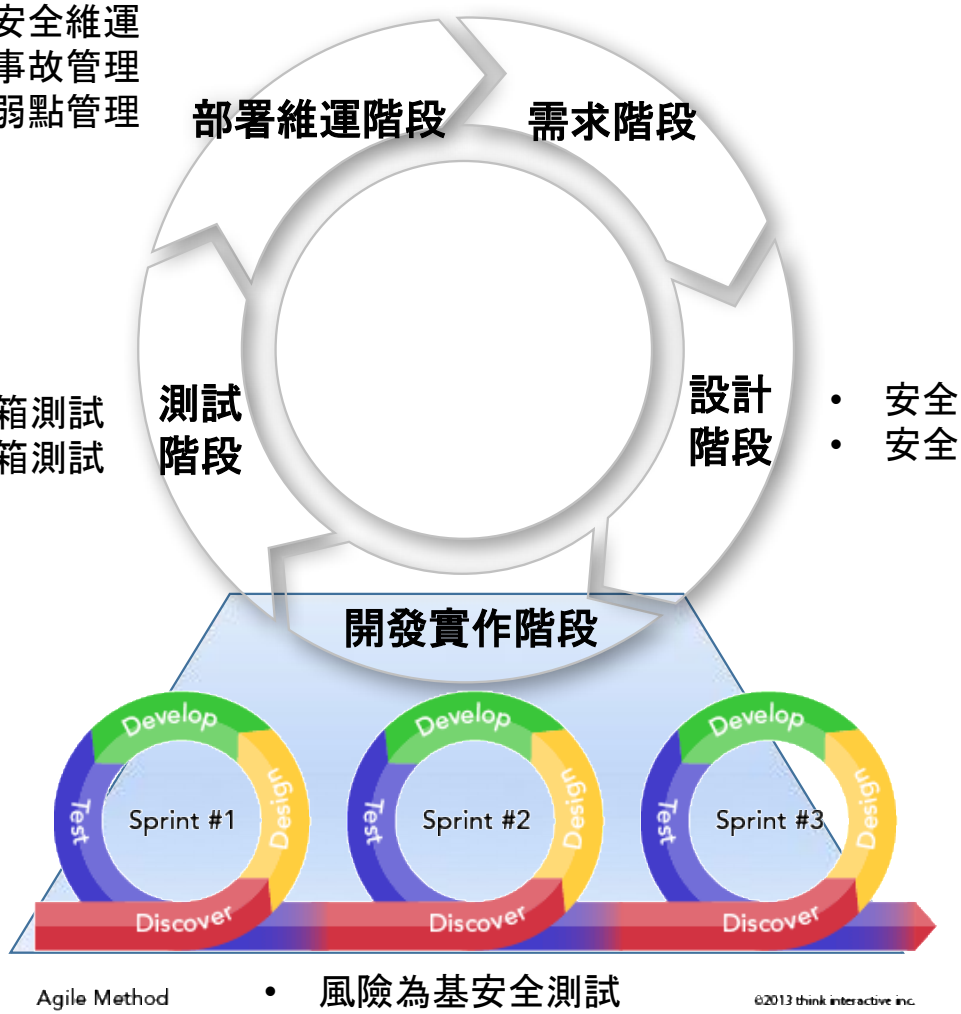
方法論比較摘述請詳見：附件1「安全軟體開發生命週期方法論比較」



資料來源：www.cigital.com

SSDLC在敏捷開發應用

- 安全維運
- 事故管理
- 弱點管理

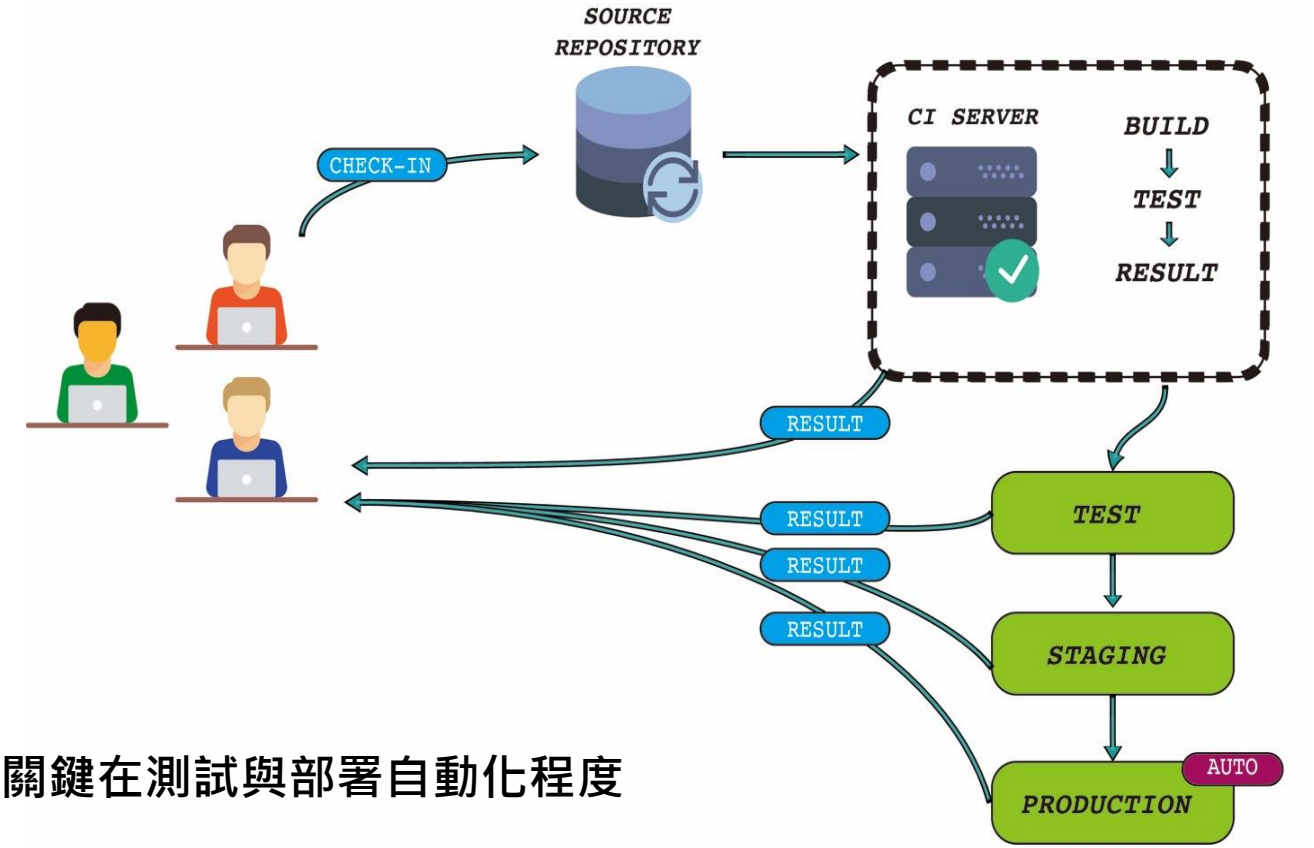


- 白箱測試
- 黑箱測試

- 安全架構與設計
- 安全測試計畫

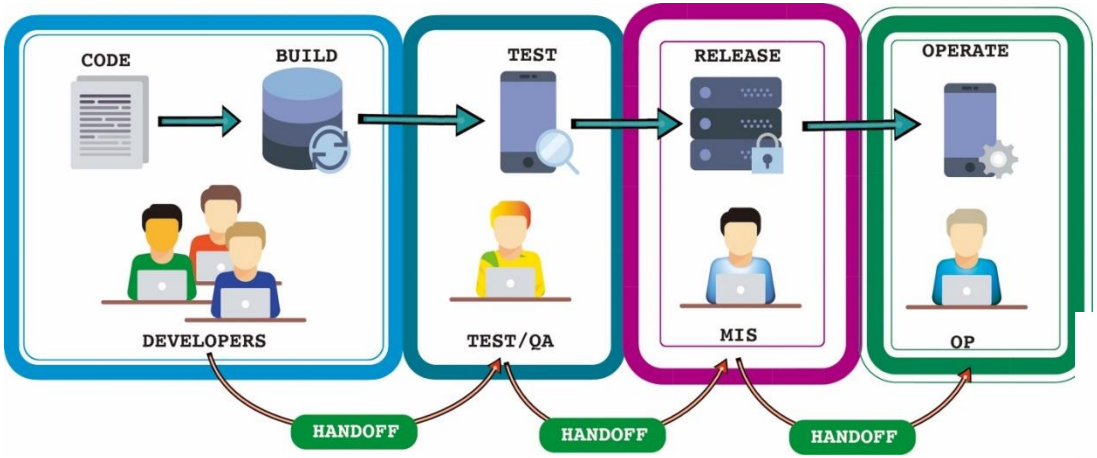
- 風險為基安全測試
- 自動化程式碼覆核

DevOps持續整合 / 交付 / 部署



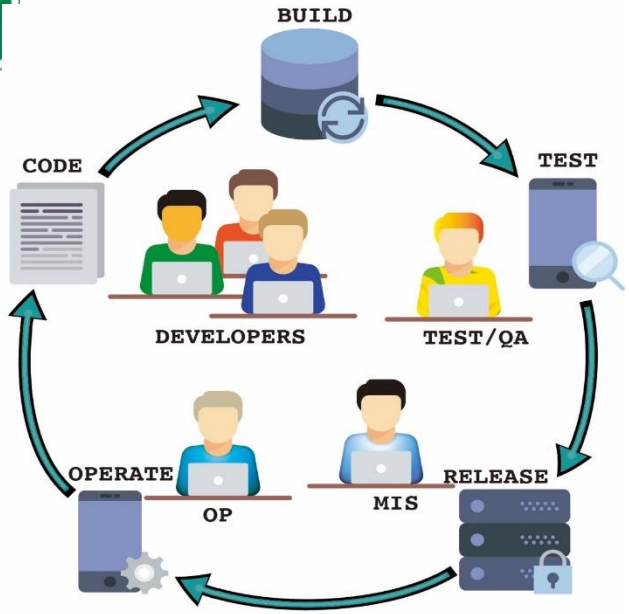
關鍵在測試與部署自動化程度

傳統開發/測試/上線/維運與DevOps的對比流程



資料來源：www.mindtheproduct.com

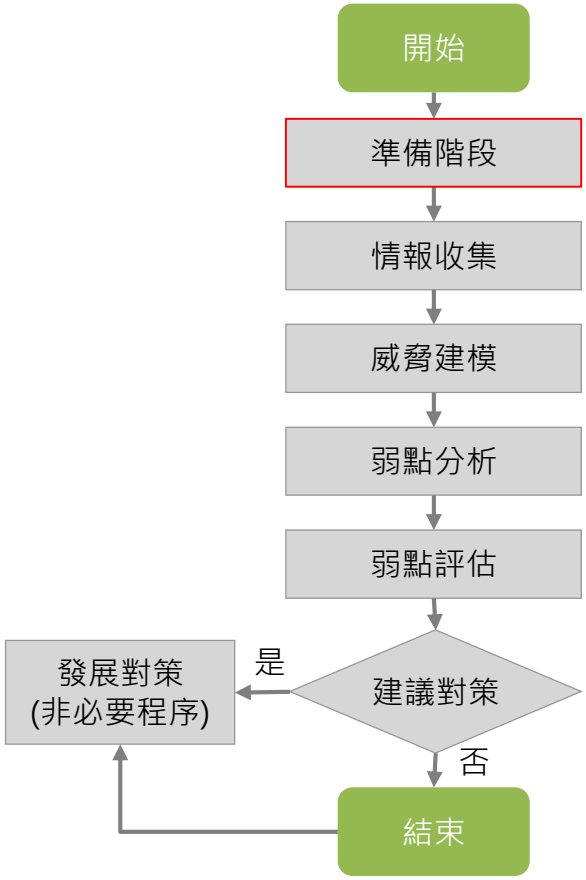
對比傳統流程最大的差異就是各角色以專案為單位整合成為單一團隊，持續整合、持續交付及持續部署不間斷，藉由自動化工具與DevOps運作團隊文化，加速App產品化的效率。



DevOps開發/測試/上線/維運流程

階段1：準備階段(Preparation)

- 主要任務
  - 建置一個單純且不受干擾之測試環境，並可操控與掌握各項控制因子，諸如越獄(JB/root)與否、系統平台、系統版本、App介面、行動裝置管理等等，可作為檢測時成為考量因素操控使用。
- 檢測前
  - 應提供檢測者關於該App之開發事項或心得等，有助於檢測者更有效率的完成檢測，並且有系統地進行檢測流程步驟及完善檢測紀錄與報告。
- 檢測過程
  - 應考量攻擊者可能的攻擊角度與手法，透過App內外部、網路或裝置存取以及可能的檢測方法與工具等。



App檢測核心流程

資料來源：The OWASP Foundation

Checklist增加必要 / 選項

- MAS:基本檢測基準必要項目
- 選用□：非基本檢測基準必要項目

附件 4 行動應用 App 開發實作階段檢核表

App 名稱　　版次：　　覆核人員：

A.安全活動

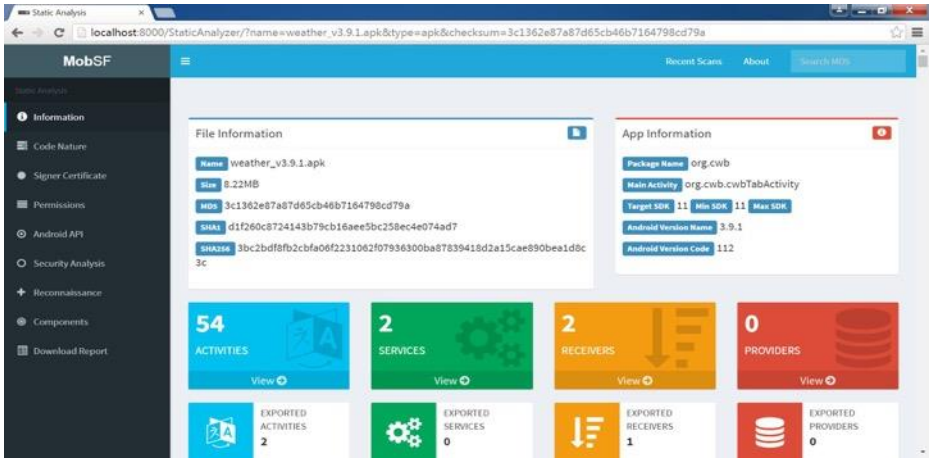
項 次	檢 核 內 容	檢 核 情 形	符 合 情 形	檢 核 人
1	自動化原始碼工具檢測		□是□否	
2	人工檢測		□是□否	
3			□是□否	

B.安全開發實務(**MAS**:基本資安檢測項目; 選用□:非 MAS 檢測項目)

項次	檢 核 內 容	檢 核 情 形	符合情形	檢 核 人
1 **MAS**	CPA-01:於行動應用程式商店提供及應用程式內實作提供隱私權政策說明連結，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 選用□	CPA-02:行動應用 App 實際權限應與於行動平台商店提供及 App 內宣告終端使用者授權約定(EULAs)、應用程式說明、程式內部通知及與 CPA-01 於欲存取之敏感性資料、行動智慧裝置資源及宣告權限用途一致。		□是□否 □不適用	
3 選用□	CPA-03:應於行動應用 App 上架前確保內部軟體品質流程及版本控制均已實作完成。		□是□否 □不適用	
4 **MAS**	CPD-06:應依 CPD-03 實作行動應用 App 存取敏感性資料權限，不要授與過度蒐集不必要敏		□是□否 □不適用	

自行檢測工具

Santoku



MobSF

Snoop-it

結論

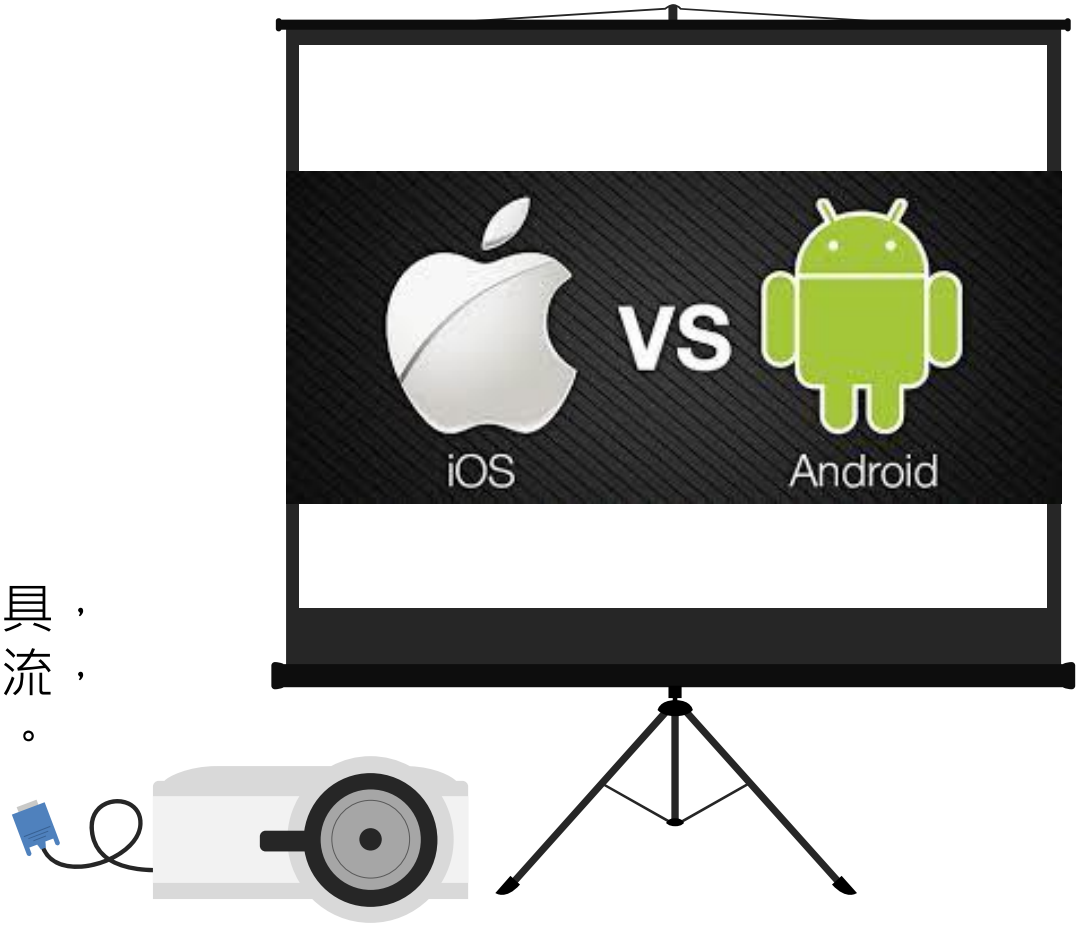
- 行動應用App，再度呼應「安全是被設計出來，不是被駭出來」
- 持續遵守「使用者意願」、「最小權限」及「密不透風」的三大安全原則，需要有一個安全開發流程 - 安全軟體開發生命週期(SSDLC)
- 協助開發者藉由安全需求、安全設計、實作安全、測試安全及上線安全開發不會濫取使用者資料、能對抗惡意攻擊的行動應用App，是本指引的期望
- 「行動應用App安全開發指引」V1.0只是一個起點，除了透過業界、學界審查而完備，未來期望能透過開發者社群的力量發現本指引不足之處，回饋實務建議以利修訂

行動應用APP安全開發培訓課程(免費)

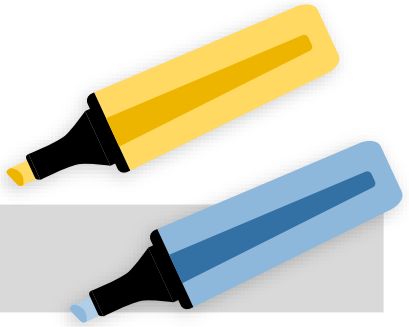
場	課程班別		時間	名額	上課地點
1	台北	Android 基礎概念班	10/19(三) AM	110 人	集思北科大 201會議室(β貝塔廳)
2		Android 設計實務班	10/19(三) PM	60 人	集思北科大 204會議室(θ西特廳)
3		iOS 基礎概念班	10/21(五) AM	110 人	集思北科大 201會議室(β貝塔廳)
4		iOS 設計實務班	10/21(五) PM	60 人	集思北科大 204會議室(θ西特廳)
5	台中	Android 基礎概念與實務入門班	10/26(三) AM	60 人	工研院台中學習中心 402會議室 (中科工商大樓)
6		iOS 基礎概念與實務入門班	10/26(三) PM	60 人	
7	高雄	Android 基礎概念與實務入門班	10/28(五) AM	60 人	高雄蓮潭國際會館 101會議室
8		iOS 基礎概念與實務入門班	10/28(五) PM	60 人	

誰需要來上這門課？

- 適用對象
  - 行動應用App開發
    - 專案經理(PM)、
    - 系統分析人員(SA)、
    - 系統設計人員(SD)、
    - 程式設計師(PG)、
    - 軟體檢測人員(QA)、
    - 資訊維運人員(MIS)
  - 本課程採理論及實務兼具，學員可於課堂上互相交流，講師亦會分享相關經驗。



你可以在課程中獲得什麼？



1	了解行動應用App的各種資安風險來源及威脅
2	了解各國對行動應用App的安全開發重視程度
3	了解Android與iOS作業系統的App開發平台和開發工具的潛在安全議題
4	了解Android與iOS行動裝置與作業系統的安全架構及開發時的注意事項
5	認識行動應用App安全開發生命週期(SSDLC)與方法論
6	了解開發生命週期各階段之安全需求及常見程式碼撰寫的缺失與漏洞，並獲得一份安全性檢核表
7	了解有哪些行動應用APP基本資安檢測項目(分初級、中級與高級)
8	了解有哪些可供 App 開發者自我檢測之行動應用App資安檢測弱點掃描方式及工具
9	以實務案例及實際操作強化所學的理論

想知道更詳細的情形嗎？

好奇有哪些生動的上課內容

提供課程簡報下載

等不及課程，想要搶先閱讀指引完整內容

正式公告於網站

想要先空出時間，以便參加課程

台北(4場) 10/19、10/21

台中(2場) 10/26

高雄(2場) 10/28

問題與討論