# 行動應用App資安檢測服務

安華聯網科技股份有限公司

資安檢測實驗室

June 27, 2017

# 大綱

- 公司簡介
- 實驗室介紹
- App檢測服務介紹
- 安華優勢

# 公司簡介

- 成立於2014年10月
- 服務項目
  - 資安檢測服務
  - 資安產品開發
  - 資安顧問服務

# Onward Security Profile

公司使命:

創造更安全的連網環境

公司願景:

全球產品資安檢測

領導品牌

公司核心價值:

專業、信賴

品質、創新

## Advantages and Experiences

**40** CVE-ID Discovered

**52** Security Certificate

**3** ISLA Awards



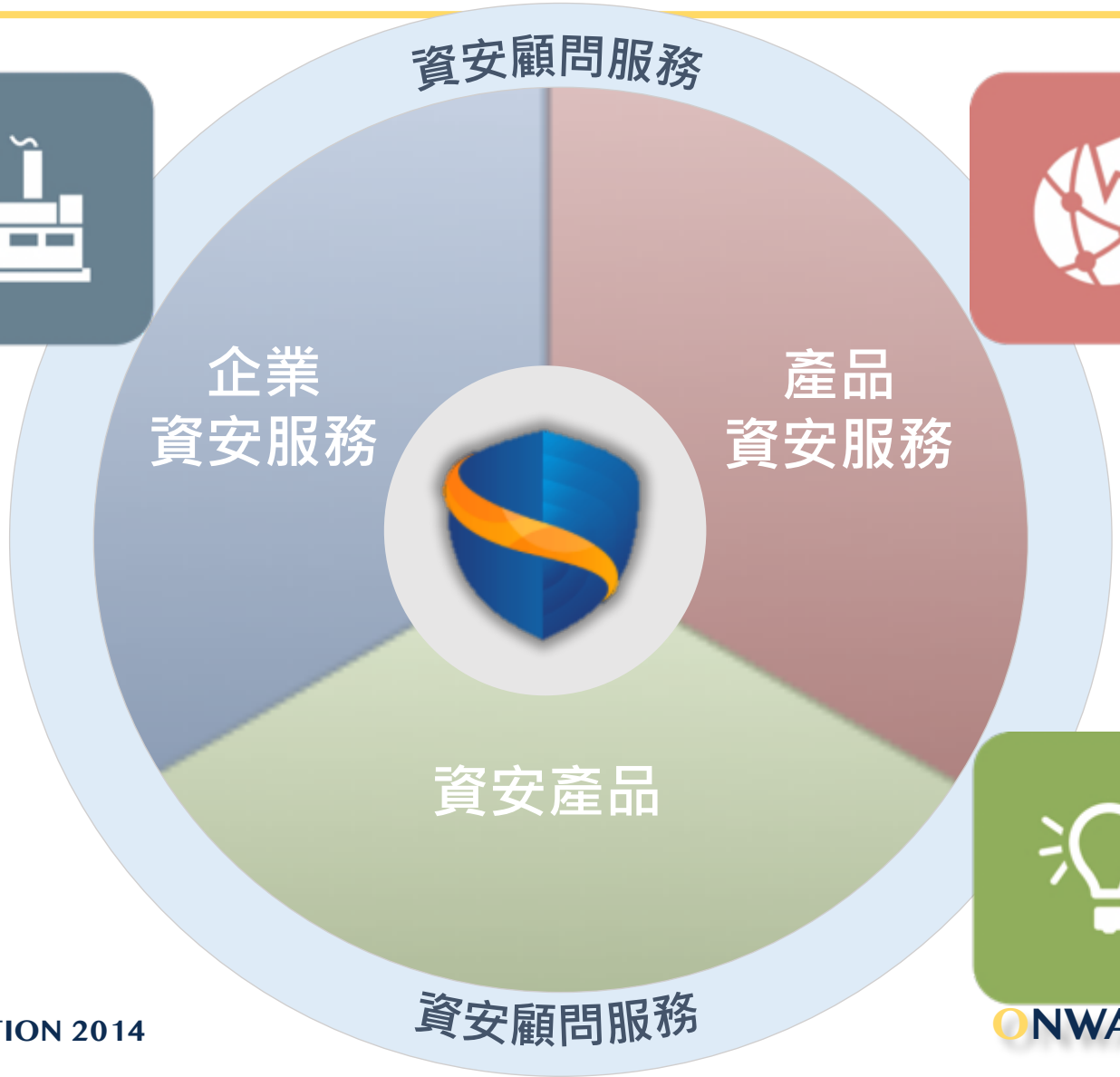
**First**

Provide Connected devices security testing lab in Taiwan with accreditation of ISO/IEC 17025

**Only One**

Testing report have been accepted by European telecom operator and U.S FTC in Taiwan

# Core Business




網路資安檢測

應用程式資安檢測

無線網路資安檢測

端點資安檢測

電子郵件社交工程

關鍵基礎設施資安檢測

嵌入式系統資安檢測

手機與App資安檢測

IOT資安檢測

車聯網資安檢測

HERCULES SECURITY PLATFORM

# Main Customers

Netcom, ICS/SCADA, Mobile manufacturer：22

Financial, Aviation industry, SI：32

# 大綱

- 公司簡介
- 實驗室介紹
- App檢測服務介紹
- 安華優勢

# ISO 17025 認可資安檢測實驗室

證書編號：L3102-170124

財團法人全國認證基金會
Taiwan Accreditation Foundation

## 認 證 證 書

茲證明

**安華聯網科技股份有限公司**

**資安檢測實驗室**

新北市新店區民權路 98 號 5 樓之 1

**為本會認證之實驗室**

認 證 依 據：ISO/IEC 17025：2005
認 證 編 號：3102
初次認證日期：一百零五年一月二十八日
認證有效期間：一百零五年一月二十八日至一百零八年一月二十七日止
認 證 範 圍：測試領域，如續頁
特定服務計畫：行動應用 APP 基本資安檢測實驗室認證服務計畫

董事長
王聰麟

中華民國一百零六年一月二十四日

本認證證書與續頁分開使用無效　第 1 頁，共 2 頁

證書編號：L3102-170124

財團法人全國認證基金會
Taiwan Accreditation Foundation

認證編號：3102
實驗室主管：劉作仁

◤ 20. 07　資訊與通訊
行動應用程式
E027
1.功能安全性測試
2.連網認證安全性測試
3.交易安全性測試
行動應用 App 基本資安檢測基準

報告簽署人:劉作仁

◤ 20. 21　資訊與通訊
嵌入式系統
E013　設備資安檢測
NIST SP800-115

報告簽署人:劉作仁

**行動應用 APP 基本資安檢測實驗室認證服務計畫**
◤ 20. 07　資訊與通訊
行動應用程式
E027
1.功能安全性測試
2.連網認證安全性測試
3.交易安全性測試
行動應用 APP 基本資安檢測基準

報告簽署人:劉作仁

(以下空白)

本認證證書與續頁分開使用無效　第 2 頁，共 2 頁

# 資安檢測實驗室能力

## ~2014

- Host, Web, Network
- Mobile, Apps
- Embedded, ICS/SCADA

## 2015

- IoT, Wireless
  - Smart Home, Wi-Fi



## 2016

- Smart Meter, Radio Frequency(RF)
  - IEC 61850
  - Bluetooth, Zigbee, Z-Wave, 2G/3G
- Automobile CAN bus


# 實驗室團隊專業證照

(ISC)²®

CSSLP®

SSCP®

EC-Council

E|CSA™ EC-Council Certified Security Analyst

C|EH™ Certified Ethical Hacker

C|HFI™ Computer Hacking Forensic INVESTIGATOR

GIAC Global Information Assurance Certification www.giac.org

GWAPT GIAC Web App Pen Tester

GPEN GIAC Certified Penetration Tester

GREM GIAC Reverse Engineering Malware

# 檢測軟體清單

## 靜態分析工具

| 名稱 | 版本 | 說明 |
|---|---|---|
| Apktool | 4.0 | Android反編譯工具 |
| QARK | 0.7.4 | 原始碼檢測工具 |
| Dex2jar | 0.0.7.8 | 轉換dex檔案至jar檔案 |
| JD-GUI | 0.3.6 | 將jar檔反組譯成java原始檔 |
| Otools | 4.0 | ipa反組譯工具 |
| iNalyzer | 5 | ipa分析工具 |
| Class-dump-z | 0.2 | ipa分析工具 |
| Sqlite3 | 3 | 開啟android資料庫 |
| maas | 3.2 | 自行開發自動化工具 |

## 動態測試工具

| 名稱 | 版本 | 說明 |
|---|---|---|
| Dozer | 2.3.4 | Andriod應用程式內模擬攻擊 |
| OSMonitor | 3.5 | 系統資訊擷取工具 |
| Android-vts | 6 | 簡易Android弱點分析 |
| Droidbox | 4.1.1 | Android Activity追蹤程式 |
| Cycript | N/A | 腳本工具，用於測試函數 |
| BigBoss Tools | N/A | 網路檢測工具 |
| Burp suite | 1.6.28 | 可攔截及修改網路請求 |
| iFunbox | 3.0 | iOS手機連線工具 |
| Adb | 1.0.32 | Android手機連線工具 |
| WireShark | 1.12.8 | 網路封包側錄軟體 |

# 大綱

- 公司簡介
- 實驗室介紹
- App檢測服務介紹
- 安華優勢

# 專案執行流程

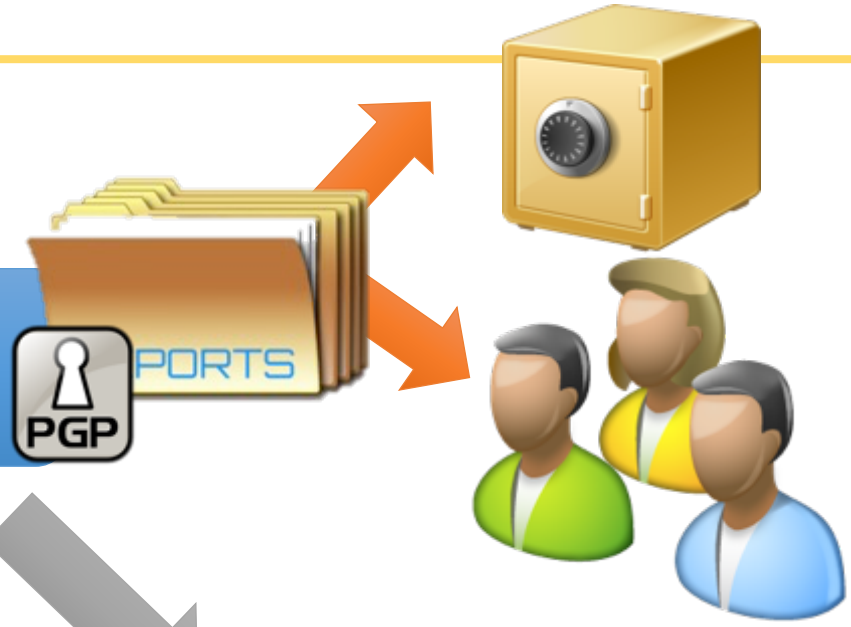
委託測試

客戶送件流程

執行測試

測試時程約 5 ~ 8 個工作天
並提供顧問諮詢服務

報告撰寫



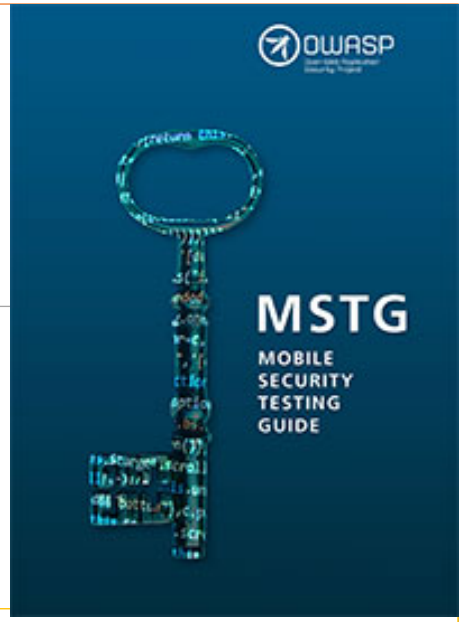

結束測試

保留資料一段時間後刪除

# 行動應用App檢測服務內容

Onward Advanced Testing Service

OWASP Mobile Testing Guide




行動應用App基本資安檢測基準


行動應用資安聯盟

# 常見未通過檢測項目統計

| 檢測編號 | 檢測項目名稱 | 未通過數量 | 不合格率 |
|---|---|---|---|
| **4.1.5.4.2** | **行動應用程式注入攻擊防護機制** | **21** | **57%** |
| **4.1.2.4.1** | **行動應用程式敏感性資料傳輸** | **17** | **45%** |
| **4.1.5.4.1** | **行動應用程式使用者輸入檢查** | **17** | **45%** |
| 4.1.2.3.7 | 行動應用程式敏感性資料硬碼(HardCode) | 16 | 42% |
| 4.1.2.1.1 | 行動應用程式敏感性資料蒐集聲明 | 13 | 38% |
| 4.1.2.3.2 | 行動應用程式提供使用者拒絕敏感性資料儲存機制 | 13 | 34% |
| 4.1.2.3.4 | 行動應用程式敏感性資料儲存限制 | 13 | 34% |

# 檢測報告格式 (1/3)

安華聯網科技股份有限公司

ONWARD SECURITY
SECURE YOUR OWN WORLD !

行動裝置應用程式資安檢測結果報告
Mobile Application Security Testing Report

| | | | |
|---|---|---|---|
| 委託單位名稱 | [VENDORNAME] | | |
| 委託單位地址 | [VendorAddress] | | |
| App 名稱 | [AppName] | 報告編號 | [ReportNo] |
| 測試件編號 | [SampleNo] | 檢測期間 | [StartDate] ~ [EndDate] |
| 報告日期 | [HardwareVersion] | 報告版本 | v1.0 |

| 報告核准人 | | 報告簽署人 | | 檢測人員 | |
|---|---|---|---|---|---|
| 簽章 | | 簽章 | | 簽章 | |

報告聲明：1.本檢測結果報告僅對委託單位所送樣品負責
2.本報告未經安華聯網書面許可不得部份複製本報告內容

資安檢測實驗室
Security Assessment Laboratory

23141 新北市新店區民權路 98 號 5 樓之 1
Rm 1,5F. ,No.98 ,Minquan Rd.,Xindian Dist.,New Taipei City 23141, Taiwan (R.O.C.)

- 測試目標資訊
  - Package Name
  - Version
  - SHA1 Hash
- 測試項目清單
  - 項目清單
  - 測試結果
- 弱點結果
  - 漏洞名稱、風險等級
  - 漏洞資訊、修補方式、測試過程

# 檢測報告格式 (2/3)

| 項次 | 安全級別 | 測試項目 | 測試結果 |
|---|---|---|---|
| T17 | 高級 | 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 | PASS |
| T18 | 高級 | 4.1.3.2.2.行動應用程式應記錄使用之付費資源與時間 | FAIL |
| T19 | 中級 | 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 | PASS |
| T20 | 中級 | 4.1.4.1.2.行動應用程式應依使用者身分授權 | PASS |
| T21 | 中級 | 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 | FAIL |
| T22 | 中級 | 4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性 | FAIL |
| T23 | 中級 | 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 | FAIL |
| T24 | 中級 | 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 | FAIL |
| T25 | 初級 | 4.1.5.1.1.行動應用程式應避免含有惡意程式碼 | FAIL |
| T26 | 中級 | 4.1.5.1.2.行動應用程式應避免資訊安全漏洞 | FAIL |

| 漏洞編號 | 漏洞名稱 | 漏洞數量 | 小計 | 總計 |
|---|---|---|---|---|
| OnSec-VUZ-MST-106-XX007 | 行動應用程式交談識別碼規則性 | 1 | 4 (33%) | |
| OnSec-VUZ-MST-106-XX008 | 行動應用程式伺服器憑證有效性 | 1 | | |
| OnSec-VUZ-MST-106-XX009 | 行動應用程式伺服器憑證簽發來源 | 1 | | |
| OnSec-VUZ-MST-106-XX010 | 行動應用程式連線安全 | 1 | | |
| OnSec-VUZ-MST-106-XX011 | 行動應用程式惡意程式碼 | 1 | 2 (17%) | |
| OnSec-VUZ-MST-106-XX012 | 行動應用程式資訊安全漏洞 | 1 | | |

# 檢測報告格式 (3/3)

**2.1.2. 行動應用程式問題回報**

測試項目資訊

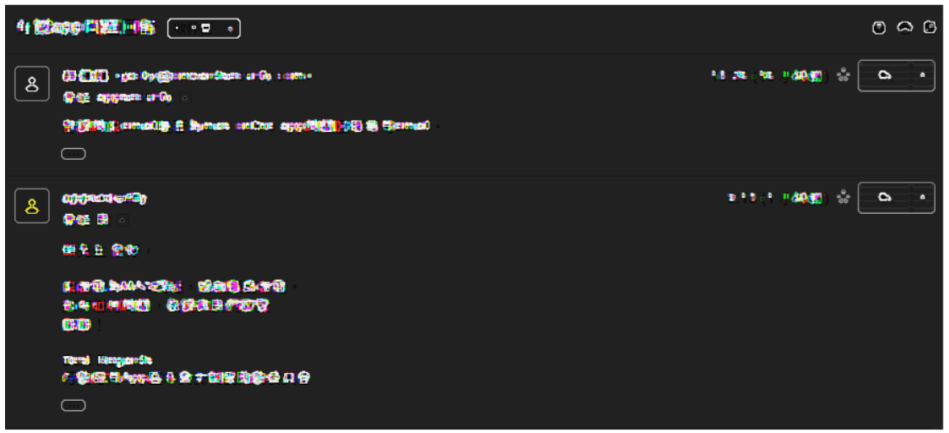
檢測編號： 4.1.1.3.1

檢測基準： 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

檢測結果： 符合

驗證過程

行動應用程式中有提供聯絡 email,實際寫信過去有得到回覆，如下圖：



**2.2.1. 行動應用程式敏感性資料蒐集聲明**

測試項目資訊

檢測編號： 4.1.2.1.1

檢測基準： 檢查行動應用程式所有蒐集之敏感性資料，是否皆已於行動應用程式內聲明並取得使用者同意

**檢測結果： 不符合**

驗證過程

執行註冊功能發現註冊前後皆無宣告相關相關敏感性資料蒐集聲明提示

# 大綱

- 公司簡介
- 實驗室介紹
- App檢測服務介紹
- 安華優勢

# 一站式服務

**測試**

依據客戶需求執行指定檢測方法論

**評估**

協助客戶送測前進行自我評估


**輔導**

協助客戶導入安全程式開發流程

## 技術窗口

- 劉作仁 協理
- 電子郵件：opp@onwardsecurity.com
- 聯絡電話：(02)2218-5020 #239

## 業務窗口

- 陳佳韻 副理
- 電子郵件：june@onwardsecurity.com
- 聯絡電話：(02)2218-5020 #222