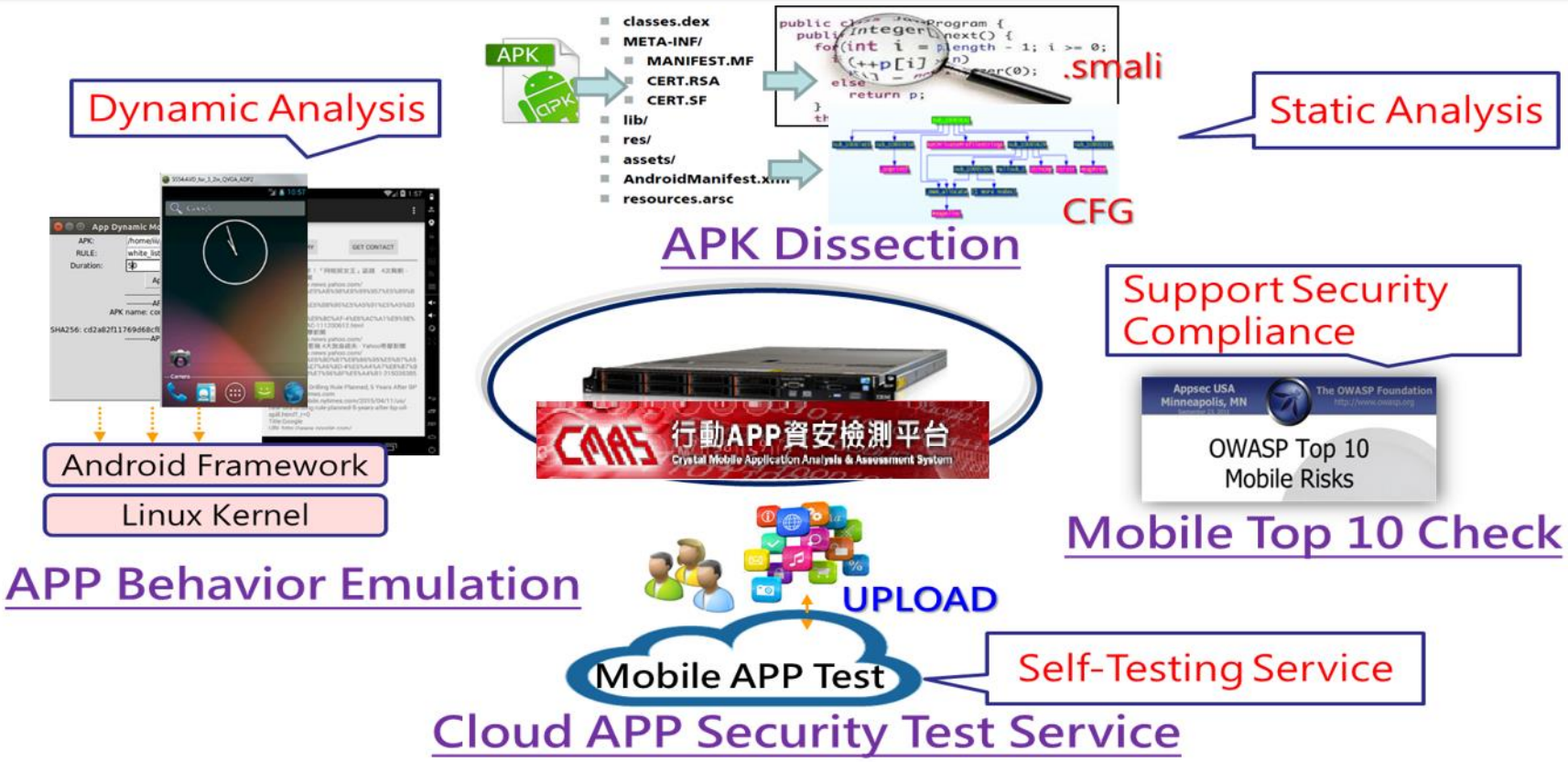
Crystal Mobile Application Analysis & Assessment System

行動應用APP基本資安檢測
初級自動化檢測工具說明

資安科技研究所

行動APP資安檢測平台 CMAS

- 結合靜態與動態檢測技術，還原APP原始執行內容，提供雲端APP資安黑箱檢測服務
- 檢測項目支援OWASP行動安全風險與工業局APP資安規範

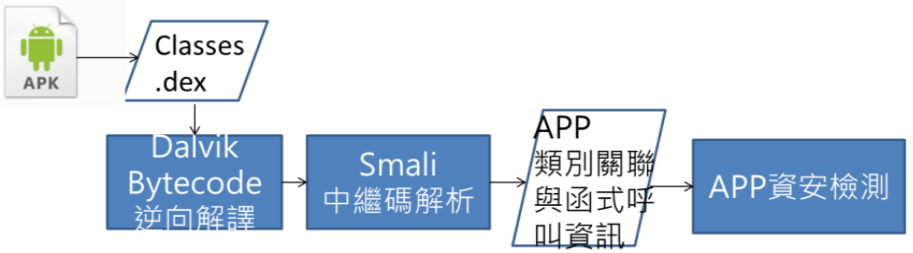


技術特色：Dalvik Bytecode反組譯分析

APP資安靜態檢測技術

技術特色：

- 解析Dalvik組語(smali)萃取APP執行內容
- 追蹤暫存器參數，取得API呼叫細節




```
.line 120
.local v2, skeySpec:Ljavax/crypto/spec/SecretKeySpec;
const-string v5, "AES/ECB/ZeroBytePadding"

invoke-static {v5}, Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

move-result-object v5

move-object v3, v5
```

Smali 中繼碼

```
Cipher cipher = Cipher.getInstance("AES/ECB/ZeroBytePadding");
import android.inputmethodservice.InputMethodService;

public class LatinIME extends InputMethodService{
    public LatinIME() {
        super();
    }
```

取得APP Java原始碼API 函式呼叫及參數內容

檢測結果比較

- 知名檢測工具偶有失敗的情況
- CMAS填補該缺漏解析APP完整內容

測試樣本： Juiker揪科

比較工具	解析率
JDGui,Dex2Jar	96.5%
Enjarify	98%
CMAS	100%

```
.method private declared-synchronized C()V
    .locals 2

    .prologue
    .line 1816
    monitor-enter p0

    :try_start_0
    iget-object v0, p0, Lorg/itri/ac;->V:La
```

解譯Dalvik組語，檢測完整APP內容

```
/* Error */
private void C()
{
  // Byte code:
  //   0: aload_0
  //   1: monitorenter
  //   2: aload_0
  //   3: getfield 349
  //   6: ifnonnull +32
```

APP解析失敗

技術特色：APP動態行為分析

APP資安動態檢測技術

技術特色：

- Android API層級監控，精準地擷取其傳入的參數值與回傳值
- 系統kernel層級監控，針對於透過JNI呼叫之C函式庫進行追蹤


```
{ "class_name":"javax.crypto.Cipher",
  "result":{ "algorithm":"DES\/CBC\/PKCS5Padding " },
  "method":"getInstance "                    }
{ "class_name":"javax.crypto.Cipher",
  "ObjectRef":"javax.crypto.Cipher@218f4710",
  "KeyValue":"Uh9bc4X76qQ=\n",
  "Opmode":1,"method":"init",
  "KeyAlgorithm":"DES"
```

Android APIs

```
open("/sdcard/mobile.txt",
  O_WRONLY|O_CREAT|O_TRUNC|O_LARGEFILE, 0600) = 50
write(50, "Hello, Bob Hello, Android!
  A129061757 0972206760 a18499@hotmail.com\n", 69) = 69
```

Kernel APIs

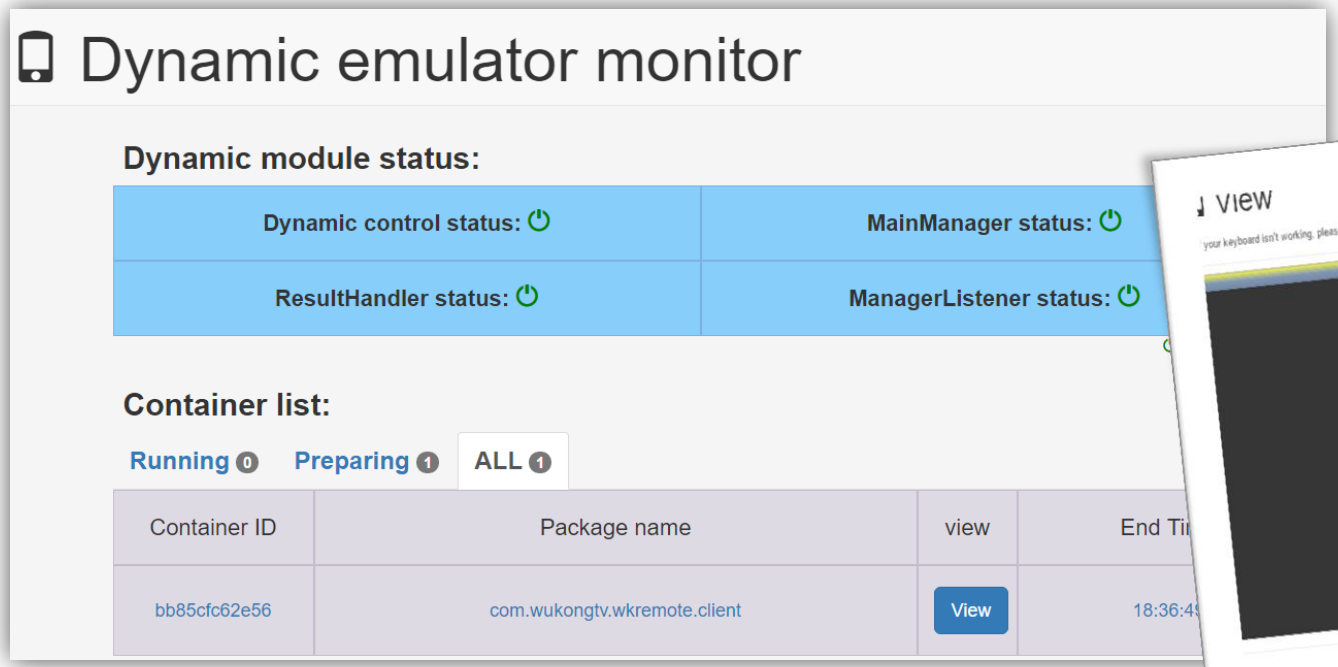
檢測技術比較

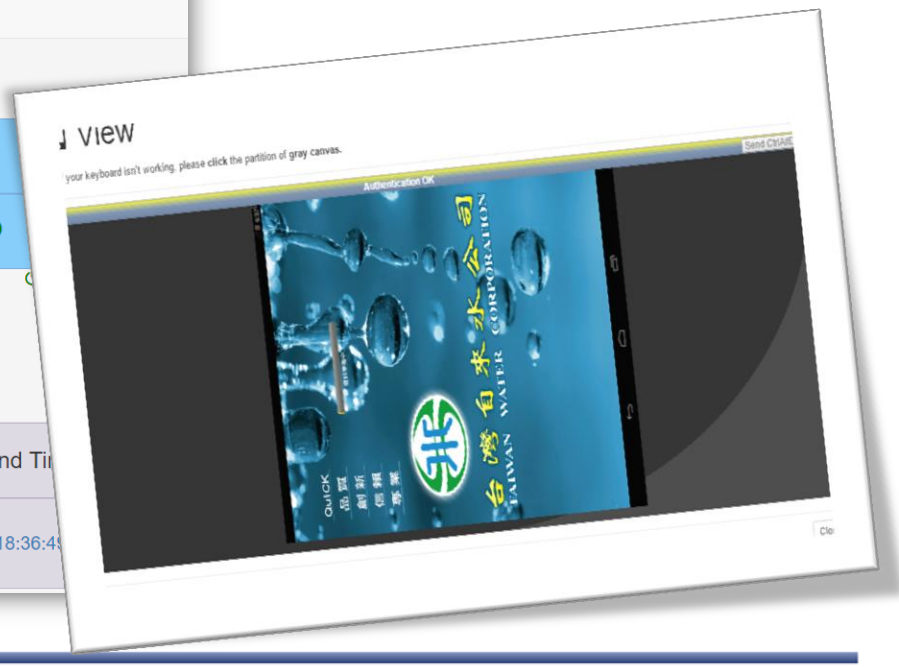
- 與常見的APP動態分析工具比較，本技術提供更全面的監控機制

比較工具	系統kernel層級監控	Android 層級監控
cuckoo-droid	X	O
Droidbox (APIMonitor)	X	O
Android-Hooker	X	O
CMAS	O	O

技術特色：半自動操作分析

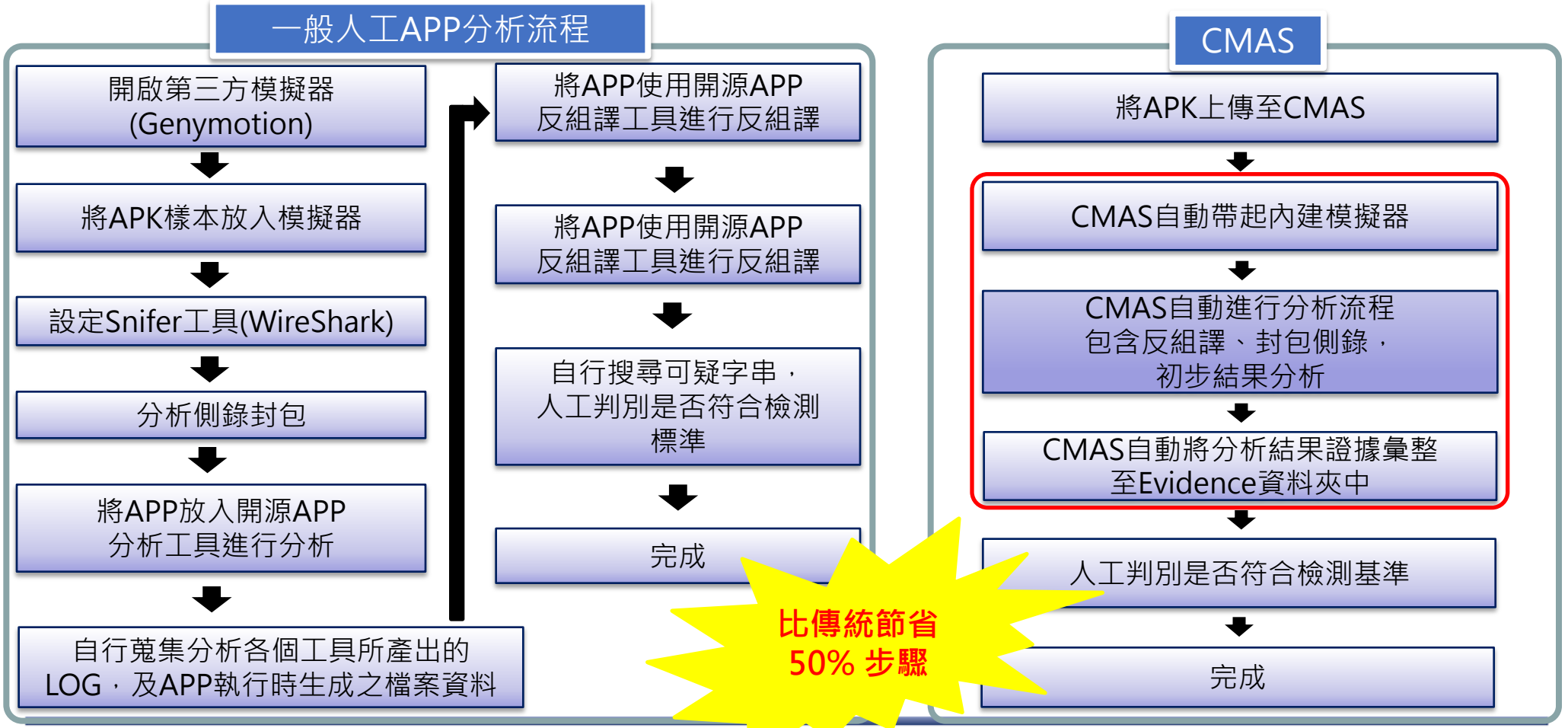
- 提供網頁介面操作Android模擬器中帶起的行動App
- 可實際操作應用程式之功能，更精確的記錄行為及網路行為
  - 登入帳密、敏感性資料輸入
  - 觸發付費功能
  - 滲透測試





系統優勢

- 提供自動化分析/半自動化操作分析
- 自動化粹析弱點風險
- 提供模擬器介面操作
- 提供完整證據資料
- 節省前置作業及蒐集證據等時間



系統規格-檢測報表及證據下載

- 提供 Android APP資安檢測，包含：

Submission Summary
App details: MD5, SHA-1, SHA-256, size, package name

Permission Check
Check suspicious permission requested by the app

App Activity/Receiver /Service Check
Check unsafe objects (activity, receiver, service) of the app

JNI Library Check
Check if the APP is using suspicious JNI library

Packed Protection Check
Identify APP packing information

App Security Analysis
Detected security risks (if any) and their full description

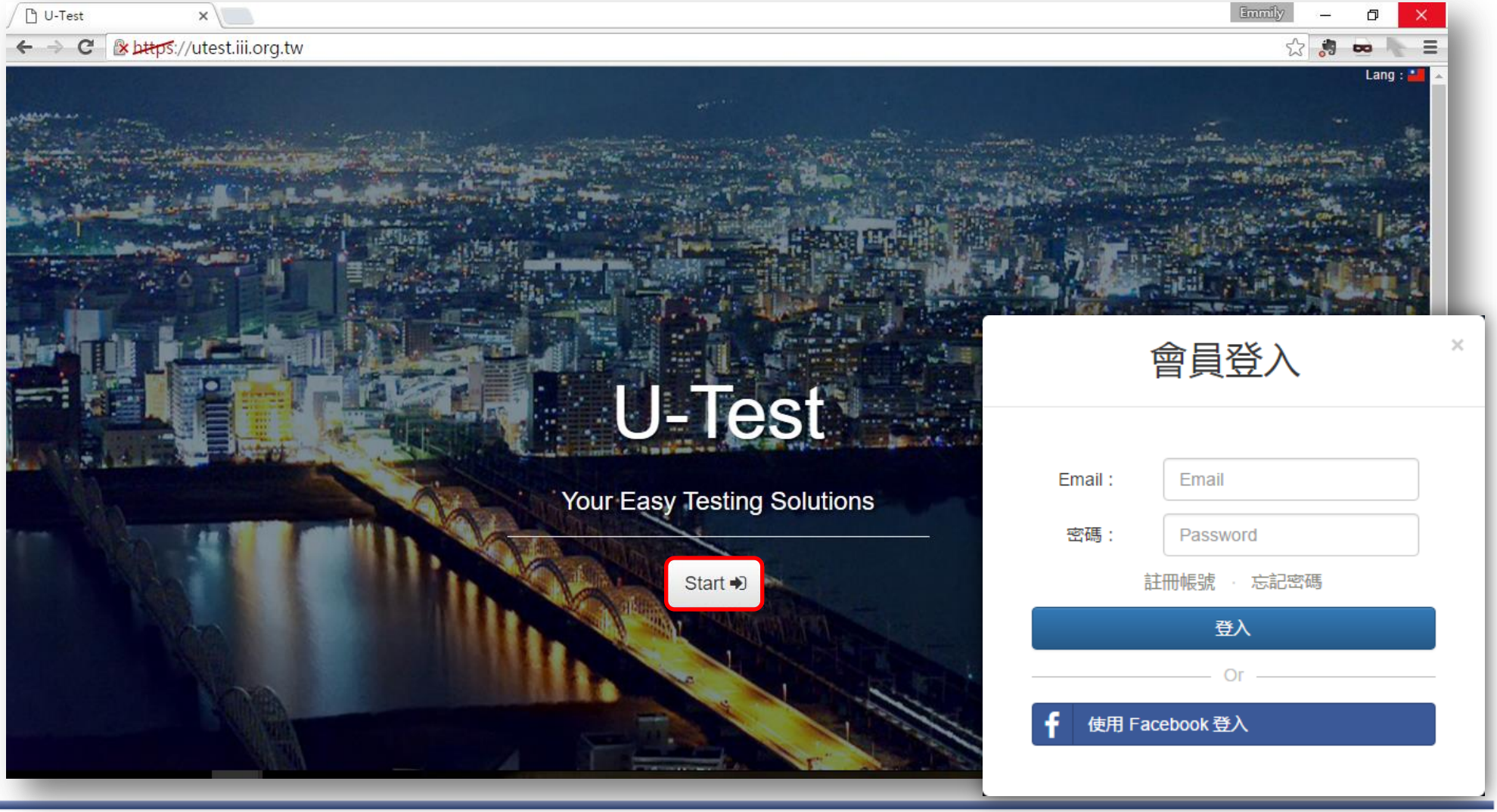
- OWASP Mobile TOP 10
- CVE Announced Threats
- 工業局行動應用 App 基本資安規範

Raw Log Download

- 行為記錄
- 網路封包
- 執行中儲存的檔案

U-Test：CMAS系統線上操作

- U-Test 上線網址：https://utest.iii.org.tw



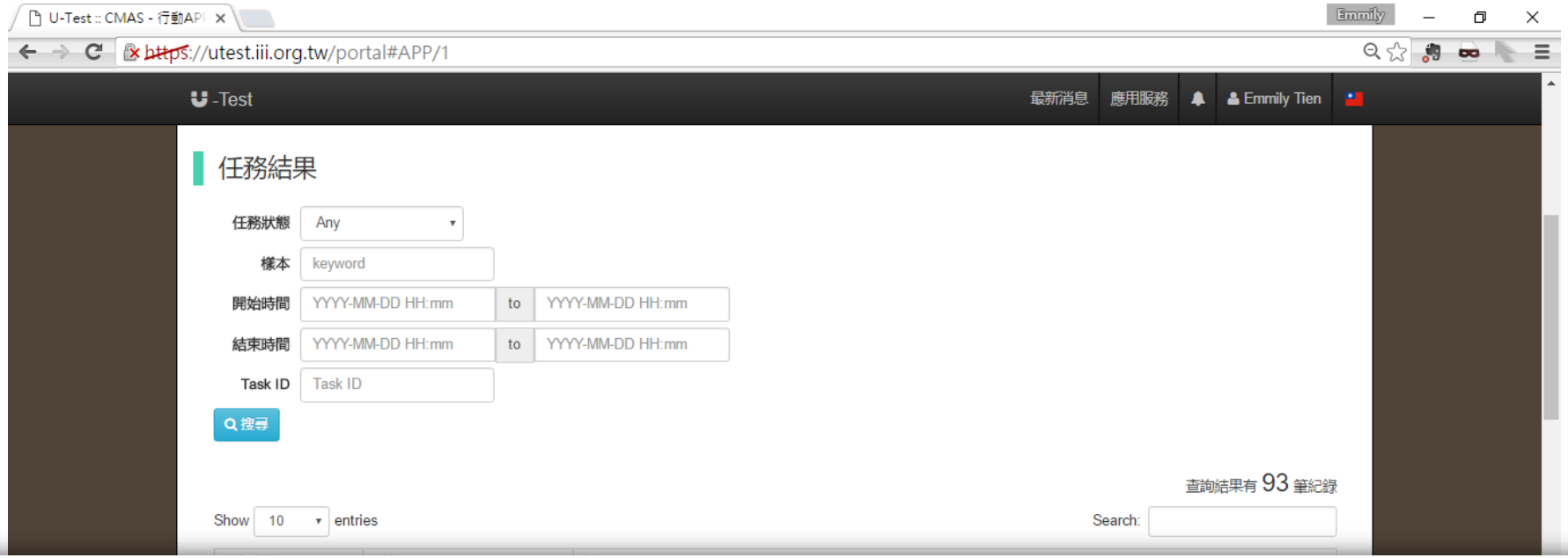
U-Test支援應用服務

- 已上線之服務：

- CMAS – 行動APP資安檢測平台
  - 2016.3月上線試營運
  - 支援初級檢測項目

CMAS 上傳操作

CMAS 下載資料操作



上傳時間	狀態	內容
2016/07/07 16:57:36	分析完成	Task ID f5df7125565b49faa3d4d1c29de6a2a8 樣本 Mail2000_v2.25.apk 參數 "redo": "true" 報表下載 意見回饋

Pdf 報表下載點

操作上有問題，
透過Email通報

系統支援初級項目說明

- **自動分析之限制：**
  不一定會觸發該項功能，且因敏感性資料種類眾多，支援有限，因此通過此測項不代表APP沒有此功能，或沒有敏感性資料。

檢測項目	自動化
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	V (註1)
4.1.2.3.5.敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存	V (註1)
4.1.2.3.6.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取	V (註1)
4.1.2.3.7.敏感性資料應避免出現於行動應用程式之程式碼	V (註1)
4.1.5.1.1.行動應用程式應避免含有惡意程式碼	△ (註2)

※ “△” 部分滿足測項內容

註 1：自動化搜尋敏感性資料：
護照號碼、Email、電話號碼(含手機)、信用卡、身分證字號、IMEI/Android ID、IMSI

註 2：僅提供惡意程式特徵比對，其餘測項因包含中級項目，故未提供在免費版作呈現

THANK YOU