駭客思維與資安攻防戰

Phil Hung

Self Introduction

- Phil Hung (Red+)
- 資歷
  - ✓ (NOW) INNO – 資安工程師
  - ✓ (NOW) ISDA台灣資訊安全聯合發展協會 – 資安研究員
  - ✓ 果核數位 – 資安工程師
  - ✓ 數聯資安 – 資安服務工程師
- 專業技能
  - ✓ Penetration Test
  - ✓ Vulnerability Assessment
  - ✓ App Testing
  - ✓ Social Engineering
  - ✓ DDoS
  - ✓ Information Security Health Check
- 專業證照
  - ✓ ECSA (資安分析專家)
  - ✓ TippingPoint Security Solutions Certificate

ISDA 台灣資訊安全聯合發展協會

ISDA,TW 協會簡介

- 中文: 臺灣資訊安全聯合發展協會
- 英文: Information Security Development Association, Taiwan
- 宗旨:
  - 1. 推動資安教育訓練(WarGame)為宗旨
  - 2. 培育專業資訊安全技術人才
  - 3. 提升臺灣整體資訊安全戰鬥與防護力
- 官方網站: http://www.isda.org.tw
- 連絡方式: isdawww [at] gmail.com

ISDA 台灣資訊安全聯合發展協會

前情提要

前情提要

- **請不要影響課程體驗**
  - ✓ 課程如有實作，請勿攻擊平台
  - ✓ 請勿使用自動化攻擊工具
  - ✓ 請勿互相提示過關密碼

- **請尊重智慧財產權**
  - ✓ 請勿公開課程內容
  - ✓ 請勿攝影及錄音
  - ✓ 本課程不提供簡報

前情提要

第 二 編 分則

第 三十六 章 妨害電腦使用罪

第 358 條　無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條　無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條　無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條　對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條　製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

課程大綱

01 跟風

02 資安教科書

03 攻擊是最好的防禦

04 麥當勞歡樂送

05 埋伏暗殺術

06 網路攻防戰

07 弱者決定生死

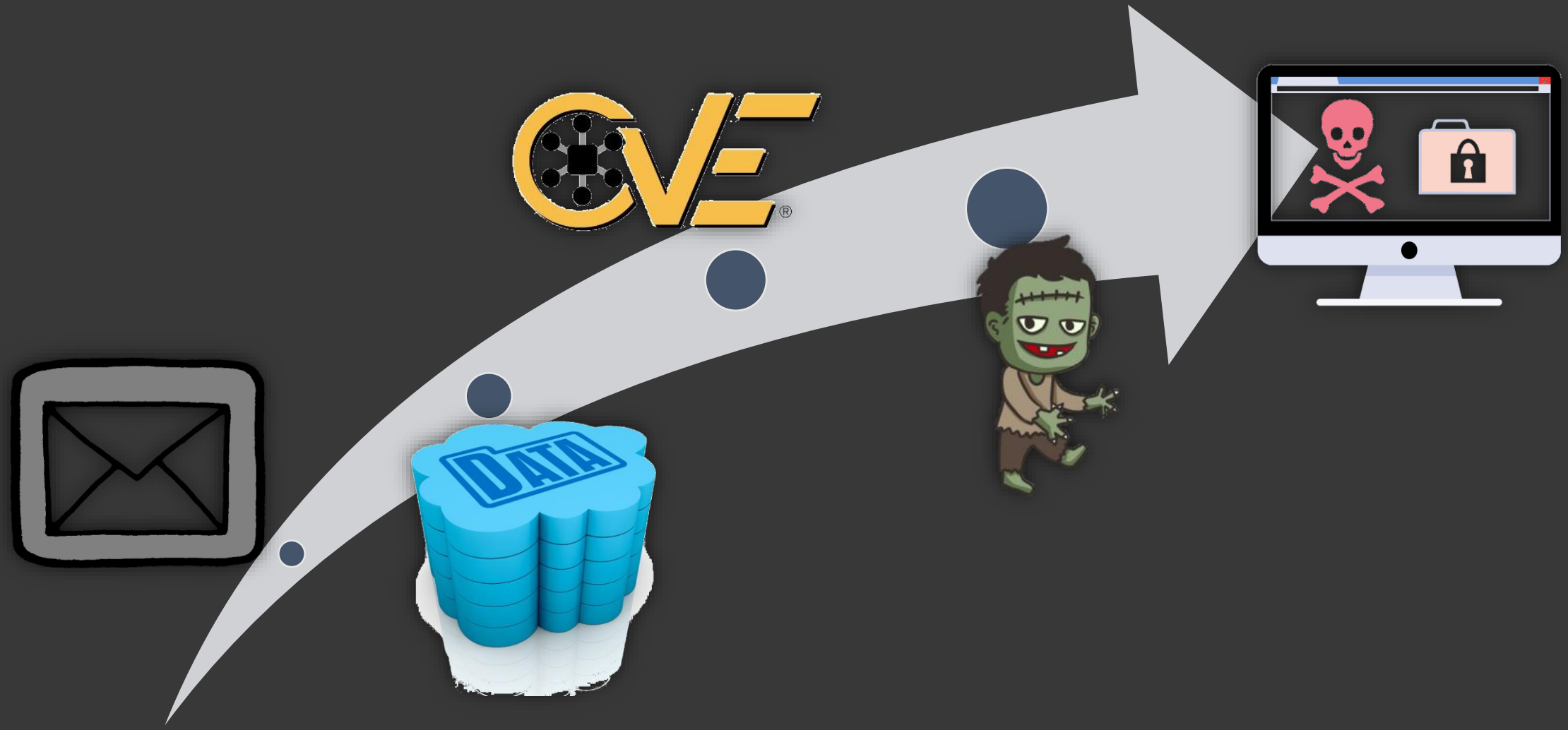
08 結語

跟風 – 資安趨勢

It is easy to be wise after the event.

不經一事，不長一智

資安趨勢



近期資安事件

iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 社群 商用電腦 搜尋

Windows 7、TeamViewer、共用密碼、沒防火牆四大安全缺陷，造成美國淨水廠遭駭

FBI也警告使用微軟已不支援的Windows 7、弱密碼及TeamViewer等桌面共享軟體有高風險，各界應以淨水廠遭駭事件為戒，檢查內部網路和存取政策

文/ 林妍溱 | 2021-02-12 發表

讚 6.4 萬 按讚加入iThome粉絲團 讚 698 分享

FBI本周發出的民間產業通知（Private Industry No
高風險，呼籲民間和聯邦政府機關檢查內部網路和存

上周五早上，美國佛羅里達州位於奧德馬爾（Oldsmar）市的淨水處理廠，內部電腦軟體遭不明人士透過TeamViewer連線存取，企圖將用於改善水質的氫氧化鈉濃度，從正常的100 ppm調高到危險的11,100 ppm。雖然最後因為管理員發現而未釀成大禍，但也引發恐慌。

近期資安事件

駭客竄改商務電子郵件 貿易公司漏看1字損失百萬元

2020-12-23 19:08 聯合報 / 記者廖炳棋／台北即時報導

+ 詐騙

讚 4 分享 分享

台北市一家貿易公司日前向外國廠商進貨時，收到駭客假冒上游廠商發送電子郵件，誆稱原本的收款帳戶因稅務檢查暫時停用，要求把貨款改匯到新帳戶，貿易公司職員沒注意對方的電子郵件帳號從原本的「…group@…com」變為「…qroup@…com」，g變成q！就依對方指示匯款，直到1個月後正牌廠商質問為何還沒收到款項，貿易公司才驚覺遇到詐騙，「1」字之差損失美金3萬3千餘元，約台幣近百萬元。

刑事局指出，竄改電子商務郵件詐騙在國際間相當猖獗，根據美國聯邦調查局網路犯罪通報中心網站公告，2014年1月到2019年10月間，該中心獲報的商務電子郵件詐騙（Business Email Compromise，BEC），被害金額高達美金2億元。

APT - 進階持續性滲透攻擊

資安教科書 – 資安概論

Books should be read with reservation.

盡信書，不如無書

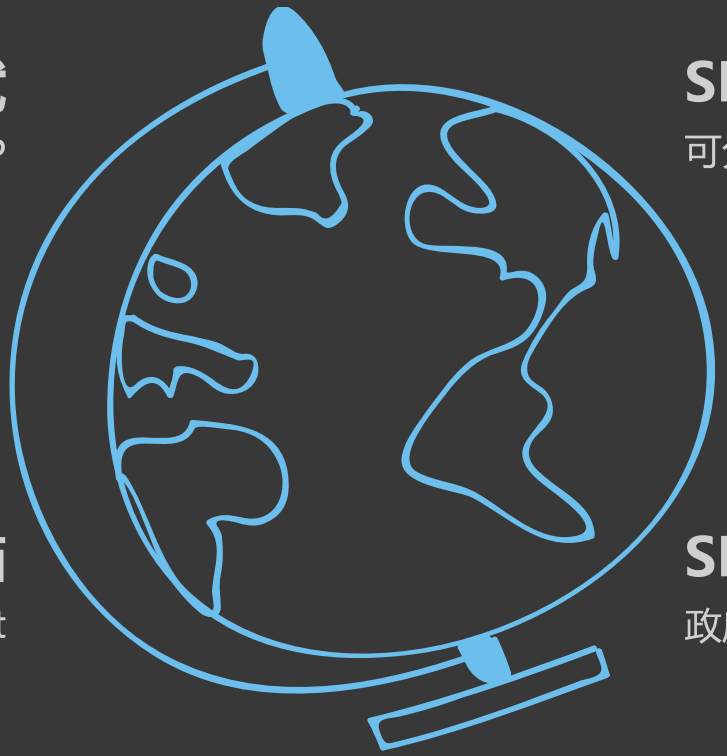
C I A

資安服務

APP檢測

PT – 滲透測試
可分Web & Host & APP

SE - 社交工程
可分演練 & 教育訓練



Code Review – 原碼檢視

DDoS演練

VA – 弱點掃描
可分Web & Host

SHC - 資安健診
政府規範 & 軟協健診包

SOC – 資安監控中心

資訊安全顧問服務
問題諮詢 & 教育訓練

資訊安全 = 系統 -> CIA

攻擊是最好的防禦 – 駭客思維

Keep your friends close but your enemies closer.

知己知彼，百戰百勝

駭客思維

Swiss Cheese Model

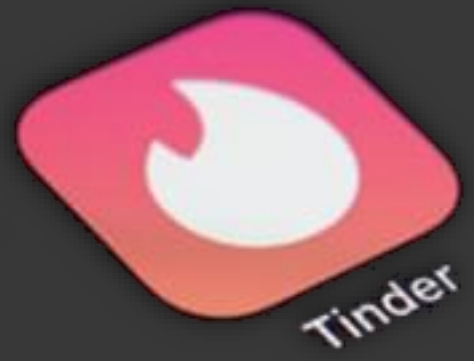
駭客任務

麥當勞歡樂送 – 社交工程

Words cut more than swords.

舌劍利於刀劍

社交？



文件社交工程

郵件社交工程

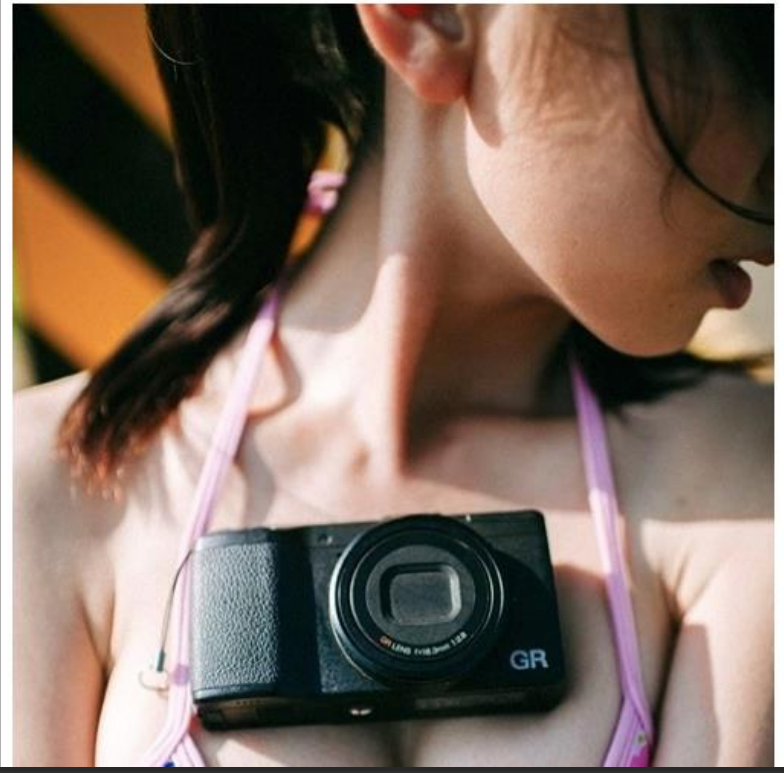
[原創]貓系正妹Tiny脾氣大!掀起上衣捧巨乳等你來馴服 只要你好好疼愛她:我要先上了(26P)

- 卡提諾論壇 <info@ck101.com>
- Phil Hung(洪嘉鴻)

2019年4月25日 星期四 下午5:50

顯示詳細資料

她是平面麻豆Tiny，有一張萌系的童顏但卻有著超強大的美胸
說她是童顏巨乳根本當之無愧啊！！！！



手機社交工程

釣魚網站

2019年5月23日 星期四

大紀元 生活網

Thu 23 May
14° / 25°

首頁 紐約新聞 美食 健康1+1 汽車 移民 旅遊 地產 教育 每日讀

首頁 > 各地分網 > 美國 > 紐約生活網-紐約華人的生活嚮導 > 紐約新聞 > 正文

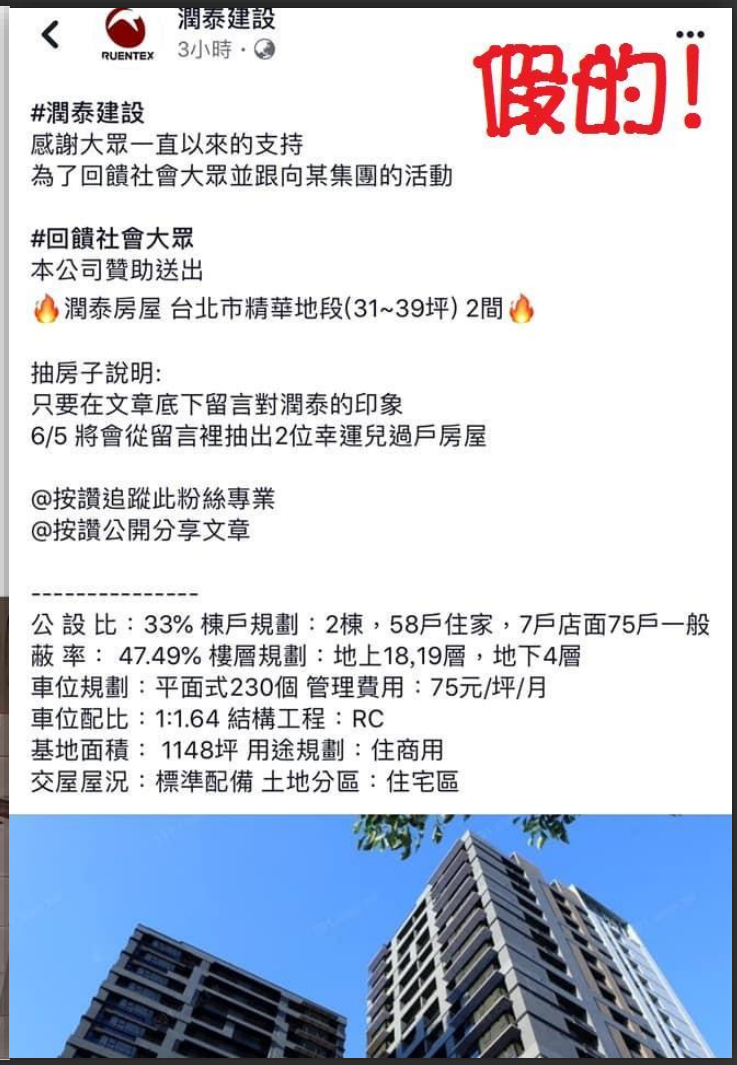
手機看新聞跳出中獎信息 華女遇騙

被告知被隨機抽中 獎品為1千元Walmart禮品卡 但要求她先購買Apple iTunes禮品卡

美食

- NEW YORK K
- 「韓式米線」
- 醫生打造健康
- 烤肉大餐無限
- Aladin Lamb

社交平台，願者上鉤



其他社交工程

回顧近10年來，我們曾經安裝過的電腦和手機病毒，絕對要閱讀的一篇文章，因為你目前電腦上可能就安裝著這些軟體。例如: oCam挖礦、Kmplayer被駭版

- oCam [1].
- Garena(GGC)[2]
- Kmplayer [3]
- Potplayer [4]
- 夜神[5]
- 網頁挖礦 [6]
- 掃描全能王 [7]
- 伊莉論壇 [8]

埋伏暗殺術 – 網頁安全

Better rely on yourself than no others.

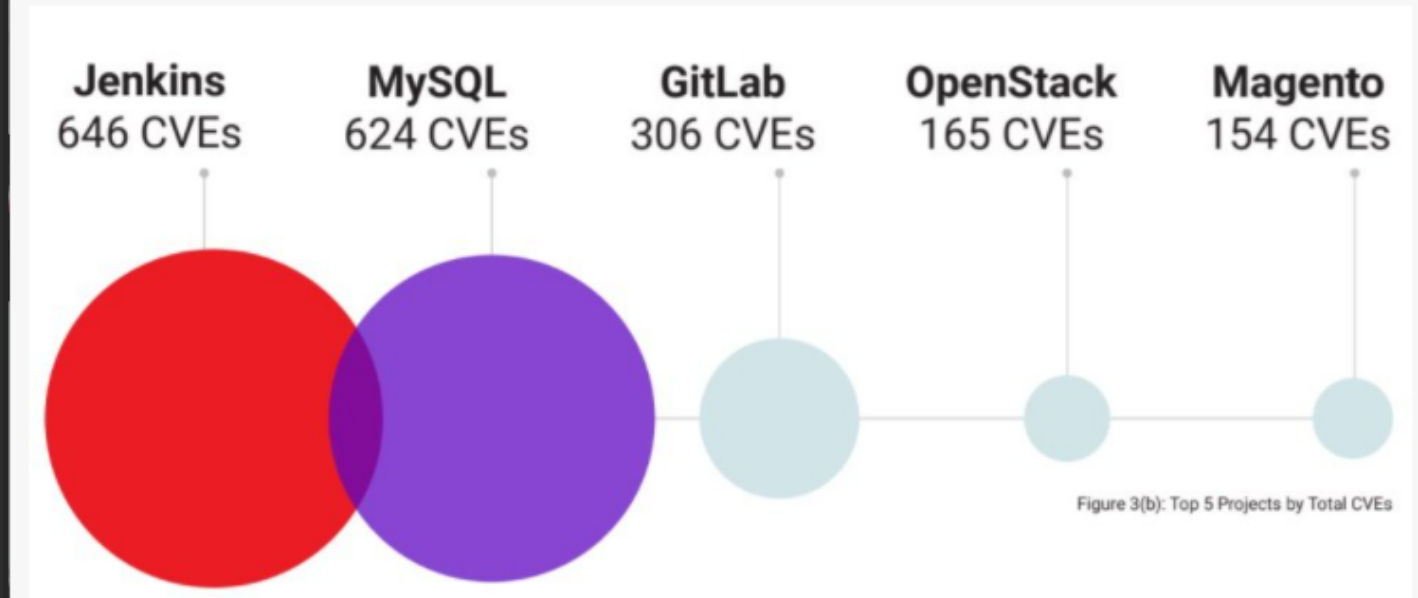
靠山山倒，靠自己最好

網頁安全

MySQL、Jenkins是漏洞最多的兩個開源碼專案

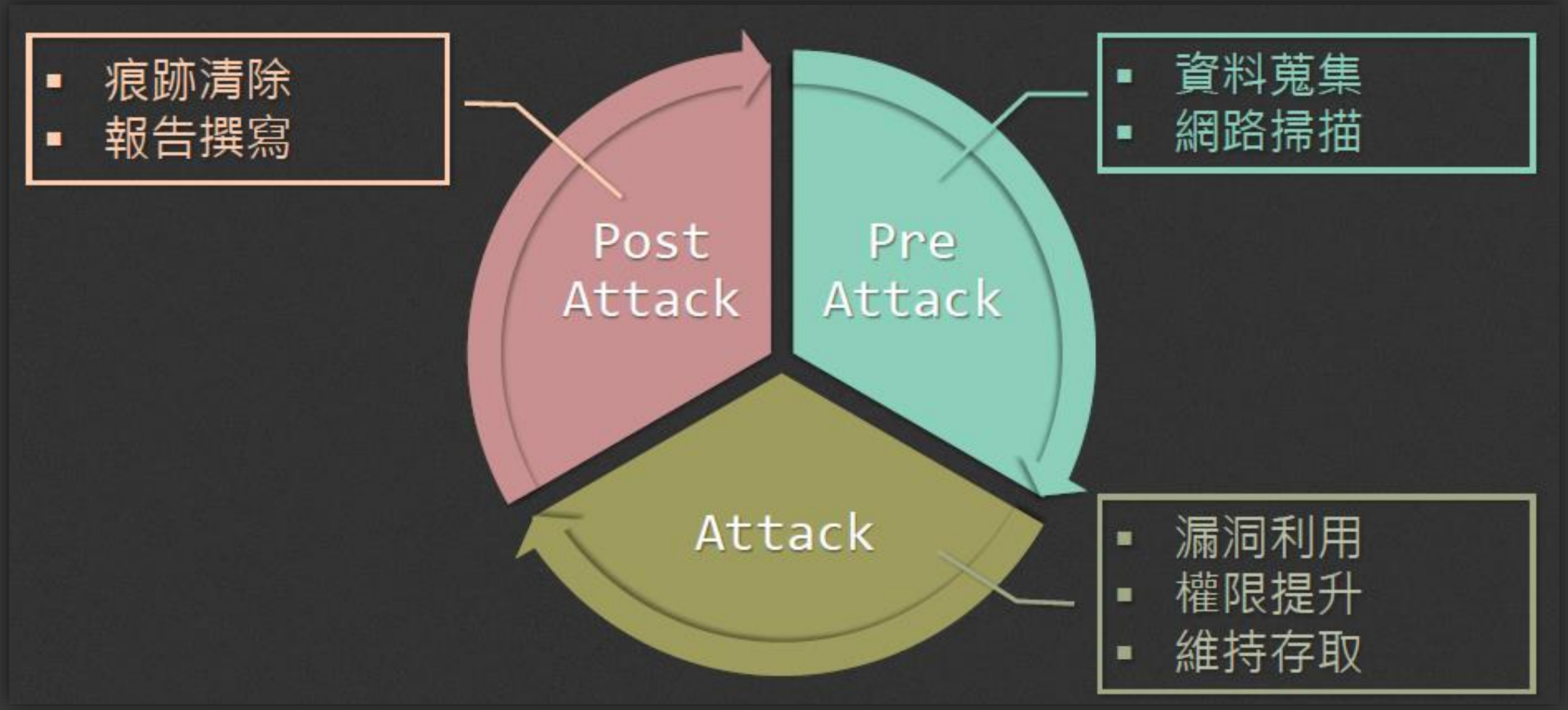
RiskSense追蹤54個主要開源專案從2015年至今公開的CVE漏洞代碼，發現過去3年來的漏洞數量，呈現逐年倍增的趨勢

文/ 林妍溱 | 2020-06-10 發表



RiskSense檢視54項主要的開源專案，從2015年到2020年3月底的公開CVE漏洞代碼，專案含有漏洞數量最多的前二大，是持續整合工具Jenkins（646項漏洞），以及資料庫軟體MySQL（624項漏洞）。（Photo by RiskSense）

網 頁 VA? PT?



OWASP TOP 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Top1 Injection

Top2 Broken Authentication

直接繞過收銀台！破解IKEA電梯漏洞　婦人狂搬商品離開

2016/11/20 08:07:00

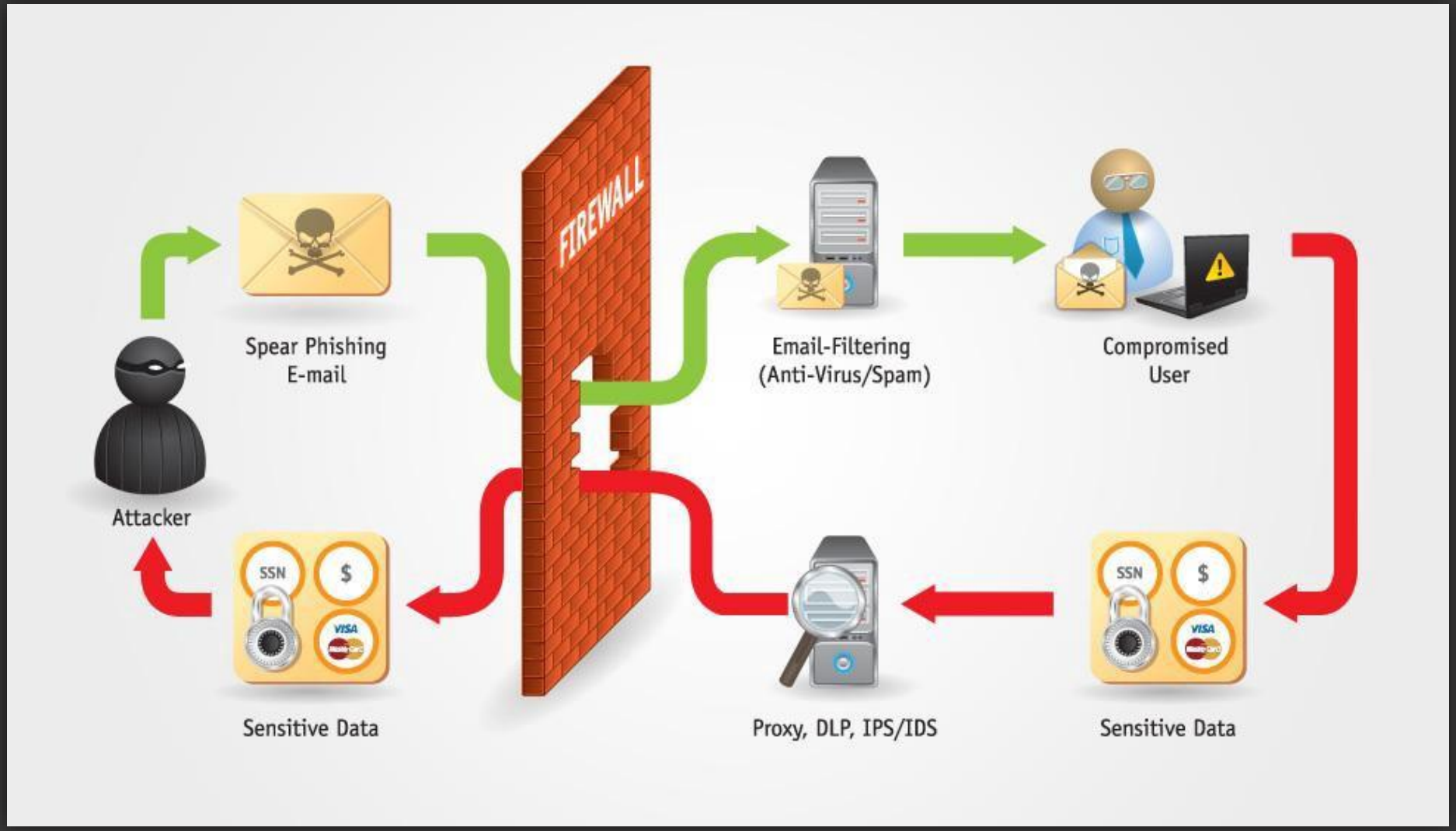
追蹤三立：

A- A A+

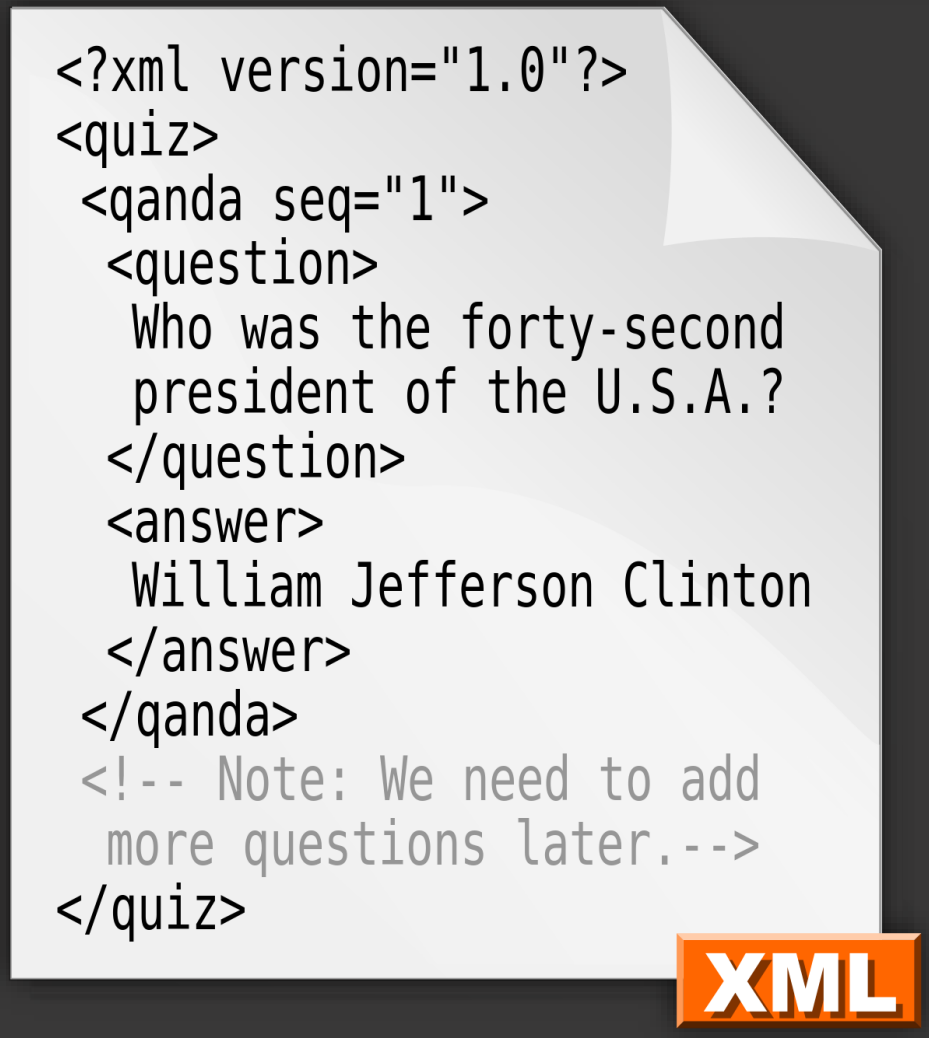
社會中心 / 綜合報導

鑽漏洞偷竊不可取！歐式家具大賣場IKEA設有客用電梯，可讓顧客直接從一樓坐到四樓挑選商品，但卻有婦人投機取巧，直接載著滿滿商品、繞過收銀台從電梯離開，更食髓知味想偷竊第二次，但被保全發現才倉皇逃逸。

Top3 Sensitive Data Exposure

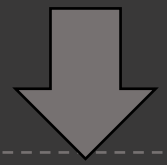


Top4 XML External Entities (XXE)

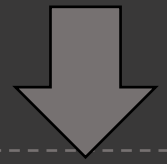


Top5 Broken Access Control

http://xxx.xxx.xxx.xxx/show.php?file=xxx.txt



http://xxx.xxx.xxx.xxx/show.php?file=../etc/passwd



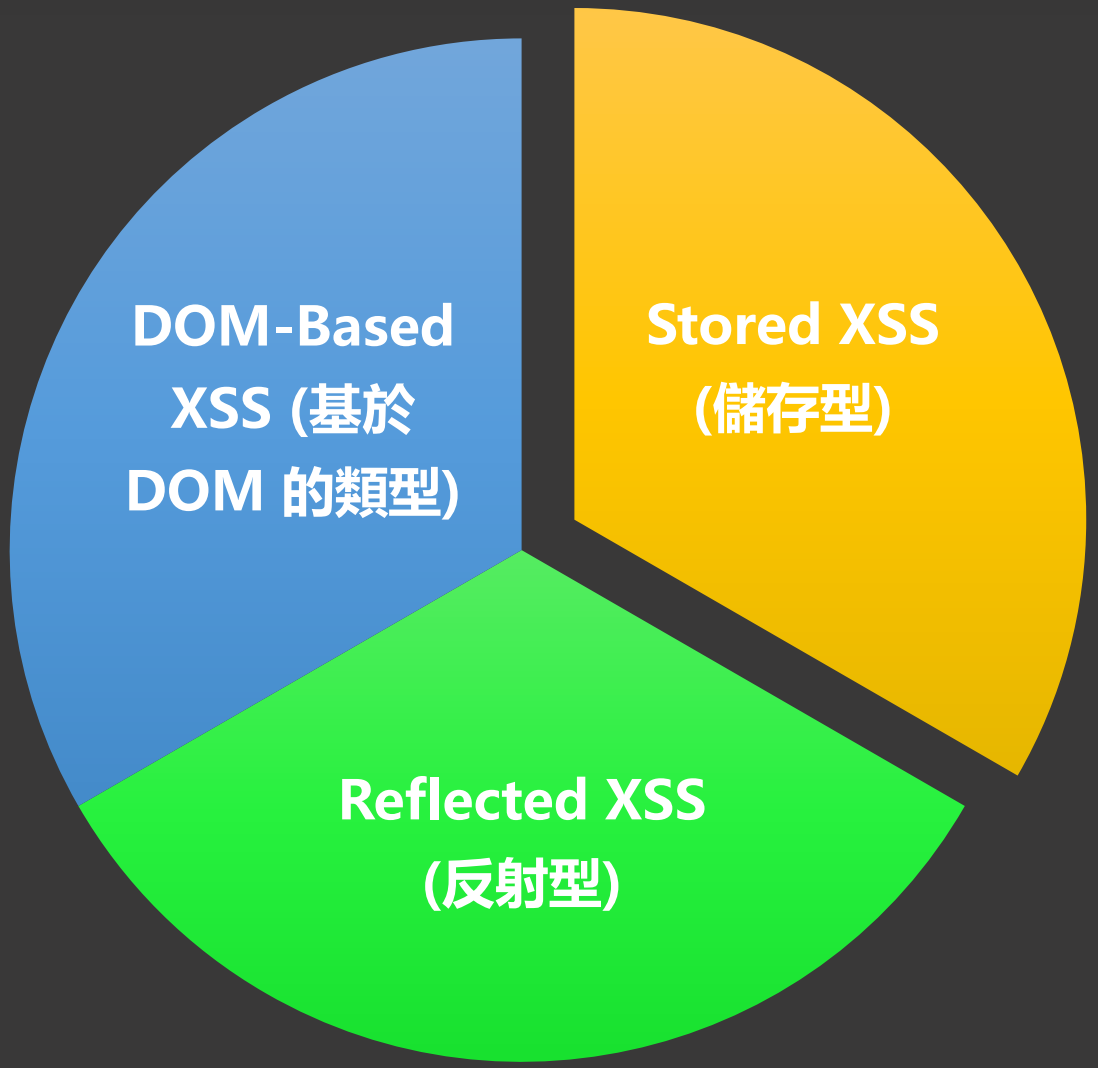
禁止 ../

http://xxx.xxx.xxx.xxx/show.php?file=%2e%2e%2fetc/passwd

Top6 Security Misconfiguration

- ✓ 駭客可透過彈跳錯誤蒐集標的資訊
- ✓ 可透過標的未修補的漏洞攻擊
- ✓ 系統被攻陷，資料外洩

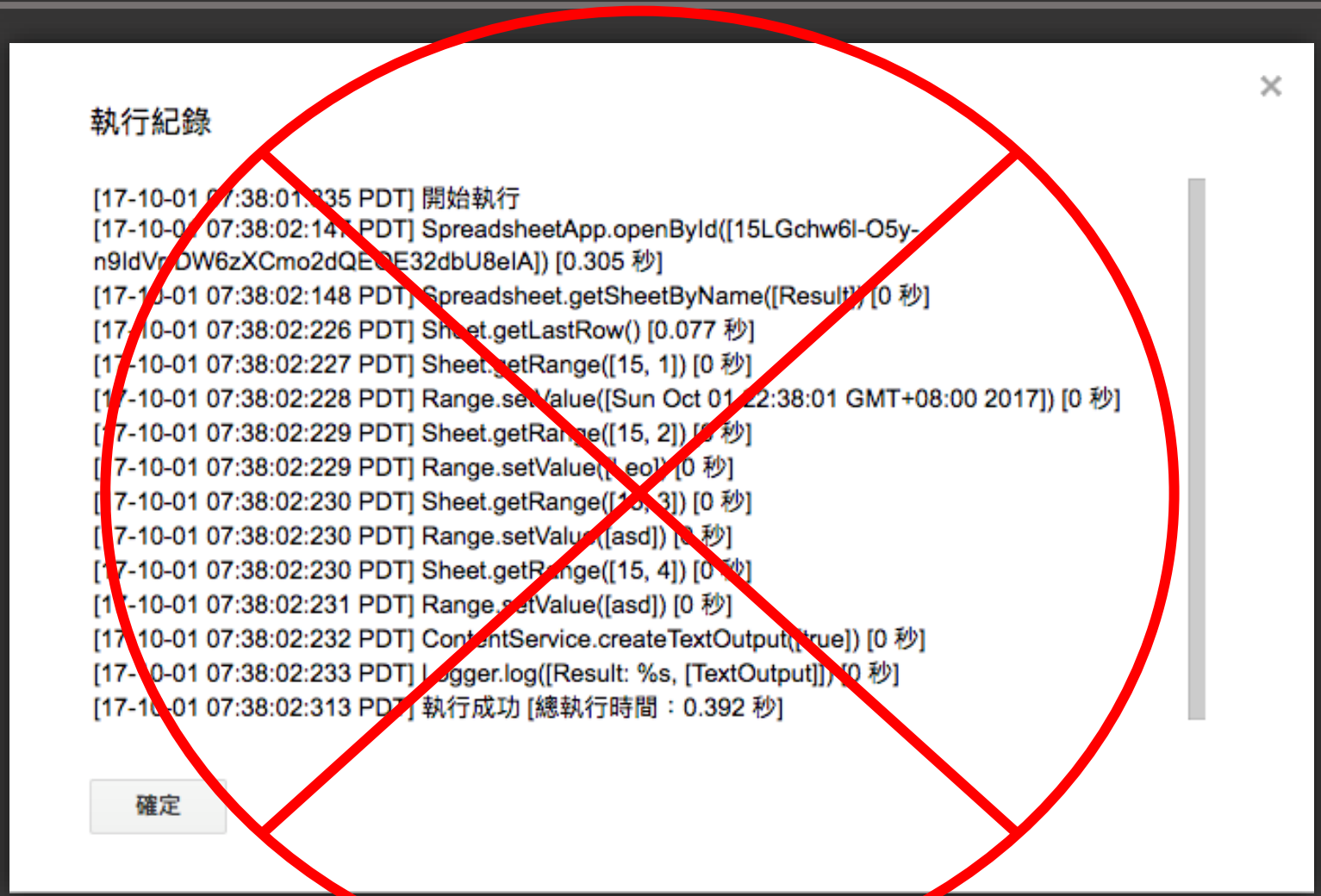
Top7 Cross-Site Scripting (XSS)



Top8 Insecure Deserialization

Top9 Using Components with Known Vulnerabilities

Top10 Insufficient Logging & Monitoring



網路攻防戰 – Wargame

Actions speak louder than words

坐而言不如起而行

Red+ Wargame

情境

駭客在逛網站的時候.....

發現網站有**錯誤的做法**導致網站秘密可能被竊取.....

Game 1

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 2

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 3

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 4

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 5

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 6

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 7

- ✓ 不要！修改USERNAME
- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game 8

- ✓ 找到本關PASSWORD
- ✓ 大家加油

Game Over

To be continued.....

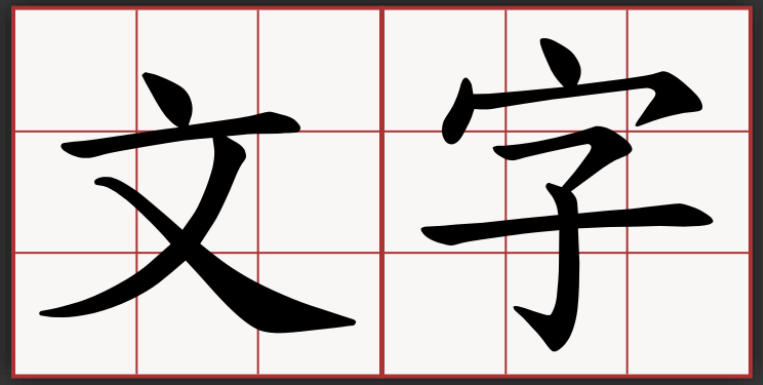
資安意識

Kind hearts are soonest wronged.

人善被人欺

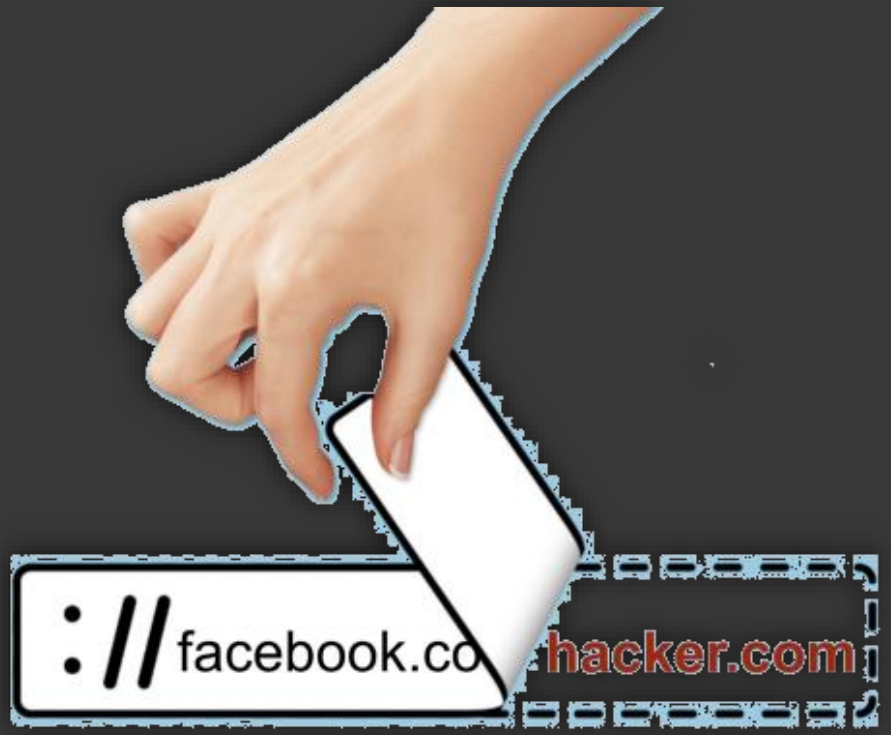
防人之心不可無

電子郵件安全



APP 安全

網頁釣魚安全

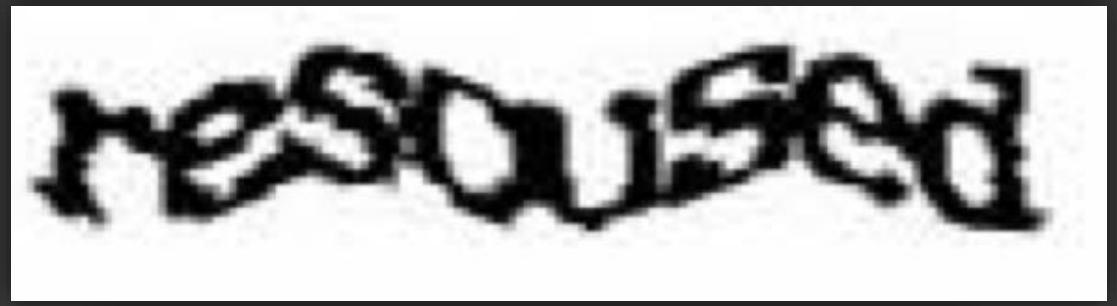


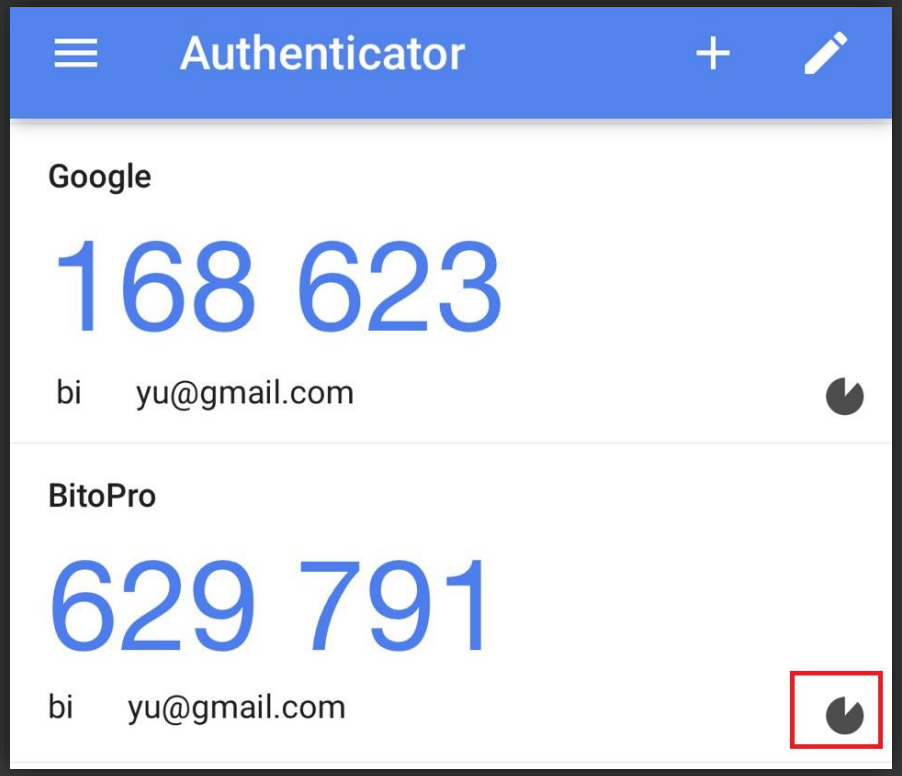
網頁安全

網頁安全

網頁安全

網頁安全





密碼安全

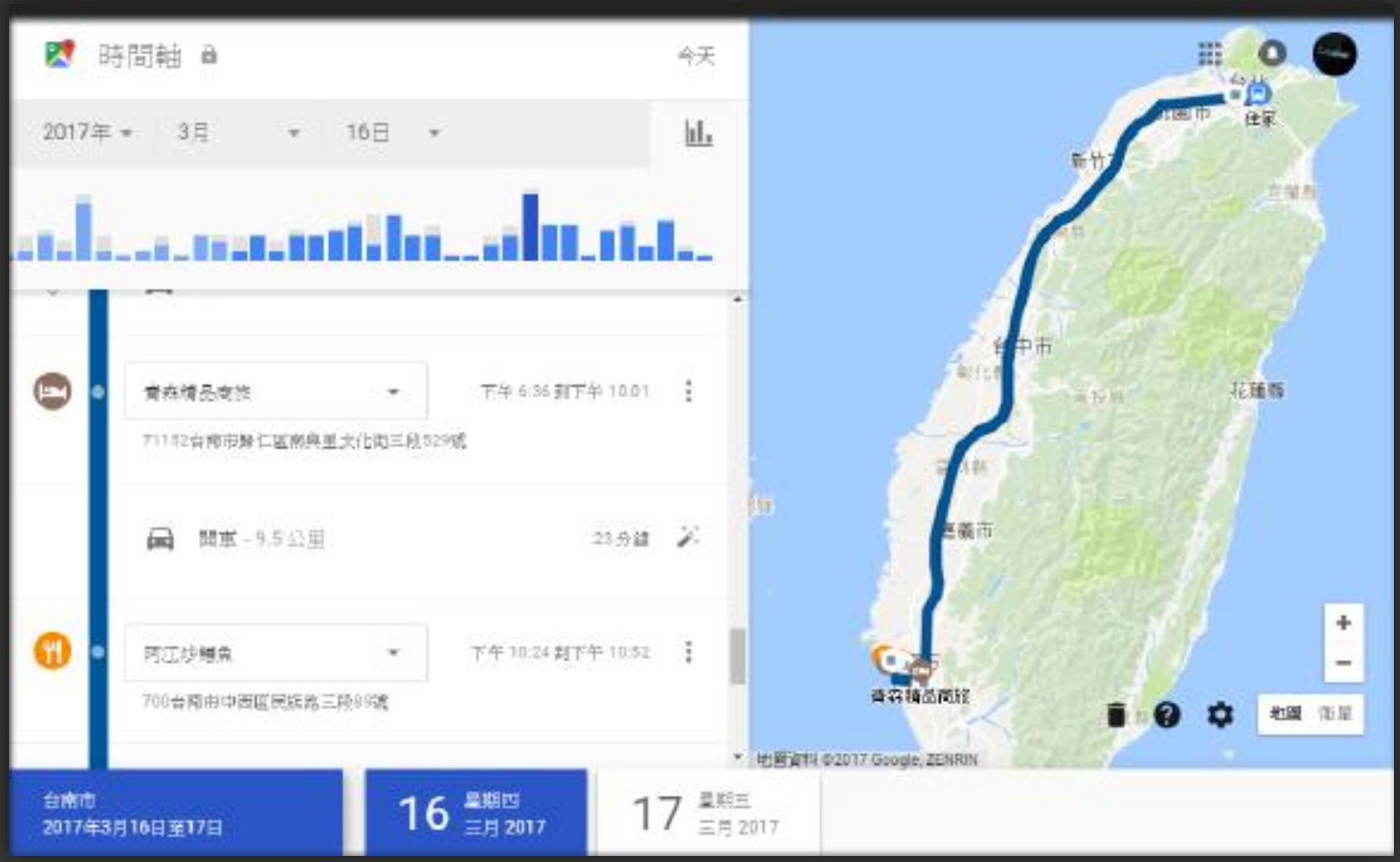
軟體安全

常被忽視的安全

一個癡漢不一定是駭客，
但一個好的駭客一定是個厲害的癡漢。

－論資料收集的重要性

常被忽視的安全



常被忽視的安全

據《泰晤士報》報道，近1000個應用程序都包含與廣告商共享的位置追蹤代碼。在12月初，《紐約時報》的一項調查顯示，許多應用程序都會告知用戶需要收集位置數據，但是卻不告知用戶這些數據會被如何使用。報告稱，這些數據會被賣給廣告商、零售公司和對沖基金以了解消費者的行為習慣。據稱，今年這些隱私信息的市場價值估計為160億英鎊(合1392億人民幣)。(實習編譯：王祎涵 審稿：李宗澤)

(責編：趙超、楊波)

結 語

Solution V.S Know How

資安健檢
檢視內部作業提供改善建議，提升資安防護能力

原始碼檢測
提供改善建議報告，協助企業提升防護能力

社交工程
以電子郵件提供受測單位，了解安全缺口做補強

弱點掃描
WEB主機或系統做安全掃描，提供結果並協助修正

滲透測試
模擬駭客攻擊方式，找出可能資安漏洞

後滲透服務
驗證保護機制或規範落實，以駭客思維檢視侵入後損失與風險

AI SOC
智慧聯防事件鑑識，快速掌握駭客攻擊方式

Incident Response
回溯資安漏洞根本原因進行修補，避免事件再發生

Cloud DDoS Service
台灣第一線服務提供者，阻擋國際大量攻擊流量

AMAZING THOR
智慧安全監控辦公室，降低管理成本與時間

IP流向檢測
72小時內提供經濟部工業局認可文件，支援雙重平台和彈性收費

Solution V.S Know How

木桶理論

一時被駭一時賠，一直被駭一直賠

近年台灣重大個資外洩事件

時間	案情	備註
2012	兆豐銀銷毀電腦造成個資外流到二手市場	金管會罰200萬
2012	台新銀將證券客戶交易資料上傳到個人網站	金管會罰400萬
2013	中信銀網路銀行個資外洩	金管會罰400萬
2015/05	丹堤咖啡遭駭，5000筆會員個資外洩，被惡意刊登在國外網站上	
2016/05	郵局商城遭駭，1.7萬筆個資外洩	
2016/10	勞動部就業通3萬筆個資外洩	
2018/03	華信航空訂票系統疑遭駭客入侵，旅客個資外洩遭詐騙	受害者提告，航空公司判賠2萬元
2017/05	雄獅旅行社36萬筆個資外洩	個資法後首宗團訟案
2018/01	佳德個資遭駭，導致數名消費者被詐騙	
2018/03	台灣宅經濟商務公司在人力銀行登載徵人廣告，藉以盜取求職人員個資供富邦人壽使用	
2018/08	北市衛生局遭駭，298萬筆個資被竊	
2019/06	銓敘部59萬筆公務員資料外洩	
2019/07	1111人力銀行20萬筆個資遭外洩	

中央社製圖

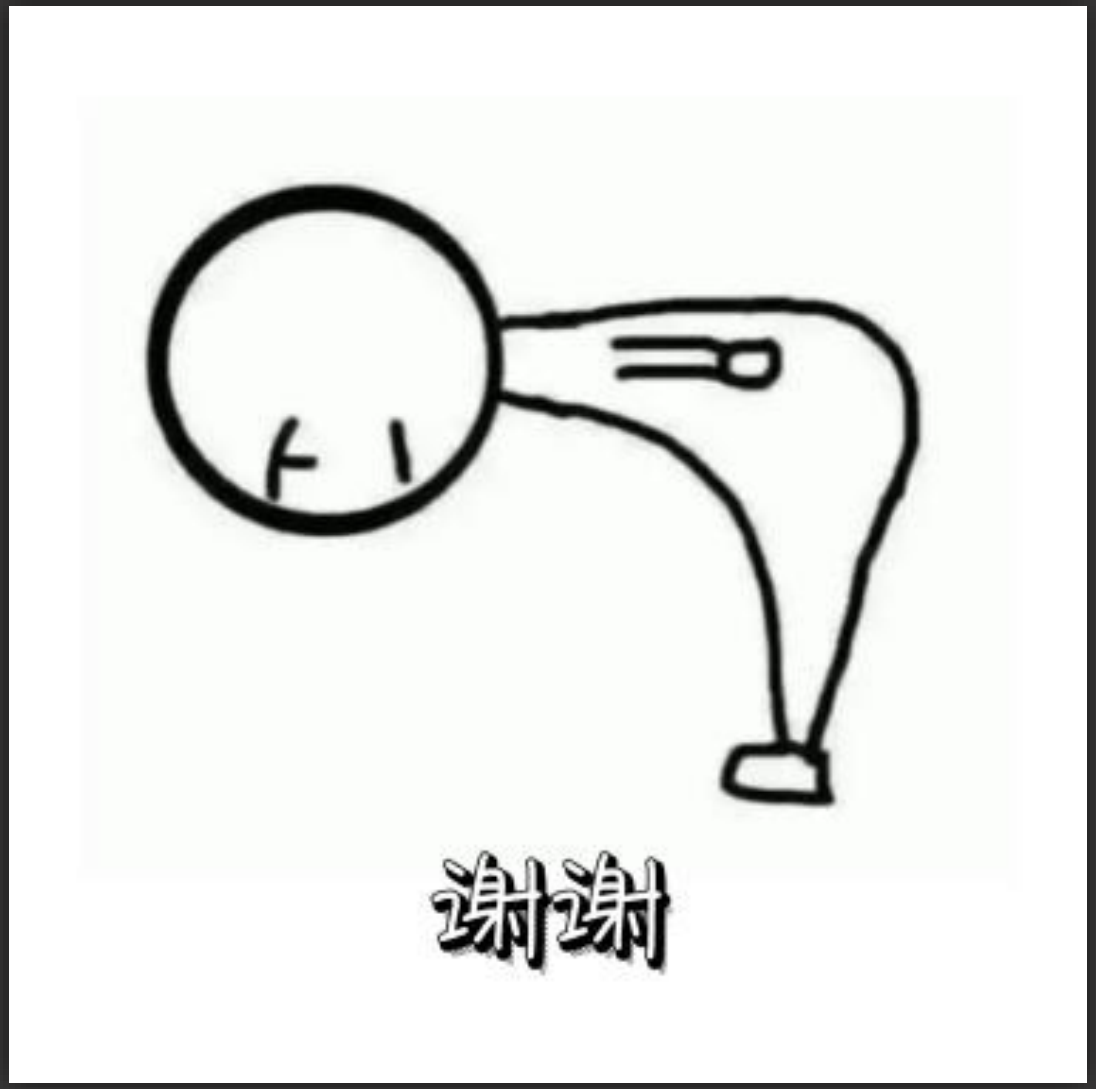
一時被駭一時賠，一直被駭一直賠

近年國外重大個資外洩事件

時間	案情	備註
2009	Heartland Payment Systems支付處理系統被植入惡意程式遭駭，退伍軍人的個資外洩，7000萬名退伍軍人受到影響	
2009	美國退伍軍人協會的電腦遺失，牽連2650萬筆美國公民資料	
2013/08	Yahoo個資外洩延燒至2016年，期間共發生3起個資外洩，前後約有30億用戶受影響，堪稱史上最大宗的個資洩漏案件	2019年4月與用戶達成新的和解方案，賠償總金額高達1.175億美元（約新台幣36.4億元）
2013年底	美國折扣零售業巨人Target因支付系統遭駭，釀成1.1億筆資料外洩	2015年與由銀行、信用組織發起的集體訴訟代表達成和解，代價是償付3936萬美元（約新台幣12.8億元）的損失
2014/05	eBay網站的用戶資料庫遭駭客入侵，約1.45 億名用戶資料遭竊	
2015	劍橋分析公司於美國總統大選期間疑似不正當使用臉書用戶個資案，約8700萬人受影響	美國聯邦貿易委員會(FTC)2019年7月決定對臉書開罰50億美元，只要美國司法部同意，將創下FTC史上最高罰款金額
2016/10	Uber遭駭客入侵，5000萬名乘客的姓名、電子郵件以及手機號碼遭外洩，700萬名駕駛的個資被存取	Uber以10萬美元代價，換取駭客刪除外洩的資料
2017/09	美國第三大消費者信用報告業者Equifax在坦承遭到駭客入侵，逾1.4億筆用戶資料外洩，超過美國1/3人口數	美國聯邦交易委員會（FTC）2019年7月22日宣布與Equifax達成和解，Equifax最高將支付7億美元的和解金額
2018/03	國泰航空，以及齊下全資子公司國泰港龍航空，共有約940萬乘客的國籍、護照號碼、信用卡號等個資外洩	
2018/06-07	新加坡保健服務集團年6月27日到7月4日遭到駭客攻擊，竊取2015年5月到2018年7月4日赴新加坡保健服務集團旗下診所看病的150萬病患病患個資，影響人數逾新加坡人口1/4，另外約有16萬人的用藥資料也遭竊	
2018/07	社交網站時光機app　Timehop遭駭，2100萬用戶個資外洩，而且駭客也曾取得用戶存取臉書、推特、IG等社交網站內容的憑證	
2018/09	Amazons　在9月查出部分員工出售機密客戶個資給第3方公司後，11月再因為技術問題而外洩部份消費者的個資	
2018/09	英國航空旗下官方網站被駭客轉移至詐騙網站，高達50萬名顧客個資被駭客偷走，包含姓名、Email、信用卡資訊等，高達38萬筆網路交易受到影響	英國資訊專員辦公室（the Information Commissioner's Office, ICO）宣布，因為英國航空（British Airways）去年的顧客個資外洩事件，判罰1.83億英鎊罰款（約71億元台幣），若判決正式生效，將創英國境內因個資外洩的史上最高罰款紀錄
2018/11	2016年萬豪收購競爭對手喜達屋（Starwood）酒店，喜達屋的旅館訂房系統遭駭客入侵，但萬豪並沒有確實檢查，造成2014年以來訂房的3億客戶個資，及信用卡個資都傳出被駭，在2018年11月爆出	
2019/07	美國第一資本銀行（Capital One）發表聲明表示，有一名駭客非法入侵銀行的電腦系統，包括客戶姓名、地址、電話、信用評等、交易紀錄等資訊在內，大約1億名美國客戶和600萬加拿大客戶個資遭到盜取	

中央社製圖

E N D



Red+ / Phil / 洪嘉鴻

資安顧問 / 資安講師
Line : @838emszv
Mail : phil830414@gmail.com
Mobile : 0966-241-011