TWCSA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

如何看懂弱點掃描報告

蔡一郎

Google Me.

現任

- ✓ 微智安聯股份有限公司 創辦人兼執行長
- ✓ 台灣數位安全聯盟 榮譽理事長
- ✓ 台灣網際空間與安全策略發展協會 理事長
- ✓ 台灣數位鑑識發展協會 理事
- ✓ 中華民國資訊安全學會 監事
- ✓ 中華民國數位金融交易暨資料保護協會 理事
- ✓ 中華民國人壽保險商業同業工會 資安顧問
- ✓ OWASP 台灣分會長
- ✓ The Honeynet Project 台灣分會長
- ✓ Cloud Security Alliance 台灣分會長
- ✓ CSCIS 亞太區副總裁
- ✓ 教育部、交通部資安稽核委員
- ✓ 自由作家，資訊圖書著作 35 本，技術專欄文章 90 餘篇
- ✓ 部落格 https://blog.yilang.org
- ✓ 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、ISO 17065、CSA STAR Auditing、CCSK

蔡一郎 Steven Tsai

國立成功大學 電腦與通信工程研究所 博士候選人

國立成功大學 電機工程研究所 碩士

曾任

- ✓ 財團法人國家實驗研究院國家高速網路與計算中心 研究員
- ✓ 台灣數位安全聯盟 理事長
- ✓ 總統府、行政院、經濟部資安稽核委員
- ✓ 中華民國資料保護協會 監事
- ✓ 數位經濟暨產業發展協會 理事
- ✓ 中華民國南部科學園區產學協會 理事 監事
- ✓ 台灣資訊安全聯合發展協會 監事

大綱

- 弱點掃瞄
  - 瞭解弱點掃描
  - 網站應用程式安全
  - 常用的工具
  - 弱點掃描報告解讀

資安、知安？

Cyber Security in Everywhere

TWCSA 台灣數位安全聯盟 Taiwan Cyber Security Alliance

TWCSA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

瞭解弱點掃描

一個真實的案例！

Warning: mysqli::mysqli(): (HY000/2002): Connection refused in **/var/www/html/ebook/system/library/db/mysqli.php** on line **7**

Warning: mysql_error() expects parameter 1 to be resource, object given in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

Warning: mysql_errno() expects parameter 1 to be resource, object given in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

Notice: Undefined variable: trace in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

Notice: Undefined variable: trace in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

Notice: Undefined variable: sql in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

Fatal error: Uncaught exception 'Exception' with message 'Error:
Error No:
 Error in: line
' in /var/www/html/ebook/system/library/db/mysqli.php:10 Stack trace: #0 /var/www/html/ebook/system/library/db.php(9): DB\MySQLi->__construct('localhost', 'root', 'Dd0917588800', 'ebook', '3306') #1 /var/www/html/ebook/system/framework.php(25): DB->__construct('mysqli', 'localhost', 'root', 'Dd0917588800', 'ebook', '3306') #2 /var/www/html/ebook/index.php(22): require_once('/var/www/html/e...') #3 {main} thrown in **/var/www/html/ebook/system/library/db/mysqli.php** on line **10**

請問有看到什麼問題嗎？

瞭解弱點掃描

- 用來檢查網路或作業系統的安全性
- 模擬攻擊者所發出的攻擊動作
- 可提供網路管理人員做為弱點修補之依據，以提昇安全性
- 與防毒軟體的做法相似，依據所謂的「弱點特徵資料庫」來測試是否存在已知的漏洞

為什麼要進行弱點檢測

- **系統安全**
  - 您的系統安全嗎？
  - 類似健康檢查的概念
  - 及早發現，避免漏洞曝露，遭受利用
  - 未發現問題，不一定代表沒問題
  - 可能影響系統安全的因素
  - 未修補的系統漏洞
  - 不安全的服務
  - 不安全的設定
  - 不安全的使用習慣
- **網路安全**
  - 了解系統上服務開放的狀況
  - 不同位置的服務開放狀況應有不同
  - 測試防火牆設定正確性及功能性

弱點掃描的過程

- 弱點掃描工具透過預先載入的系統漏洞資訊對目標資訊設備進行模擬攻擊。
- 弱點掃描的 5 個階段：
  - 主機探索
  - 連接埠掃描
  - 系統服務確認
  - 漏洞探測
  - 安全評估結果產出
- 弱點掃描型態
  - 主動式 V.S. 被動式。
  - 網路型 V.S. 主機型。

弱點掃描工具

- 網路型 V.S. 主機型
  - 網路型
    - 主要是透過網路進行弱點稽核作業。
  - 主機型
    - 安裝在受測的主機上。
    - 所以有完全的權限進行更多的檢測。

弱點掃描工具(Cont.)

- 網路型 – 弱點掃描工具
  - 可以掃描存在於網路上的任何設備及主機，發掘企業網路上一些未知或未授權的設備與主機。
  - 可以偵測出到底有哪些服務在網路上運作。
  - 檢查是否有不該開啟的通訊端口(port)在運作。
  - 快速地檢測可能的弱點或安全漏洞。
  - 提供了每個弱點之相關訊息與修補的方法。
  - 產生完整的檢測報表。

弱點掃描工具(Cont.)

- 網路型 – 弱點掃描工具部署需注意的地方
  - 是否有透過防火牆進行掃描檢測
  - 是否對於受測的主機有足夠的權限。
- 優點: 部署彈性大，管理及報表集中，較方便進行企業的完整安全評估。
- 缺點: 可偵測弱點數受限於對目標主機的權限。

弱點掃描工具(Cont.)

- 主機型 – 弱點掃描工具
  - 可以檢測出主機上所存在的不正確的檔案權限設定。
  - 可以檢測不當的軟件設定問題。
  - 可以檢測其它的安全弱點與漏洞。
- 優點: 掃描方式較多，可偵測到更多的弱點。
- 缺點: 集中管理不易。

選擇合適的弱點掃描與評估工具

- 選擇工具時需注意以下五點：
  - 弱點特徵資料庫的更新是否夠快
  - 弱點特徵資料的描述和修補建議是否完整明確
  - 掃描的效率以及對目標系統的影響
  - 使用者介面的易用性
  - 分析報告的形式是否符合需求

掃瞄注意事項: 弱點掃描時機

- 運作情況
  - 未運作、未上線主機
    - 不限，可以測試所有弱點。
  - 已運作(執行中)主機
    - 以不影響伺服器正常運作為前提。
- 檢測時間
  - 定期檢測:檢測固定項目。
  - 不定期檢測:檢測特定項目。

掃瞄注意事項: 弱點掃描時機 (cont.)

- 弱點掃瞄可能讓服務或主機掛掉 •
  - DoS 類弱點
  - 服務或主機處於高負載
  - 弱點利用失敗
    - 檢查banner
    - 弱點特徵檢查(根據特定request之回應結果)
    - 弱點利用(大多數的弱點掃瞄不會執行)

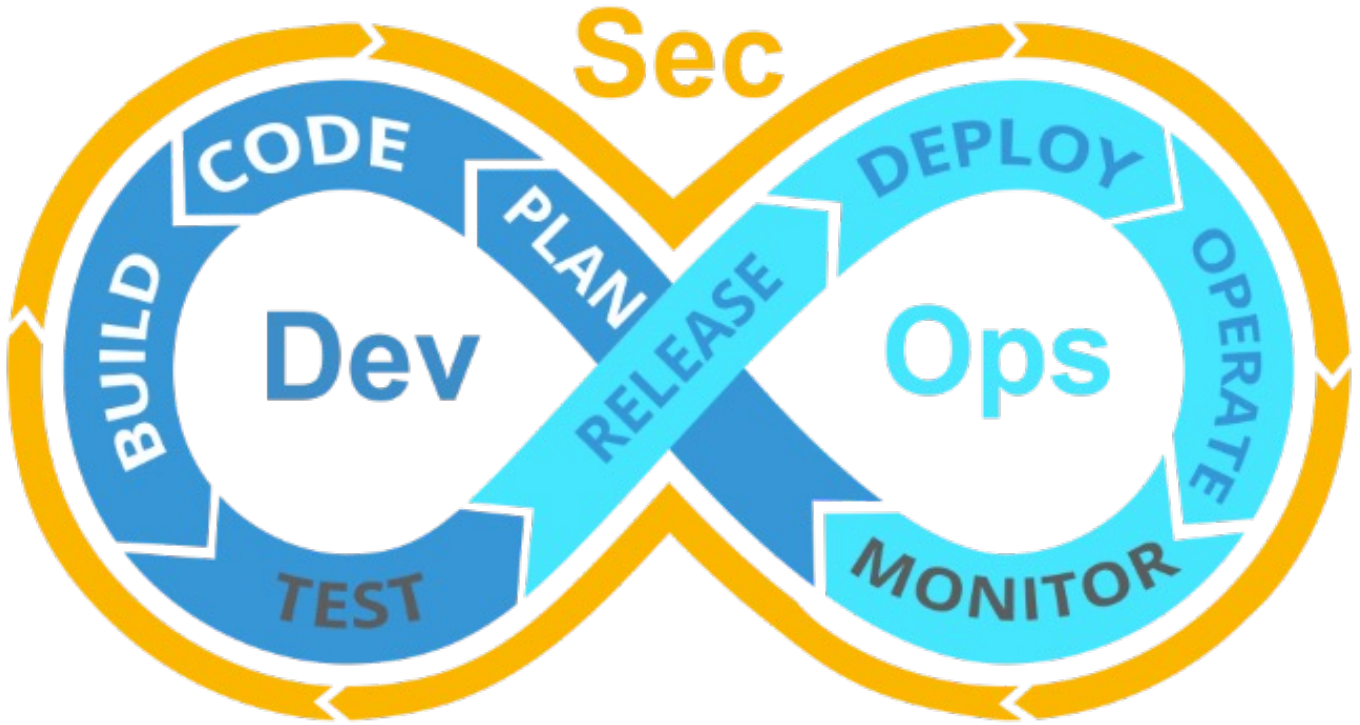
掃描結果影響因素

- 誤判原因
  - 系統為unix-like卻掃出IIS漏洞。
  - 自行建置系統(port:10000)卻檢測出webadmin問題。
- 網路環境架構的影響(如防火牆影響、NAT環境影響)
  - 無法跨越NAT。
  - 防火牆只開放21、22和80 port。

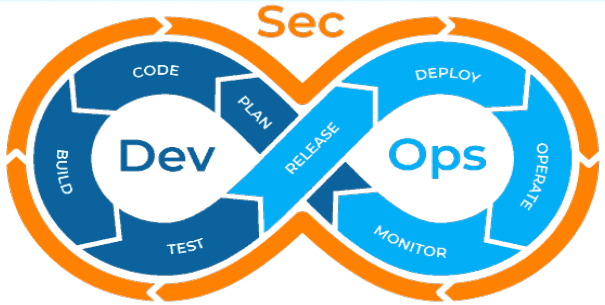
TWCSA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

網站應用程式安全

從 Dev 到 Ops 結合 Sec



思考未來的挑戰- DevSecOps



開發 + 維運 + 資安

- 以「**資安**」拉近「**開發**」與「**維運**」的邊界
- 提供「**開發**」與「**維運**」需要的「**資安**」工具與方法
- 建立以「**資安**」為基礎的「**開發**」與「**維運**」的作業流程

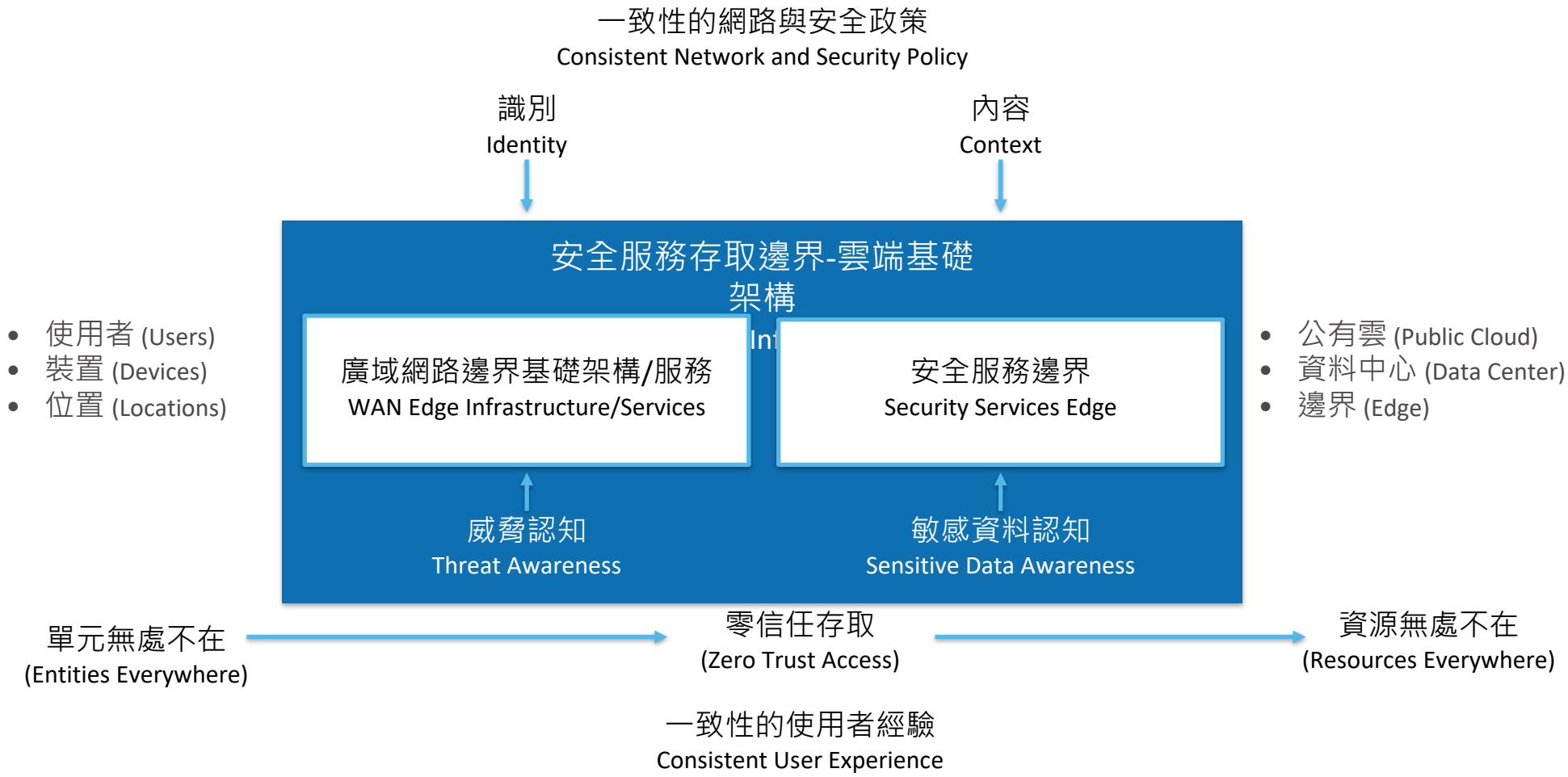
	準備階段	設計階段	建構階段	部署階段	執行階段
	資產、威脅模型、風險評估、量化	評估現有資安架構、存取控制、機敏資訊管理方法等	靜態掃描、程式碼安全檢測	環境互動測試、第三方函式庫測試、動態測試、安全配置	監控、自我保護、威脅偵測與應變、整合至維運管理作業
工具與方法	• 風險評鑑 • 採用國際慣用之評估模型 • 現行資安架構可能的風險	• 選擇適合的程式開發與設計工具 • 確定機敏資訊的保護機制 • 盤合網路與系統的存取控制機制	• 程式碼安全檢測 (Checkmarx等) • 開源程式碼安全檢測 (WhiteSource等)	• 應用服務平台弱點檢測 (Burp Suite、OWASP ZAP等) • 系統安全弱點檢測(Kali、Nessus	• 全天候資安維運中心 (SOC) • 資安智能監控平台(IBM Qradar等) • 應用程式安全弱點與威脅監控

零信任的時代

- 典型的資訊架構無法滿足現有資訊服務的需求
- 資安威脅與日俱增，打破傳統的防禦思維
- 行動化、數位化、虛擬化的世代
- 關鍵基礎設施的防護成為關鍵
- 對於任何的連線來源與請求，都必須審慎首待
- 應用軟體已成為資安防禦的邊界
- 新型態的攻擊手法與資訊服務架構，帶來新的資安問題

TWCSA 台灣數位安全聯盟 Taiwan Cyber Security Alliance

安全服務存取邊界 (SASE)



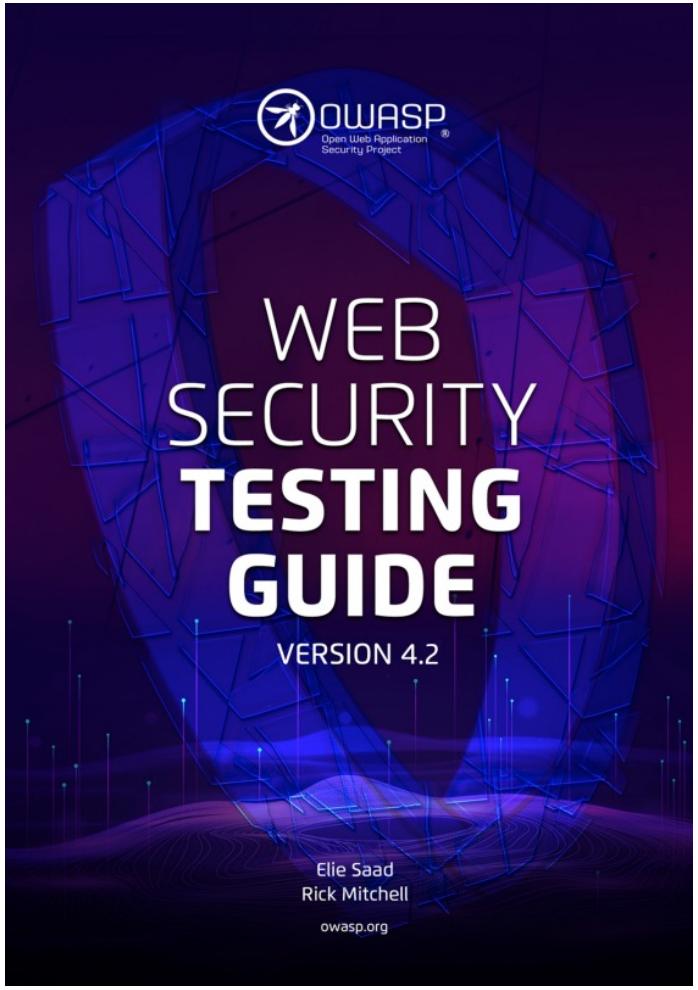
*SASE=Secure Access Service Edge

OWASP 簡介

OWASP(Open Web Application Security Project)為全球主要針對開放網頁應用程式安全進行研究的非營利組織，目前已有超過 45,000 名的志願參與者，針對頁應用程式相關的資安問題，進行關鍵的研究並發佈相關的研究成果，對於現今以網頁程式運作為主的資訊環境，更顯得 OWASP 正扮演著舉足輕重的角色；於 2017 年 OWASP 重新啟動台灣分會的運作，希望以更積極主動的方式，將國際間的熱鬧資安議題，以及研究的成果，透過社群活動、大型會議等方式，分享給國內的參與者，OWASP 台灣分會依循全球一致的原則，以中立的角色連結產管學研界，希望凝聚國內資安社群的能量，以接軌國際資安社群，能夠同步發佈全球已公開的研究資料，將有助於改善與提昇國內的資安防禦技能與產業環境。

企業主要面臨的資安威脅

- COVID-19 全球疫情帶來企業營運模式轉變
- 資訊科技發展快速，大量使用雲端應用服務平台
- 資安認知不足，層出不窮的資安事件
- 資訊系統弱點，造成營運資料外洩
- 數位轉型未審慎思考資安風險
- 典型資安防禦機制，無法因應企業轉型需求

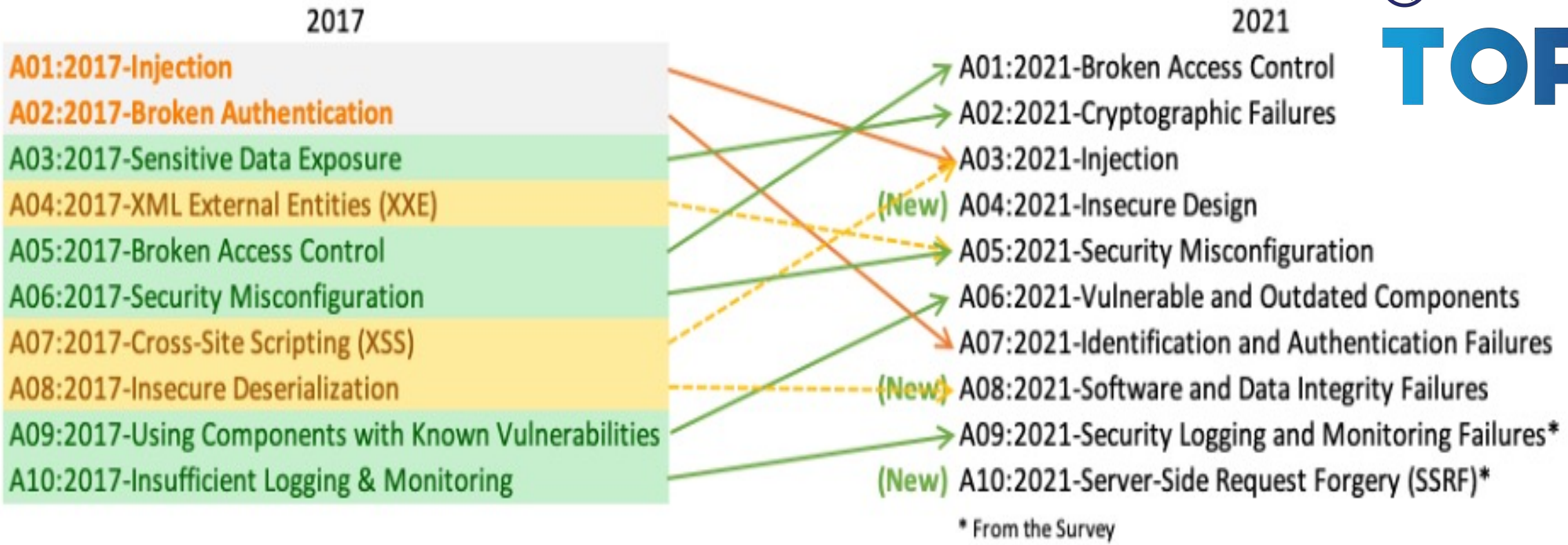


https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

OWASP Top 10 : 2021

- A01 權限控制失效
- A02 加密機制失效
- A03 注入式攻擊
- A04 不安全設計
- A05 安全設定缺陷
- A06 危險與過舊的元件
- A07 認證與驗證機制失效
- A08 軟體及資料完整性失效
- A09 資安紀錄及監控失效
- A10 伺服器請求偽造

OWASP Top 10 : 2021



https://owasp.org/www-project-top-ten/

如何正確的使用 OWASP Top 10

- OWASP Top 10 最主要是一個提升意識及資安認知形態的文件。
- 但是，從 2003 年開始，這並沒有讓任何的企業或組織停止使用它當作預設的應用安全標準。
- 如果你想要用使用 OWASP Top 10 當作程式設計或是驗證測試的一個標準，要先知道這只是一個最低限度的指標並且也只是一個開始。

使用案例	OWASP Top 10 2021	OWASP 應用安全驗證標準 (ASVS)
認知性	是	
教育訓練	基礎	完整
設計及架構	偶爾	可以
程式標準	最低限度	可以
安全程式驗證	最低限度	可以
同行評審清單	最低限度	可以
單元測試	偶而可以	可以
整合測試	偶而可以	可以
滲透測試	最低限度	可以
支援工具	最低限度	可以
安全供應鏈	偶而可以	可以

鼓勵任何希望能套用應用安全標準的人可以利用 OWASP 應用安全驗證標準（ASVS），因為它本身的設計就是可被測試及驗證的，並可以在安全軟體開發生命週期的所有階段都可被運用。

感謝 OWASP 台灣分會社群志工

OWASP Top 10:2021 | OWASP/Top10 ☆2.9k 636

OWASP Top 10:2021

首頁

注意事項

OWASP 2021 介紹

如何正確使用 OWASP Top 10 為標準

如何使用 OWASP Top 10 啟動 AppSec

OWASP 相關

Top 10:2021 名單

A01 權限控制失效

A02 加密機制失效

A03 注入式攻擊

A04 不安全設計

A05 安全設定缺陷

A06 危險或過舊的元件

A07 認證及驗證機制失效

A08 軟體及資料完整性失效

A09 資安記錄及監控失效

A10 伺服端請求偽造

下一步

OWASP Top 10 2021 介紹

歡迎來到最新版本的 OWASP Top 10！！OWASP Top 10 2021 是一個全新的名單，包含了你可以列印下來的新圖示說明，若有需要的話，你可以從我們的網頁上面下載。

在此我們想對所有貢獻了他們時間和資料的人給予一個極大的感謝。沒有你們，這一個新版本是不會出現的。**謝謝**。

Top 10 for 2021 有什麼新的變化？

這次在 OWASP Top 10 for 2021 有三個全新的分類，有四個分類有做名稱和範圍的修正，並有將一些類別做合併。

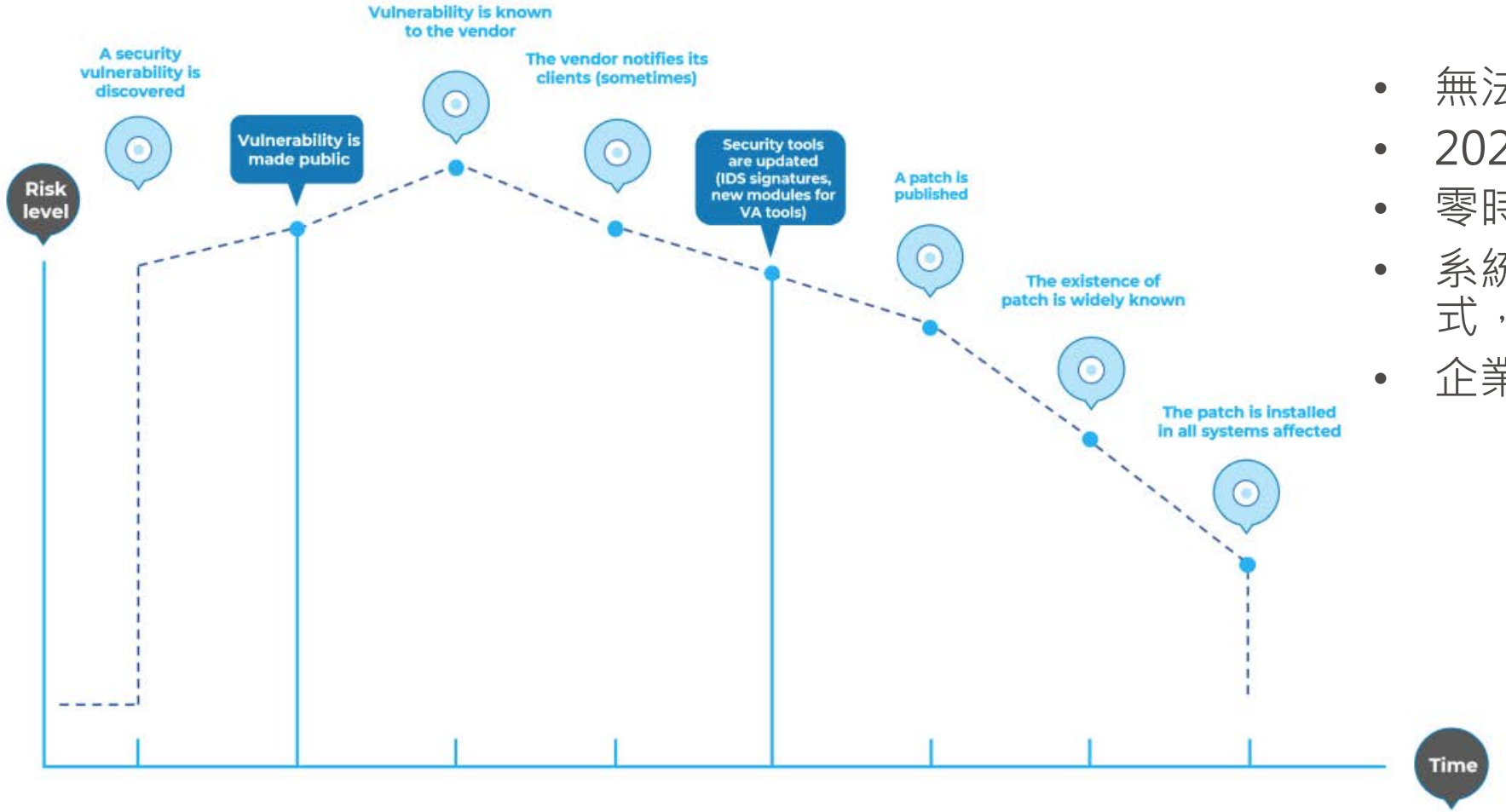
A01:2021-權限控制失效 從第五名移上來; 94% 被測試的應用程式都有驗測到某種類別權限控制失效的問題。在權限控制失效這個類別中被對應到的 34 個 CWEs 在驗測資料中出現的次數都高於其他的弱點類別。

Table of contents

https://owasp.org/Top10/zh_TW/

TWCSA 台灣數位安全聯盟 Taiwan Cyber Security Alliance

談資安弱點與風險控制



- 無法避免隨時可能出現的資安漏洞
- 2021 年的 CVE 弱點超過 4 萬個
- 零時差弱點，提高企業資安風險
- 系統、軟體或設備廠商釋出修補程式，資安風險降低
- 企業面對 2022 的挑戰？

TWCSA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

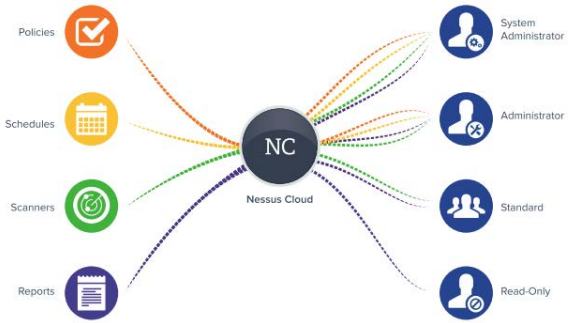
常用的工具

常見掃描工具

- 針對系統服務的弱點評估
  - Nessus ®
  - OpenVAS ®
  - Rapid Nexpose ®
  - MBSA ® …etc.
- Web Application Level
  - HP WebInsepect ®
  - IBM Appscan ®
  - Acunetix ®
  - Nikto …etc.

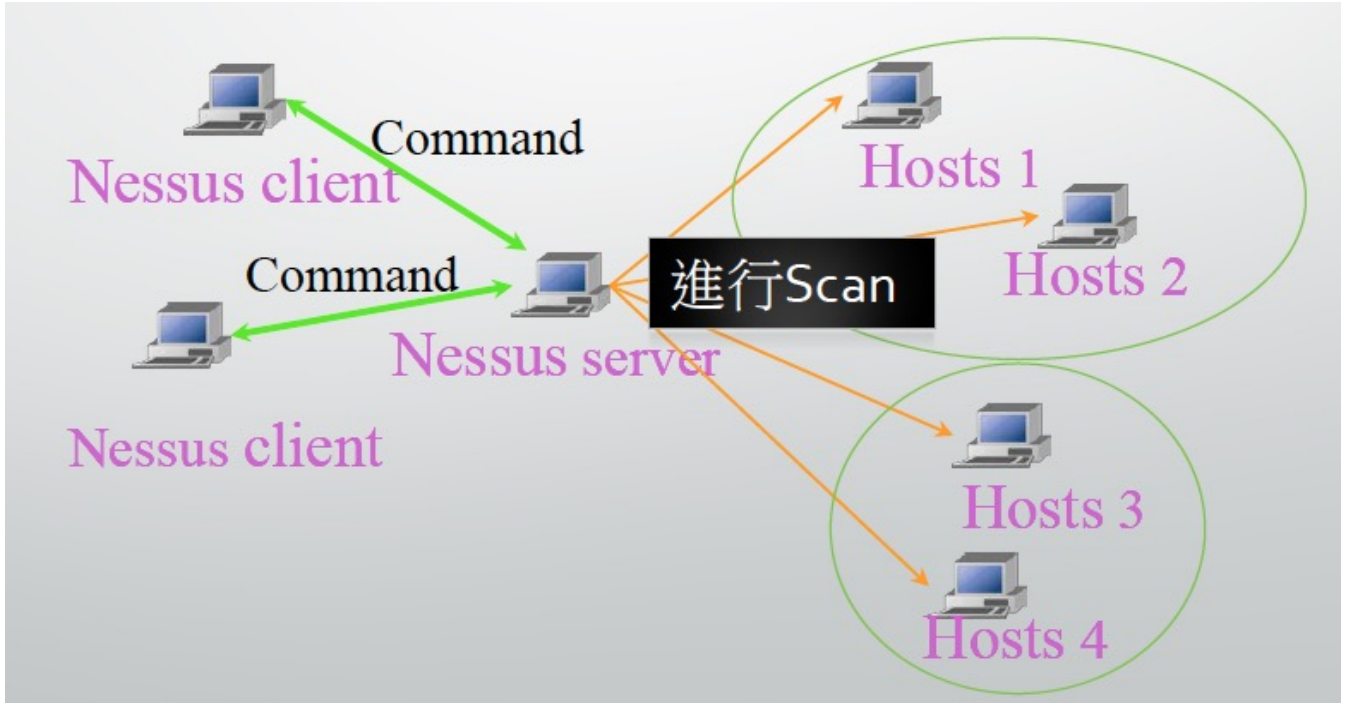
Nessus

- 為一免費的網路安全檢測工具受GPL保護的免費軟體
- 在1998年，由法國的RenaudDeraison發展
- Nessus網頁：http://www.nessus.org/
- 由3.0版本開始不提供原始碼
- 提供弱點特徵資料庫更新免費下載版會慢7天更新弱點資料



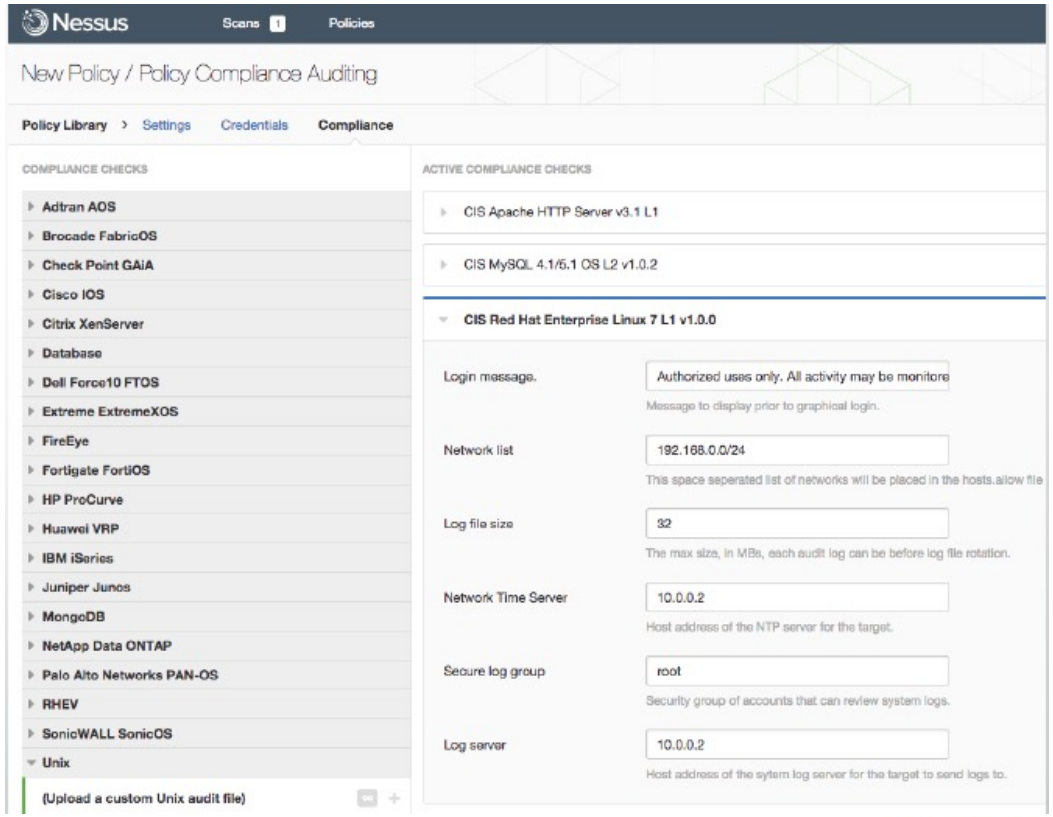
Nessus

- Nessus由兩部份組成Server是真正執行攻擊測試的部份
- Client則是前端介面以作為收集測試結果之用
- **Server與Client亦可安裝於同台主機**



Nessus

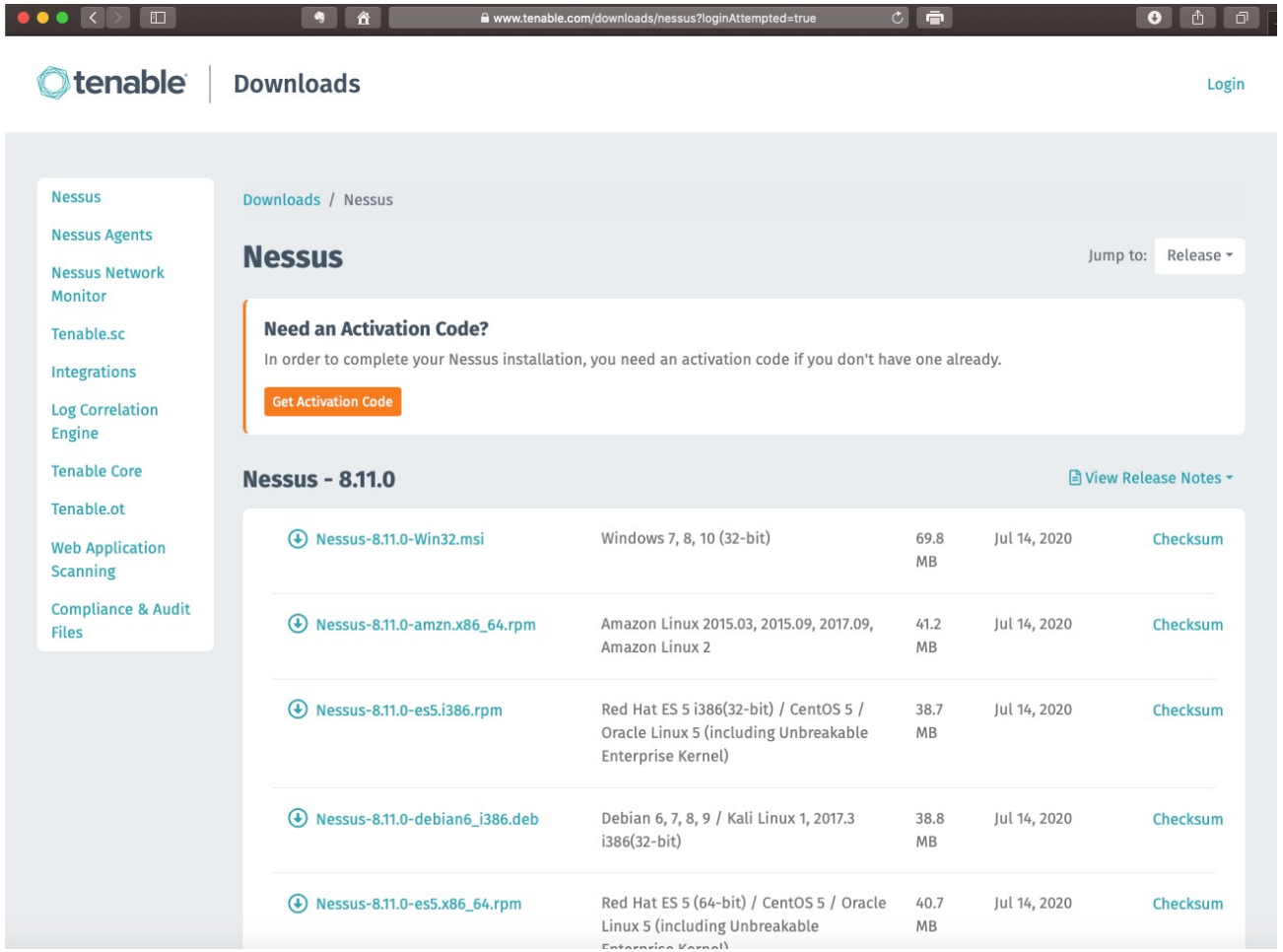
- 從弱點報告中可獲得一些資訊，包含
  - 弱點的種類
  - 弱點簡介
  - 弱點評分
  - 修補方式

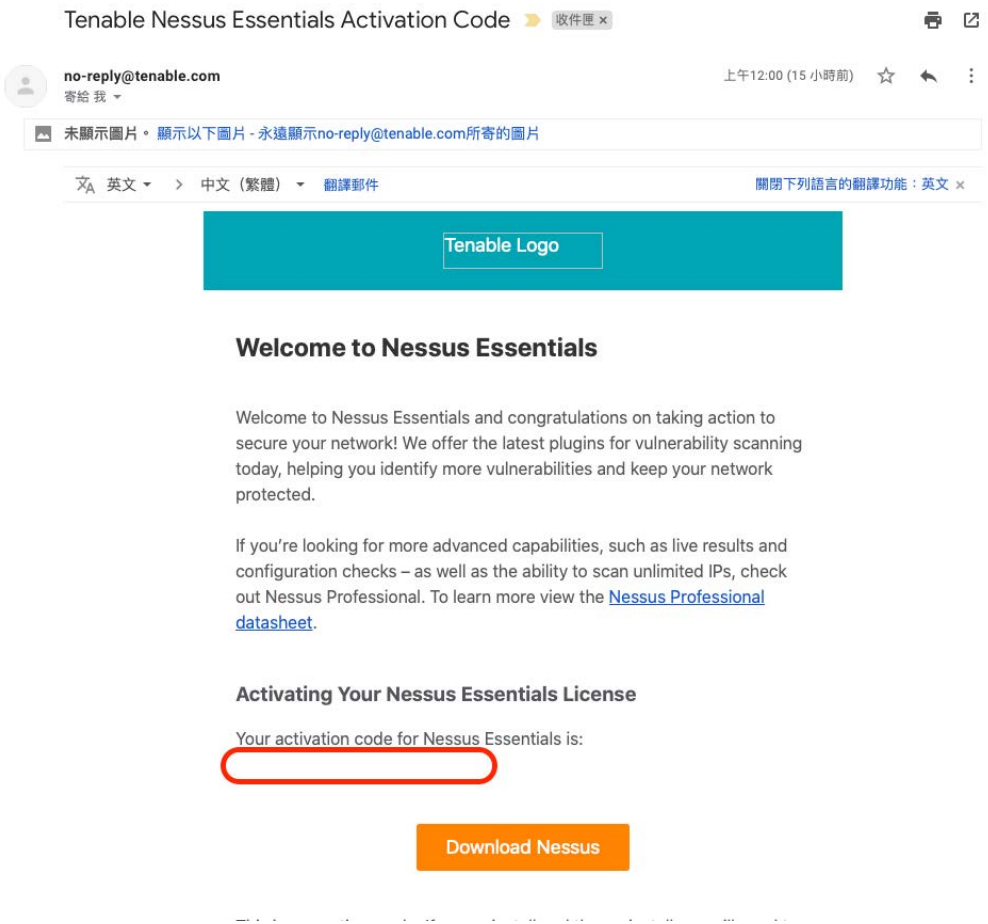


資料來源：Nessus官方網站
http://www.nessus.org

Nessus工具介紹-安裝方式

Nessus工具介紹-安裝方式

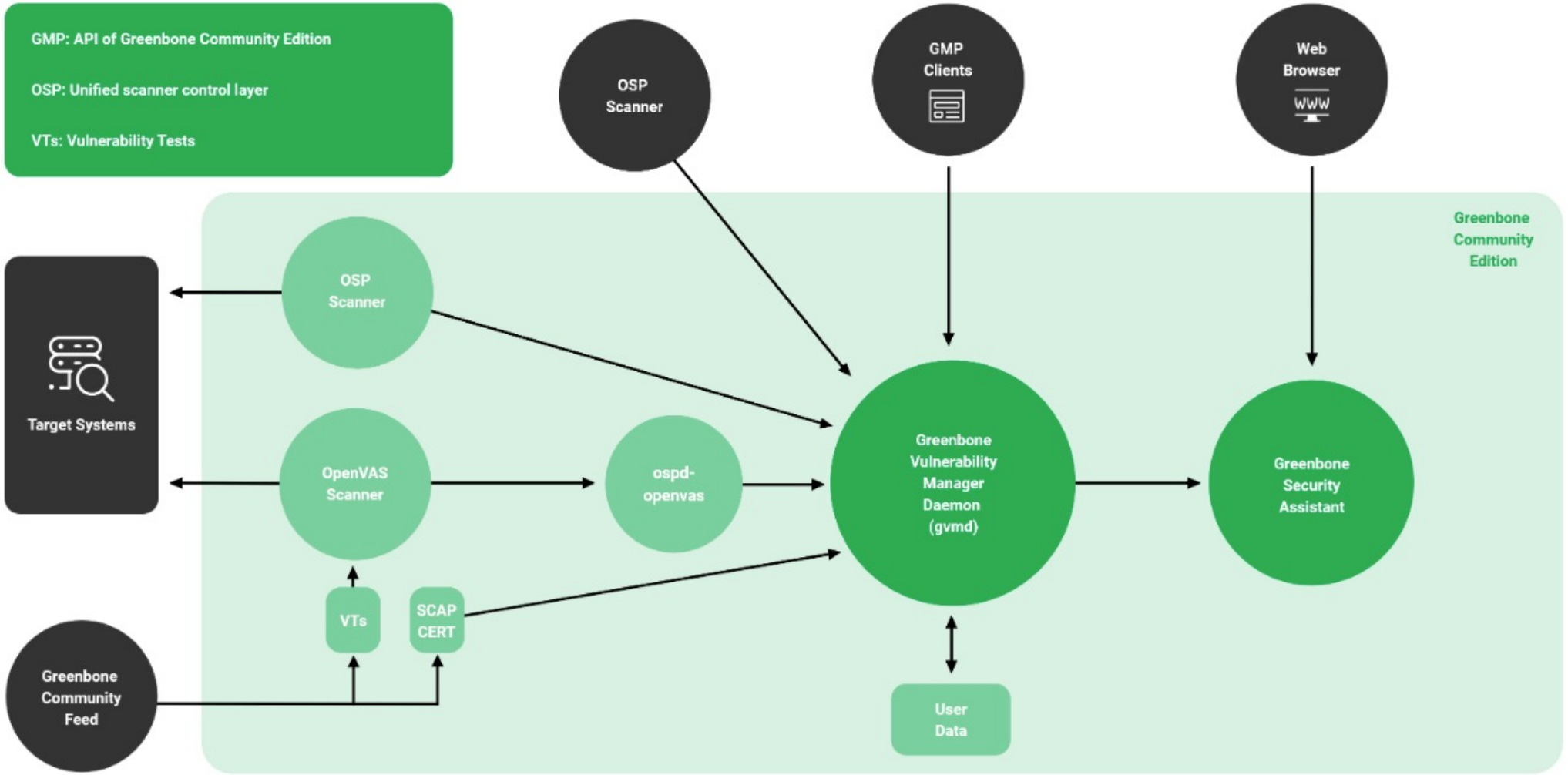




OpenVAS

- OpenVAS 為一套全面且強大的漏洞掃描及管理解決方案的一個框架
- OpenVas 是使用 Nessus 2 為基礎發展的開放原始碼弱點掃描軟體。
- 弱點資料庫：NVTs(Network Vulnerability Tests)
  - 由Greenbone負責維護
  - 目前數量已超過50000個

OpenVAS 架構


GMP: API of Greenbone Community Edition
OSP: Unified scanner control layer
VTs: Vulnerability Tests
OSP Scanner
GMP Clients
Web Browser
Greenbone Community Edition
OSP Scanner
Target Systems
OpenVAS Scanner
ospd-openvas
Greenbone Vulnerability Manager Daemon (gvmd)
Greenbone Security Assistant
VTs
SCAP CERT
Greenbone Community Feed
User Data

Greenbone Security feed

- https://www.greenbone.net/en/security-feed/
  - Content: Thousands of Network Vulnerability Tests (NVTs) as well as compliance rule sets
  - Started: 2008
  - Security: Encrypted and signed
  - Transfer: Optimized synchronization
  - Update: Daily
  - Access/Support: Greenbone Subscription

TWCSA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

弱點掃描報告解讀

Workshop’s Time

- 請解讀課堂上所提供的弱點掃瞄報告，並完成指定任務。

台灣數位安全聯盟
Taiwan Cyber Security Alliance

www.twcsa.org
service@twcsa.org