

# 網站安全檢測實務

蔡一郎



# Google Me.

## 現任

- ✓ 來毅數位科技股份有限公司 資安長
- ✓ 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
- ✓ 台灣資訊暨資安服務聯盟 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公會 資安顧問/資安工作小組委員
- ✓ InfoSec Taiwan 國際資安組織大會 創辦人、大會主席
- ✓ 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
- ✓ 政府部會資安稽核委員
- ✓ 自由作家，資訊圖書著作 37 本，技術專欄文章 100+ 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、ISO 42001 LAC、CSA STAR Auditing、CCSK、CMMC Essential、CSM



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

- ✓ 微智安聯股份有限公司 創辦人兼執行長
- ✓ 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
- ✓ 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

# 課程大綱

- 解析常見的系統與網站弱點
- 實務操作有效防禦策略
- 網站弱點檢測工具與報告解讀

# 課程目的

本課程將著重在網站應用服務，探討相關的安全性議題，介紹OWASP Top 10 2021所挑選出來的十大風險，同時搭配Lab實作環境學員學習如何評估一個網站的安全性，探討如何做好基本的網站應用程式安全防範，以降低網站被入侵的風險。

## ● 課程涵括

- 網頁攻擊手法介紹
- OWASP Top 10 2021
- 網頁檢測工具介紹與操作
- 網頁弱點分析實戰

# 常見的系統與網站弱點





```
23:07:51 amun.events New attack from Moscow, Russia (55.75, 37.62) to Taiwan (23.50, 121.00)
23:07:52 cowrie.sessions New attack from Alblasterdam, Netherlands (51.87, 4.66) to Taiwan (23.50, 121.00)
23:07:52 amun.events New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:52 amun.events New attack from Guayaquil, Ecuador (-2.17, -79.90) to Taiwan (23.50, 121.00)
23:07:53 amun.events New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:53 amun.events New attack from Hanoi, Vietnam (21.03, 105.85) to Taipei, Taiwan (25.05, 121.53)
23:07:53 cowrie.sessions New attack from Macroom, Ireland (51.90, -8.95) to Taiwan (23.50, 121.00)
23:07:53 cowrie.sessions New attack from Macroom, Ireland (51.90, -8.95) to Taiwan (23.50, 121.00)
23:07:54 amun.events New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:54 amun.events New attack from Guayaquil, Ecuador (-2.17, -79.90) to Taiwan (23.50, 121.00)
23:07:54 amun.events New attack from Caracas, Venezuela (10.50, -66.92) to Taipei, Taiwan (25.05, 121.53)
```

# 常見的網路攻擊流程

## 攻擊流程

**Reconnaissance:**  
被動資料收集

**Scanning:**  
掃描目標, 了解目標主機配置狀態與弱點對應

**Gaining Access:**  
獲得權限

**Maintaining Access:**  
維持存取權限(如後門或木馬)

**Clearing Tracks:**  
破壞足跡的完整性, 並把自己藏在正常行為中

## 2024年重大資安事件回顧 超過10億筆個資外洩

• 2024-10-15

編譯／Cynthia

2024年成為全球資料外洩事件的高峰期，超過10億筆資料遭駭客竊取，創下歷史新高。駭客手法日趨複雜，從網路釣魚到勒索軟體、憑證盜用，幾乎無孔不入，許多企業和機構的資安防護無法應對，導致頻繁的重大外洩事件，不論是科技大廠、通訊業者，還是醫療及金融機構，無一倖免，資料外洩對全球各行各業及個人安全產生重大影響，除了損害企業聲譽，更對個人隱私造成無法估量的損失。



今年成為全球資料外洩事件的高峰期，超過10億筆資料遭駭客竊取，創下歷史新高。(圖／123RF)

## 獨家 / 每個人都是受害者！全國戶籍資料外洩案內政部調查進度曝光

三立新聞網

2024年11月26日

2022年10月，有媒體曝光我國戶籍資料被放到暗網販售，並查證該資料為真。為此，台灣人權促進會於2024年3月15日前往台北高等行政法院，對內政部提起請求公開個資外洩相關政府資訊的行政訴訟，盼法院能基於機關違法，要求內政部公開戶役政系統介接現況等資訊。今(26)日首度開庭，消息人士透露，內政部指該案「尚在調查中，尚未偵結」。

2022年10月，我國2300萬筆戶籍資料被放到暗網上販售，經調查，除名字被亂數竄改之外，該資料為2018年我國戶役政資料，當時全立法院立委都收到自己家庭個資，就連當時數發部長唐鳳、現任總統賴清德等相關戶籍資料都清楚登載，引發爭議，連帶政府也日益重視個資法，並於2023年修改個資外洩罰則，但是對公部門外洩國人個資的進度、懲處幾乎從未曝光。

在內政部遭台灣人權促進會告上法院後，今(26)日首度開庭，由於許多民眾以為本案歷時甚久，且司法機關還掌握收款帳戶人身份，以為已經簽結，但是消息人士向《三立新聞網》透露，內政部尚在偵查中。

回顧該案，由於戶籍案自2022年10月，出現網站公開兜售2300多萬筆台灣人個資以來，內政部從未向社會大眾舉體說明哪些公、私部門曾參與介接台灣國人的戶役政個資。非政府組織，台灣人權促進會認為，該次個資外洩規模幾乎涵蓋全體國民，資料詳細程度更包含身分證字號、姓名、家庭成員、戶籍、原住民族身分、兵役別、遷入時間等，理應為內政部管理之戶役政系統內的個資。

## 臺藝大校友網站個資驚傳外洩，校方緊急關閉網站、請求Google協助清除暫存內容

本週臺灣藝術大學發出資安公告，指出他們的校友聯絡中心網站存在資安問題，任何人透過Google搜尋就有機會看到申請校友證的個資，他們緊急將網站關閉，並對於含有機敏個資的中級系統，全面進行弱點掃描

文/ 周峻佑 | 2024-05-24 發表

讚 56

分享



國立臺灣藝術大學 National Taiwan University of Arts | 校友聯絡中心 Alumni Association Center

### 【重要公告】

因本校校友聯絡中心網站出現資安相關問題  
現已暫時關閉

校友證申辦服務請掃描左方QR Code，  
加入臺藝大校友聯絡中心LINE官方帳號，  
由專人為您一對一服務。

服務時間 | 每週一至週五上午9:00至下午5:00  
服務專線 | 02-8969-7523



2024 iThome 鐵人賽

加入 2024 iThome 鐵人賽

從 8 / 1  
開始報名

不要錯過!

Share More Games

## 長榮航空證實資料外洩，不明人士存取逾300名旅客個資

長榮航空證實有不明人士存取388筆旅客資料，但究竟對方如何取得旅客的帳號？該公司表示不清楚

文/ 周峻佑 | 2024-04-26 發表

讚 15

分享

本資料由 (上市公司) 2618 長榮航 公司提供

序號	1	發言日期	113/04/25	發言時間	23:04:03
發言人	陳耀銘	發言人職稱	公共關係室副總經理	發言人電話	02-25001122
主旨	本公司發生網路資安事件				
符合條款	第	26	款	事實發生日	113/04/25
說明	1. 事實發生日: 113/04/25 2. 發生緣由: 本公司監控發現有不明人士利用不明來源之旅客資訊，透過惡意IP登入本公司官網，並有388筆旅客資料可能遭不當瀏覽；包含姓名、行程及聯絡資訊等個資，不含信用卡資訊。 3. 處理過程: 本公司內部發現此狀況後，已立即依公司程序應變，並採取必要的防護措施將影響降到最低。本公司已主動通報相關主管機關，亦會通知可能受影響的旅客。 4. 預計可能損失或影響: 目前評估對公司所有業務均不受影響。				



iThome 鐵人講堂

看直播送好禮

鐵人賽車 鐵人賽艇 鐵人賽馬

抽親筆簽名書

超商購物序號 50-

# HITCON ZeroDay



The screenshot shows the HITCON ZeroDay website. At the top, there is a navigation bar with a logo on the left and links for '漏洞', '消息', '排行榜', '組織', '獎勵計劃', and '人才媒合' in the center. On the right side of the navigation bar, there are links for '註冊 or 登入'. Below the navigation bar, the main content area features a paragraph of text describing the platform's purpose: 'HITCON ZeroDay 是一個讓資安專家通報組織漏洞的可靠平台。一旦 ZeroDay 團隊接獲您的通報，將盡快確認該漏洞之成因及影響，並聯繫該組織有效窗口，在最短的時間內協助組織修正。此外，ZeroDay 平台也將提供漏洞處理進度給通報者，令通報者得以即時了解該漏洞修補的狀況。' This is followed by another paragraph: '我們期待各位的加入及響應，能讓 HITCON ZeroDay 漏洞通報平台成為資安專家和組織間的溝通管道，幫助組織面對、解決資安問題，同時也令組織更加信賴、尊重資安專業人才，一起為更好的資安環境努力。' Below this text is a horizontal line, and then a section titled '特點' (Features). This section contains four circular icons with corresponding text: 1. '資訊開放透明' (Information Open and Transparent) with a document icon, and subtext '處理進度一目了然，修正後將漏洞細節公開' (Processing progress is clear at a glance, details of the vulnerability will be public after correction). 2. '即時狀態通知' (Real-time Status Notification) with a notification icon, and subtext '漏洞及處理狀態第一時間通知組織及通報者' (Vulnerability and processing status notified to the organization and reporter at the first time). 3. '建立互信關係' (Building Mutual Trust) with a checkmark icon, and subtext '透過中立的平台，累積組織及通報者間信賴' (Through a neutral platform, accumulate trust between organizations and reporters). 4. '資安人才媒合' (Cybersecurity Talent Matching) with a group of people icon, and subtext '組織將來可透過平台，徵求到更多資安人才' (Organizations can recruit more cybersecurity talent through the platform in the future).

資料來源：HITCON ZeroDay. <https://zeroday.hitcon.org/>

The screenshot shows the Zone-h website interface. At the top is the logo "zone-h unrestricted information" and a navigation menu with links: Home, News, Events, Archive, Archive ★, Onhold, Notify, Stats, Register, Login, and a search bar. The main content area features an article titled "Dedicated to all the hackers - Pho3nix (Roulette Cinese)" dated 24/03/2014, written by Roberto SyS64738 Preatoni. The article text discusses the conclusion of a Hacker Visual Contest and thanks participants. Below the text is a video player for "roulette cinese - PH03N1X R3M1X" with a play button overlay. To the right of the article are three boxes: "ZONE-H In Numbers" with statistics (News: 4,738, Admins: 3, Registered Users: 162,032, etc.), a "Login" form with fields for username and password, and an "Events" calendar for September 2022.

**zone-h**  
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

### Dedicated to all the hackers - Pho3nix (Roulette Cinese)

24/03/2014 Written by Roberto SyS64738 Preatoni

We finally concluded the Hacker Visual Contest through which we collected videoclips and artwork from the hacker world which we used to assemble the official videoclip for the song "Pho3nix" (Roulette Cinese) dedicated to the hacker world.  
I feel obliged to thank all of the participants, credits are added at the end of the clip with a special mention to Christan Milani for the outstanding remix, to Roberto "SyS64738" Preatoni for promoting the idea throughout the hacker world and to Gianluca Zenone aka Alex Dreiser for the videoclip realization.  
Thanks again to all of you and... enjoy the clip.

Joe Raggi (Roulette Cinese)  
(for what is worth: <https://itunes.apple.com/it/artist/roulette-cinese/id286575097>)

roulette cinese - PH03N1X R3M1X

10730 複製連結

到以下平台觀看 : YouTube

### ZONE-H In Numbers

News: **4.738**  
Admins: **3**  
Registered Users: **162.032**  
Early Warning subscriptions: **8032**  
Digital Attacks: **15.035.399**  
Attacks On Hold: **476.602**  
Online Users: **134**

### Login

Login :   
Password :

### Events

< September 2022 >

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

# 我的密碼沒加密

ZD-2022-00647 發信 台灣電力公司

## [Bounty] 台灣電力公司 不安全的忘記密碼功能

不安全的忘記密碼功能

### 處理狀態

公開  
Last Update : 2022/11/01

- 新提交
- 已審核
- 已通報
- 已修補
- 已複測
- 公開



### 修補建議

1. 禁止使用密碼提示功能。改以使用第三方管道，例如透過 email 驗證來重設密碼
2. 禁止將使用者密碼以明文儲存在伺服器上

# Awesome-Web-Hacking

README.md

## awesome-web-hacking

This list is for anyone wishing to learn about web application security but do not have a starting point.

You can help by sending Pull Requests to add more information.

If you're not inclined to make PRs you can tweet me at `@infoslack`

### Table of Contents

- [Books](#)
- [Documentation](#)
- [Tools](#)
- [Cheat Sheets](#)
- [Docker](#)
- [Vulnerabilities](#)
- [Courses](#)
- [Online Hacking Demonstration Sites](#)
- [Labs](#)
- [SSL](#)
- [Security Ruby on Rails](#)

<https://github.com/infoslack/awesome-web-hacking>

# 弱點的起因

- 實作階段 (Implementation Phase)
  - 輸入驗證的錯誤(Input validation error)
    - 沒有檢查輸入值的資料 (例如：SQL Injection)
  - 界限(範圍)檢查的錯誤(Boundary check error)
    - 未正確檢查傳入資訊的長度，導致緩衝區溢位 (Buffer Overflow)或程式計算錯誤
  - 競爭情況(Race condition)
    - 指多個行程(Process)並行存取共用資源，系統若 做好排程將可能造成資源內的資料不正確
- 操作階段 (Operation Phase)
  - 錯誤的設定與疏忽
    - 未正確設定檔案權限，導致攻擊者可以存取隱私資訊相關檔案
  - 系統設定或操作的知識不足

# 弱點的起因

- 人性弱點 (Human Nature)
  - 脆弱的密碼(Weak Passwords)
    - 密碼與使用者帳號相同
    - 生日或學號
    - 太過簡單的密碼 (例如：12345)
  - 不良的使用習慣(Unsafe habits)
    - 將密碼告訴別人 (共用同一組密碼?)
    - 寫下貼在螢幕或桌面 (ISMS?)

# 弱點掃描流程

- 主機探索
- 連接埠掃描
- 系統服務確認
- 漏洞檢測
- 產出安全評估報告

# 弱點的等級與定義

- 嚴重(Critical)
  - 利用該弱點可以進行大量的散佈與感染，例如：網蟲的行為
- 重要(Important)
  - 利用該弱點可能攻陷電腦，竊取使用者資訊或造成機敏資料外洩等
- 中度(Moderate)
  - 該弱點的利用需在特定條件下，例如：預設設定、不安全的設定、難以達成的參數等，如果沒有該特定條件配合，則弱點無法利用或可能減輕弱點的影響力
- 低(Low)
  - 該弱點的利用是相當困難或影響程度比較小

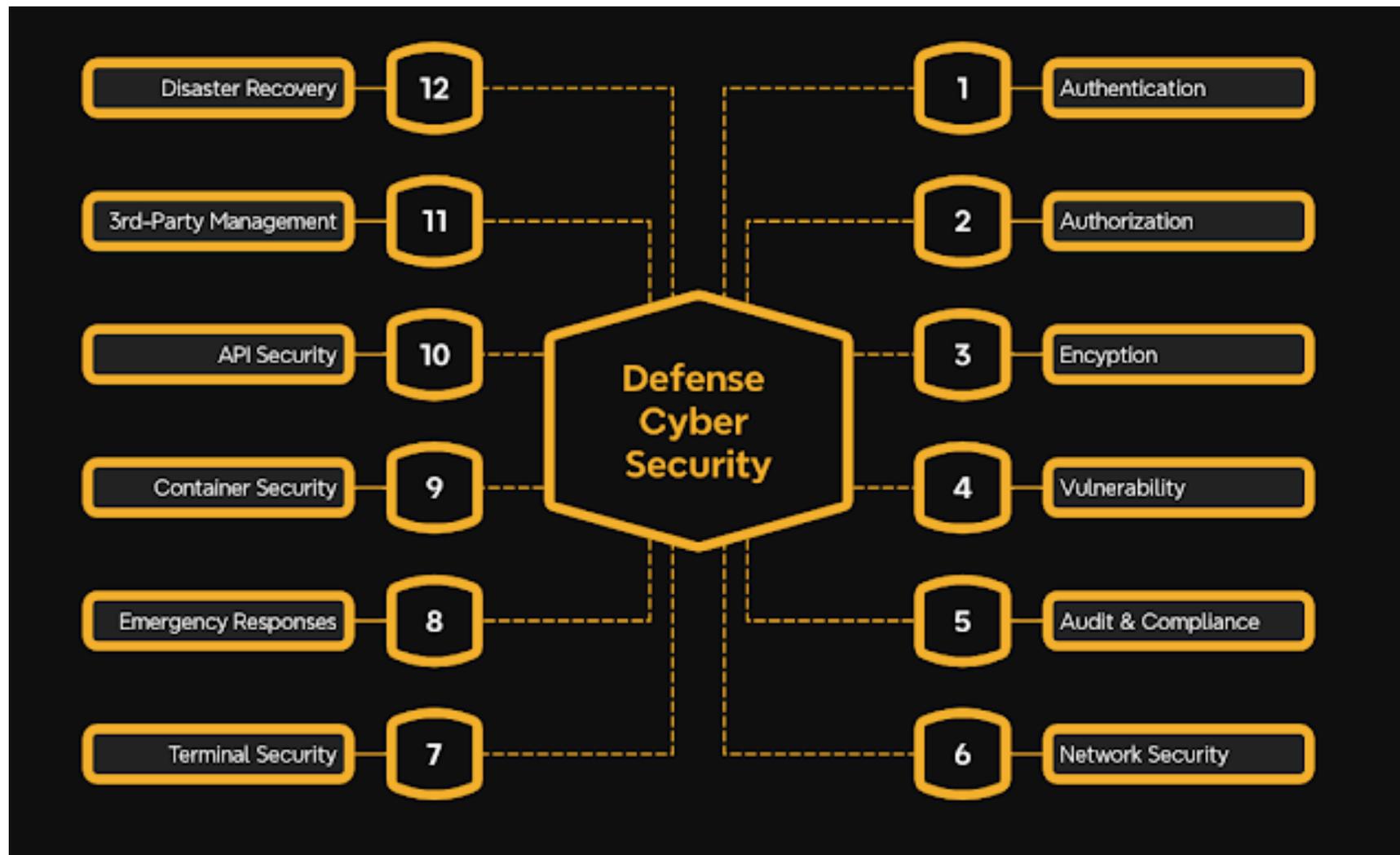
# 通用弱點與漏洞編號

- Common Vulnerabilities & Exposures
  - 訂定一個唯一的名稱
  - 提供一個標準的描述
  - 使評估報告更容易被理解與解讀
- CVE編號格式 (CVE-XXXX-XXXX)
  - 第一組數字表示年度
  - 第二組數字表示該年度被發現的序號

# 弱點掃描與滲透測試的差異

- 滲透測試
  - 以駭客的角度來進行各種攻擊測試
  - 可能發現潛在的漏洞
- 弱點掃描
  - 針對已知的弱點進行檢測
  - 可藉由自動化的工具來大幅減少檢測的時間
  - 誤判率較高

# 資訊安全的十二個面向



- 目前應該要思考的十二個面向，如何進行企業所需要的資訊安全防禦，
- 而這些不同的面向仍然會因為企業的屬性、使用的平台以及商業模式的不同，而有不同的權重比例
- 從 ESG 角度思考企業資安管理已成未來的趨勢

# 實務操作有效防禦策略

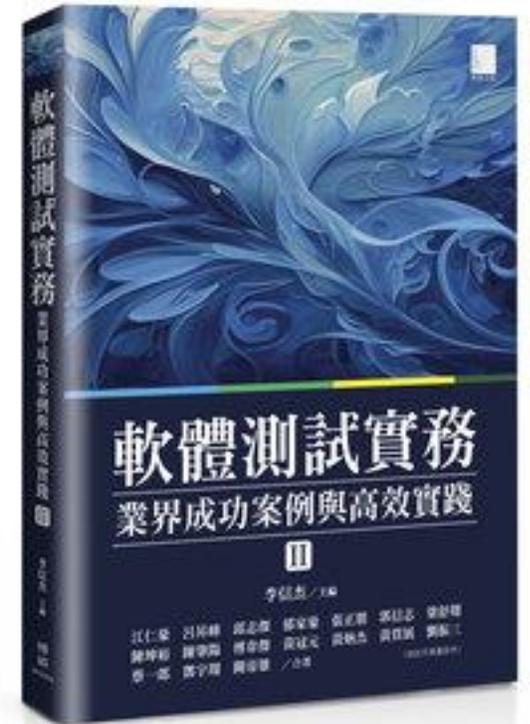
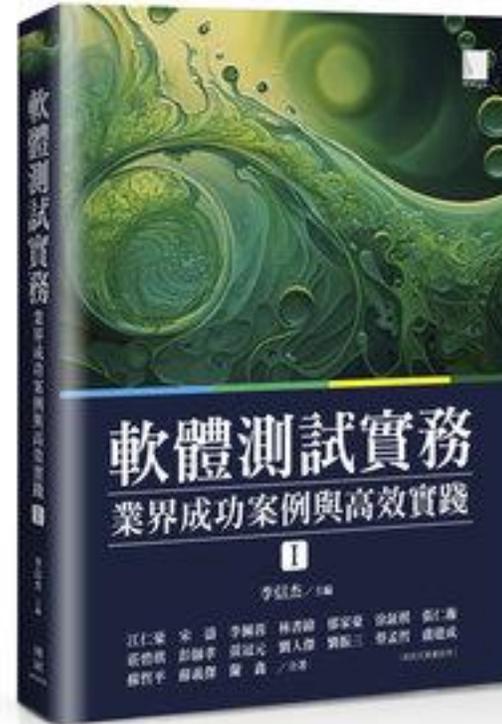


# 從兩本「軟體測試實務」的撰寫談起...

我們都知道  
應用程式安全很重要！

軟體測試是確保軟體品質與安全的重要手段。然而，現代軟體市場激烈競爭與開發迭代速度加快，對軟體測試的效率與效果提出了更高的要求。軟體測試領域知識與主題繁多，且由於測試品質常仰賴施測者的實務經驗，較缺乏測試經驗的人難以入門。因此，本書設計的精神即為幫助讀者「參考業界成功經驗，快速實踐軟體測試」，期望透過本書有效地分享業界寶貴的軟體測試成功經驗，加速國內專業軟體測試人才的培育，提高軟體品質和安全水準。

~主編 李信杰



# 常見的弱點掃描工具(Host)

- Nessus (<http://www.tenable.com/products/nessus>)
- Nexpose (<http://www.rapid7.com/products/nexpose/>)
- Openvas (<http://www.openvas.org/>)





## Downloads

[Nessus](#)

[Nessus Agents](#)

[Nessus Network Monitor](#)

[SecurityCenter](#)

[Log Correlation Engine](#)

[Tenable Virtual Appliances](#)

[Industrial Security](#)

[Web Application Scanning](#)

[Compliance & Audit Files](#)

## Nessus

Binary download files for Nessus Professional, Nessus Manager, and connecting Nessus Scanners to Tenable.io & SecurityCenter.

Releases ▾

### Nessus - 7.0.3 📄

#### Release Date

03/14/2018

#### Release Notes:

[Nessus 7.0.3](#)

Name	Description	Details
 <a href="#">Nessus-7.0.3-x64.msi</a>	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	<a href="#">Checksum</a>
 <a href="#">Nessus-7.0.3-es5.i386.rpm</a>	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	<a href="#">Checksum</a>
 <a href="#">Nessus-7.0.3.dmg</a>	macOS (10.8 - 10.13)	<a href="#">Checksum</a>
 <a href="#">Nessus-7.0.3-debian6_i386.deb</a>	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	<a href="#">Checksum</a>



Free Trial

Sign In

About For Customers

[Home](#) // [Products](#) // [Nexpose](#) // [Download](#)

## Free Vulnerability Scanner Trial

### Get full functionality of InsightVM or Nexpose for 30 days

Vulnerabilities pop up all the time. You need constant intelligence to discover them, prioritize them for your business, and confirm your exposures have been fixed. Rapid7 offers two core vulnerability management products to help you do this: InsightVM and Nexpose.

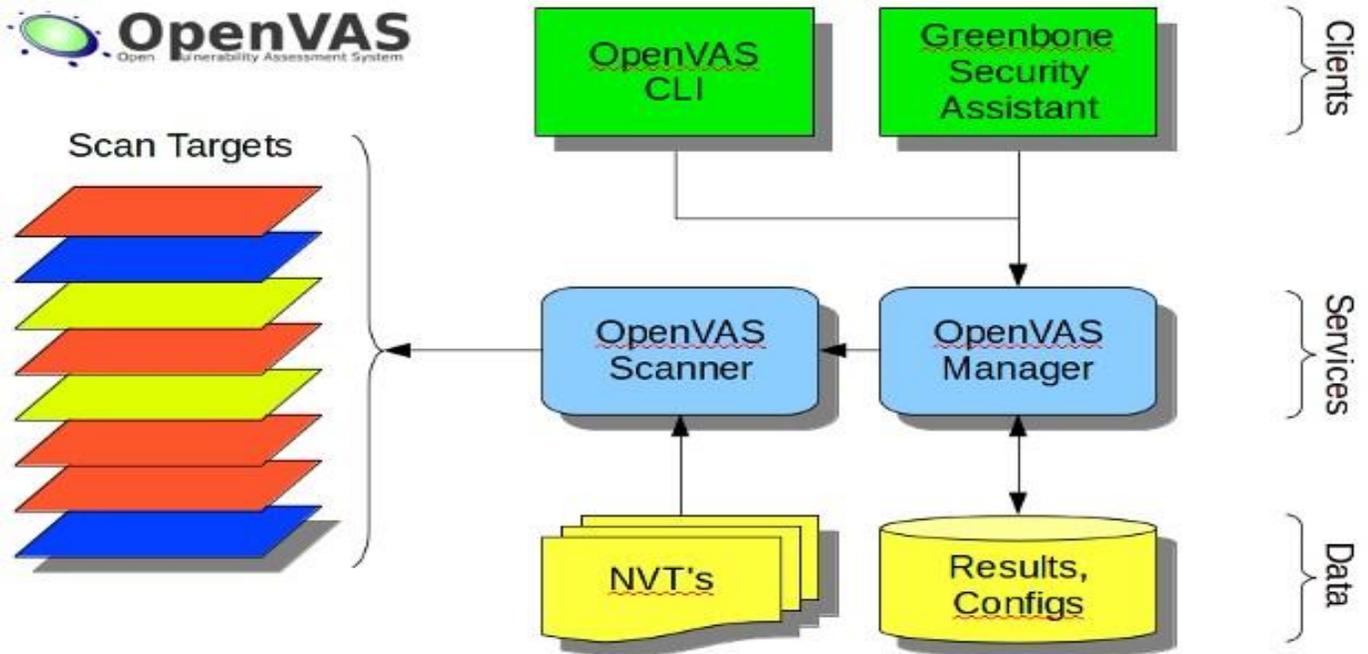
Our original vulnerability scanner, Nexpose, is an on-premise solution for all size companies.

# OpenVAS (Free)

The screenshot shows the OpenVAS website with a navigation menu (About, Try out, Support, Development, Contact), a 'Download OpenVAS/Greenbone' button, a cartoon character, a system architecture diagram, and a 'News' section listing releases from 2014 to 2017.

## The world's most advanced Open S scanner and manager

OpenVAS is a framework of several services and tools offering a comprehensive vulnerability management solution. The framework is part of Greenbone N solution from which developments are contributed to the Open Source con



# OpenVAS (Free)



Refresh every 30 S...

Logged in as Admin **admin** | Logout  
Wed May 16 09:02:51 2018 CST

Scans

Assets

SecInfo

Configuration

Extras

Administration

Help

PDF

Filter:

first=1 rows=100 autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 sort-reverse=severity levels=hmlg



Report: Results (143 of 333)

Done

## Details

1 - 100 of 143

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	172.16.67.49	512/tcp	
Twiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	172.16.67.49	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	172.16.67.49	8787/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	172.16.67.49	1099/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	172.16.67.49	1524/tcp	
OS End Of Life Detection	10.0 (High)	80%	172.16.67.49	general/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	172.16.67.49	3632/tcp	
MySQL / MariaDB weak password	9.0 (High)	95%	172.16.67.49	3306/tcp	
VNC Brute Force Login	9.0 (High)	95%	172.16.67.49	5900/tcp	
PostgreSQL weak password	9.0 (High)	99%	172.16.67.49	5432/tcp	
SSH Brute Force Logins With Default Credentials Reporting	9.0 (High)	95%	172.16.67.49	22/tcp	
DistCC Detection	8.5 (High)	95%	172.16.67.49	3632/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	172.16.67.49	5432/tcp	
Check for rlogin Service	7.5 (High)	70%	172.16.67.49	513/tcp	
phpinfo() output accessible	7.5 (High)	80%	172.16.67.49	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	80%	172.16.67.49	80/tcp	

# 常見的弱點掃描程式(Web Service)

- Acunetix (<https://www.acunetix.com/>)
- WPScan (<https://wpscan.org/>)
- W3af (<http://w3af.org>)
- OWASP ZAP ([https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project))
- Pentest-Tools (<https://pentest-tools.com/>)

The banner features the Acunetix logo in the top left. The navigation menu includes: TRY, BUY, COMPANY, SUPPORT, LEARN, BLOG, a search icon, and a phone icon. The main headline reads: "Is Your Website Hackable? 70% are. Detect and action with Acunetix". Below the headline are two buttons: "Download" and "Online Scan". The background is a blurred city street at night with red light trails. A progress indicator shows the first of five steps is active. Below the banner is a row of eight feature categories: Vulnerability Scanner, Indepth Crawl & Analysis, Highest Detection Rate, Lowest False Positives, Vulnerability Management, WordPress Checks, Network Security, and Advanced Features.

## Online Scanner with Free Network Scans

Rectifying your network security vulnerabilities has never been easier – and now this can be done for FREE with **Acunetix Online**. The Acunetix online scanner performs a full web and network security scan from Acunetix servers. No download or installation is required. The 14-day trial scans for all web vulnerabilities but exact location will not be shown. The Network Security Scan will report full details and remains active for one year. You can scan our test websites to review a sample of web vulnerability scan details.

**i** Minimum 8 characters, containing at least 3 of the following - 1 number, 1 small letter, 1 capital letter

# WPScan

## WPScan

WPScan is a black box WordPress vulnerability scanner.

[View the Project on GitHub](#)

Download  
ZIP File

Download  
TAR Ball

View On  
GitHub

[Follow us on Twitter](#)



This project is maintained by the [WPScan Team](#) which comprises of [@erwan\\_lr](#), [@\\_FireFart\\_](#) & [@ethicalhack3r](#).

# WPScan®

build error coverage not found dependencies up to date docker pulls 55k

## LICENSE

### WPScan Public Source License

The WPScan software (henceforth referred to simply as "WPScan") is dual-licensed - Copyright 2011-2018 WPScan Team.

Cases that include commercialization of WPScan require a commercial, non-free license. Otherwise, WPScan can be used without charge under the terms set out below.

#### 1. Definitions

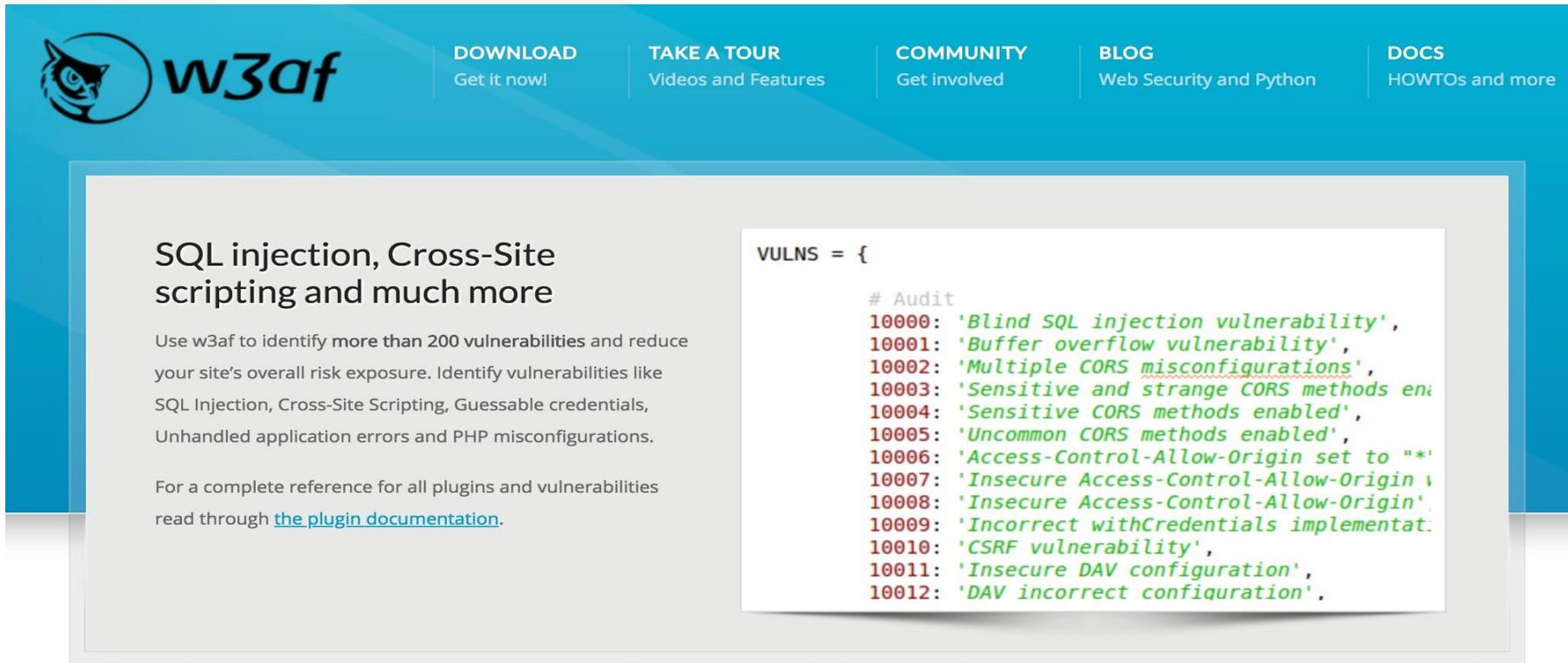
1.1 "License" means this document.

1.2 "Contributor" means each individual or legal entity that creates, contributes to the creation of, or owns WPScan.

1.3 "WPScan Team" means WPScan's core developers, an updated list of whom can be found within the CREDITS file.

#### 2. Commercialization

A commercial use is one intended for commercial advantage or monetary



The screenshot shows the W3af website homepage with a navigation bar and a main content area. The navigation bar includes links for 'DOWNLOAD', 'TAKE A TOUR', 'COMMUNITY', 'BLOG', and 'DOCS'. The main content area features a section titled 'SQL injection, Cross-Site scripting and much more' with a description of the tool's capabilities and a code snippet showing a list of vulnerabilities.

**DOWNLOAD**  
Get it now!

**TAKE A TOUR**  
Videos and Features

**COMMUNITY**  
Get involved

**BLOG**  
Web Security and Python

**DOCS**  
HOWTOs and more

## SQL injection, Cross-Site scripting and much more

Use w3af to identify more than 200 vulnerabilities and reduce your site's overall risk exposure. Identify vulnerabilities like SQL Injection, Cross-Site Scripting, Guessable credentials, Unhandled application errors and PHP misconfigurations.

For a complete reference for all plugins and vulnerabilities read through [the plugin documentation](#).

```
VULNS = {  
    # Audit  
    10000: 'Blind SQL injection vulnerability',  
    10001: 'Buffer overflow vulnerability',  
    10002: 'Multiple CORS misconfigurations',  
    10003: 'Sensitive and strange CORS methods enabled',  
    10004: 'Sensitive CORS methods enabled',  
    10005: 'Uncommon CORS methods enabled',  
    10006: 'Access-Control-Allow-Origin set to "**',  
    10007: 'Insecure Access-Control-Allow-Origin',  
    10008: 'Insecure Access-Control-Allow-Origin',  
    10009: 'Incorrect withCredentials implementat',  
    10010: 'CSRF vulnerability',  
    10011: 'Insecure DAV configuration',  
    10012: 'DAV incorrect configuration'.
```



w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web

Our project has [an interesting history](#) which has defined our [long and short term objectives](#) and told us many important lessons. Don't forget to follow our [blog](#) and [twitter](#) account for news,



# OWASP 以應用程式安全出發的國際資安組織



PROJECTS CHAPTERS EVENTS ABOUT 🔍

🛒 Store

Donate

Join

## About the OWASP Foundation



The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Our programming includes:

- Community-led open source projects including code, documentation, and standards
- Over 250+ local chapters worldwide
- Tens of thousands of members
- Industry-leading educational and training conferences

We are an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of our projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security. The OWASP Foundation launched on December 1st, 2001, becoming incorporated as a United States non-profit charity on April 21, 2004.

For two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. [Donate](#), [Become a Member](#), or become a [Corporate Supporter](#) today.

👁 Watch 163

☆ Star 471

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

### Upcoming OWASP Global Events

[OWASP Global AppSec Lisbon 2024](#)

- June 24–28, 2024

[OWASP Global AppSec San Francisco 2024](#)

- September 23–27, 2024

[OWASP Global AppSec Washington DC 2025](#)

- November 3–7, 2025

[OWASP Global AppSec San Francisco 2026](#)

- November 2–6, 2026

<https://owasp.org/>

# 認識應用程式安全

- 應用程式安全(AppSec)，包括向開發團隊引入安全軟體開發生命週期的所有任務
- 最終目標是改進安全實踐，並通過它來發現、修復並防止應用程式中的安全問題
- 它涵蓋了從需求分析、設計、實施、驗證和維護的整個應用程序生命週期
- 網站應用程式安全，專門處理網站、Web 應用程式和Web 服務的安全性
- 多種自動化工具可用於識別應用程式中的漏洞。用於識別應用程式漏洞的常用工具類別包括：
  - 靜態應用程式安全測試 ( SAST ) 在應用程式開發過程中分析安全漏洞的原始碼
  - 動態應用程式安全測試 ( DAST ，通常稱為漏洞掃描器 ) 通過抓取和分析網站自動檢測漏洞
  - 交互式應用程式安全測試 ( IAST ) 使用軟體工具從內部評估應用程式

# 雲端服務風險

就雲端服務部署方式，常見雲端服務風險參考歐洲網路與資通安全局(European Network and Information Security Agency, ENISA)，以雲端服務風險分析，針對政策與組織風險、法規風險及技術風險3個面向歸納如下：

## • 政策與組織風險

- ✓ 供應商綁定(Provider Lock-in)。
- ✓ 喪失管理(Loss of Governance)。
- ✓ 遵循與合規上之挑戰(Compliance Challenges)。
- ✓ 組織名譽損失源於其他用戶行為(Loss of Business Reputation Due to Co-tenant Activities)。
- ✓ 雲端服務之中止與失效(Cloud Service Termination or Failure)。
- ✓ 雲端供應商之收購(Cloud Provider Acquisition)。
- ✓ 供應鏈失效(Supply Chain Failure)。

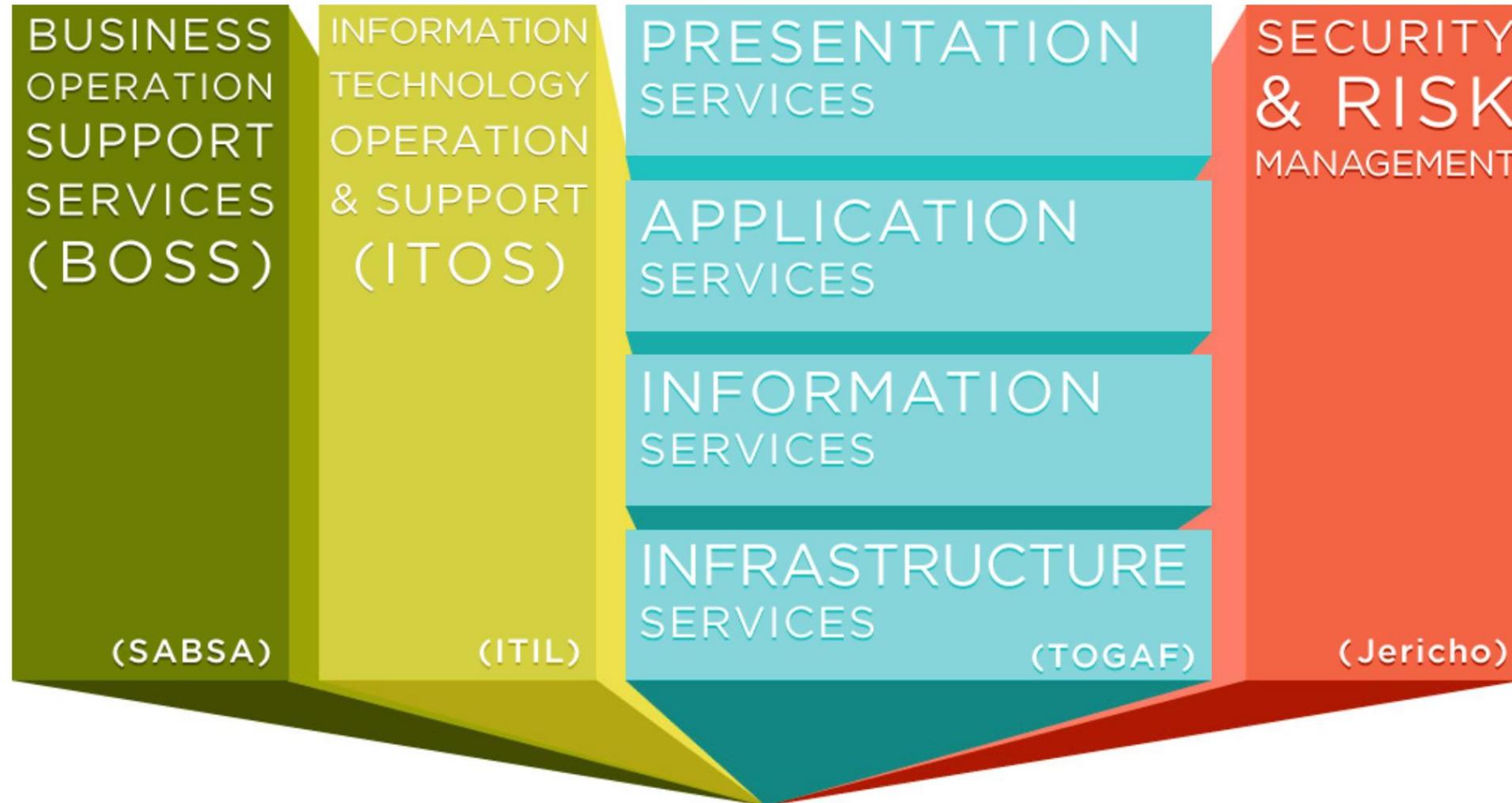
## • 法規風險

- ✓ 傳票與電子蒐證(Subpoena and E-discovery)。
- ✓ 管轄權變更之風險(Risk from Changes of Jurisdiction)。
- ✓ 資料保護風險(Data Protection Risks)。
- ✓ 授權之風險(Licensing Risks)。

## • 技術風險

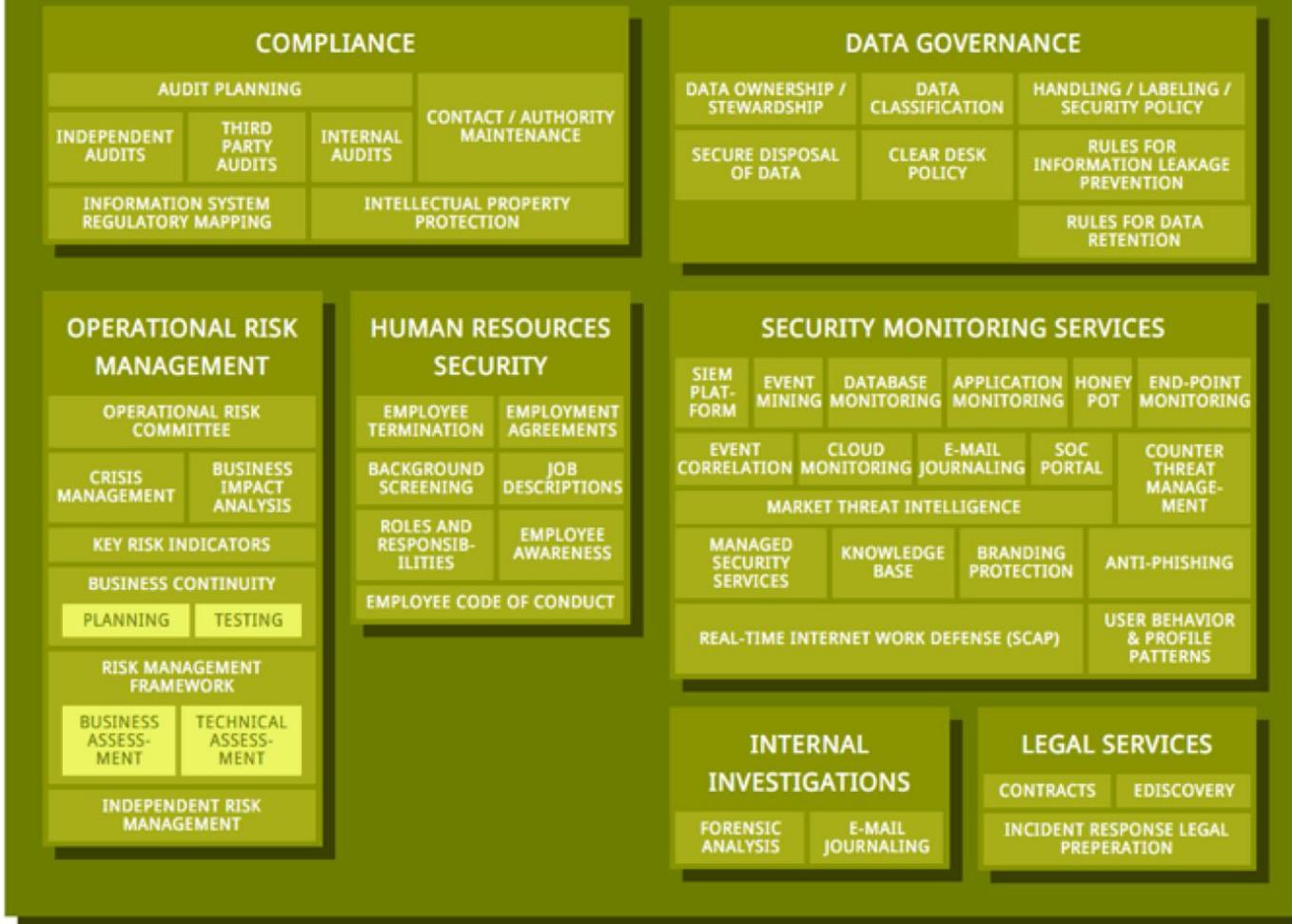
- ✓ 資源匱乏風險(Resource Exhaustion)。
- ✓ 隔離失效(Isolation Failure)。
- ✓ 惡意內部人員(Cloud Provider Malicious Insiders)。
- ✓ 管理介面被破解(Management Interface Compromise)。
- ✓ 傳輸資料攔截風險(Intercepting Data in Transit)。
- ✓ 資料傳輸時之外洩風險(Data Leakage on Up/download)。
- ✓ 不安全或無效之資料移除(Insecure or Ineffective Deletion of Data)。
- ✓ 分散式阻斷服務攻擊風險(DDoS)。
- ✓ 加密金鑰遺失與外洩(Loss of Encryption Keys)。
- ✓ 服務引擎弱點攻擊(Compromise Service Engine)。
- ✓ 用戶嚴謹之程序與雲端環境衝突(Conflict Between Customer Hardening Requirement and Cloud Environment)。

# 企業的資安面向(架構)

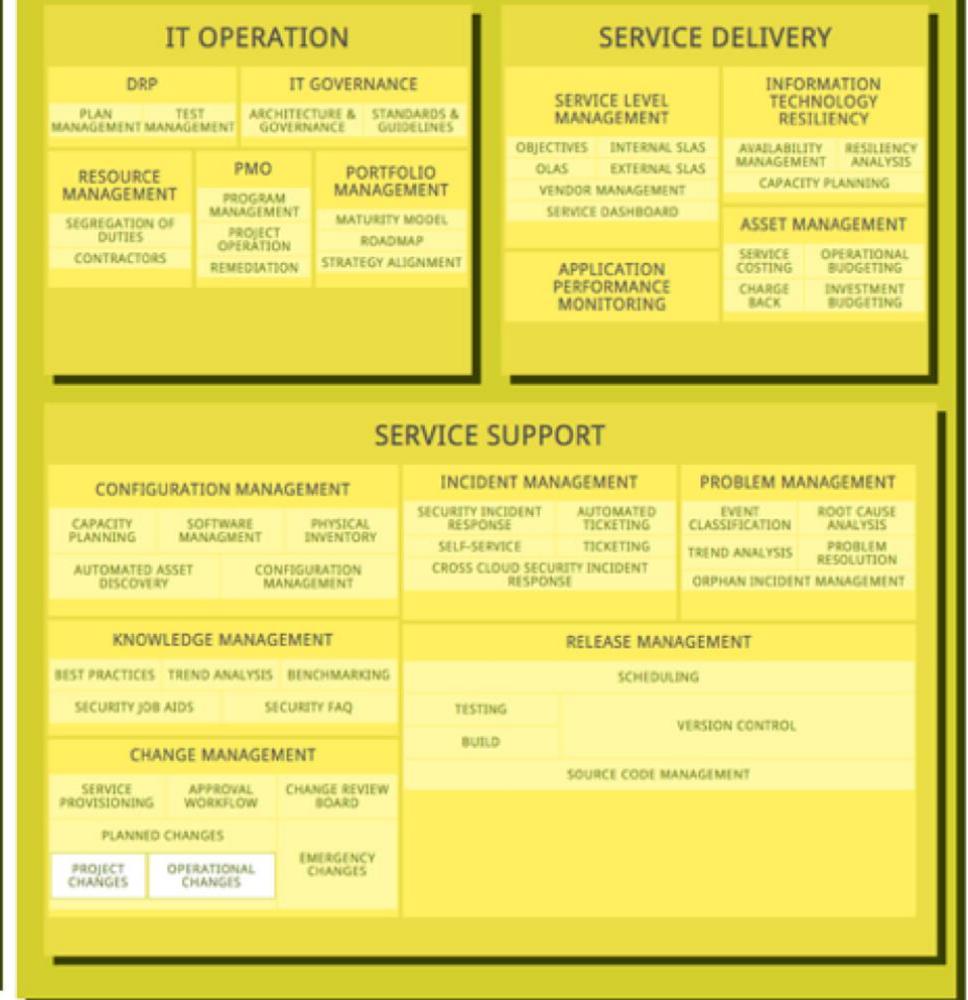


# 企業的資安面向(架構)

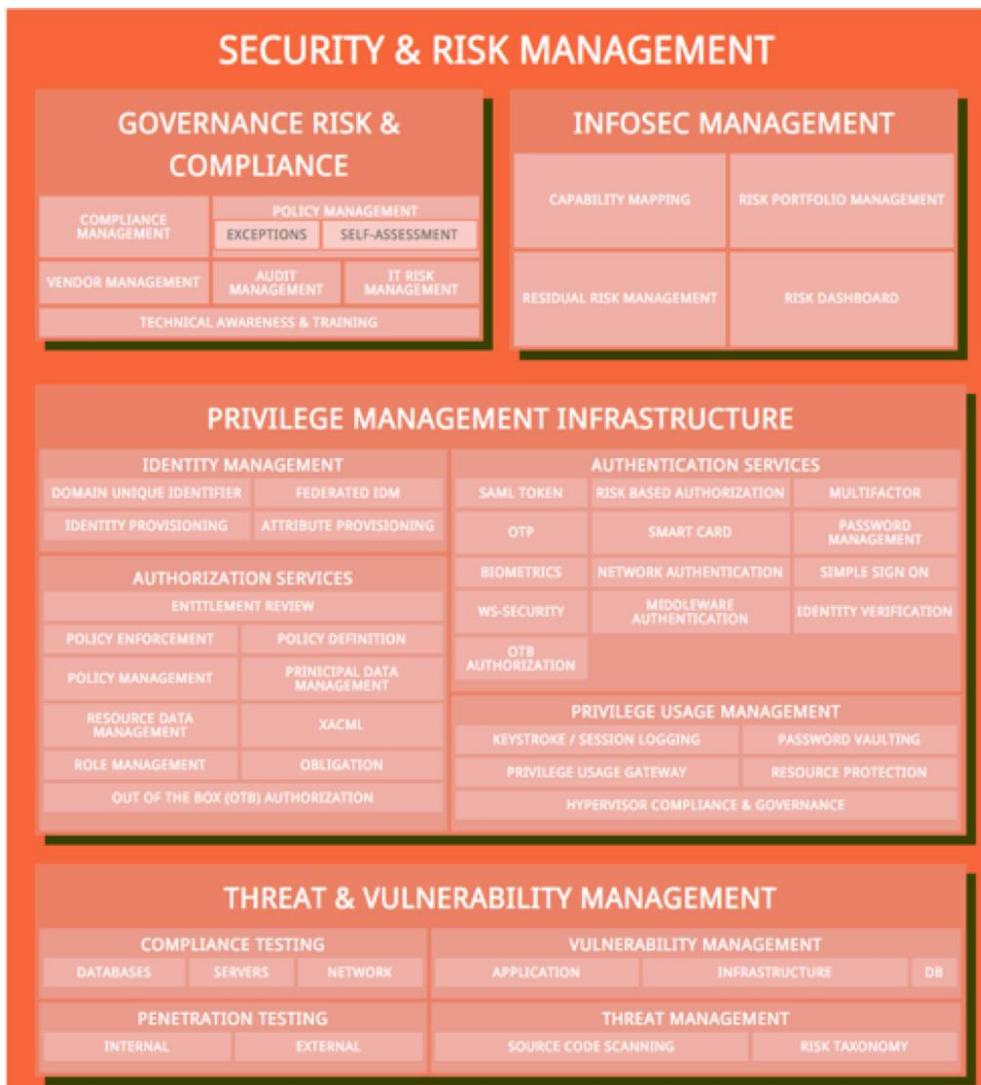
## BUSINESS OPERATION SUPPORT SERVICES (BOSS)



## INFORMATION TECHNOLOGY OPERATIONS & SUPPORT (ITOS)



# 企業的資安面向(架構)



# 檢查一下自己的網站

The screenshot shows the WebCheck website analysis tool interface. On the left, there is a logo with a checkmark and the text 'WebCheck'. Below it, the main heading reads 'We give you X-Ray Vision for your Website'. A sub-headline states 'In just 20 seconds, you can see *what attackers already know*'. There is a text input field containing 'E.g. github.com' and a large button labeled 'Analyze URL'. The right side of the interface displays various analysis results in a dark theme:

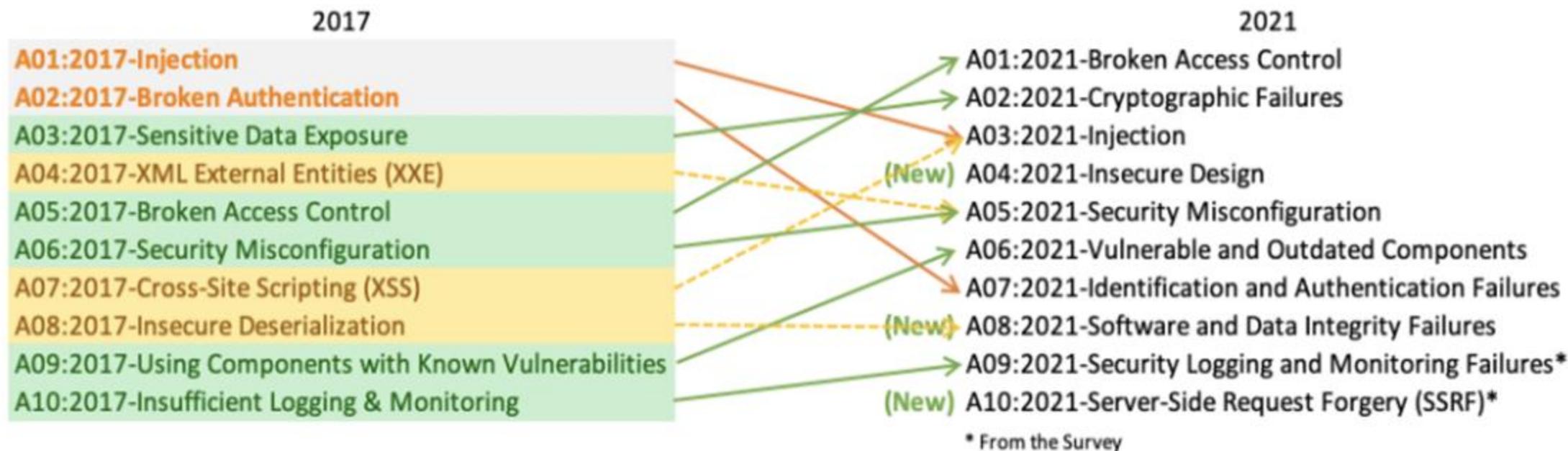
- Extended Key Usage:** TLS Web Server Authentication, TLS Web Client Authentication.
- DNS Records:** A (151.101.64.81), AAAA (151.101.128.81, 151.101.64.81, 151.101.0.81, 151.101.192.81), MX (2a04:4e42:600::81, 2a04:4e42:400::81, 2a04:4e42:200::81, 2a04:4e42::81), CNAME (ddns1.bbc.com, dns0.bbc.co.uk, dns0.bbc.com, dns1.bbc.co.uk, dns1.bbc.com, ddns0.bbc.co.uk, ddns0.bbc.com, ddns1.bbc.co.uk).
- Cookies:** SOCS (expires: Tue, 06-Aug-2024 16:42:15...), AEC (Ad49MVeTQVG6LH6KJy7oJI0cK...), CONSENT (PENDING+192).
- Crawl Rules:** User-agent (\*), Disallow (/bitesize/search?), Disallow (/bitesize/study-support), Disallow (/cbbc/search\$).
- Pages:** Last Modified (16 October 2018), Change Frequency (monthly), Priority (1.00). List of pages: /about, /donations, /app, /hiring, /privacy, /press, /newsletter, /spread, /bangs, /settings.
- Security.Txt:** Present (Yes), File Location (.well-known/security.txt), PGP Signed (Yes), Hash (SHA512), Contact (/cloudflare), Contact1 (mailto:security@cloudflar...), Contact2 (/abuse/), Preferred-Languages (en), Encryption (/pgp/security-at-cloudfla...), Canonical (.well-known/security.txt), Policy (/disclosure), Hiring (/careers/jobs/), Expires (22 March 2023).
- Linked Pages:** Summary, Internal Link Count (329), External Link Count (8). Internal Links, External Links (https://shop.forex.com/, https://twitter.com/thepracticaldev).

<https://web-check.xyz/>

# OWASP Top 10 - 2021

## What's changed in the Top 10 for 2021

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021. We've changed names when necessary to focus on the root cause over the symptom.



# 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



# TOP10

# OWASP Top 10 - 2021

- **A01: 權限控制失效 (Broken Access Control)**

- ▶ 從 OWASP Top 2017 第五名晉升至 2021 第一名，超過 94% 的應用程式都存在此問題。

**情境 #1：** 應用程式在存取帳戶資訊的SQL呼叫中使用未經驗證的資料：

```
pstmt.setString(1, request.getParameter("acct"));  
  
ResultSet results = pstmt.executeQuery( );
```

攻擊者只需修改瀏覽器的“acct”參數即可發送他們想要的任何帳號。如果沒有正確驗證，攻擊者可以存取任何用戶的帳戶。

<https://example.com/app/accountInfo?acct=notmyacct>

# OWASP Top 10 - 2021

- A01: 權限控制失效 (Broken Access Control)

情境#2：攻擊者僅強迫瀏覽某些目標網址。存取管理頁面需要管理員權限。

```
https://example.com/app/getapplInfo
```

```
https://example.com/app/admin_getapplInfo
```

如果未經身份驗證的用戶可以存取任一頁面，那就是一個缺陷。如果一個非管理員可以存取管理頁面，這也是一個缺陷。

- **A02: 加密機制失效 (Cryptographic Failures)**

- ▶ OWASP Top 10 2017 稱為「機敏資料外洩」，2021 版將此重新進行定義，並將問題核心定義在加密機制的失敗，因而造成機敏資料外洩或系統遭受破壞。
- ▶ 通訊傳輸協定是否有使用資料加密機制？  
常見未加密通訊資料的協定有HTTP、FTP、TELNET等。
- ▶ 使用不安全的加密演算法，例如：MD5、SHA1、WEP等。

- **A02: 加密機制失效 (Cryptographic Failures)**

**情境 #1:** 有一個應用程式使用自動化資料庫加密來加密資料庫中的信用卡卡號，但是資料被存取時是被自動解密的，進而允許透過SQL注入缺陷來存取信用卡卡號明文。

**情境 #2:** 有一個站台沒有對所有頁面強制使用TLS或支援脆弱的加密，攻擊者監控網路流量(如在不安全的無線網路)，將連線從HTTPS降級成HTTP，並攔截請求竊取使用者的會話(session) cookies，之後攻擊者重送竊取到的會話(session) cookies並劫持用戶(認證過的)的會話，進而存取或修改使用者的隱私資料。除了上述以外，攻擊者也能修改傳輸的資料，如匯款收款人。

**情境 #3:** 密碼資料庫使用未被加鹽或簡單的雜湊來儲存每個人的密碼，一個檔案上傳的缺陷可以讓攻擊者存取密碼資料庫，所有未被加鹽的雜湊可以被預先計算好的彩虹表公開。即使雜湊有被加鹽，由簡單或快速的雜湊法算出的雜湊仍能被GPU破解。

# OWASP Top 10 - 2021

- **A03: 注入式攻擊 (Injection)**



SQL Injection

- ▶ NoSQL Injection
- ▶ Command Injection
- ▶ LDAP Injection
- ▶ JSON Injection
- ▶ CSS Injection
- ▶ ...



根據統計資料顯示,

**SQL Injection** 仍是目前**最常見**的網站資安風險

- A03: 注入式攻擊 (Injection)

情境 #1: 應用程式使用了不被信任的資料在脆弱的 SQL 呼叫中：

```
String query = "SELECT * FROM accounts WHERE custID=" + request.getParameter("id") + "";
```

情境 #2: 類似地，應用程式對框架的盲目信任，可能導致仍然在漏洞的查詢，(例如：Hibernate 查詢語言 (HQL))：

```
Query HQLQuery = session.createQuery("FROM accounts WHERE custID=" + request.getParameter("id") + "");
```

在這兩個情境中，攻擊者在他們的瀏覽器修改了 "id" 參數值，送出 ' or '1'='1，例如：

```
http://example.com/app/accountView?id=' or '1'='1
```

這兩個查詢的含義將產生改變，而回應所有帳戶資料表中的紀錄，更危險的攻擊將可能修改或刪除資料，以及影響資料的儲存過程。

- **A04: 不安全設計 (Insecure Design)**

- ▶ 此為 2021 版新增的項目，定義與應用程式設計缺陷相關的風險。
- ▶ 例如：機敏資料加密沒有實作方法、OTP非隨機數且不具時效性。

- ▶ 情境：

某網站提供前 100 名訪問用戶一組優惠碼，但設計上存在缺陷，導致有心人士利用不同 IP 位址方式，取得 99 組優惠碼，並透過獲取優惠碼購買商品轉售。

- **A05: 安全設定缺陷 (Security Misconfiguration)**

- ▶ 有 90% 受測的應用程式存在某種類別的安全設定缺陷，在 OWASP Top 10 2017 版本中的 XML 外部實體注入攻擊 (XML External Entities) 被合併於這個類別。
- ▶ 啟用或安裝不需要的功能、預設帳號位停用或密碼未變更、系統自動更新未啟用、未針對預設設定進行調整或啟用安全功能等，都是導致此問題發生的主要原因。

- **A05: 安全設定缺陷 (Security Misconfiguration)**

- ▶ 情境 #1：營運用的程式伺服器，含有未移除的預設程式，  
這個程式有已知的安全缺陷，可被攻擊者利用入侵伺服器。  
例如：預設的程式帶有管理者介面，並且有未變更的帳號，  
攻擊者可以透過預設的密碼登入，並取得系統控制權限。
- ▶ 情境 #2：資料夾列表指令並未在伺服器上關閉。攻擊者能找出並且下載，  
已編譯過 Java 檔案，並透過反編譯與逆向工程等手法，查看  
原始碼，再因此找出程式中，嚴重的存取控制缺陷。

- **A05: 安全設定缺陷 (Security Misconfiguration)**

- ▶ 情境 #3：程式伺服器的設定，允許輸出帶有詳細內容的錯誤訊息，  
例如：堆疊追蹤，供用戶查看。這有可能導致敏感訊息的外洩，  
或間接透露出，使用中，並帶有脆弱性的元件版本。
- ▶ 情境 #4：一個雲端伺服器，提供了預設權限分享，給其他在網際網路的  
CSP用戶。這將導致雲端儲存的敏感資料可以被存取。

# OWASP Top 10 - 2021

- **A06: 危險或過舊的元件 (Vulnerable and Outdated Components)**
  - ▶ OWASP Top 10 2017版在第九名的位置，2021版本爬升到第六名的位置，這也是唯一沒有任何 CVE 能被對應到 CWE 內的類別。

- **A07: 認證及驗證機制失效 (Identification and Authentication Failures)**
  - ▶ OWASP Top 10 2017 版在第二名的位置，2021 版本下滑到第七名的位置，因為多數服務均支援或強制啟用多重方式認證，故此風險有降低的趨勢。
  - ▶ 允許使用弱密碼、未抵擋暴力破解攻擊、未啟用多因子認證機制、暴露 Session 於網址中、Session 管控機制不足等，都是造成此項問題最主要的原因。

- **A08: 軟體及資料完整性失效 (Software and Data Integrity Failures)**
  - ▶ 程式碼或基礎架構未能保護軟體及資料之完整性
  - ▶ 不安全的反序列化
  - ▶ 使用不受信任來源之套件、函式庫、模組等
  - ▶ 不安全的持續性整合 / 部署 (CI / CD) 流程
  - ▶ 使用缺乏充足完整性驗證的自動更新

- **A09: 資安記錄及監控失效 (Security Logging and Monitoring Failures)**
  - ▶ OWASP Top 10 2017 版在第十名的位置，2021 版本爬升到第九名的位置，通常需要以訪談或詢問之方式，檢驗有無偵測滲透測試的攻擊活動。
  - ▶ 未紀錄可被稽核的事件（例如：登入成功、登入失敗等）、告警或錯誤訊息未產生、未針對可疑的活動進行監測、日誌僅儲存於本地端等，都是導致此問題的主要原因。

- **A10: 伺服器端請求偽造 (Server-Side Request Forgery)**

- ▶ 攻擊者可以利用偽造伺服器端請求來攻擊在 WAF、防火牆、或網路 ACL 後面的系統，可能採取之情境如下：

- ▶ **情境 #1：對內部伺服器 Port Scan** |

如果網路架構未被切割，攻擊者能透過結果或連線狀態，判斷內部服務 Port 情況。

- ▶ **情境 #2：機敏資料洩漏** |

攻擊者可以存取本地端檔案或內部服務取得機敏資料。

- ▶ **情境 #3：滲透內部服務** |

攻擊者可以濫用內部服務去執行更進一步的攻擊，例如：RCE或DoS。

# OWASP API Top 10 : 2023

API  
01

物件級授權被破壞

API  
02

認證失效

API  
03

破碎物件屬性級授權

API  
04

資源消耗不受限制

API  
05

功能等級授權被破壞

API  
06

伺服器端請求偽造

API  
07

安全配置錯誤

API  
08

缺乏針對自動化威脅的保護

API  
09

資產管理不當

API  
10

API 的不安全使用



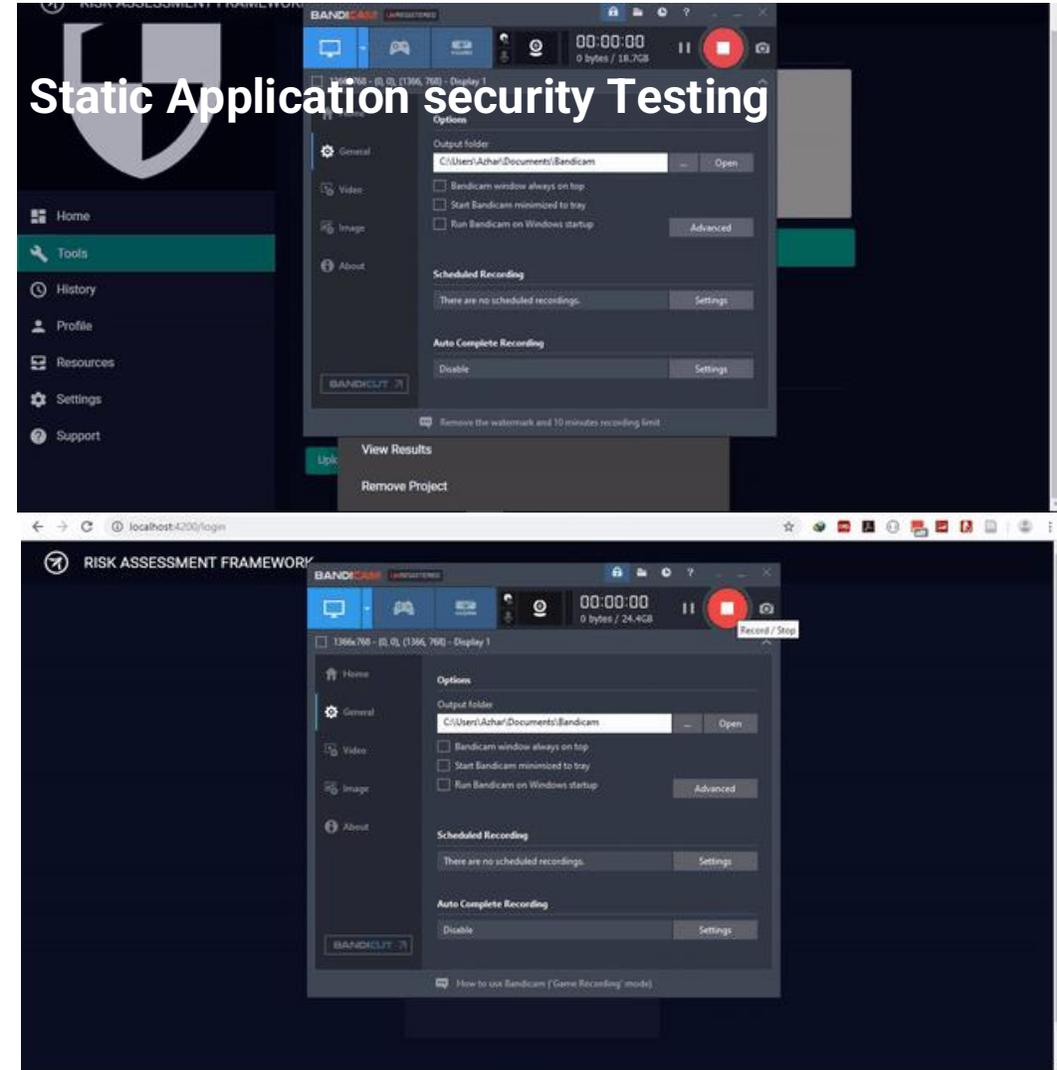
**OWASP API Security**  
Top Ten - 2023



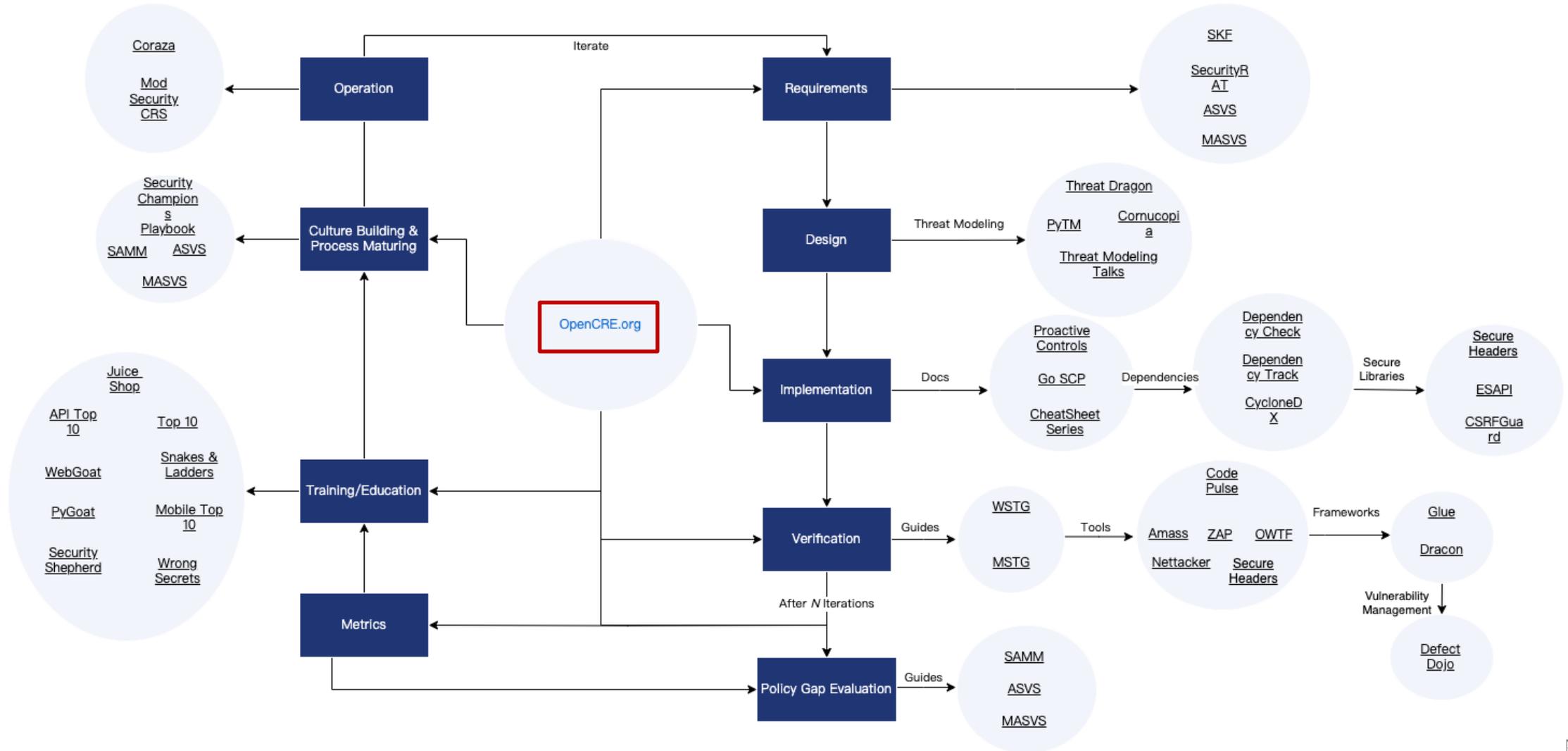
# API Security Top 10 - 2023



<https://owasp.org/API-Security/>



# OWASP Wayfinder



TWCSA

台灣數位安全聯盟

Taiwan Cyber Security Alliance

# 網頁檢測工具介紹與操作

OWASP ZAP 漏洞分析、報告解讀



# 企業資安成熟度 – 以資安演練/滲透測試驗證

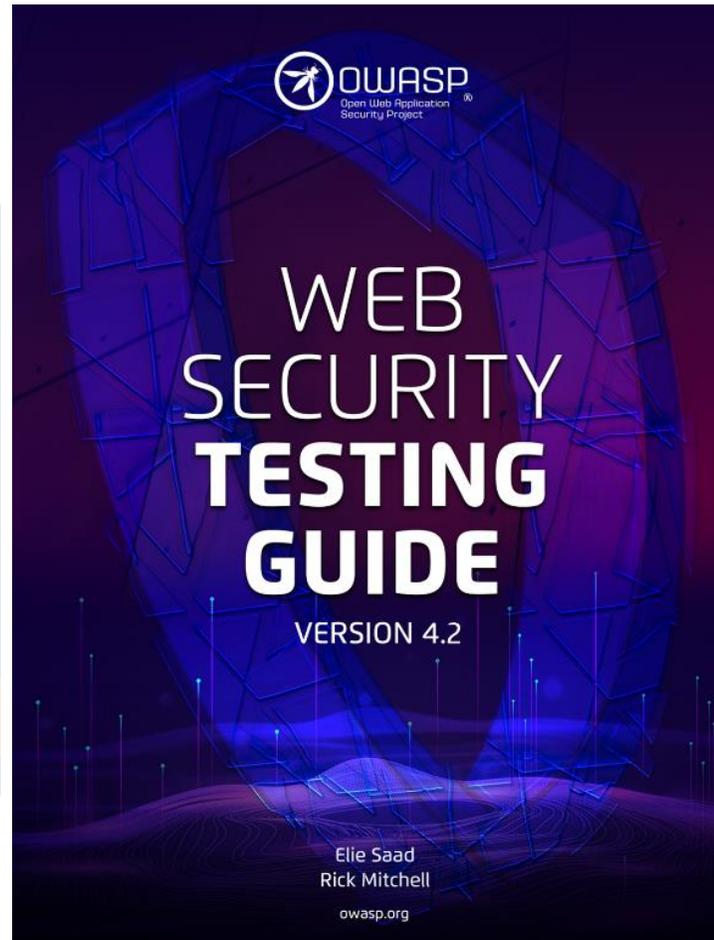
## OSSTMM 3

The Open Source Security Testing Methodology Manual  
Contemporary Security Testing and Analysis



Created by Pete Herzog  
Developed by ISECOM

ISECOM



目標設定

紅軍攻擊演練範圍為需求方進行相關目標訂定

目標偵查

透過各種不同的方法包含進行一些被動和主動的偵查

利用漏洞

透過目標偵查之後確認哪些攻擊路徑可以使用

探測與擴大攻擊手段

將以取得權限之後會在系統中移動，尋找可利用的目標

報告與分析

攻擊結果報告，與藍隊團隊調整相關的偵測規則

# OWASP ZAP



[Home](#) [Blog](#) [Videos](#) [Documentation](#) [Community](#) [Sponsor](#) [Search](#)

[Download](#)



## OWASP® Zed Attack Proxy (ZAP)

The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers. A GitHub Top 1000 project.

[Quick Start Guide](#)

[Download Now](#)



### Intro to ZAP

If you are new to security testing, then ZAP has you very much in mind. Check out our ZAP in Ten video series to learn more!



### Automate with ZAP

ZAP provides range of options for security automation. Check out the automation docs to start automating!



### ZAP Marketplace

ZAP marketplace contains add-ons that have been contributed by the community. Check out how you can extend ZAP with the add-ons!



## ZAPping the OWASP Top 10 (2021)

This document gives an overview of the automatic and manual components provided by OWASP Zed Attack Proxy (ZAP) that are recommended for testing each of the OWASP Top Ten Project 2021 risks.

For the previous Top Ten see [ZAPping the OWASP Top 10 \(2017\)](#)

Note that the [OWASP Top Ten Project](#) risks cover a wide range of underlying vulnerabilities, some of which are not really possible to test for in a completely automated way. If a completely automated tool claims to protect you against the full OWASP Top Ten then you can be sure they are being 'economical with the truth'!

The component links take you to the relevant places in an online version of the ZAP User Guide from which you can learn more.

### Common Components

The 'common components' can be used for pretty much everything, so can be used to help detect all of the Top 10

Manual	<a href="#">Manipulator-in-the-middle proxy</a>
Manual	<a href="#">Manual request / resend</a>
Manual	<a href="#">Scripts</a>
Manual	<a href="#">Community Scripts</a>
Manual	<a href="#">Search</a>

### A1 Broken Access Control

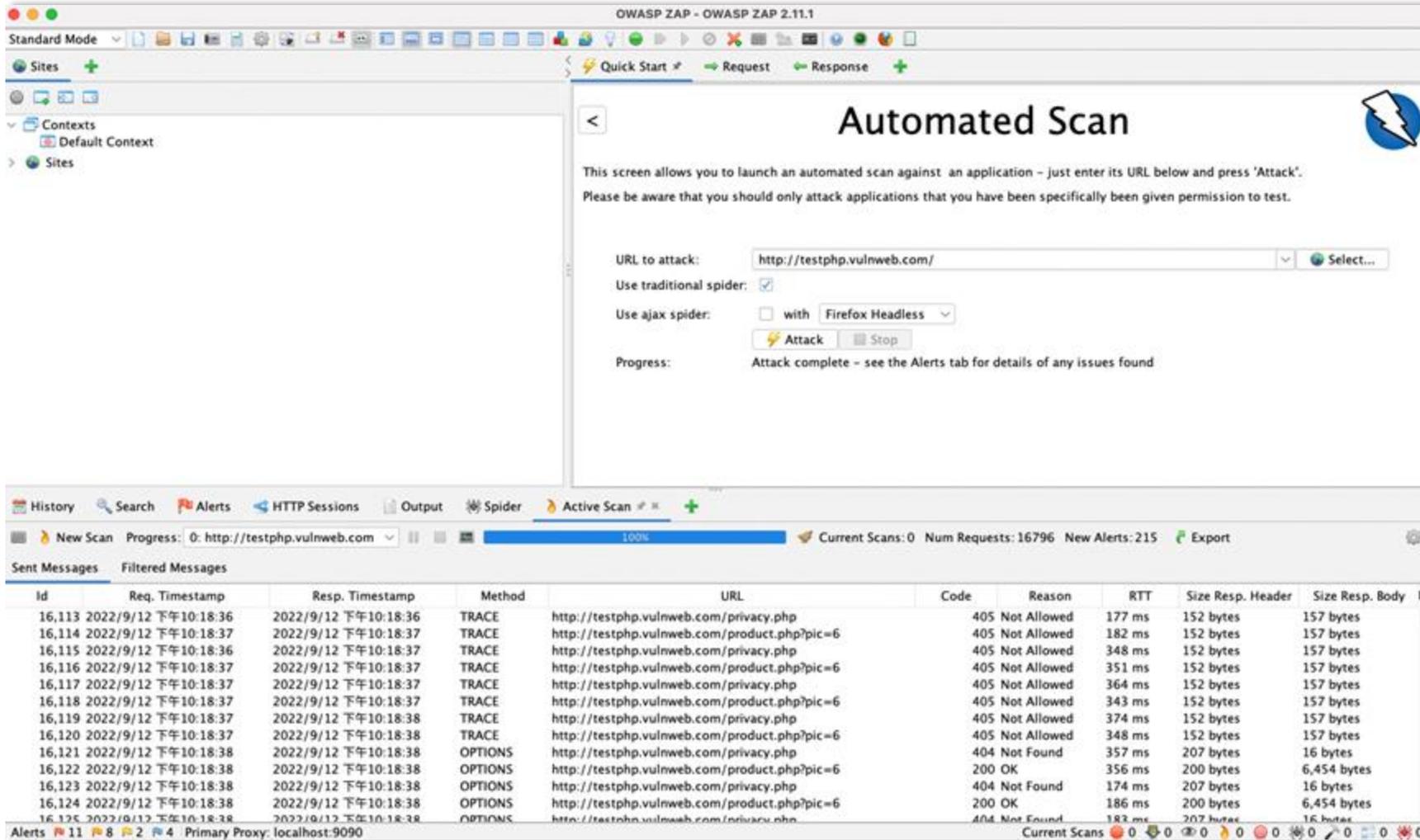
Automated	Scan Rules tagged with: <a href="#">OWASP_2021_A01</a>
-----------	--

<https://www.zaproxy.org/docs/guides/zapping-the-top-10-2021/>

- 功能介紹

- ▶ 動態掃描（自動診斷工具）
- ▶ Forced Browse（使用字典找尋目錄、檔案）
- ▶ Spider（網路爬蟲）
- ▶ AjAX Spider（Javascript 網路爬蟲）
- ▶ Fuzzer（自動化插入參數之模糊測試）
- ▶ Proxy（代理伺服器）

# OWASP ZAP - Automated Scan



**Automated Scan**

This screen allows you to launch an automated scan against an application – just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:  Select...

Use traditional spider:

Use ajax spider:  with Firefox Headless

Attack Stop

Progress: Attack complete – see the Alerts tab for details of any issues found

History Search Alerts HTTP Sessions Output Spider Active Scan +

New Scan Progress: 0: http://testphp.vulnweb.com 100% Current Scans: 0 Num Requests: 16796 New Alerts: 215 Export

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
16,113	2022/9/12 下午10:18:36	2022/9/12 下午10:18:36	TRACE	http://testphp.vulnweb.com/privacy.php	405	Not Allowed	177 ms	152 bytes	157 bytes
16,114	2022/9/12 下午10:18:37	2022/9/12 下午10:18:37	TRACE	http://testphp.vulnweb.com/product.php?pic=6	405	Not Allowed	182 ms	152 bytes	157 bytes
16,115	2022/9/12 下午10:18:36	2022/9/12 下午10:18:37	TRACE	http://testphp.vulnweb.com/privacy.php	405	Not Allowed	348 ms	152 bytes	157 bytes
16,116	2022/9/12 下午10:18:37	2022/9/12 下午10:18:37	TRACE	http://testphp.vulnweb.com/product.php?pic=6	405	Not Allowed	351 ms	152 bytes	157 bytes
16,117	2022/9/12 下午10:18:37	2022/9/12 下午10:18:37	TRACE	http://testphp.vulnweb.com/privacy.php	405	Not Allowed	364 ms	152 bytes	157 bytes
16,118	2022/9/12 下午10:18:37	2022/9/12 下午10:18:37	TRACE	http://testphp.vulnweb.com/product.php?pic=6	405	Not Allowed	343 ms	152 bytes	157 bytes
16,119	2022/9/12 下午10:18:37	2022/9/12 下午10:18:38	TRACE	http://testphp.vulnweb.com/privacy.php	405	Not Allowed	374 ms	152 bytes	157 bytes
16,120	2022/9/12 下午10:18:37	2022/9/12 下午10:18:38	TRACE	http://testphp.vulnweb.com/product.php?pic=6	405	Not Allowed	348 ms	152 bytes	157 bytes
16,121	2022/9/12 下午10:18:38	2022/9/12 下午10:18:38	OPTIONS	http://testphp.vulnweb.com/privacy.php	404	Not Found	357 ms	207 bytes	16 bytes
16,122	2022/9/12 下午10:18:38	2022/9/12 下午10:18:38	OPTIONS	http://testphp.vulnweb.com/product.php?pic=6	200	OK	356 ms	200 bytes	6,454 bytes
16,123	2022/9/12 下午10:18:38	2022/9/12 下午10:18:38	OPTIONS	http://testphp.vulnweb.com/privacy.php	404	Not Found	174 ms	207 bytes	16 bytes
16,124	2022/9/12 下午10:18:38	2022/9/12 下午10:18:38	OPTIONS	http://testphp.vulnweb.com/product.php?pic=6	200	OK	186 ms	200 bytes	6,454 bytes
16,125	2022/9/12 下午10:18:38	2022/9/12 下午10:18:38	OPTIONS	http://testphp.vulnweb.com/privacy.php	404	Not Found	183 ms	207 bytes	16 bytes

Alerts 11 8 2 4 Primary Proxy: localhost:9090 Current Scans 0



# OWASP ZAP 網站漏洞分析

The screenshot displays the OWASP ZAP web application security tool interface. The main window shows a list of alerts under the 'Alerts (11)' section, with 'Cross Site Scripting (Reflected) (14)' selected. The 'Edit Alert' dialog box is open, providing details for a specific alert:

- Alert Type:** Cross Site Scripting (Reflected)
- URL:** http://testphp.vulnweb.com/listproducts.php?cat=%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E
- Risk:** High
- Confidence:** Medium
- Parameter:** cat
- Attack:** <img src=x onerror=prompt()>
- Evidence:** <img src=x onerror=prompt()>
- CWE ID:** 79
- WASC ID:** 8
- Description:** Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object...
- Reference:** <http://projects.webappsec.org/Cross-Site-Scripting>, <http://cwe.mitre.org/data/definitions/79.html>
- Alert Tags:** OWASP\_2021\_403, [https://owasp.org/Top10/A03\\_2021](https://owasp.org/Top10/A03_2021)

The background shows the ZAP interface with a 'Header: Text' and 'Body: Text' view, displaying HTML code and a warning message: 'Warning: mysql Error: You use near 'x onerror=prompt()' in /hj/var/www/listproducts'.

# OWASP ZAP 網站漏洞分析

← → × 不 unsafe | testphp.vulnweb.com/listproducts.php?cat=<img+src%3Dx+onerror%3Dprompt%28%29>

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

**Links**

- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

Error: You have an error in your SQL syntax; check the documentation that corresponds to your MySQL server version for the right syntax to use near '' at line 1 Warning: mysql\_fetch\_array() expects parameter 1 to be a resource, boolean given in /hj/var/www/listproducts.php on line 74

testphp.vulnweb.com 顯示

取消 確定

# Domain ~ IP address

**Mirror saved on:** 2020-10-19 03:50:20

**Notified by:** chinafans

**Domain:** <http://tcimmersion-hakka.gov.tw/o.htm>

**IP address:** 143.95.40.187 

**System:** Win 2012

**Web server:** IIS/8.5

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2020-10-19 03:50:20



<http://www.zone-h.org/mirror/id/34287373>

# 讓我們繼續看下去...

各位有看到什麼可疑的問題嗎？

Source	Domain	Record Data	Record Type	First Seen	Last Seen
VirusTotal	<a href="http://www.helipto.com.tw">www.helipto.com.tw</a>	143.95.40.187	A	2020-12-20 12:41:03	2020-12-20 12:41:03
VirusTotal	<a href="http://www.d-lai.com.tw">www.d-lai.com.tw</a>	143.95.40.187	A	2020-12-20 09:48:35	2020-12-20 09:48:35
VirusTotal	<a href="mailto:mail.hengshan.com.tw">mail.hengshan.com.tw</a>	143.95.40.187	A	2020-12-19 10:10:33	2020-12-19 10:10:33
VirusTotal	<a href="http://ez123.tw">ez123.tw</a>	143.95.40.187	A	2020-12-10 06:12:56	2020-12-10 06:12:56
VirusTotal	<a href="mailto:mail.yifa.tw">mail.yifa.tw</a>	143.95.40.187	A	2020-11-30 04:34:32	2020-11-30 04:34:32
VirusTotal	<a href="mailto:mail.pacific-edu.com">mail.pacific-edu.com</a>	143.95.40.187	A	2020-11-27 12:49:48	2020-11-27 12:49:48
VirusTotal	<a href="http://youdetw.com">youdetw.com</a>	143.95.40.187	A	2020-11-21 13:24:38	2020-11-21 13:24:38
VirusTotal	<a href="http://tcimmersion-hakka.gov.tw">tcimmersion-hakka.gov.tw</a>	143.95.40.187	A	2020-10-22 02:47:06	2020-10-22 02:47:06
VirusTotal	<a href="http://www.tcimmersion-hakka.gov.tw">www.tcimmersion-hakka.gov.tw</a>	143.95.40.187	A	2020-10-22 02:46:56	2020-10-22 02:46:56
VirusTotal	<a href="http://www.apex-arms.com">www.apex-arms.com</a>	143.95.40.187	A	2020-10-11 09:23:16	2020-10-11 09:23:16
VirusTotal	<a href="http://juicexpress.com.tw">juicexpress.com.tw</a>	143.95.40.187	A	2020-10-09 09:09:04	2020-10-09 09:09:04
VirusTotal	<a href="http://jypump.com">jypump.com</a>	143.95.40.187	A	2020-07-20 23:20:26	2020-07-20 23:20:26
VirusTotal	<a href="http://comerich.com.tw">comerich.com.tw</a>	143.95.40.187	A	2020-05-08 17:43:13	2020-05-08 17:43:13
VirusTotal	<a href="http://www.comerich.com.tw">www.comerich.com.tw</a>	143.95.40.187	A	2020-05-08 17:43:11	2020-05-08 17:43:11
VirusTotal	<a href="http://tw-comerich.com.tw">tw-comerich.com.tw</a>	143.95.40.187	A	2020-04-23 08:50:31	2020-04-23 08:50:31
VirusTotal	<a href="http://www.tw-comerich.com.tw">www.tw-comerich.com.tw</a>	143.95.40.187	A	2020-04-23 08:50:27	2020-04-23 08:50:27

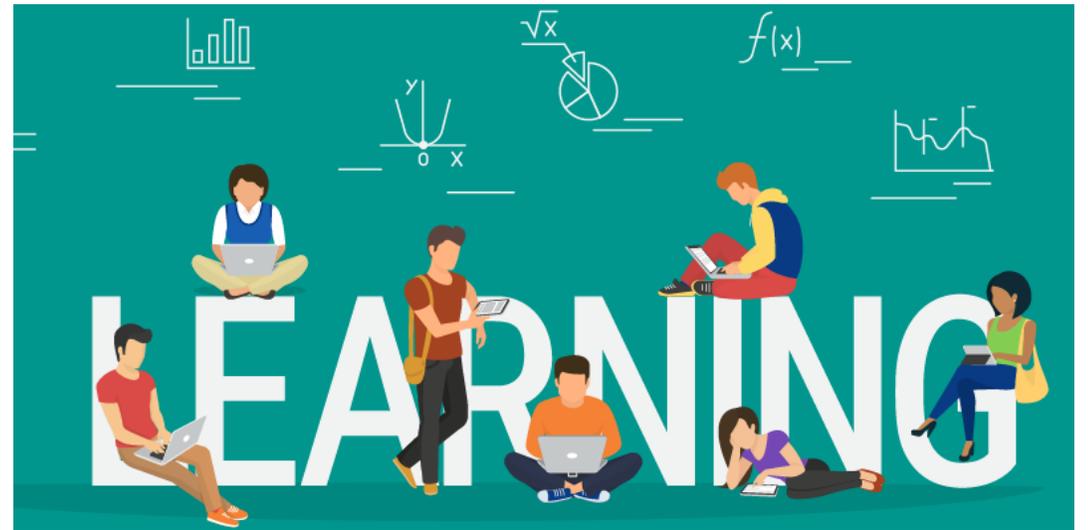
# 優先移除與復原

- 事件調查關鍵報告
- 依事件的影響衝擊決定處理流程
- 以「業務恢復」與「營運持續」為主要目標
- 依難易度配置投入資源
- 決定優先順序與關聯性
- 應變團隊須清楚知道處理流程與步驟



# 從每個事件中學習教訓

- 事件應變之後的分享
  - 建立事件處理生態系統
  - 嘗試找出根本原因
  - 「紅隊測試」與「藍隊防禦」思維
- 避免類似事件再度發生
  - 資源投入
  - 改善已知問題
- 建立應變流程與基礎
  - 標準化與客製化
  - 5W2H (What、Who、When、Where、Why、How與How much)



# 韌性才是王道

- 面對「資安事件」帶來的挑戰，思考如何在事件發生後存活下來
- 從「系統」、「網路」、「應用程式」、「數位資料」等不同面向思考備援方案
- 由「人」、「事」、「時」、「地」、「物」盤點數位韌性的資源
- 做為因應對策與執行方案，等待「資安事件的發生」



# Q&A

