正修科技大學
CHENG SHIU UNIVERSITY

TACCST

教育體系滲透測試常見問題與防護

圖書資訊處 資訊技術組 組長
洪瑞展

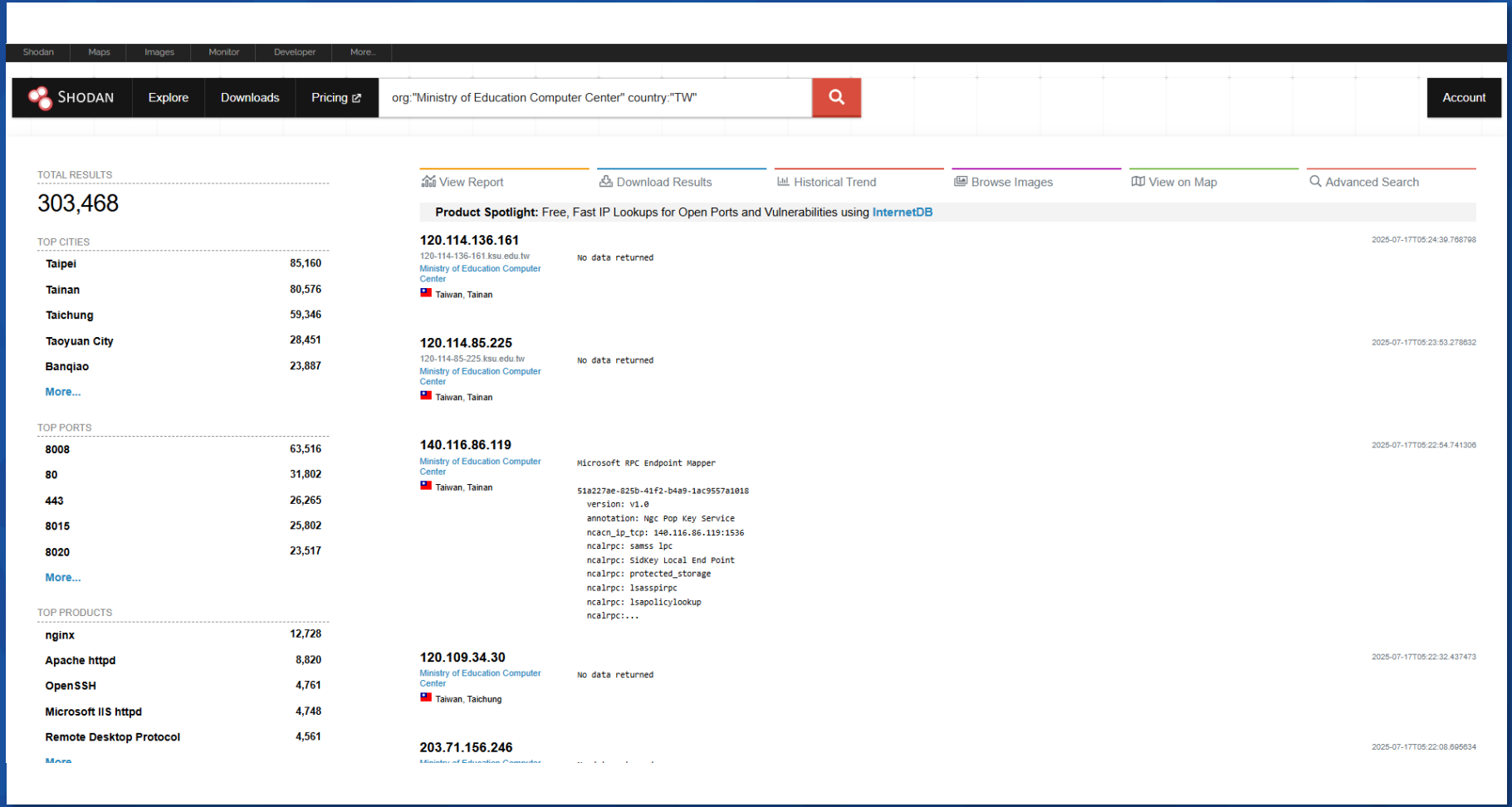
whoami

洪瑞展
Benson Hung

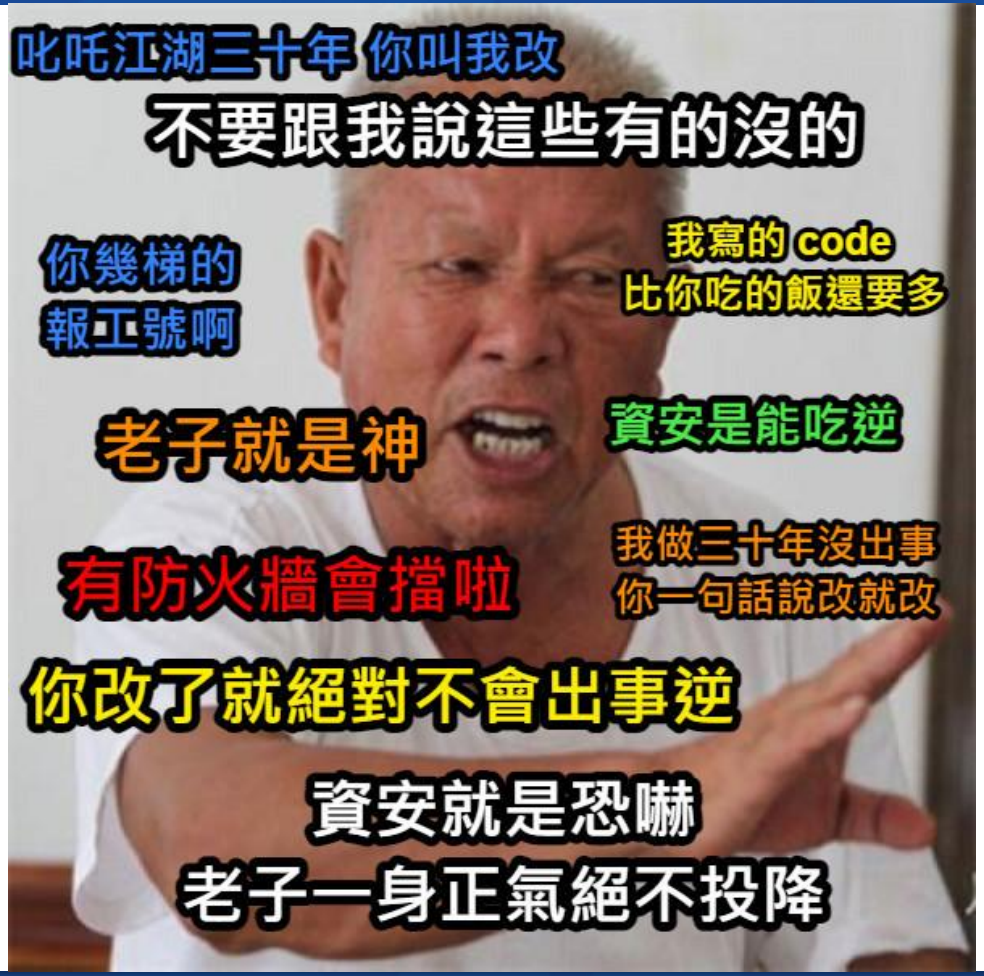
- **現任職務：**
  正修科技大學 圖書資訊處 / 資訊技術組組長
  正修科技大學 資訊管理系 / 兼任講師
  瑞淀科技有限公司 / 資訊總顧問
  教育體系資安檢核技術中心 高級技術檢測員
  教育機構資安驗證中心 實地稽核技術面委員
  教育部轄下醫療領域資訊安全推動中心 實地稽核技術面稽核委員

- **專長領域：**
  資訊安全、網路管理、程式設計、雲端服務

- **技能認證：**
  ISO 27001 LA、ISO 27701 LA、BS10012 LA
  CEH、CHFI、RHCE、LPIC-2、CCNP


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
org:"Ministry of Education Computer Center" country:"TW"
Account
TOTAL RESULTS
303,468
TOP CITIES
Taipei 85,160
Tainan 80,576
Taichung 59,346
Taoyuan City 28,451
Banqiao 23,887
More...
TOP PORTS
8008 63,516
80 31,802
443 26,265
8015 25,802
8020 23,517
More...
TOP PRODUCTS
nginx 12,728
Apache httpd 8,820
OpenSSH 4,761
Microsoft IIS httpd 4,748
Remote Desktop Protocol 4,561
More
View Report
Download Results
Historical Trend
Browse Images
View on Map
Advanced Search
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB
120.114.136.161
120-114-136-161.ksu.edu.tw
Ministry of Education Computer Center
Taiwan, Tainan
No data returned
2025-07-17T05:24:39.768798
120.114.85.225
120-114-85-225.ksu.edu.tw
Ministry of Education Computer Center
Taiwan, Tainan
No data returned
2025-07-17T05:23:53.278632
140.116.86.119
Ministry of Education Computer Center
Taiwan, Tainan
Microsoft RPC Endpoint Mapper
51a227ae-825b-41f2-b4a9-1ac9557a1018
version: v1.0
annotation: Ngc Pop Key Service
ncacn_ip_tcp: 140.116.86.119:1536
ncalrpc: samss lpc
ncalrpc: SidKey Local End Point
ncalrpc: protected_storage
ncalrpc: lsasspirpc
ncalrpc: lsapolicylookup
ncalrpc:...
2025-07-17T05:22:54.741306
120.109.34.30
Ministry of Education Computer Center
Taiwan, Taichung
No data returned
2025-07-17T05:22:32.437473
203.71.156.246
2025-07-17T05:22:08.695634


資安主管
肥宅工程師
你的code漏洞
多到比你臉上粉刺還多!!!


叱吒江湖三十年 你叫我改
不要跟我說這些有的沒的
你幾梯的
報工號啊
我寫的 code
比你吃的飯還要多
老子就是神
資安是能吃逆
有防火牆會擋啦
我做三十年沒出事
你一句話說改就改
你改了就絕對不會出事逆
資安就是恐嚇
老子一身正氣絕不投降


前端&後端
維護&開發
文件撰寫
資安&滲透測試
資料庫優化


外包工程師超人


校園資安悲慘日常
外部攻擊者


認真對校內同仁講解資安的你
蛤


TACCST
Viggle.ai
說已經做了資通安全責任等級之應辦事項

我們的領隊

A組王者
育彰老師

全國最知名大師
甘霖老師

B組大師
聖全老師

三台柱

TACCST 教育體系資安檢測技術服務中心


主導:今天結果共有5個高風險


什么叫做假！
翻譯翻譯這他X的是什麼漏洞
長官

相關法條

法規名稱：中華民國刑法 EN

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

中華民國刑法 （民國 111 年 02 月 18 日 ） EN

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。

請先取得受測機關同意

並留下佐證資料

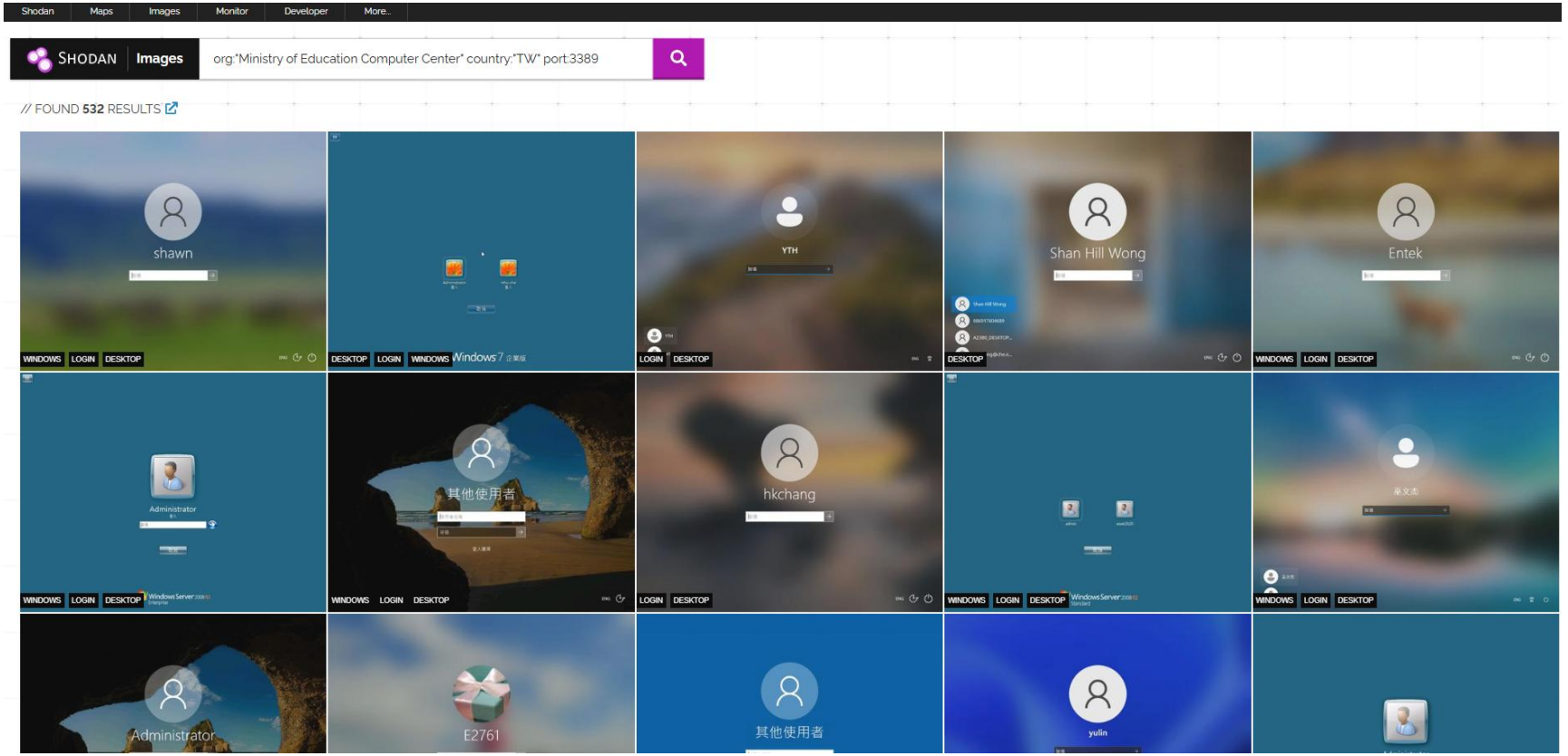
TACCST

正修科技大學
CHENG SHIU UNIVERSITY

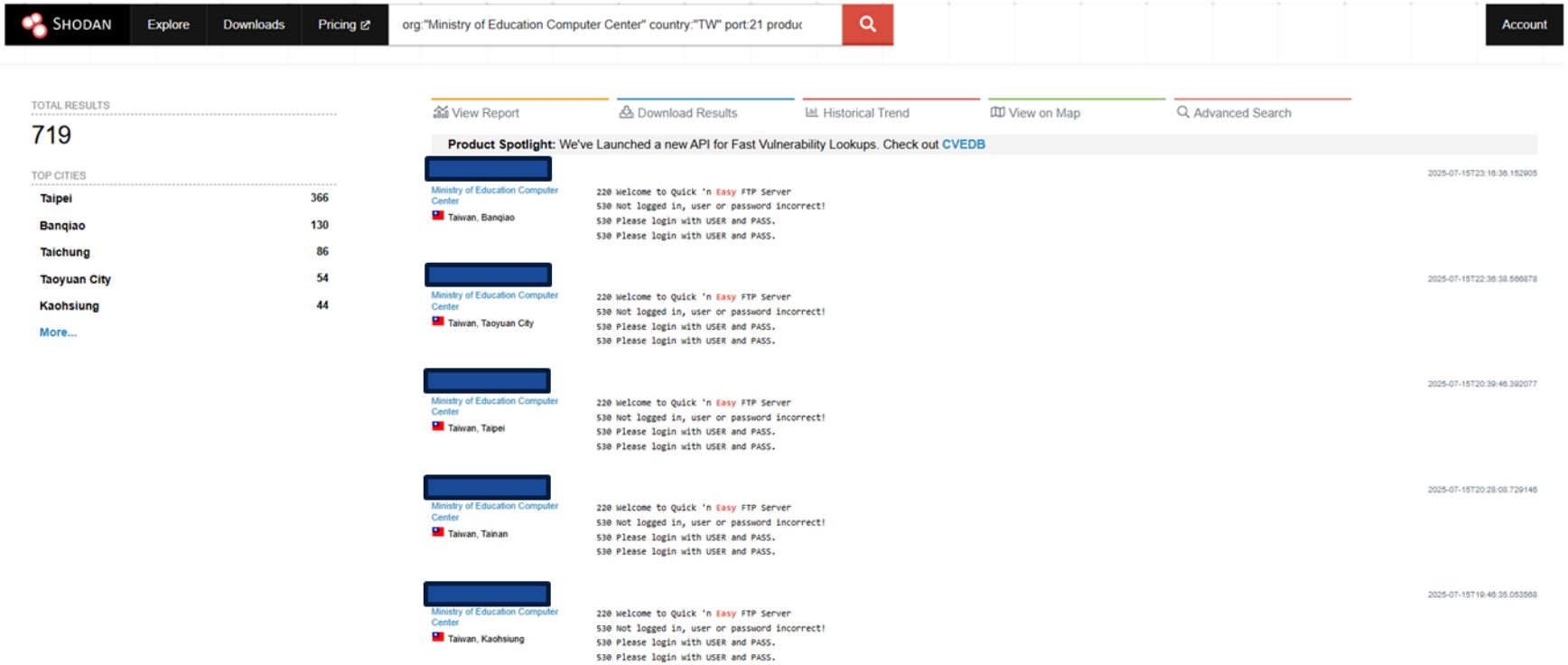
PART 01

使用者電腦安全檢測

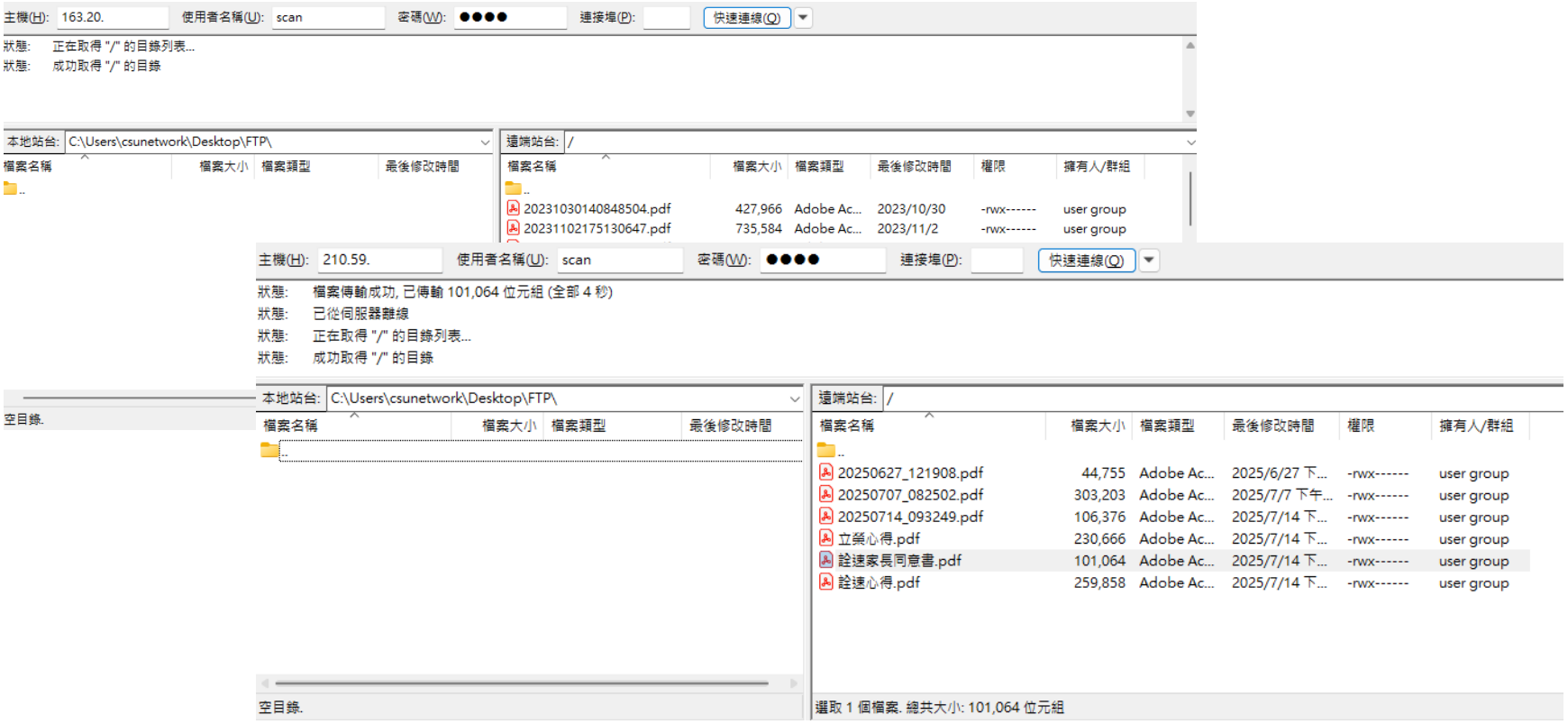
使用者電腦安全檢測


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Images
org:"Ministry of Education Computer Center" country:"TW" port:3389
// FOUND 532 RESULTS
shawn
YTH
Shan Hill Wong
Entek
Administrator
其他使用者
hkchang
Administrator
E2761
其他使用者
yulin

使用者電腦安全檢測


SHODAN
Explore
Downloads
Pricing
org:"Ministry of Education Computer Center" country:"TW" port:21 produc
Account
TOTAL RESULTS
719
TOP CITIES
Taipei 366
Banqiao 130
Taichung 86
Taoyuan City 54
Kaohsiung 44
More...
View Report
Download Results
Historical Trend
View on Map
Advanced Search
Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB
Ministry of Education Computer Center
Taiwan, Banqiao
220 Welcome to Quick 'n Easy FTP Server
530 Not logged in, user or password incorrect!
530 Please login with USER and PASS.
530 Please login with USER and PASS.
2025-07-15T23:16:36.152905
Ministry of Education Computer Center
Taiwan, Taoyuan City
220 Welcome to Quick 'n Easy FTP Server
530 Not logged in, user or password incorrect!
530 Please login with USER and PASS.
530 Please login with USER and PASS.
2025-07-15T22:36:38.566878
Ministry of Education Computer Center
Taiwan, Taipei
220 Welcome to Quick 'n Easy FTP Server
530 Not logged in, user or password incorrect!
530 Please login with USER and PASS.
530 Please login with USER and PASS.
2025-07-15T20:39:46.392077
Ministry of Education Computer Center
Taiwan, Tainan
220 Welcome to Quick 'n Easy FTP Server
530 Not logged in, user or password incorrect!
530 Please login with USER and PASS.
530 Please login with USER and PASS.
2025-07-15T20:28:08.729146
Ministry of Education Computer Center
Taiwan, Kaohsiung
220 Welcome to Quick 'n Easy FTP Server
530 Not logged in, user or password incorrect!
530 Please login with USER and PASS.
530 Please login with USER and PASS.
2025-07-15T19:46:35.053568

使用者電腦安全檢測


主機(H): 163.20.
使用者名稱(U): scan
密碼(W): ●●●●
連接埠(P):
快速連線(Q)
狀態: 正在取得 "/" 的目錄列表...
狀態: 成功取得 "/" 的目錄
本地站台: C:\Users\csunetwork\Desktop\FTP\
檔案名稱 檔案大小 檔案類型 最後修改時間
遠端站台: /
檔案名稱 檔案大小 檔案類型 最後修改時間 權限 擁有人/群組
20231030140848504.pdf 427,966 Adobe Ac... 2023/10/30 -rwx------ user group
20231102175130647.pdf 735,584 Adobe Ac... 2023/11/2 -rwx------ user group
主機(H): 210.59.
使用者名稱(U): scan
密碼(W): ●●●●
連接埠(P):
快速連線(Q)
狀態: 檔案傳輸成功, 已傳輸 101,064 位元組 (全部 4 秒)
狀態: 已從伺服器離線
狀態: 正在取得 "/" 的目錄列表...
狀態: 成功取得 "/" 的目錄
空目錄.
本地站台: C:\Users\csunetwork\Desktop\FTP\
檔案名稱 檔案大小 檔案類型 最後修改時間
遠端站台: /
檔案名稱 檔案大小 檔案類型 最後修改時間 權限 擁有人/群組
20250627_121908.pdf 44,755 Adobe Ac... 2025/6/27 下... -rwx------ user group
20250707_082502.pdf 303,203 Adobe Ac... 2025/7/7 下午... -rwx------ user group
20250714_093249.pdf 106,376 Adobe Ac... 2025/7/14 下... -rwx------ user group
立榮心得.pdf 230,666 Adobe Ac... 2025/7/14 下... -rwx------ user group
詮速家長同意書.pdf 101,064 Adobe Ac... 2025/7/14 下... -rwx------ user group
詮速心得.pdf 259,858 Adobe Ac... 2025/7/14 下... -rwx------ user group
空目錄.
選取 1 個檔案. 總共大小: 101,064 位元組

使用者電腦安全檢測

[redacted] 113 學年度學生職場參訪

「職場體驗」活動　家長同意書

茲同意敝子弟參加[redacted]4/30 安排之職場參訪活動，並已責令其於參訪期間注意安全，遵守各項規定，聽從師長指導，如有違規事件願接受校規及相關法規之處理。

謹致

學生姓名：高[redacted]

班　　級：[redacted]

手　　機：09[redacted]

家長(監護人)[redacted]

行動電話：0[redacted]

中　華　民　國　　年　　月　　日　填　具

新北市[redacted]小學

領　款　收　據

計劃案名稱	性平案調查報告撰稿費		所屬年度月份	中華民國 113 年 12 月	
費別	☐演講費 ■撰稿費 ☐審稿費 ☐出席費 ☐鐘點費 ☐諮詢費 ☐命題費 ☐口試費 ☐顧問費 ☐工作費 ☐臨時工資 ☐訪評費				
摘要	單位	單位數	單位金額	合計金額	代扣繳金額	實發金額
撰稿費(8,978字)	千字	8.9	1,100	9,790	0	9,790

姓名：[redacted]

服務單位：

行動電話：

e-mail：

戶籍地址：

(鄰里皆需填寫)

☑郵局：局號：[redacted] (7碼)帳號：[redacted] (7碼)

☐銀行：[redacted]分行 帳號

☐是 ☐否：附存摺影本。(匯款用，若曾與本校合作已附過可填否)

領款收據：茲收到新台幣　仟元整　上述款項已照數收訖　此據

簽名：[redacted]　中華民國 113 年 12 月 19 日

使用者電腦安全檢測

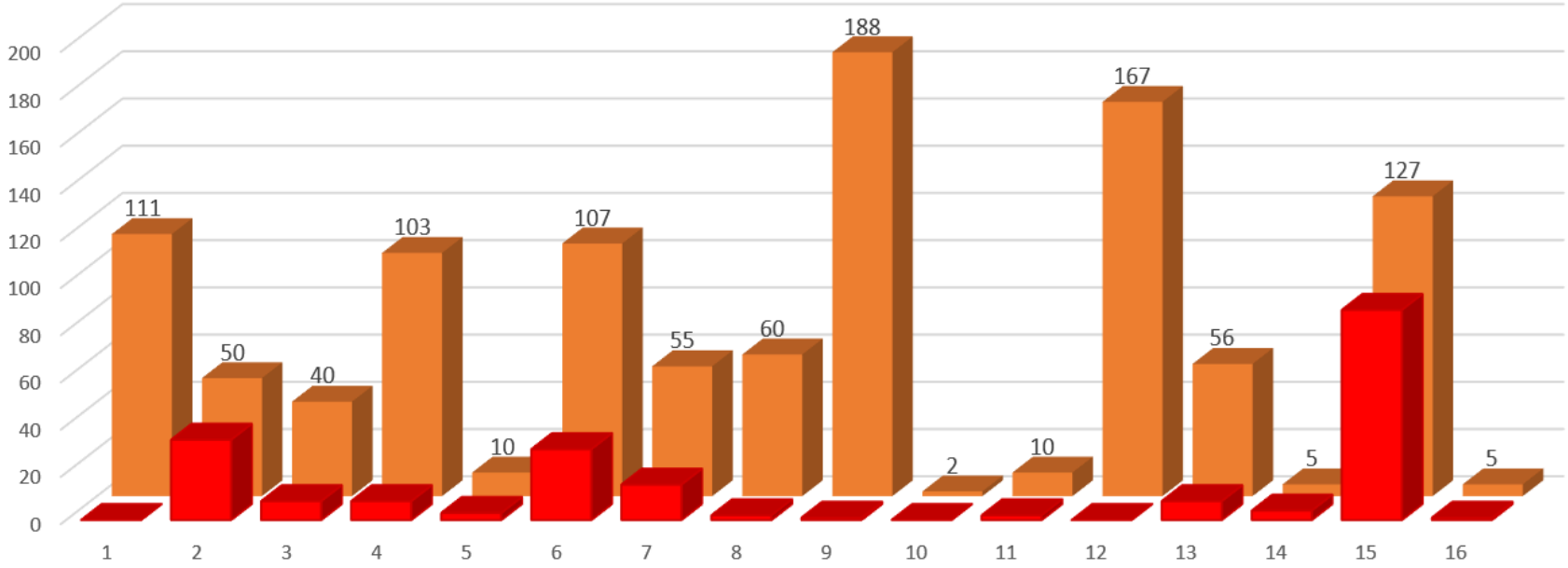
（一）使用者電腦弱點掃描結果，多具中、高風險弱點

（二）使用者電腦人工檢測結果發現

（三）未依機關政策落實系統安全性及更新、安裝具CVE弱點之軟體

使用者電腦安全檢測

（一）使用者電腦弱點掃描結果，多具中、高風險弱點



感謝育章老師的統計

使用者電腦安全檢測

常見中高風險弱點：

- SWEET32
- 弱加密 TLS 1.0 & 1.1
- 終止支援的作業系統
- 終止支援的應用程式
- 具CVE弱點的應用程式
- 授權不明的應用程式
- 系統更新後未重新開機，或累積更新未安裝
- 匿名登入/弱密碼/發現個資未刪除
- 不明惡意程式

使用者電腦安全檢測

常見中高風險弱點：

- SWEET32

改善方法：

- 禁用 3DES 加密套件

使用者電腦安全檢測

常見中高風險弱點：

- 弱加密 TLS 1.0 & 1.1

改善方法：

- 升級 TLS 版本，TLS 1.0 和 1.1 已不安全，應升級至 TLS 1.2 或 1.3。

使用者電腦安全檢測

SSL自我驗證(改善前後)

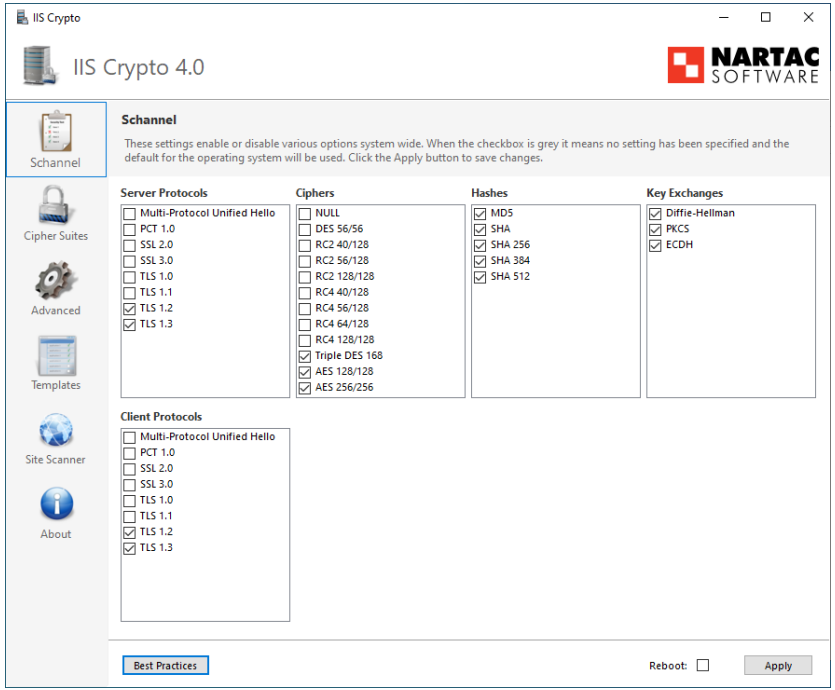
```
└─# nmap -script ssl-enum-ciphers -p8443 1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 10:39 CST
Nmap scan report for 1
Host is up (0.00084s latency).

PORT     STATE SERVICE
8443/tcp open  https-alt
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
```

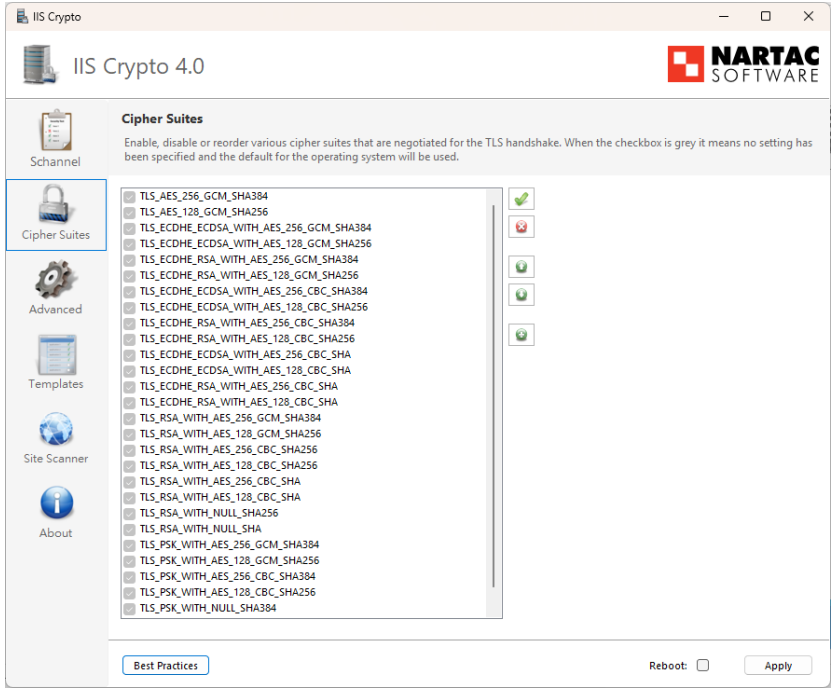
```
└─# nmap --script ssl-enum-ciphers -p 8834 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-21 01:47 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000043s latency).

PORT     STATE SERVICE
8834/tcp open  nessus-xmlrpc
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     cipher preference: server
|_  least strength: A
```

nmap –script ssl-enum-ciphers -443 www.abc.edu.tw

使用者電腦安全檢測

SSL自我驗證(改善前後)





https://www.nartac.com/Products/IISCrypto

使用者電腦安全檢測

常見中高風險弱點：

- 終止支援的作業系統

改善方法：

- 升級

Windows 10 支援已於 2025 年 10 月 14 日終止

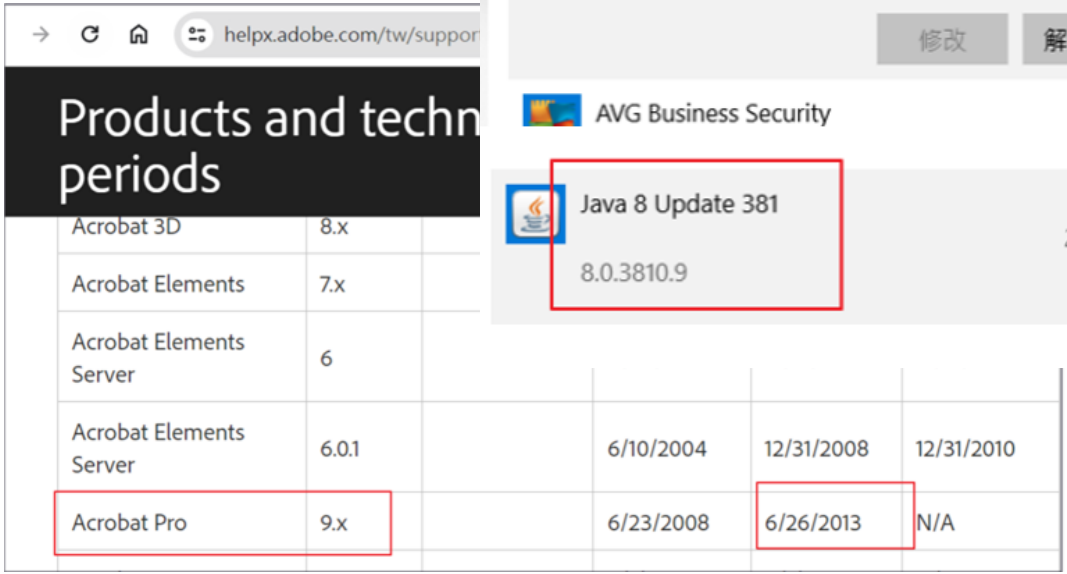
使用者電腦安全檢測

常見中高風險弱點：

- 終止支援的應用程式

改善方法：

- 更新



使用者電腦安全檢測

Windows 10 版本資訊

發行項 • 2025/02/25 • 3 位參與者　　意見反應

本文內容

- Windows 10 目前版本 (依服務選項)
- Windows 10 發行歷程記錄

注意

Windows 10 的最終版本是版本 22H2，將於 2025 年 10 月 14 日終止服務。

服務選項	更新類型	推出日期	組建	知識庫文章
正式版本通道	2025-04 B	2025-04-08	19045.5737	KB5055518
正式版本通道	2025-03 D	2025-03-25	19045.5679	KB5053643
正式版本通道	2025-03 B	2025-03-11	19045.5608	KB5053606
正式版本通道	2025-02 D	2025-02-25	19045.5555	KB5052077
正式版本通道	2025-02 B	2025-02-11	19045.5487	KB5051974
正式版本通道	2025-01 D	2025-01-28	19045.5440	KB5050081
正式版本通道	2025-01 B	2025-01-14	19045.5371	KB5049981
正式版本通道	2024-12 B	2024-12-10	19045.5247	KB5048652

https://learn.microsoft.com/zh-tw/windows/release-health/release-information

使用者電腦安全檢測

終止支援的產品

將於 2025 年終止支援下列受固定原則規範的產品與版本。

產品	終止支援
Dynamics C5 2015 Dynamics CRM 2015 Dynamics NAV 2015 Dynamics SL 2015 Visual Studio 2022 版本 17.6 (LTSC 通道)	2025 年 1 月 14 日
Dynamics GP 2015 Dynamics GP 2015 R2	2025 年 4 月 8 日
Microsoft SQL Server 2012、延伸安全更新第 3 年 SQL Server 2014 延伸安全更新第 1 年 Visual Studio 2022 版本 17.8 (LTSC 通道)	2025 年 7 月 8 日
Access 2016 Access 2019 Dynamics 365 Business Central 內部部署 (固定原則) Excel 2016 Excel 2019 Exchange Server 2016 Exchange Server 2019 Microsoft Office 2016 Microsoft Office 2019	2025 年 10 月 14 日

產品淘汰

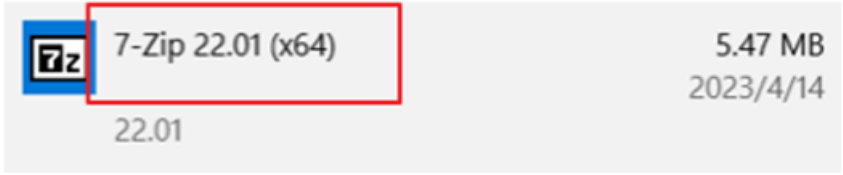
下列受新式原則規範的產品於 2025 年淘汰。

產品	退休
Microsoft Genomics	2025 年 1 月 6 日
Visual Studio App Center	2025 年 3 月 31 日
SAP HANA 大型執行個體 (HLI)	2025 年 6 月 30 日
適用於 MariaDB 的 Azure 資料庫	2025 年 9 月 19 日
Azure Basic Load Balancer Azure HPC Cache Azure 遠端轉譯 Azure 服務對應 Azure SQL Edge Azure 非受控磁碟 Azure vFXT	2025 年 9 月 30 日
Windows 10 企業版與教育版 Windows 10 家用版與專業版 Windows 10 IoT Enterprise	2025 年 10 月 14 日

使用者電腦安全檢測

常見中高風險弱點：

- 具CVE弱點的應用程式



改善方法：

- 更新

CVE-2025-0411 Detail

Description

7-Zip Mark-of-the-Web Bypass Vulnerability. This vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of archived files. When extracting files from a crafted archive that bears the Mark-of-the-Web, 7-Zip does not propagate the Mark-of-the-Web to the extracted files. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current user. Was ZDI-CAN-25456.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

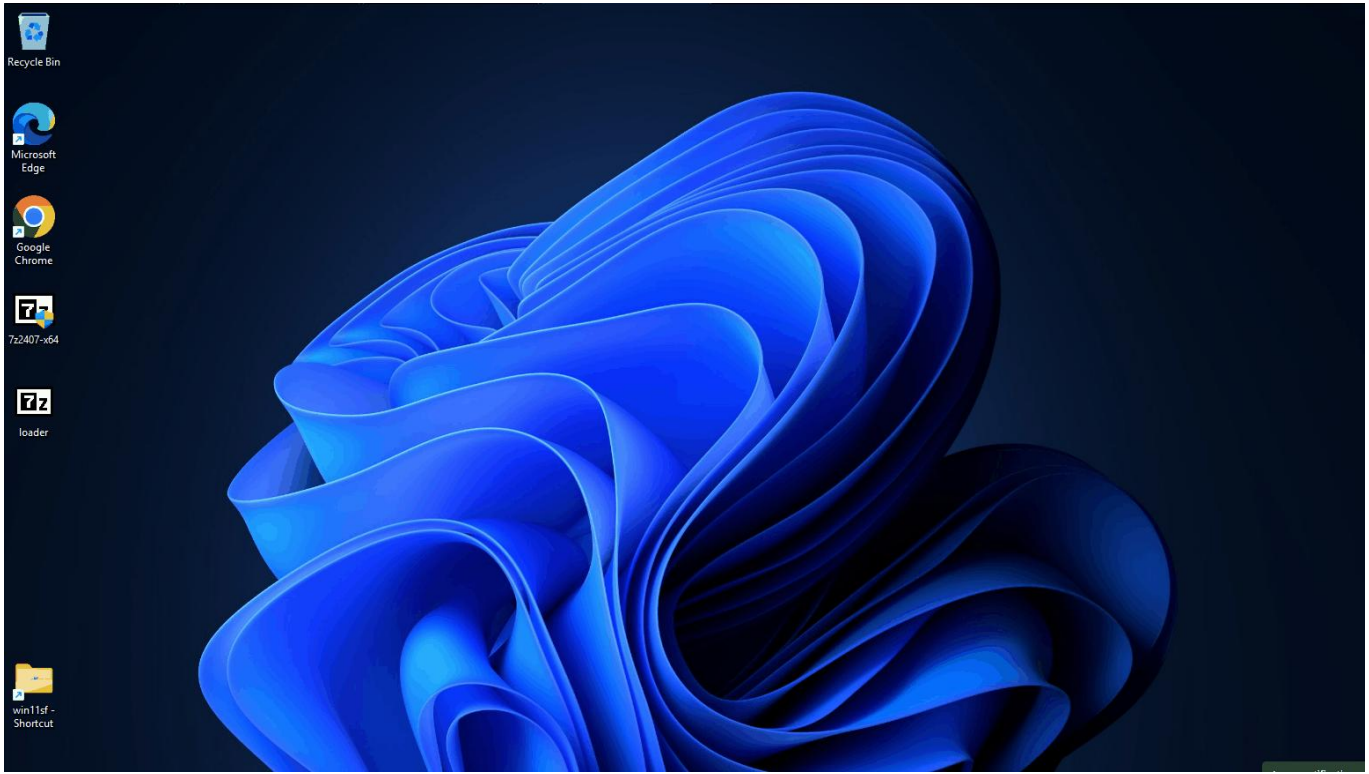
NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 7.0 HIGH	**Vector:** CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
CNA: Zero Day Initiative	**Base Score:** 7.0 HIGH	**Vector:** CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

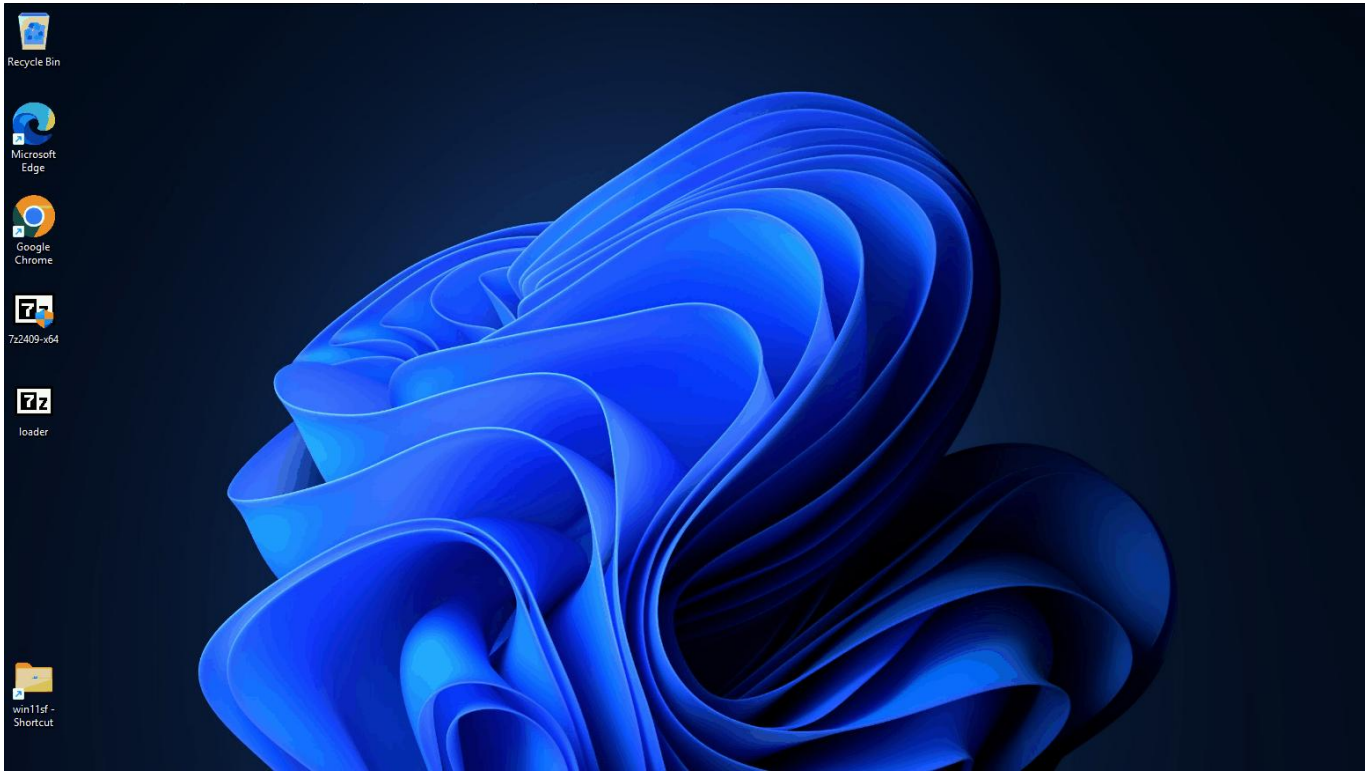
使用者電腦安全檢測

7Zip 24.07



使用者電腦安全檢測

7Zip 24.09



使用者電腦安全檢測

常見中高風險弱點：

- 授權不明的應用程式

改善方法：

- 檢查授權
- 或移除

CVE-2025-31334 Detail

Description

Issue that bypasses the "Mark of the Web" security warning function for files when opening a symbolic link that points to an executable file exists in WinRAR versions prior to 7.11. If a symbolic link specially crafted by an attacker is opened on the affected product, arbitrary code may be executed.

使用者電腦安全檢測

常見中高風險弱點：

- 授權不明的應用程式

改善方法：

- 檢查授權
- 或移除

CVE-2025-31334 Detail

Description

Issue that bypasses the "Mark of the Web" security warning function for files when opening a symbolic link that points to an executable file exists in WinRAR versions prior to 7.11. If a symbolic link specially crafted by an attacker is opened on the affected product, arbitrary code may be executed.

試用到期了，我還可以繼續用呀！

這會怎樣嗎？

RAR 壓縮工具使用及散佈使用權

以官方最新版本WinRAR中之License.txt為準

使用者授權合約

淺藍科技公司為 WinRAR 在台灣與中國之總代理，網址 https://rar.tw

中文版翻譯僅供參考。實際規定以下列英文條文為準。
本授權合約係 RAR (包括其視窗版本 - WinRAR) 壓縮軟體 (以下簡稱軟體) 用以規範 win.rar GmbH(以下簡稱授權方)與安裝、存取或其他任何使用此軟體的使用者(以下簡稱使用者)之條文。

1. 作者暨著作權所有人為 Alexander L. Roshal。授權方，亦即簽發授權者，亦即全球獨家使用權持有者包含重製權、發售及以能任何形式公開發佈者為 win.rar GmbH,Marienstr. 12, 10117 Berlin, Germany
2. 本軟體係以先試用後購買的形式發售，此定義為使用者在最多40天以內試用本軟體皆屬免費，在試用期滿後，使用者須購買授權才能繼續使用。
3. 本軟體除以下例外條件，皆能在不以任何形式更動原始封裝的條件下自由傳播:
    - 無書面授權者不得拆解本軟體封裝後加以傳播，但 UnRAR 元件例外。
    - 無書面授權者不得將未授權的試用版包裝於其他軟體之中。
    - 未更動的 WinRAR 安裝檔必須單純提供，不得與任何軟體搭配。任何搭售為禁止行為。未經 win.rar GmbH 書面同意，任何形式的搭售，特別是使用下載或安裝之軟體為禁止的行為。
    - 散播試用版者不得收錄、轉介或暗示駭客、破解、註冊金鑰或金鑰產生器等。
    - 倘若違反上述條件，則授權條件即自動立刻失效。

使用者電腦安全檢測

常見中高風險弱點：

- 系統更新後未重新開機，
  或累積更新未安裝

改善方法：

- 定期安裝與重開

使用者電腦安全檢測

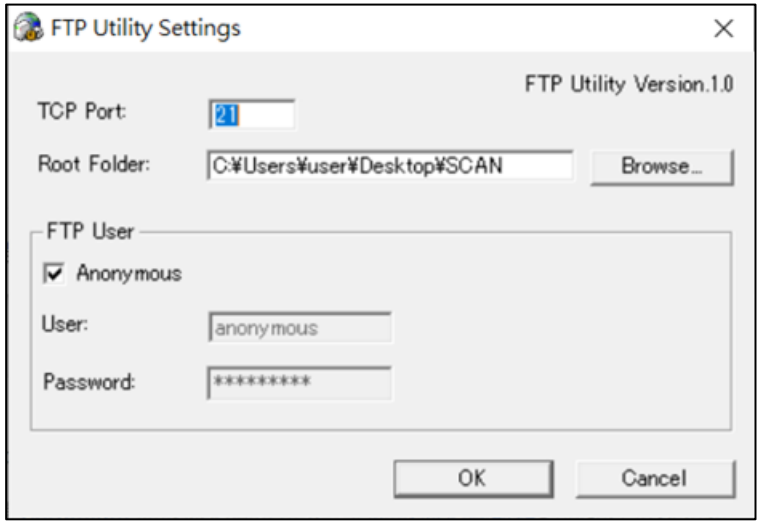
常見中高風險弱點：

- 匿名登入/弱密碼/發現個資未刪除

改善方法：

- ~~把事務機廠商抓來罰站~~
- 依存取控制建議設定

admin	qwerty
password	12345678
123456	admin123
root	123123
guest	scan
administrator	123



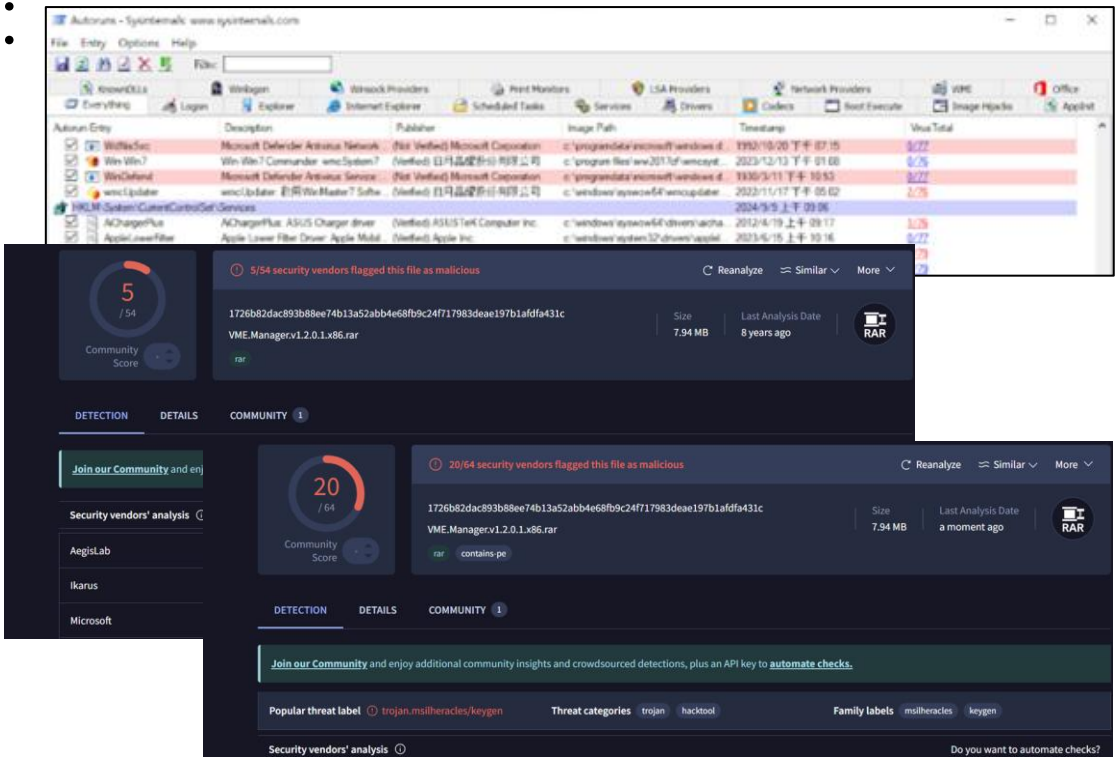
使用者電腦安全檢測

常見中高風險弱點：

- 不明惡意程式

改善方法：

- 確認程式用途
- 移除惡意程式



TACCST

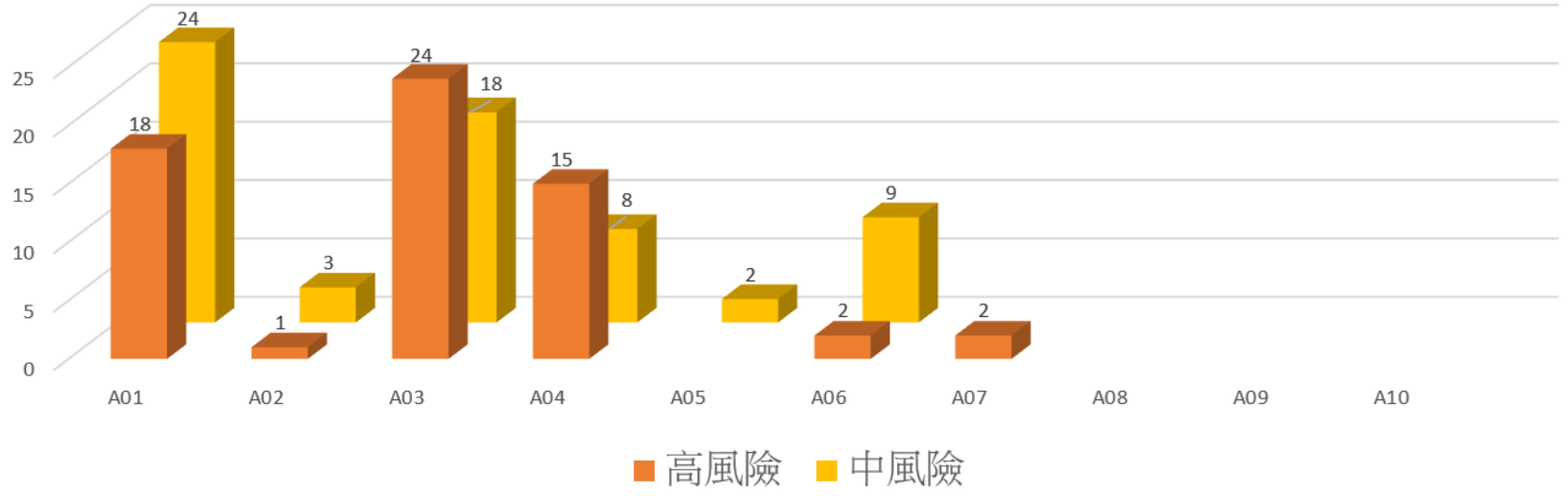
正修科技大學
CHENG SHIU UNIVERSITY

PART 02

資通系統安全檢測

資通系統安全檢測

（一）核心資通系統存在漏洞（僅統計高、中風險）



請問，這是什麼編碼？

this%20is%20web%20page

- URL encode
  - **URL只能包含ASCII字元**，URL不能存在非ASCII或含有不安全字元，瀏覽器會自動替換成合法的ASCII字元。
    - 例如：空白字元會用%20或+來替代。
      - https://www.example.com/news?str=this is web page會變成
      - https://www.example.com/news?str=this%20is%20web%20page

請問，這又是什麼編碼？

<script>alert("Hi")</script>

- HTML Escape
  - HTML要顯示**保留字**時需會使用**替代字元**。
    - 例如：

      顯示 < 要使用 <

      顯示 > 要使用 >

      顯示 “ 要使用 "

那，請問，這些又是什麼呢？

SGkgZ3V5c34=

a3886a8079dd5fa34995a6434b72932a

ChatGPT

分享

請問這是什麼，可以解開嗎
a3886a8079dd5fa34995a6434b72932a

2/2

這是一個 **MD5 雜湊值 (hash)**，它通常用於加密儲存密碼、文件驗證等用途。MD5 是單向加密演算法，理論上無法直接解密回原始內容，但可以嘗試透過 **彩虹表 (Rainbow Table)** 或字典攻擊來尋找可能的對應值。

如果這個 MD5 是來自常見的字串（例如密碼或短語），可以嘗試使用 **線上 MD5 反查工具**（如 md5decrypt.net 或 hashes.com）來看看是否已經有相對應的解密記錄。

如果你知道這個雜湊值來自什麼類型的資料（例如某個單詞、數字組合等），可以提供一些線索，我可以幫你試著破解看看！ 🚀

ChatGPT

分享

請問這是什麼，可以解開嗎
SGkgZ3V5c34=

這段文字看起來像是 Base64 編碼的字串。我來幫你解碼看看：

解碼後的結果是：**"Hi guys~"** 🎉

這是一段 Base64 編碼的文字，常用來對純文字進行簡單的編碼處理。

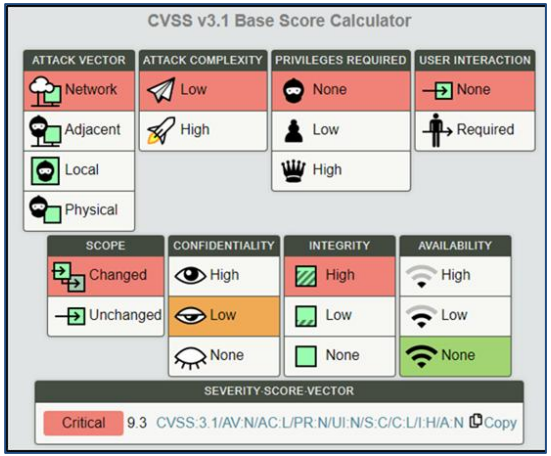
- Base64
  - **基於64個可列印字元來表示二進位資料的方法，每6 bits為一字元，24 bits(3 bytes)為一組，尾端不足3 bytes時，加上==或=表示缺乏的字元組數。**
    - echo -n Hi guys~ | base64 顯示 SGkgZ3V5c34=
    - echo SGkgZ3V5c34= | base64 -d 顯示Hi guys~
- MD5、SHA 雜湊
  - **雜湊函式把資料壓縮成訊息摘要，使資料量變小，固定資料長度**(wiki)。
  - 不能直接解密成原本的文字，但可以使用字典檔去對照來破解。
    - hello,world123 經過MD5雜湊後是 a3886a8079dd5fa34995a6434b72932a

- Cookie
  - **Cookie是一段由Server送給使用者瀏覽器的「資料(文檔)」，讓瀏覽器記下一些特定的資訊以便未來能夠更加方便被使用。**
- Session
  - **Session則是將資料紀錄在Server端上，Session 機制會在一個用戶完成身分認證後，接著產生一組對應的 ID ，存下所需的使用者資料。**

弱點的風險嚴重性評估

- 可使用如何衡量弱點低、中、高、嚴重等級？
  - **CVSS 3.1(Common Vulnerability Scoring System)**，使用8個因子計算。
    - 可用CVSS計算機協助計算，如CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N

因子	說明
攻擊向量 Attack Vector (AV)	透過{網路(N)/相鄰(A)/內部(L)/實體(P)}介面進行攻擊
攻擊複雜度 Attack Complexity (AC)	{低(L)、高(H)}複雜度
使用者操作 User Interaction (UI)	{無(N)、要(R)}求使用者介入
提權 Privileges Required (PR)	{無(N)、低(L)、高(H)}權限
影響範圍 Scope (S)	漏洞是否{有(U)、無(C)}影響其它元件
機密性影響 Confidentiality (C)	{高(H)、低(L)、無(N)}
完整性影響 Integrity (I)	{高(H)、低(L)、無(N)}
可用性影響 Availability (A)	{高(H)、低(L)、無(N)}



CVSS評估範例

- CVE-2024-4577 - PHP 遠端程式碼執行 - PHP CGI
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H　9.8 Critical

因子	說明
攻擊向量 Attack Vector (AV)	【N】弱點利用只要透過網路即可攻擊目標。
攻擊複雜度 Attack Complexity (AC)	【L】弱點已具備現成的攻擊程式或攻擊步驟簡易，不需要複雜攻擊步驟。
使用者操作 User Interaction (UI)	【N】弱點不需使用者進行額外操作，惡意程式，或變更預設值。
提權 Privileges Required (PR)	【N】弱點可在無特殊權限下被利用達到攻擊目的。
影響範圍 Scope (S)	【U】弱點被利用後，儘影響漏洞本身，不影響系統其它元件。
機密性影響 Confidentiality (C)	【H】針對目標系統進行評估，此例為每一項都是H。
完整性影響 Integrity (I)	
可用性影響 Availability (A)	


漏洞
消息
排行榜
組織
獎勵計劃
人才媒合
註冊 or 登入
漏洞
全部
活動中
修補中
公開
搜尋結果
有關 cve-2024-4577 的漏洞
搜尋漏洞
通報漏洞
某單位 CVE-2024-4577
ZD-2025-00553
[修補中] 風險：高
CVE-2024-4577 PHP遠端程式碼執行
某單位 公司CVE-2024-4577
ZD-2025-00551
[通報未回應] 風險：高
CVE-2024-4577 PHP遠端程式碼執行
某單位 公司CVE-2024-4577
ZD-2025-00548
[通報未回應] 風險：高
CVE-2024-4577 PHP遠端程式碼執行
某單位 CVE-2024-4577
ZD-2025-00547
[關閉] 風險：高
CVE-2024-4577 PHP遠端程式碼執行
1 / 12
+10

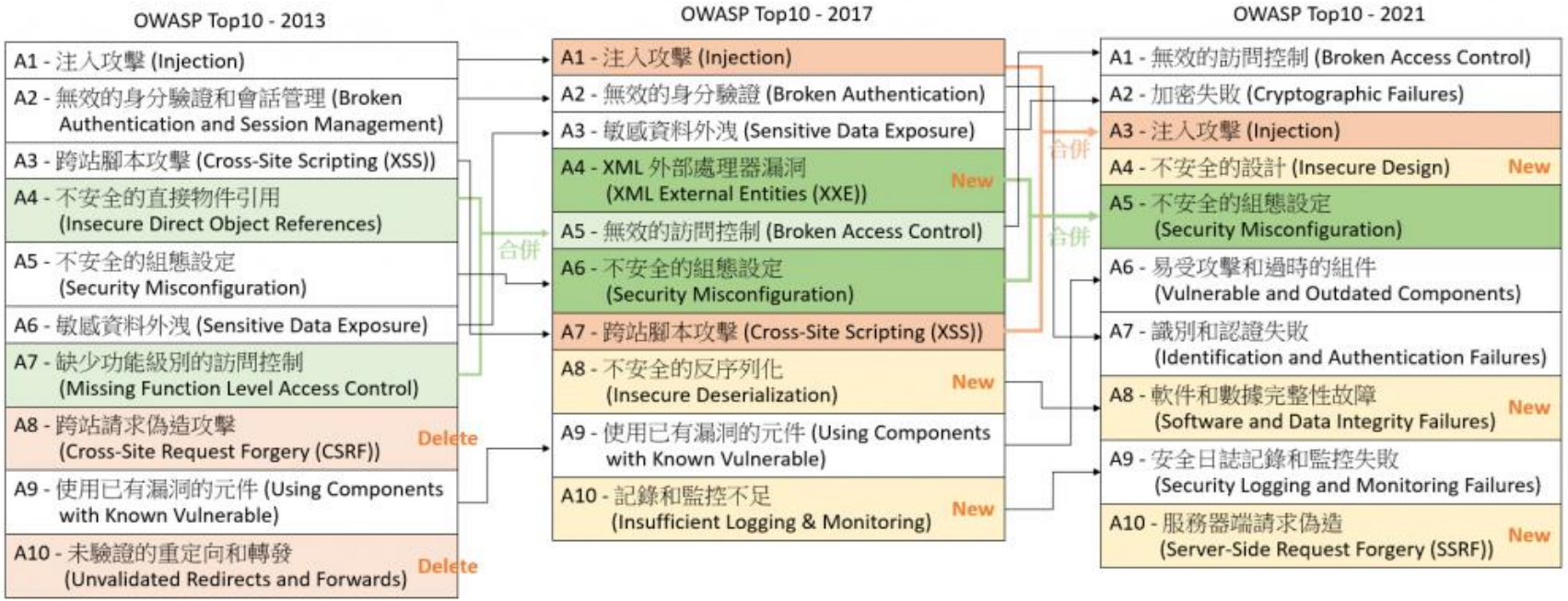
OWASP

- Open Web Application Security Project, OWASP基金會，非營利組織，關注軟體安全議題，最為人所知的是OWASP TOP 10、ZAP及OWASP Web Security Testing Guide。
- 2003年首次出版的「Top 10」整理常見的Web應用程式安全漏洞，並提出防護方法，可用來學習安全議題，並可讓我們知道需要優先檢測的項目。
- OWASP Top 10:2021 網站應用程式
- OWASP IoT Top 10:2018 物聯網設備
- OWASP Mobile Top 10:2016 行動裝置
- OWASP Top 10 for LLM Applications 2025 大型語言模型

資通系統安全檢測

- V A01:2021-Broken Access Control（權限控制失效）
- V A02:2021-Cryptographic Failures（加密機制失效）
- V A03:2021-Injection（注入式攻擊）
- V A04:2021-Insecure Design（不安全設計）
- V A05:2021-Security Misconfiguration（安全設定缺陷）
- V A06:2021-Vulnerable and Outdated Components（危險或過舊的元件）
- V A07:2021-Identification and Authentication Failures（認證及驗證機制失效）
- A08:2021-Software and Data Integrity Failures（軟體及資料完整性失效）
- A09:2021-Security Logging and Monitoring Failures（資安記錄及監控失效）
- A10:2021-Server-Side Request Forgery, SSRF（伺服端請求偽造）

資通系統安全檢測



圖片來源: https://ithelp.ithome.com.tw/articles/10304214

資通系統安全檢測

A01: 注入（ Injection ）

1.Sony PlayStation Network (2011) SQL 注入

攻擊者利用 SQL 注入漏洞竊取用戶資料庫中 7700 萬筆帳號資訊。

2.TalkTalk (2015) SQL 注入

英國電信公司遭受 SQL 注入攻擊，導致 15 萬客戶個資外洩。

3.Heartland Payment Systems (2009) SQL 注入

收單銀行系統的 SQL 注入漏洞，導致超過 1.3 億張信用卡資料遭竊。

4.Joomla! (CVE-2015-8562) PHP 物件注入

Joomla! 核心擴充元件的反序列化漏洞，可經由物件注入執行任意程式碼。

5.Adobe Magento (2016) SQL 注入漏洞

Magento 電商平台漏洞被利用，造成多家線上商店客戶資料外洩。

資通系統安全檢測

（一）核心資通系統存在漏洞

➢ 1. A01 權限控制失效（Broken Access Control）

➢ 例：**I**nsecure **D**irect **O**bject **R**eferences (IDOR)

https://insecure-website.edu.tw/posts/edit?id=132355

修改URL中id參數可繞過驗證機制↓ (No check)

https://insecure-website.edu.tw/posts/edit?id=132356

➢ 改善建議：

1) 使用者存取資源時確實檢查存取權限。
2) 避免將私密物件曝露給使用者、使用Index/Hash (salted)等方法而非直接讀取檔案。

https://portswigger.net/web-security/access-control/idor

資通系統安全檢測

- 修改 id 即可查別人的成績。

```
<td style="font-size: 10pt; color: darkred; cursor: pointe
r;" onmouseover="this.style.color='blue';" onmouseout="thi
s.style.color='darkred';" onclick="go_next('[redacted]','11
3','1','C[redacted]')" title="請按我可查詢歷年 成績">歷年 成績
</td> == $0
```

- 改善建議：使用者存取資源時確實檢查存取權限。

資通系統安全檢測

- 修改 id 即可修改他人密碼。

- 改善建議：使用者存取資源時確實檢查存取權限。

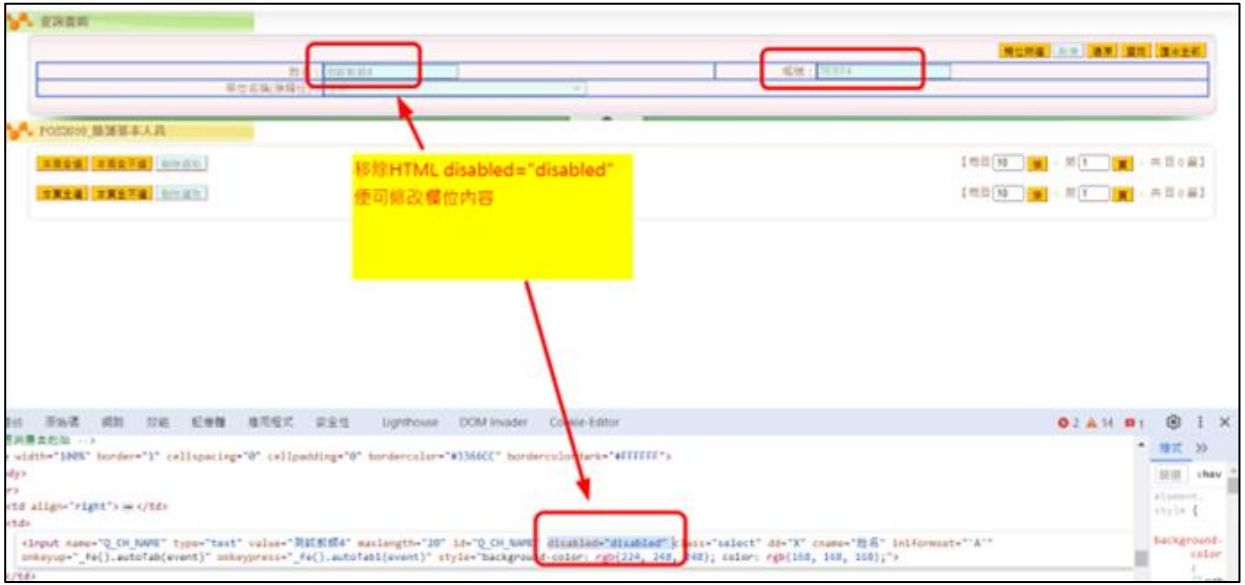
資通系統安全檢測

- 儲存時修改變數即可取得管理權限。

- 改善建議：使用者存取資源時確實檢查存取權限。

資通系統安全檢測

- 按F12去除disabled屬性即可使用該功能。



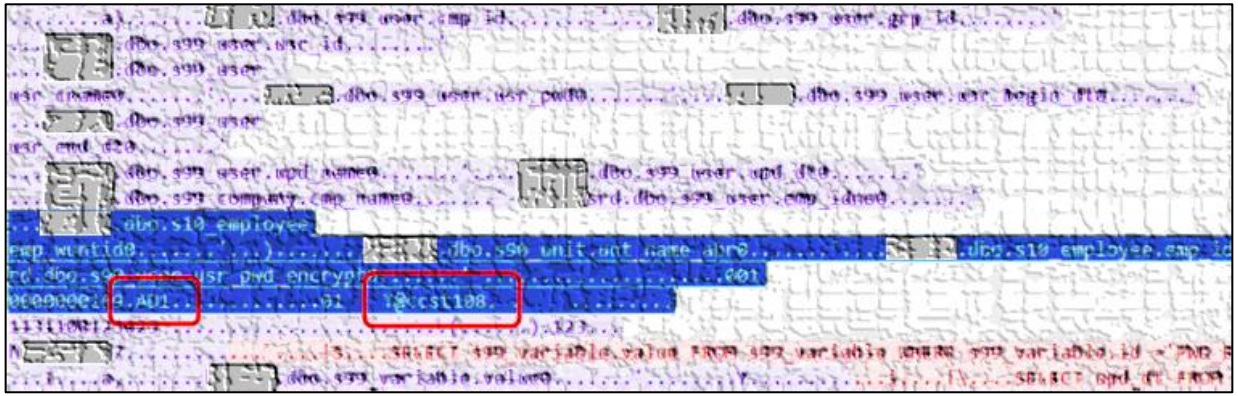
- 改善建議：應於伺服器端檢查權限。

資通系統安全檢測

（一）核心資通系統存在漏洞

➢ 2. A02 加密機制失效（Cryptographic Failures）

連線資料庫時未加密, 連線帳密與語法可被網路竊聽取得



➢ 改善建議：資料庫存取時應使用加密連線(尤其是 Client-Server 架構)。

資通系統安全檢測

（一）核心資通系統存在漏洞

➢ 3. A03 注入式攻擊（Injection）

SQL注入式攻擊(SQL injection)

跨網站腳本攻擊（Cross-Site Scripting, XSS）

- **反射性XSS (Reflected)**
- **儲存型XSS (Stored)**
- **DOM-based XSS**

➢ 改善建議：

- 程式使用參數化查詢方式(prepared statement)連接資料庫。
- 輸入資料驗證與Encoding (將使用者輸入轉成安全的資料再進行顯示或儲存)。

資通系統安全檢測

（一）核心資通系統存在漏洞

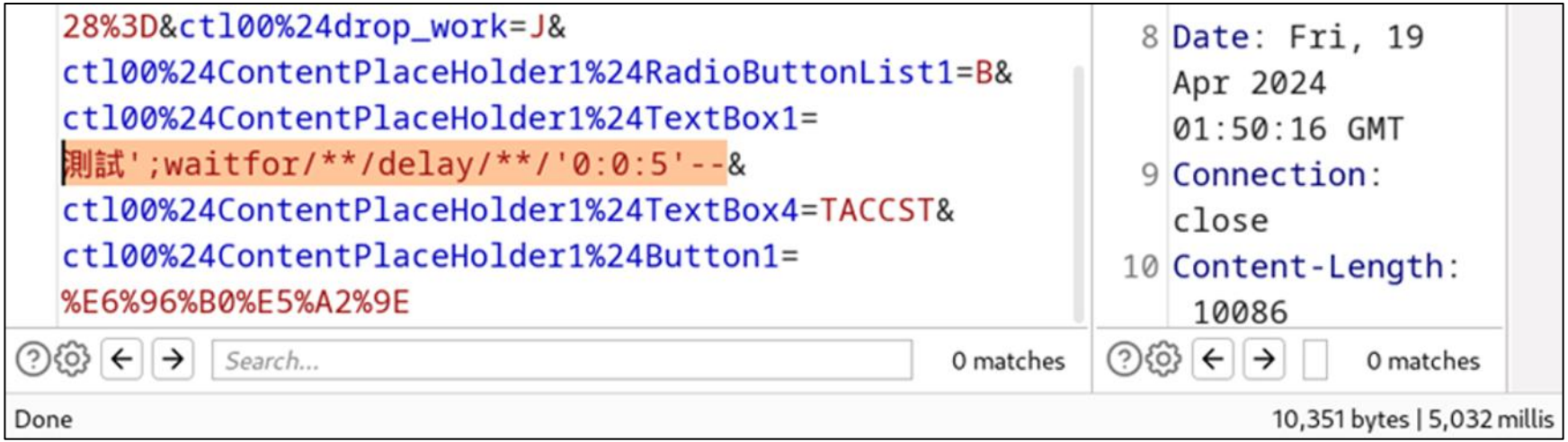
➢ 3. A03 注入式攻擊（Injection）

透過這類攻擊
實際檢測時撈到
很多個資

➢ 改善建議：程式使用參數化查詢方式(prepared statement)連接資料庫。

資通系統安全檢測

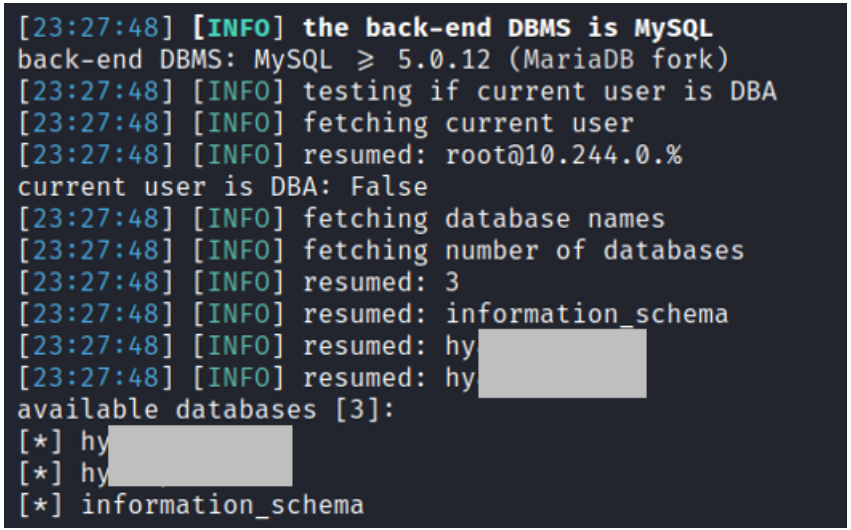
- 未正確過濾輸入資料，導致SQL注入語法生效(延遲5秒)。



- 改善建議：程式使用參數化查詢方式(prepared statement)連接資料庫。

資通系統安全檢測

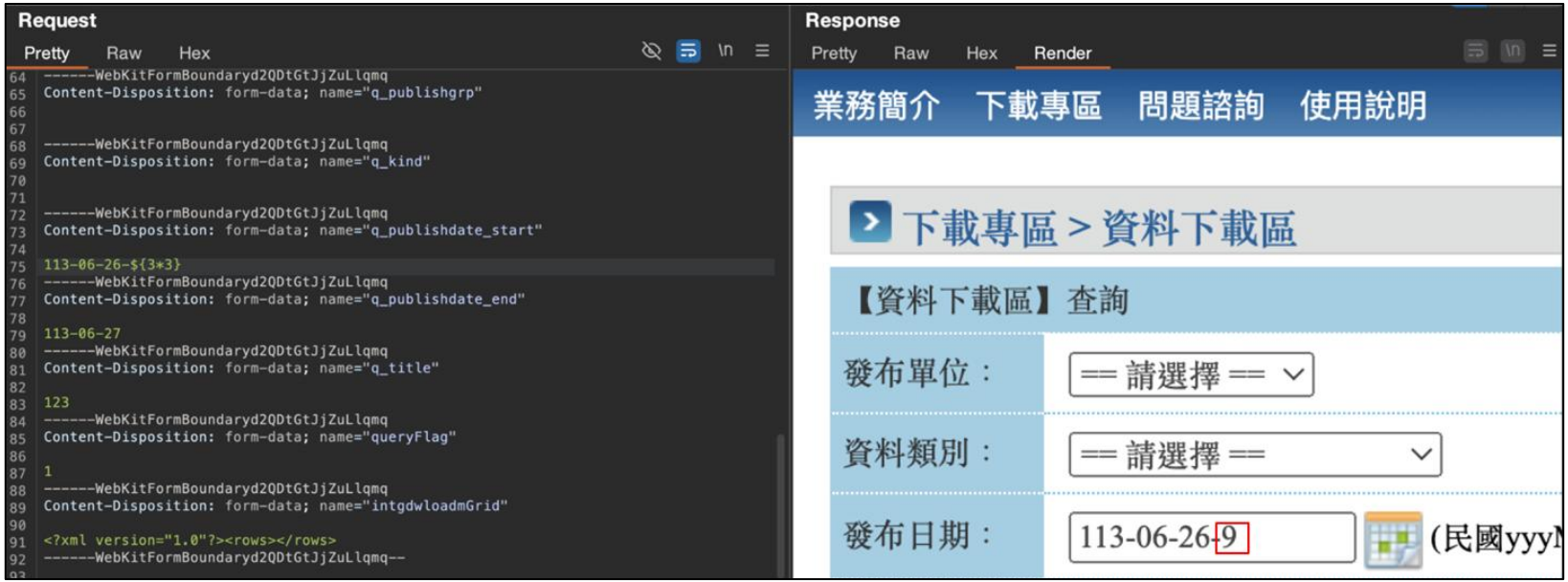
- 未正確過濾輸入資料，導致SQL注入語法生效。



- 改善建議：使用參數化查詢方式(prepared statement)連接資料庫。

資通系統安全檢測

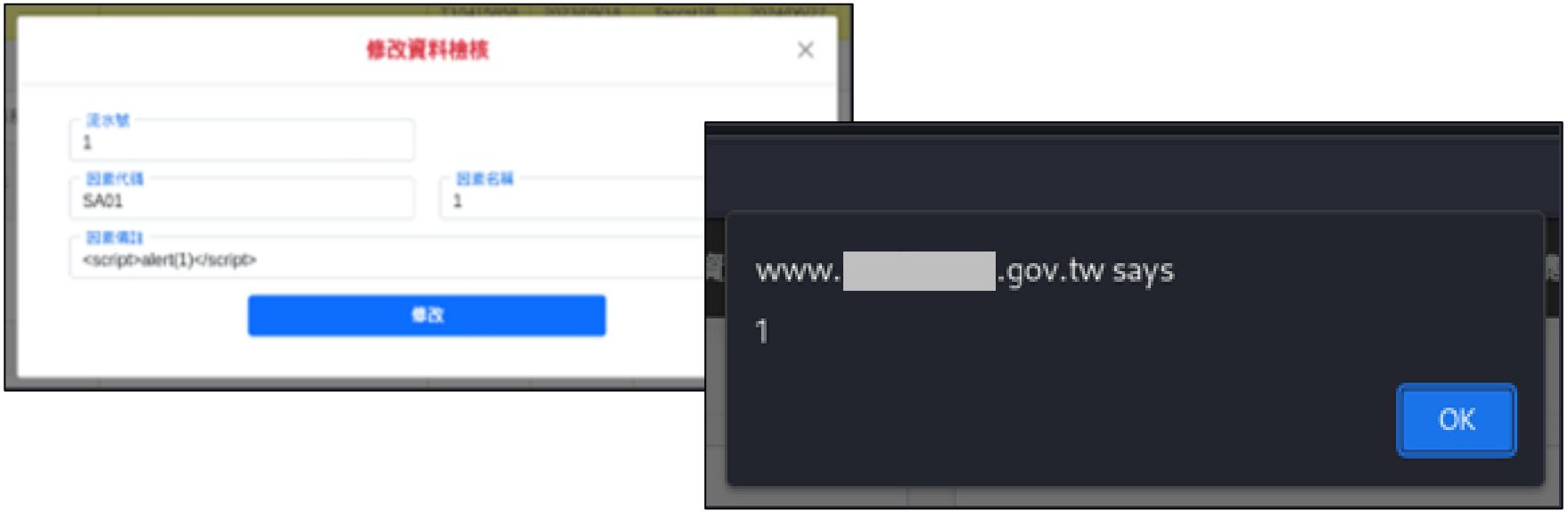
- 未正確過濾輸入資料，導致注入樣版語法生效(執行乘法運算)。



- 改善建議：應過濾使用者輸入資料。

資通系統安全檢測

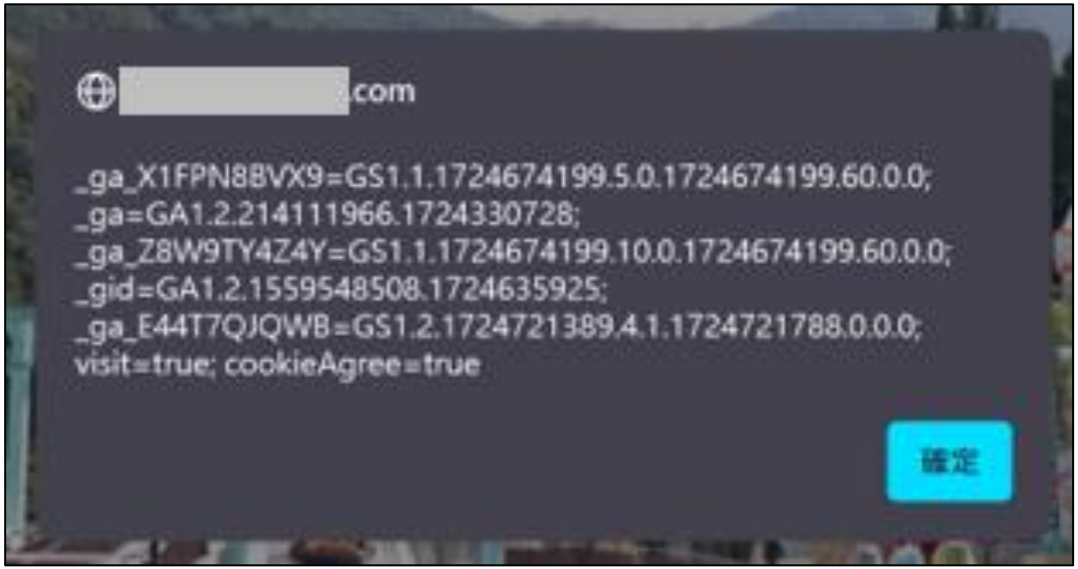
- 未正確過濾輸入資料，導致 xss 注入成功。



- 改善建議：應過濾使用者輸入資料。

資通系統安全檢測

- 未正確過濾輸入資料，導致 XSS 注入成功。



- 改善建議：應過濾使用者輸入資料+HTTPOnly。

資通系統安全檢測

（一）核心資通系統存在漏洞

➢ 4. A04 不安全設計（Insecure Design）

這類漏洞的高風險實例通常是被上傳Webshell

可上傳執行檔並執行

前端繞過

➢ 改善建議：於伺服器端檢查檔案類型，且勿讓使用者直接存取。

資通系統安全檢測

- 未正確檢查上傳檔案類型，導致遭上傳webshell。

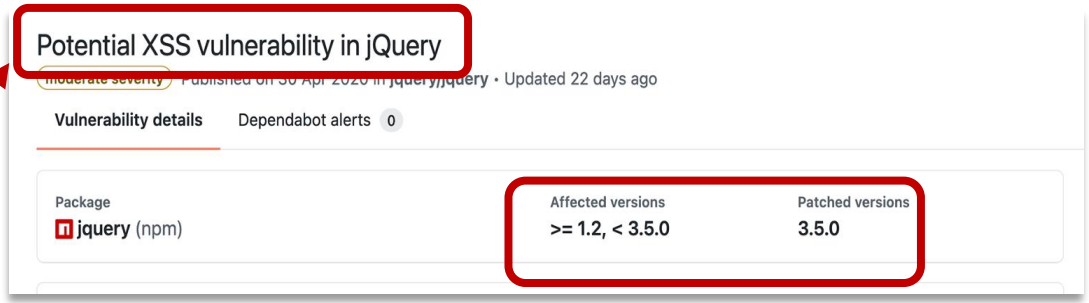
- 改善建議：於伺服器端檢查檔案類型，且勿讓使用者直接存取。

資通系統安全檢測

（一）核心資通系統存在漏洞

➢ 5. A06 危險或過舊元件（Vulnerable and Outdated Components）

- ➢ 例：如使用不安全的函式庫(Libraries)、框架(Framework)、模組(Module)等。



- ➢ 改善建議：網站及主機定期弱點掃描，並檢查使用元件版本有無安全性漏洞。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

分級	控制措施	數量	分級	控制措施	數量
普	處理錯誤訊息	14	中	系統使用規定	4
普	更新與修補	11	中	於伺服器端檢查輸入	4
普	密碼複雜度	10	中	校時	4
普	帳戶鎖定機制	9	中	遠端存取授權	4
普	日誌留存	4	中	遮蔽密碼	3
中	身分驗證	5	高	採用自動化監控工具	4

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。

- 改善建議：建議客製化錯誤頁面，僅顯示聯絡相關資訊與簡短錯誤代碼。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。

圖片來源：資通系統防護基準驗證實務

- 改善建議：系統管理者應盤點並保留業務運作必要開放之服務與埠口，作業系統應定期安裝更新檔案，亦應進行元件更新與弱點修補。

資通系統安全檢測

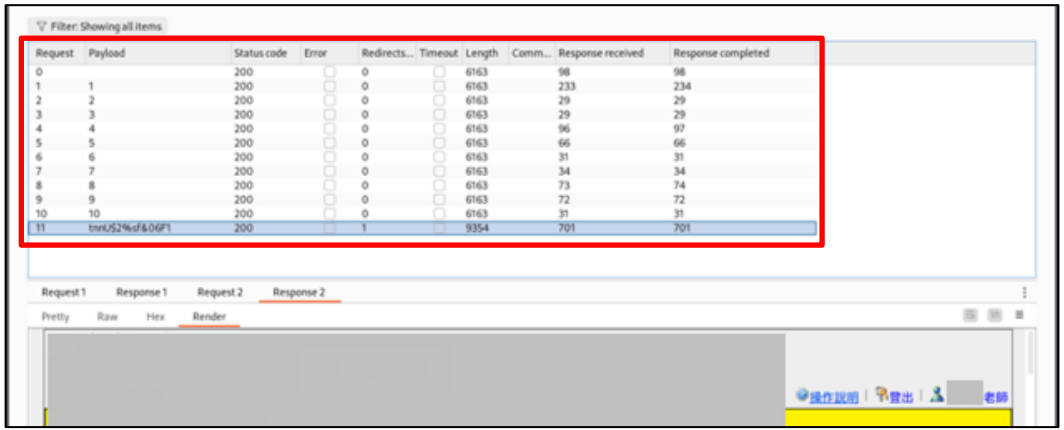
（二）未確實落實資通系統防護基準安全控制措施

- **使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。**
- 最低密碼複雜度目的在確保產生數量足夠之密碼組合，如密碼長度或組成字元種類基本要求等。
- 密碼最短效期則在**避免使用者為規避密碼歷程限制**，而於短時間內頻繁變更密碼。（多換幾次後換回來？）
- 強制密碼最長效期，可避免使用者長期使用同一個密碼而提高被破解之風險，建議以**不超過 6 個月為原則**。
- 改善建議：系統管理者應盤點並保留業務運作必要開放之服務與埠口，作業系統應定期安裝更新檔案，亦應進行元件更新與弱點修補。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。



- 改善建議：系統應實作帳戶鎖定機制以防範密碼破解攻擊。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。

資料來源：資通系統防護基準驗證實務

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

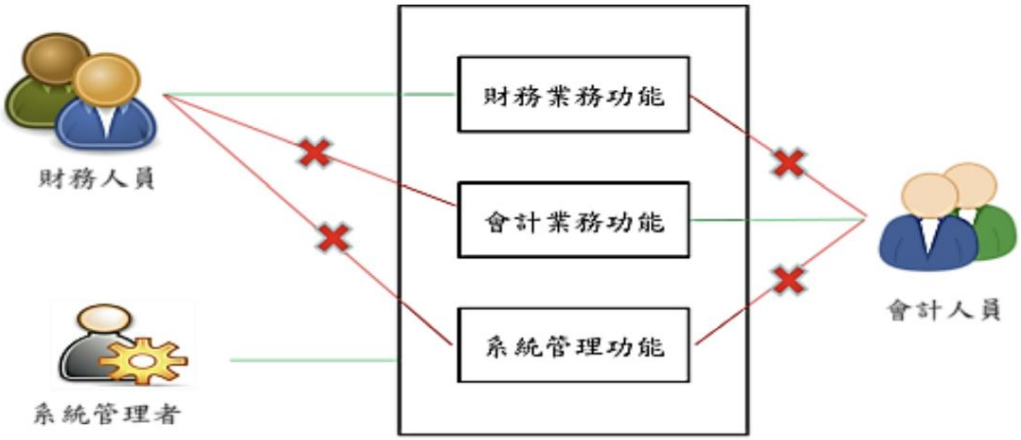
- 改善建議：請參考上表保留相關系統日誌。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。

圖片來源：資通系統防護基準驗證實務

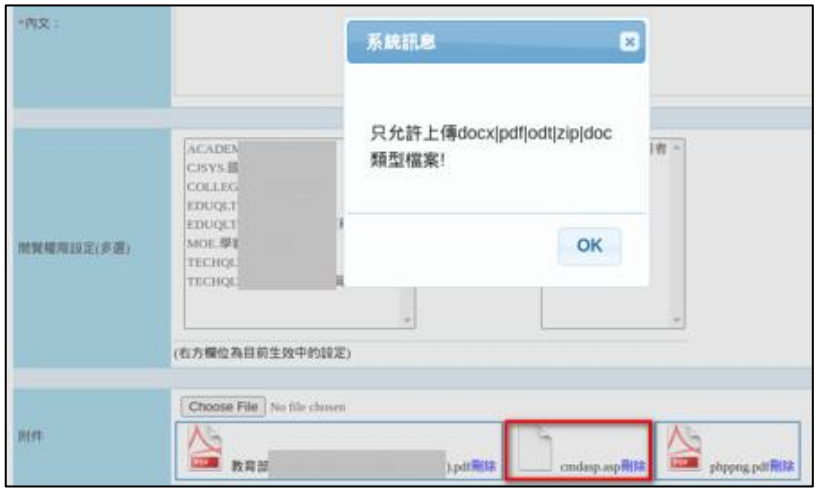


- 改善建議：請定期檢視授權是否正確。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- **使用者輸入資料合法性檢查應置放於應用系統伺服器端。**



系統顯示只允許上傳 docx、pdf、odt、zip、doc 等檔案類型，**卻被上傳 asp 檔**

- 改善建議：建議實作方式如於伺服器端建立資訊輸入白名單等，指定已知可信賴來源資訊輸入與可接受格式，或是以黑名單過濾惡意資料。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

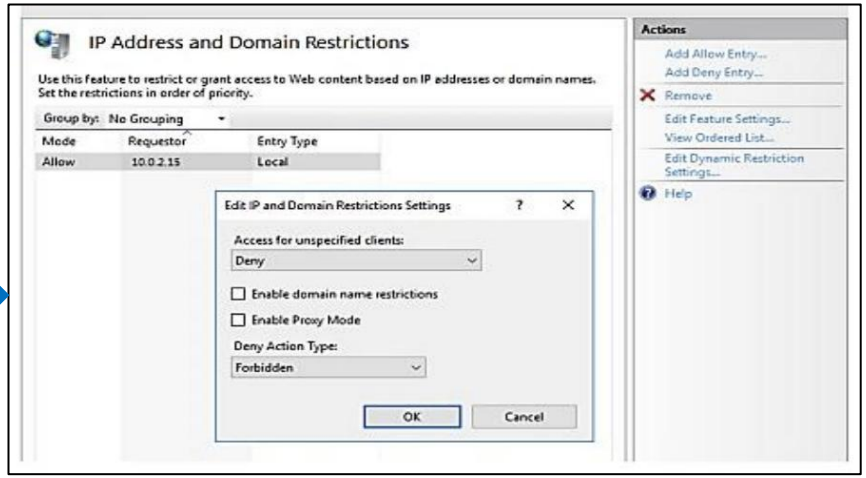
- **系統內部時鐘應定期與基準時間源進行同步。**
- 若以人工定期校正時間雖仍可保持時間正確性，但效率不佳且容易疏漏，故實務上常使用網際網路時間伺服器(NTP Server)或由機關自建之伺服器，並設定由系統依排程自動同步處理。
- 使用情境如 AD 成員主機向 AD 伺服器同步時間，而 AD 伺服器則與網際網路伺服器(如time.stdtime.gov.tw 等)進行同步。
- 改善建議：建議機關內設備皆向同一時間源同步時間，或特定閘道器向網際網路時間伺服器同步時間，其他設備則皆向該閘道器同步時間。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 遠端存取之來源應為機關已預先定義及管理之存取控制點。

圖片來源：資通系統防護基準驗證實務



IIS 限制連線來源操作範例

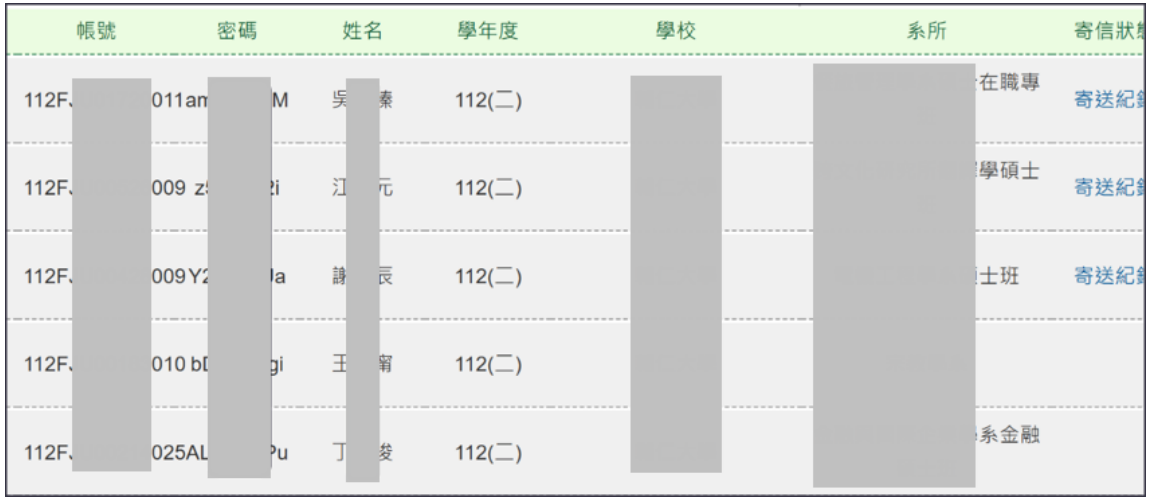
- 改善建議：遠端存取行為應通過授權後始可放行，如識別來源主機、來源或目的端 IP 位址、埠口及通訊協定等連線限制，避免全面性開放存取。

資通系統安全檢測

（二）未確實落實資通系統防護基準安全控制措施

- 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。

密碼明碼儲存



帳號	密碼	姓名	學年度	學校	系所	寄信狀態
112F	011am	M	112(二)		在職專	寄送紀錄
112F	009 z	i	112(二)		學碩士	寄送紀錄
112F	009Y2	a	112(二)		士班	寄送紀錄
112F	010 b	gi	112(二)			
112F	025AL	Pu	112(二)		系金融	

- 改善建議：密碼儲存時應經過加密或雜湊保護，實務上建議實作雜湊加鹽(Salted Hashing)技術，可有效對抗彩虹表等密碼破解攻擊手法。

資通系統安全檢測


2025 OWASP Top 10 List for LLM and Gen AI
LLM01:25
Prompt Injection
This manipulates a large language model (LLM) through crafty inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.
LLM02:25
Sensitive Information Disclosure
Sensitive info in LLMs includes PII, financial, health, business, security, and legal data. Proprietary models face risks with unique training methods and source code, critical in closed or foundation models.
LLM03:25
Supply Chain
LLM supply chains face risks in training data, models, and platforms, causing bias, breaches, or failures. Unlike traditional software, ML risks include third-party pre-trained models and data vulnerabilities.
LLM04:25
Data and Model Poisoning
Data poisoning manipulates pre-training, fine-tuning, or embedding data, causing vulnerabilities, biases, or backdoors. Risks include degraded performance, harmful outputs, toxic content, and compromised downstream systems.
LLM05:25
Improper Output Handling
Improper Output Handling involves inadequate validation of LLM outputs before downstream use. Exploits include XSS, CSRF, SSRF, privilege escalation, or remote code execution, which differs from Overreliance.
LLM06:25
Excessive Agency
LLM systems gain agency via extensions, tools, or plugins to act on prompts. Agents dynamically choose extensions and make repeated LLM calls, using prior outputs to guide subsequent actions for dynamic task execution.
LLM07:25
System Prompt Leakage
System prompt leakage occurs when sensitive info in LLM prompts is unintentionally exposed, enabling attackers to exploit secrets. These prompts guide model behavior but can unintentionally reveal critical data.
LLM08:25
Vector and Embedding Weaknesses
Vectors and embeddings vulnerabilities in RAG with LLMs allow exploits via weak generation, storage, or retrieval. These can inject harmful content, manipulate outputs, or expose sensitive data, posing significant security risks.
LLM09:25
Misinformation
LLM misinformation occurs when false but credible outputs mislead users, risking security breaches, reputational harm, and legal liability, making it a critical vulnerability for reliant applications.
LLM10:25
Unbounded Consumption
Unbounded Consumption occurs when LLMs generate outputs from inputs, relying on inference to apply learned patterns and knowledge for relevant responses or predictions, making it a key function of LLMs.
CC4.0 Licensed - OWASP GenAI Security Project
genai.owasp.org

資通系統安全檢測

ChatGPT search tool vulnerable to manipulation and deception, tests show

Exclusive: Guardian testing reveals AI-powered search tools can return false or malicious results if webpages contain hidden text

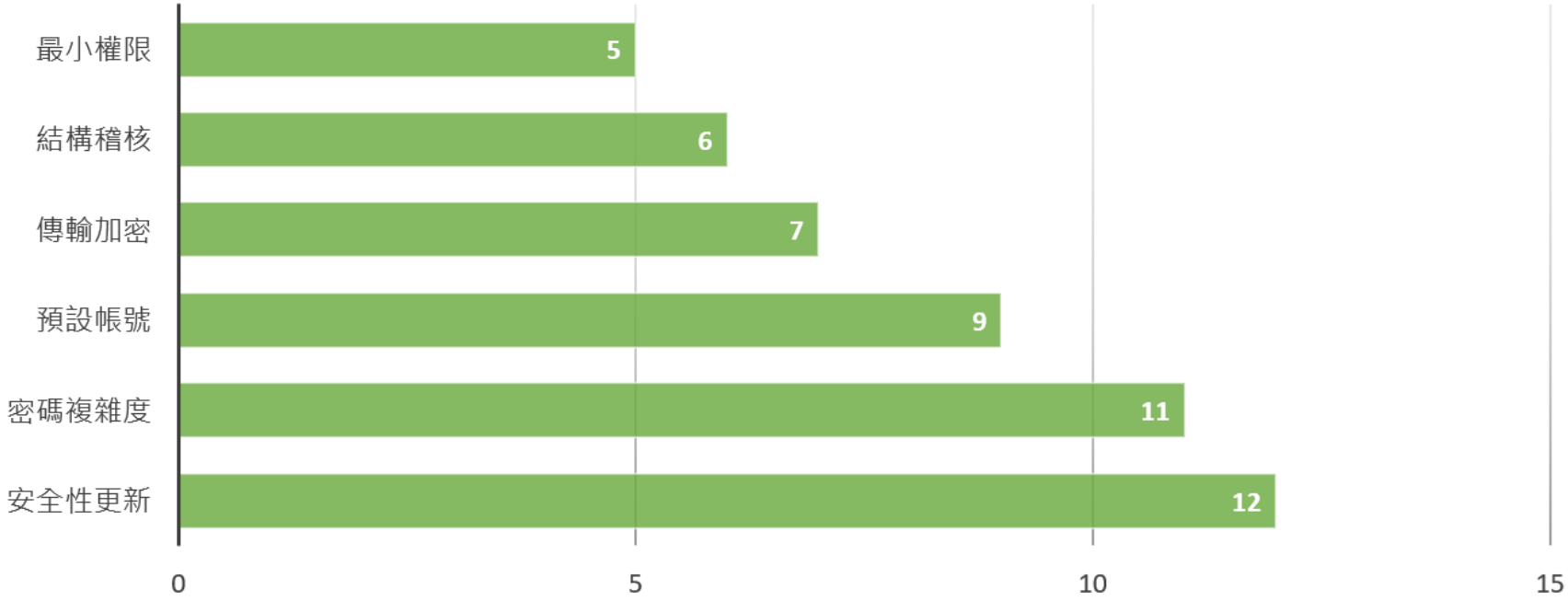
ChatGPT is being promoted as a search tool by OpenAI, but early testing shows a number of potential flaws with the current release. Composite: Angga Budhiyanto/Zuma Press Wire/Shutterstock

TACCST 正修科技大學 CHENG SHIU UNIVERSITY

PART 03

資料庫安全檢測

資料庫安全檢測



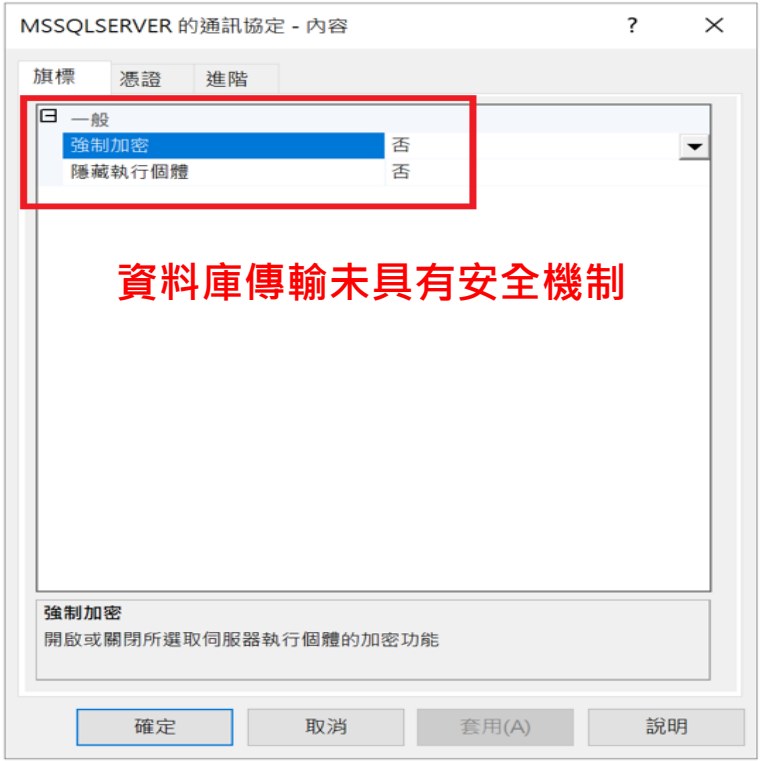
資料庫安全檢測

常見發現不符合事項

- **弱點管理：修補**資料庫主機**安全性更新**項目
- **特權帳號管理：啟用密碼複雜度**原則
- **特權帳號管理：變更**資料庫**預設管理帳號**
- **資料加密：**資料庫**傳輸具有安全機制**
- **稽核紀錄：**啟用**資料結構變更**稽核
- **存取授權：**資料庫**帳號權限最小**原則

資料庫安全檢測


登入屬性 - sa
選取頁面
一般
伺服器角色
使用者對應
狀態
指令碼
說明
設定
連線到資料庫引擎的權限:
授與(G)
拒絕(D)
登入:
已啟用(E)
已停用(S)
狀態
SQL Server 驗證:
登入已經鎖定(L)
連線
檢視連接屬性

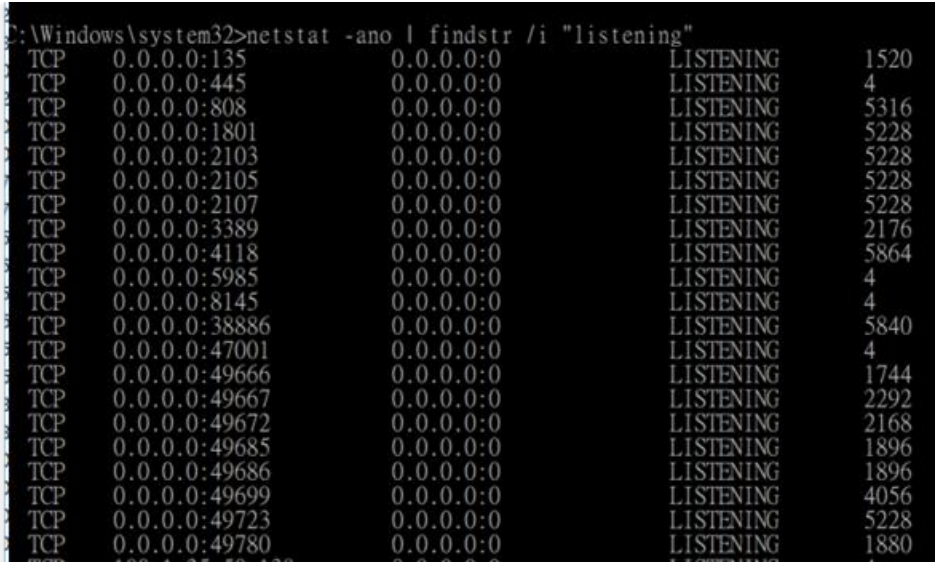

MSSQLSERVER 的通訊協定 - 內容
旗標
憑證
進階
一般
強制加密
否
隱藏執行個體
否
資料庫傳輸未具有安全機制
強制加密
開啟或關閉所選取伺服器執行個體的加密功能
確定
取消
套用(A)
說明

資料庫安全檢測

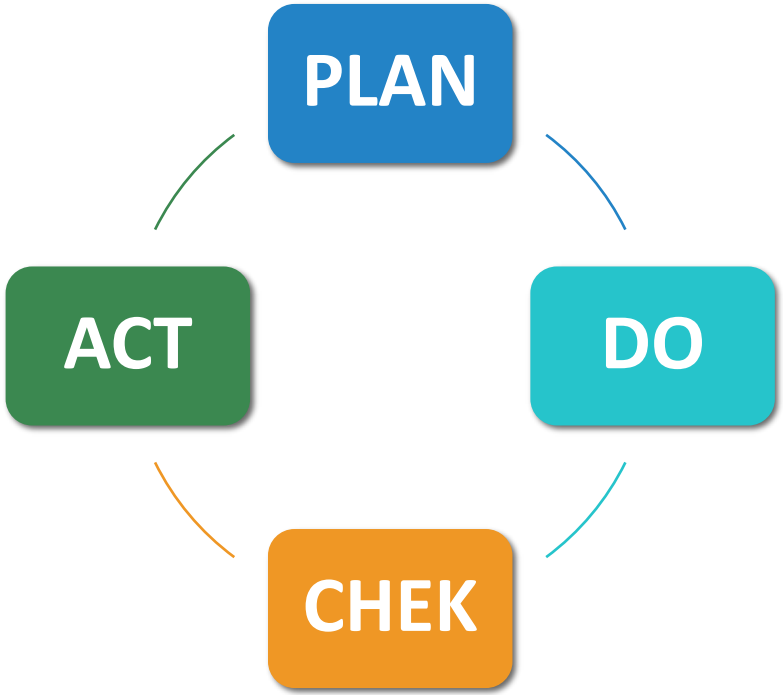

安全性實體
狀態
連線
Windows 驗證(W)
SQL Server 驗證(S)
密碼(P):
確認密碼(C):
指定舊密碼(I)
舊密碼(O):
未啟用密碼複雜度原則
強制執行密碼原則(F)
強制執行密碼逾期(X)
已對應到憑證(R)
已對應到非對稱金鑰(T)
對應到認證(M)
加入(A)
已對應的認證
認證
提供者

資料庫安全檢測

未限制遠端存取來源



```
C:\Windows\system32>netstat -ano | findstr /i "listening"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1520
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING       5316
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       5228
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       5228
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       5228
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       5228
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2176
  TCP    0.0.0.0:4118           0.0.0.0:0              LISTENING       5864
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:8145           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:38886          0.0.0.0:0              LISTENING       5840
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1744
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2292
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       2168
  TCP    0.0.0.0:49685          0.0.0.0:0              LISTENING       1896
  TCP    0.0.0.0:49686          0.0.0.0:0              LISTENING       1896
  TCP    0.0.0.0:49699          0.0.0.0:0              LISTENING       4056
  TCP    0.0.0.0:49723          0.0.0.0:0              LISTENING       5228
  TCP    0.0.0.0:49780          0.0.0.0:0              LISTENING       1880
```



弱點修補要留意
是否確實修復

細心驗證以確認

工商服務

教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology


台湾百種の味
台灣美食地圖
100 tastes of Taiwan
©YICHI'S ILLUSTRATION
北
台北
桃園
宜蘭
金門
台中
花蓮
澎湖
台南
台東
高雄
古早味 / 古い味
冰・飲品 / アイス・ドリンク
早餐 / 朝食
點心 / おやつ
伴手禮 / お土産
主食配菜 / 主食とおかず
ようこそ

教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

正修科技大學
CHENG SHIU UNIVERSITY

E N D