Pickle Rick

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!

- Kiểm tra view-source ta tìm thấy 1 thông tin quan trọng

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <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 find the last three secret ingredients to finish my pickle-reverse potion. The 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: R1ckRul3s

  -->

</body>
</html>

```

- Username: R1ckRul3s
- Có lẽ sẽ dùng đến sau này

- Ta cũng không tìm thấy gì khi quét Nmap:

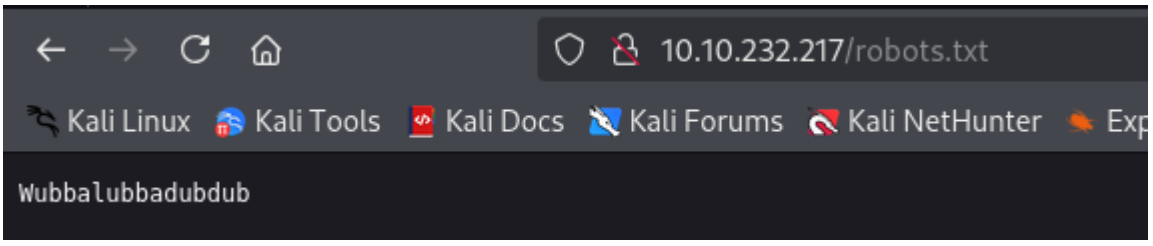
```
┌──(trantrien㉿kali)-[~]
└─$ nmap -p- -sV -sC 10.10.232.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-08 01:25 EDT
Nmap scan report for 10.10.232.217
Host is up (0.22s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 5e:b3:05:4c:ee:37:f7:33:5e:a1:26:a1:9e:79:97:37 (RSA)
|   256 61:5b:1c:d8:50:9b:3a:8c:64:a7:2d:a4:45:eb:90:de (ECDSA)
|_  256 aa:bf:eb:68:0f:6d:fe:cc:1f:2d:15:10:92:8a:f2:16 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 1268.55 seconds
```

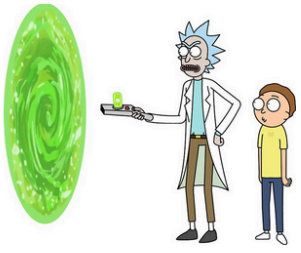
- Sử dụng gobuster:

```
┌──(trantrien㉿kali)-[~]
└─$ gobuster dir -u http://10.10.232.217 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.232.217
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/robots.txt           (Status: 200) [Size: 17]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/assets               (Status: 301) [Size: 315] [--> http://10.10.232.217/assets/]
```

- Ta vào robot.txt



- Có lẽ đây là mật khẩu cho user??
- Ta tiếp tục khám phá với portal.php:



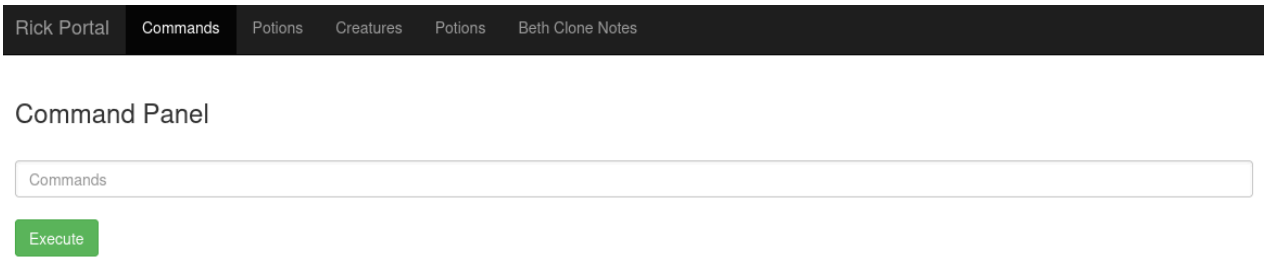
Portal Login Page

Username:

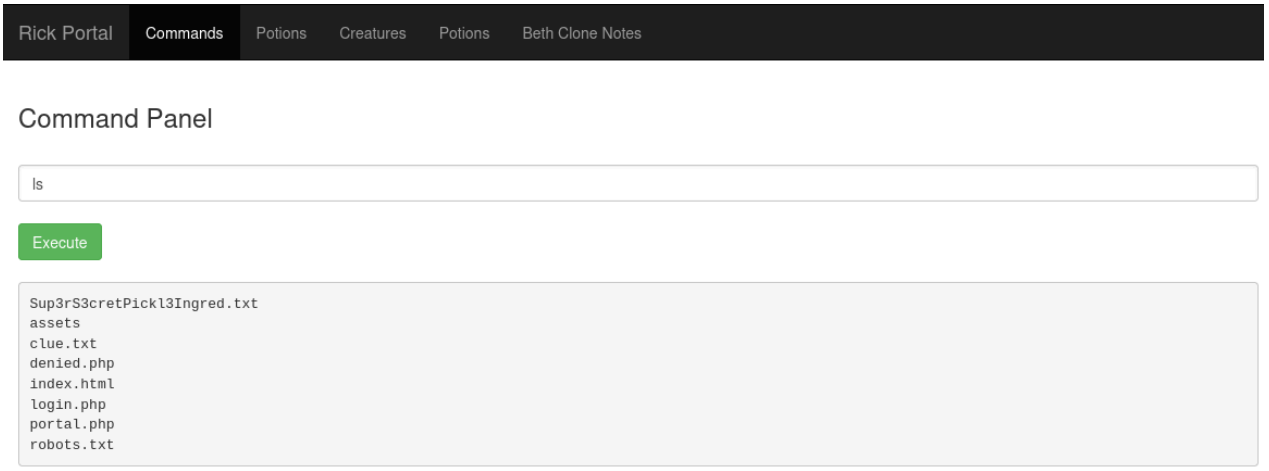
Password:

Login

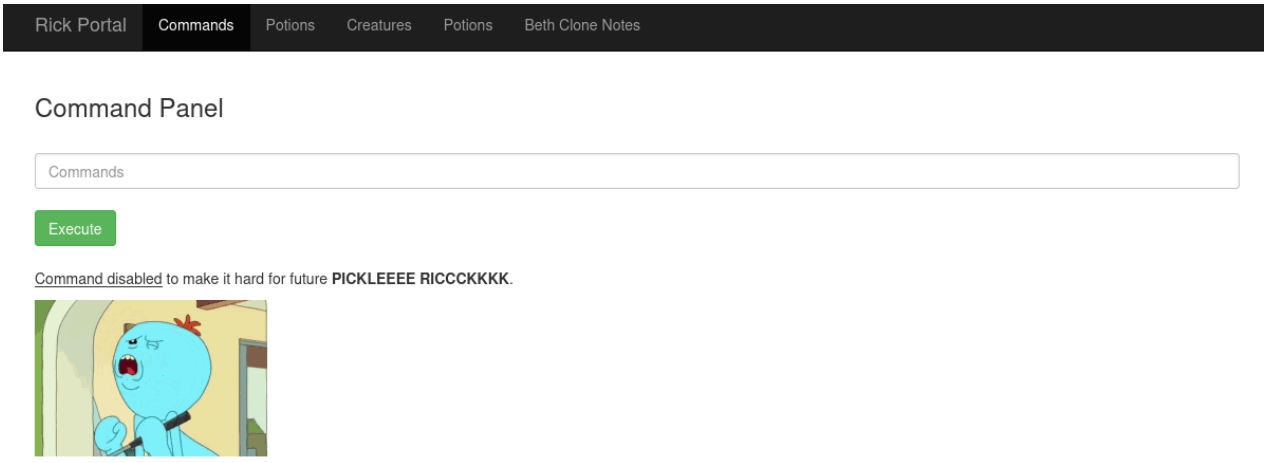
- Tiến hành đăng nhập thử với username và pass



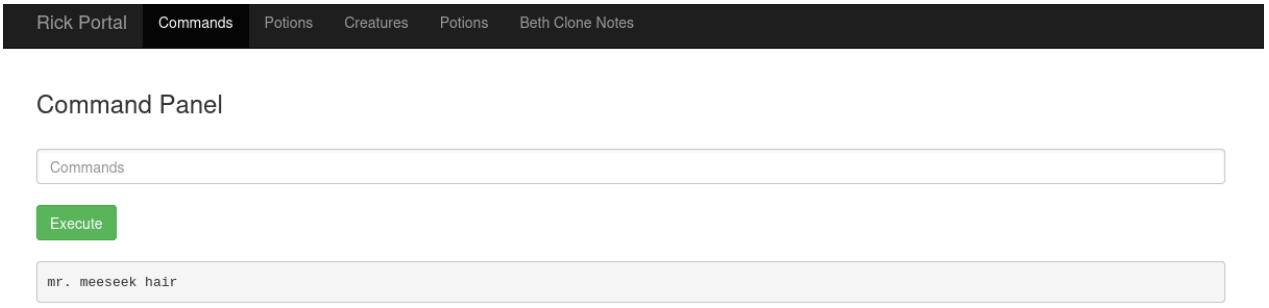
- Có lẽ ta đang đi đúng hướng
- Thử 1 vài lệnh trong linux vì ta thấy Command Panel



- Khi sử dụng lệnh cat ta thấy:

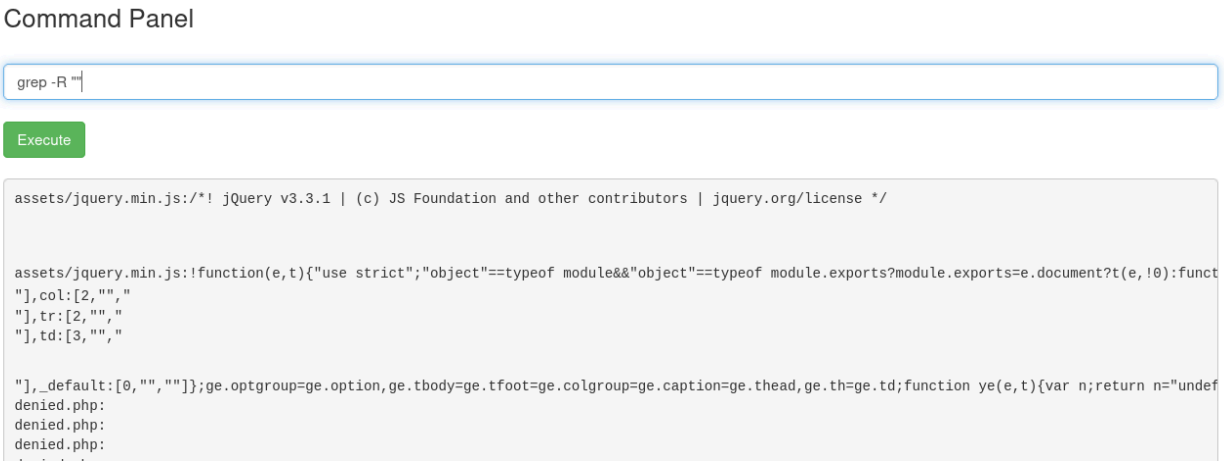


- Có lẽ nó không thể sử dụng được nhưng hãy thử với lệnh khác chẳng hạn như less:

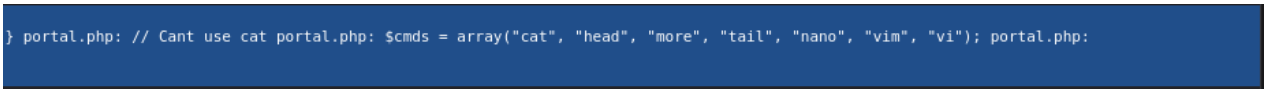


- Chúng ta đã có được thành phần đầu tiên.

- Chúng ta cần biết tại sao lệnh cat không sử dụng được

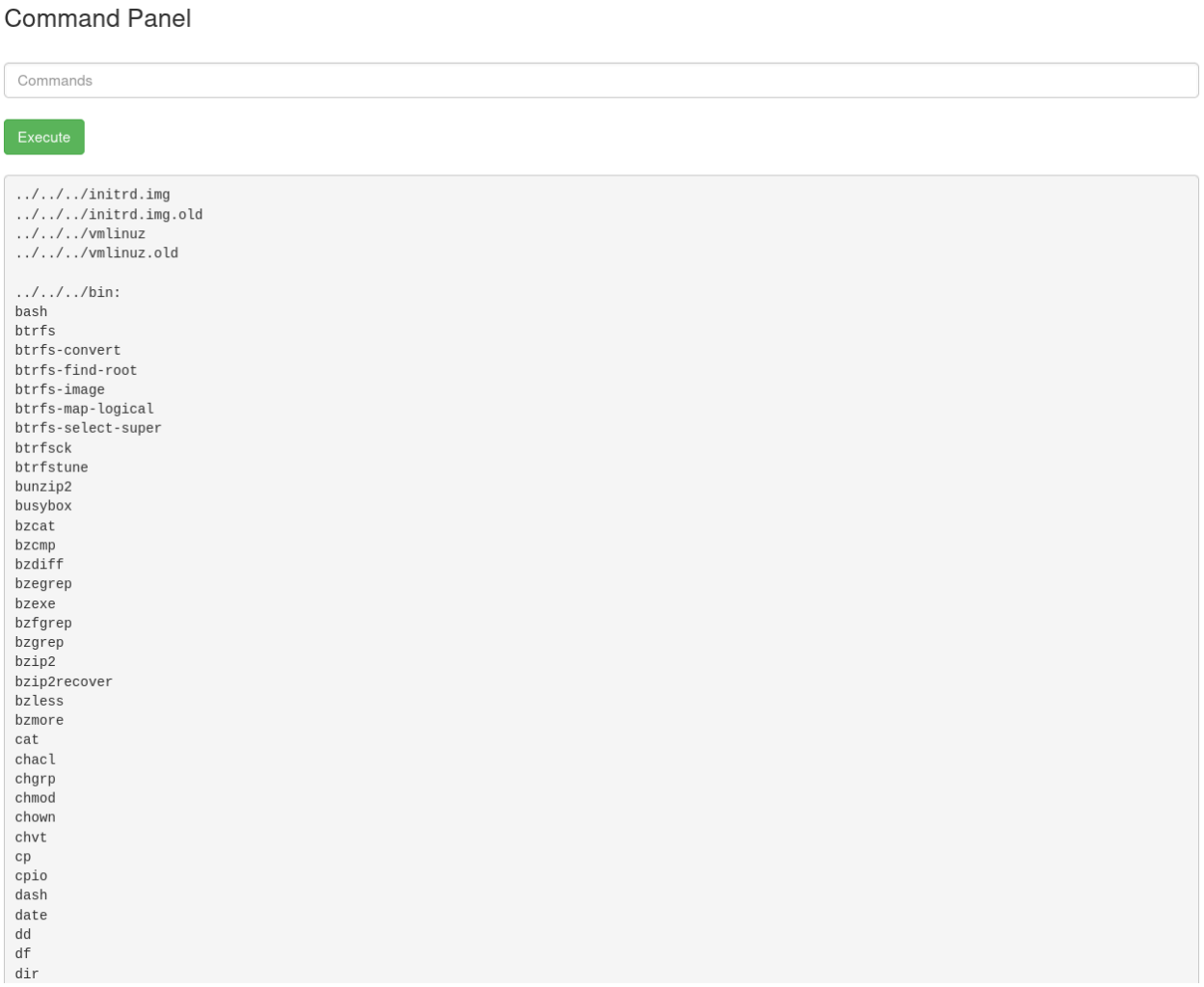


- Có lẽ do file denied.php chăng? Chúng ta inspector trang này và thấy được 1 vài lệnh đã bị cấm không thể dùng:



- Hãy thử 1 vài lệnh và bạn sẽ thấy ta cần sử dụng sudo để privileges.

- Để tìm cờ thử 2 và 3 bạn cần sử dụng lệnh sudo ls ../../../*:



- Khám phá hết tất cả các thư mục và bạn sẽ tìm được cờ thứ 2 ở /home/rick/second ingredients và cờ thứ 3 ở : root/3rd.txt
- Khi bạn đã làm quen thì bạn nên chú ý các thu mục như home, root trước.