**TryHackMe: Pickle Rick Room Write-Up [No Answers]**

A picture containing diagram

Description automatically generated

TryHackMe Pickle Rick Room Logo

**Room Description:** *“A Rick and Morty CTF. Help turn Rick back into a human!”*

**Task 1**: **Pickle Rick**

**Task Description:** 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.

Deploy the virtual machine on this task and explore the web application: 10.10.120.246

You can also access the web app using the following link: [https://10-10-120-246.p.thmlabs.com](https://10-10-120-246.p.thmlabs.com/) (this will update when the machine has fully started)

**CTF Start:** Now that the VM has started we can access the web app and have a look around.

Graphical user interface, website

Description automatically generated

Pickle Rick Web App (Rick is sup4r cool)

One thing that I always like to do with web apps is to have a look at the robots.txt (Robots.txt is a text file webmasters create to instruct web robots (typically search engine robots) how to crawl pages on their website).

Graphical user interface, text, application

Description automatically generated

robots.txt Contains Rick’s catchphrase “**Wubbalubbadubdub**”.

Now let’s have a look at the Source Code for the page, see if there is anything worth our time.

A screenshot of a computer

Description automatically generated with medium confidence

The Source Code has a Username

Found a username (**R1ckRul3s**) in the Source Code.

Now that we found a username we can start looking for a login page, and that starts with some **enumeration** on the website.

First choice is to run Nmap on the IP.

Text

Description automatically generated

Running Nmap on the IP address

Running Nikto (Web Server Scanner) on the VM

Text

Description automatically generated

Nikto Scan

Nikto was a lot faster than Nmap (but louder).

We found that the VM is running Apache/2.4.18 (9 CVEs, it doesn’t look good).

Nikto also found a login page, exactly what we were looking for (/login.php).

Graphical user interface, application

Description automatically generated

Pickle Rick Login Page

Now it would be a good idea to use GoBuster or DirBuster to bruteforce any directories to find any files available on the web site. I will be using GoBuster with 2.3-medium.txt wordlist.

Text

Description automatically generated

GoBuster

GoBuster found 2 directories (assets & server-status).

Graphical user interface, text, email

Description automatically generated

403 Forbidden for server-status

Graphical user interface, text, application, email

Description automatically generated

Access to assets

Well, server-status requires perms but assets does not. Well, I’m going to try to go back to GoBuster and run it again with different file extensions and see if anything will come up (-x php,html,htm).

Text

Description automatically generated

Found a few more directories

Now I am a bit lost with this CTF so I am gonna try to see if I can do anything with the login.php page. Afterall, we found a username that might be working.

And the Username alongside the text from robots.txt seem to be working and we’re in. Now the fun begins.

Graphical user interface, text, application, email

Description automatically generated

portal.php

There is a command Panel, let’s see what works inside here. ls maybe?

Graphical user interface, text, application, email

Description automatically generated

Command Panel

Graphical user interface, text, application, chat or text message

Description automatically generated

ls Worked

So ls worked on the Command Panel and now we have a new text file (**Sup3rS3cretPickl3Ingred.txt**). Now I’m wondering if cat would work to see the file.

Graphical user interface, text, application

Description automatically generated

Sad, cat does not work.

A screenshot of a computer

Description automatically generated with medium confidence

Source Code

Though the Source Code might contain something useful, This is not Base64 Encoding.

Now let’s use different commands until we can get the first ingredient.

Graphical user interface, text, application

Description automatically generated

tac for the win



First Ingredient done

And we got the First Ingredient (Part 1/3 of this CTF).

Going back to the Command Panel we can have a look around the /home directory for anything interesting.

Graphical user interface, text, application, chat or text message

Description automatically generated

ls ../../../home

Graphical user interface, text, application, chat or text message

Description automatically generated

ls ../../../home/rick

And it seems that we found the second ingredient! Going to use tac again to get it just like the first one.

Graphical user interface, text, application, chat or text message

Description automatically generated

tac for the win#2

Now let’s have a look at the root directory and see if we have any access.

Graphical user interface, text, application, chat or text message

Description automatically generated

sudo ls ../../../root works

Graphical user interface, text, application, chat or text message

Description automatically generated

3rd Ingredient Secured

Well this was easy. And with that we have completed this CTF.



3/3 in Terms of Ingredients

Graphical user interface, application

Description automatically generated

100%!

Thank you for reading my Pickle Rick Room Write-Up and if you want to try the room yourself the link is below. I have also attached my LinkTree if you want to get in contact with me. And thank you [tryhackme](https://tryhackme.com/p/tryhackme) for this room.

Pickle Rick Room Link: <https://tryhackme.com/room/picklerick>

My LinkTree — <https://linktr.ee/StefanPBargan>