**Write-up Pickle Rick CTF (Try Hack Me)**

I have to find three ingredients (flags) for a potion to help Rick transform himself back into a human from a pickle.

Enumeration

The first step is to open the web application in the browser. The website does not seem to have any clickable pages.

Let’s look in the source code to find additional clues. In the body there is a comment that the username is R1ckRul3s.

Looking at the robots.txt page, it says Wubbalubbadubdub. This might be a password, but we don’t know yet.

The next step is to perform a directory scan with Gobuster. At the same time, we will be searching for any interesting file extensions such as .conf, .config, .html, .php., .txt. This returns some interesting things, most notably: login.php, portal.php and clue.txt.

Looking further into the login.php page, it is obviously a login page. Looking at the source code I don’t find any obvious interesting information for this page. The portal.php page seems to redirect to login.php. Lastly, the clue.txt page gives me the hint to ‘Look around the file system for the other ingredient.’. The source code for this page shows no additional information.

Web log-in

We have a username and a text string that could possibly be a password. Trying this combination on the login page indeed works. We are now at the actual portal.php page.

Continued enumeration

Looking at the source code for this page, we can find a commented text string that may be some kind of hash: Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkliRmhoTVhCb1ZsWmFWMVpWTVVWaGVqQT0==. However, Crackstation does not recognize the text string as a hash. For now, let’s keep it in mind.

Clicking on the other links in the navigation bar, all return to denied.php telling me that only the real Rick has access. The source code holds no interesting information.

Command panel

On the Commands tab of the portal.php page a command panel can be found. Let’s try listing the directory with ls. The command seems to work as it lists similar results as the Gobuster directory scan, along with an additional file called Sup3rS3cretPickl3Ingred.txt. This may be our first ingredient! Browsing to this page returns mr. meeseek hair. This fits the answer format for the first ingredient and entering it confirms it is a correct answer.

Let’s see what users exist using the command cd /home; ls. This returns ubuntu and rick. Let’s look at the directory of rick using the command cd /home/rick; ls. This returns a file named second ingredients! Let’s open this file with cat second ingredients. We get a message that this command is disabled. To work around this, let’s create a reverse shell.

Shell

To do create a reverse shell, I first create a payload using the command msfvenom cmd/unix/reverse\_netcat. Then I start a Netcat listener. Then I enter the resulting payload from msfvenom in the command panel. I can now see on the local machine that I made a connection! Now I try to open the file with the command cat /home/rick/”second ingredients”, which says: 1 jerry tear. The third ingredient will probably be located in the root. At this moment I am not the root user, since the whoami command returns www-data. So I need to do privacy escalation.

Privacy escalation

Let’s see what commands I’m able to use as super user with the command sudo -l. This returns that I can run anything without password. So let’s run the command sudo vi and type :!sh. Now I have opened a shell to the root user. Let’s now have a look at /root. This directory contains snap and 3rd.txt. The latter is what we need, so let’s open it with the command cat 3rd.txt, which reveals the final ingredient: fleeb juice.