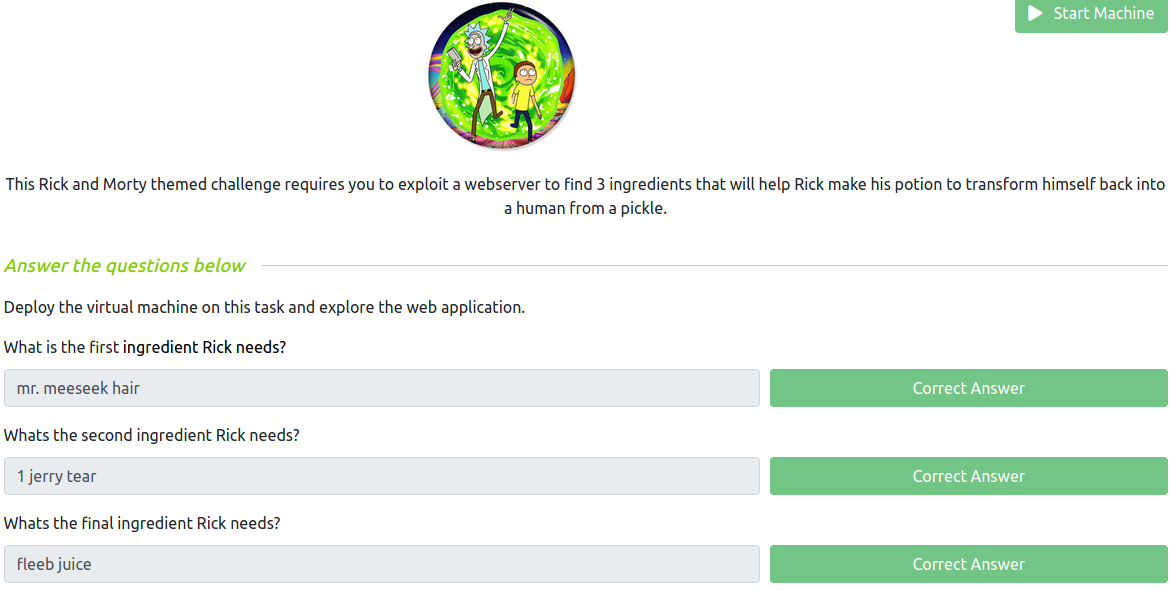
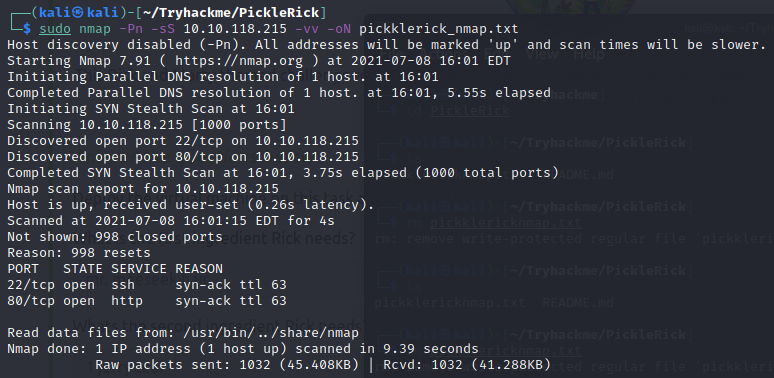
**Pickle Rick write-up**

This is a write-up Pickle Rick which is a web server exploit CTF to get all 3 flags/ingredients that hide in file system of server machine

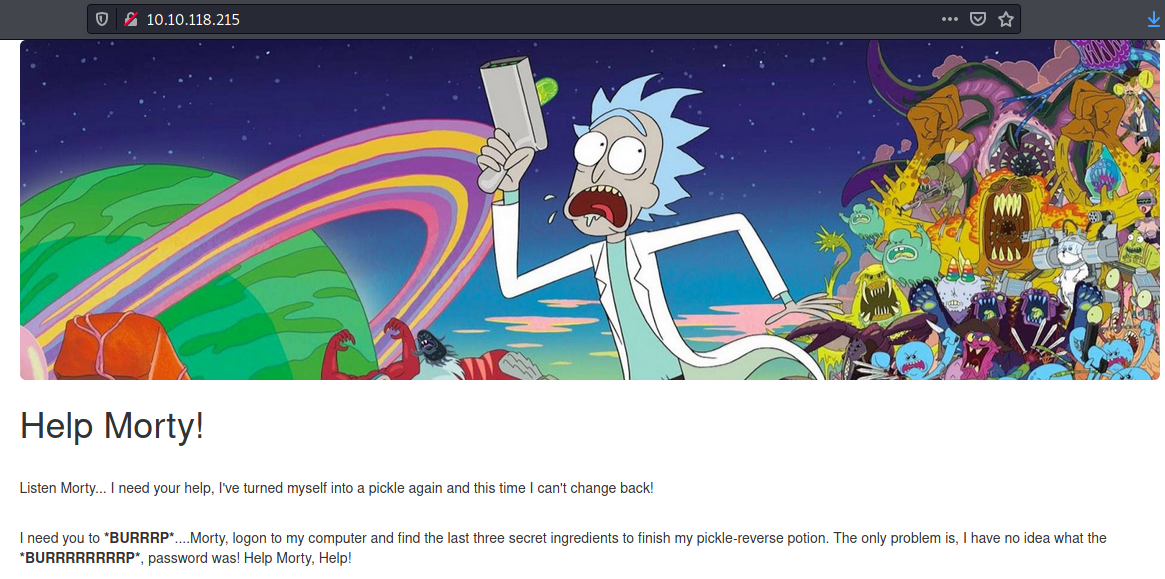
Site: <https://tryhackme.com/room/picklerick>



Start with nmap scan, I do recommend –sC –sV but it won’t get much more useful information from this



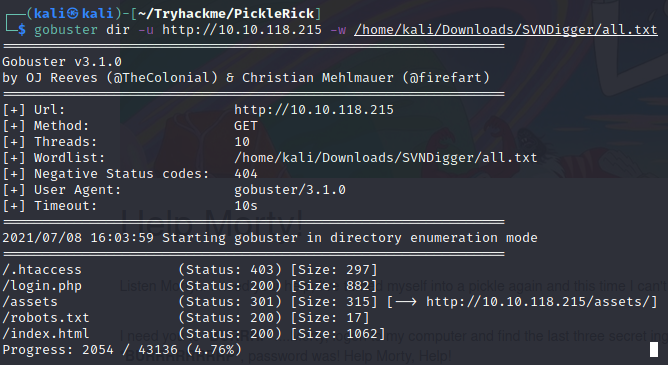
We found http port open so get into this website



At this point we will do directory bruteforce right away after found it it’s dead-end but let’s just view-source code first and jackpot! A username



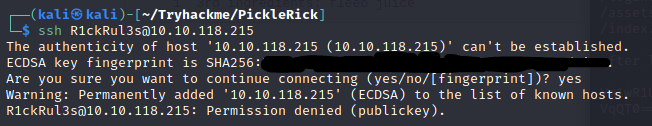
Bruteforce directory with gobuster since it’s faster than dirb and we found robots.txt which tell crawler what they will behaved and even login.php



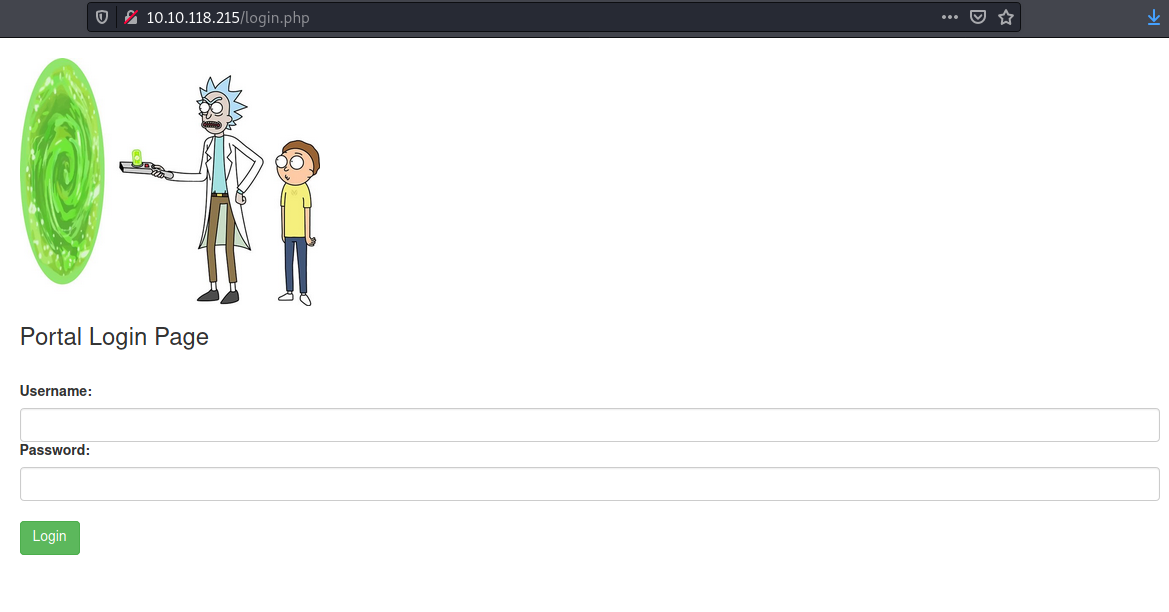
It seems like we got a potentially password here



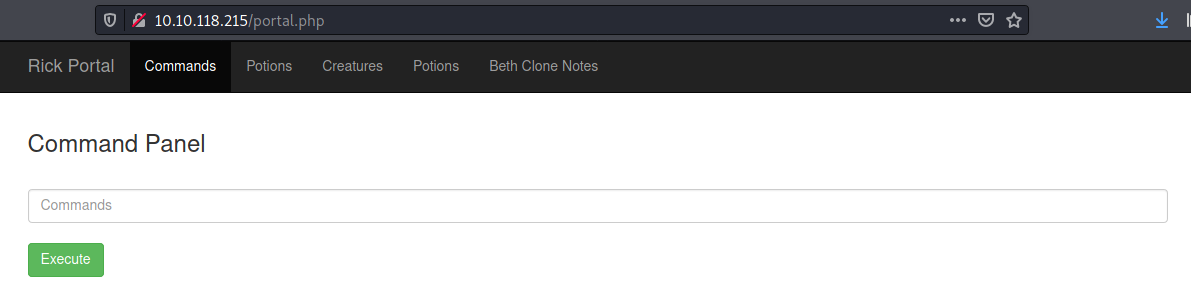
Tried to connect via SSH but it’s not the real password for SSH, too bad



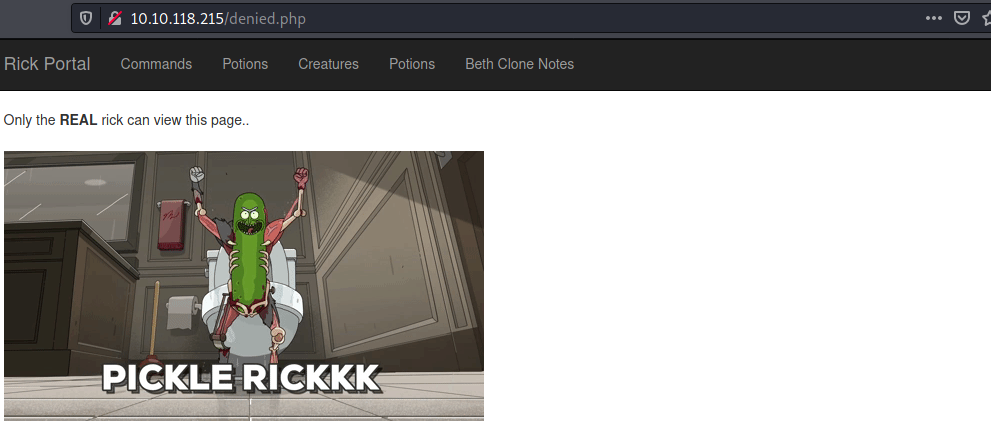
But at least we have login.php page so let’s login here



After come in we found a command panel which suspect to be a shell command



Which if we go to other page we will be redirected to denied.php

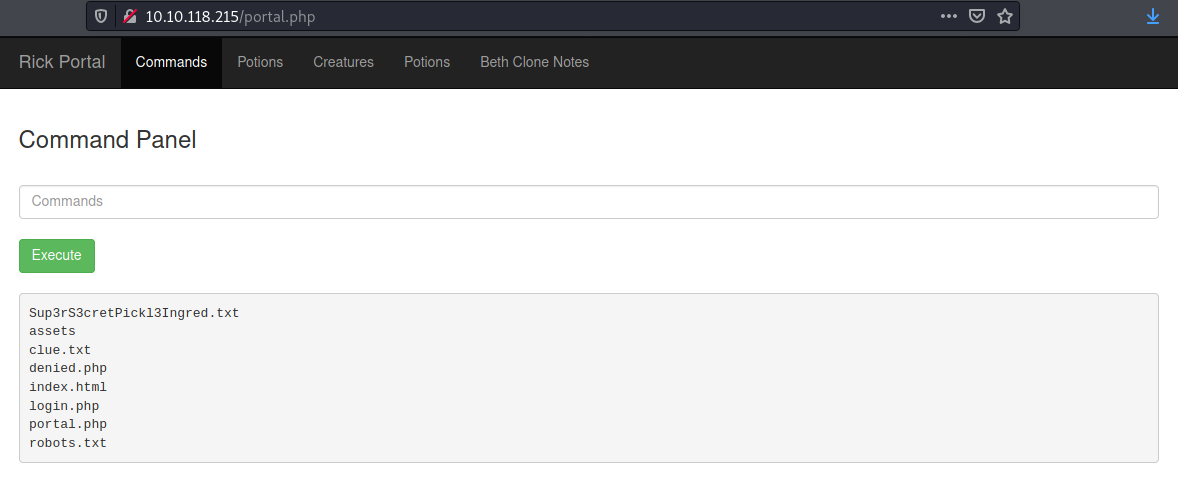


Tried to view source code and this comment stand out which could be a base64 judging from = at the end

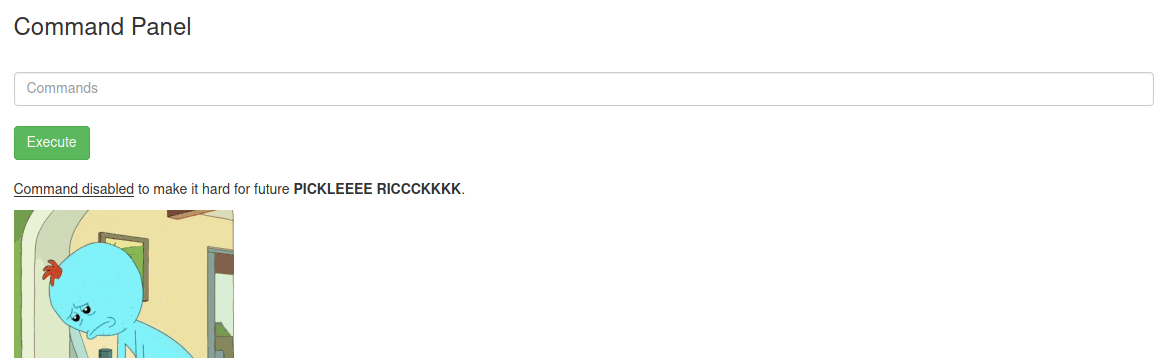


And it’s a trap when I decoded it many times it came out with **rabbit hole** which is not an ingredient

Tried basic command ls to list all files in current directory and bang! First ingredient and a clue!



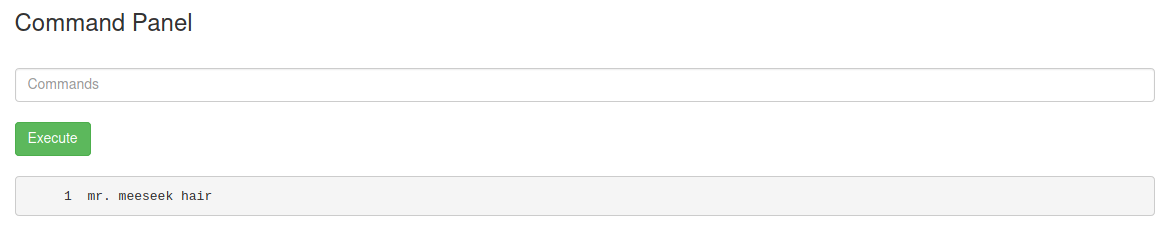
Read **clue.txt** first but.. We got a command blacklist!



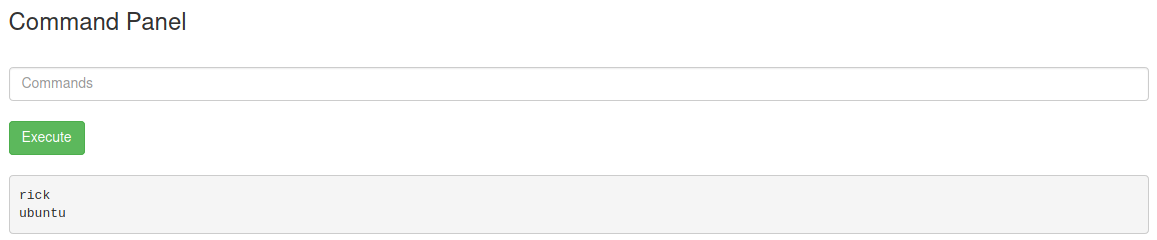
But Linux has many command to read the files and I’ve found **nl** that can pass the blacklist ( or we can use **grep . clue.txt**)



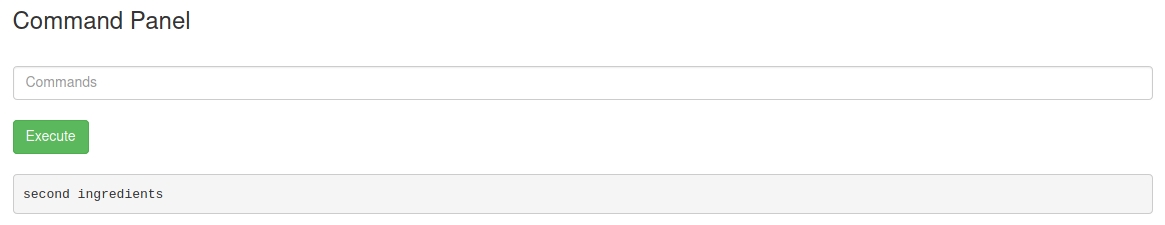
Capture the first flag!



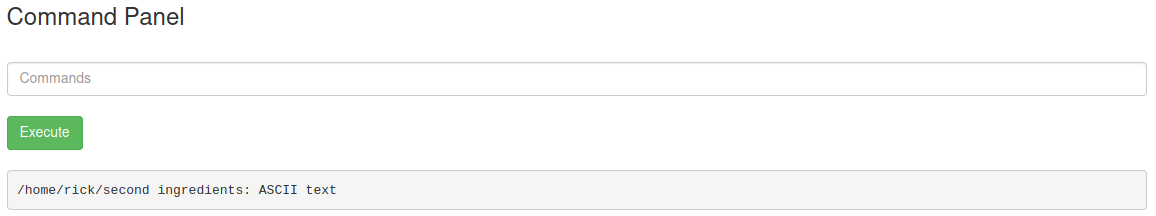
Time for second flag which could be in user directory, let’s list everything not included hidden files in home directory which we will found 2 users directory and rick should be our target here



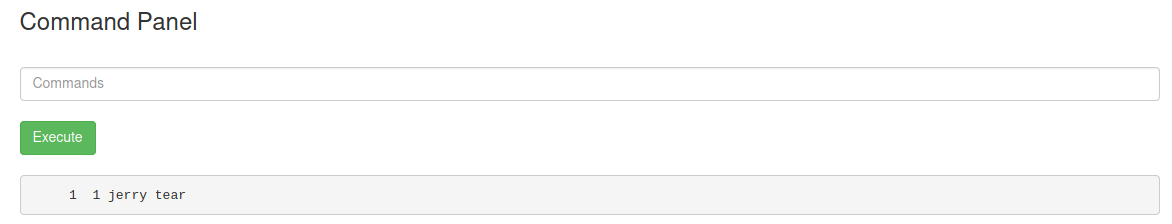
List everything in rick directory and we found our second flag



Just make sure with **file /home/rick/second” “ingredients**



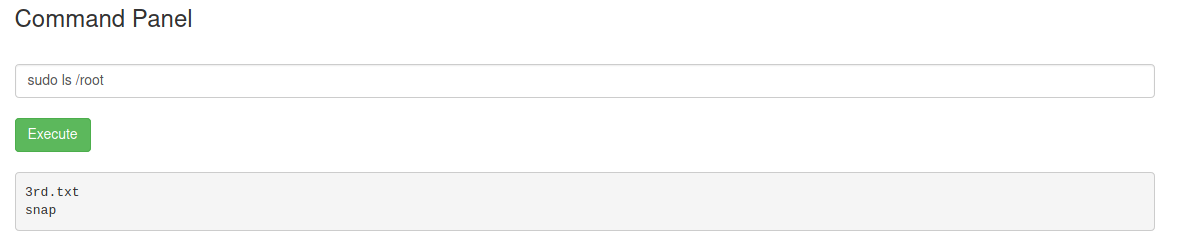
And capture our second flag!



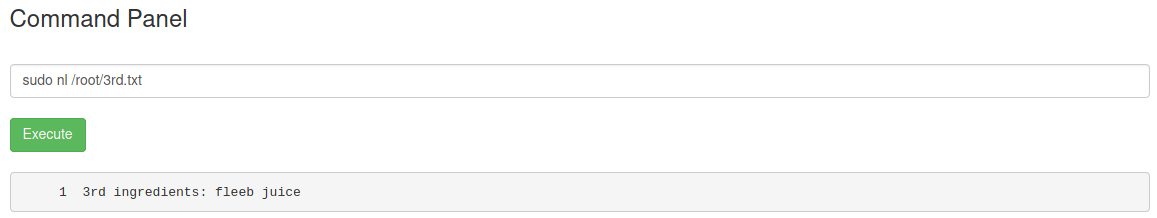
And the last flag maybe hidden in root directory so let’s find a way to elevate our privilege, with easiest one first just like sudo and jackpot! We can use sudo for no password for everything



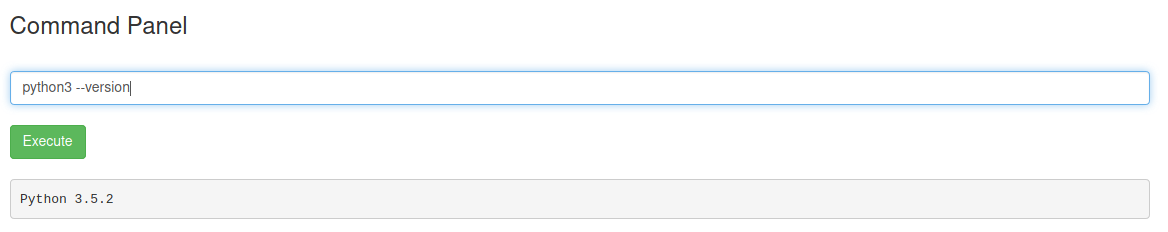
List everything in root directory so we can see our last flag there



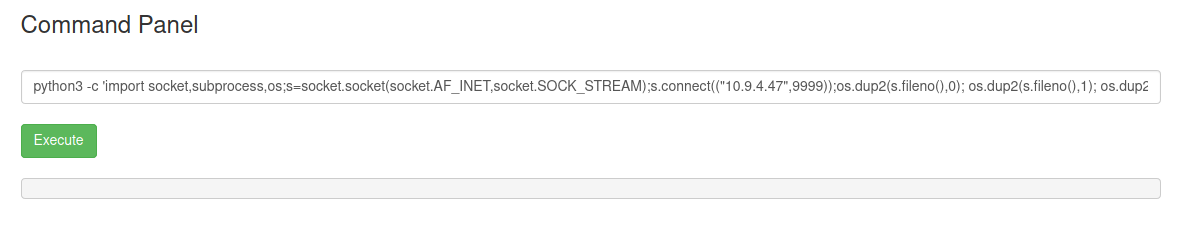
Capture our last flag! And we’re done!



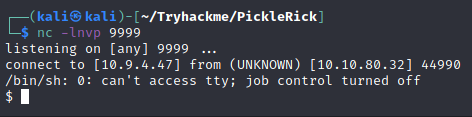
Another way to rock this box is to get a reverse shell cause we have python 3 in this box



Copy reverse shell code from reverse shell cheatsheet, set netcat listener and execute it



Easy shell



Now you know the drill

