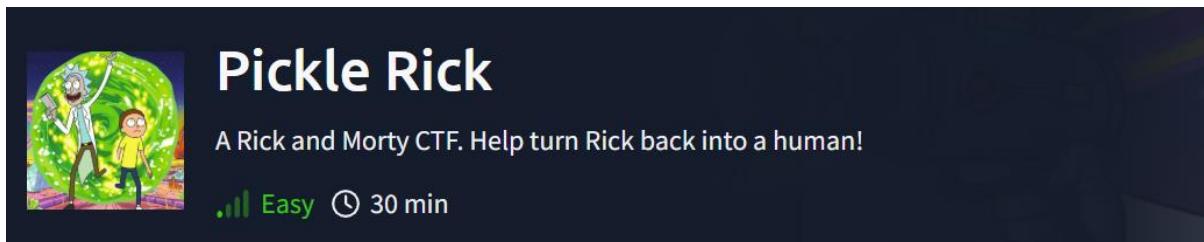


# OWASP- KERALA CYBER-SECURITY BOOTCAMP TASK1

BY: YASHAS R NAIR

ROOM SLOVED: [PICKEL RICK \(FROM TRYHACKME\)](#)

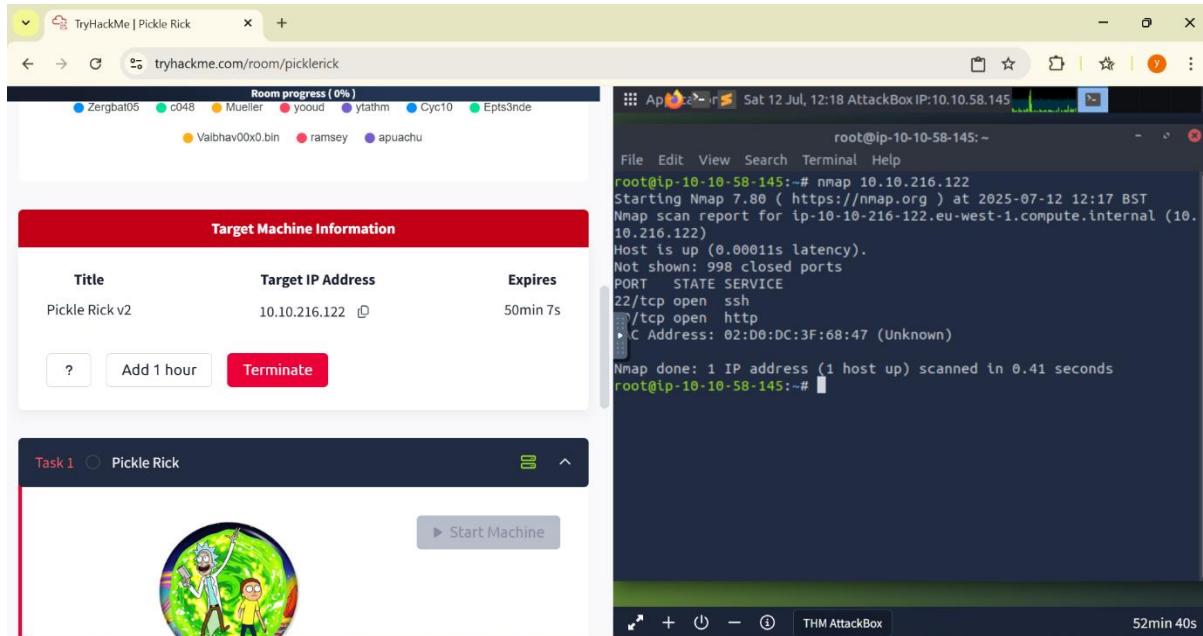


OBJECTIVE: TO FIND THE MAIN 3 INGRIDIENTS TO TURN RICK BACK INTO HUMAN FORM

STEP 1: START THE TRAGET MACHINE AND FIND THE IP ADDRESS (10.10.216.122)

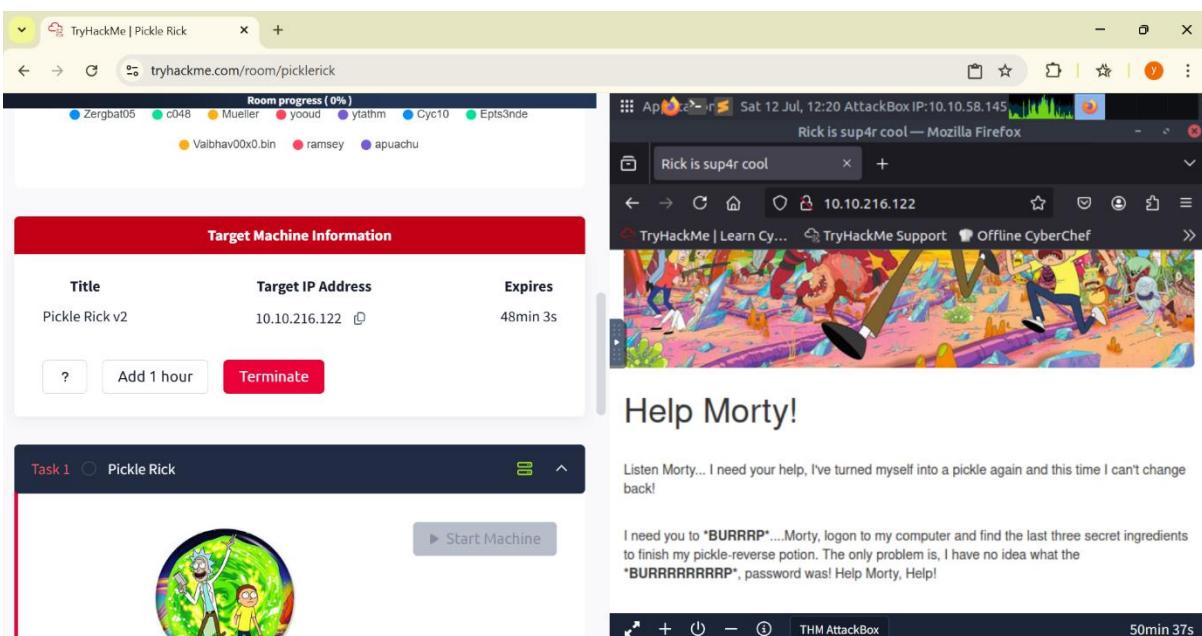
A screenshot of the TryHackMe task interface for 'Pickle Rick'. At the top, there's a header bar with the title 'TryHackMe | Pickle Rick' and a progress bar showing 'Room progress ( 0% )'. Below the header is a red bar titled 'Target Machine Information'. It contains a table with three columns: 'Title' (Pickle Rick v2), 'Target IP Address' (10.10.216.122), and 'Expires' (58min 9s). There are also buttons for '?', 'Add 1 hour', and 'Terminate'. Below this is a main content area. On the left, there's a sidebar with 'Task 1' and 'Pickle Rick'. In the center, there's a circular thumbnail image of Rick and Morty. On the right, there's a button labeled '▶ Start Machine'. At the bottom of the main content area, there's a descriptive text: 'This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.' and 'Deploy the virtual machine on this task and explore the web application: 10.10.216.122'.

## STEP 2: STARTED THE ATTACK BOX(PROVIDED BY TRY HACKME) AND RAN AN NMAP SCAN ON THE TRAGET IP

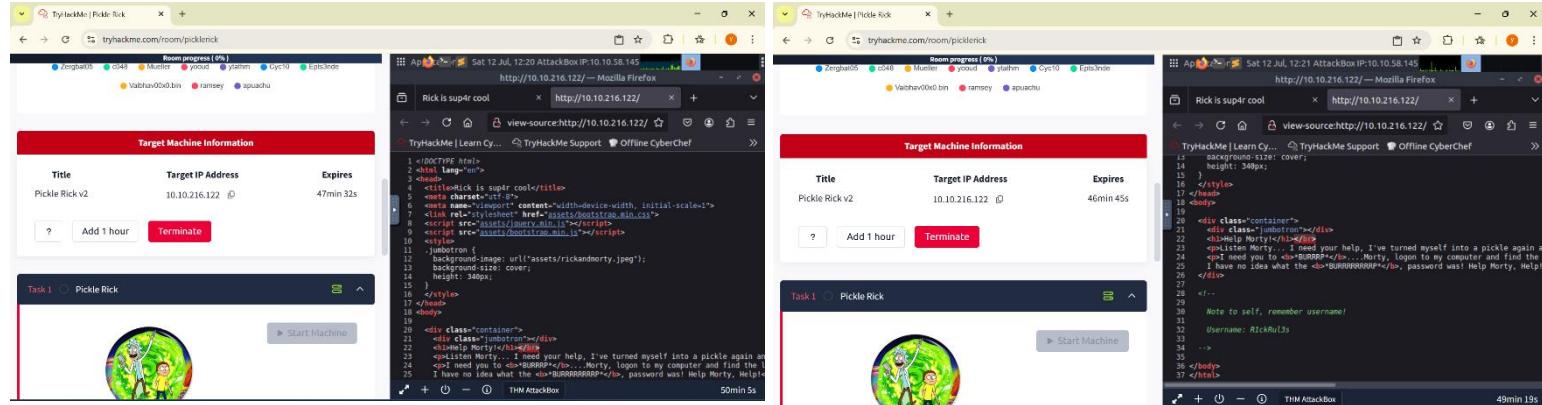


AFTER THE SCAN WE FOUND THAT 2 PORTS (SSH, HTTP) ARE OPEN SINCE WE DON'T HAVE THE USERNAME OR THE PASSWORD TO LOGIN SSH WE WILL GO TO THE SITE

## STEP 3: THE HTTP SITE FRONT DID NOT GAVE US ANYTHING SPECIAL SO LET INSPECT THE SITE

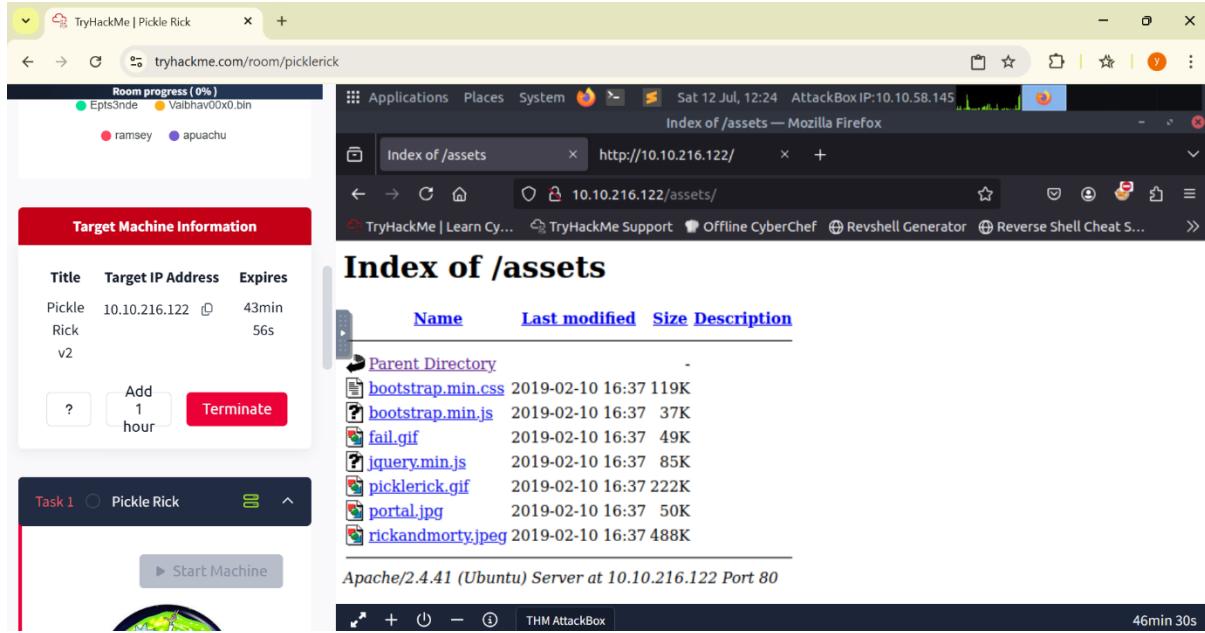


## **STEP 4: ON INSPECT THE SITE**



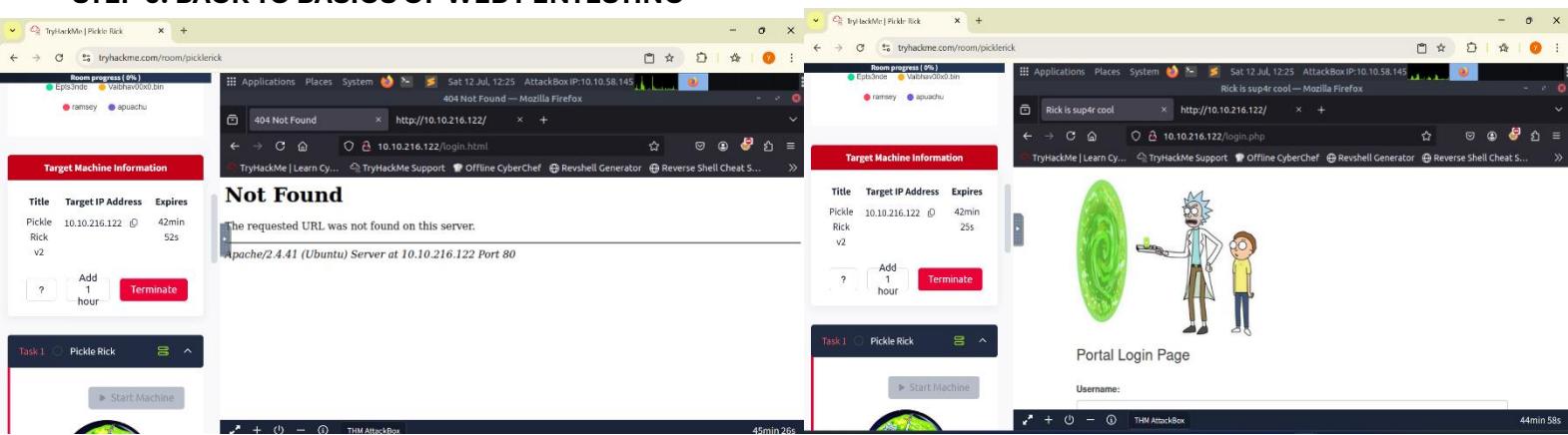
**WE COULD FIND THE USER NAME IN THE COMMENTS AND ALSO, I FOUND THAT THERE IS AN ASSETS FOLDER**

## **STEP 5: EXPLOR THE ASSETS FOLDER**



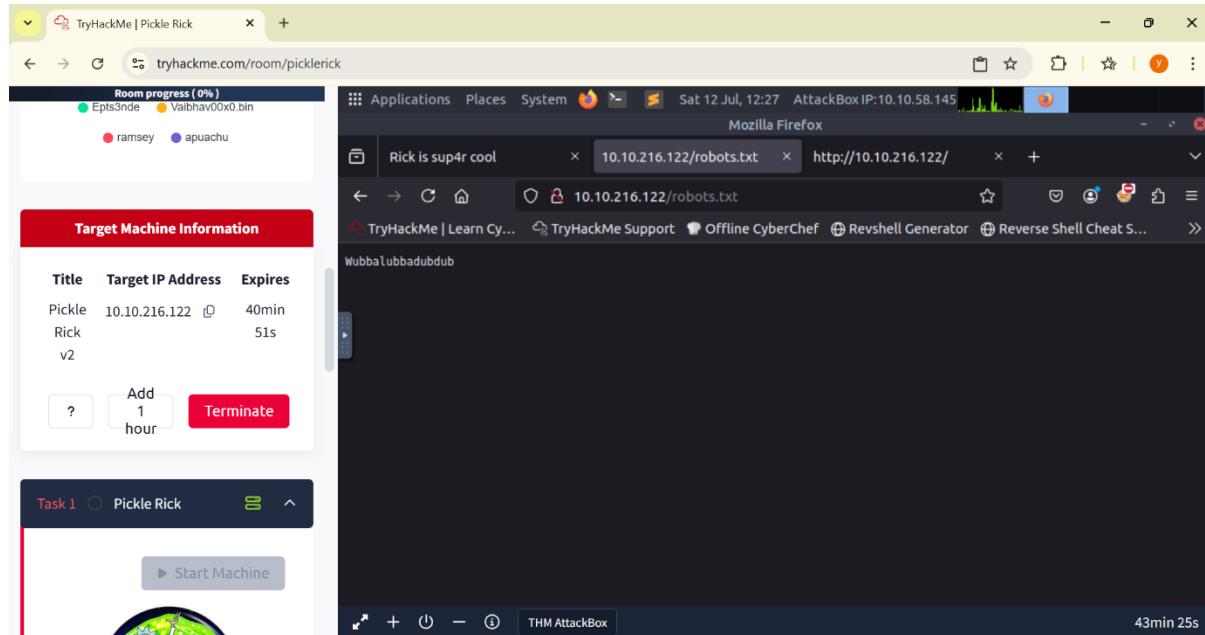
ON CHECKING THE ASSETS FOLDER WE COULD ONLY SEE SOME CSS , JS , GIF(OR JIF) AND IMAGES AND NOT ANY PARTICULAR FILES OR CONTENTS, BUT BEING AN WEB DEV ONE FILE CAUGHT MY ATTENTION THAT IS THE “JQUERY.MIN.JS” FILE THAT MADE ME THINK THAT THIS SITE COULD ME MADE WITH PHP OR PURE HTML

## STEP 6: BACK TO BASICS OF WEB PENTESTING



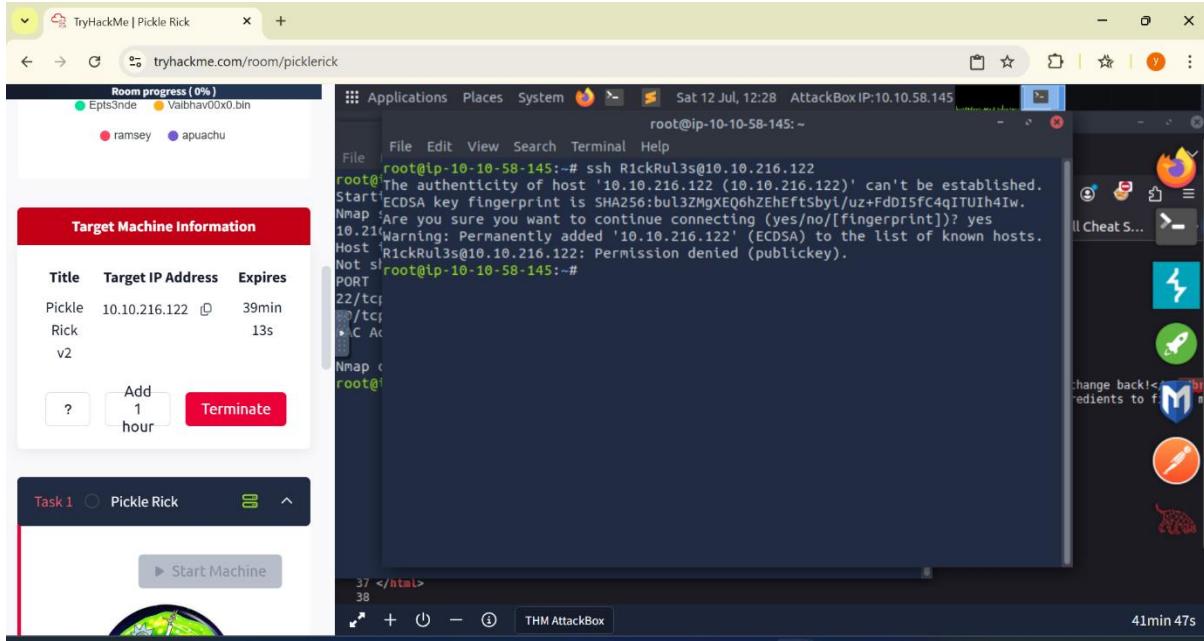
THE BEST STEP WAS THIS CAUSE THIS PROVED MY BELIEF OF BEING AN PHP SITE SINCE “/LOGIN.HTML DID NOT WORK AND /LOGIN.PHP WORKED” NOW WE KNOW THAT ITS AN PHP SITE WE CAN CHECK FOR “ROBOTS.TXT” CAUSE PHP NEEDS THIS FILE TO HOST

## STEP 7: CHECK FOR ROBOTS



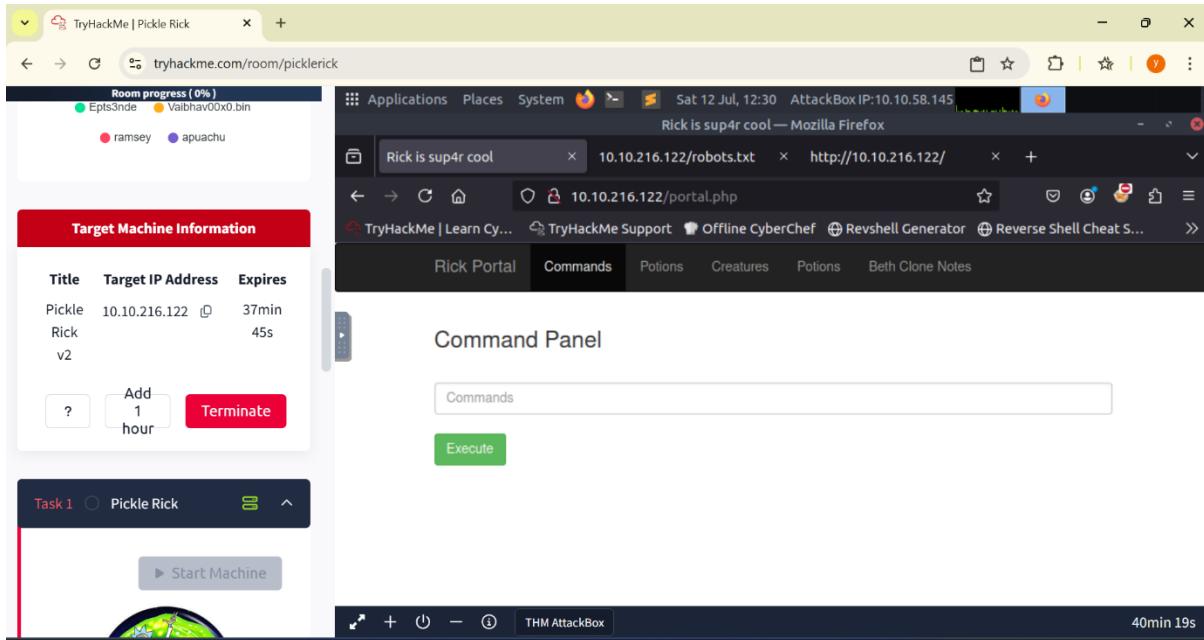
JUST LIKE THAT I THINK WE FOUND THE PASSWORD NOW LETS SSH INTO THE MACHINE

## STEP 8: SSH INTO TRAGET MACHINE



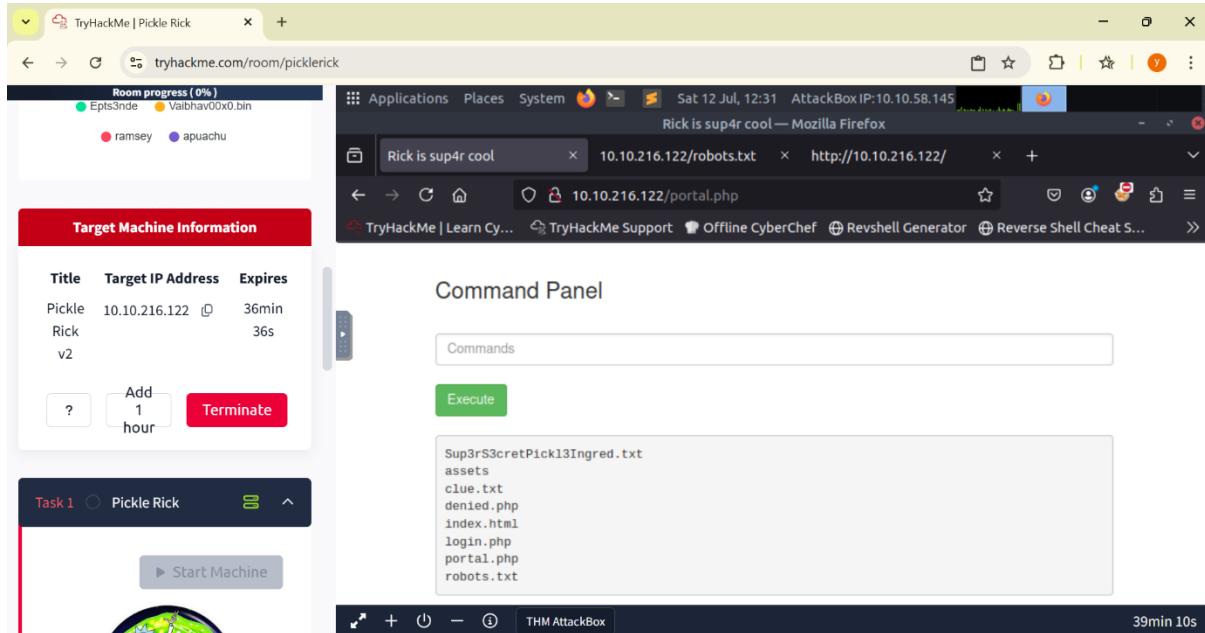
SINCE SSH DOES NOT ALLOW THE USER RickRul3s I THINK WE CAN TRY IT ON THE /LGOIN.PHP PAGE

## STEP 9: TRYING TO LOGIN IN ON THE PHP PAGE



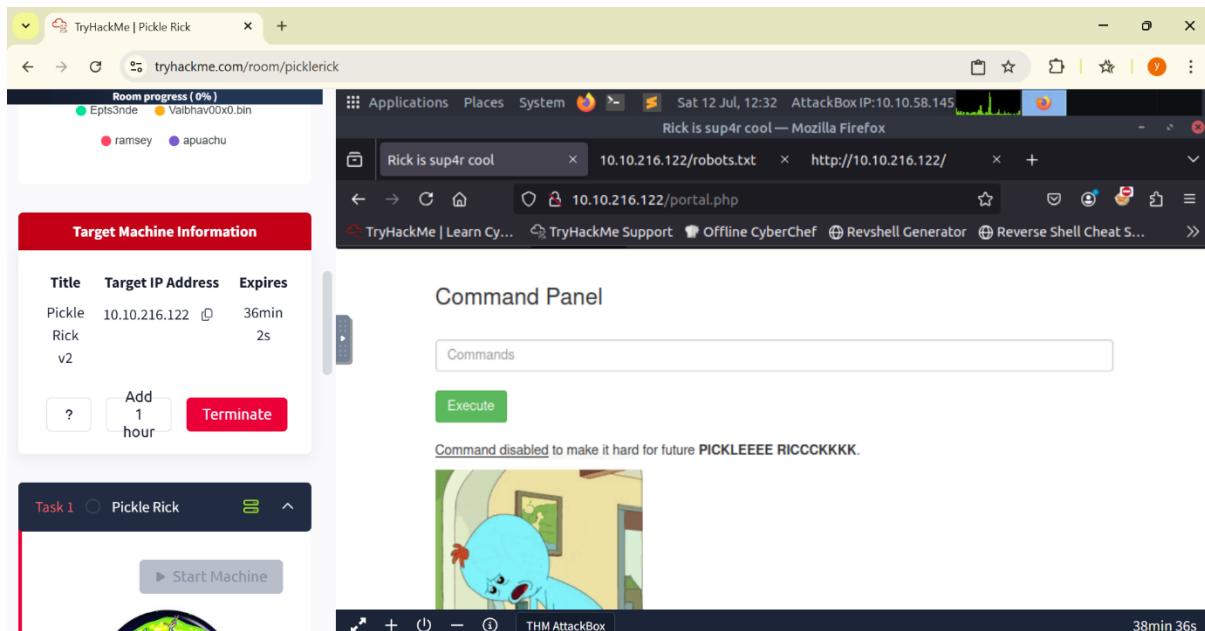
AND WE ARE IN THIS COMMAND PANEL IS JUST LIKE AN TERMINAL SO LETS TRY EXECUTING COMMANDS

## STEP 10: LS COMMAND



THE LS COMMAND SHOWS US THE CONTENTS AND WE CAN SEE “Sup3rS3cretPICKL3Ingr3d.txt” LET’S CAT THE CONTENTS OF THE FILE

## STEP 11: CAT COMMAND



SINCE THE COMMAND IS DISABLED I THINK WE CAN USE THE LESS COMMAND TO READ THE FILE (MY MAN RICK IS AN SMART ASS)

## STEP 12: LESS COMMAND TO READ THE FILE

The screenshot shows the TryHackMe interface. On the left, there's a sidebar titled 'Target Machine Information' with a table showing a task named 'Pickle Rick' with an IP of 10.10.216.122 and an expiration of 34min. Below it is a 'Task 1' section with a 'Start Machine' button. The main area is a 'Command Panel' with a text input field containing 'mr. meeseek hair'. A green 'Execute' button is below the input field.

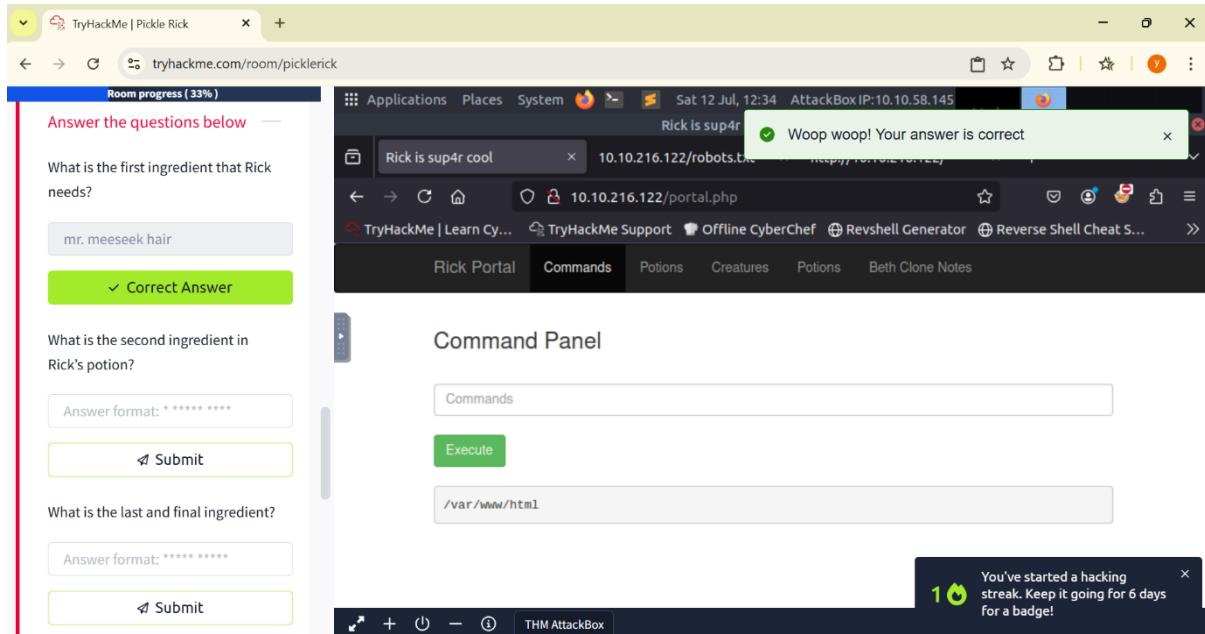
AND YES WE FOUND THE FIRST INGREDIENT LETS CHECK IT

## STEP 13 : CHECKING THE KEY

The screenshot shows the TryHackMe interface after executing the command. A message box says 'Woop woop! Your answer is correct'. At the bottom right, a badge indicates '10 You've started a hacking streak. Keep it going for 6 days for a badge!'. The sidebar on the left contains questions about Rick's potion ingredients and the machine configuration.

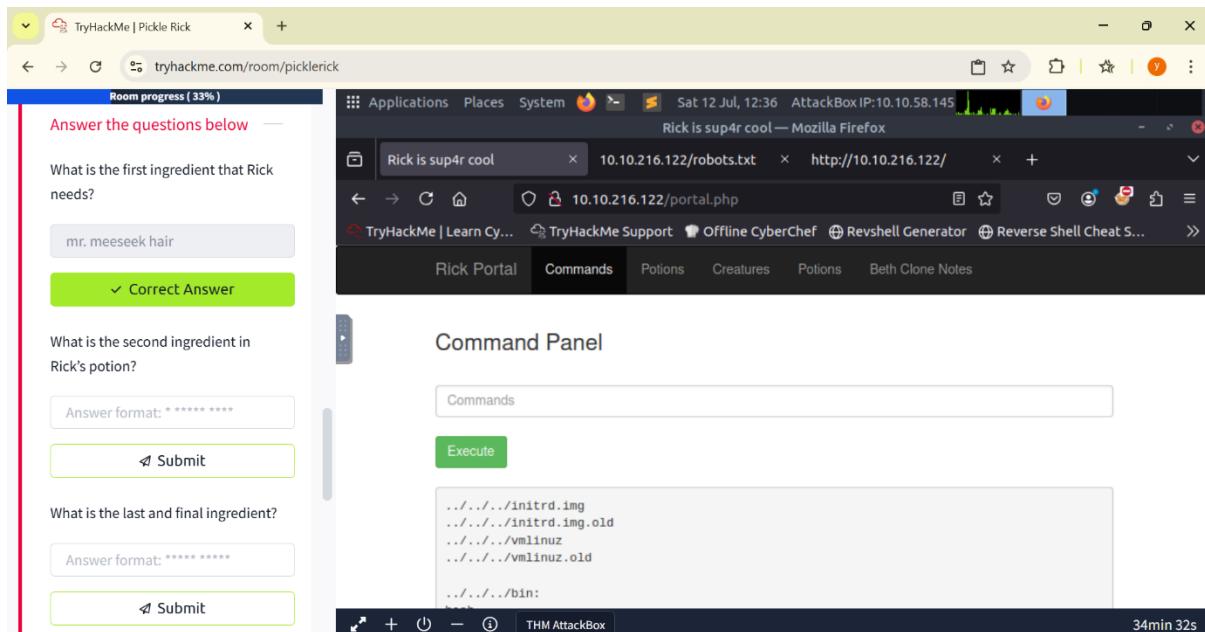
YES WE FOUND THE FIRST INGREDIENT, AS WE KNOW THAT THE SITE IS HOSTED WITH APACHE SERVER AND THAT WE COULD ONLY SEE THE SITE CONTENTS SO LETS CHECK THE WORKING DIRECTORY

## STEP 14: PWD COMMAND



YES JUST LIKE I KNEW IT WE WHERE IN THE SERVER DIRECTORY TIME TO CHECK ALL THE CONTENTS OF THE MACHINE USING THE GODMOD COMMAND

## STEP 15: THE SUDO LS ../../.../\* COMMAND



WE GOT ALL THE CONTENTS OF THE ENTIRE MACHINE NOW LETS CHECK FOR HOME DIRECTORY

## STEP 16: /HOME DIR

The screenshot shows a web browser window for 'tryhackme.com/room/picklerick'. On the left, there's a sidebar with 'Room progress (33%)' and several questions about Rick's potion ingredients. The main area has a terminal window showing the output of the 'ls' command:

```
vim  
vmware-tools  
vtrgb  
wgetrc  
xattr.conf  
xdg  
xml  
zsh_command_not_found  
..  
..../home:  
rick  
ubuntu  
..  
..../lib:  
apparmor  
console-setup  
cpp  
cryptsetup  
firmware
```

Below the terminal is a status bar showing '/home' and 'THM AttackBox'.

SO WE CAN SEE THAT THERE ARE TWO USERS IN THE MACHINE LETS LS THE CONTENTS IN THE RICK USER DIRECTORY BY USING THE COMMAND “SUDO LS ..../..../HOME/RICK”

## STEP 17: RICK

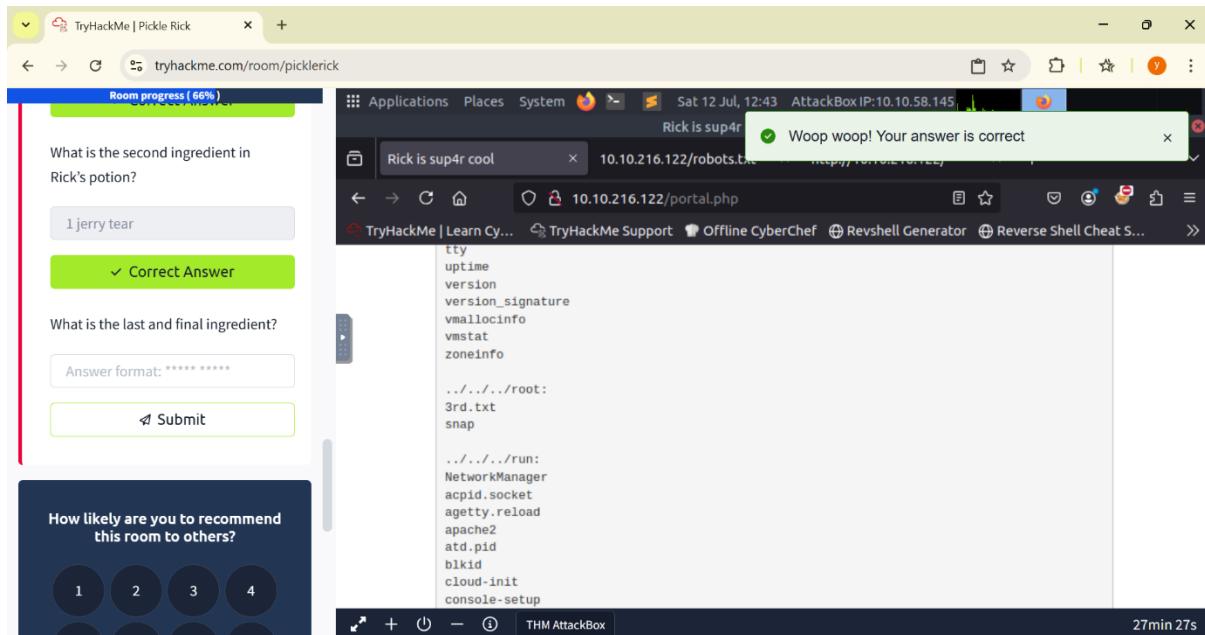
The screenshot shows a web browser window for 'tryhackme.com/room/picklerick'. On the left, there's a sidebar with 'Room progress (33%)' and several questions about Rick's potion ingredients. The main area has a terminal window showing the output of the 'ls' command in the '/home/rick' directory:

```
Rick Portal Commands Potions Creatures Potions Beth Clone Notes  
Command Panel  
Commands  
Execute  
second ingredients  
/home  
Highlight All Match Case Match Diacritics Whole Words 1c
```

Below the terminal is a status bar showing '/home' and 'THM AttackBox'.

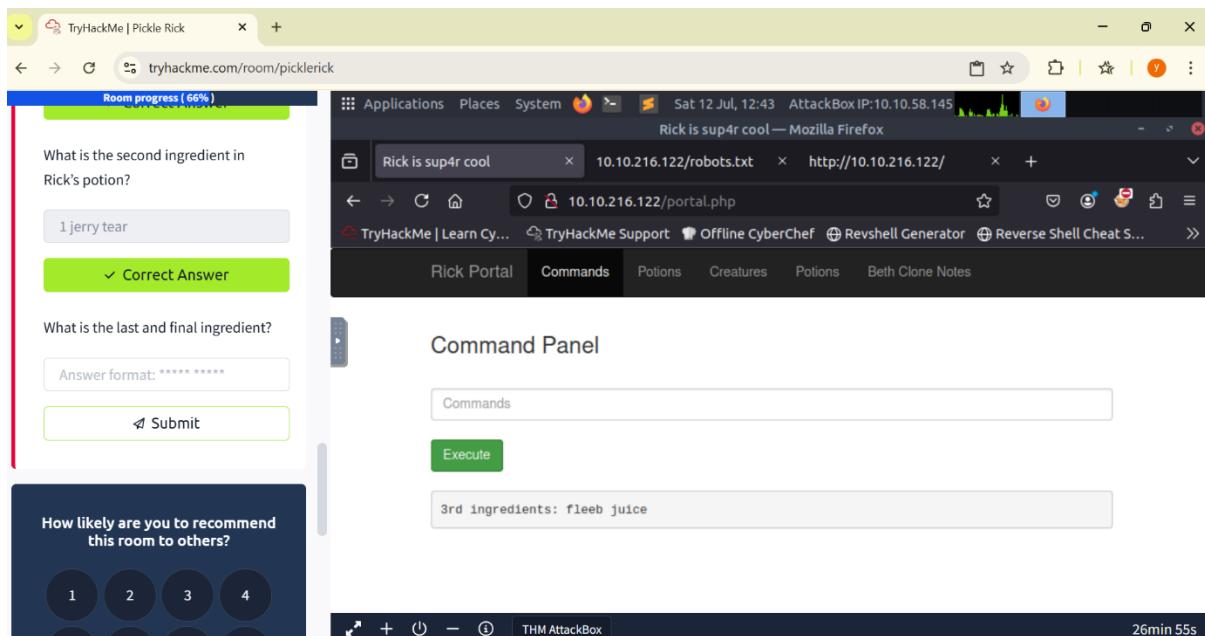
AND JUST LIKE THAT WE FOUND THE SECOND INGREDIENT LETS “LESS” IT OUT AND VERIFY THE KEY

## STEP 18: SEARCH FOR THE 3<sup>RD</sup> INGRIDENT



AGAIN EXECUTED THE GOD MODE COMMAND TO FIND THE 3<sup>RD</sup> INGRIDENT AND FOR LOOKING IT IN THE MESS I FOUND AND FILE CALLED 3RD.TXT LET'S TRY TO “LESS” IT OUT

## STEP 19: 3<sup>RD</sup>.TXT



AND JUST LIKE THAT WE FOUND THE 3<sup>RD</sup> INGRIDENT 🎉🎉🔥

## STEP 20: BRING PICKE RICK BACK TO HUMAN FORM

The screenshot shows a browser window for TryHackMe with the title "TryHackMe | Pickle Rick". The URL in the address bar is "tryhackme.com/room/picklerick". The main content features a circular icon with Rick and Morty characters, followed by the text "Congratulations on completing Pickle Rick!!! 🎉". Below this are five stats boxes: "Points earned 90", "Completed tasks 1", "Room type Challenge", "Difficulty Easy", and "Streak 1". A note at the bottom states "This room counted toward joining the league 🎯".

AND THERE WE CURED RICK



THAT'S IT FROM ME  
SINGING OFFF..

---YASHAS R NAIR