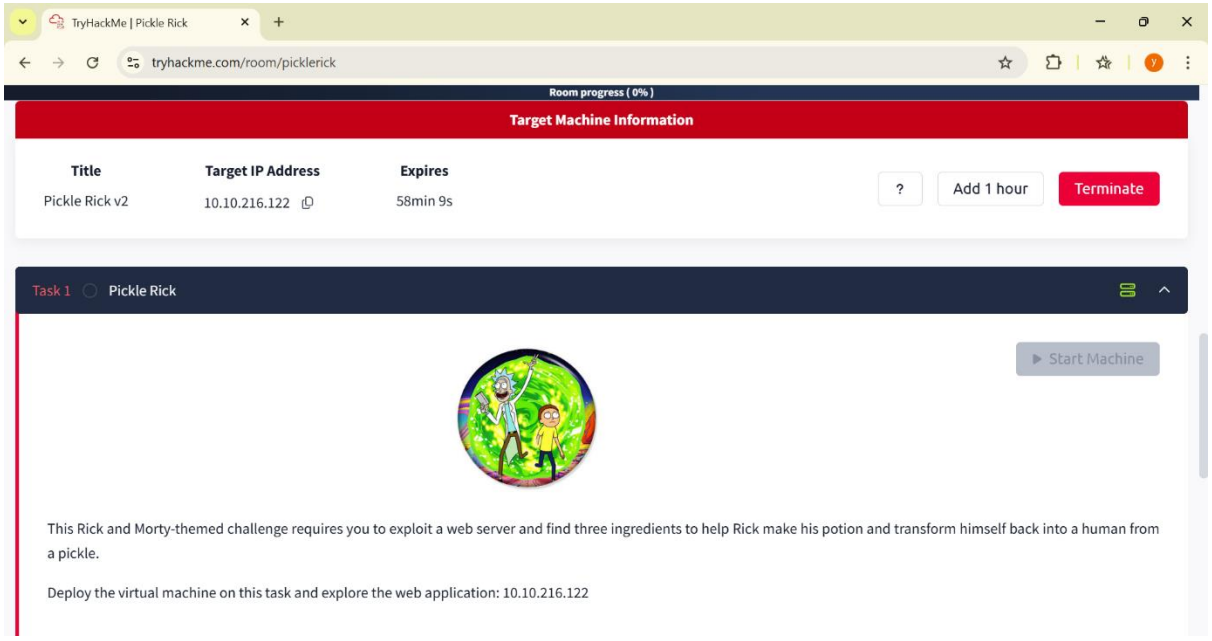
OWASP- KERALA CYBER-SECURITY BOOTCAMP TASK1

BY: YASHAS R NAIR

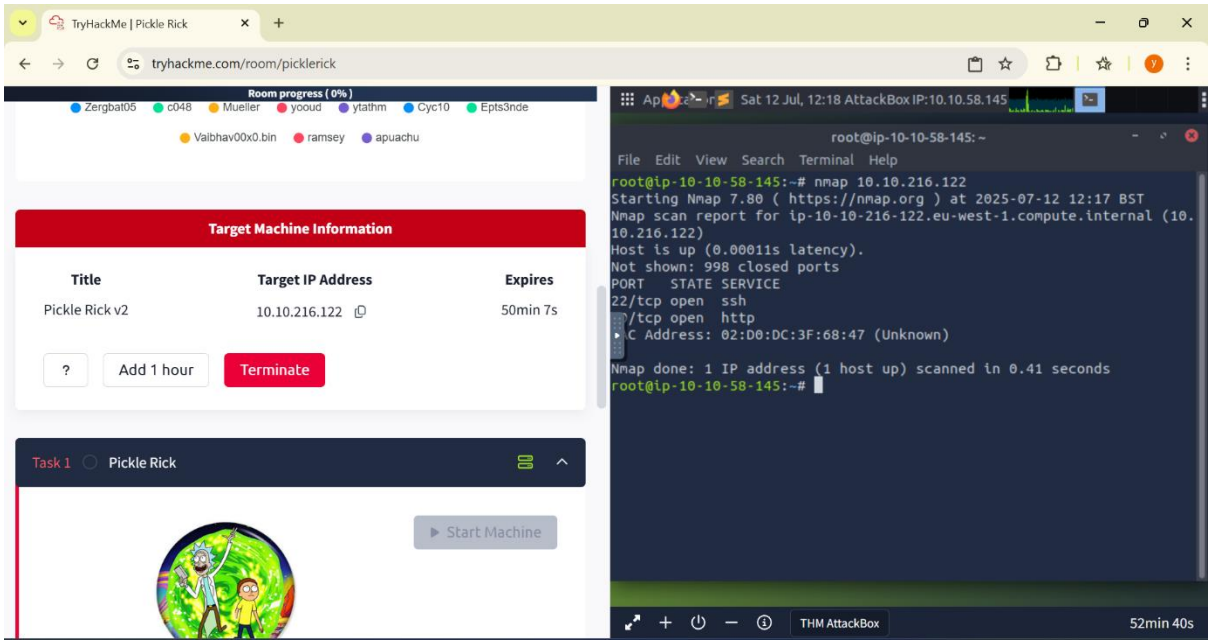
ROOM SLOVED: PICKEL RICK (FROM TRYHACKME)

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)

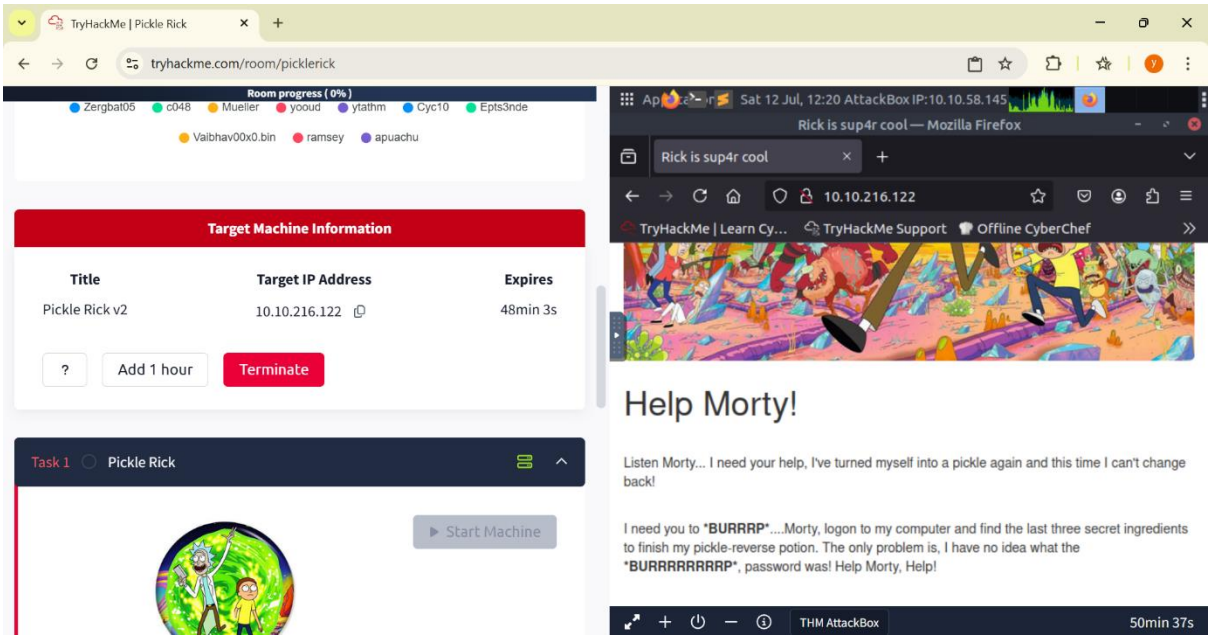


STEP 2: STARTED THE ATTACK BOX(PROVIDED BY TRY HACKME) AND RAN AN NMAP SCAN ON THE TRAGET IP

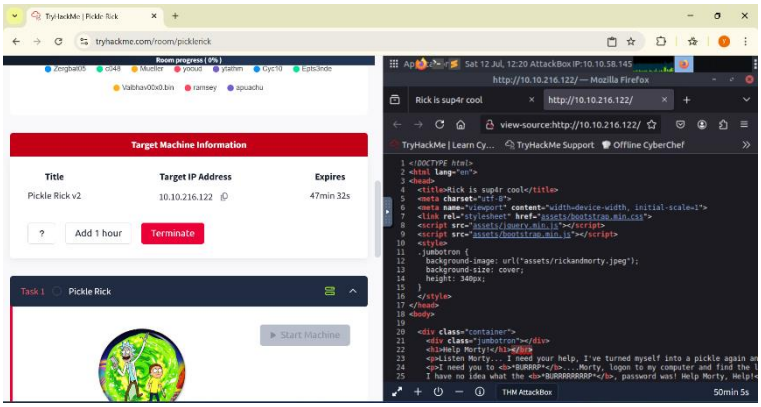


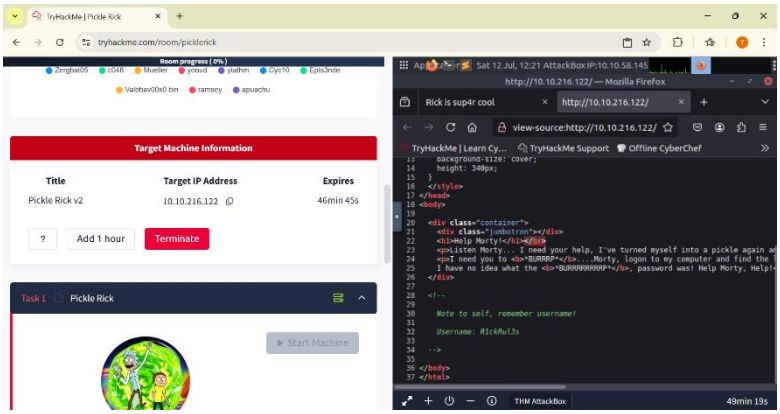
AFTER THE SCAN WE FOUND THAT 2 PORTS (SSH, HTTP) ARE OPEN SINCE WE DON'T HAVE THE USERNAME OR THE PASSWORD TO LOGIN SSH WE WILL GO TO THE SITE

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



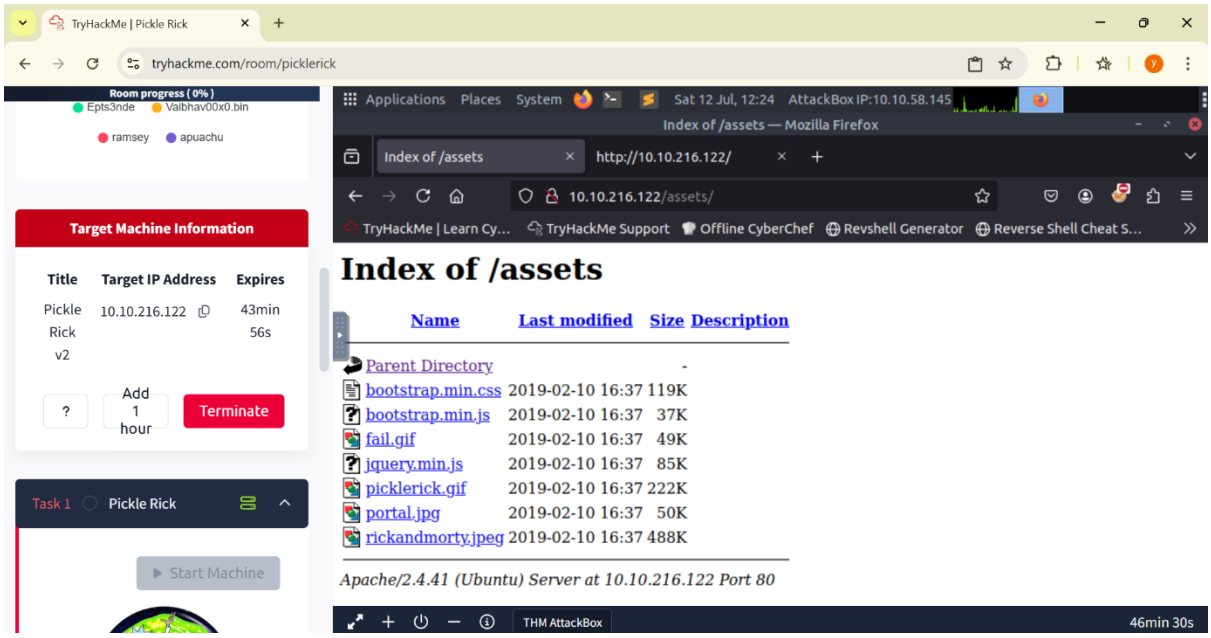
STEP 4: ON INSPECT THE SITE





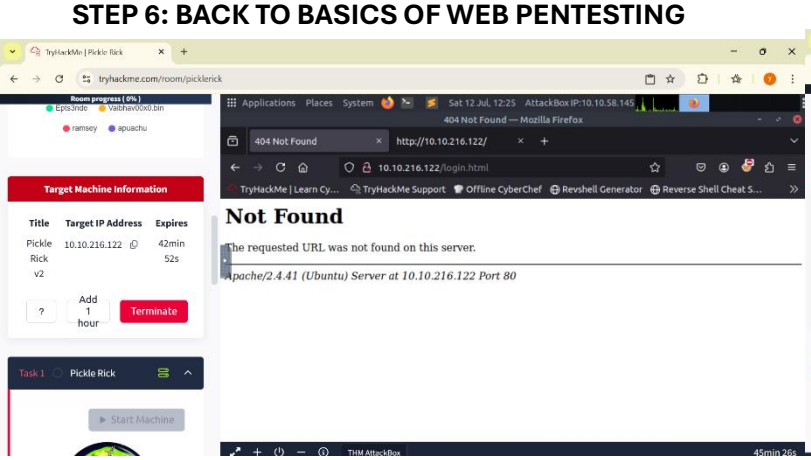
WE COULD FIND THE USER NAME IN THE COMMENTS AND ALSO, I FOUND THAT THERE IS AN ASSETS FOLDER

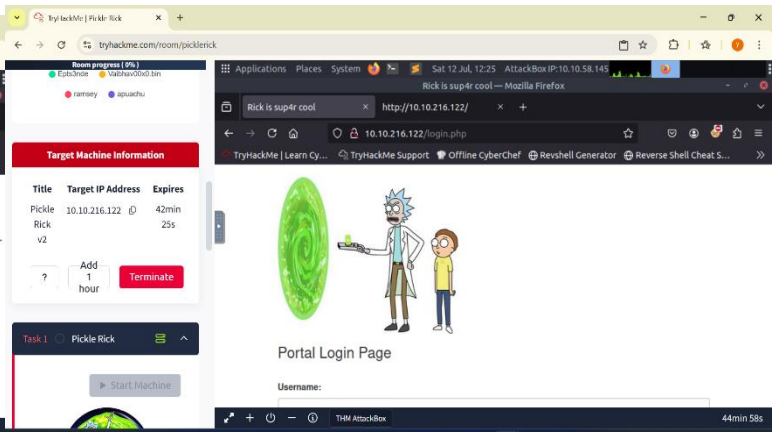
STEP 5: EXPLOR THE ASSETS FOLDER



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

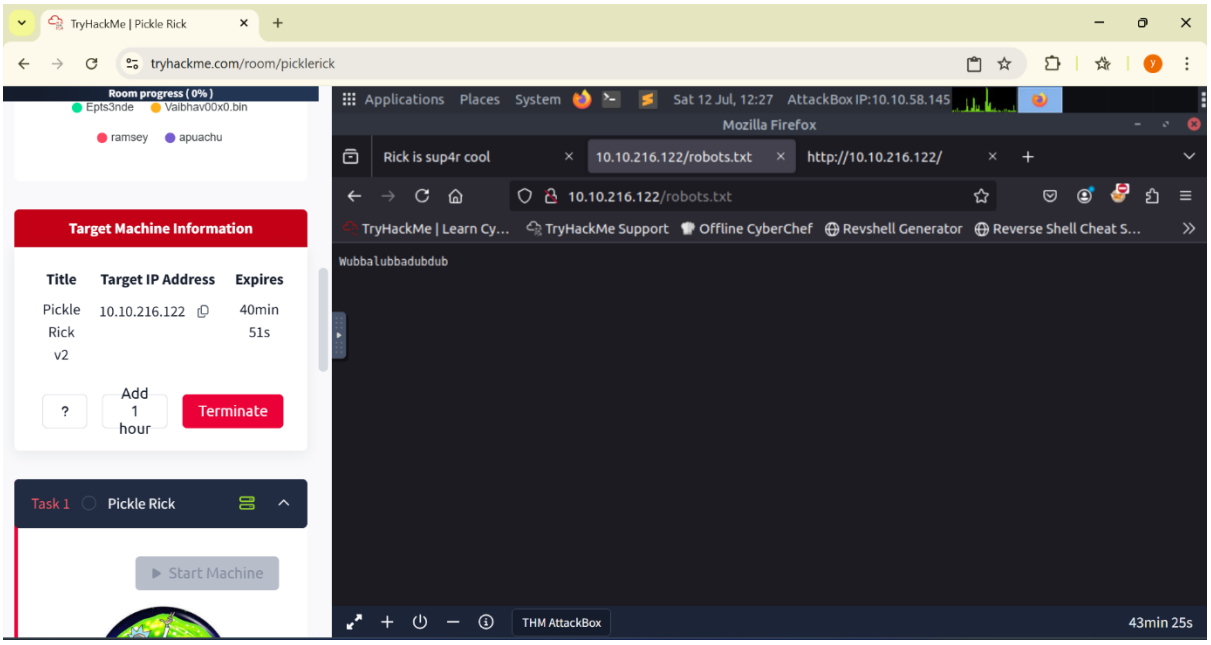
STEP 6: BACK TO BASICS OF WEB PENTESTING





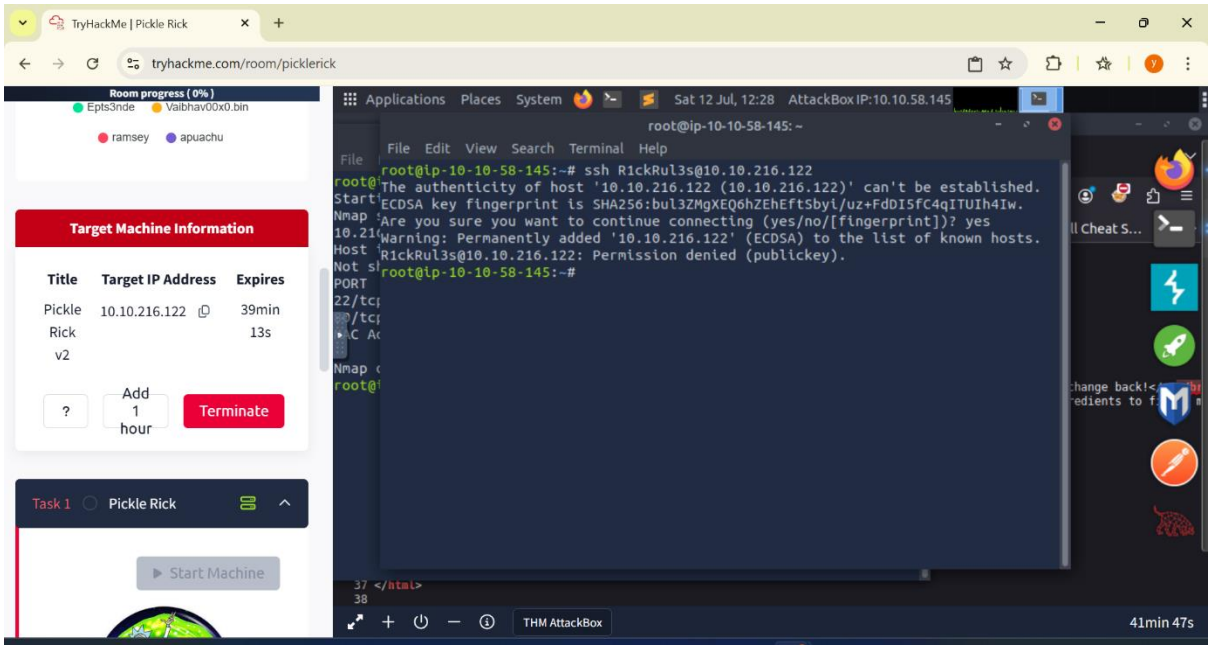
THE BEST STEP WAS THIS CAUSE THIS PROVED MY BELIFE OF BEING AN PHP SITE SINCE "/LOGIN.HTML DID NOT WORK AND /LOGIN.PHP WORKED" NOW WE KNOW THAT ITS AN PHP SITE WE CAN CHECK FOR "ROBOTS.TXT" CAUSE PHP NEEDS THIS FILE TO HOST

STEP 7: CHECK FOR ROBOTS



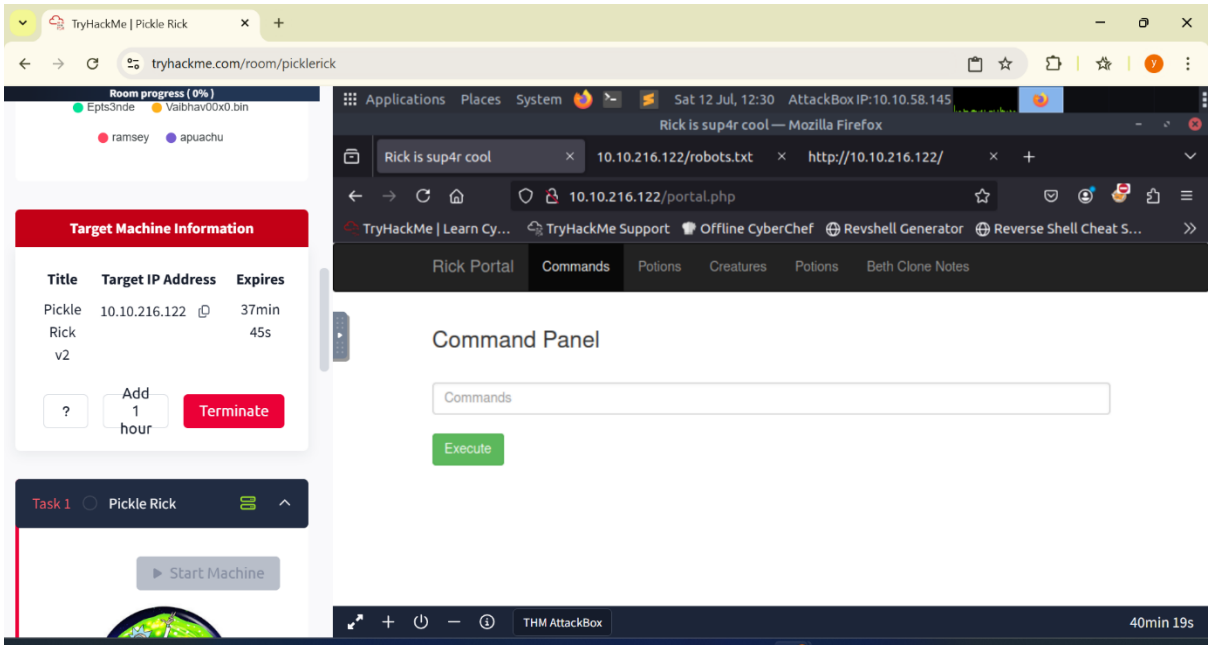
JUST LIKE THAT I THINK WE FOUND THE PASSWORD NOW LETS SSH IN TO THE MACHINE

STEP 8: SSH INTO TRAGET MACHINE



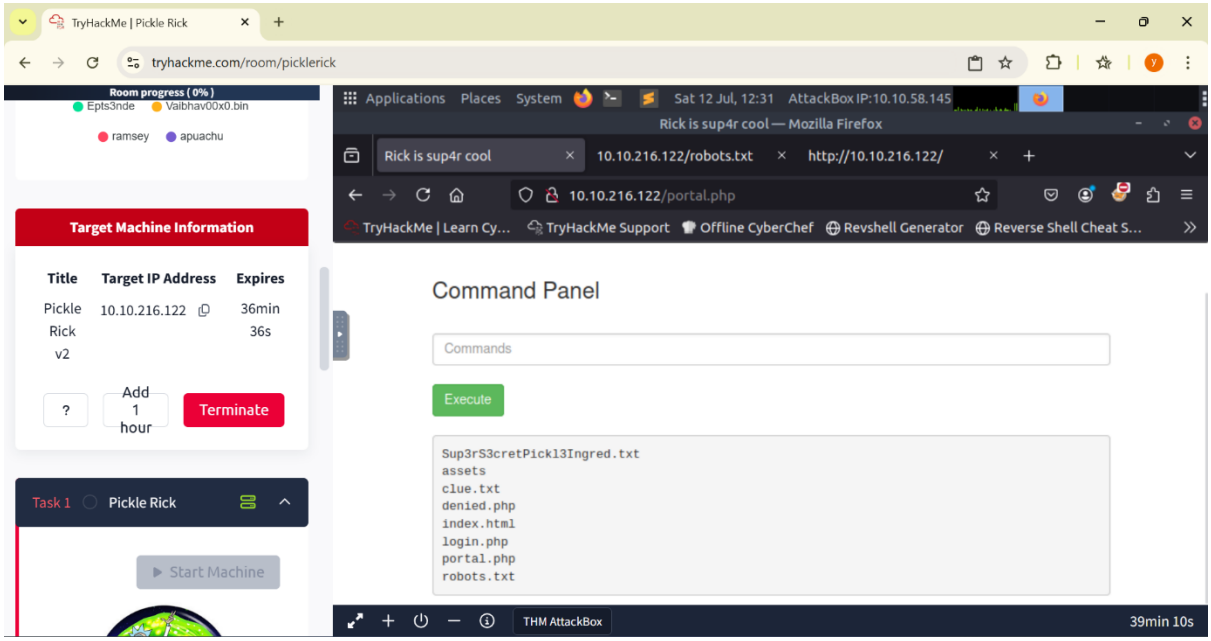
SINCE SSH DOES NOT ALLOW THE USER RickRul3s I THINK WE CAN TRY IT ON THE /LGOIN.PHP PAGE

STEP 9: TRYING TO LOGIN IN ON THE PHP PAGE



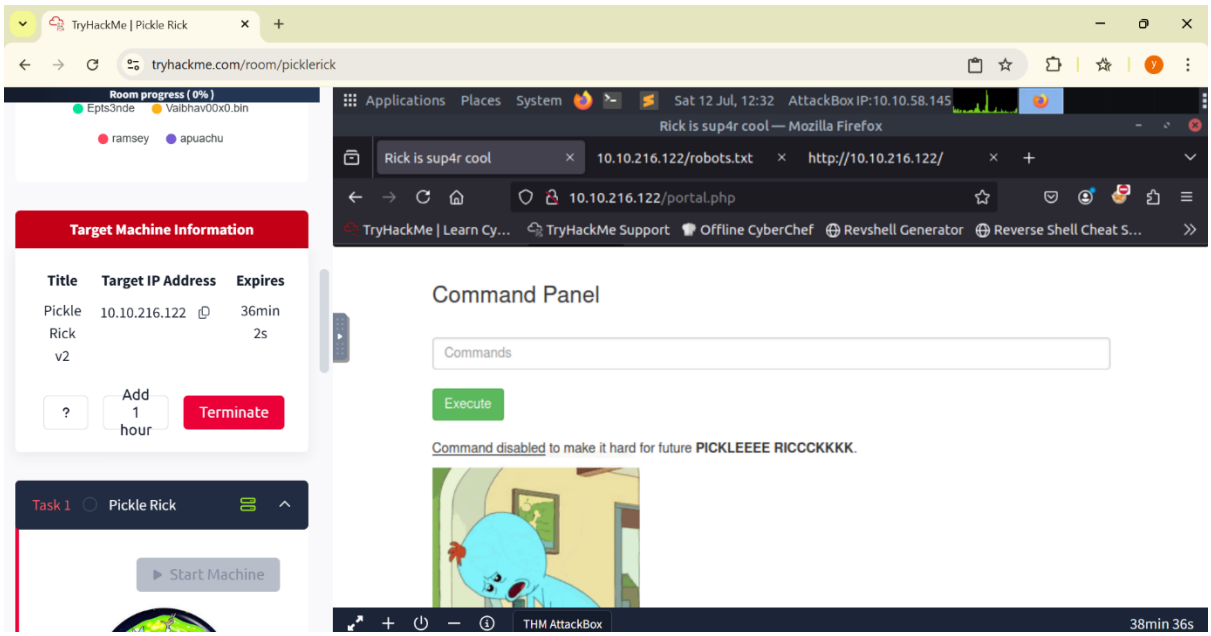
AND WE ARE IN THIS COMMAND PANEL IS JUST LIKE AN TERMINAL SO LETS TRY EXECUTING COMMANDS

STEP 10: LS COMMAND



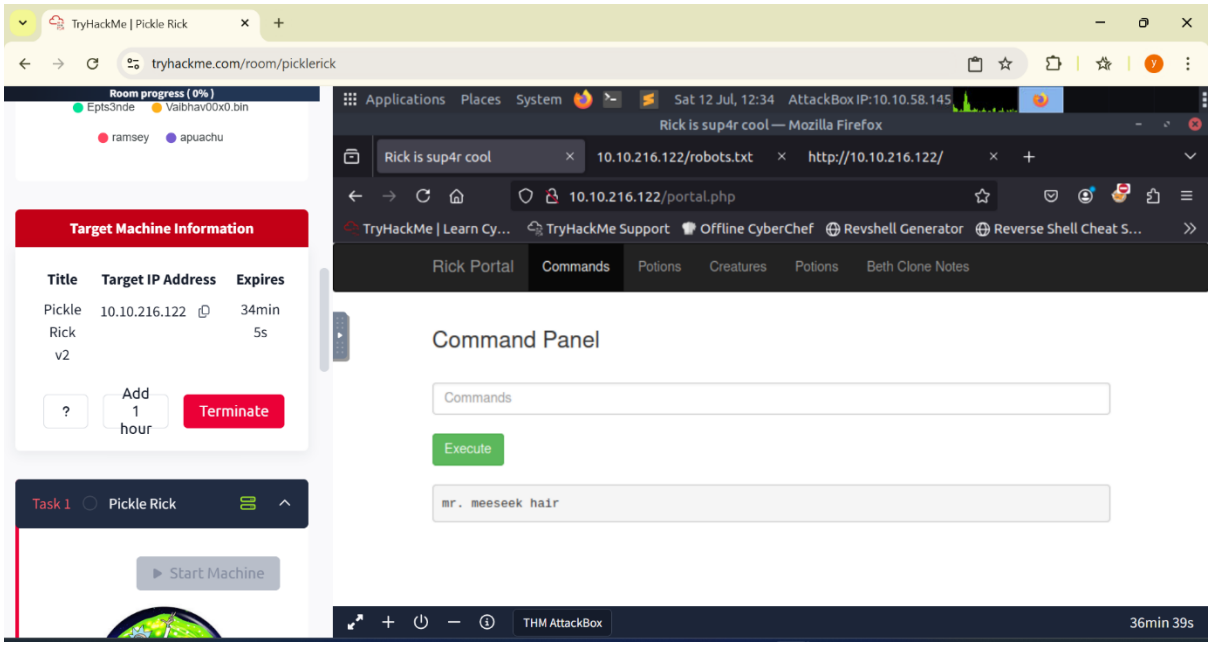
THE LS COMMAND SHOWS US THE CONTENTS AND WE CAN SEE “Sup3rS3cretPickl3Ingred.txt” LET’S CAT THE CONTENTS OF THE FILE

STEP 11: CAT COMMAND



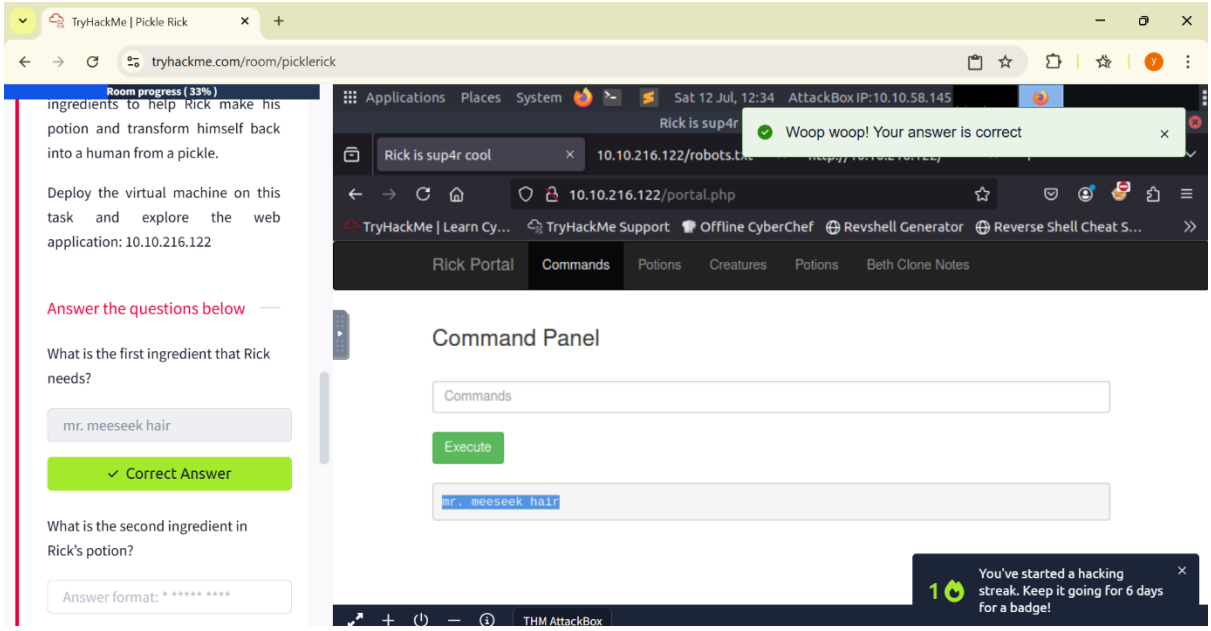
SINCE THE COMMAND IS DISABLED I THINK WE CAN USE THE LESS COMMAND TO READ THE FILE (MY MAN RICK IS AN SMART ASS)

STEP 12: LESS COMMAND TO READ THE FILE



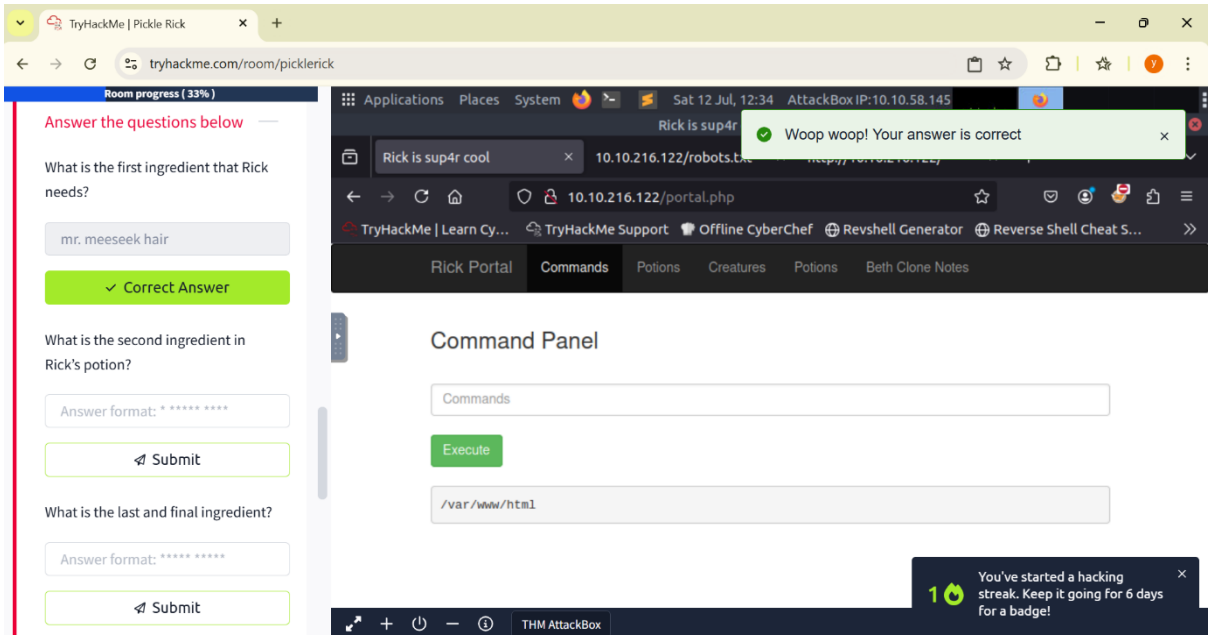
AND YES WE FOUND THE FIRST INGRIDENT LETS CHECK IT

STEP 13 : CHECKING THE KEY



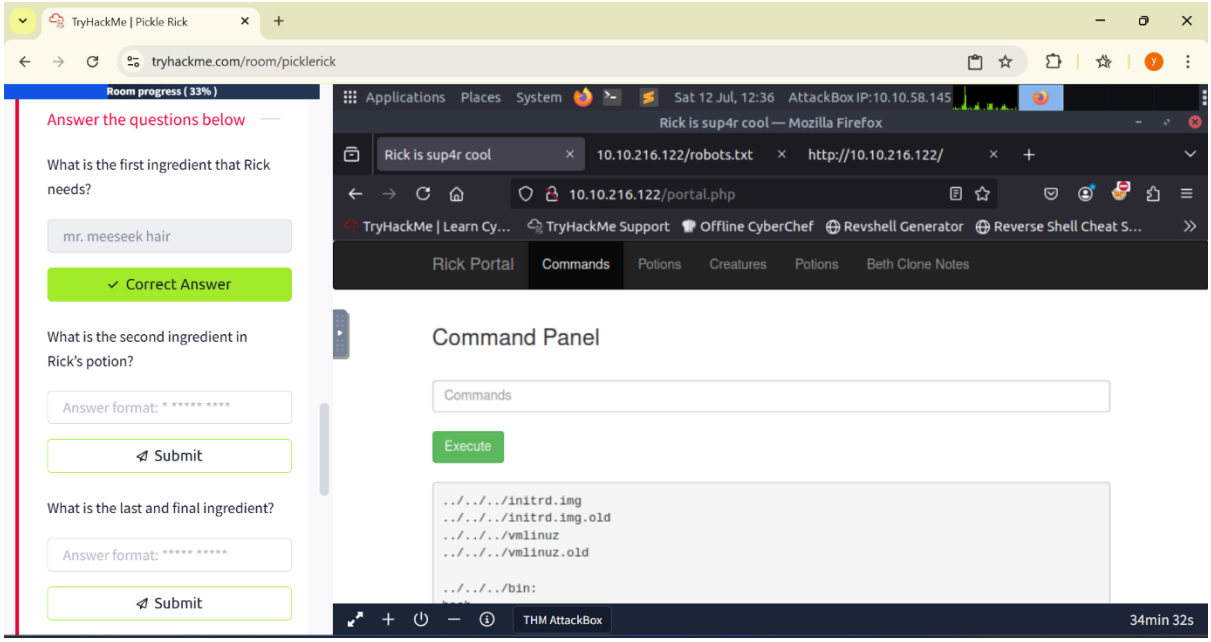
YES WE FOUND THE FIRST INGRIDENT, AS WE KNOW THAT THE SITE IS HOSTED WITH APACHE SERVER AND THAT WE COULD ONLY SEE THE SITE CONTENTS SO LETS CHECK THE WORKING DIRECTORY

STEP 14: PWD COMMAND



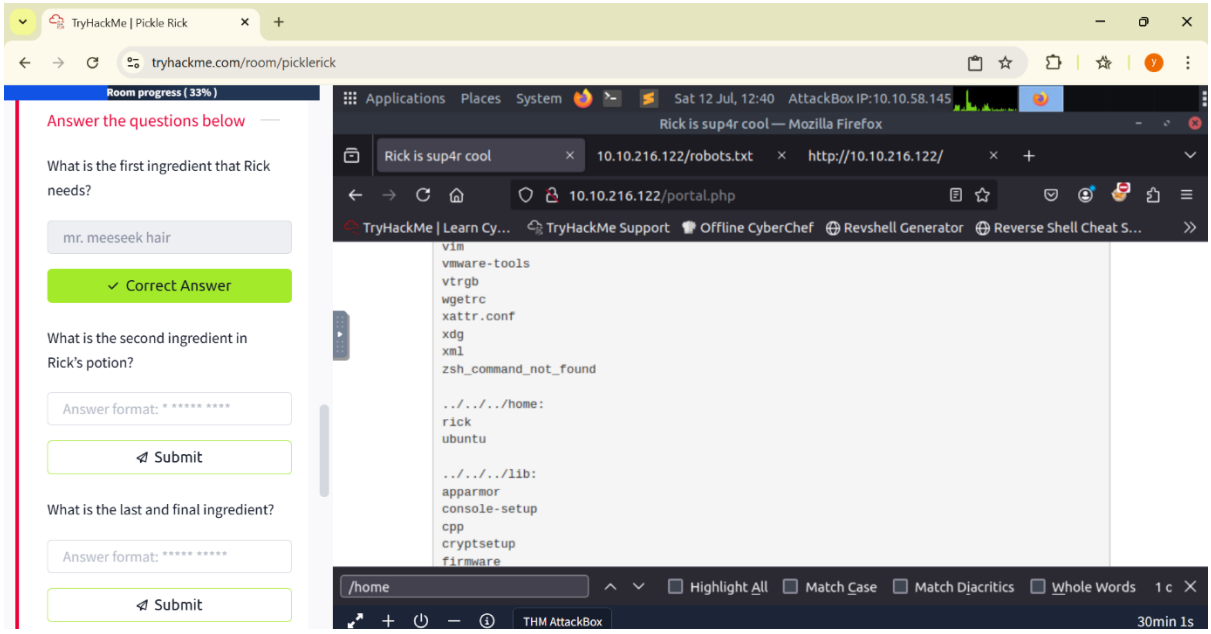
YES JUST LIKE I KNEW IT WE WHERE IN THE SERVER DIRECTORY TIME TO CHECK ALL THE CONTENTS OF THE MACHINE USING THE GODMOD COMMAND

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



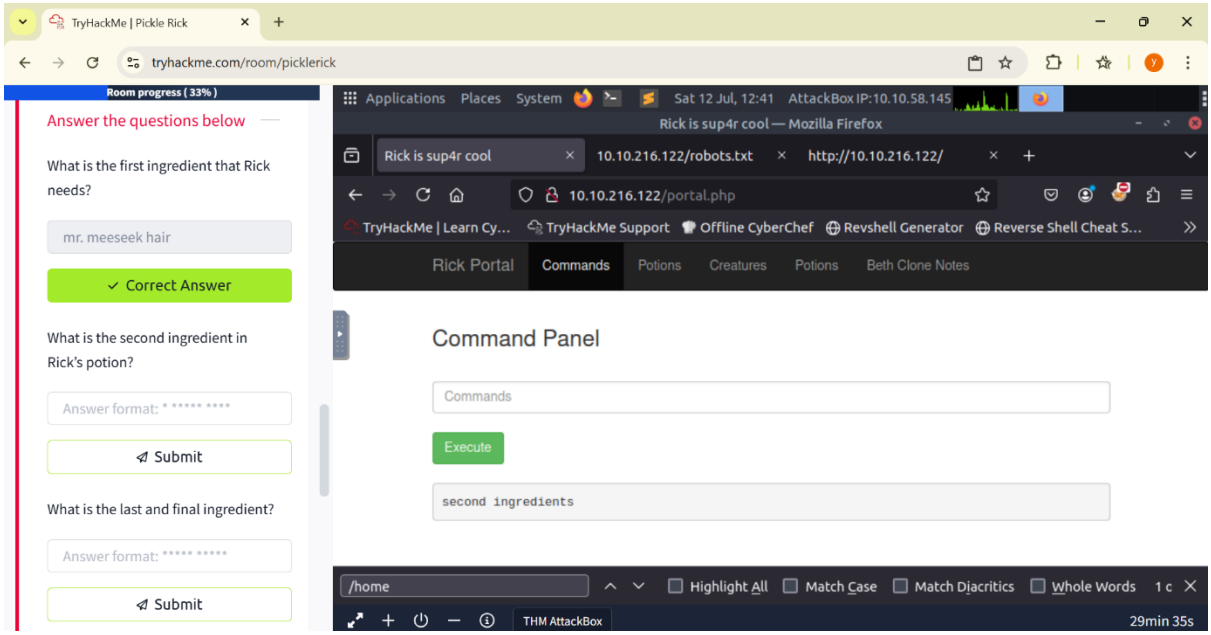
WE GOT ALL THE CONTENTS OF THE ENITRE MACHINE NOW LETS CHECK FOR HOME DIRECTORY

STEP 16: /HOME DIR



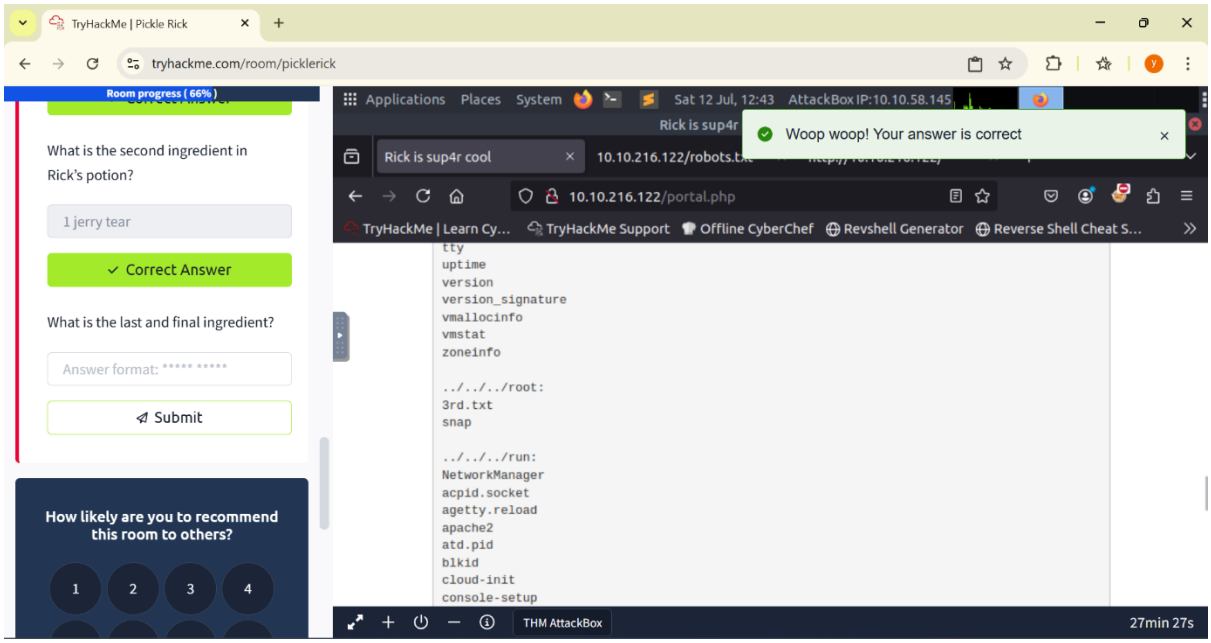
SO WE CAN SEE THAT THERE ARE TWO USERS IN THE MACHINE LETS LS THE CONTENTS IN THE RICK USER DIRECTORY BY USING THE COMMAND "SUDO LS ../../../HOME/RICK"

STEP 17: RICK



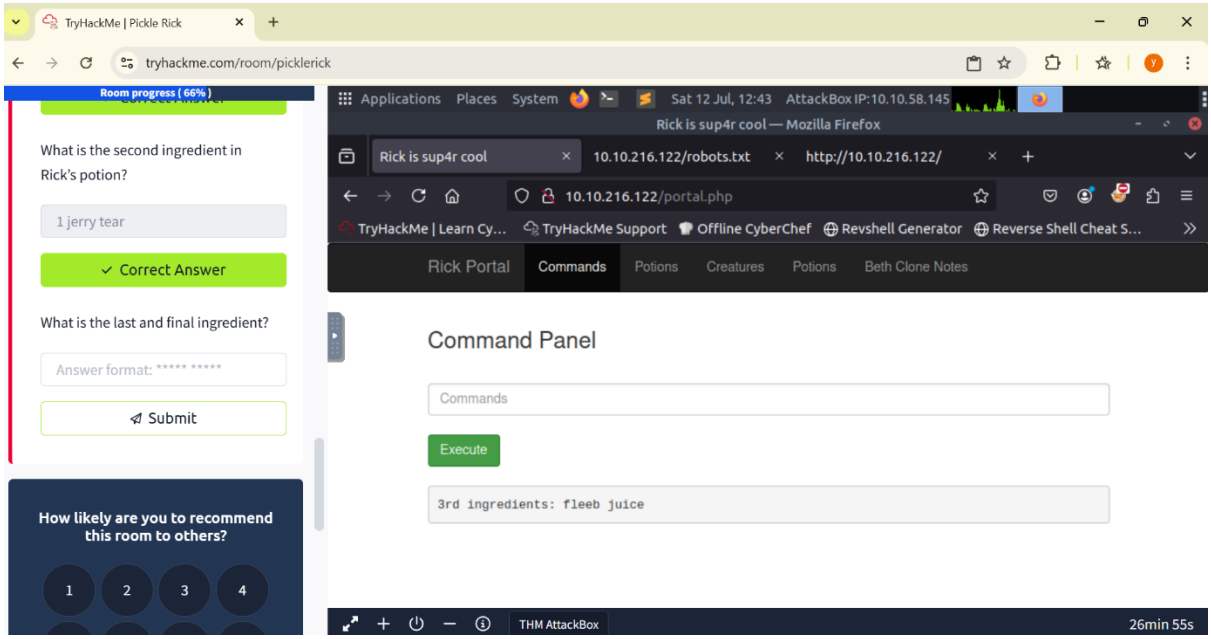
AND JUST LIKE THAT WE FOUND THE SECOND INGREDIENT LETS "LESS" IT OUT AND VERIFY THE KEY

STEP 18: SEARCH FOR THE 3RD INGRIDENT



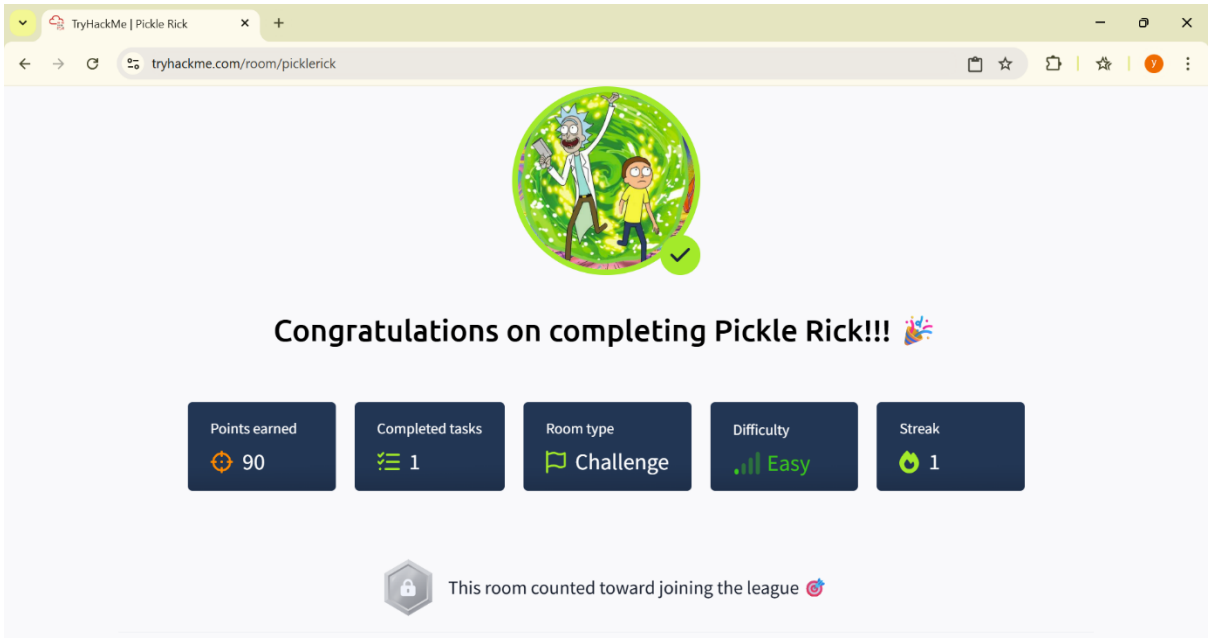
AGAIN EXECUTED THE GOD MODE COMMAND TO FIND THE 3RD INGRIDENT AND FOR LOOKING IT IN THE MESS I FOUND AND FILE CALLED 3RD.TXT LET'S TRY TO "LESS" IT OUT

STEP 19: 3RD.TXT



AND JUST LIKE THAT WE FOUND THE 3RD INGRIDENT 🧑‍🎤🧑‍🎤🔥

STEP 20: BRING PICKEL RICK BACK TO HUMAN FORM



AND THERE WE CURED RICK

THAT'S IT FROM ME
SINGING OFFF..

---YASHAS R NAIR