**CRYPTONITE**

**TASK PHASE 2**

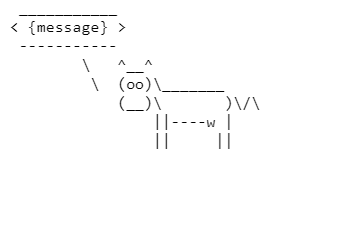
**WEB EXPLOITATION**

**CASS**

With this CTF, I copied the link of website and opened it on browser. The link showed me the URL

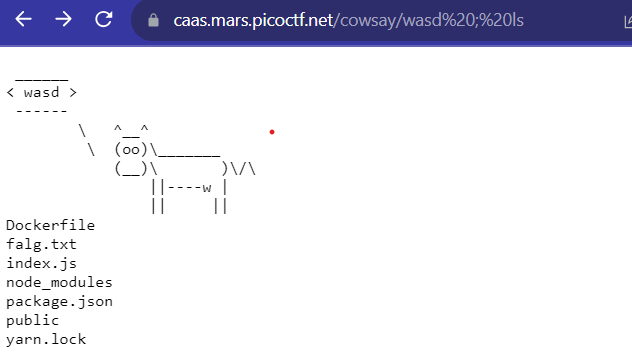


The URL clearly suggests that if you type any message at the end it would be displayed.



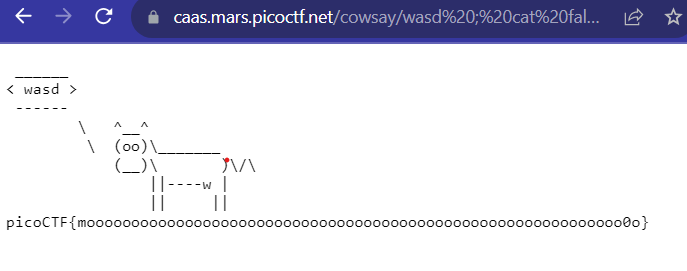
To get the flag, I used the terminal commands on the URL.

Here I used wasd ; ls to get the list of directories



Only falg.txt seemed to contain the password.

On concating it, I got the flag



**FINAL FLAG:** picoCTF{moooooooooooooooooooooooooooooooooooooooooooo0o}

**FORBIDDEN PATHS**

The website showed this text.

On searching or clicking the txt files, it showed the very big poem. Ignore that

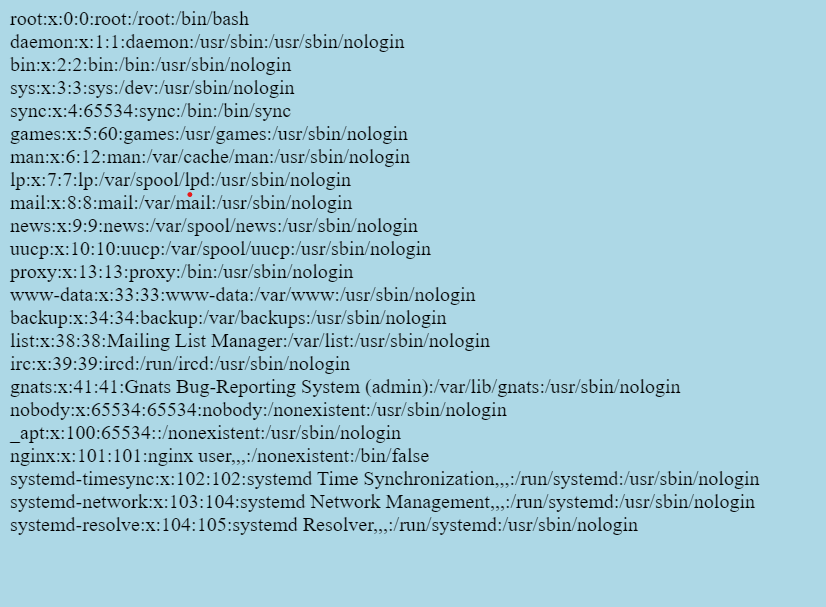
Tried getting the flag.txt file, but it didn’t show anything.



Put the following code below:

../../../../../etc/passwd

Got the below result



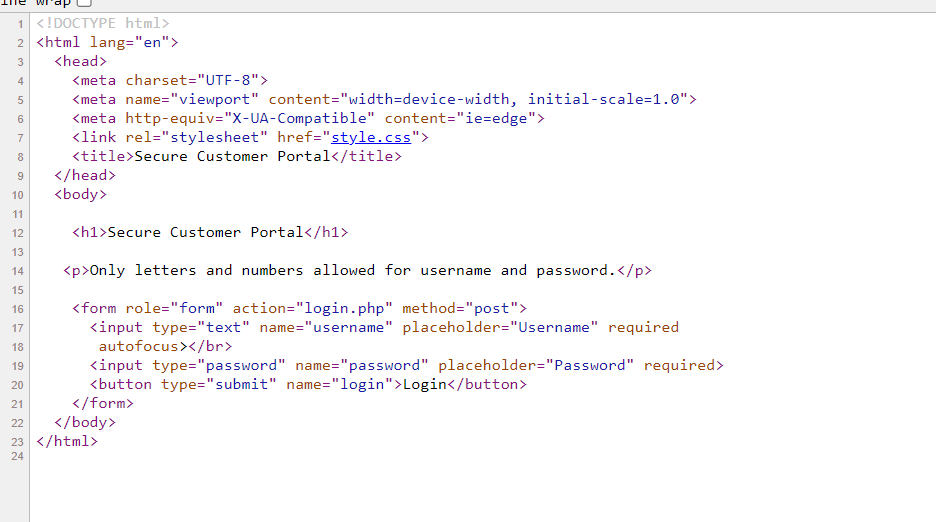
It showed the following things. I tried it again to bypass the security and the ctf Flag.



picoCTF{7h3\_p47h\_70\_5ucc355\_e5a6fcbc}

**LOCAL AUTHORITY**

I opened the website and went to source code.

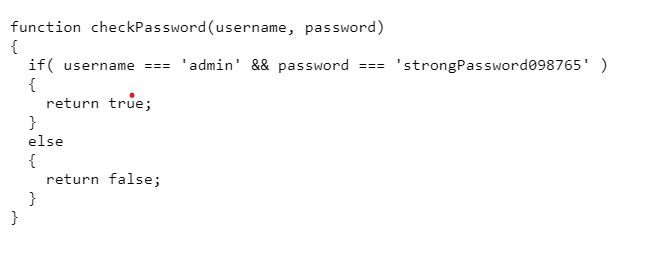
****

I entered the wrong username and password and then went to source code again to see if there are any changes. It showed a secure.js file in its code.

****

I opened the js file and got another code which showed me the username and password.

I entered both of them and got the CTF

****

PicoCTF{j5\_15\_7r4n5p4r3n7\_05df90c8}