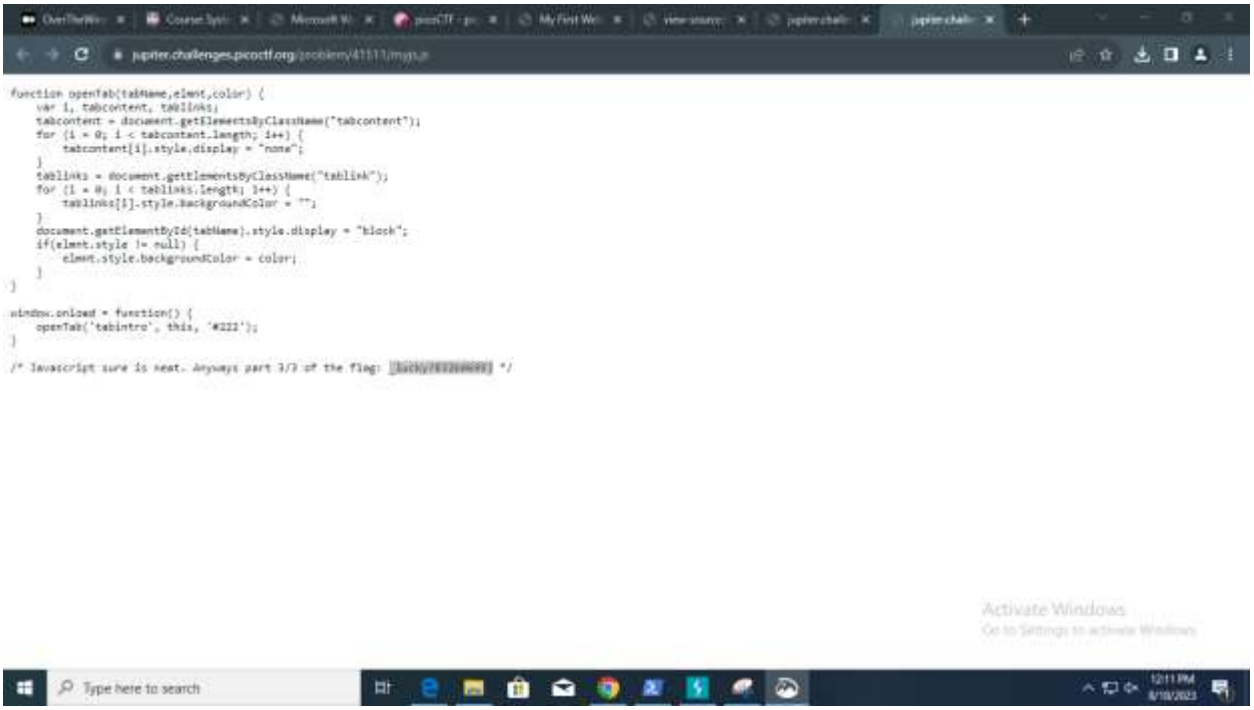
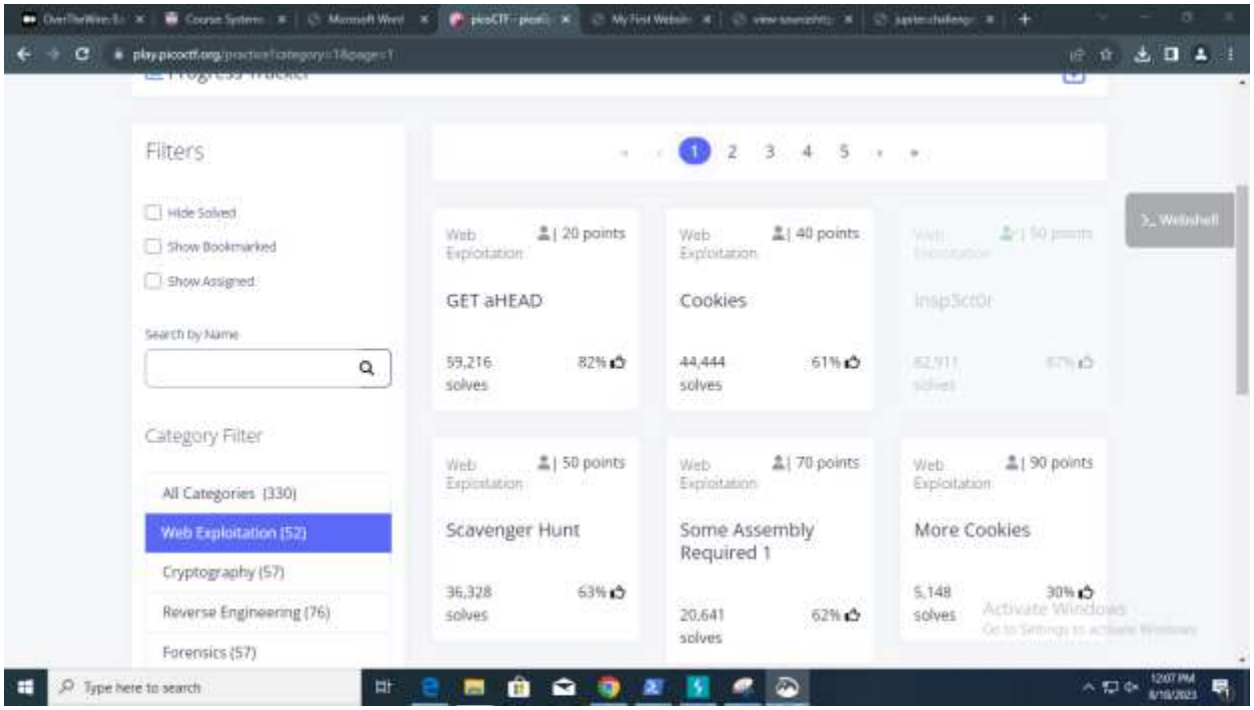
01 - Insp3ct0r

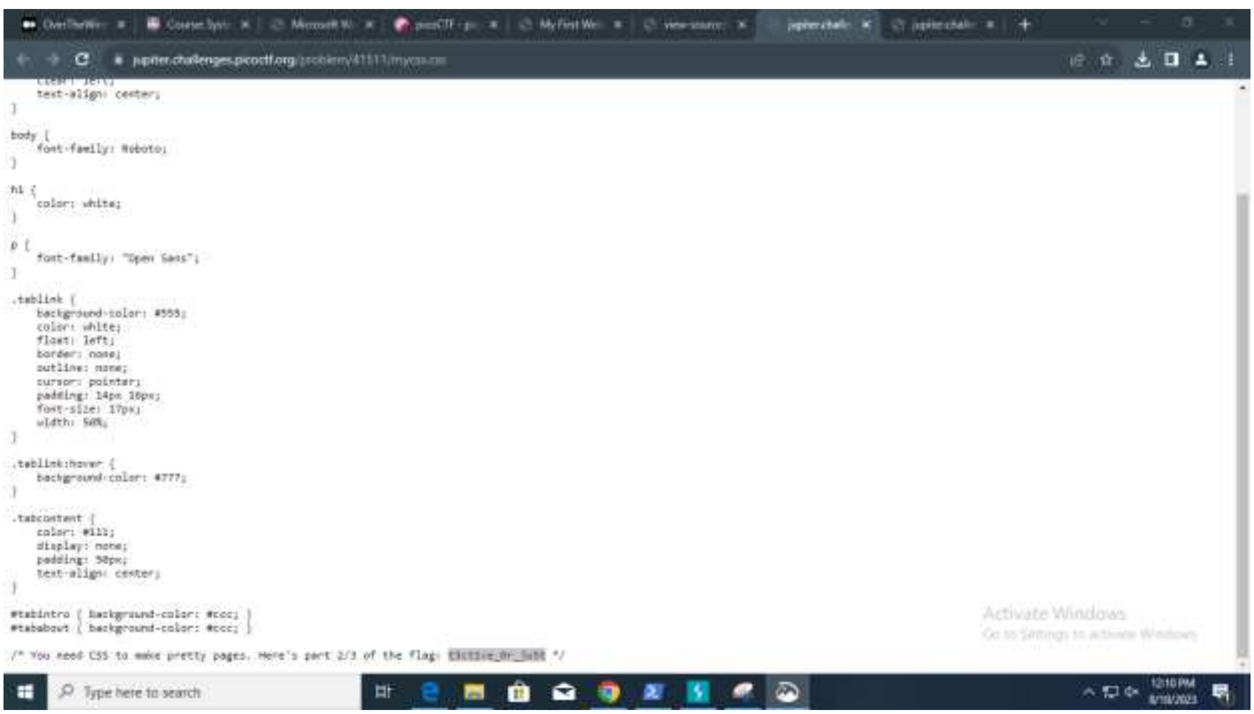
first inpect or view the page source the you'll find the first part of the flag.

then the other parts are on CSS and .js file.

picoCTF{tru3_d3 t3ct1ve_0r_ju5t _lucky?832b0699}




play.picoctf.org/practice?category=1&page=1
Filters
Hide Solved
Show Bookmarked
Show Assigned
Search by Name
Category Filter
All Categories (330)
Web Exploitation (52)
Cryptography (57)
Reverse Engineering (76)
Forensics (57)
Web Exploitation
20 points
GET aHEAD
59,216 solves
82%
Web Exploitation
40 points
Cookies
44,444 solves
61%
Web Exploitation
50 points
Scavenger Hunt
36,328 solves
63%
Web Exploitation
70 points
Some Assembly Required 1
20,641 solves
62%
Web Exploitation
90 points
More Cookies
5,148 solves
30%
Webshell
Type here to search


jupiter.challenges.picoctf.org
text-align: center;
}
body {
font-family: Roboto;
}
h1 {
color: white;
}
p {
font-family: "Open Sans";
}
.tablink {
background-color: #555;
color: white;
float: left;
border: none;
outline: none;
cursor: pointer;
padding: 14px 16px;
font-size: 17px;
width: 50%;
}
.tablink:hover {
background-color: #777;
}
.tabcontent {
color: #111;
display: none;
padding: 50px;
text-align: center;
}
#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }
/* You need CSS to make pretty pages. Here's part 2/3 of the flag: */
Type here to search

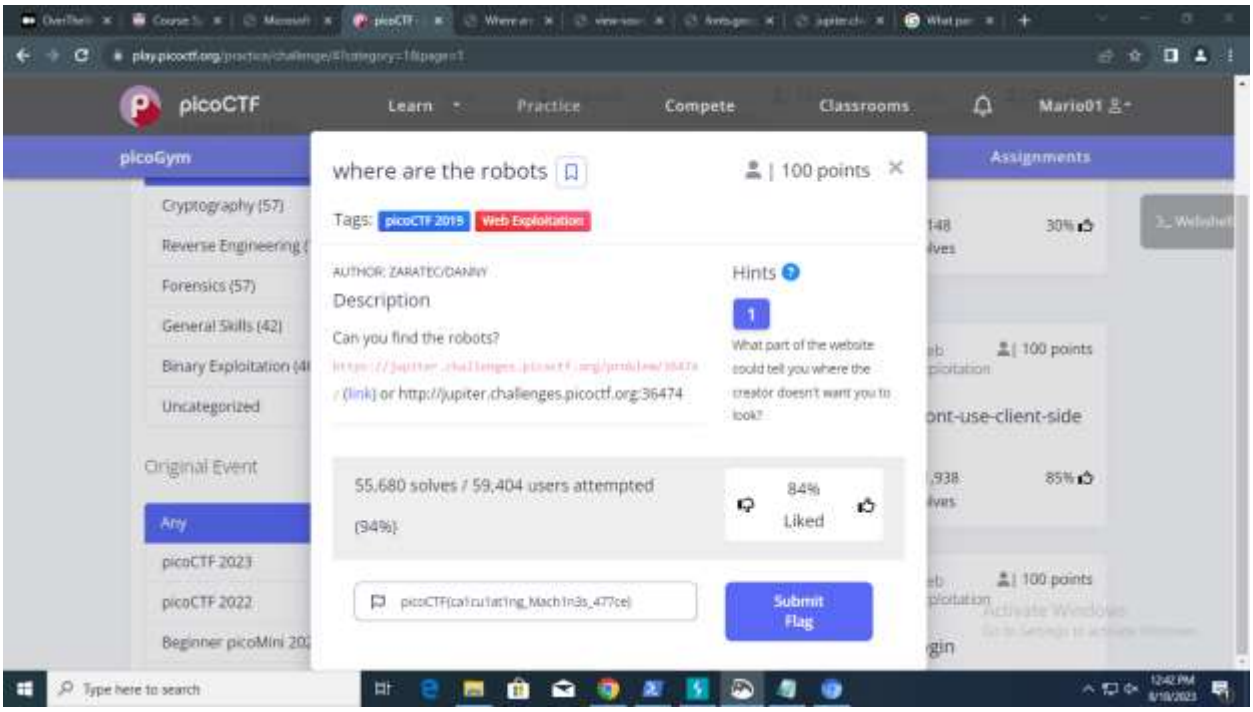
02- Wherer are the Robots

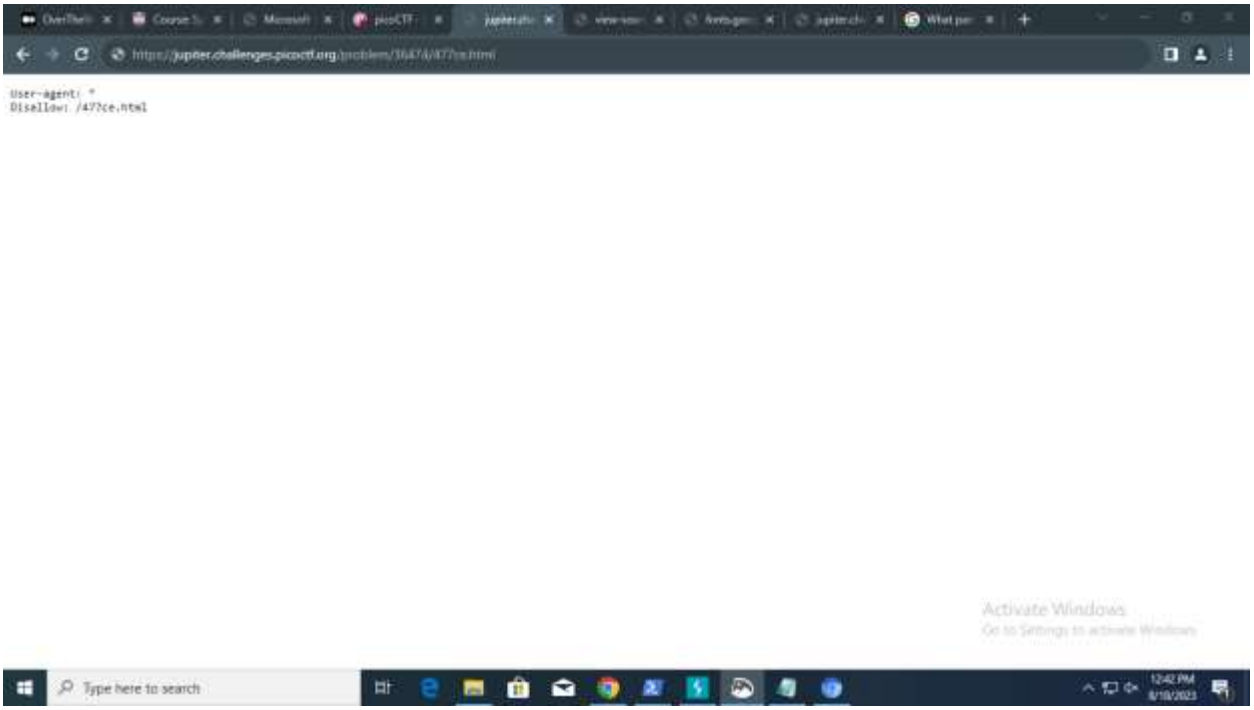
you neeed to go to the robots.txt

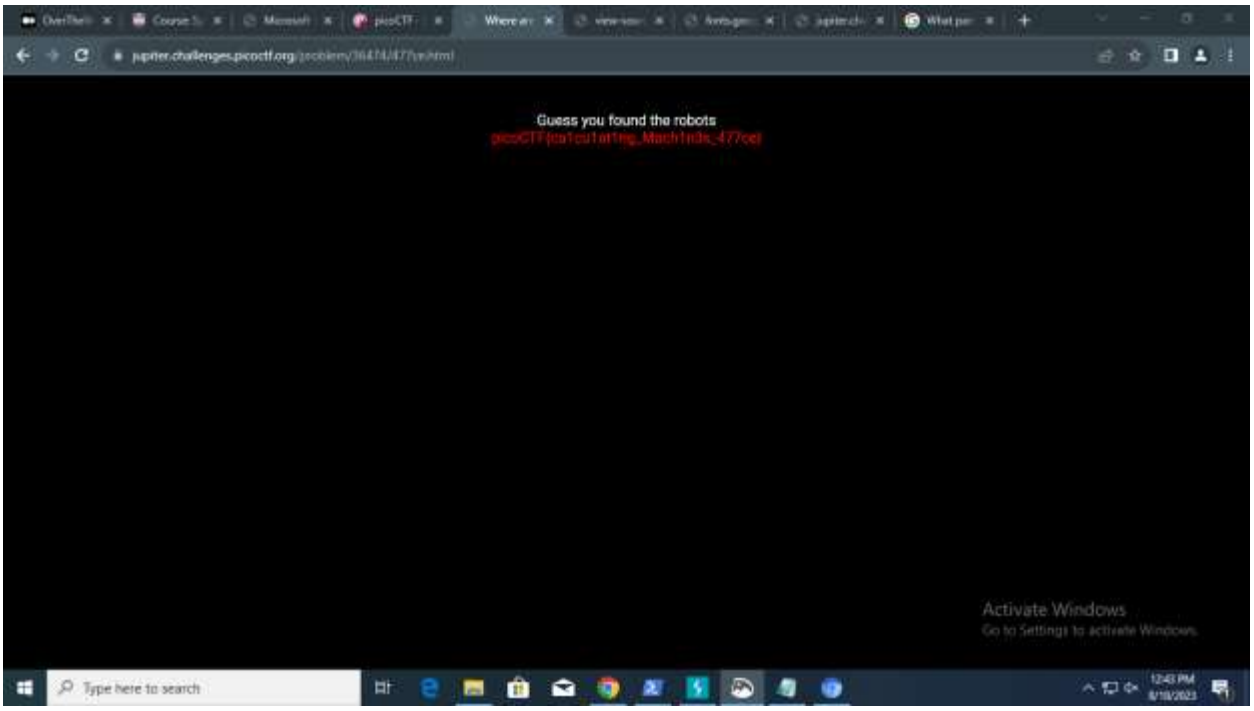
https://jupiter.challenges.picoctf.org/problem/36474/robots.txt

/477ce.html

picoCTF{ca1cu1at1ng_Mach1n3s_477ce}



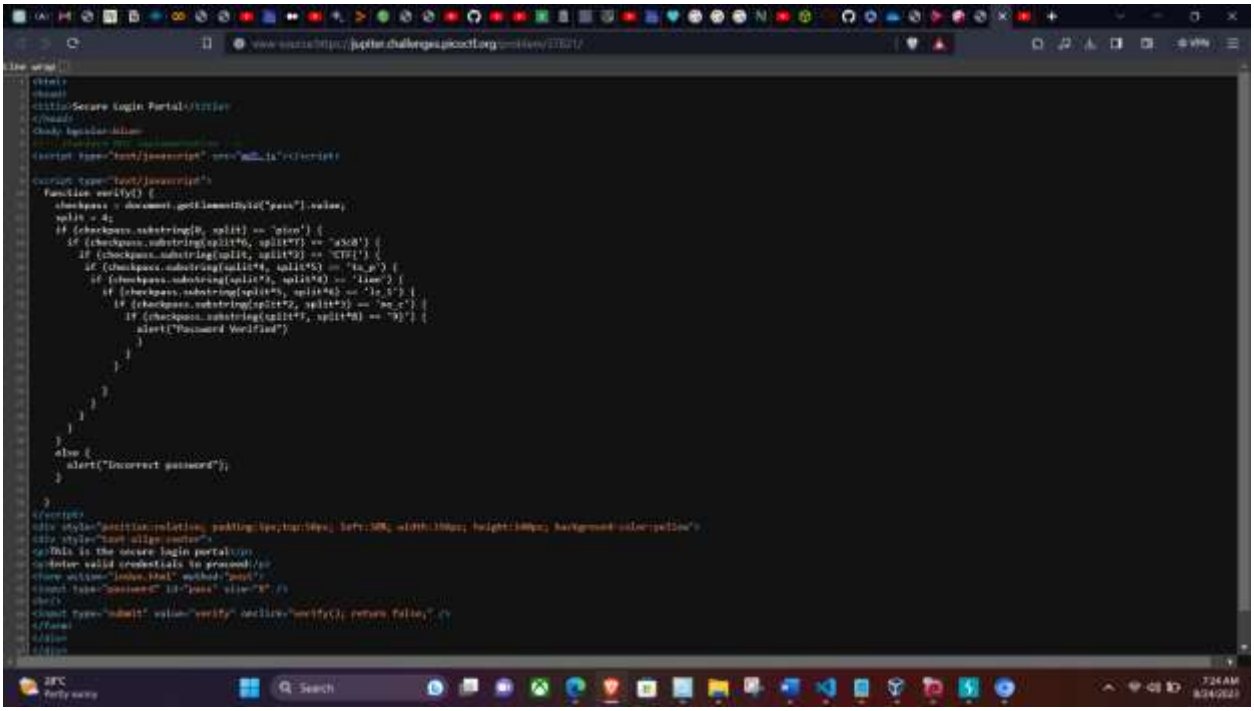

User-agent: *
Disallow: /47?ce.html
Activate Windows
Go to Settings to activate Windows.
Type here to search


Guess you found the robots
Activate Windows
Go to Settings to activate Windows.
Type here to search

03 - Dont use Clientside

flag is on the page source you need to replace it to proper order.

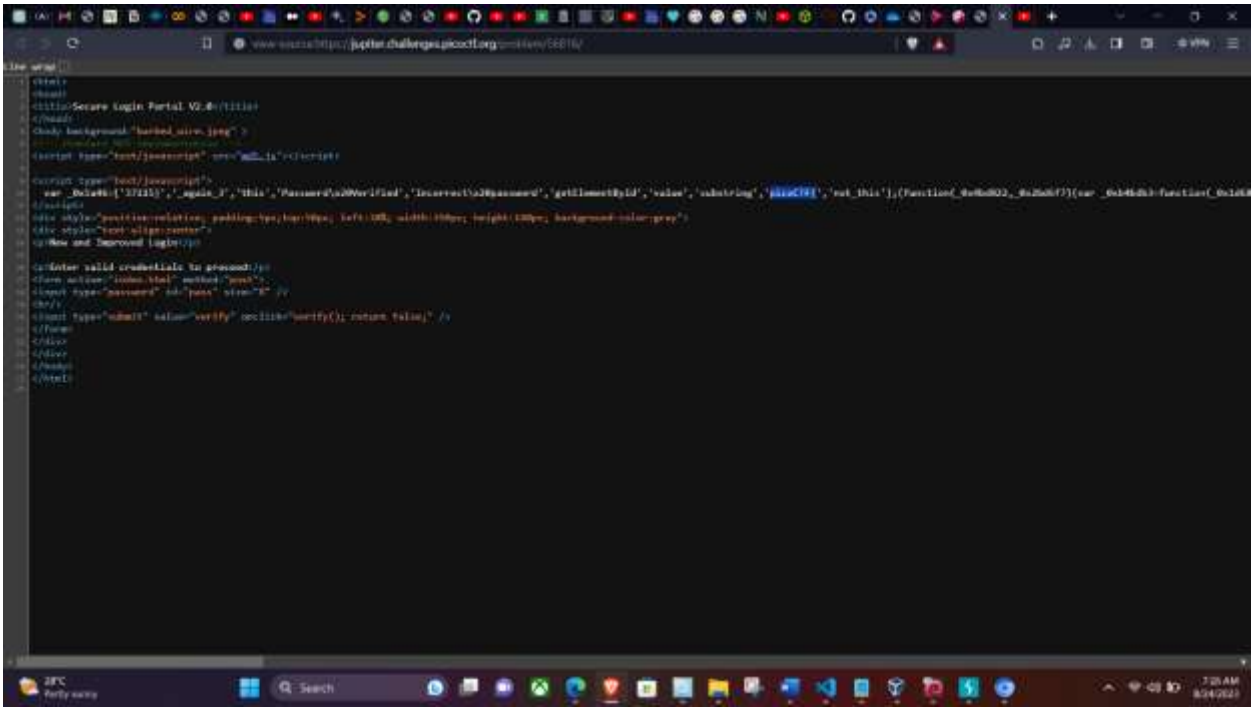
picoCTF{no_clients_plz_1a3c89}



04 - Client Side Again

Password is hidden in the java script tag ypu need to find it snd arrange it to an order

picoCTF{not_this_again_337115}



05 - Flag shop

integer overflow in the calculation of total_cost. An integer in C typically has a range of values it can represent. For a 32-bit integer, the range is from -2,147,483,648 to 2,147,483,647.

2,147,483,647/900 = 2386092

total_cost = 900 * number_flags;

account_balance = account_balance - total_cost;

If number_flags is a large positive value (like 2386396), the multiplication 900 * 2386396 will result in a value that exceeds the maximum positive value that a 32-bit integer can hold. This will cause an integer overflow, and the value of total_cost will wrap around and become a negative value due to the way two's complement representation works. Then we can get the flag.

To fix this issue, you can use a larger data type, such as long long, which can hold larger .

picoCTF{m0n3y_bag5_9c5fac9b}

```c
#include <stdio.h>
#include <stdlib.h>
int main()
{
   setbuf(stdout, NULL);
   int con;
   con = 0;
   int account_balance = 1100;
   while(con == 0){

      printf("Welcome to the flag exchange\n");
      printf("We sell flags\n");

      printf("\n1. Check Account Balance\n");
      printf("\n2. Buy Flags\n");
      printf("\n3. Exit\n");
      int menu;
      printf("\n Enter a menu selection\n");
      fflush(stdin);
      scanf("%d", &menu);
      if(menu == 1){
         printf("\n\n\n Balance: %d \n\n\n", account_balance);
      }
      else if(menu == 2){
         printf("Currently for sale\n");
         printf("1. Defintely not the flag Flag\n");
         printf("2. 1337 Flag\n");
```

```
        int auction_choice;
        fflush(stdin);
        scanf("%d", &auction_choice);
        if(auction_choice == 1){
            printf("These knockoff Flags cost 900 each, enter desired quantity\n");

            int number_flags = 0;
            fflush(stdin);
            scanf("%d", &number_flags);
            if(number_flags > 0){
                int total_cost = 0;
                total_cost = 900*number_flags;
                printf("\nThe final cost is: %d\n", total_cost);
                if(total_cost <= account_balance){
                    account_balance = account_balance - total_cost;
                    printf("\nYour current balance after transaction: %d\n\n", account_balance);
                }
                else{
                    printf("Not enough funds to complete purchase\n");
                }


            }




        }
        else if(auction_choice == 2){
            printf("1337 flags cost 100000 dollars, and we only have 1 in stock\n");
            printf("Enter 1 to buy one");
            int bid = 0;
            fflush(stdin);
            scanf("%d", &bid);

            if(bid == 1){

                if(account_balance > 100000){
                    FILE *f = fopen("flag.txt", "r");
                    if(f == NULL){

                        printf("flag not found: please run this on the server\n");
                        exit(0);
                    }
                    char buf[64];
                    fgets(buf, 63, f);
                    printf("YOUR FLAG IS: %s\n", buf);
                    }

                else{
                    printf("\nNot enough funds for transaction\n\n\n");
                }}
```

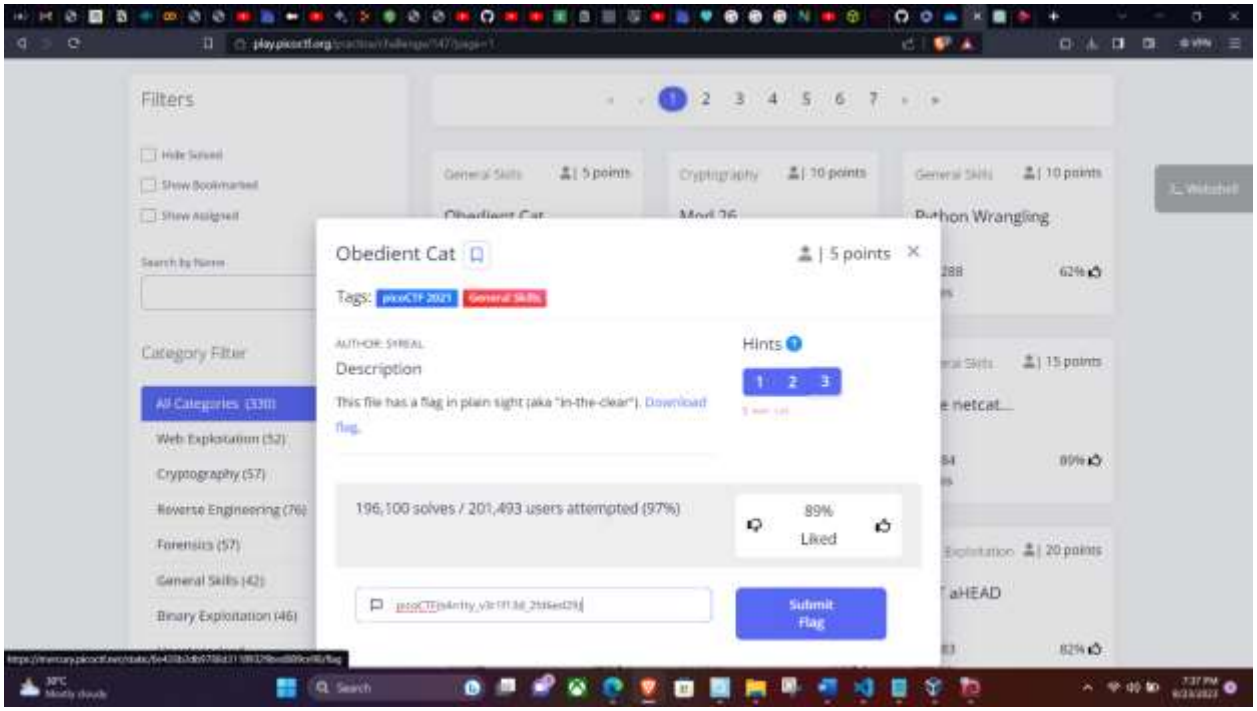
```
            }
        }
        else{
            con = 1;
        }

    }
    return 0;
}
```

06 - obedient Cat

when you download the file they give it contains the flag.

picoCTF{s4n1ty_v3r1f13d_2fd6ed29}



07 - GO AHEAD

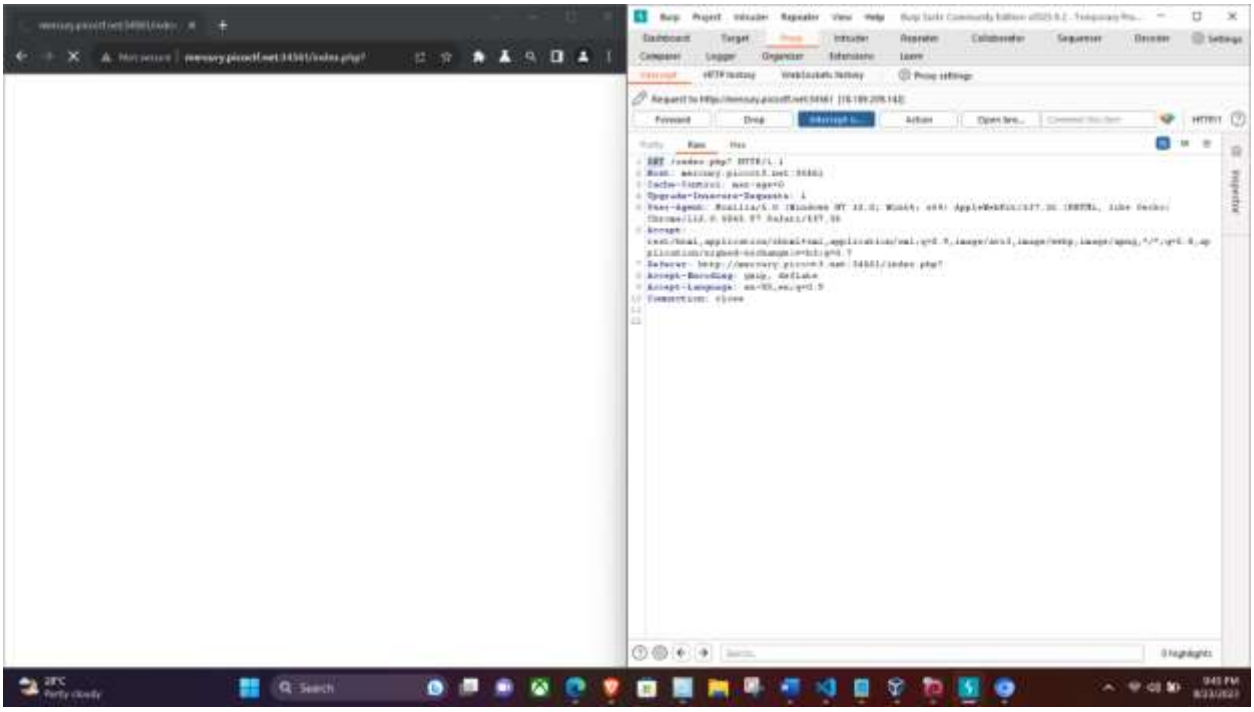
In this challenge we need to change the https request

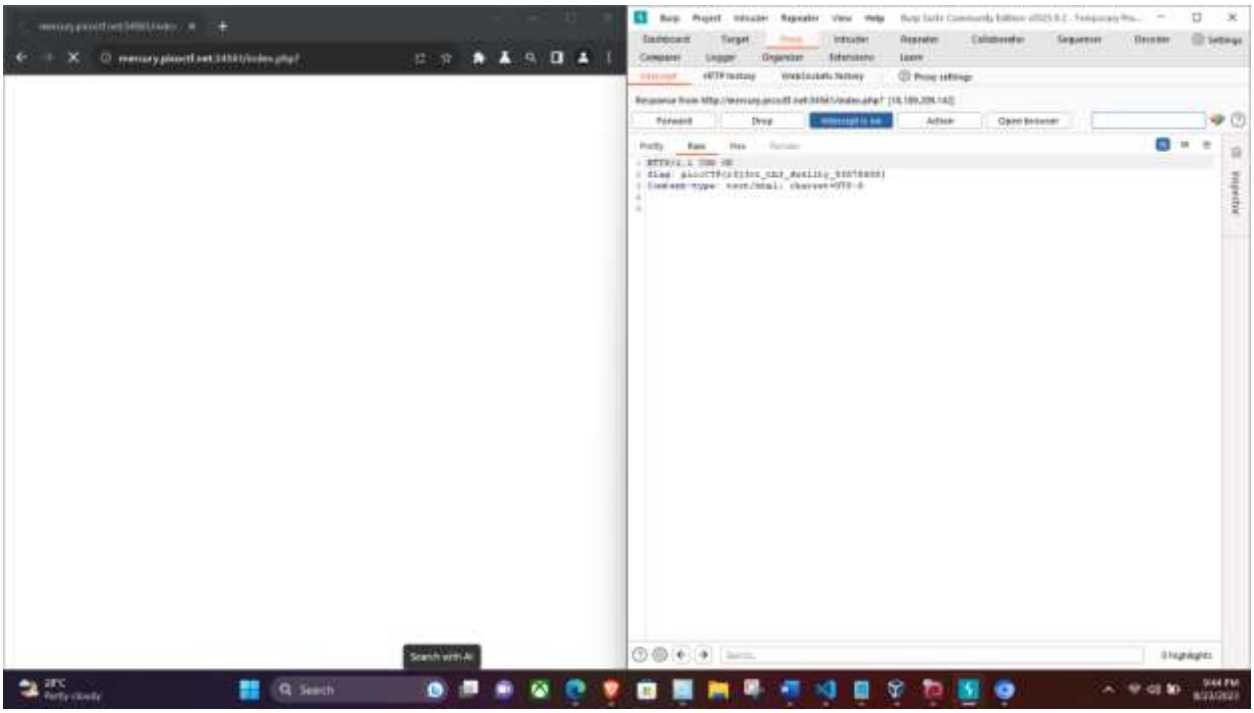
there are many req methods such as GET, POST, HEAD

HEAD - Purpose: Similar to GET, but only retrieves the headers of the response, not the actual data.

USING BURPSUITE change the req and forward it the you'll get the flag.

picoCTF{r3j3ct_th3_du4l1ty_8f878508}





08 - Crackme.py

wget https://mercury.picoctf.net/static/b7cabaae6561256c50728d3515db3058/crackme.py

download the file and

vim or nano crackme.py

comment the part in the code that gives us the largest number we need to get the flag there for change the code

bezos_cc_secret = "A:4@r%uL`M-^M0c0AbcM-MFE07b34c`_6N" this is the ecooded secrect we'll print it out.

#choose_greatest()

decode_secret(bezos_cc_secret)

python crackme.py

picoCTF{1|\/|_4_p34|\|ut_f3bc410e}

09 - Lets Warm Up

Decimal Number	ASCII Character	Hex Value
112	p	0x70
113	q	0x71
114	r	0x72
115	s	0x73

then the answer is picoCTF{p}

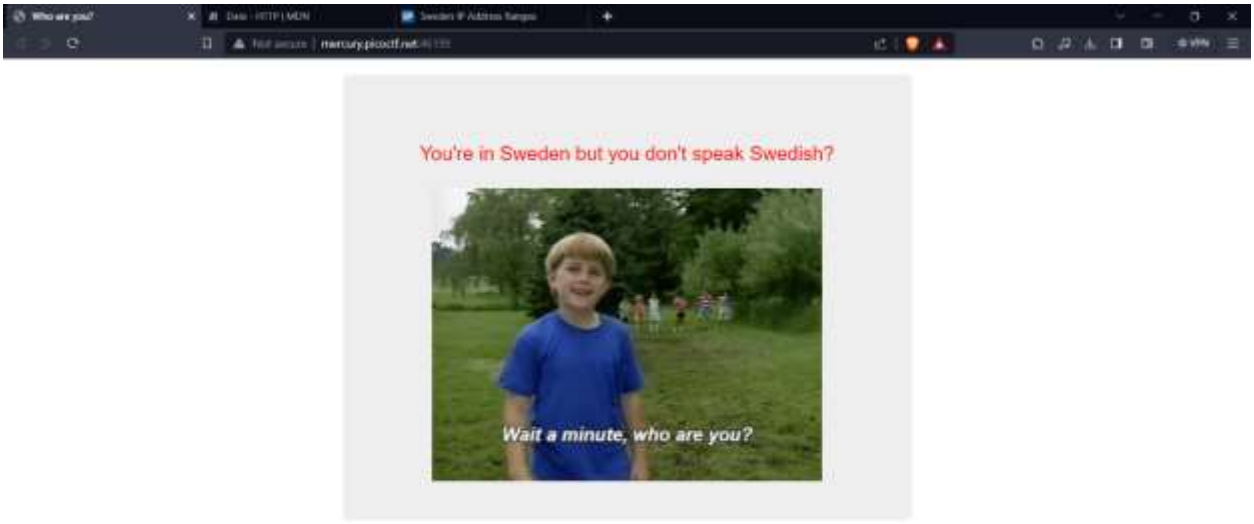
10 - Who are you

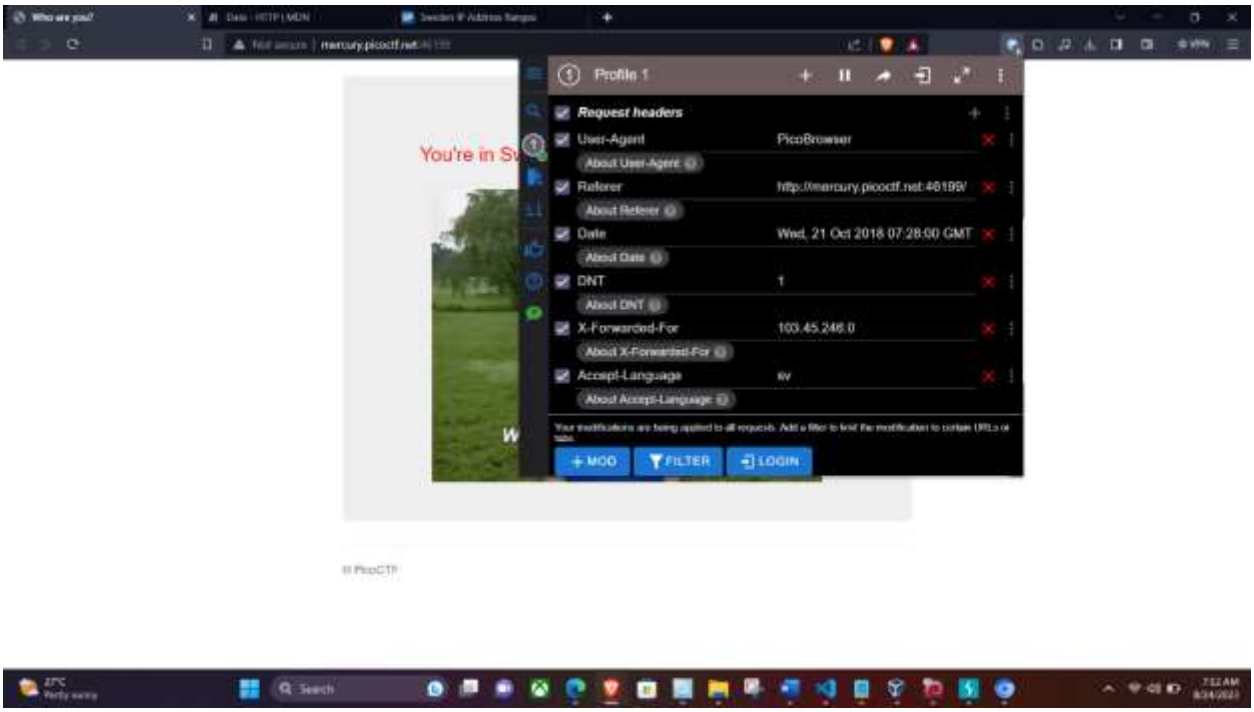
in this challenge we need to change request headers

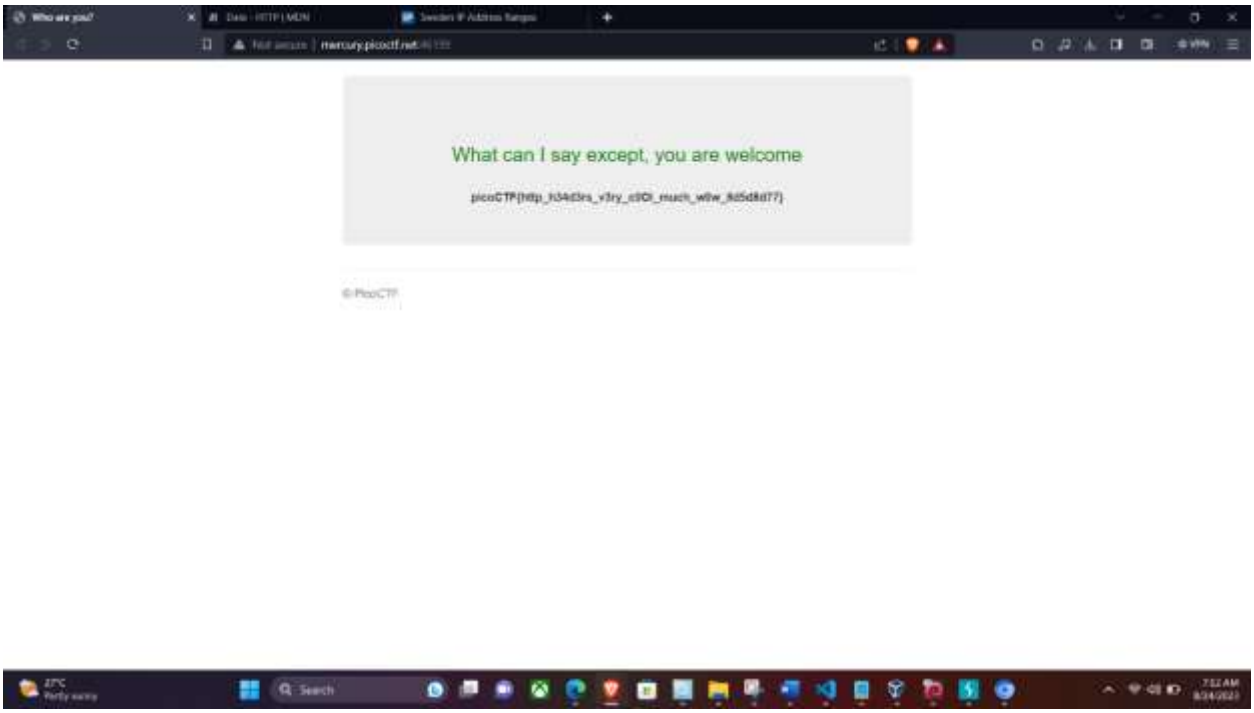
i used a extension called "Mod header"

then i changed header requests according to the challenge and got the password.

picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_8d5d8d77}


You're in Sweden but you don't speak Swedish?
Wait a minute, who are you?


Profile 1
Request headers
User-Agent
PicoBrowser
About User-Agent
Referer
http://mercury.picoctf.net:46199/
About Referer
Date
Wed, 21 Oct 2018 07:28:00 GMT
About Date
DNT
1
About DNT
X-Forwarded-For
103.45.246.0
About X-Forwarded-For
Accept-Language
sv
About Accept-Language
+ MOD
FILTER
LOGIN


What can I say except, you are welcome
picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_8d5d8d77}