

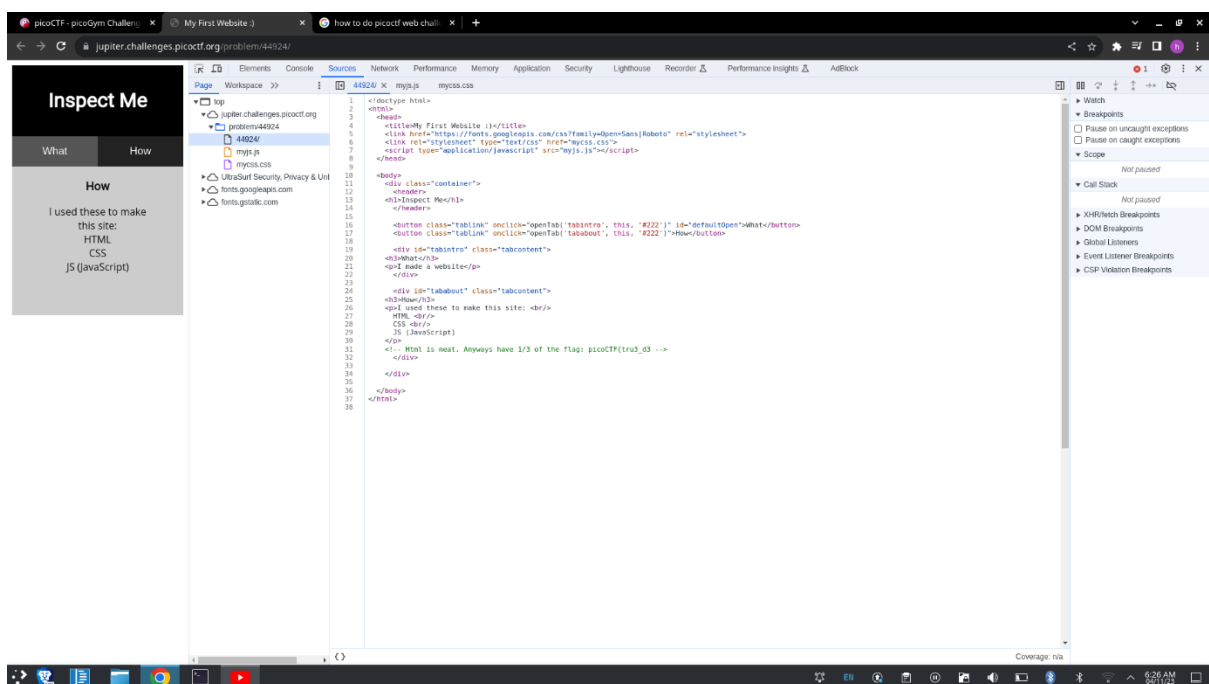
PICO CTF

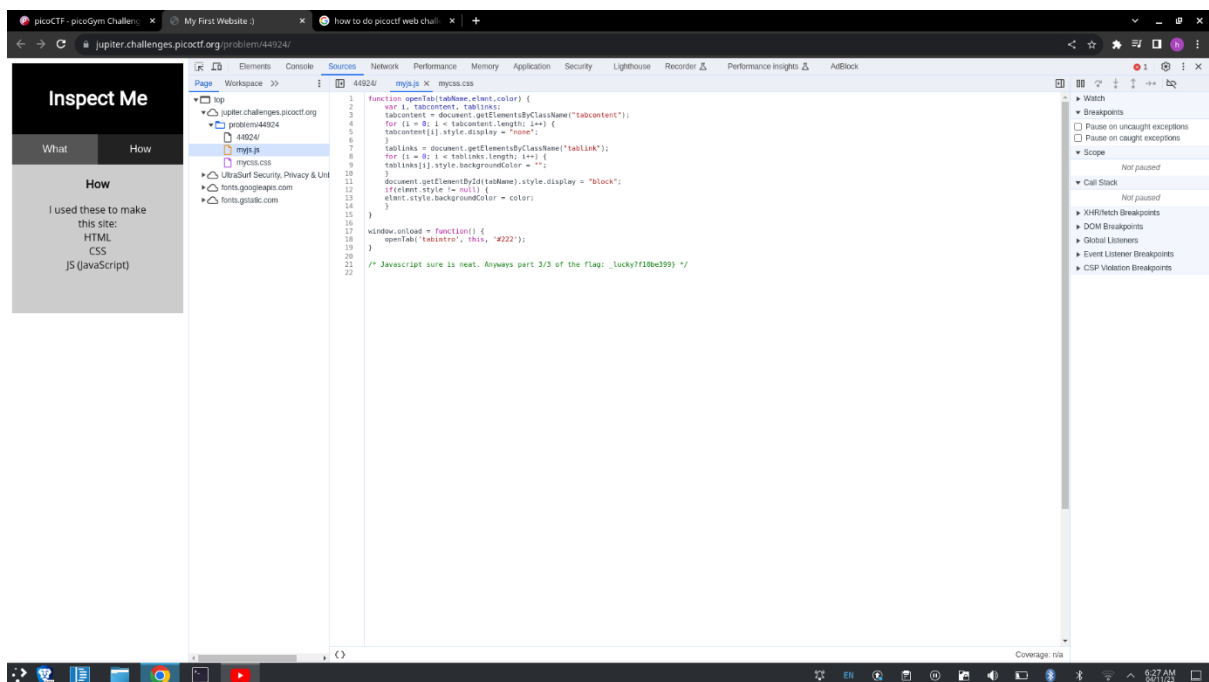
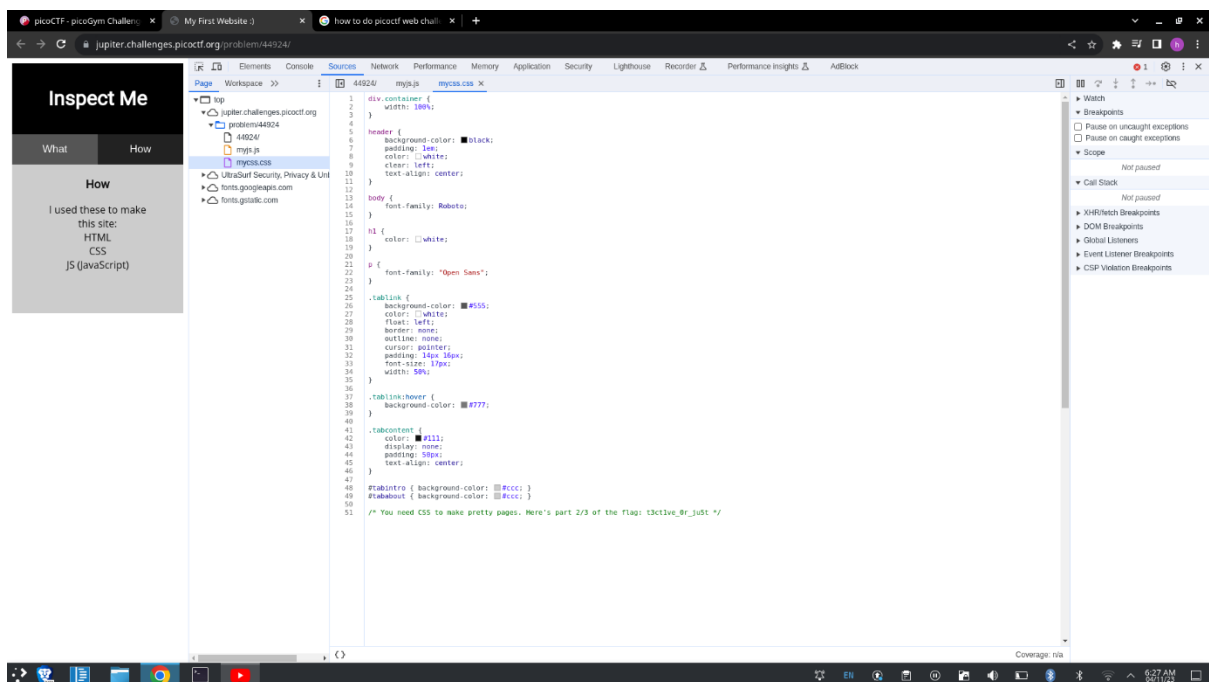
BY, JAIFIN B ALOOR

PICOGYM WEB EXPLAITATION PRATICE CHALLENGES

INSP3CTOR CHALLENGE

First I right clicked on the website and opened the inspect window. Then I went to the page sources and clicked on the JS file , CSS file and the HTML file and these files had the parts that made up the flag.

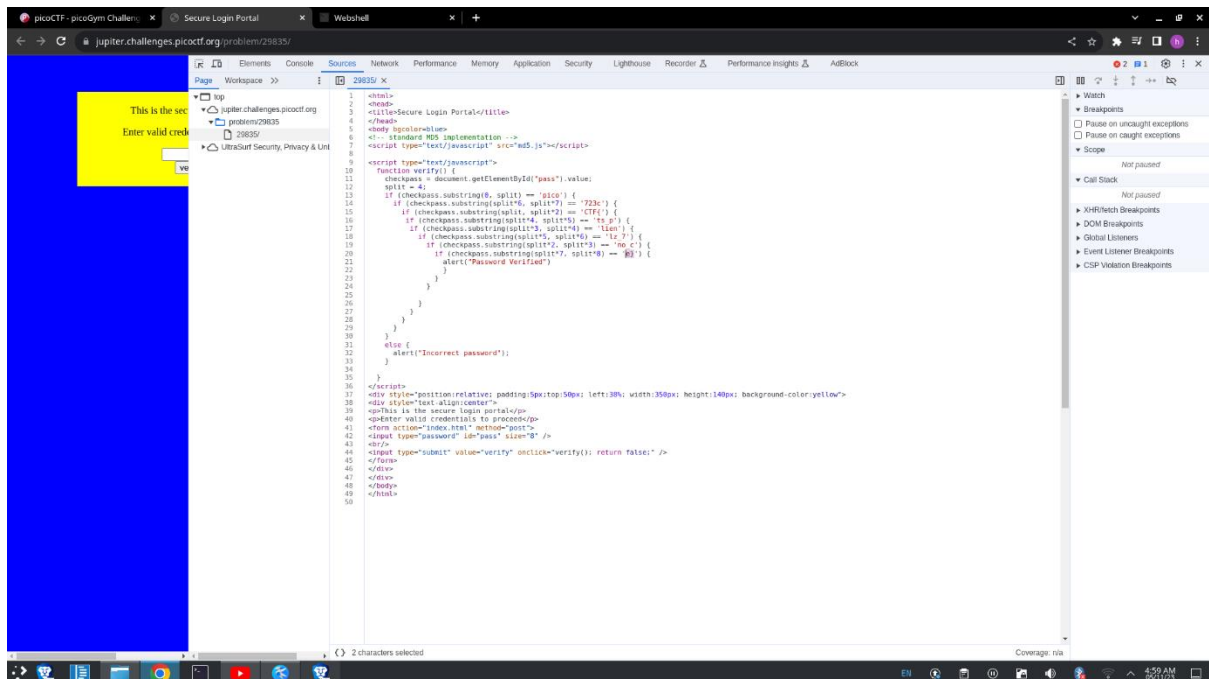




DONT-USE-CLIENT-SIDE CHALLENGE

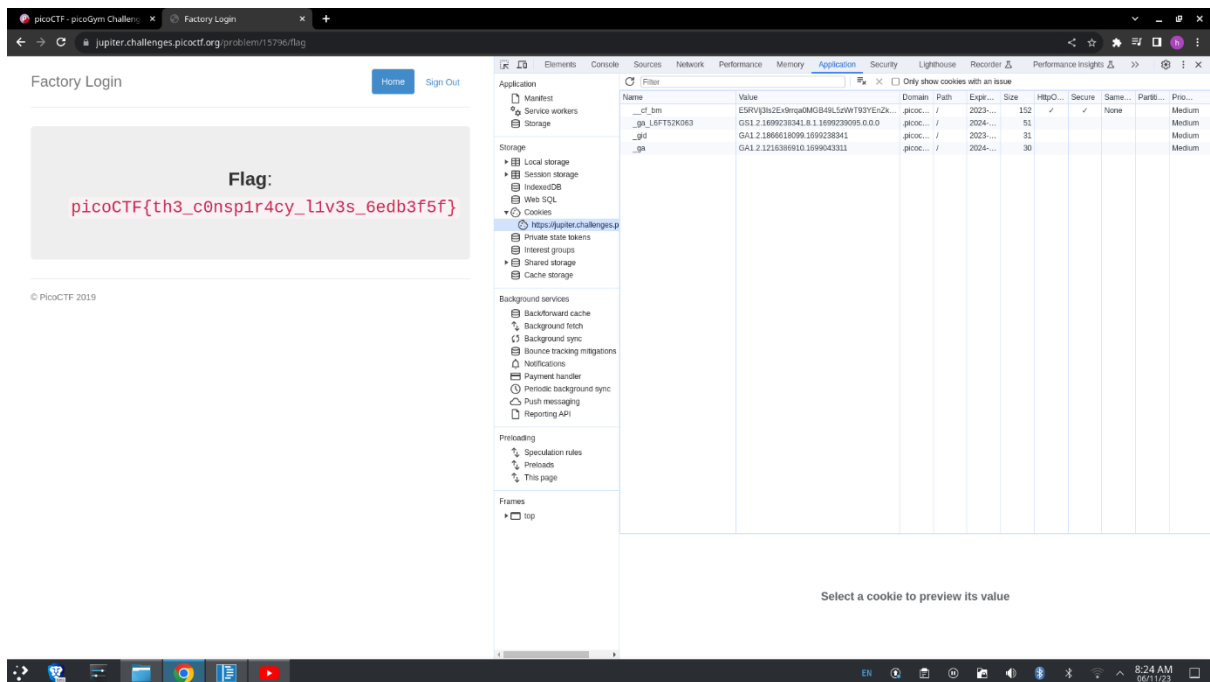
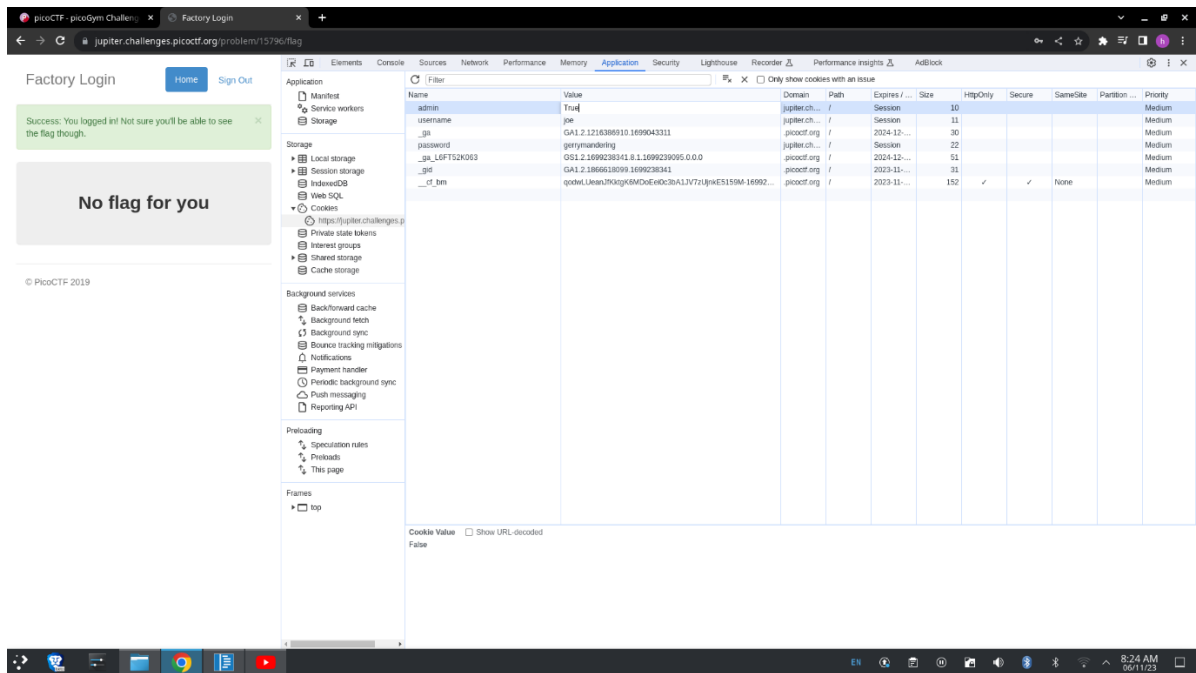
First I went to the inspect window and went to the page sources .
And in the JS part of the html file the flag was divided to parts and

was scrambled . The point of this challenge is that we shouldn't use verification or authentication on client side cause its not secure.



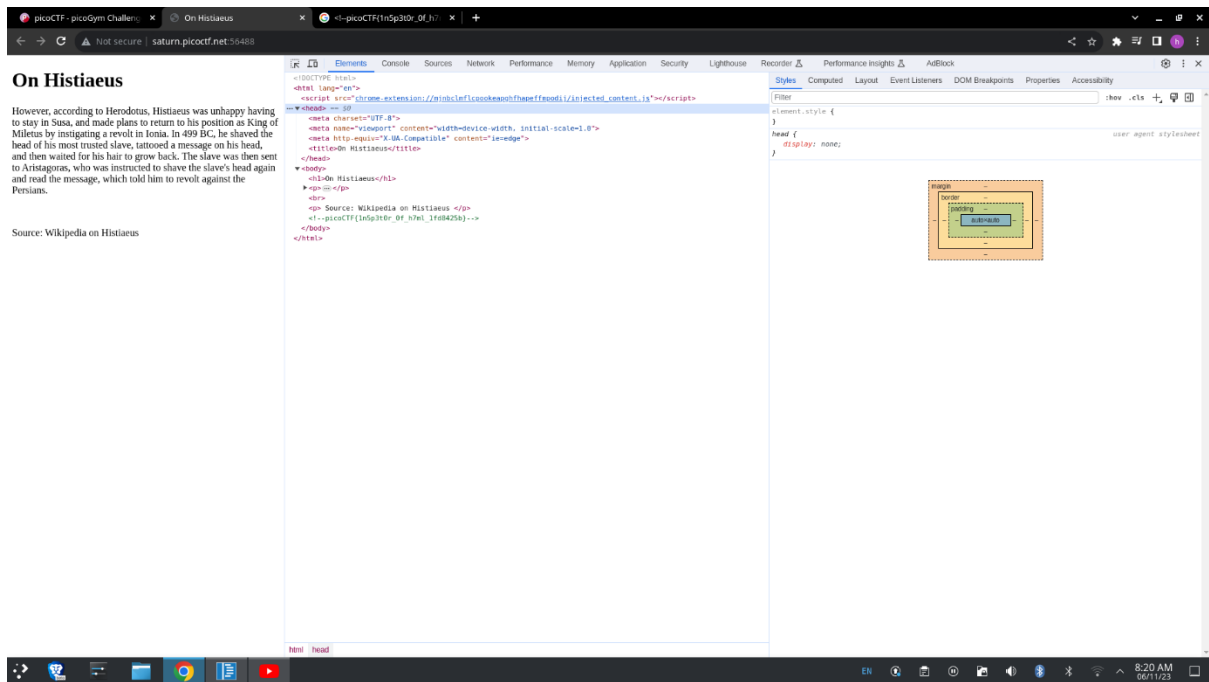
LOGON CHALLENGE

I logged in with the username joe and the site showed a message "no flag for you". I went to the inspect window and went to the cookies section in applications , and changed the value of admin to true from false and refreshed the page and got the flag.



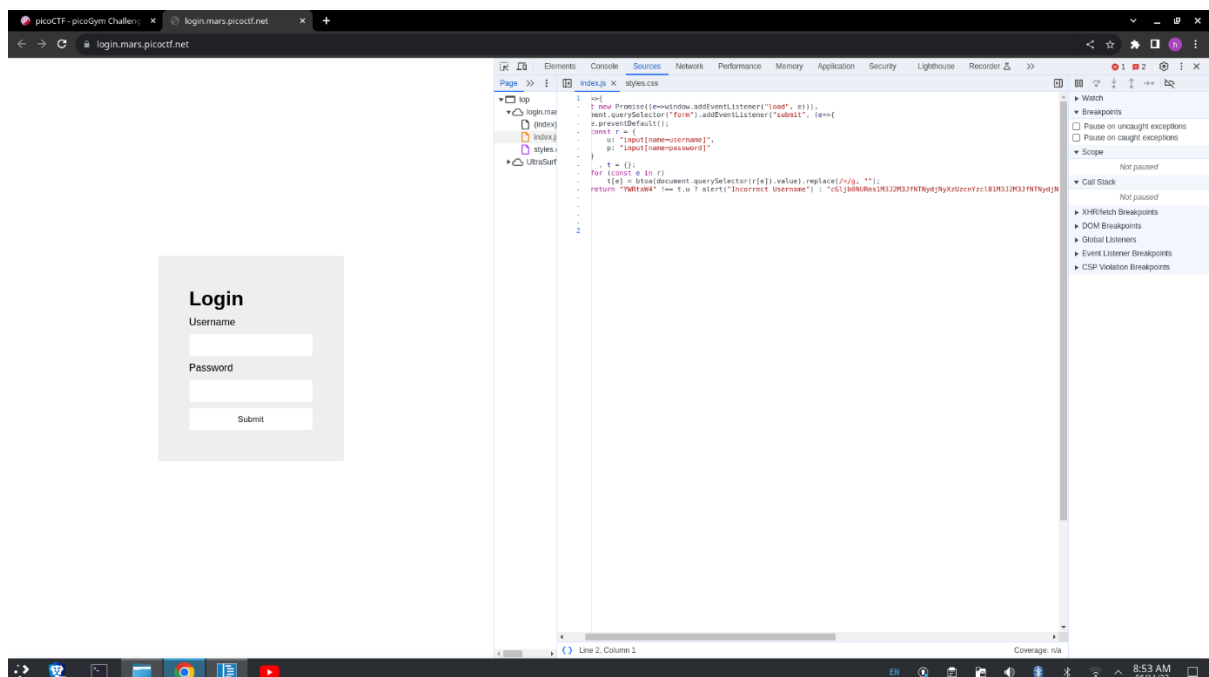
INSPECT HTML CHALLENGE

I literally just went to the HTML part of the inspect window and the flag was in the body part of the HTML.



LOGIN CHALLENGE

I went to the JS file in inspect. There was a function called btoa which converts a base 64 encoded string to a normal string. Base64 is a way to encode and decode strings. so I opened terminal and typed "echo 'cg1jb0nurns1m3j2m3jfntnydjnyxzuzcnyczl81m3j2m3jfntnydjnyfq' | base64 -d" and got the flag.



Basic data partition

```
(jaifin@batcomputer)-[~]  
$ sudo echo 'YWRtaW4' | base64 -d  
adminbase64: invalid input  
  
(jaifin@batcomputer)-[~]  
$ sudo echo 'cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ' | base64 -d  
picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}base64: invalid input  
  
(jaifin@batcomputer)-[~]  
$
```

PICO CTF FLAGS

1. insp3ct0r flag

picoCTF{tru3_d3t3ctlve_0r_ju5t_lucky?10be399}

2. don't-use-client-side flag

picoCTF{no_clients_plz_7723ce}

3. logon flag

picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}

4. inspect HTML flag

picoCTF{1n5p3t0r_of_h7ml_1fd8425b}

5. login flag

picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}

1. Why do you want to join the club?

I want to join the club because I want to learn hacking. I want to become a white hat hacker in my life, that's why I chose my CSE specialization in cybersecurity. I once saw one of my friends (who is already in bios) learning a lot of stuff (C language, JavaScript, web exploitation ...) and I too wanna learn all the things the bios club would teach me and ultimately become a white hat hacker.

2. Why didn't you play the recruitment CTF's?

At first when I came to this college I didn't have a laptop for myself. I brought my laptop during the Onam holidays and I couldn't get my hands on it till mid September (cause it was delivered to my house but after I returned to college after the Onam holidays). By then most of the participants had already attained a lot of points and I thought there is no point in starting then. I regret not even trying.

3. What skills do you have in cybersecurity?

I learned C++ language in 11th grade and 12th grade. I also know a bit of SQL as I learned MySQL in school. I also learned Python for college.

I have experience using Linux distros (Ubuntu and Kali). I know a bunch of terminal commands. Also I want to learn more things and acquire more skills. That's why I want to join bios.

4. Some information about yourself

I am Jaifin B Aloor. I come from Thrissur, Kerala. I am currently doing my engineering degree in Computer Science with specialization in Cybersecurity. I am 18 years old. My dad works in KSEB as an Assistant Engineer and my mother is a high school teacher. I want to

become an ethical hacker when I grow up. I wanted to be a hacker since I was young cause I watch a lot of movies and I was inspired by a bunch of movies such as hackers(1995) , black hat(2015) , the italian job(2003) , the fifth estate(2013) , the girl with the dragon tattoo(2009) among many others.