CTF Writeup-:

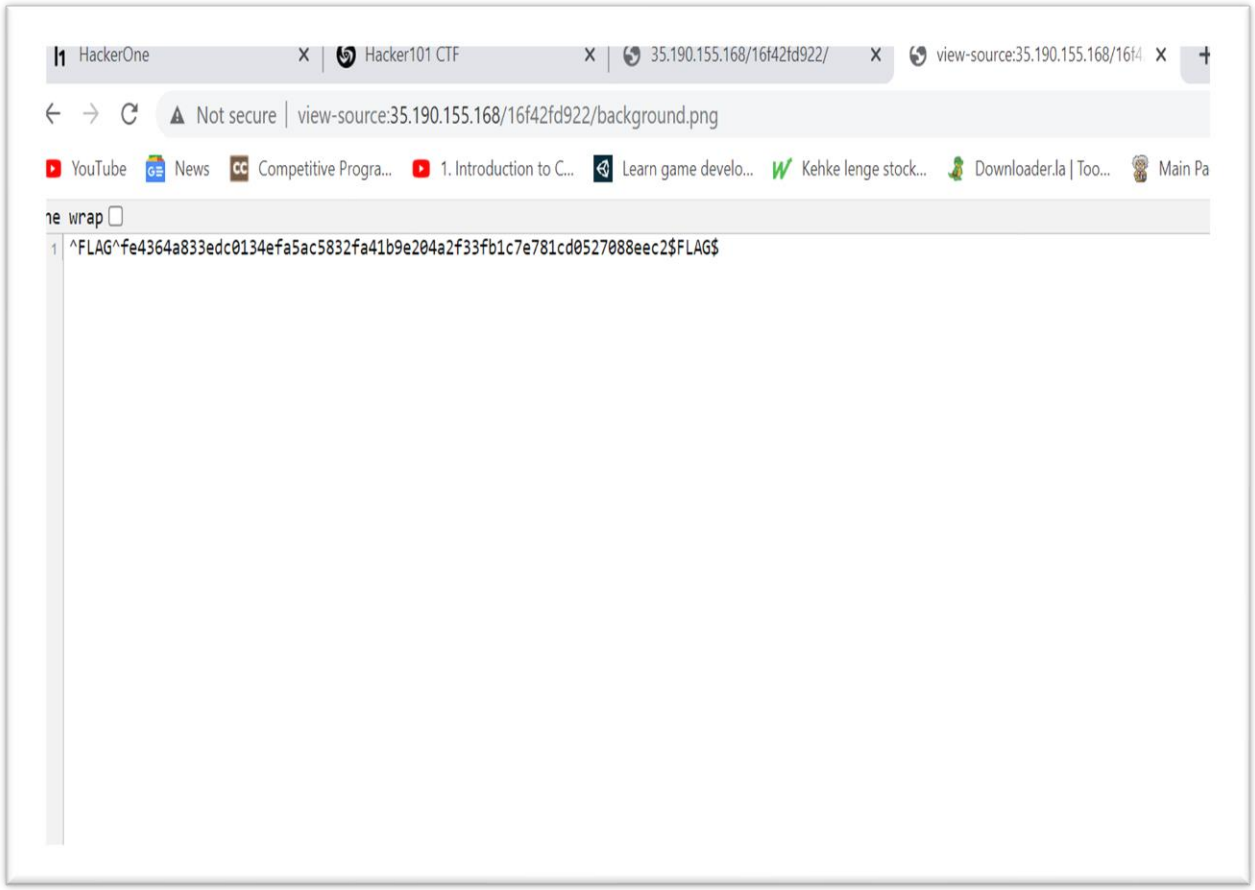
This report consists of three CTF challenges from Hackerone.

Challange1(A little something to get you started):

Flag1- It is first CTF challenged and I tried this without hints.

First, I went to source code section, there I saw one line of code i.e., 'background-image: url("background.png");'.

I thought for a while and then searched for it by adding in page URL. This gave me my first flag.



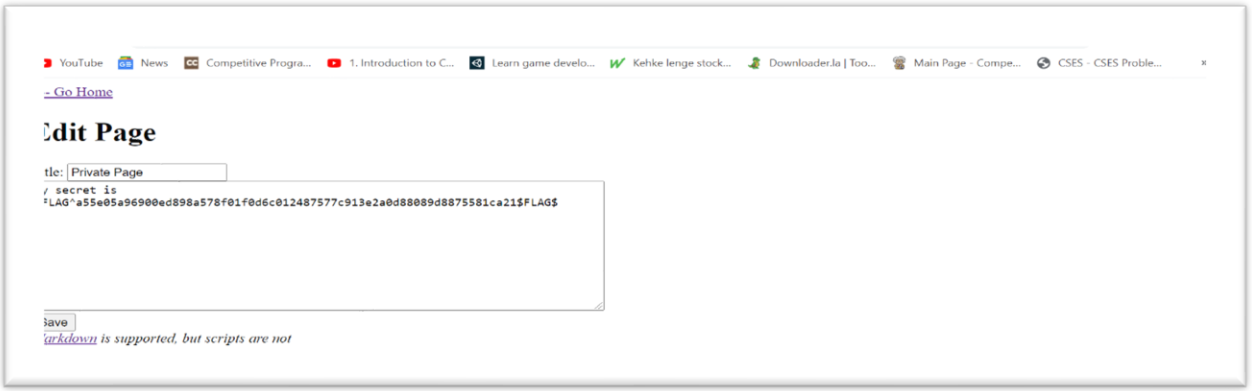
Challange2(Micro-CMS v1):

Flag1-firstly I visited all the three links given in the challenge.

Also had a quick look into their page source. Then I took hint,

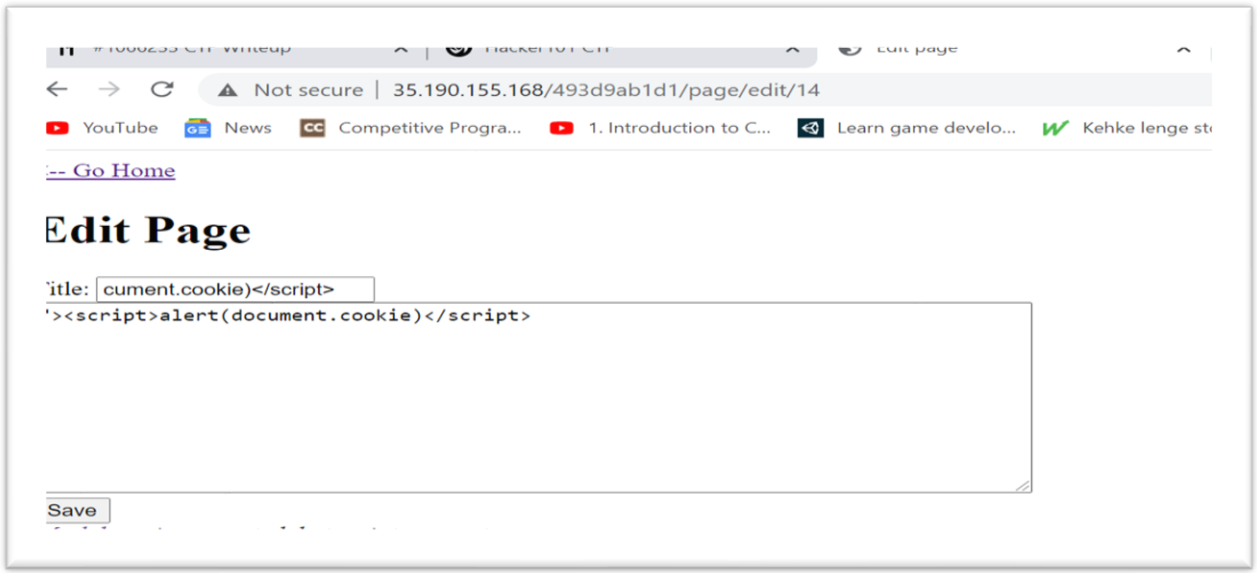
Which suggest me to create a new page, after creating I noticed that id of new page in URL is page/13.

Changing page numbers from URL, page/7 has different msg from other pages. Hints helped me to go to edit this page and in that when I searched for page/edit/7, I got my 1st flag.

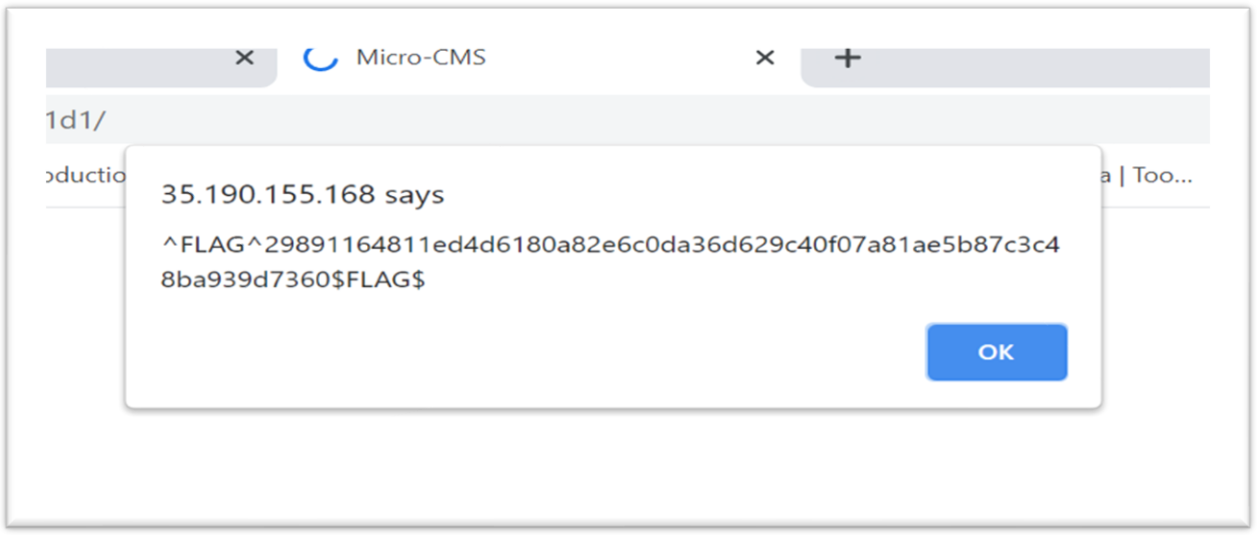


Flag2- Again I used hint for this one, it urged me to go to create page and enter some XSS payload.

Payload – “><script>slert(document.cookie)</script>

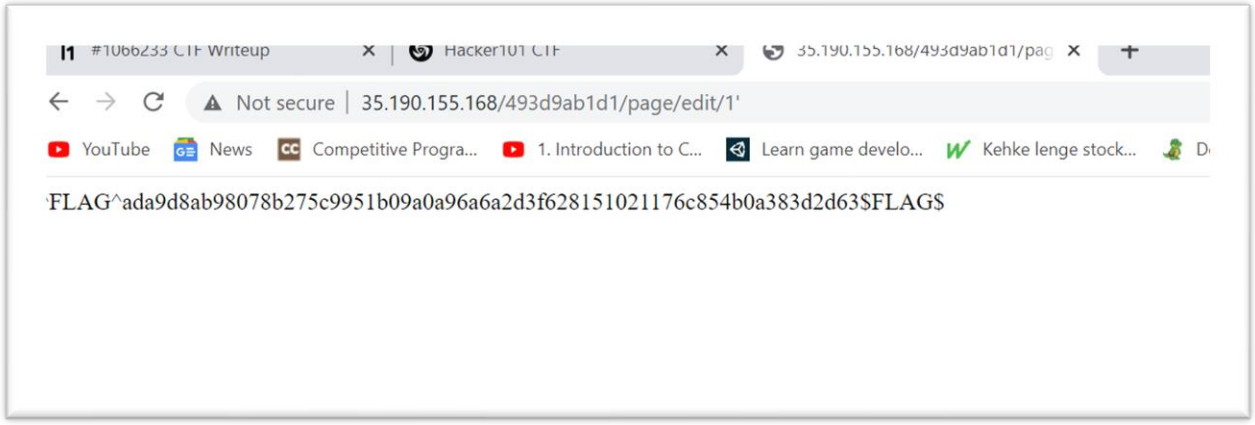


After saving when I clicked on ‘Go Home’ I got my second flag.



Flag3- In previous hint it was said to use both XSS and SQL tools, we already used XSS and got our second flag now lets try with SQL.

I modified URL by writing *page/1'*, but it didn't work. Then I tried same in page edit *page/edit/1'* and got my third flag.

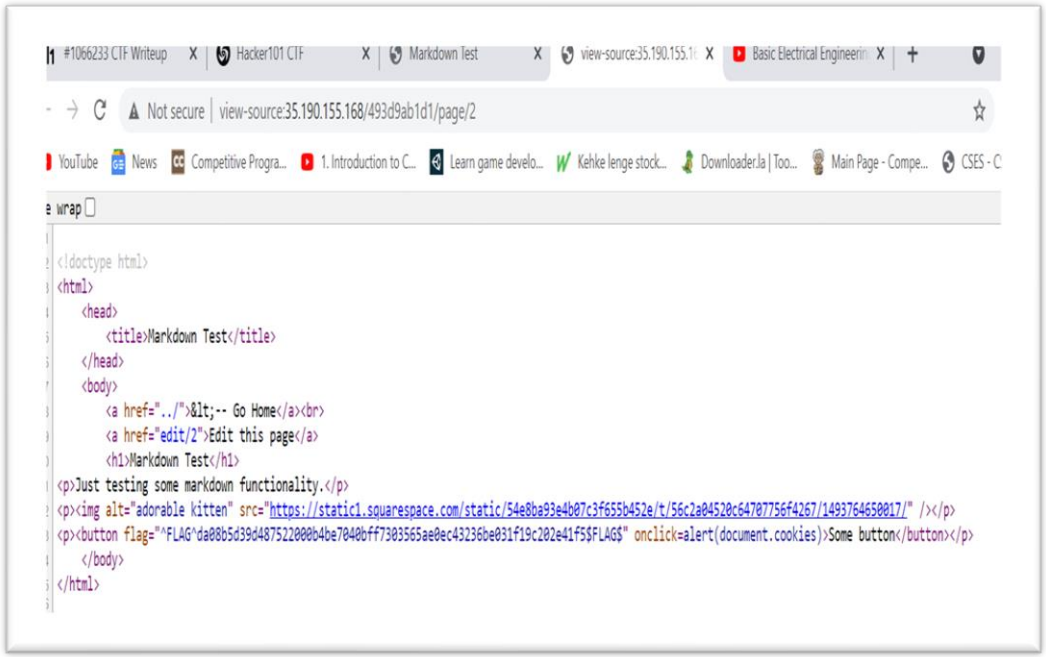


Flag4- In this hint says 'Script tags are great, but what other options do you have?'. So, we have to try something different that can do same as script.

Option we have is a button in Markdown edit page,

So again we used payload, 'onclick=alert(document.cookies)'

After this when we go to page source, we get our fourth flag.



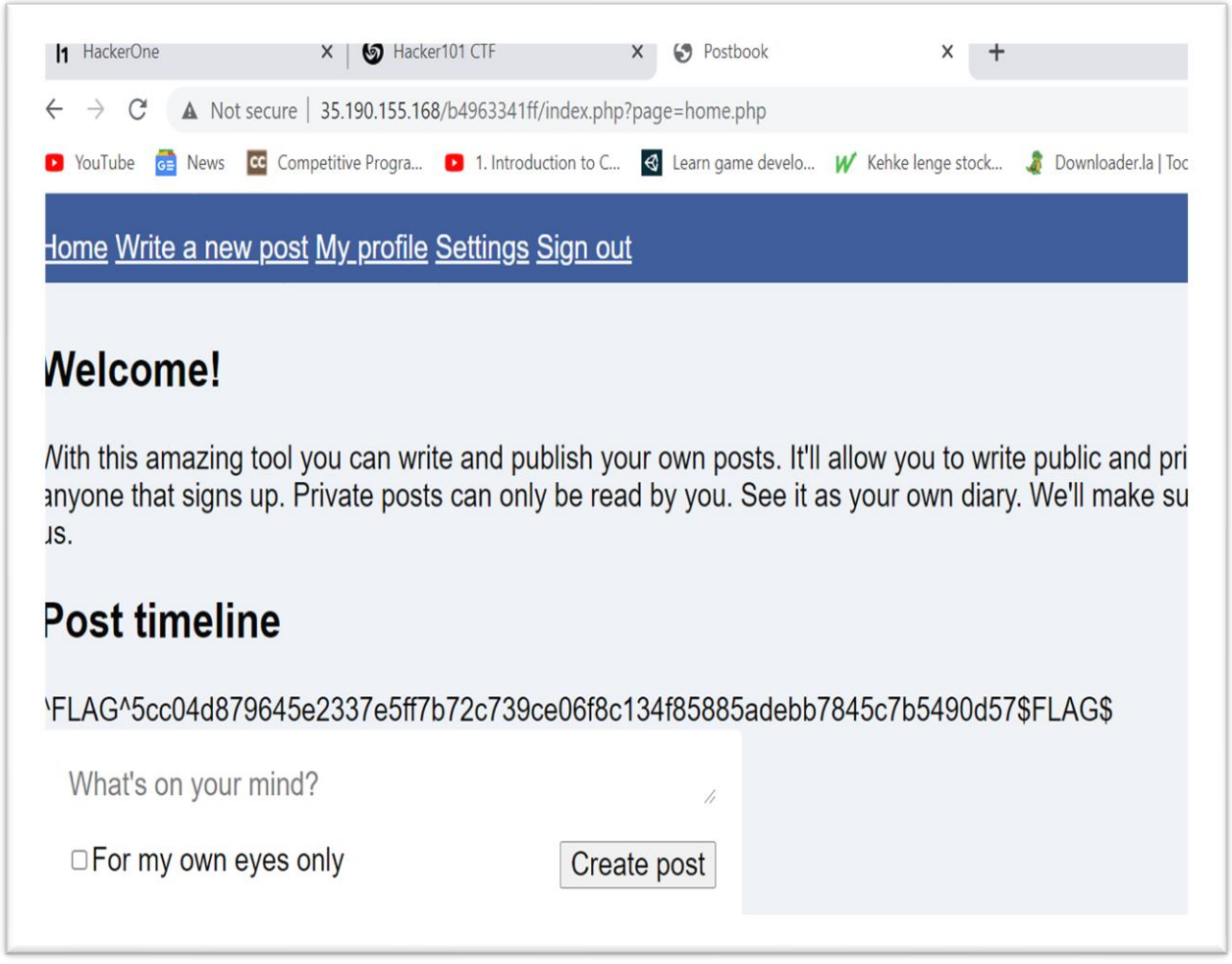
Challange3(Postbook):

Flag1- For this challenge I have taken hints, and after reading very first hint I got in my mind that I have to go for brute force method.

Some of very easy id password can be

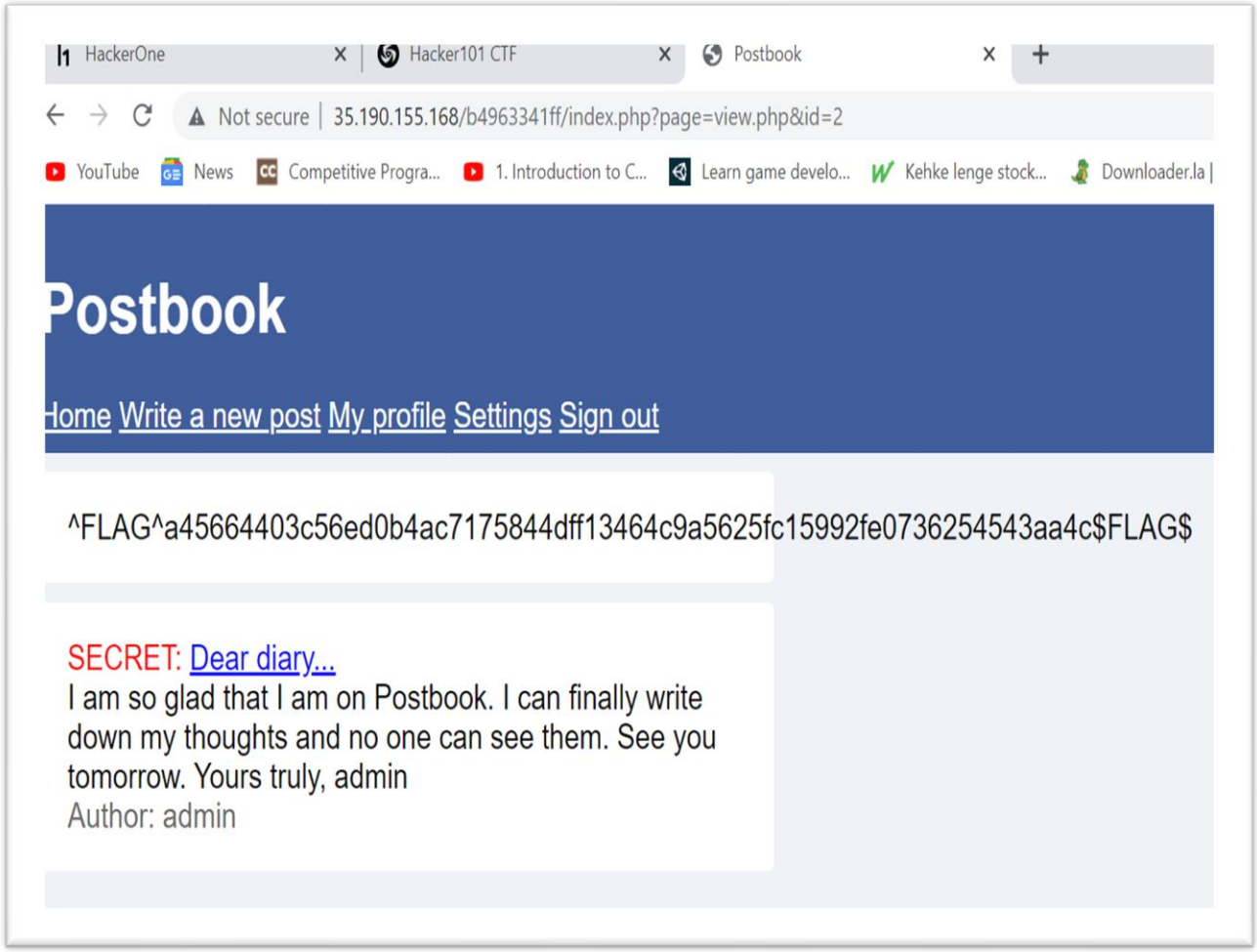
- abab 1234
- user user
- user password
- user pass
- admin admin

trying all this user password worked for me and I got my first flag.

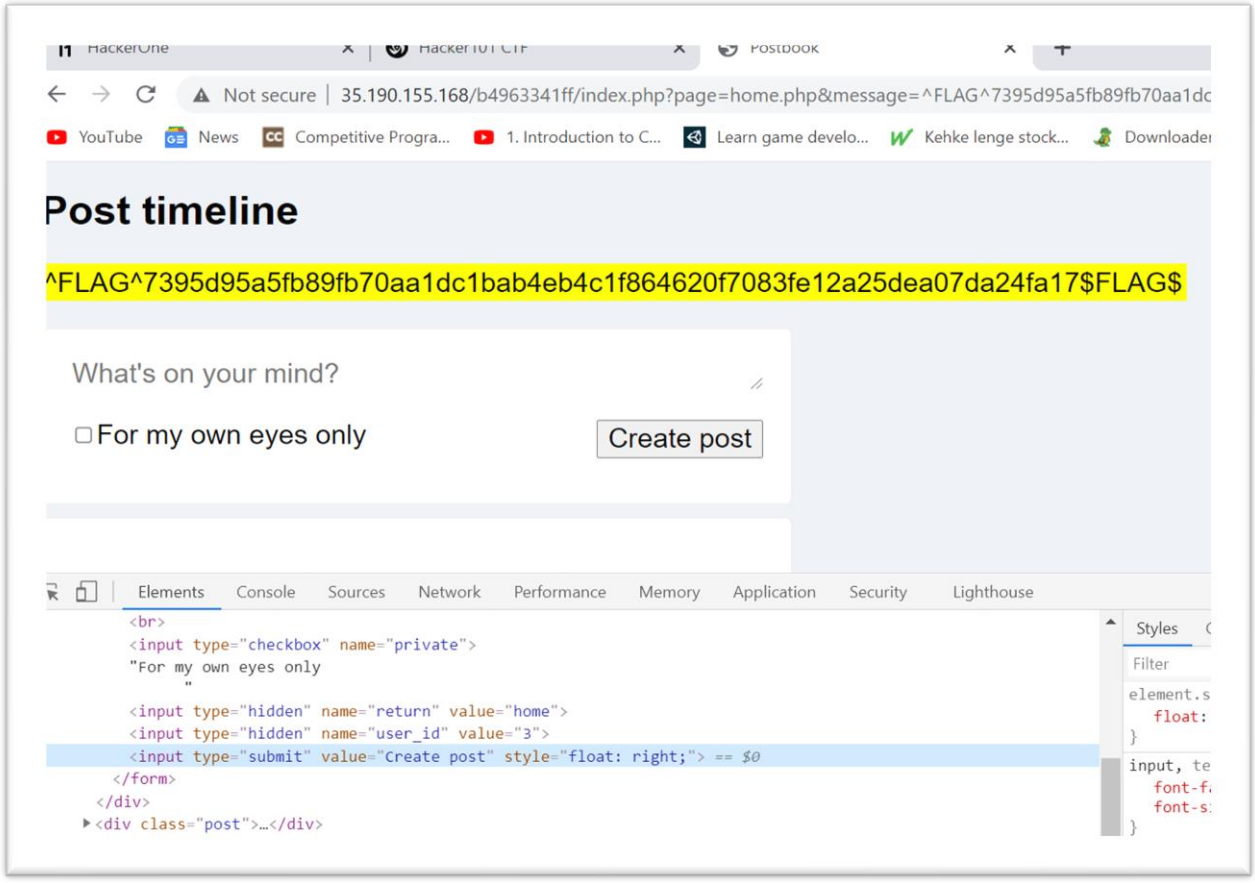


Flag2- Hint says I have to view my own post and change id, that's what I have done. Firstly I clicked the Hello everyone!

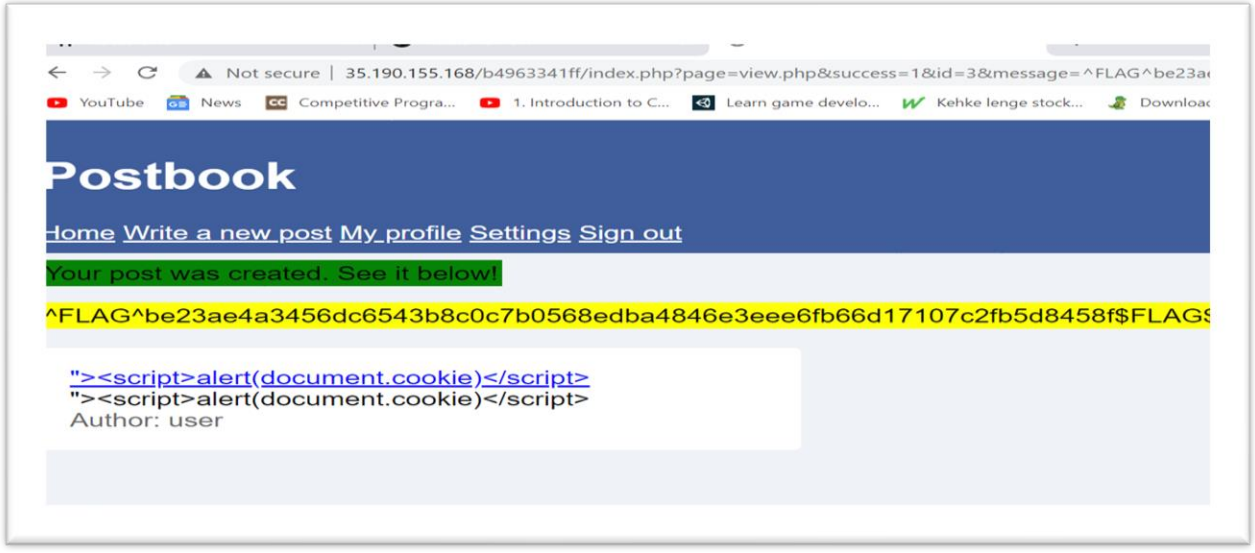
and tried to change id, than I tried same with Hello world msg after changing 2 3 values I got a secret msg of admin and my 2nd flag with it.



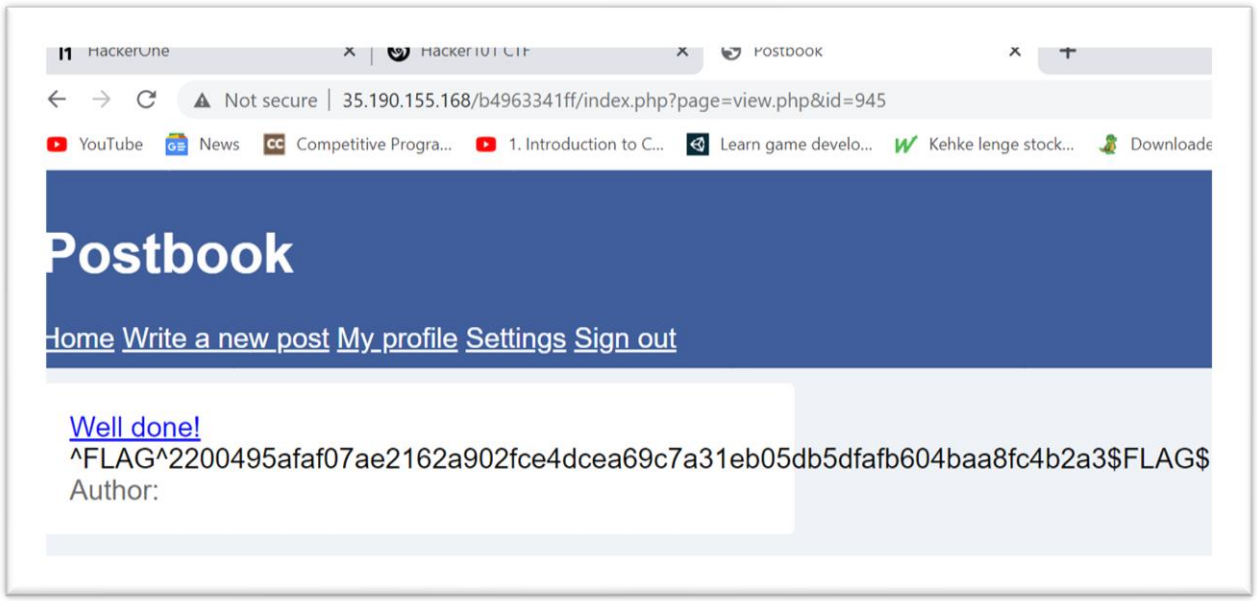
Flag3- Third hint suggest that I have to look at inspection page of my own posts. So first I created a post. Than going to inspection part I have changed some values and obtain my third flag.



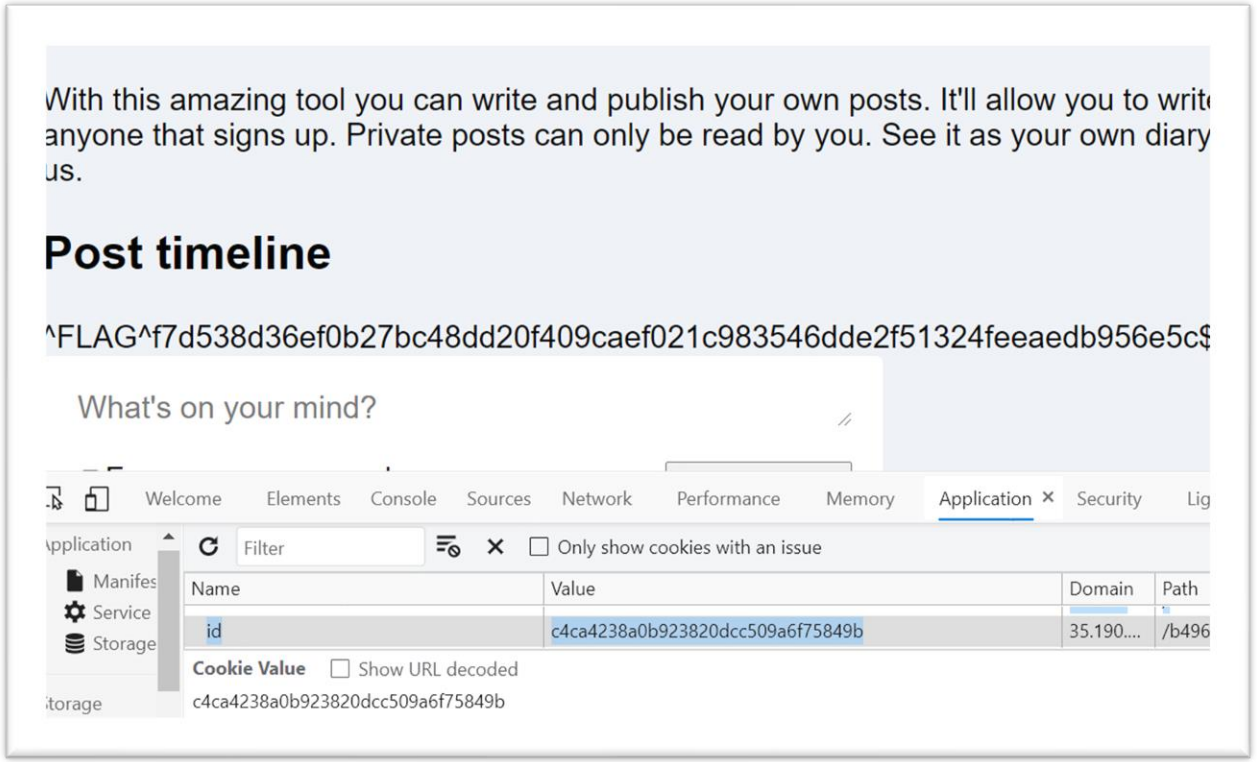
Flag4- From hint for this flag I have foccused more on editing post part, I have written payload to give edit option with post and than traversed to different page from url writing this same payload in admins public post I got my fourth flag.



Flag5- In this hint says 185*9 i.e., 945 so I changed page id to 945 and got my fifth flag.



Flag6- In hints it says about cookies, when I looked at cookies for this page going to storage section, there were different values in value coloumn. I changed that and refreshed that gave me my sixth flag.



Flag7- Hint seven says about deleting post, while doing that when I looked in page source code I searched for all ids of different page and changed their values also when I put code of 1 in page 5 index id and than refresh by putting all this in url I got my last flag of this challange.