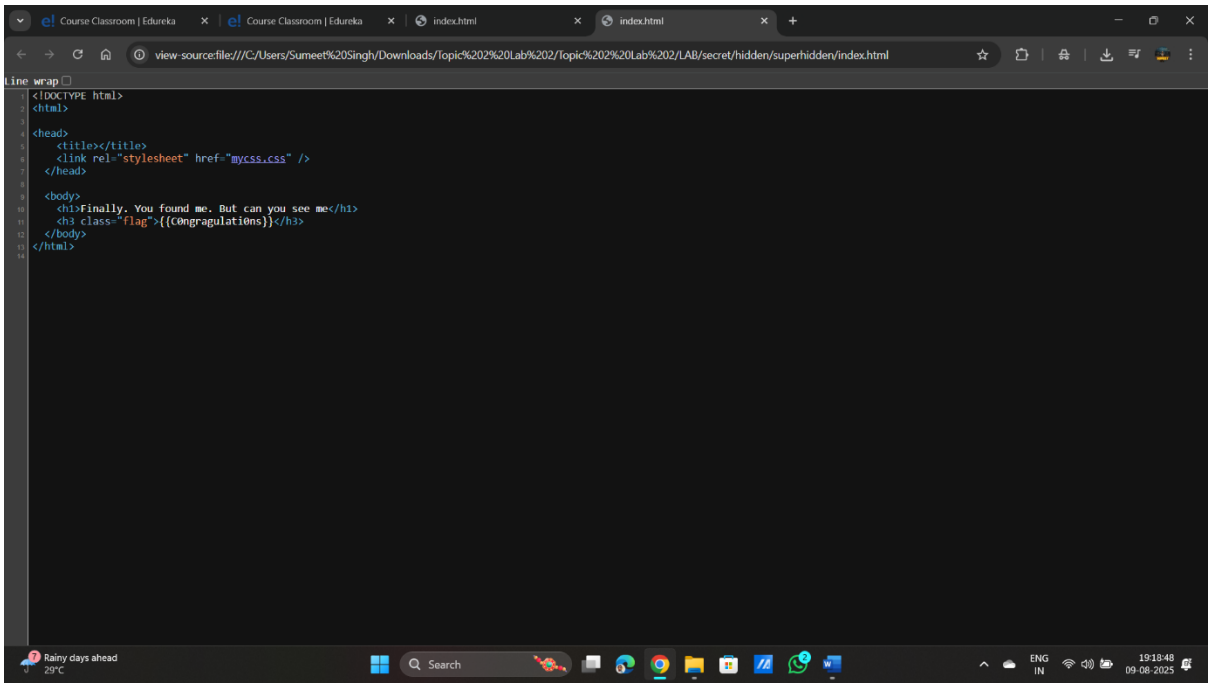
Lab 1

In this project we have to find out the vulnerability in the giving file after extracting we will get two folder that is “Topic 2 Lab 2” and another is “ctf” folder.

So in LAB 1 we have to work in “Topic 2 Lab 2” folder to check the vulnerability in the HTML files that are been given and in that we have check each and every file folder so that we can find the vulnerability and we have to check the only “**Chrome HTML Document**” and in that we have to see the code of that file by clicking “**ctrl + U**” that is we have to see the “ **View source page**” of that “**Chrome HTML Document**” or we can also do that after opening the “**Chrome HTML Document**” we can do that by clicking the left click on the page and from there we can see the option of “**View source page**” on opening that we can see the HTML codes of that document. By checking all this file, we have found that one of the HTML files have the something hidden in that file and by looking that we have found that there is some vulnerability present in that file code.

Here is the file path and the file screenshot that show the flag and the vulnerability in “**Chrome HTML Document**” file.

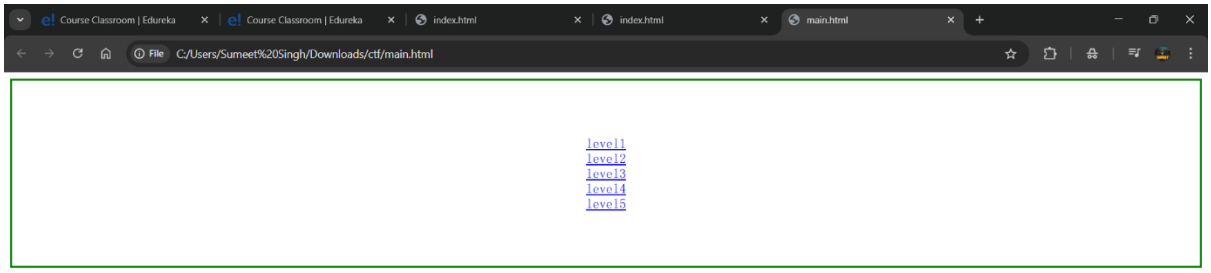
C:\Users\Downloads\Topic 2 Lab 2\Topic 2 Lab 2\LAB\secret\hidden\superhidden\index



Lab 2

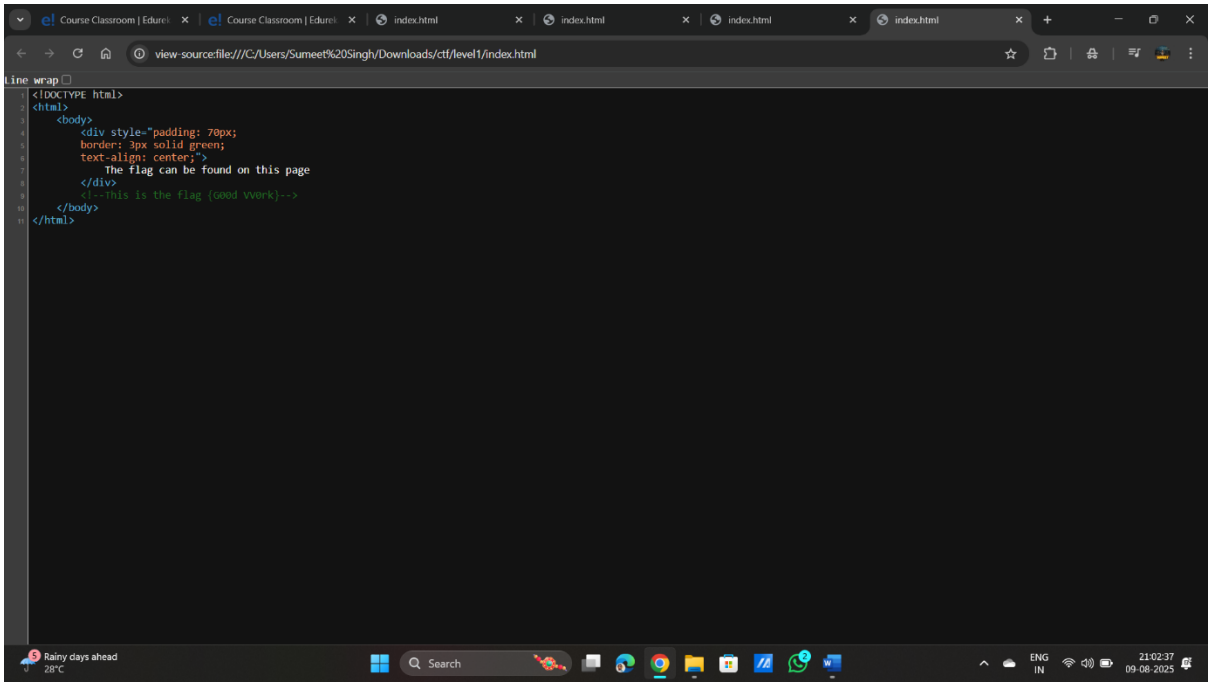
Now in Lab 2 we have to work on the “**ctf**” folder that we have extracted from the given file and that file we have seen that there are many files and folders are been presented and there is one “main” file is been present and that file is “**Chrome HTML Document**” file

C:\Users\Downloads\ctf\main

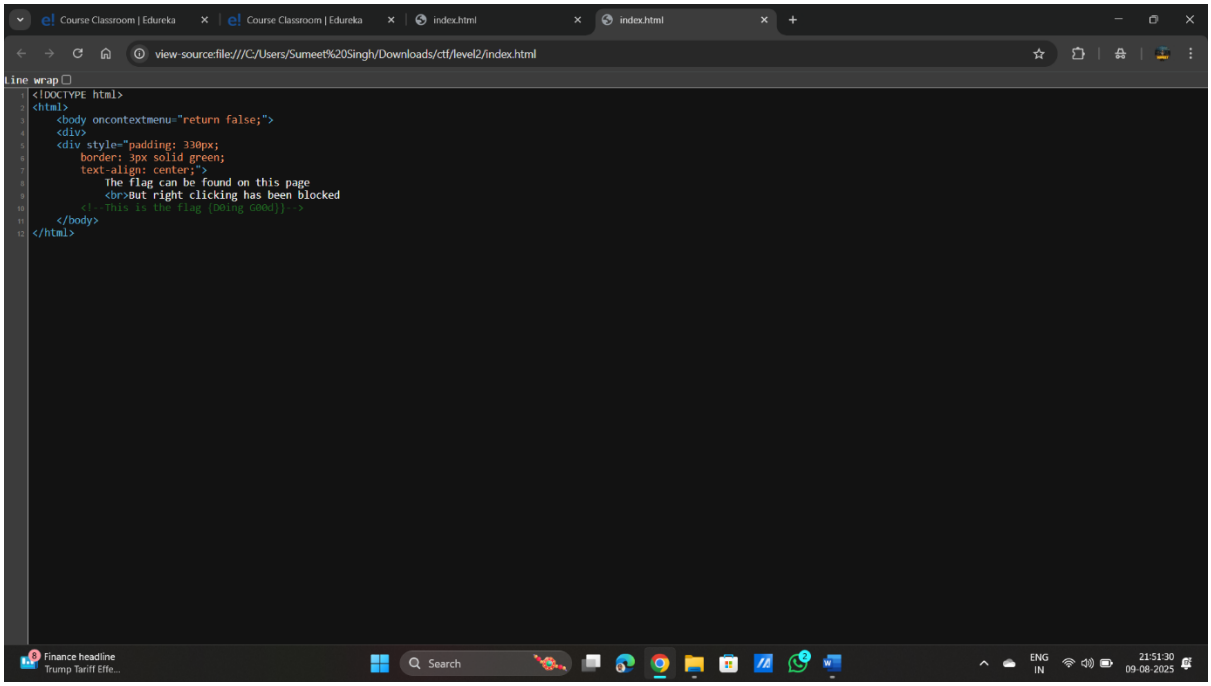


After opening the “**main**” file we can see that we found the different levels here. So, what we are going to do that we will check each and every level form **level 1 to level 5** and see the any vulnerability are present or not. To check the vulnerability simple what we are going to that we will open the level 1 hyperlink and check the source code of that webpage and find the any vulnerability is present or not.

After opening the **level 1** hyperlink we simply click “**ctrl + U**” to see the source code of that webpage. After seeing the source code of level 1 hyperlink we have found some vulnerability in the form of comment.



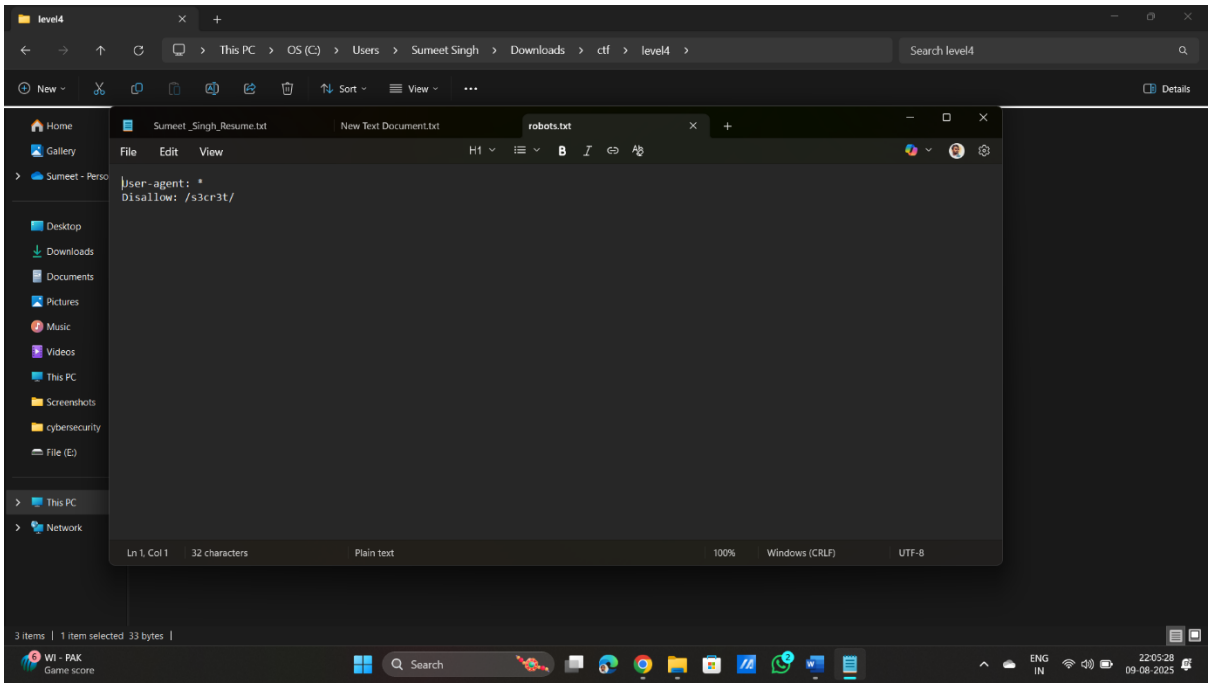
Now again we will be going to check the **level 2** and see the source code and find out the any vulnerability is present or not. After checking the **level 2** we find that there are some vulnerabilities that are presented in the form of comment in the **level 2** hyperlink



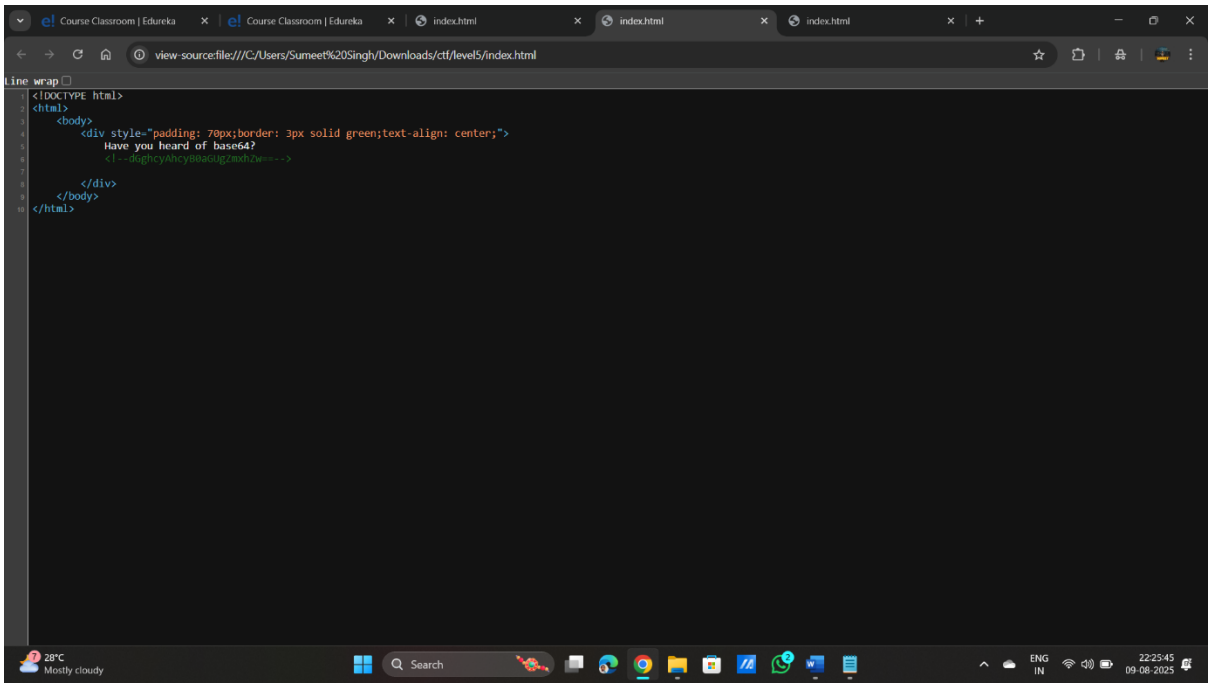
Now again we will be going to check the **level 3** and see the source code of that level and see that any vulnerability is presented or not. While checking the vulnerability we see that there is no vulnerability are present in the **level 3** source code.

Now again we will be going to check the **level 4** and see the same thing source code and check the vulnerability in that **level 4**. While opening the **level 4** hyperlink the new webpage is open and on there, we see that a message has been delivered that "**Ask robot for the help**" now we

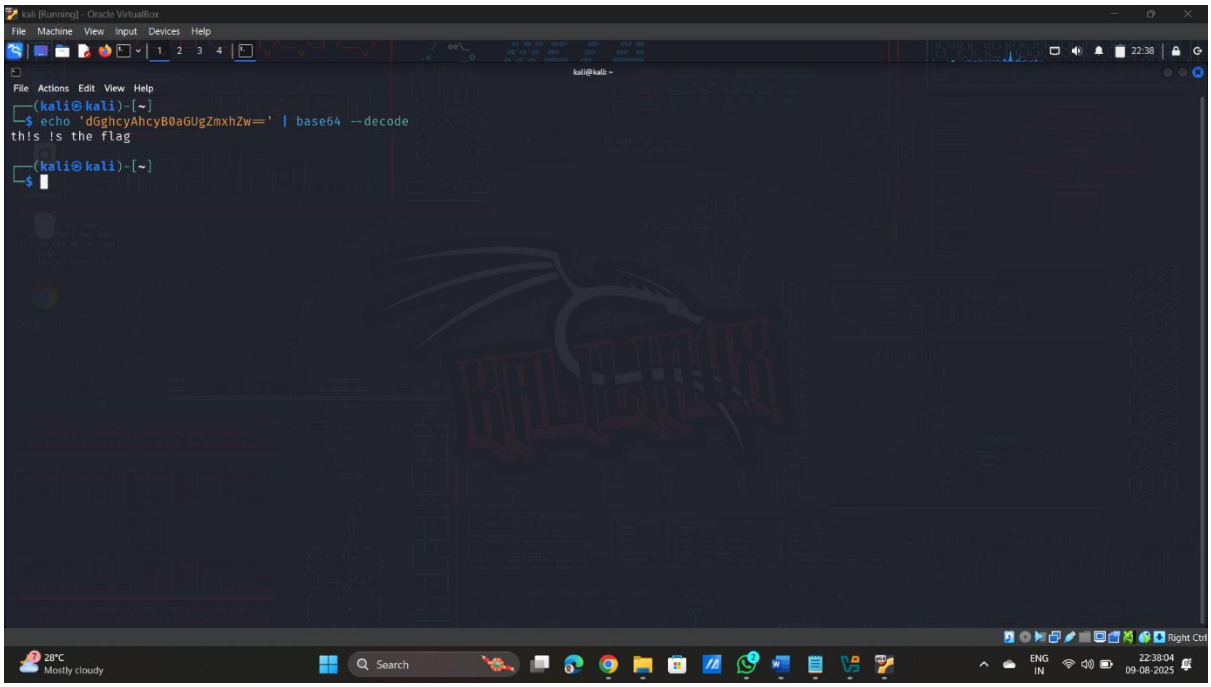
will check reset of the folders that are presented in the “**ctf**” folder to and find out the “**robot.txt**” file and see the vulnerability on that file.



Now again we will be going to check the last hyperlink that are has been presented in the “**main**” HTLM Document that is **level 5** hyperlink after opening the hyperlink we have found something like this mention in that webpage “**Have you heard of base64?**” after viewing the source code we found this in that source code.



There is comment in this source code about the base64 now what we are going to do that we will de-encrypt this code in the Kali Linux and de-encrypt this code by using the echo code.



Here we can see that we have decode the given code and we have found the vulnerability and flag in the level 5.