# ASSIGNMENT-2

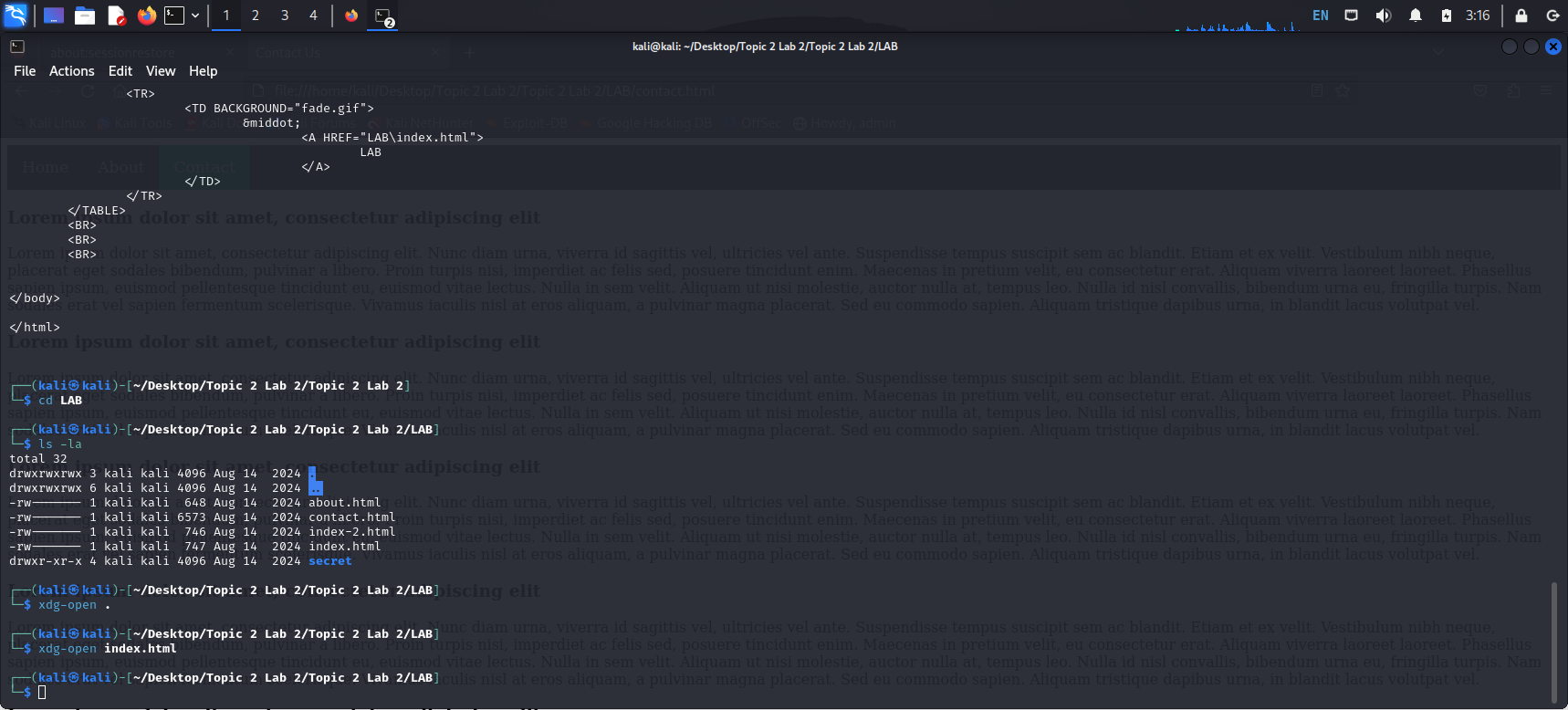
## Web Application Source Code Vulnerability Analysis

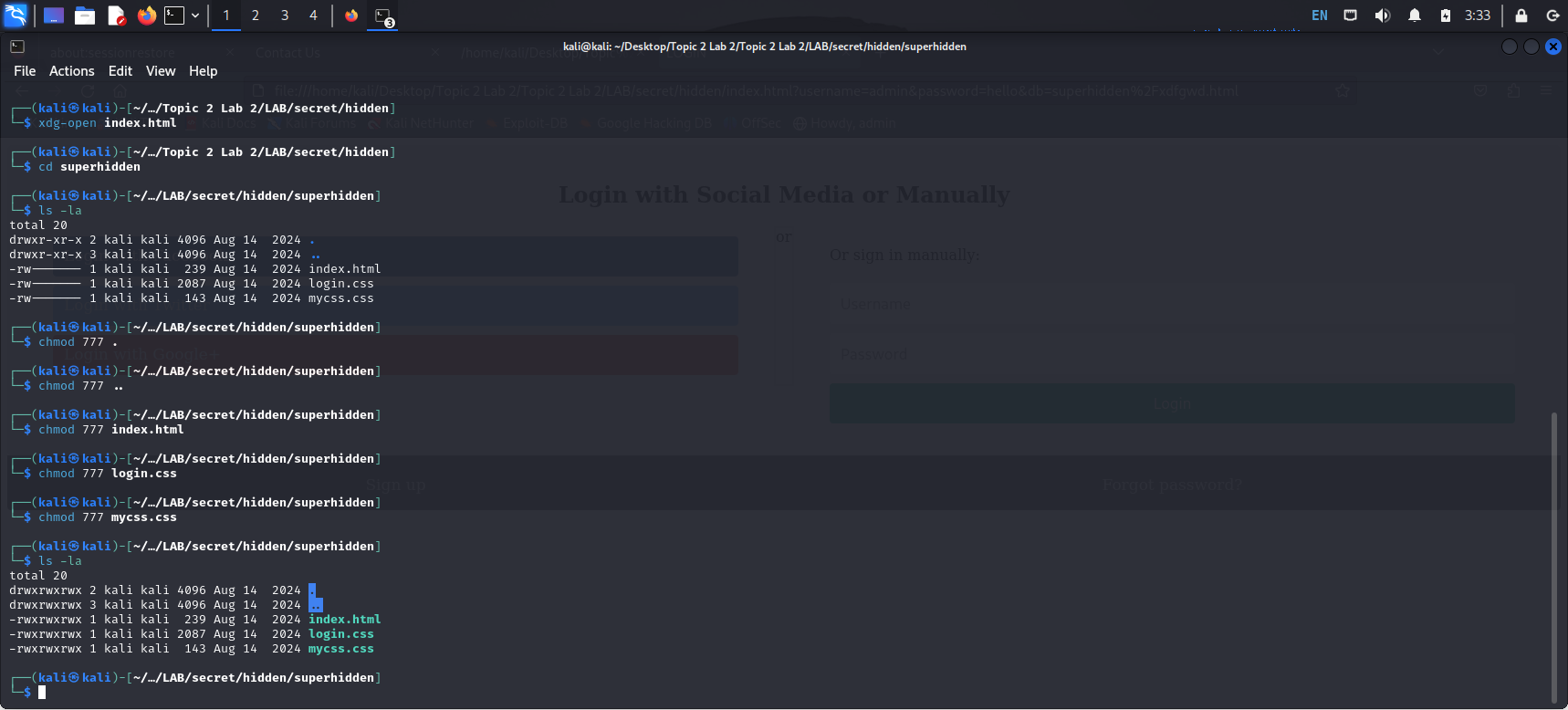
To complete the task we need to follow few steps:

1.Download the folder ie\_cseh\_additional\_files\_v1\_szv\_9smpy02 into your c drive.

2. Upload it to the kali linux machine the folder is present in the desktop .

3. Now we open the folder we can find Topic 2 lab 2 folder we can find many other files and folders, change all the permissions of the folders as well as files

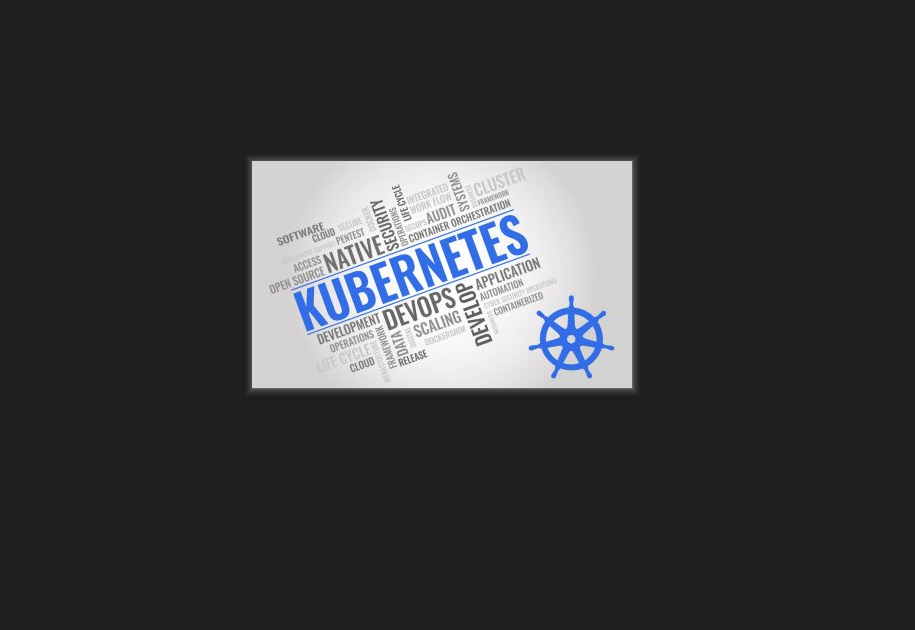


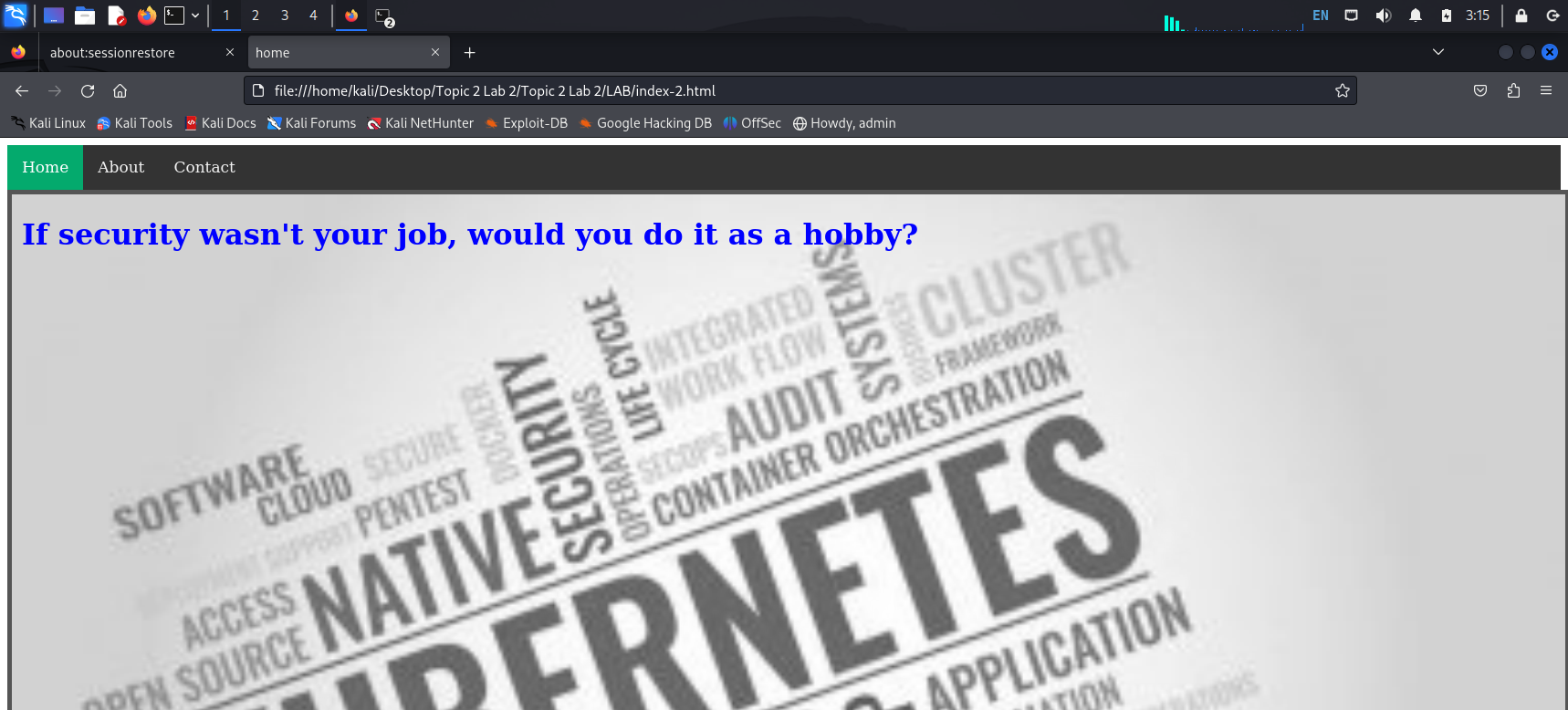


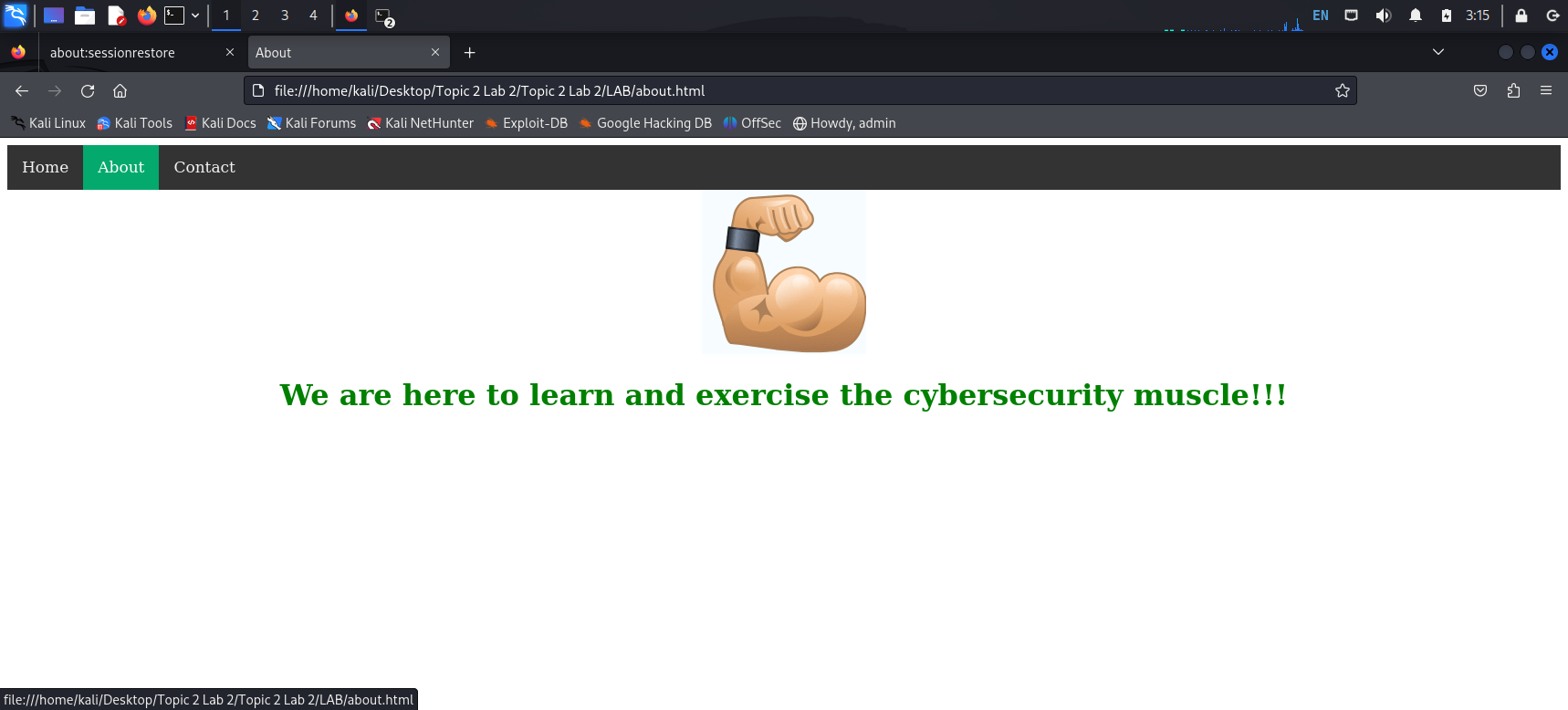
4. using chmod 777 index.html.

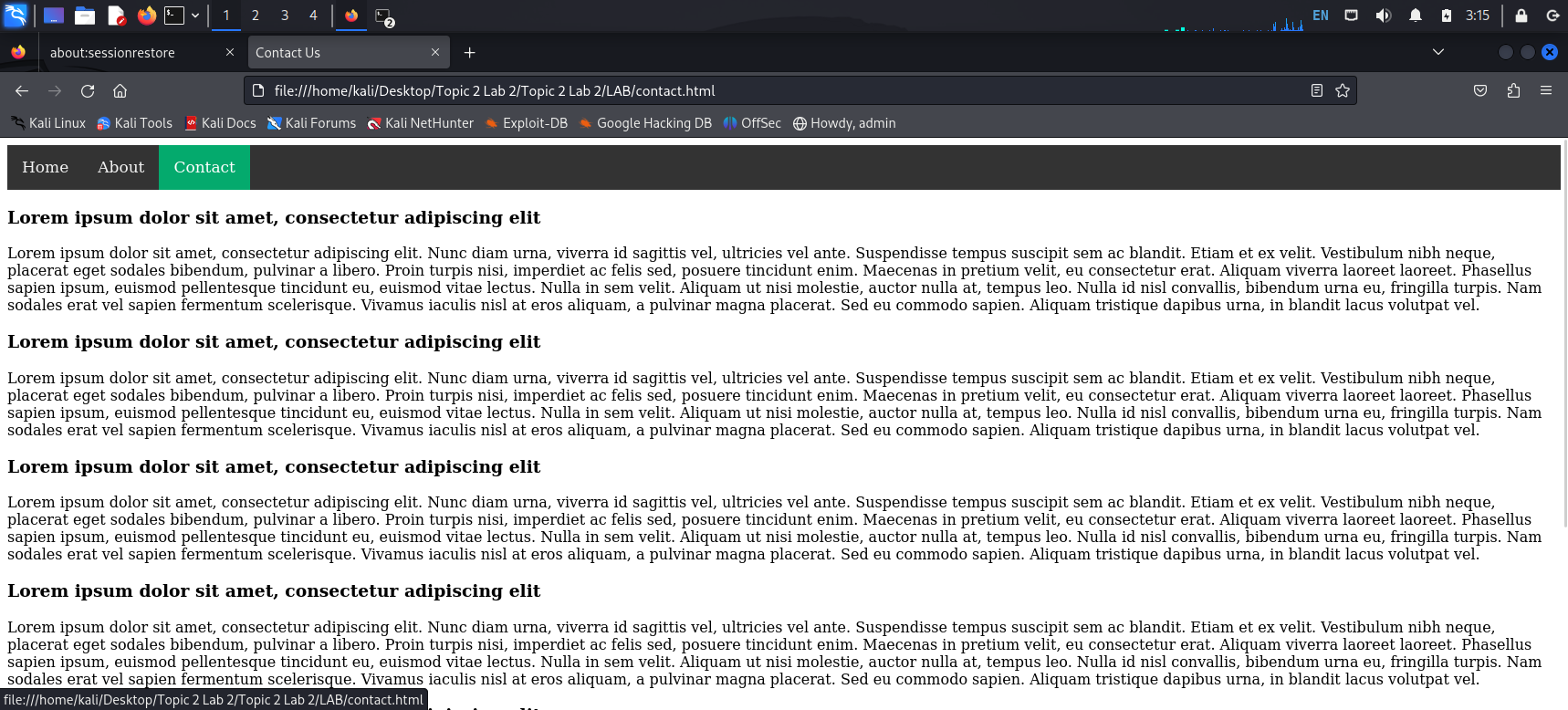
5.we can change all the files permissions using above command.

6. when we open this index.html files we can find home page .



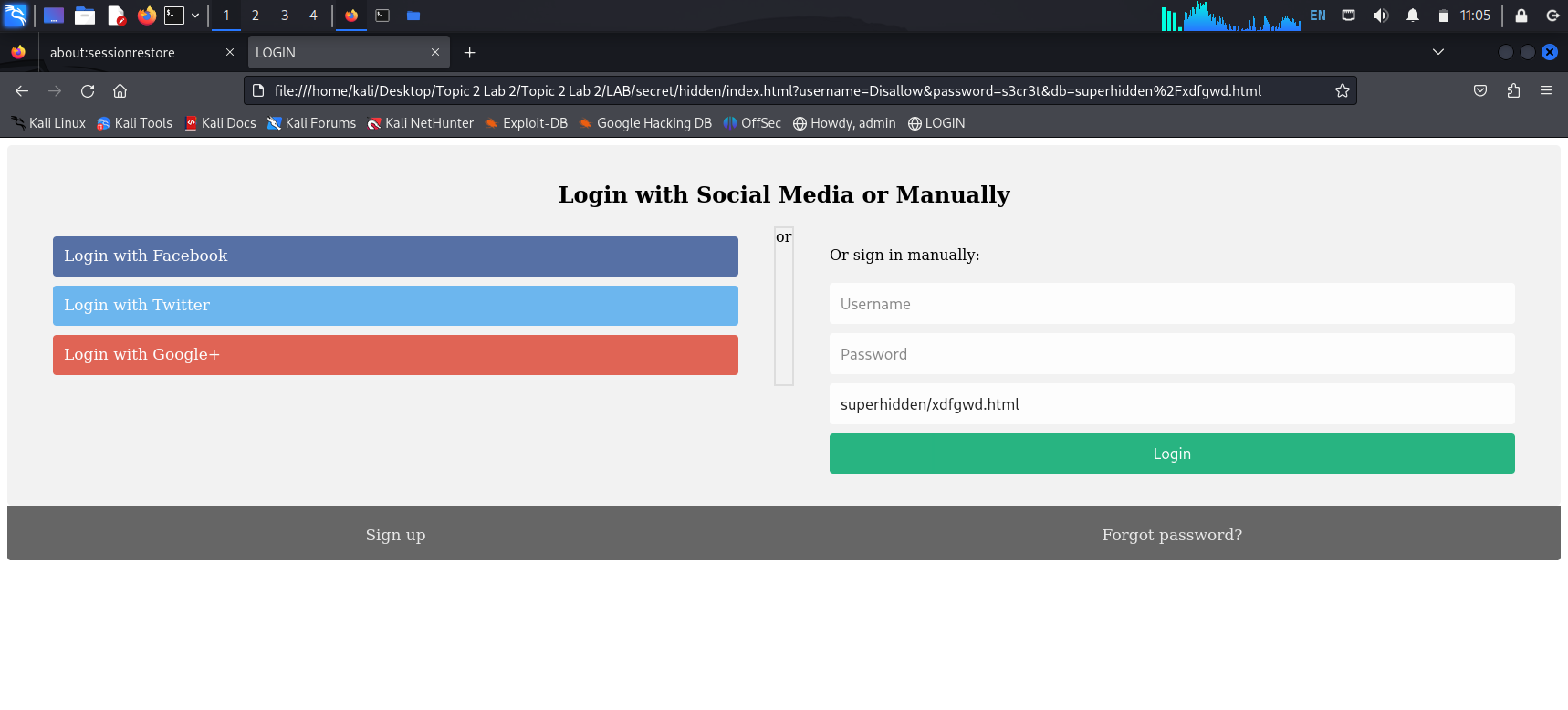




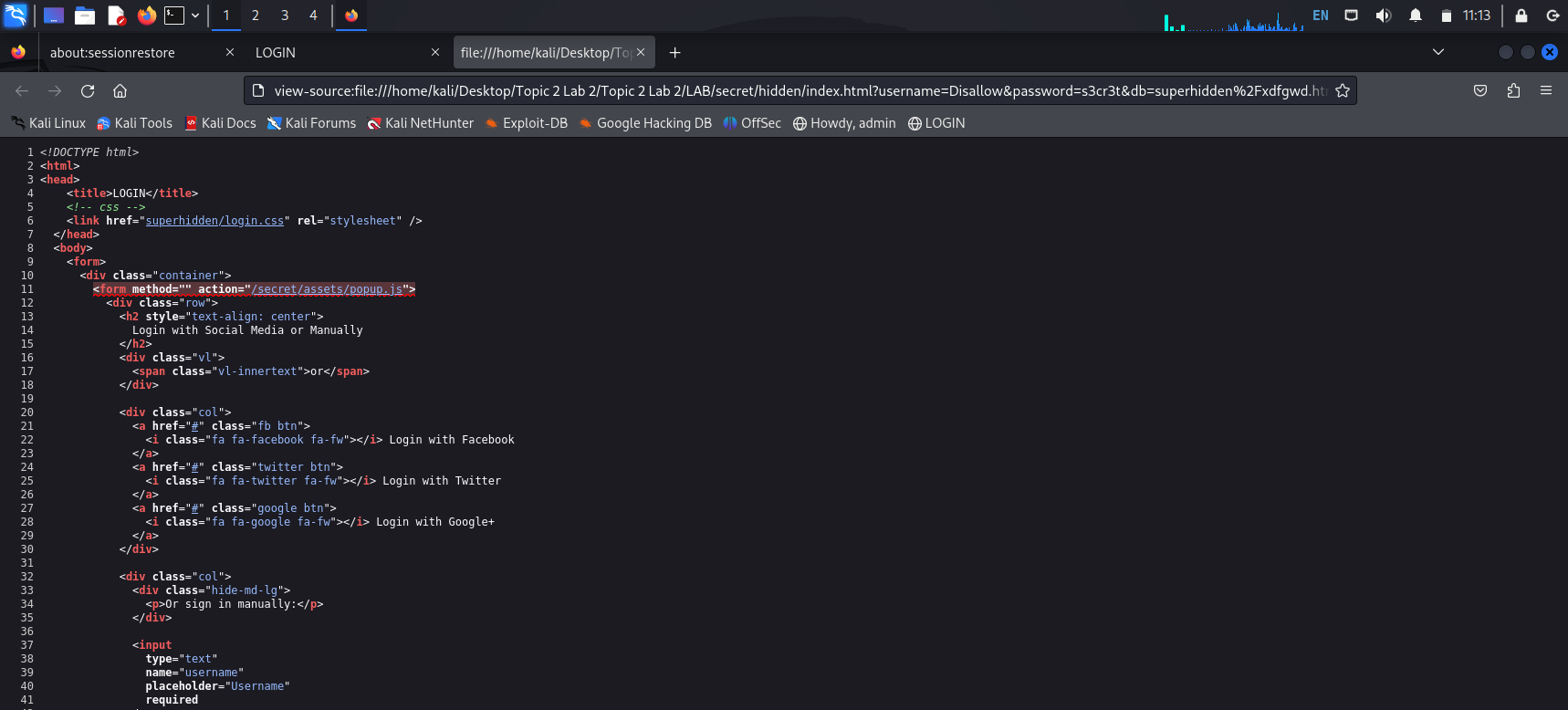


7.in topic 2 lab 2 folder we have another folder lab and finally we get a login page which is fake

Just to shift our focus on that.

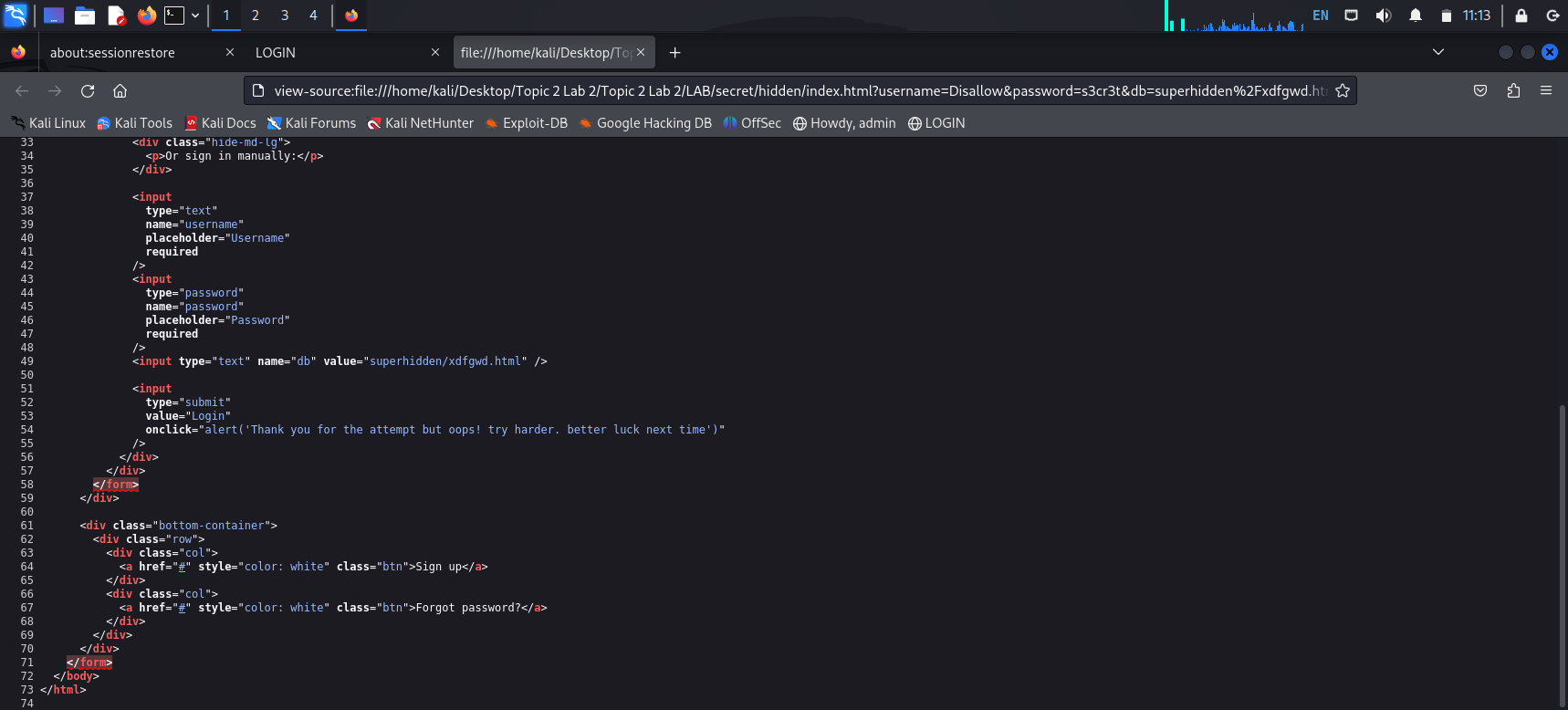


8.there are links which are misleading us from the goal we can view it from the source code page for this we need to press ctrl +u or right click.



9.secret/assets/popup.js is a misleading link and we have supperhidden/xdfgwd.html

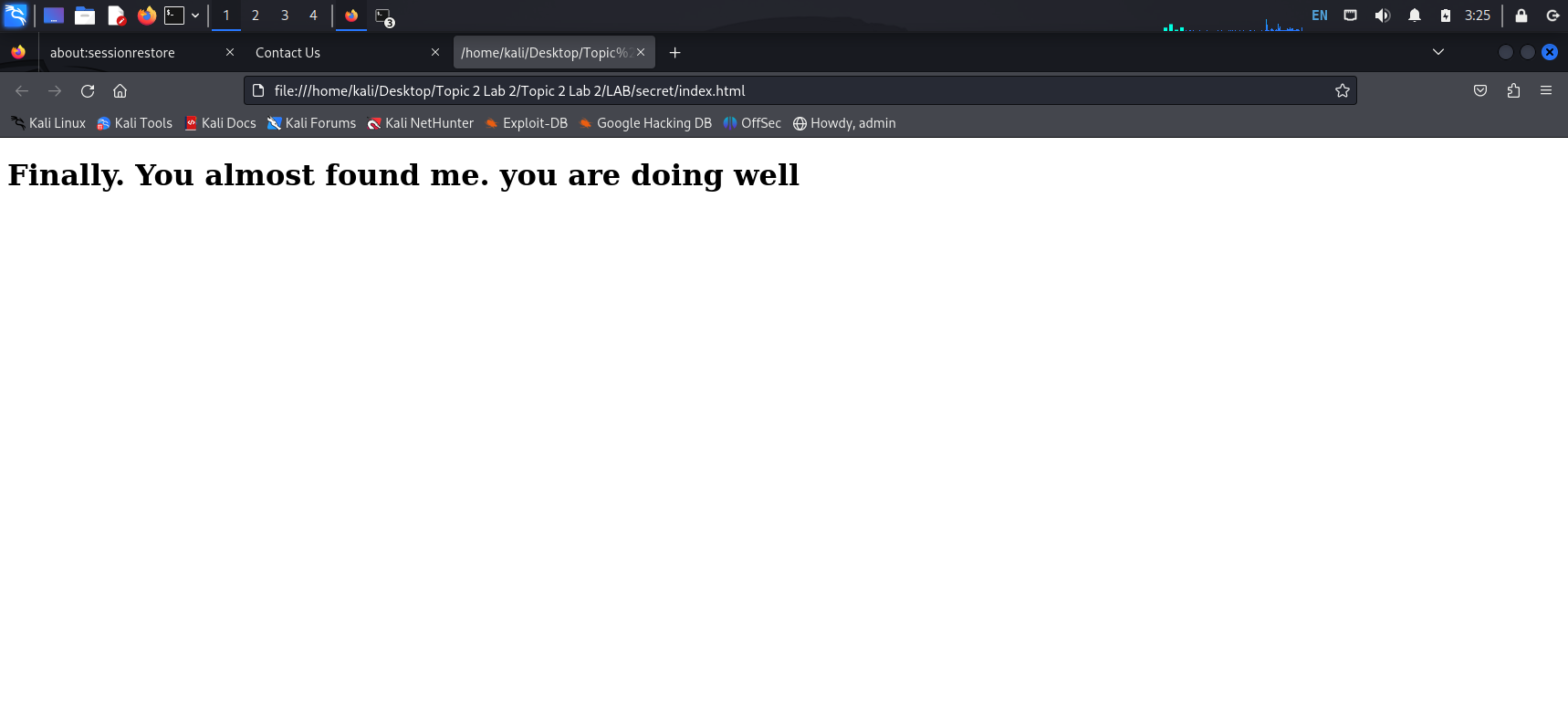
Which is of no use.



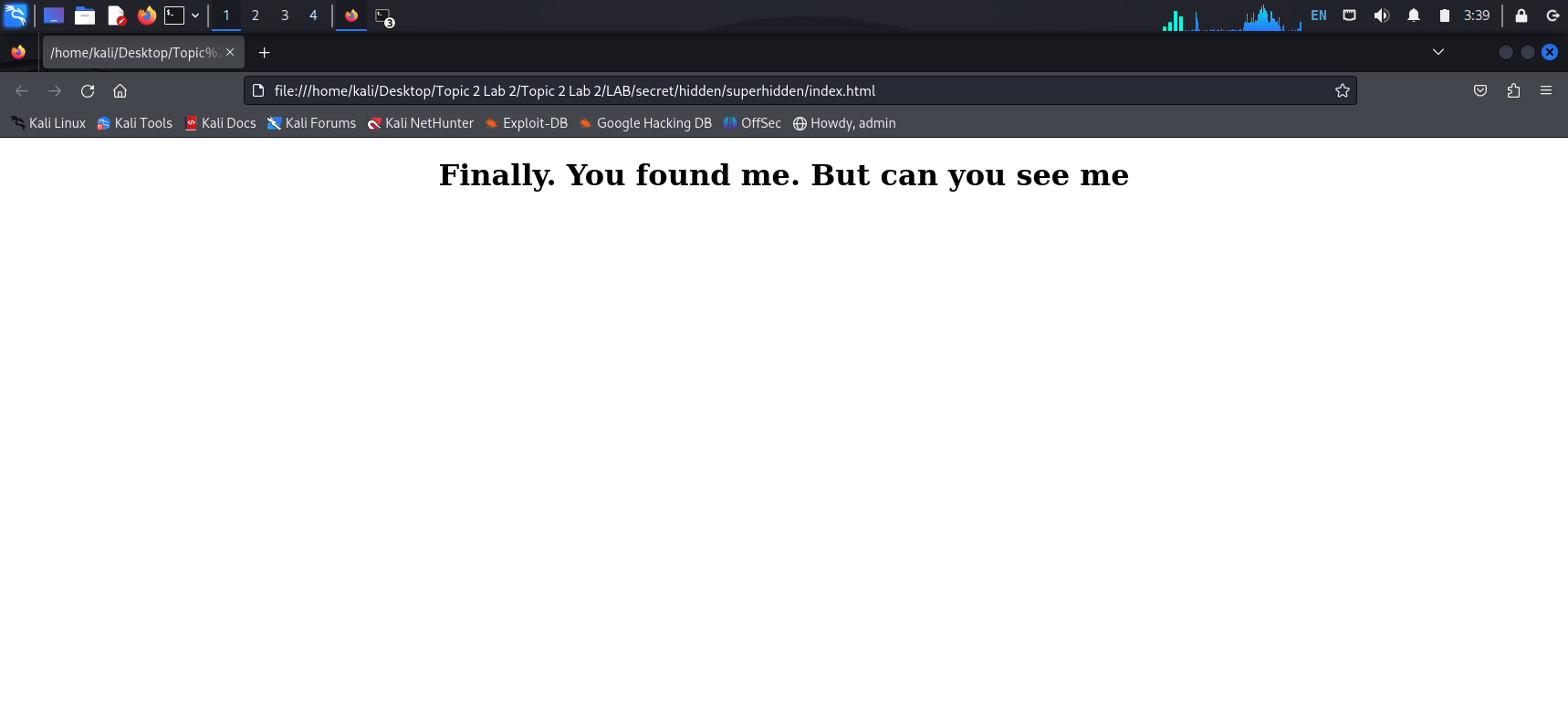
10. Desktop/Topic%202%20Lab%202/Topic%202%20Lab%202/LAB/secret/index.html

We have found a clue here so we can move to the next step.

11. [file:///home/kali/Desktop/Topic%202%20Lab%202/Topic%202%20Lab%202/LAB/secret/hidden/superhidden/index.html](https://d.docs.live.net/home/kali/Desktop/Topic%202%20Lab%202/Topic%202%20Lab%202/LAB/secret/hidden/superhidden/index.html).



12.We can use this command xdg-open index.html to open any file and when we open it we could see this message below in the screenshot so we need to change the code.

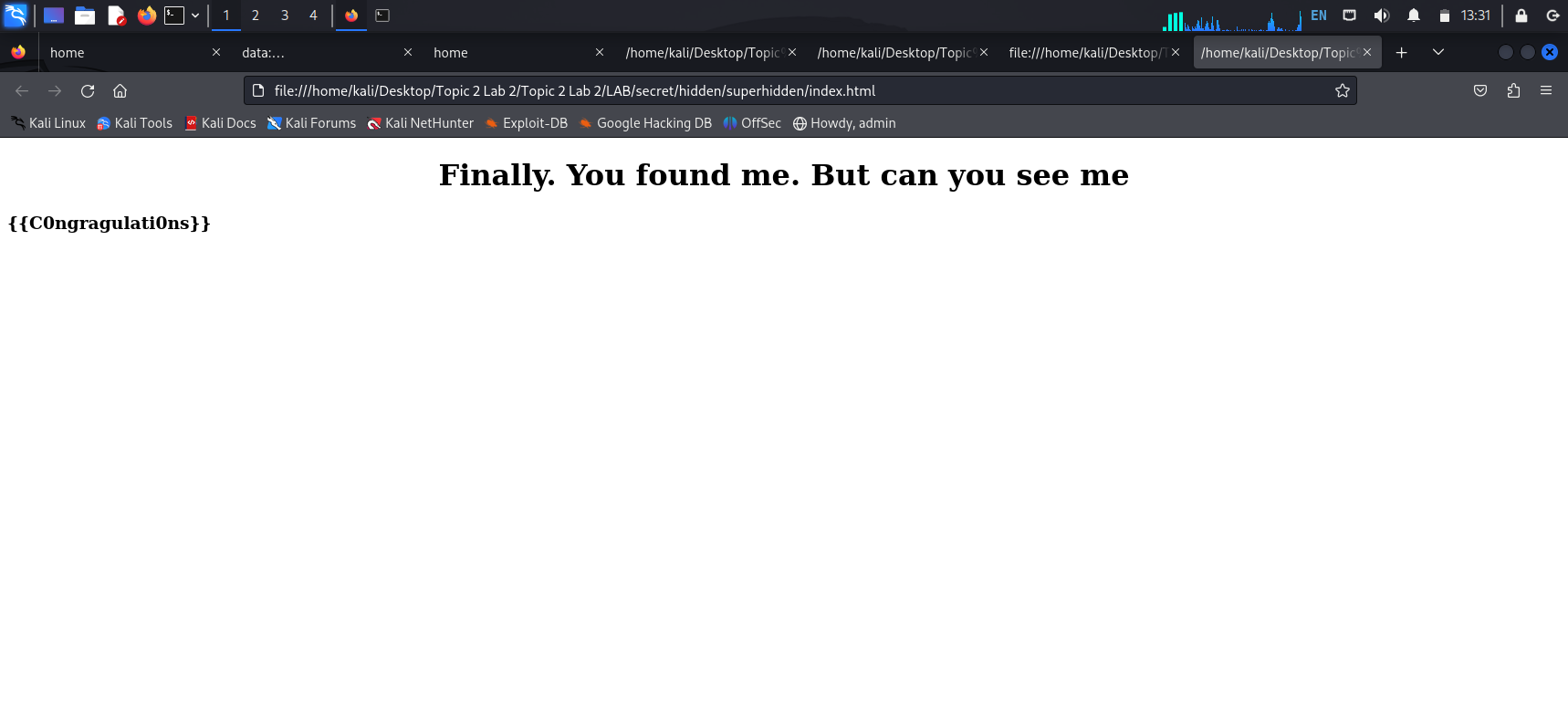


13. In this below code we have to change the colour of image code from white to black

So the message will be displayed.

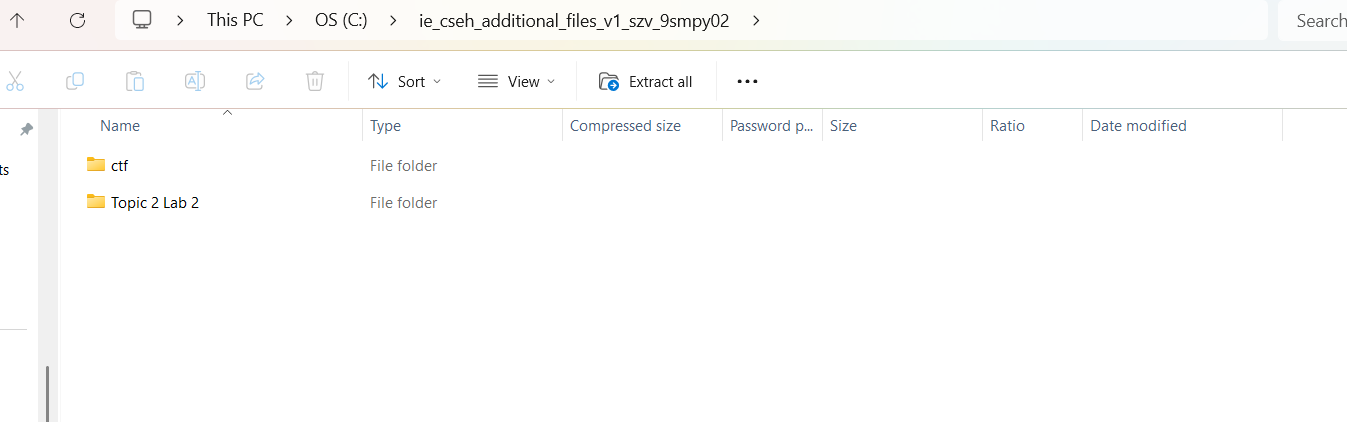


14. Finally we have found the message Congratulations!!!.

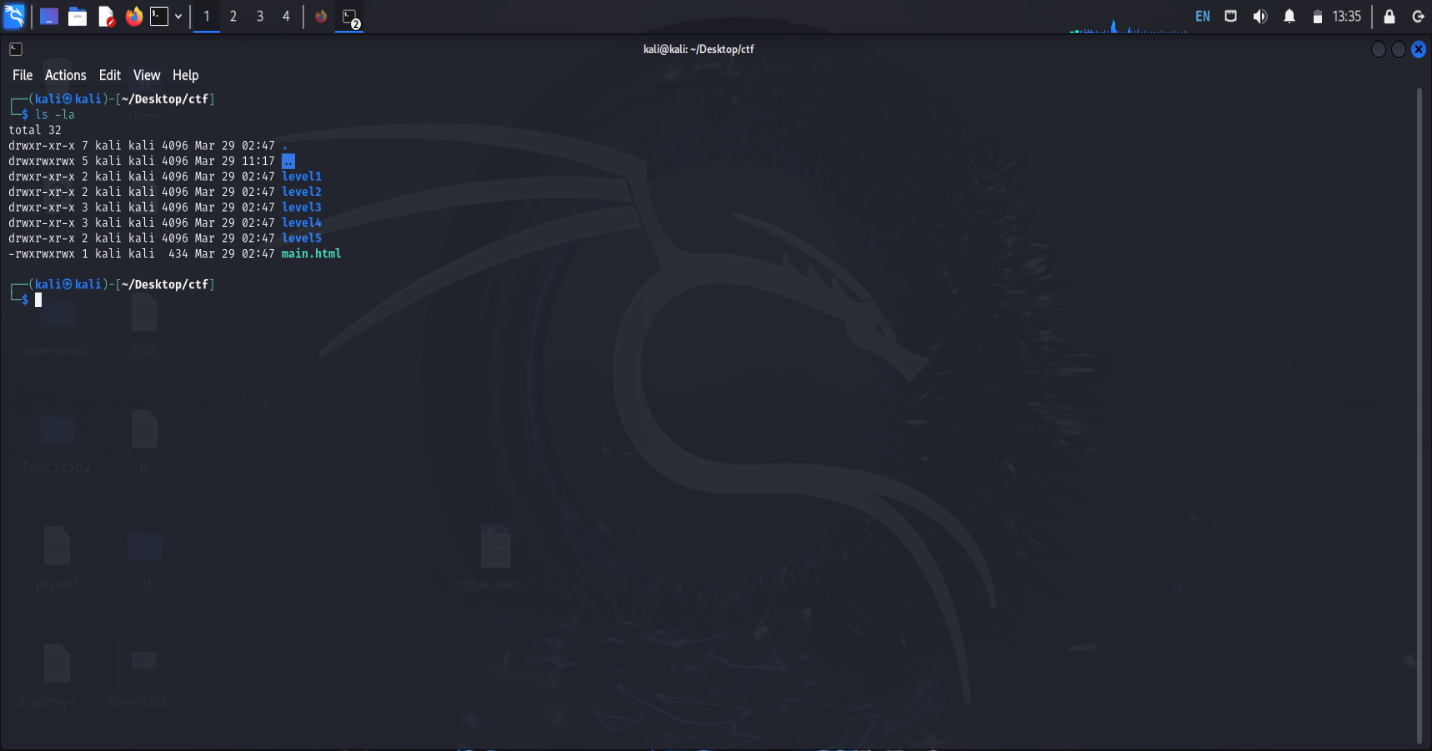


# Lab-2

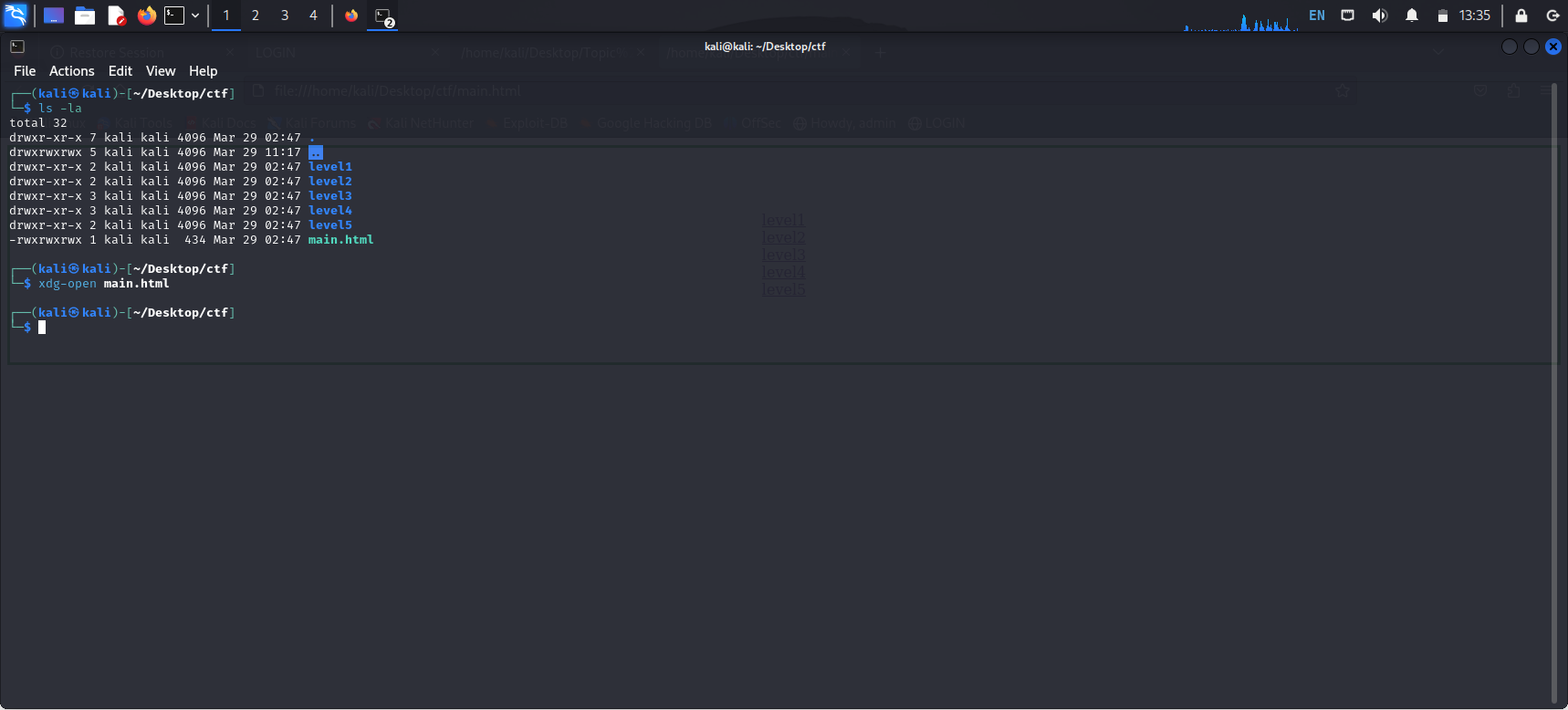
We also have cft folder in cseh\_additional\_files\_v1\_szv\_9smpy02.

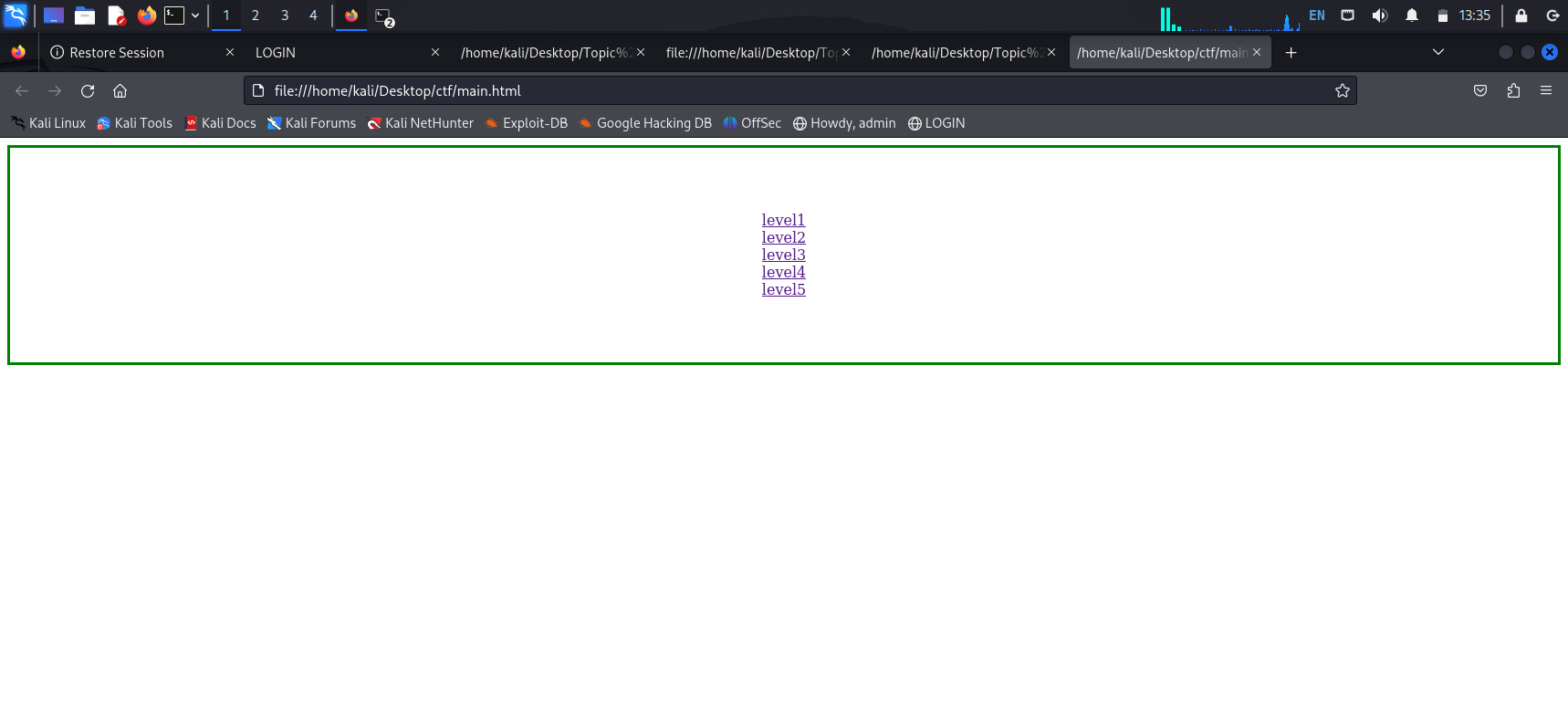


Change all the permissions of all the files and dictonary.

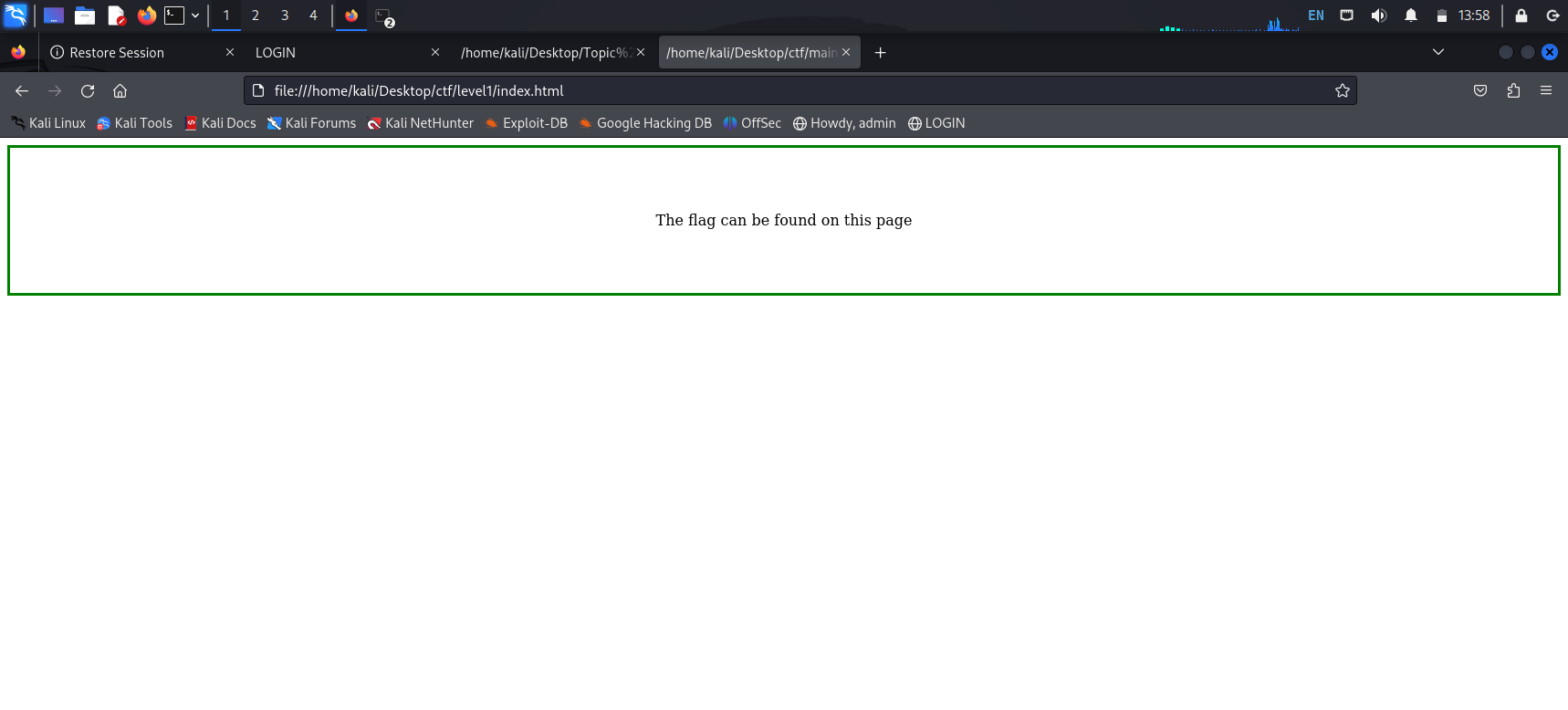


When we open the main.html file using the below commands.

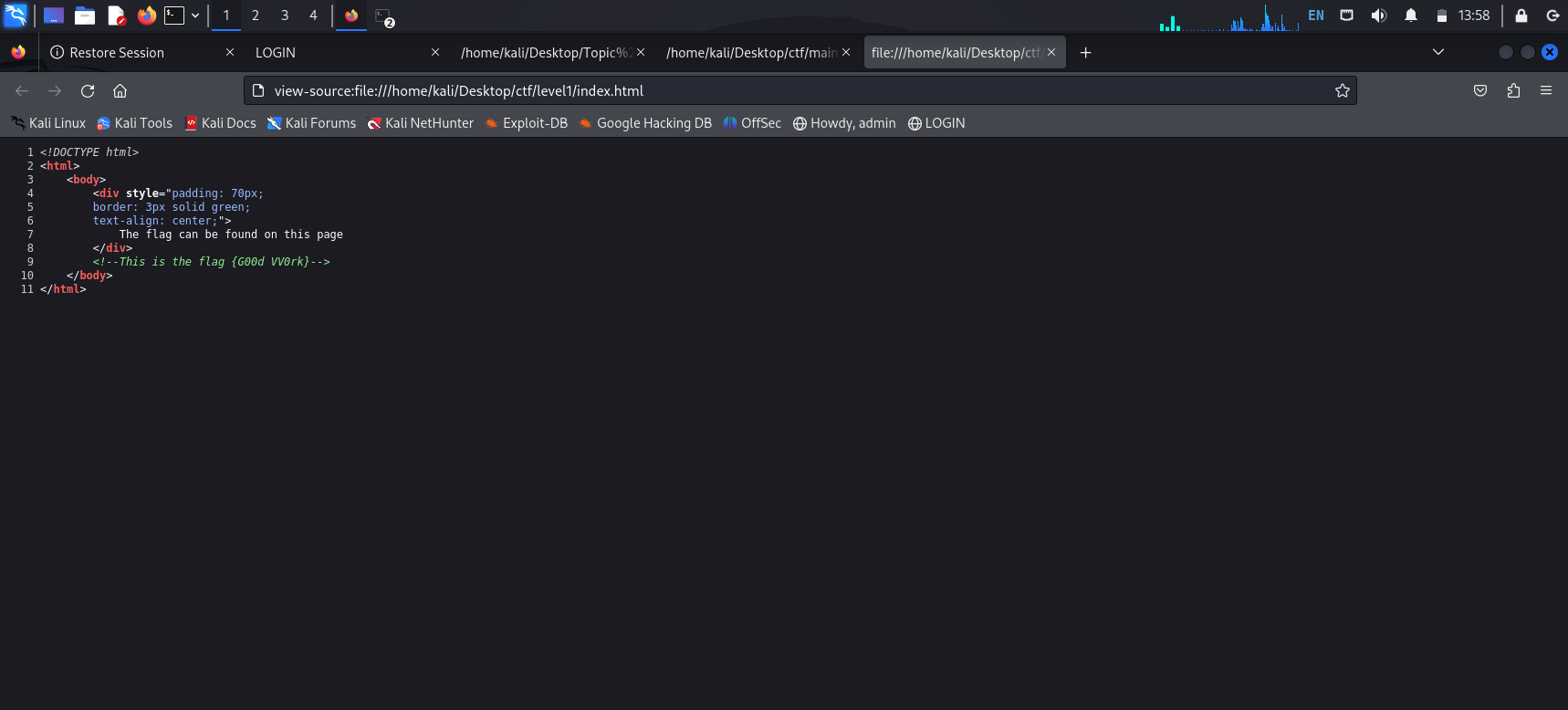




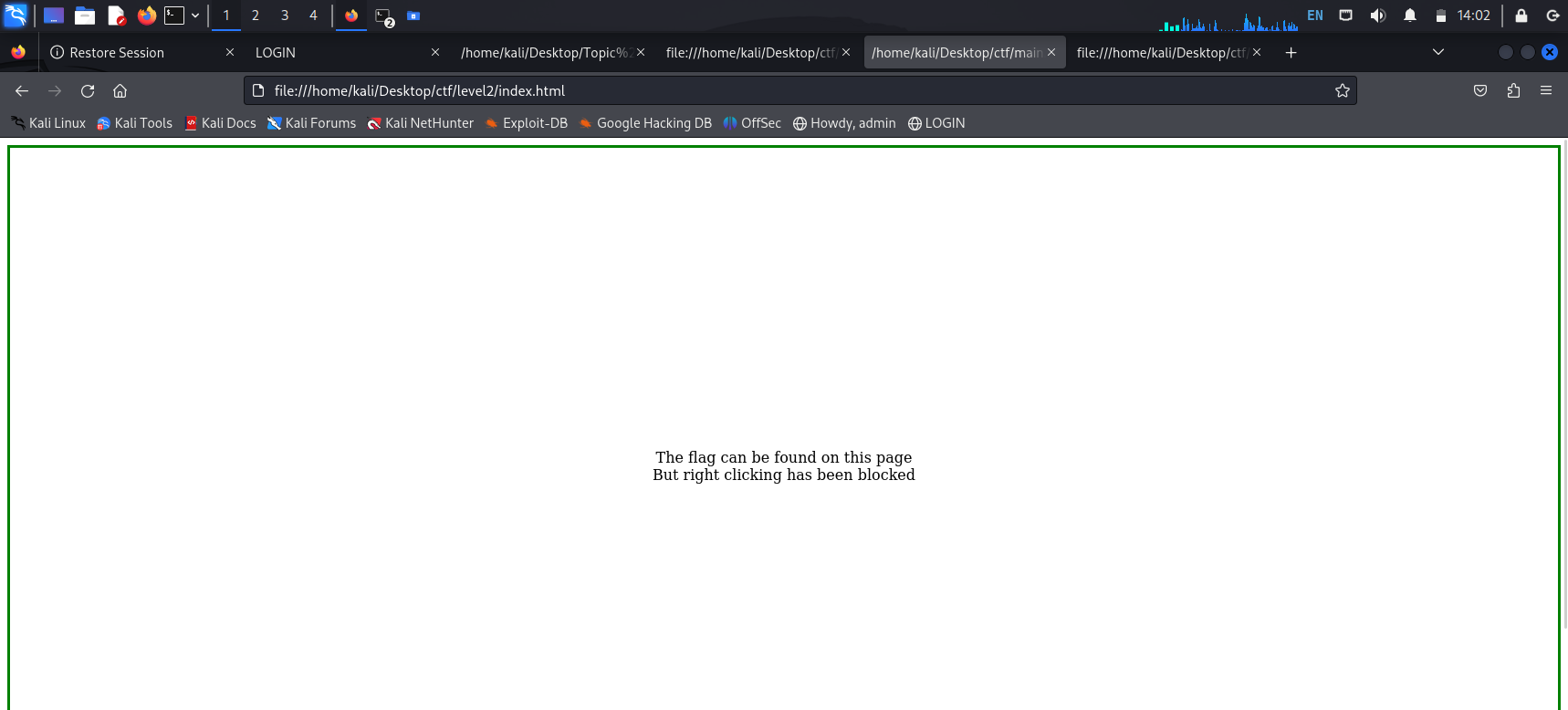
In each level we can find flags here

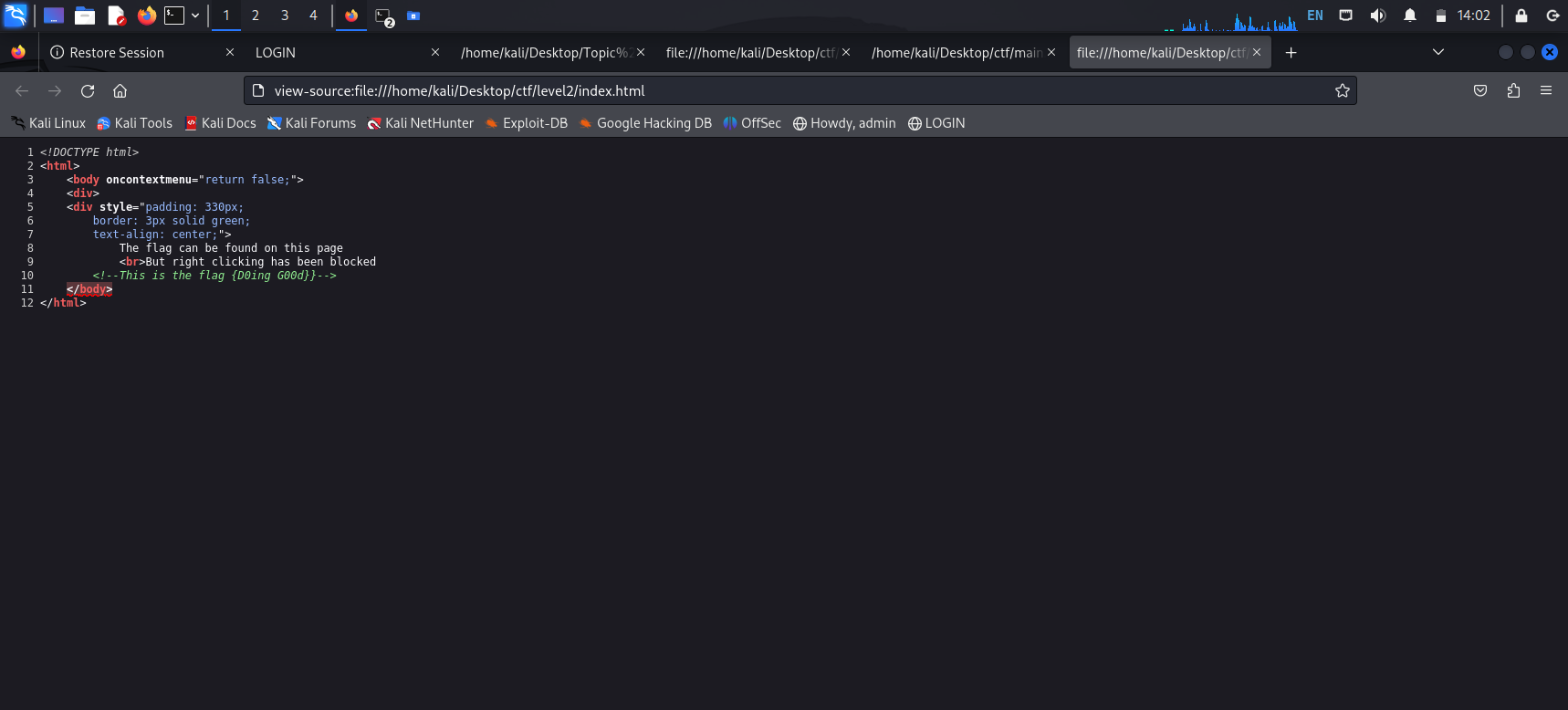


Right click and go to view source code we can find .

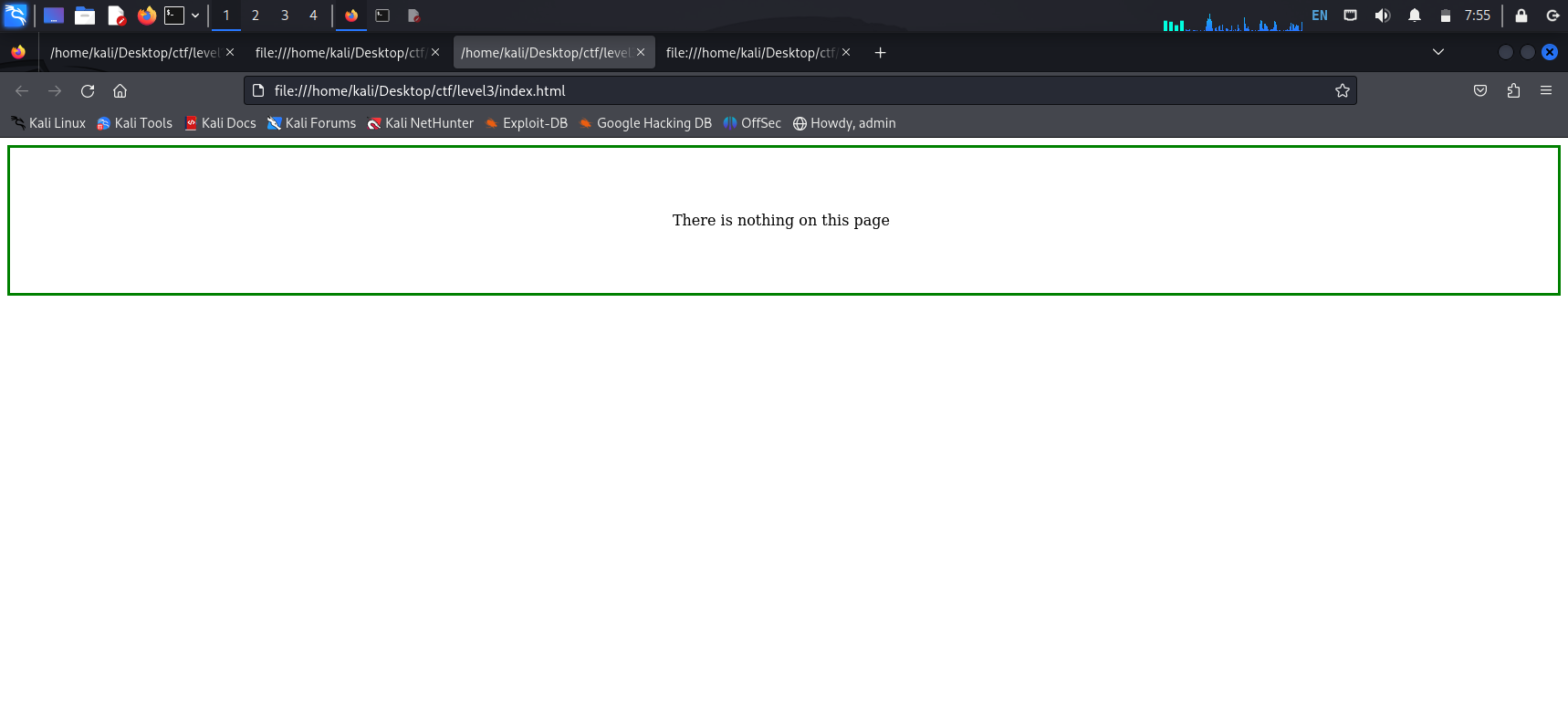


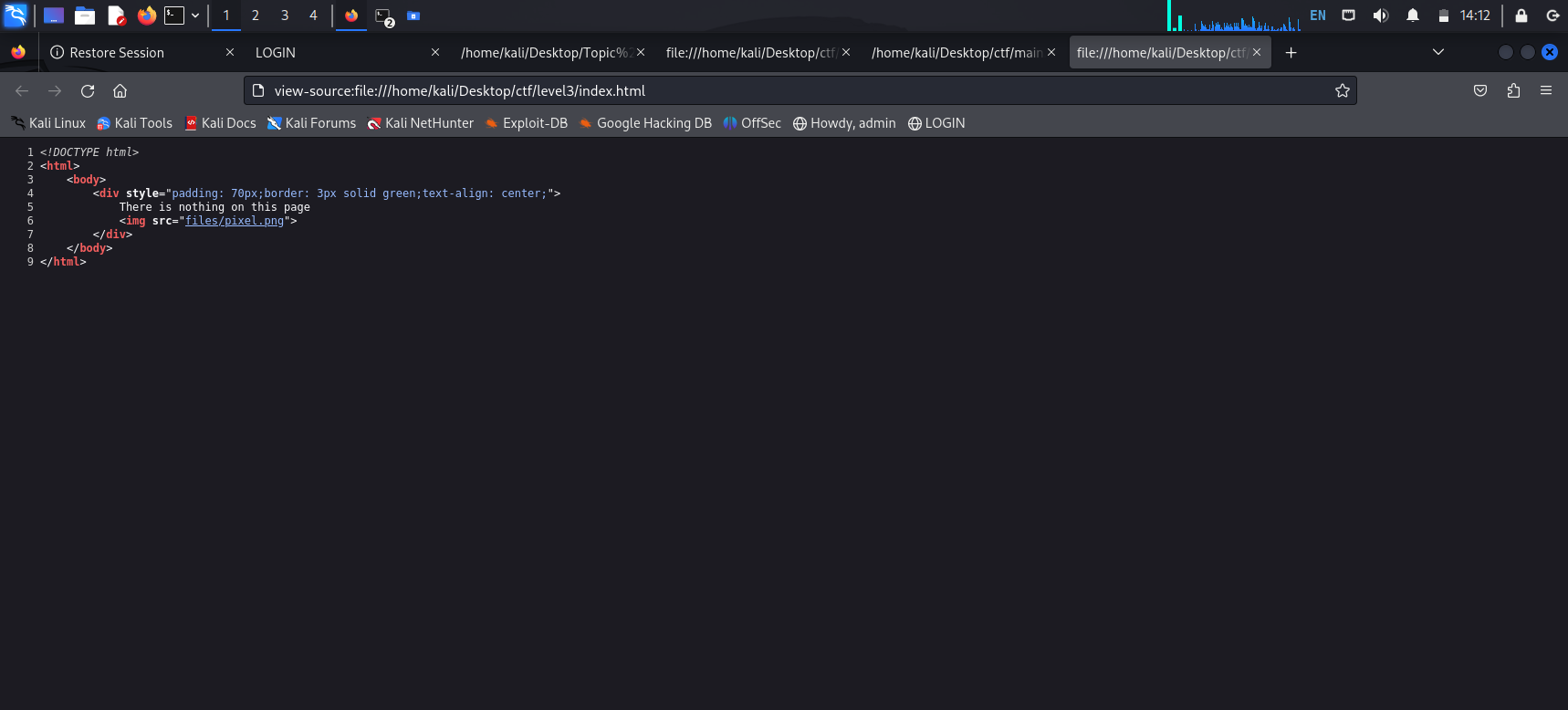
In level2 there is no flag press ctrl u to view source code.



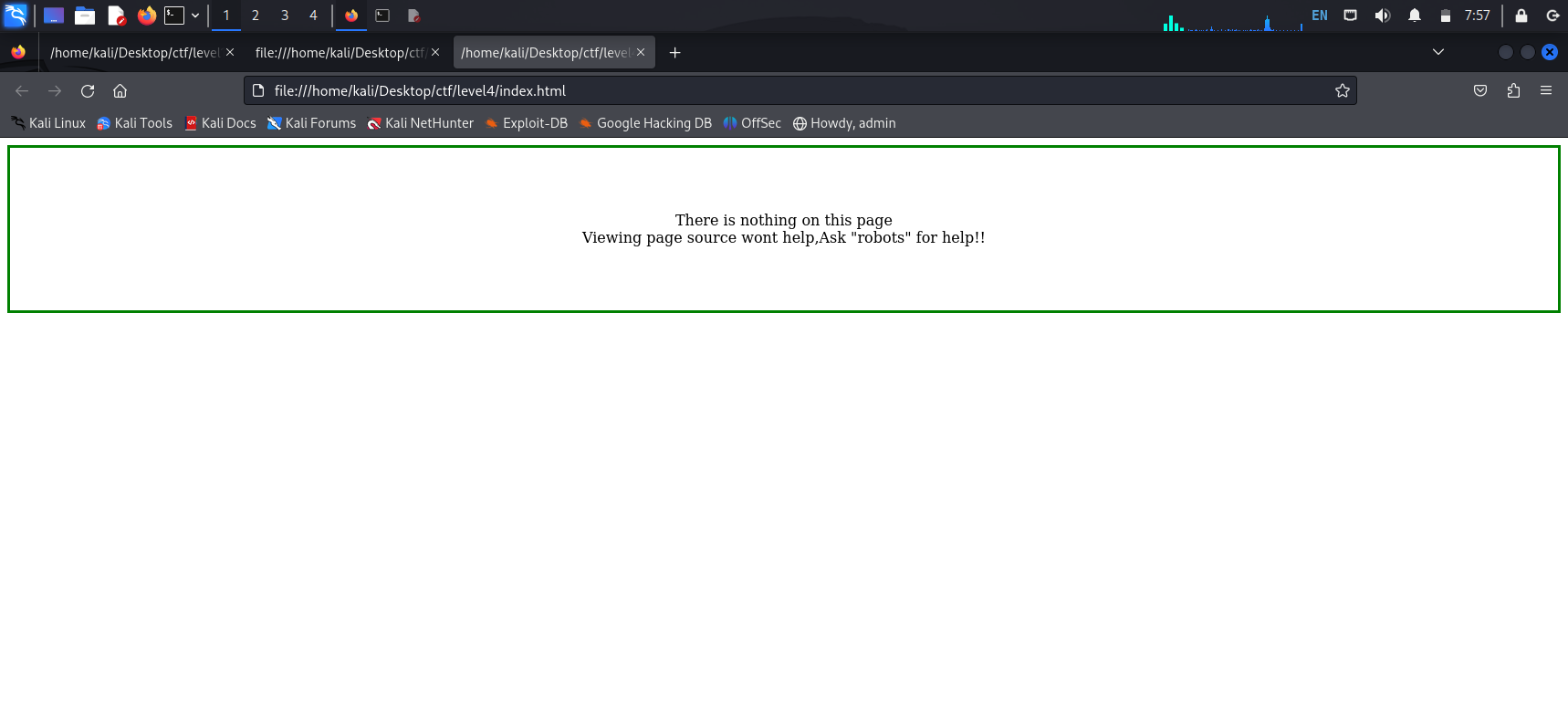


When go to level 3

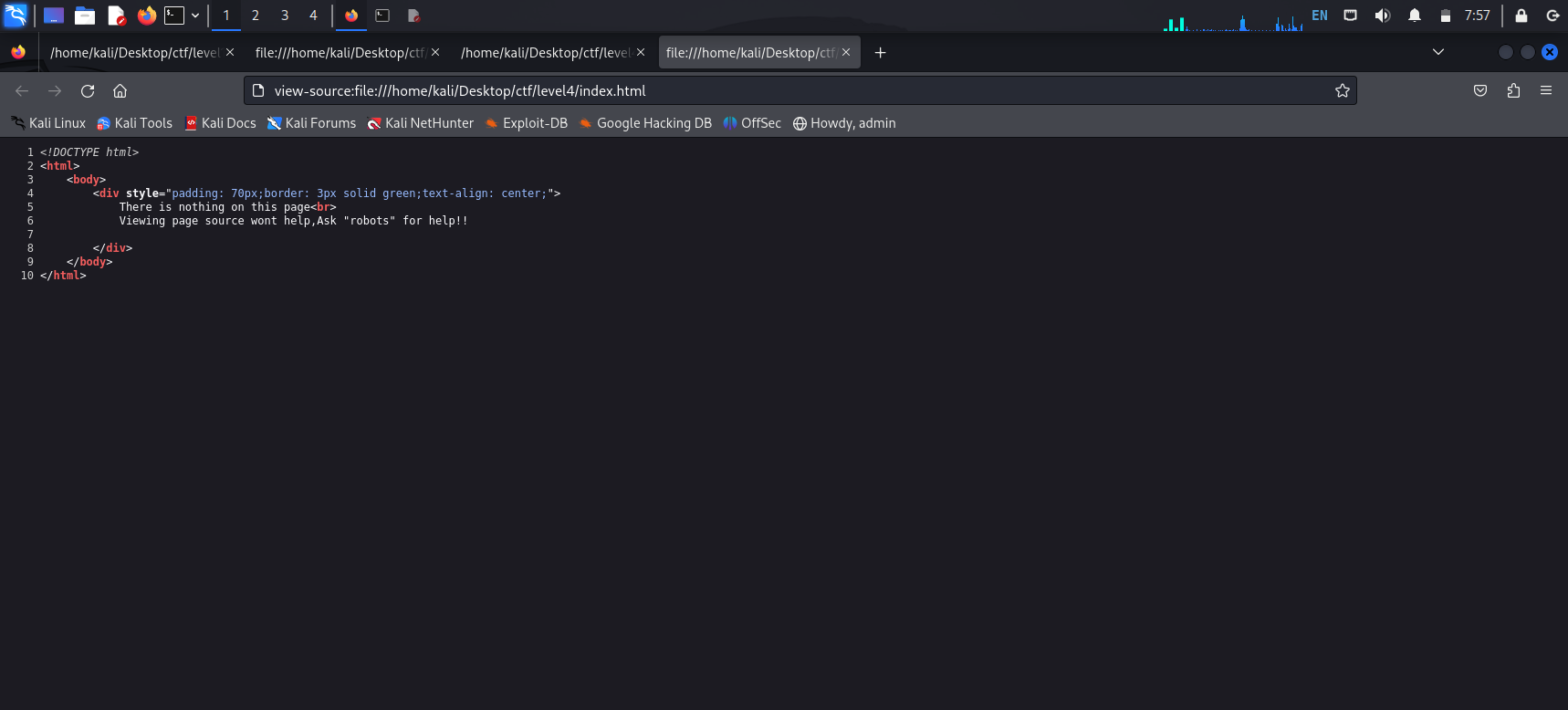




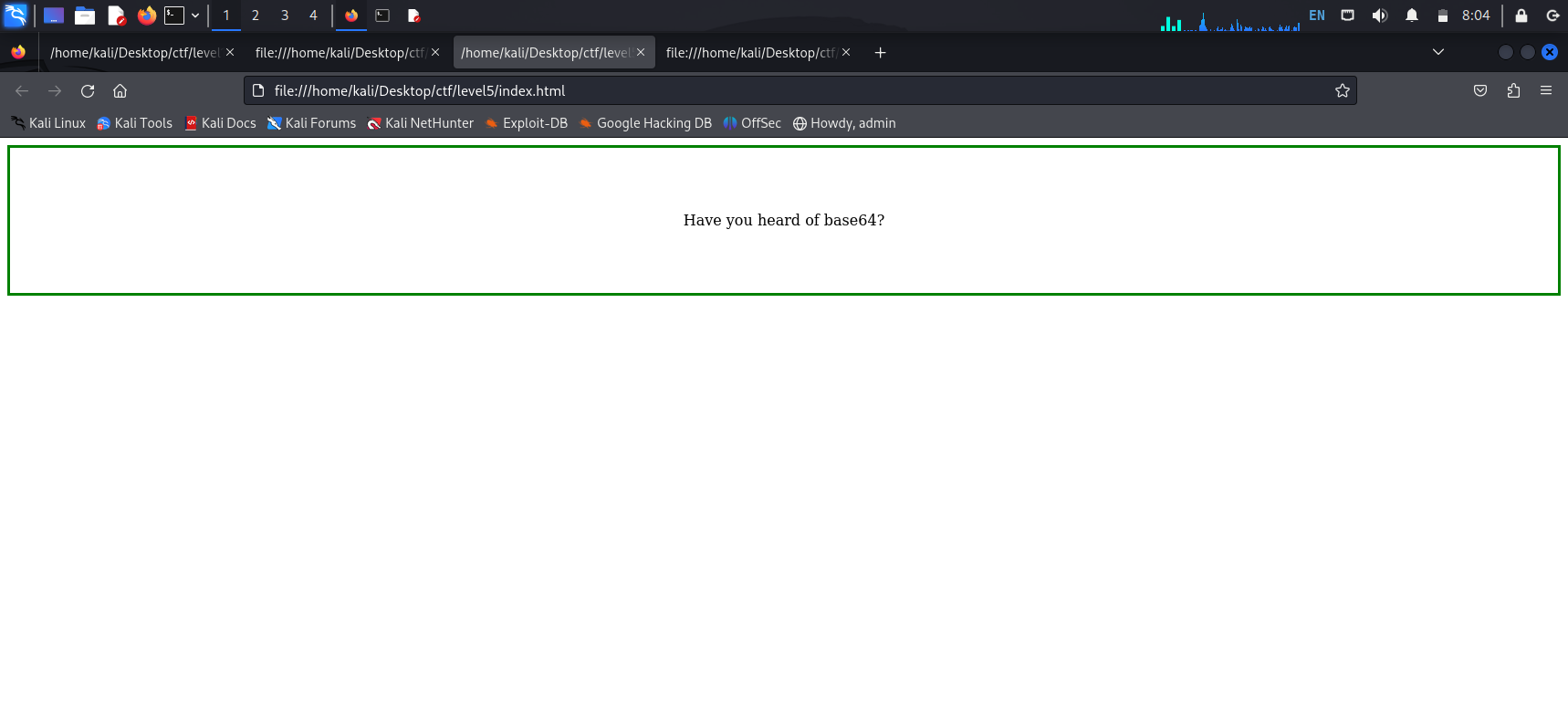
Level4



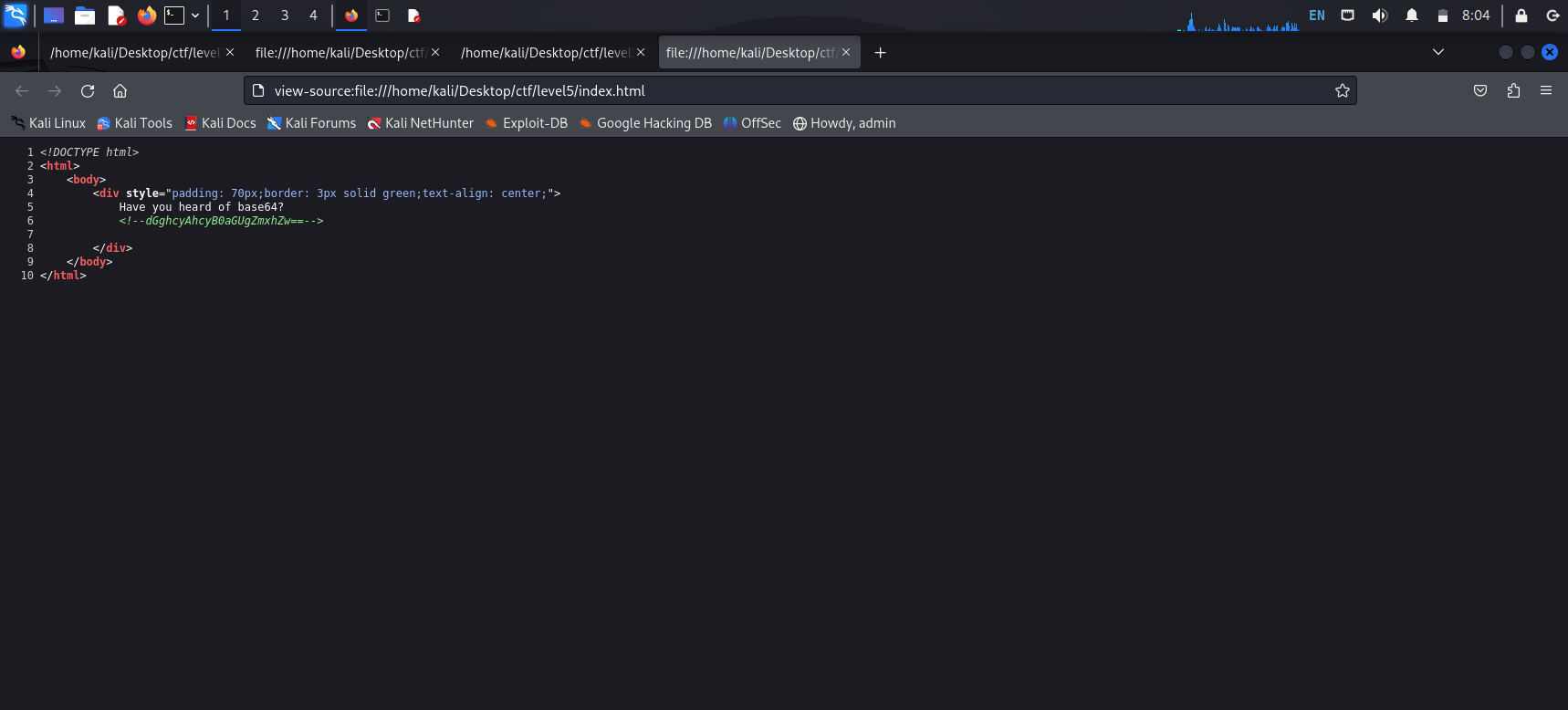
We can view source code from this page.



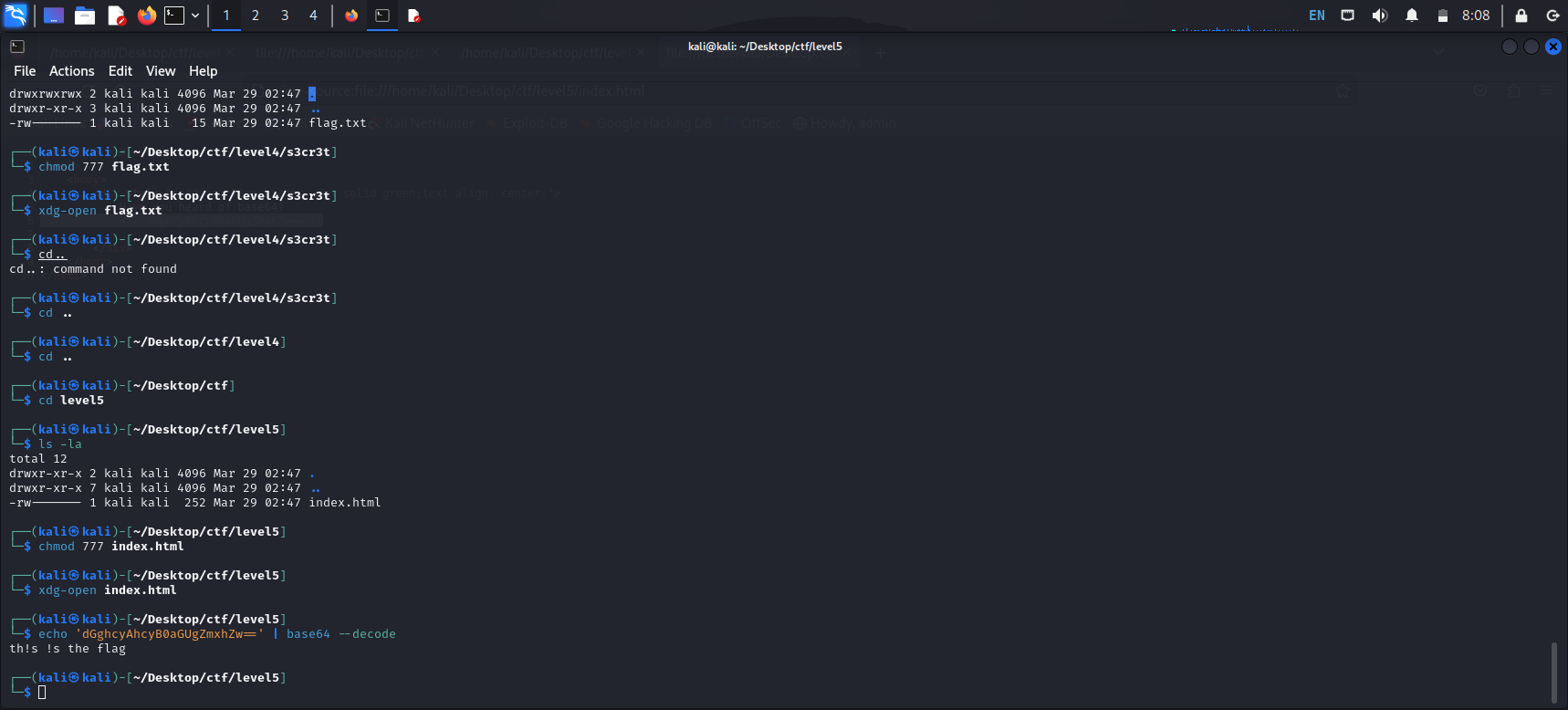
In level5 five we need to code the file with the help of base64.



Here we can see the source code where we can find a code we have decode this code for decoding we have used base64.



The final flag is here



Final flag is found.