

## 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

The image shows a Kali Linux desktop environment. At the top, there is a taskbar with various application icons and system status indicators (EN, 3:16). The main window is a terminal titled 'kali@kali: ~/Desktop/Topic 2 Lab 2/Topic 2 Lab 2/LAB'. The terminal output shows the execution of a curl command to a local web server (127.0.0.1:8080). The output is an HTML document with a table containing a form and a 'secret' button. The form has a 'name' field and a 'submit' button. The 'secret' button is highlighted in blue. Below the table, there is a paragraph of Lorem Ipsum text. The terminal also shows the output of a 'cat' command, displaying the contents of a file named 'secret', which is 'secret'. The terminal window has a dark background with light-colored text.

```
kali@kali: ~/Desktop/Topic 2 Lab 2/Topic 2 Lab 2/LAB/secret/hidden/superhidden
File Actions Edit View Help

(kali@kali)~/Topic 2 Lab 2/LAB/secret/hidden
$ xdg-open index.html

(kali@kali)~/Topic 2 Lab 2/LAB/secret/hidden
$ cd superhidden

(kali@kali)~/LAB/secret/hidden/superhidden
$ ls -la
total 20
drwxr-xr-x 2 kali kali 4096 Aug 14 2024 .
drwxr-xr-x 3 kali kali 4096 Aug 14 2024 ..
-rw-r--r-- 1 kali kali 239 Aug 14 2024 index.html
-rw-r--r-- 1 kali kali 2087 Aug 14 2024 login.css
-rw-r--r-- 1 kali kali 143 Aug 14 2024 mycss.css

(kali@kali)~/LAB/secret/hidden/superhidden
$ chmod 777 .

(kali@kali)~/LAB/secret/hidden/superhidden
$ chmod 777 ..

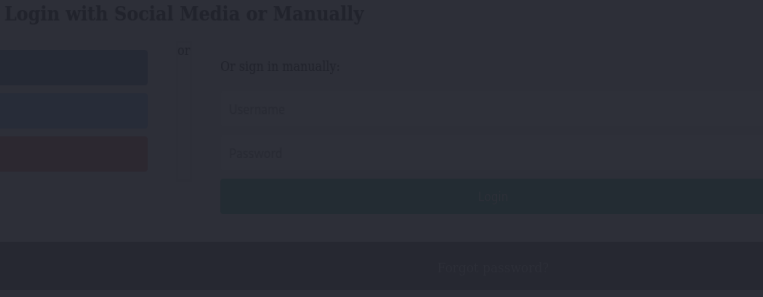
(kali@kali)~/LAB/secret/hidden/superhidden
$ chmod 777 index.html

(kali@kali)~/LAB/secret/hidden/superhidden
$ chmod 777 login.css

(kali@kali)~/LAB/secret/hidden/superhidden
$ chmod 777 mycss.css

(kali@kali)~/LAB/secret/hidden/superhidden
$ ls -la
total 20
drwxrwxrwx 2 kali kali 4096 Aug 14 2024 .
drwxrwxrwx 3 kali kali 4096 Aug 14 2024 ..
-rwxrwxrwx 1 kali kali 239 Aug 14 2024 index.html
-rwxrwxrwx 1 kali kali 2087 Aug 14 2024 login.css
-rwxrwxrwx 1 kali kali 143 Aug 14 2024 mycss.css

(kali@kali)~/LAB/secret/hidden/superhidden
$
```

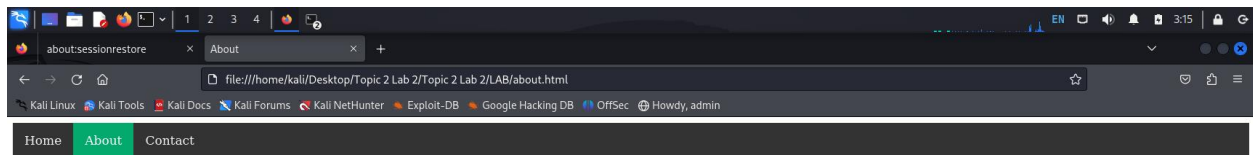
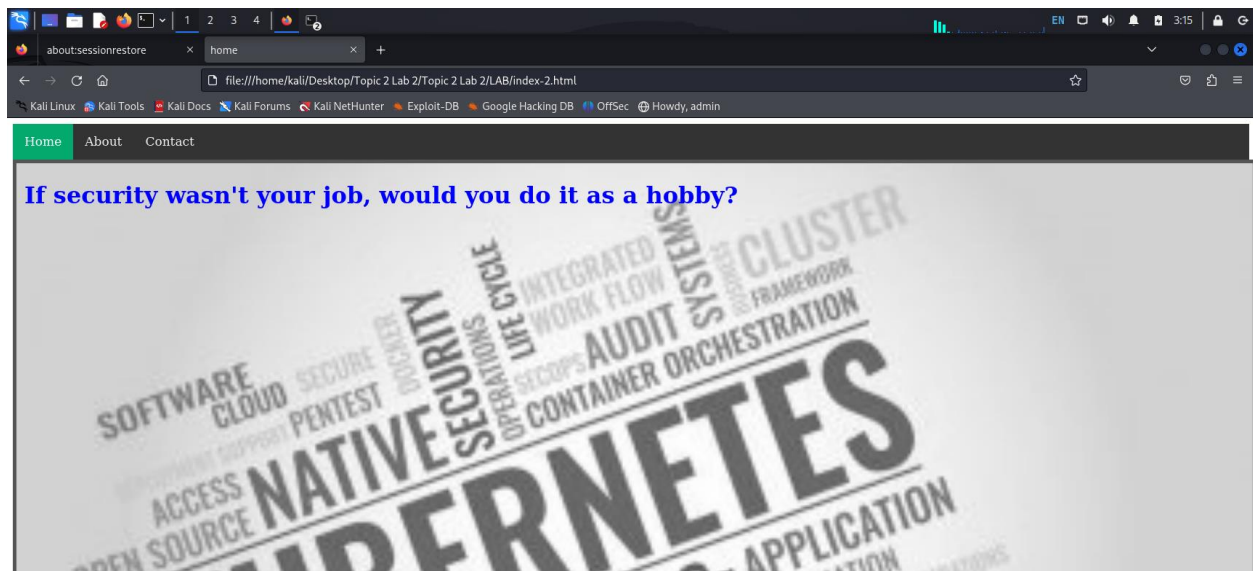


4. using chmod 777 index.html.

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

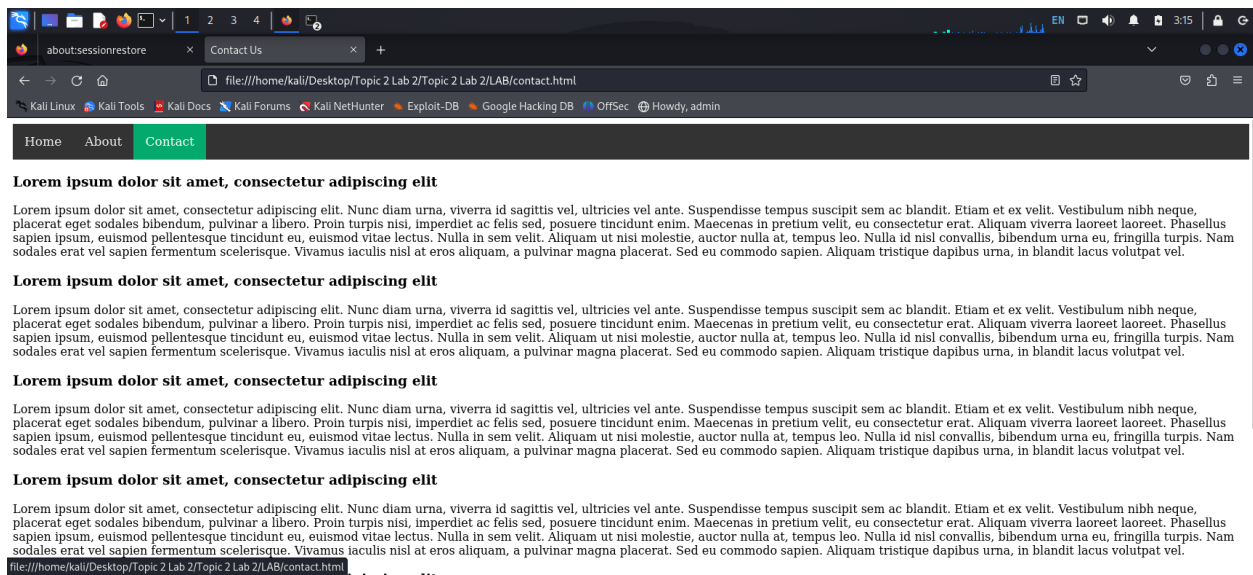
6. when we open this index.html files we can find home page .



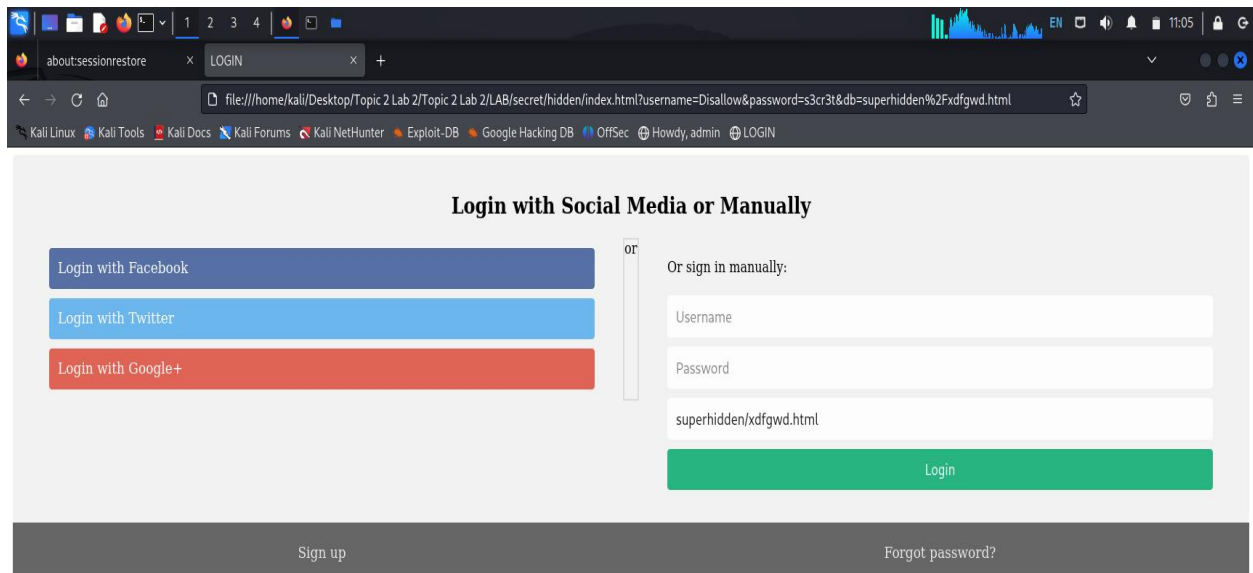


**We are here to learn and exercise the cybersecurity muscle!!!**

file:///home/kali/Desktop/Topic 2 Lab 2/Topic 2 Lab 2/LAB/about.html



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.

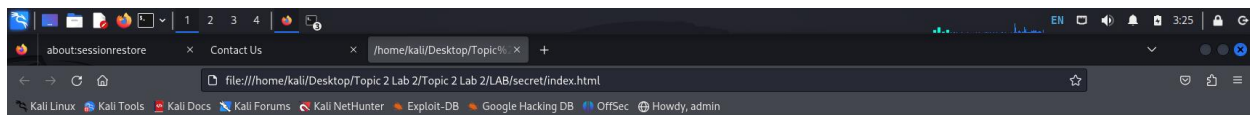
```
1 </DOCTYPE html>
2 <html>
3 <head>
4 <title>LOGIN</title>
5 <!-- CSS -->
6 <link href="superhidden/login.css" rel="stylesheet" />
7 </head>
8 <body>
9 <form>
10 <div class="container">
11 <form method="" action="/secret/assets/popup.js">
12 <div class="row">
13 <div style="text-align: center;">
14 Login with Social Media or Manually
15 </div>
16 <div class="vl">
17 <span class="vl-innertext">or</span>
18 </div>
19
20 <div class="col">
21 <a href="#" class="fb btn">
22 <i class="fa fa-facebook fa-fw"></i> Login with Facebook
23 </a>
24 <a href="#" class="twitter btn">
25 <i class="fa fa-twitter fa-fw"></i> Login with Twitter
26 </a>
27 <a href="#" class="google btn">
28 <i class="fa fa-google fa-fw"></i> Login with Google+
29 </a>
30 </div>
31
32 <div class="col">
33 <div class="hide-md-lg">
34 <or sign in manually:</p>
35 </div>
36
37 <input
38 type="text"
39 name="username"
40 placeholder="Username"
41 required
42 />
43
44 <input
45 type="password"
46 name="password"
47 placeholder="Password"
48 required
49 />
50 <input type="text" name="db" value="superhidden/xdfgwd.html" />
51
52 <input
53 type="submit"
54 value="login"
55 onclick="alert('Thank you for the attempt but oops! try harder, better luck next time!'"
56 />
57 </div>
58 </form>
59 </div>
60
61 <div class="bottom-container">
62 <div class="row">
63 <div class="col">
64 <a href="#" style="color: white;" class="btn">Sign up</a>
65 </div>
66 <div class="col">
67 <a href="#" style="color: white;" class="btn">Forgot password</a>
68 </div>
69 </div>
70 </div>
71 </form>
72 </body>
73 </html>
```

9.secret/assets/popup.js is a misleading link and we have superhidden/xdfgwd.html  
Which is of no use.

```
33 <div class="hide-md-lg">
34 <or sign in manually:</p>
35 </div>
36
37 <input
38 type="text"
39 name="username"
40 placeholder="Username"
41 required
42 />
43
44 <input
45 type="password"
46 name="password"
47 placeholder="Password"
48 required
49 />
50 <input type="text" name="db" value="superhidden/xdfgwd.html" />
51
52 <input
53 type="submit"
54 value="login"
55 onclick="alert('Thank you for the attempt but oops! try harder, better luck next time!'"
56 />
57 </div>
58 </form>
59 </div>
60
61 <div class="bottom-container">
62 <div class="row">
63 <div class="col">
64 <a href="#" style="color: white;" class="btn">Sign up</a>
65 </div>
66 <div class="col">
67 <a href="#" style="color: white;" class="btn">Forgot password</a>
68 </div>
69 </div>
70 </div>
71 </form>
72 </body>
73 </html>
```

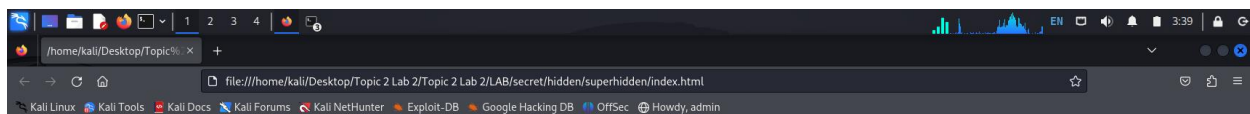
10. Desktop/Topic%202%20Lab%202/Topic%202%20Lab%202/LAB/secret/index.html  
We have found a clue here so we can move to the next step.

11.  
<file:///home/kali/Desktop/Topic%202%20Lab%202/Topic%202%20Lab%202/LAB/secret/hidden/superhidden/index.html>.



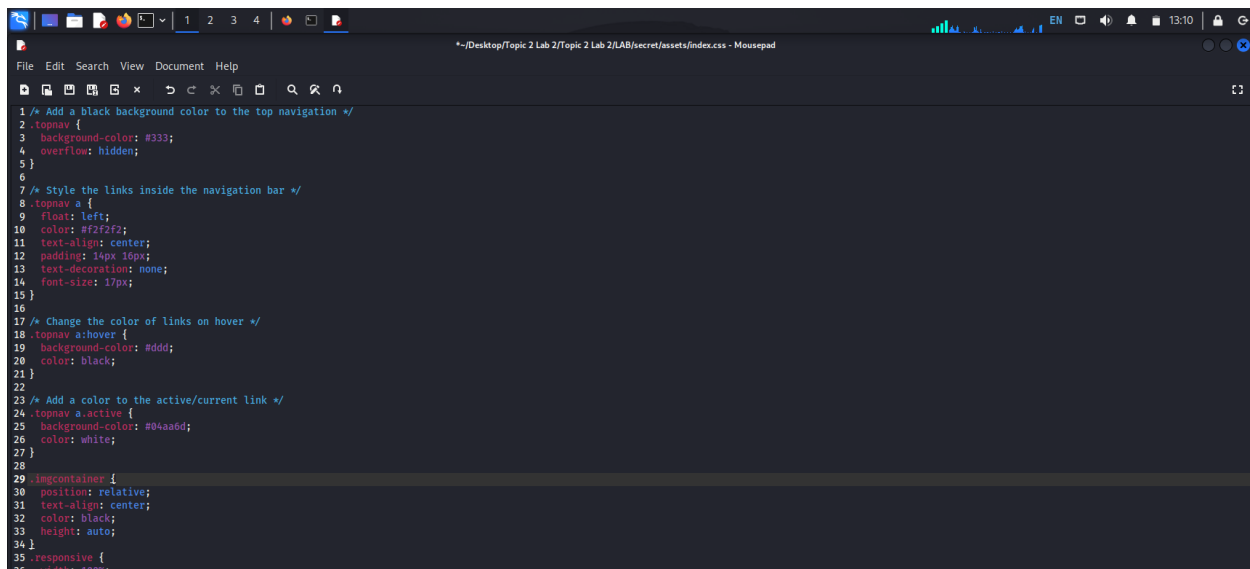
**Finally. You almost found me. you are doing well**

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.



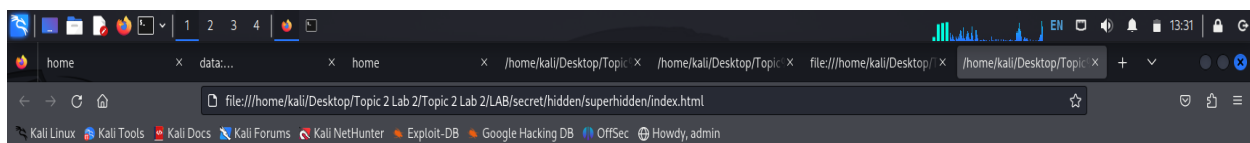
**Finally. You found me. But can you see me**

13. In this below code we have to change the colour of image code from white to black  
So the message will be displayed.

A screenshot of a Linux desktop environment. The top panel shows system icons and the time 13:10. The main window is a terminal titled "~/Desktop/Topic 2 Lab 2/Topic 2 Lab 2/LAB/secret/assets/index.css - Mousepad". It contains CSS code for styling a navigation bar. The code includes comments in /\* \*/ and CSS rules for .topnav, .topnav a, .topnav a:active, .topnav a:active, .imgcontainer, and .responsive. The code is as follows:

```
1 /* Add a black background color to the top navigation */
2 .topnav {
3   background-color: #333;
4   overflow: hidden;
5 }
6
7 /* Style the links inside the navigation bar */
8 .topnav a {
9   float: left;
10  color: #f2f2f2;
11  text-align: center;
12  padding: 14px 16px;
13  text-decoration: none;
14  font-size: 17px;
15 }
16
17 /* Change the color of links on hover */
18 .topnav a:active {
19   background-color: #ddd;
20   color: black;
21 }
22
23 /* Add a color to the active/current link */
24 .topnav a:active {
25   background-color: #04aa6d;
26   color: white;
27 }
28
29 .imgcontainer {
30   position: relative;
31   text-align: center;
32   color: black;
33   height: auto;
34 }
35 .responsive {
```

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

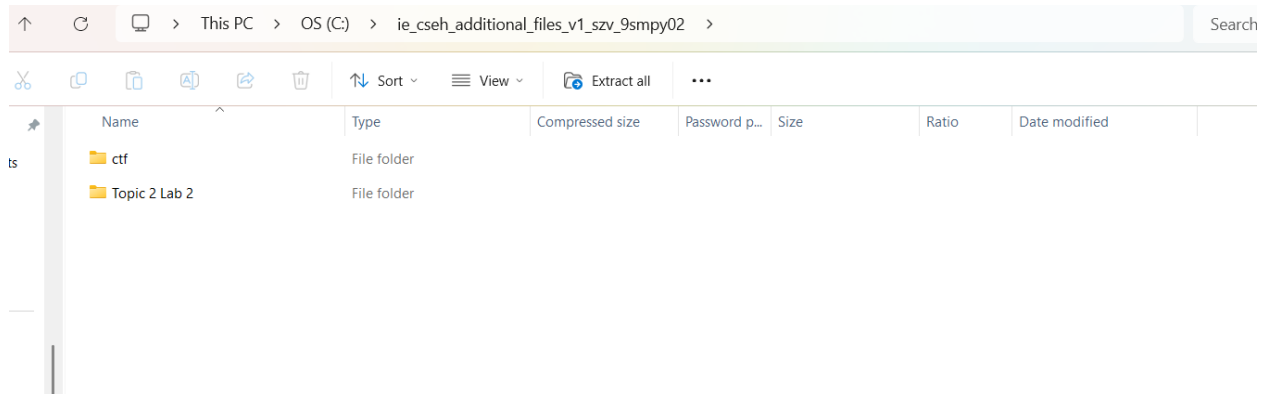


**Finally. You found me. But can you see me**

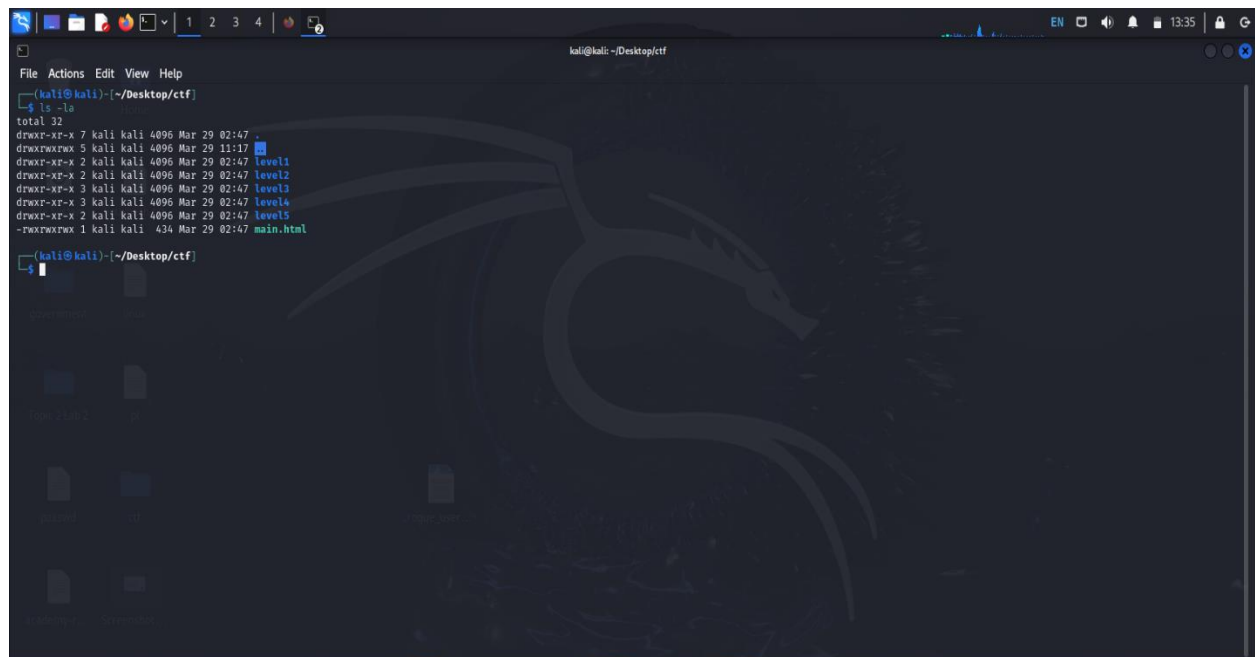
{{C0ngragulat0ns}}

## Lab-2

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



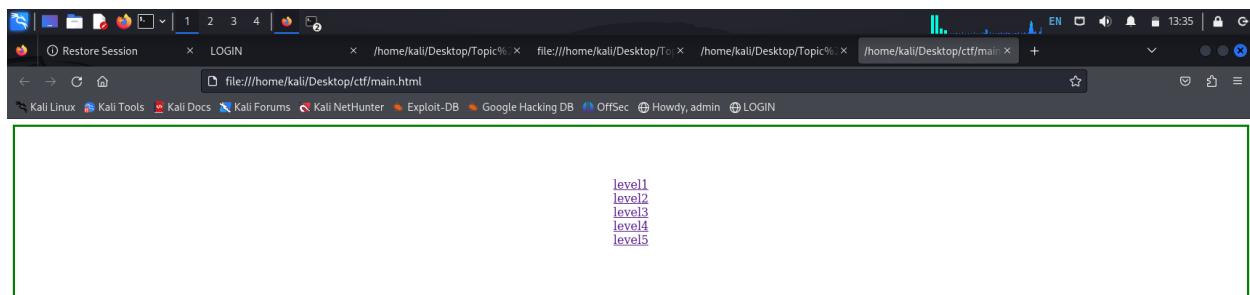
Change all the permissions of all the files and dictionary.



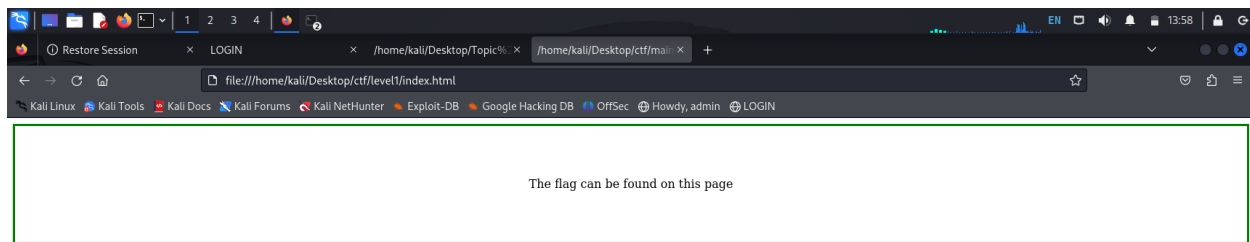
When we open the main.html file using the below commands.



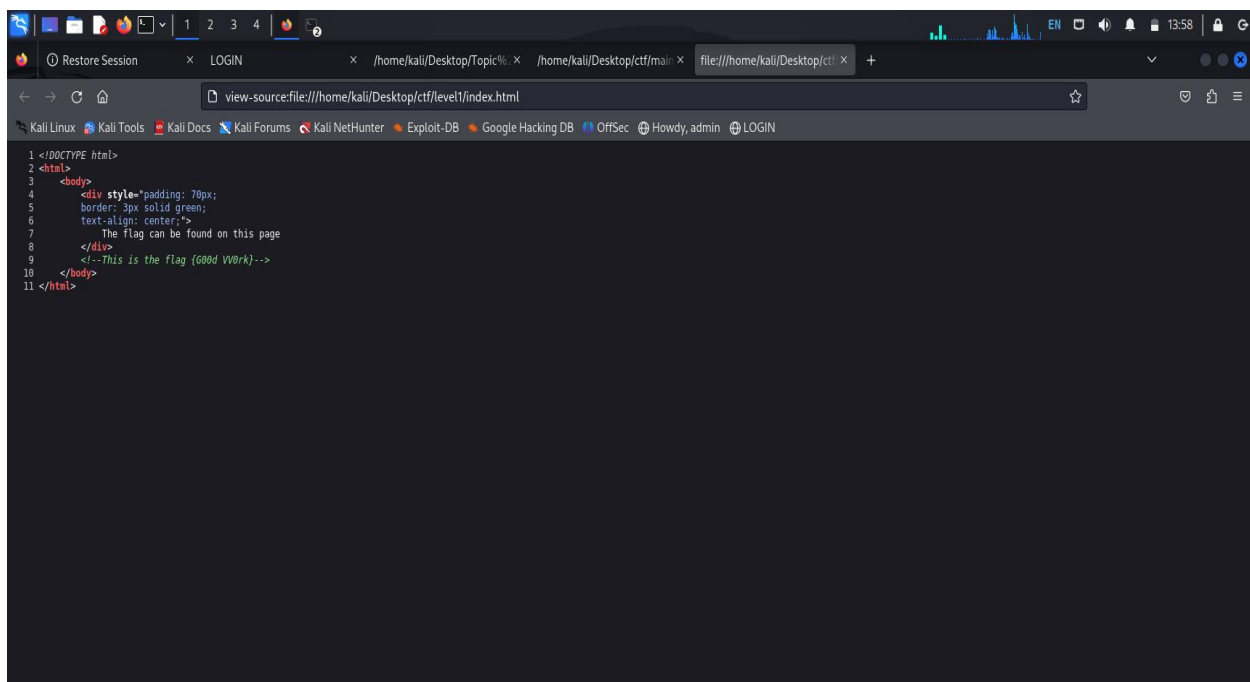
```
File Actions Edit View Help
(kali@kali)~/Desktop/ctf
$ ls -la
total 32
drwxr-xr-x 7 kali kali 4096 Mar 29 02:47 .
drwxrwxrwx 5 kali kali 4096 Mar 29 11:17 ..
drwxr-xr-x 2 kali kali 4096 Mar 29 02:47 level1
drwxr-xr-x 2 kali kali 4096 Mar 29 02:47 level2
drwxr-xr-x 3 kali kali 4096 Mar 29 02:47 level3
drwxr-xr-x 3 kali kali 4096 Mar 29 02:47 level4
drwxr-xr-x 2 kali kali 4096 Mar 29 02:47 level5
-rwxrwxrwx 1 kali kali 434 Mar 29 02:47 main.html
                                level1
                                level2
                                level3
                                level4
                                level5
(kali@kali)~/Desktop/ctf
$ xdg-open main.html
(kali@kali)~/Desktop/ctf
$
```



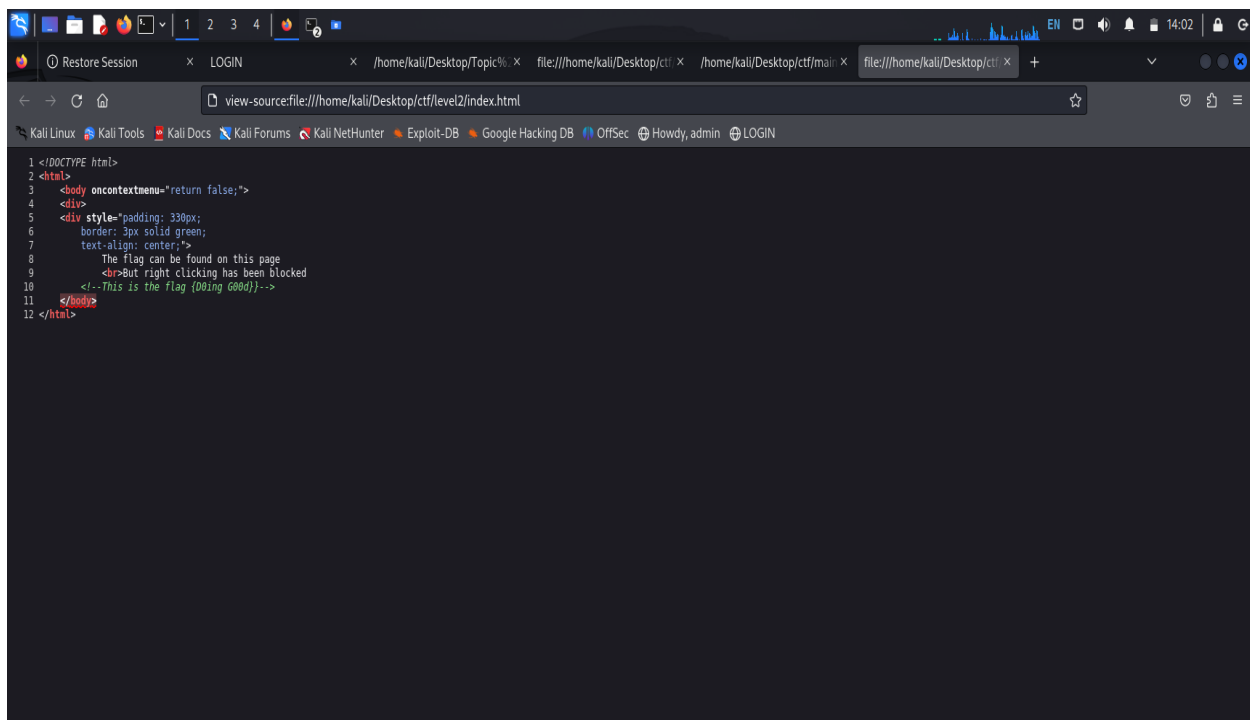
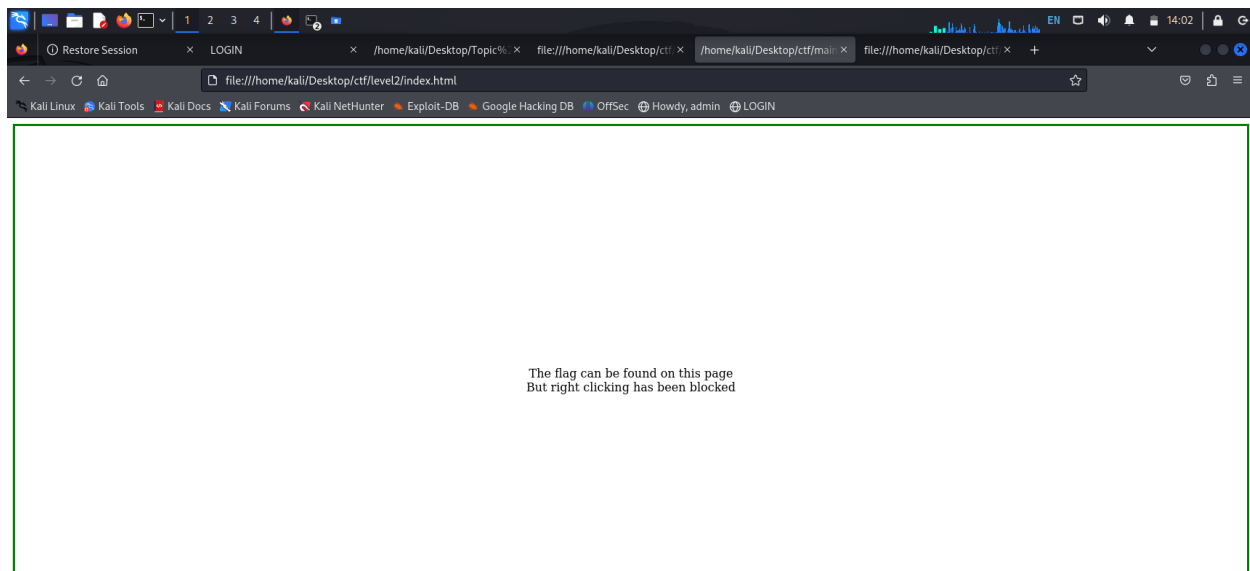
In each level we can find flags here



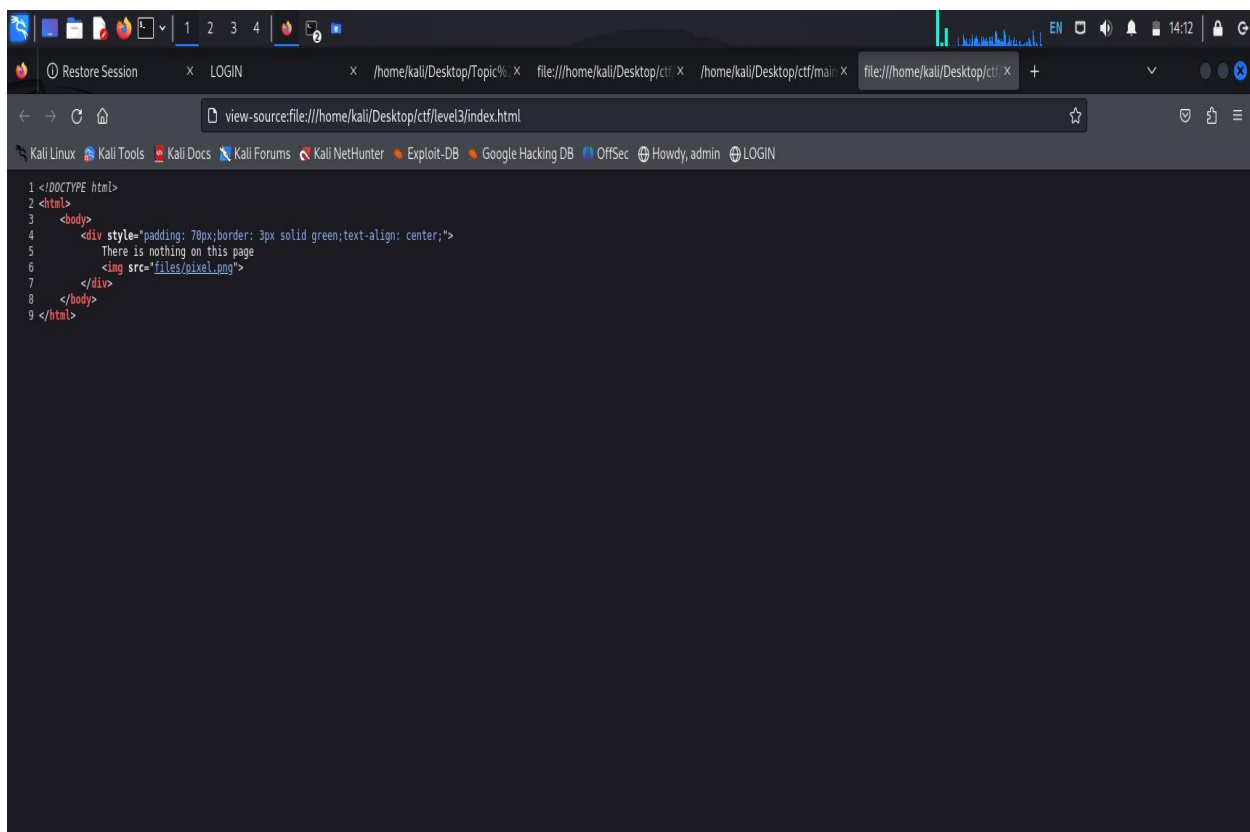
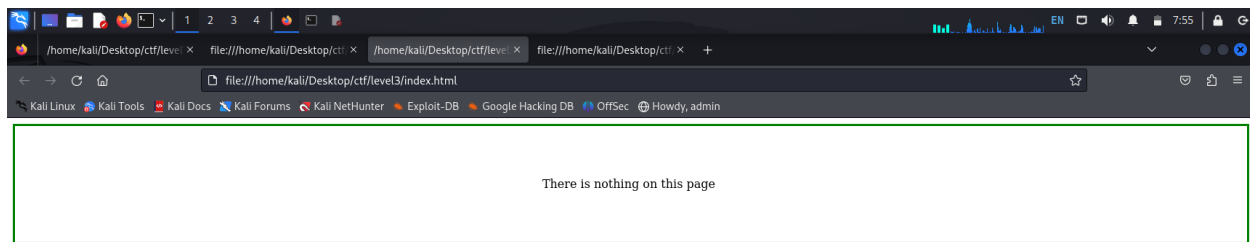
Right click and go to view source code we can find .



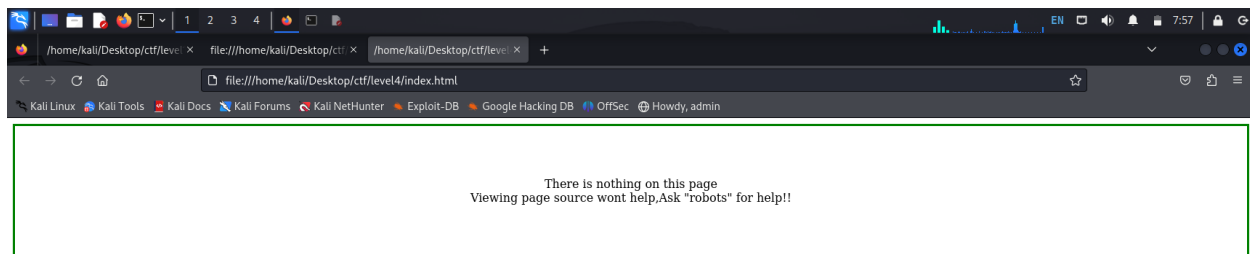
In level2 there is no flag press ctrl u to view source code.



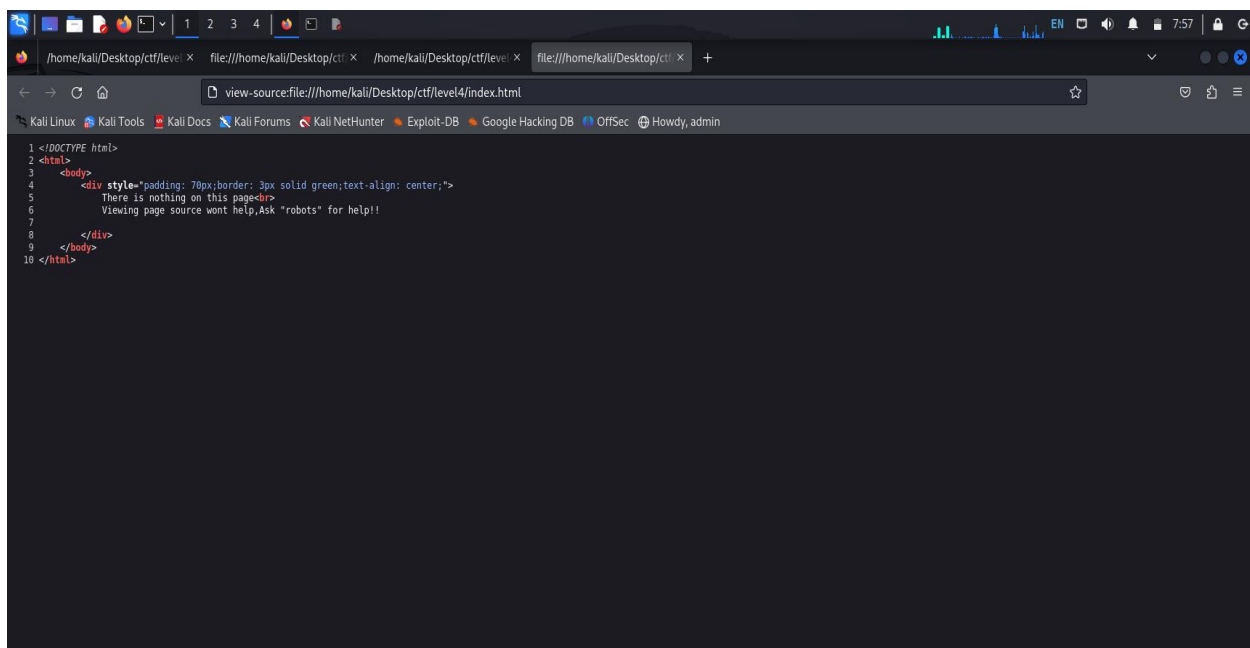
When go to level 3



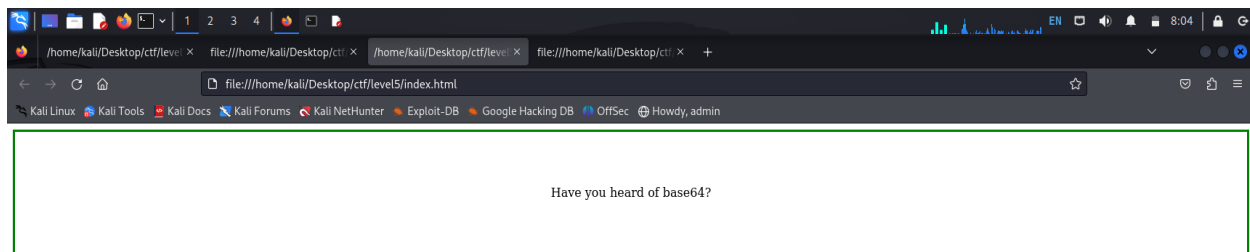
Level4



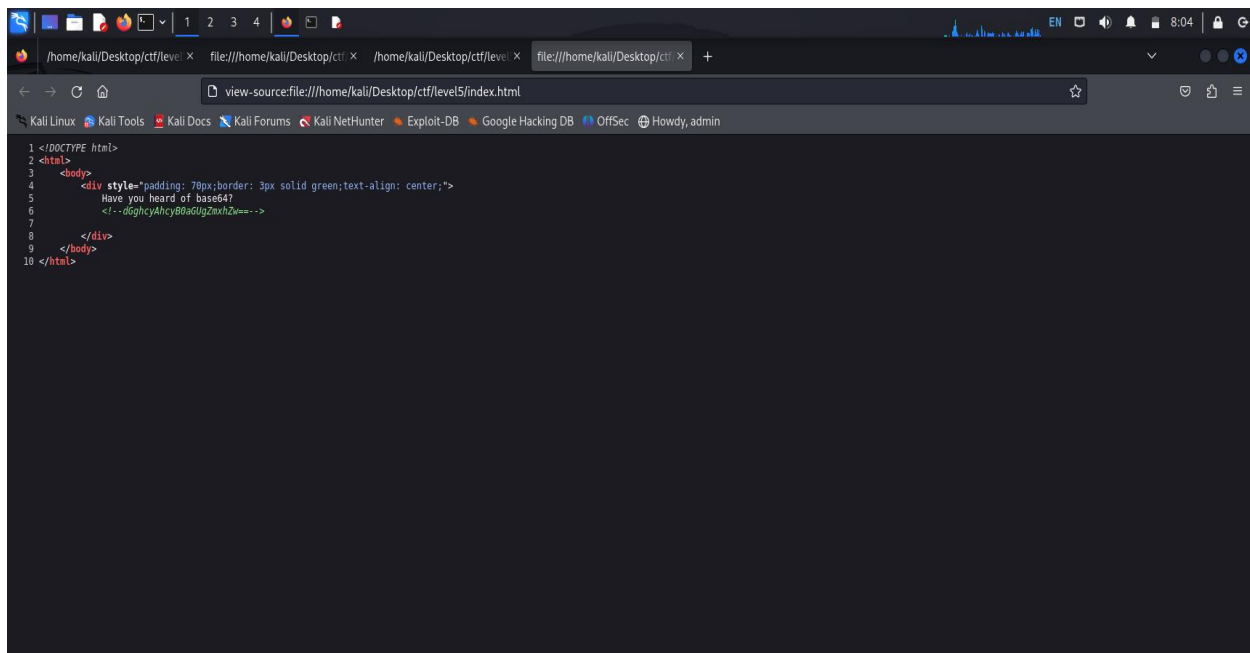
We can view source code from this page.



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

```
kali@kali: ~/Desktop/ctf/level5

File Actions Edit View Help

drwxr-xr-x 2 kali kali 4096 Mar 29 02:47 .
drwxr-xr-x 3 kali kali 4096 Mar 29 02:47 ..
-rw-r--r-- 1 kali kali 15 Mar 29 02:47 flag.txt

(kali@kali)~/Desktop/ctf/level4/s3cr3t$
$ chmod 777 flag.txt

(kali@kali)~/Desktop/ctf/level4/s3cr3t$
$ xdg-open flag.txt

(kali@kali)~/Desktop/ctf/level4/s3cr3t$
$ cd..
cd.: command not found

(kali@kali)~/Desktop/ctf/level4/s3cr3t$
$ cd ..

(kali@kali)~/Desktop/ctf/level4$
$ cd ..

(kali@kali)~/Desktop/ctf$
$ cd level5

(kali@kali)~/Desktop/ctf/level5$
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Mar 29 02:47 .
drwxr-xr-x 7 kali kali 4096 Mar 29 02:47 ..
-rw-r--r-- 1 kali kali 252 Mar 29 02:47 index.html

(kali@kali)~/Desktop/ctf/level5$
$ chmod 777 index.html

(kali@kali)~/Desktop/ctf/level5$
$ xdg-open index.html

(kali@kali)~/Desktop/ctf/level5$
$ echo 'dGhcyAhcyB0aGUGZmxhZw==' | base64 --decode
this is the flag

(kali@kali)~/Desktop/ctf/level5$
$
```

Final flag is found.