

1. What is this weird site? (100 points)

Go to the site. <https://mathurninaad.github.io/webexctf/>

Step 1) Changing the value of the cookie.

The screenshot shows a web browser with the LNMHacks site. The page has a blue header with "Welcome to LNMHacks!!!", a light blue bar with "Click me!" and "No! Click Me!", and a white body with an "Unlock the Flag" button and the text "First part of the flag: hacks{WH". The Application tab is open, showing the "Cookies" section for the URL "https://mathurninaad.github.io/webexctf/". A table lists cookies with the following data:

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Priority	Creation Time	Last Access Time
flagStatus	true	m...	/	2...	14						

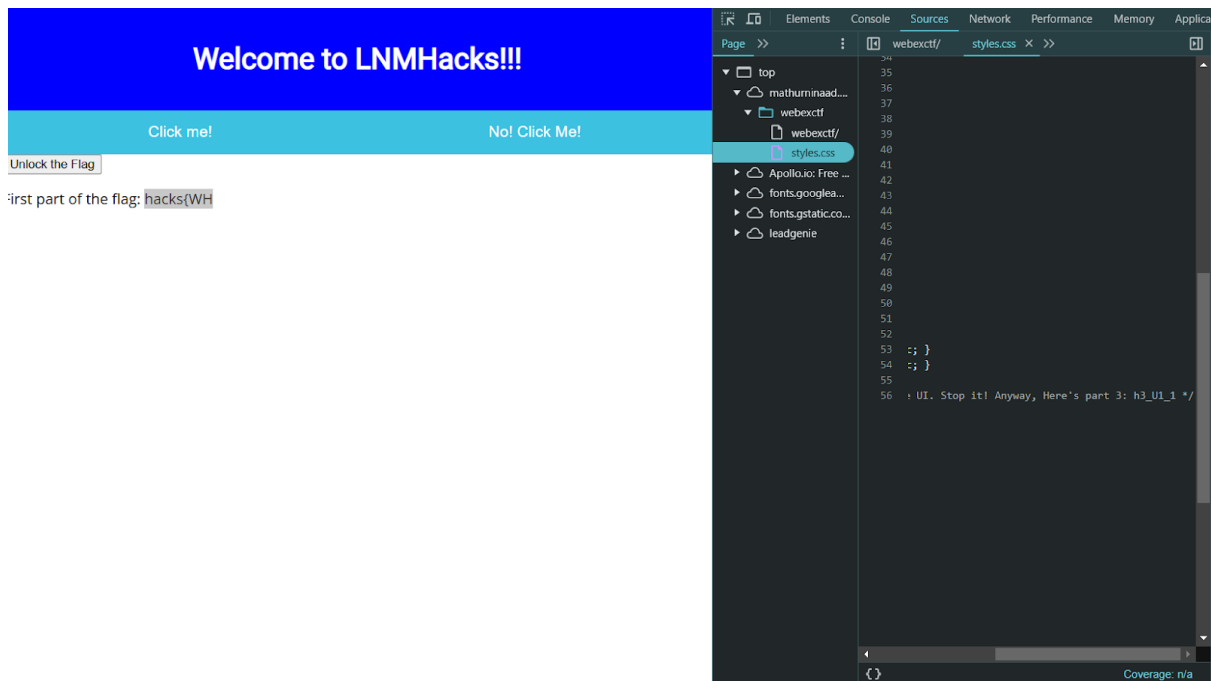
Step 2) Inspect the html part of the site.

The screenshot shows the same web browser with the LNMHacks site. The "webexctf" directory is selected in the browser's file explorer. The "Sources" tab is open, showing the HTML code of the page. The code is as follows:

```
</head>
45
46
47
48 <div class="container">
49   <header>
50     <h1>Welcome to LNMHacks!!!</h1>
51   </header>
52
53   <button class="tablink" onclick="openTab('t
54   <button class="tablink" onclick="openTab('t
55
56   <div id="tabintro" class="tabcontent">
57     <h3>Click me!</h3>
58     <p>Don't criticize the UI!</p>
59   </div>
60
61   <div id="tababout" class="tabcontent">
62     <h3>No! Click Me!</h3>
63     <p>You can find these <br />
64     HTML <br />
65     CSS <br />
66     JS (JavaScript)
67   </p>
68   <!--second part of the flag: 00_t -->
69 </div>
70
71   <div>
72     <button onclick="unlockFlag()">Unlock the
73     <p id="flagPart1" style="display: none;">
74   </div>
75 </div>
76 </body>
77 </html>
78
```

You'll get the second part of the flag here.

Step 3) Inspect the css file.



Step 4) Go to the hidden script.js file with the help of the hint in the html file.

```
// Function to get a cookie value
// Where is the other script?
```

script.js

```
function openTab(tabName,elmnt,color) {
    var i, tabcontent, tablinks;
    tabcontent = document.getElementsByClassName("tabcontent");
    for (i = 0; i < tabcontent.length; i++) {
        tabcontent[i].style.display = "none";
    }
    tablinks = document.getElementsByClassName("tablink");
    for (i = 0; i < tablinks.length; i++) {
        tablinks[i].style.backgroundColor = "";
    }
    document.getElementById(tabName).style.display = "block";
    if(elmnt.style != null) {
        elmnt.style.backgroundColor = color;
    }
}

window.onload = function() {
    openTab('tabintro', this, '#222');
}

/* I don't want google to index my website. Please help me with that!!!! Yup! I'm still learning*/
```

Step 5) Go to robots.txt using the previous hint. This points to .htaccess

Content of .htaccess

```
# Part 5: g_R1ght_  
# You know just use the flag created so far, and find something good
```

Step 6) Go to the url containing the flag created so far.

https://mathurninaad.github.io/webexctf/hacks%7BWHOO_th3_U1_1s_4m4zing_R1ght_

Here, you'll find the last part of the flag

```
(data (i32.const 1024) "HAHAHAHA Final Part: gu7${?}}\00\00")
```

Final Flag: hacks{WHOO_th3_U1_1s_4m4zing_R1ght_gu7\${?}}