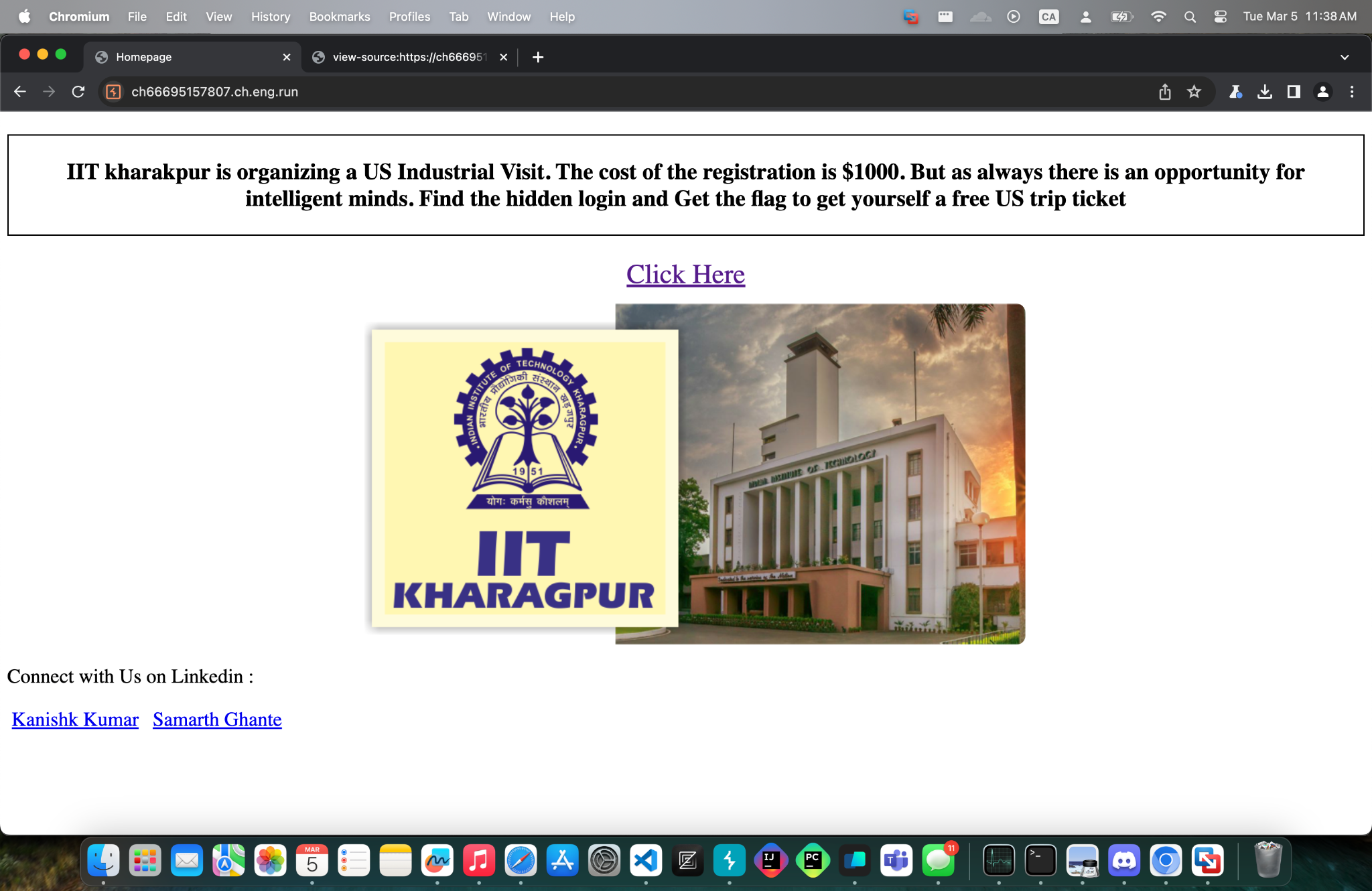
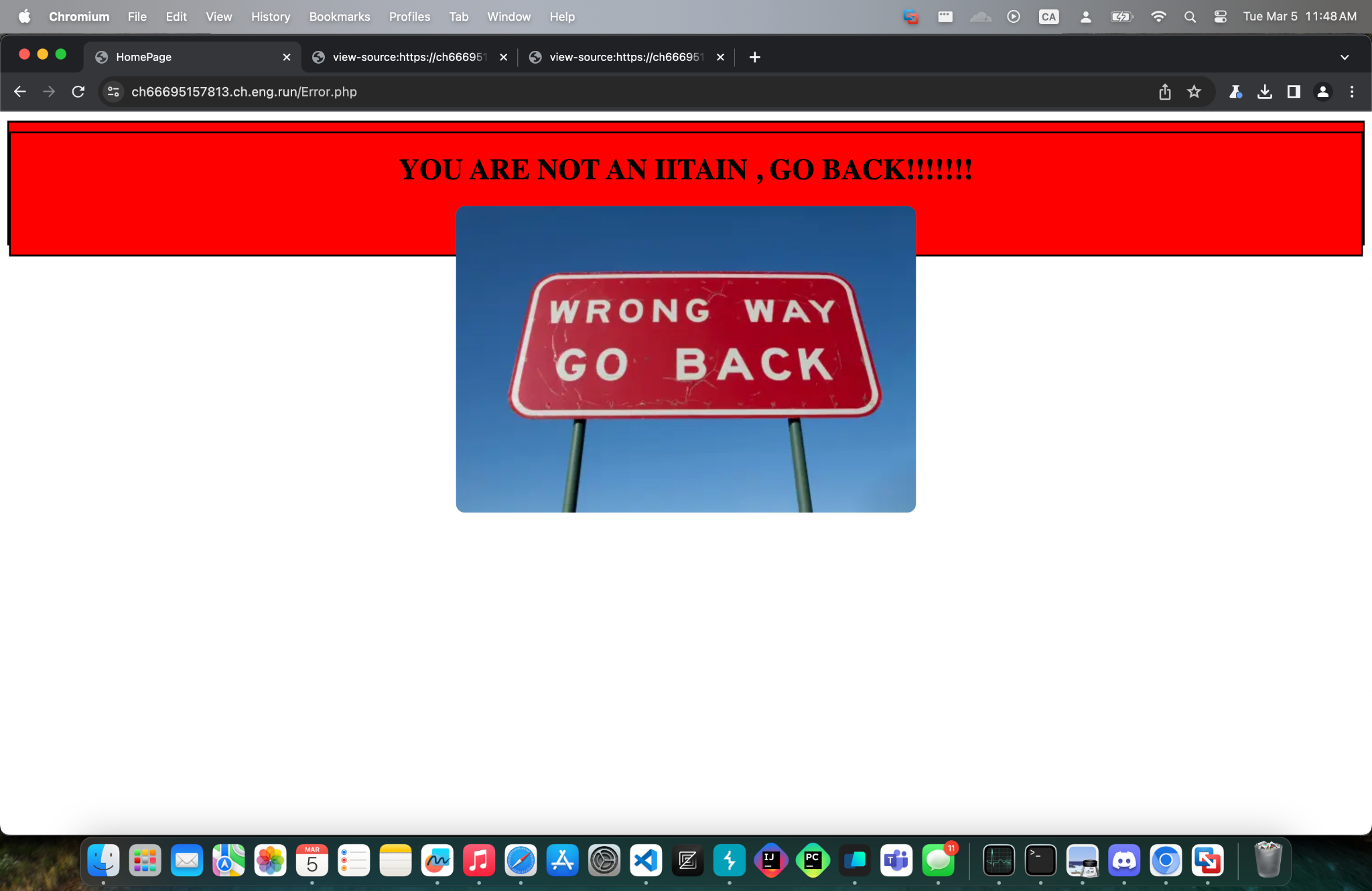
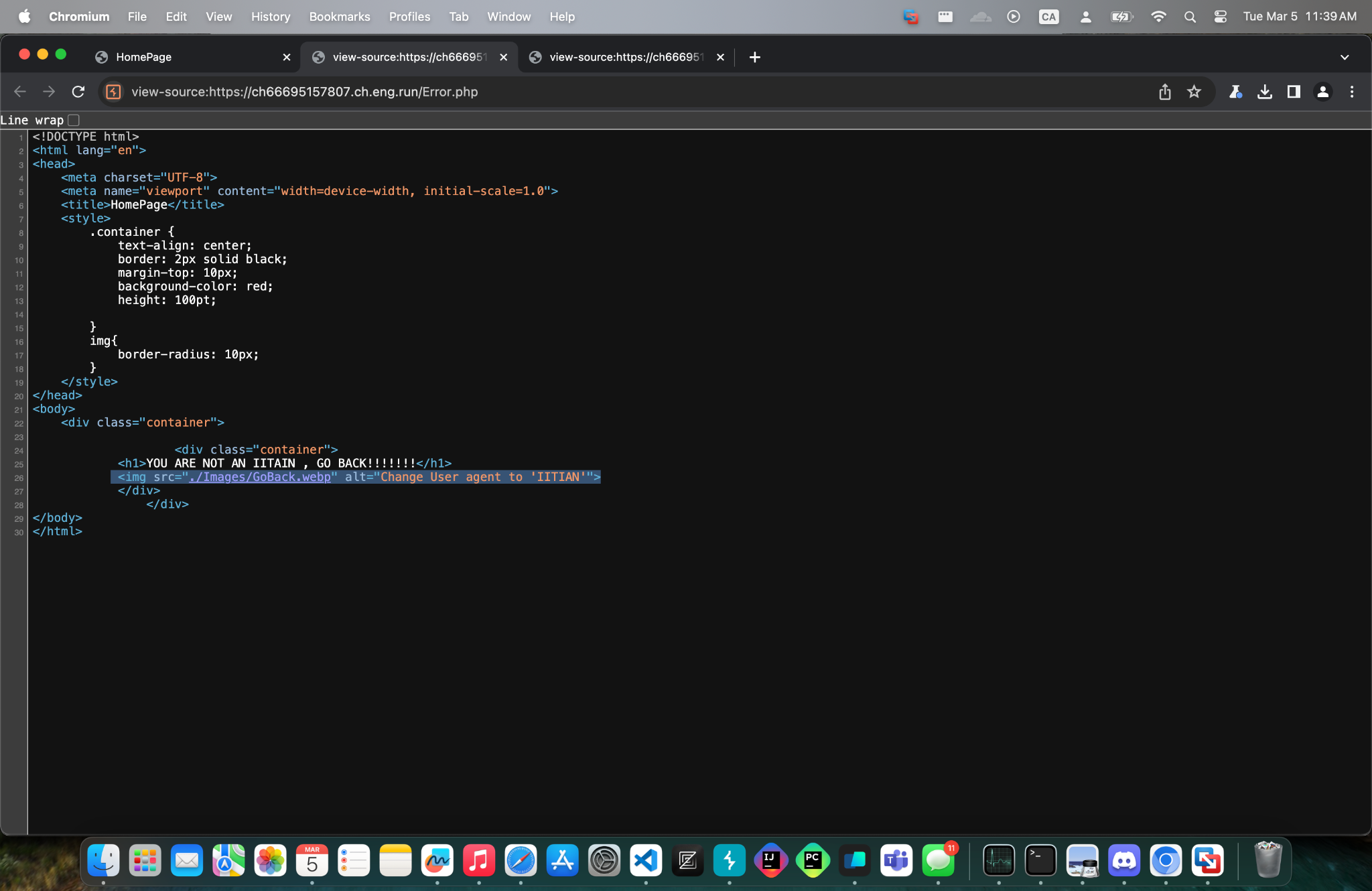
Trip to us

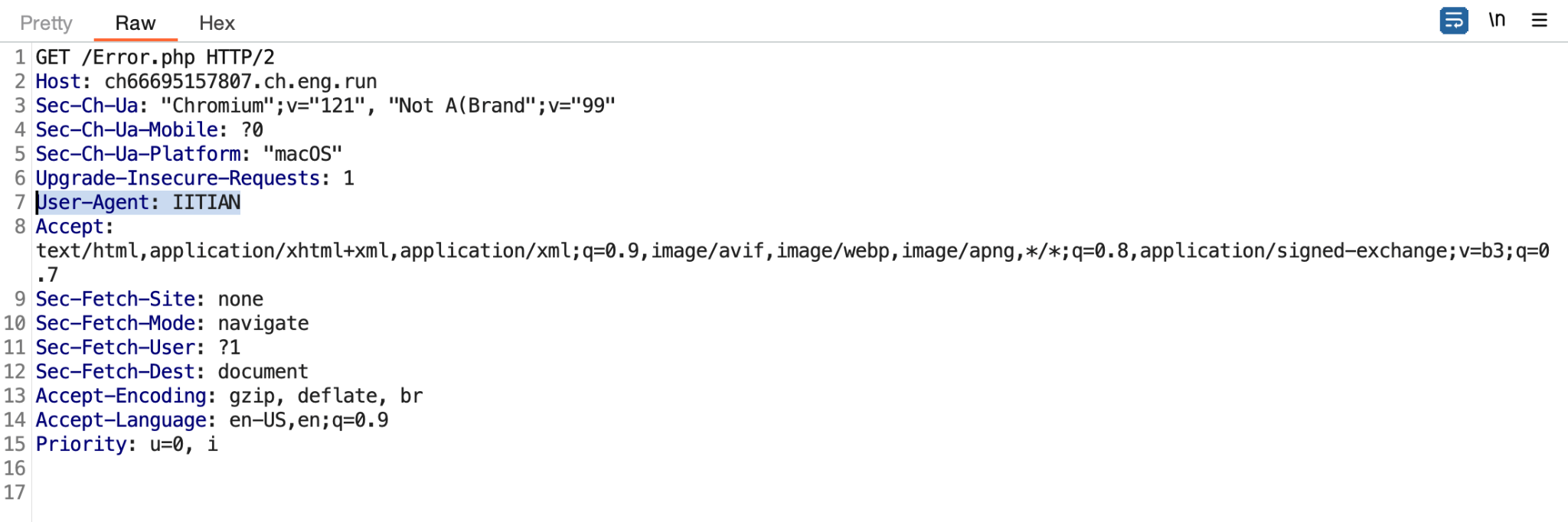


We’re given a website for a US Industrial Visit. Noticing right away there’s a “Click Here” button, and I proceeded to click on that.

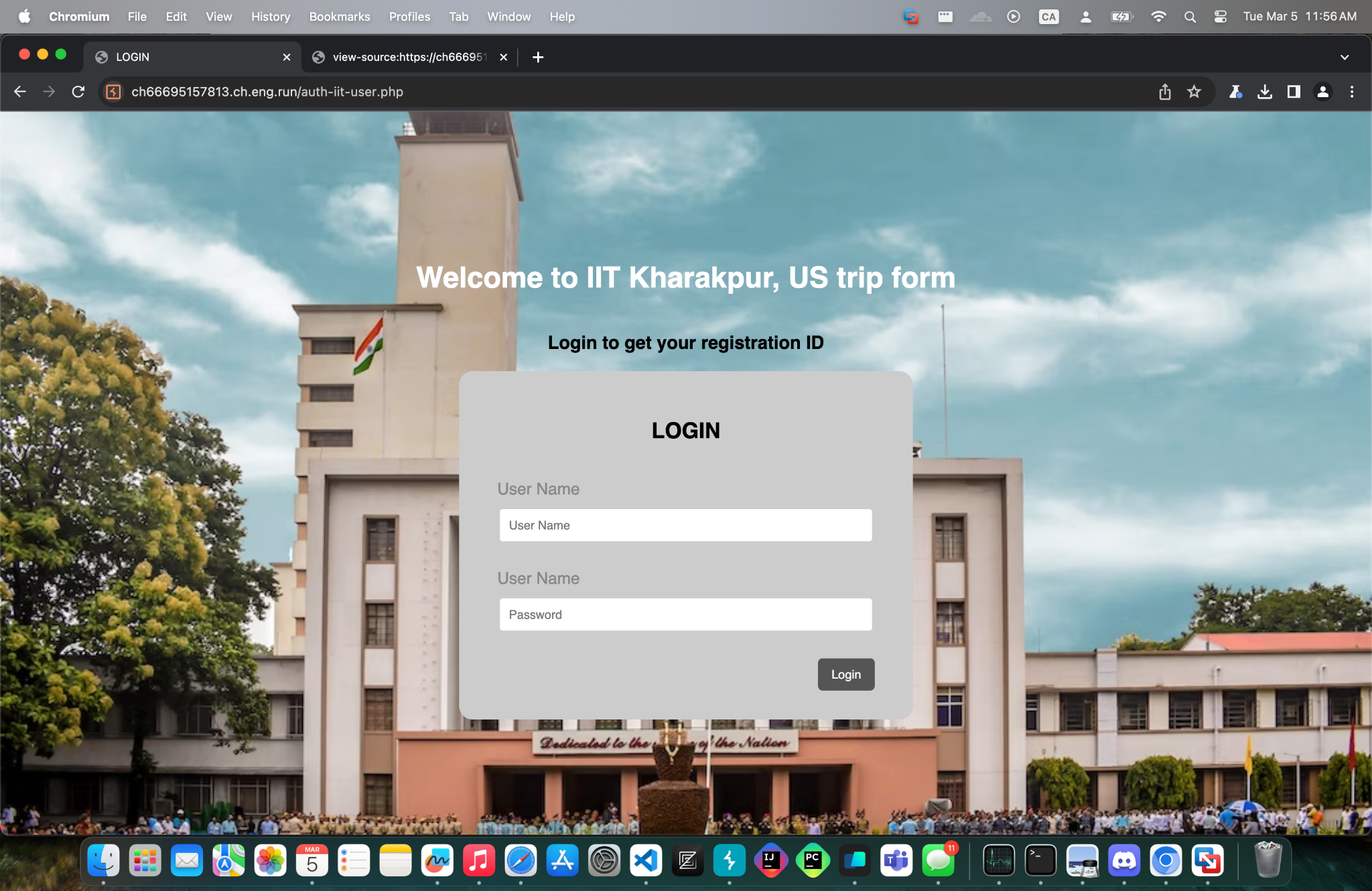


After clicking on the button, I got redirected to this error page. Immediately, I opened up the page-source to have a further inspection.

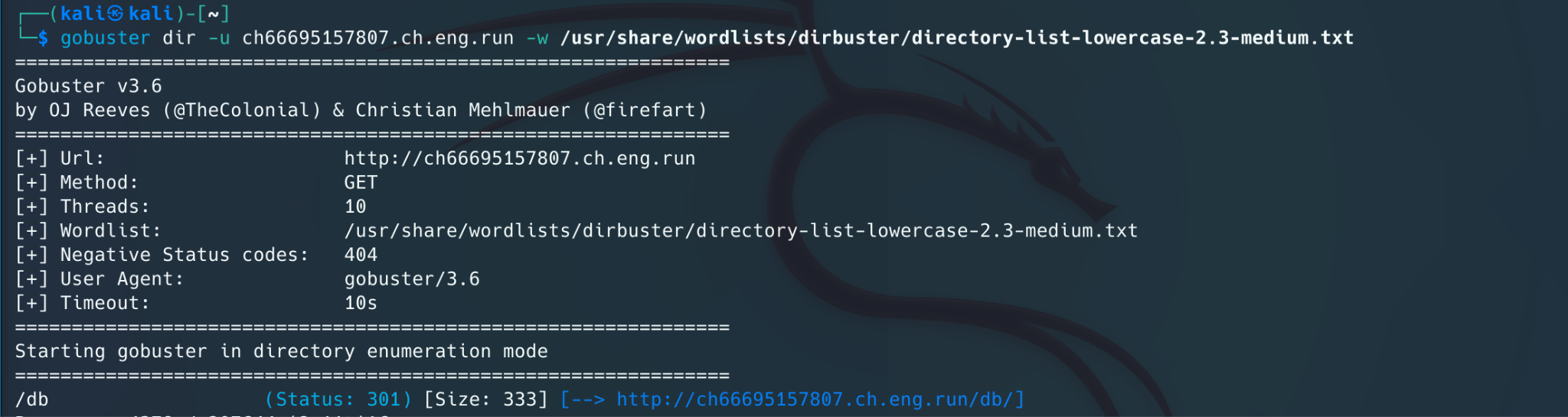
Right here I see a tag with an alternative parameter with the text “Change User agent to ‘IITIAN’”.



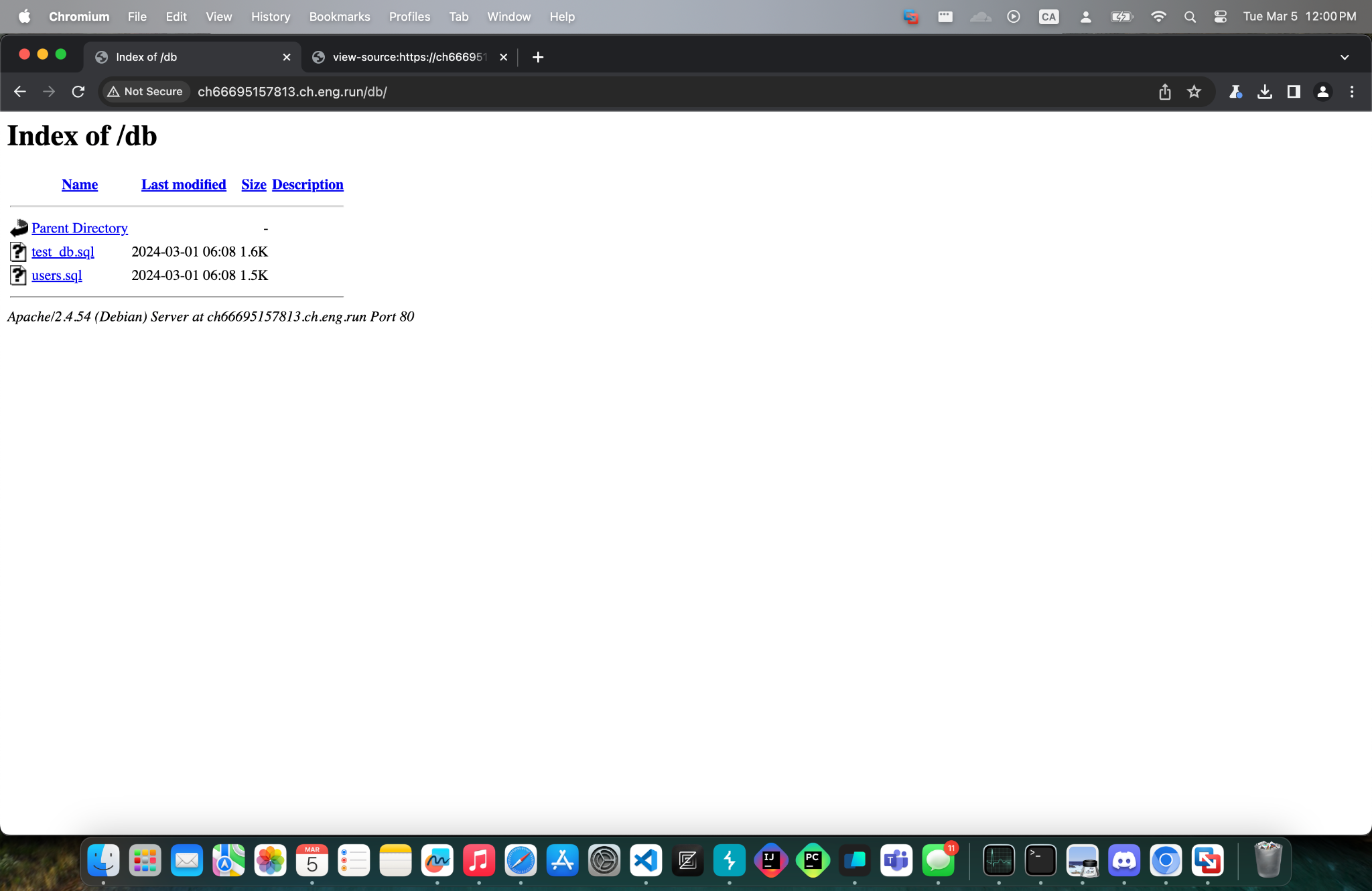
Then I went to Burp to change the “User-Agent:” to IITIAN.



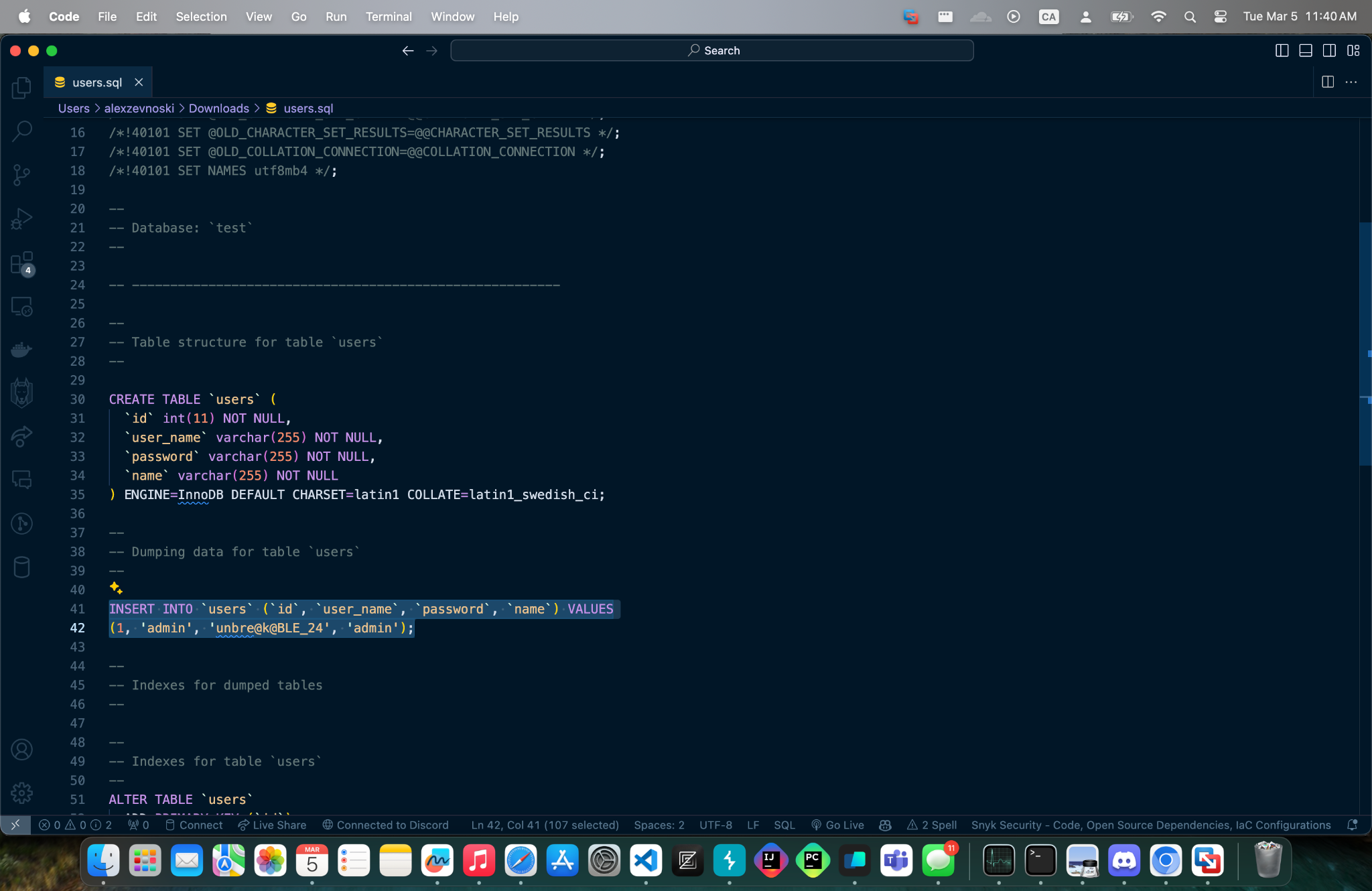
I changed the user agent in Burp and I was successfully redirected to this login page. Without any further information that I could use from the page-source and since this is a black-box challenge, directory brute-forcing is one of the most common methods to use in case.



After running gobuster for a while, I saw that the /db directory end point revealed at the end.



Visiting the end point, there are 2 files that look really interesting so I downloaded the user.sql first to examine what’s in there.



I opened up the file and saw the plain text credentials of the admin. Using the information in the downloaded database, I was able to login and retrieve the flag.

**FLAG:** VishwaCTF{y0u\_g0t\_th3\_7r1p\_t0\_u5}

