Name: Sameed Ahmed Siddiqui

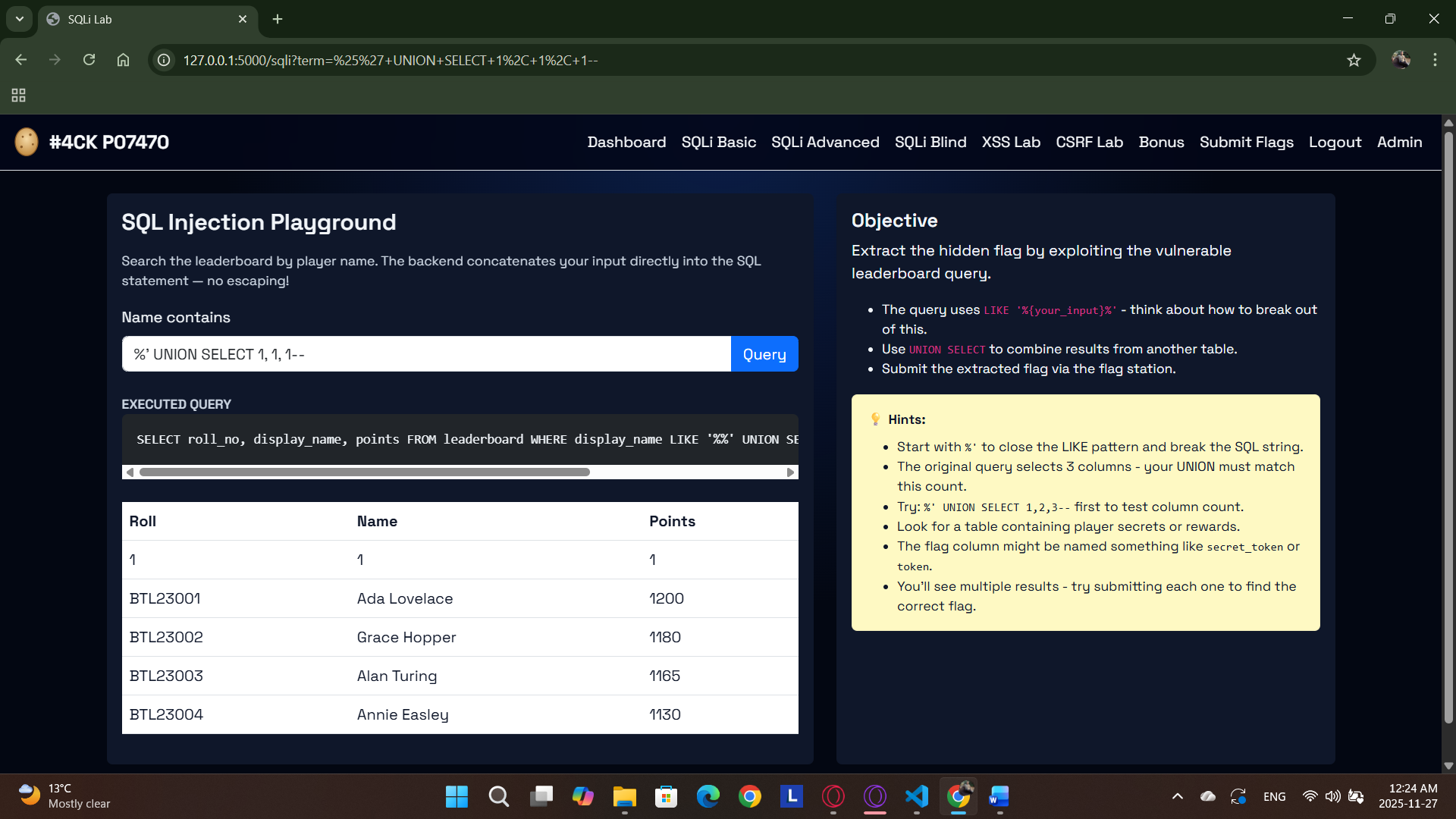
Section: 7B

Roll-no: 22i-8223

Course: Information Security

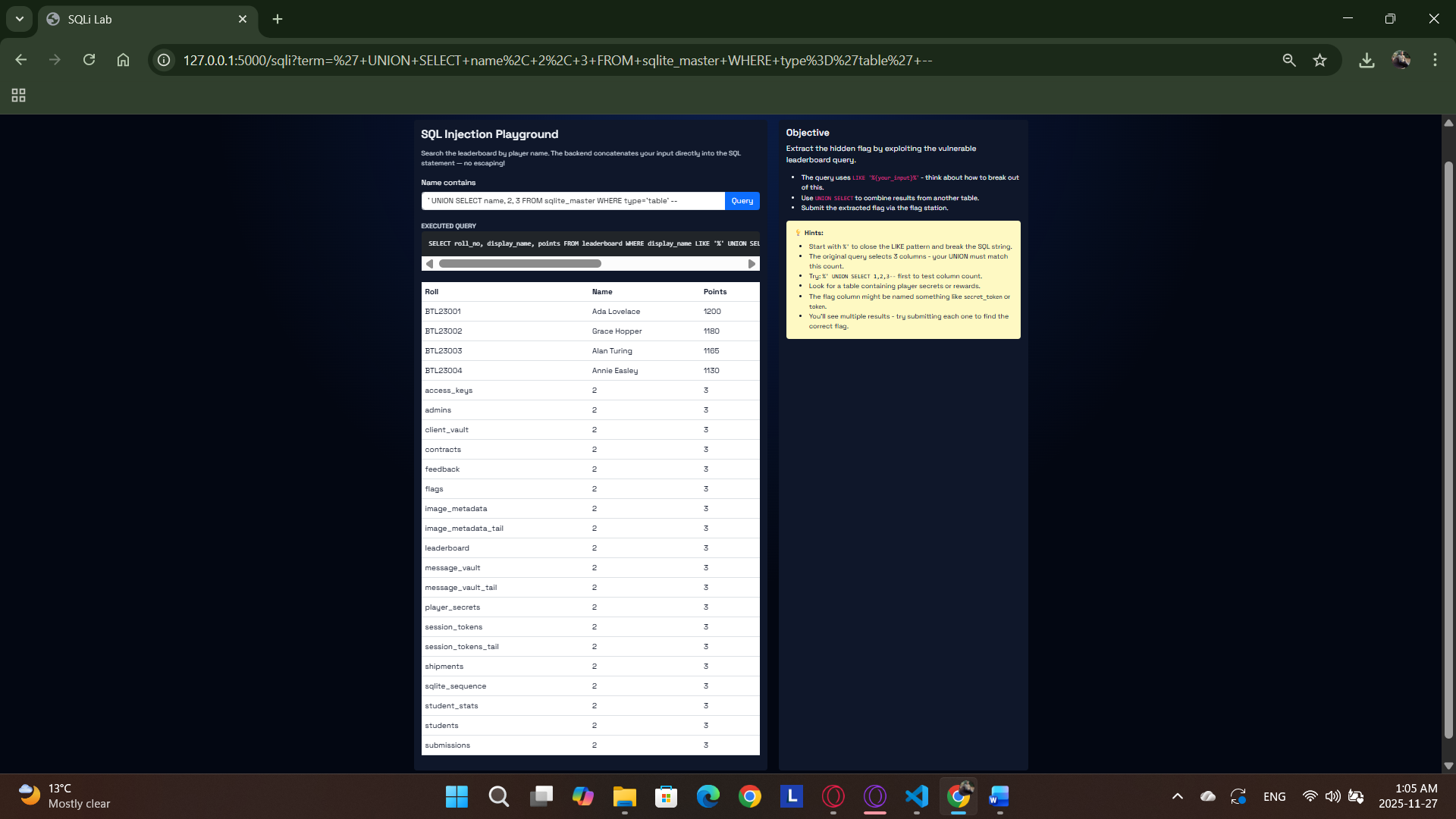
Q1)

Screenshots:



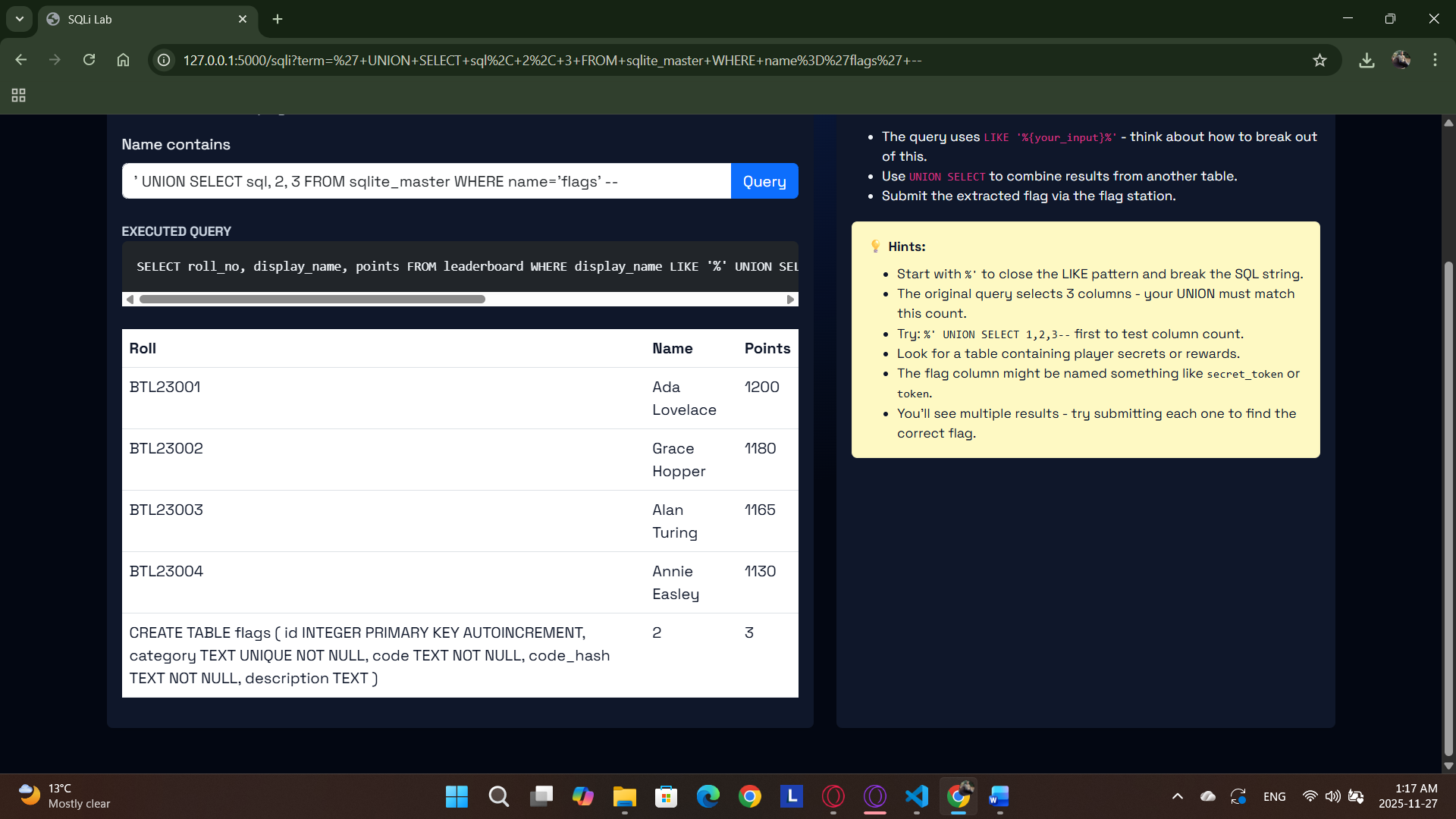
Sameed Ahmed Siddiqui

22i-8223



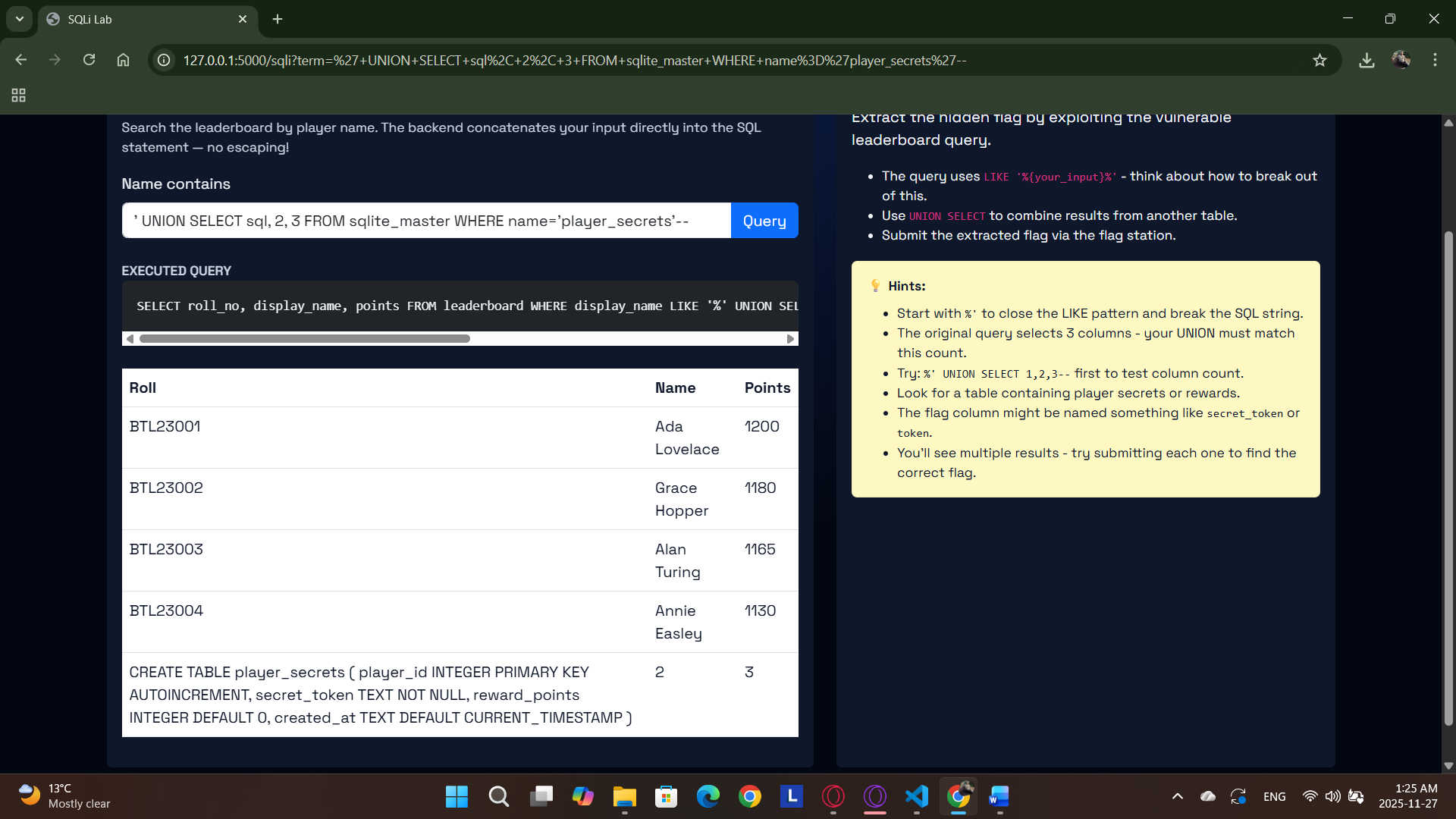
Sameed Ahmed Siddiqui

22i-8223



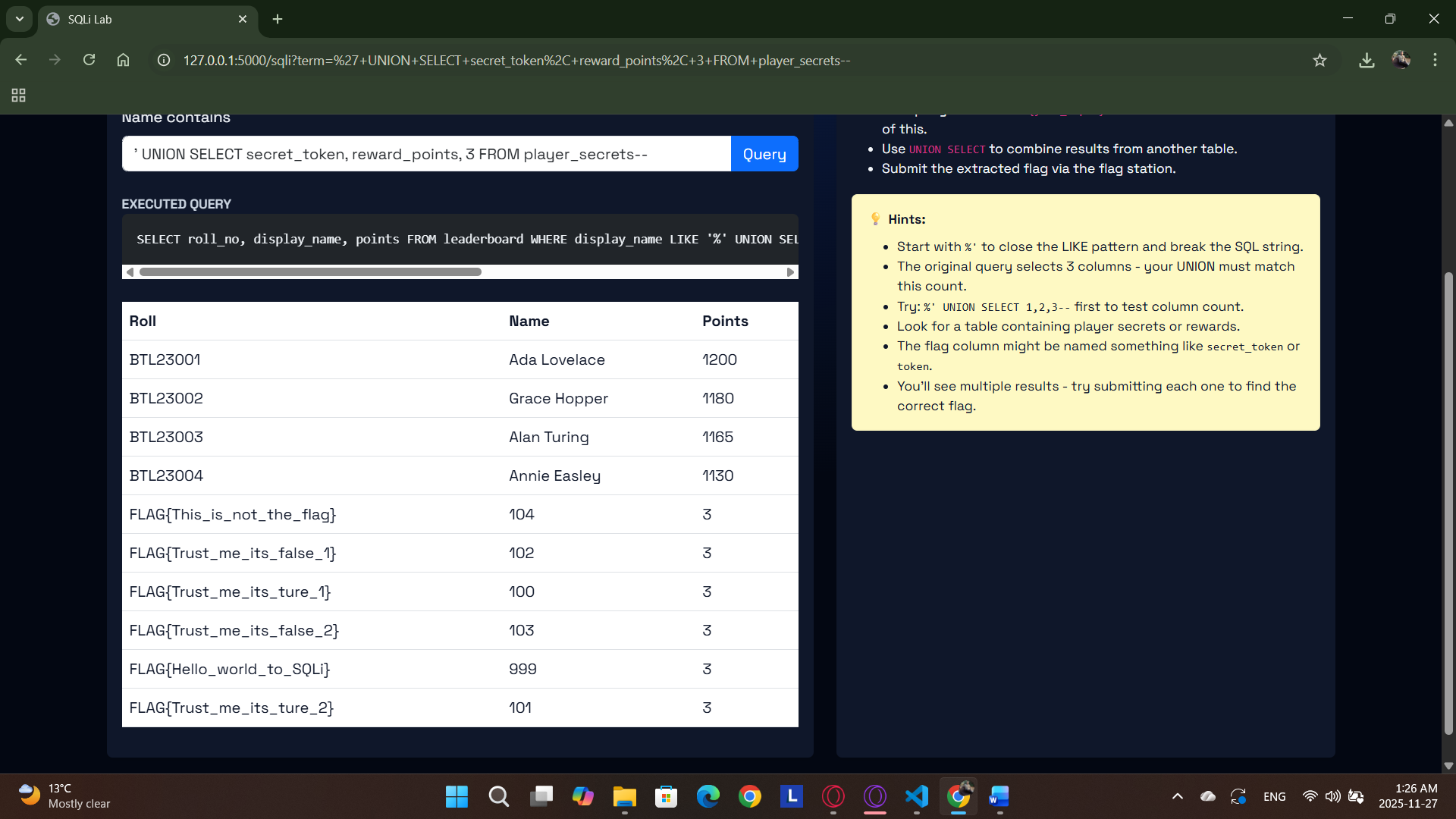
Sameed Ahmed Siddiqui

22i-8223



Sameed Ahmed Siddiqui

22i-8223



Sameed Ahmed Siddiqui

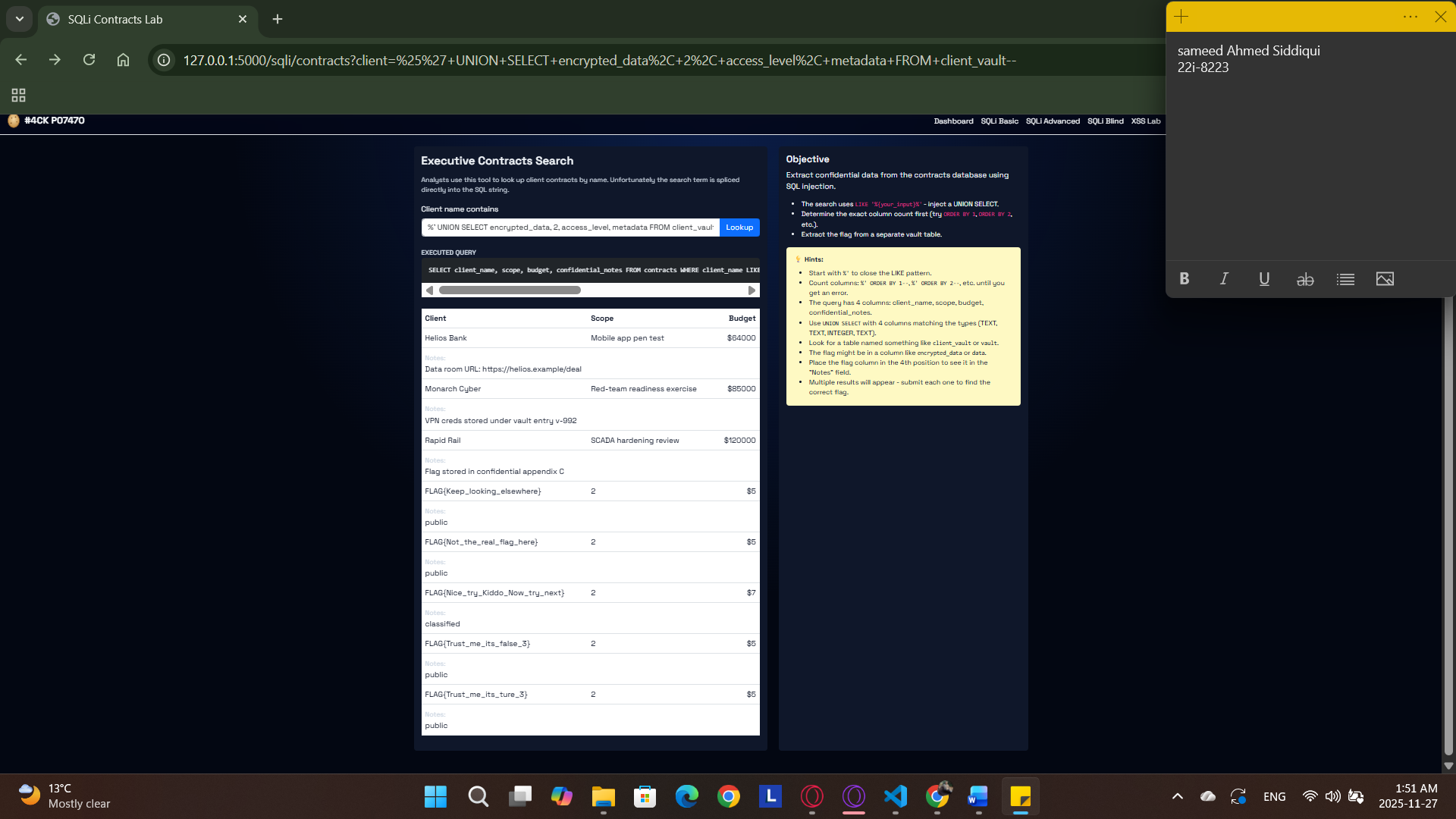
22i-8223

Used UNION SELECT 1, 1, 1 – to confirm col num. Then used sqlite\_master to get table names and then the structure of table. After that used reward points and secret token to find the flag in table player secrets.

Q2)

Screenshots:

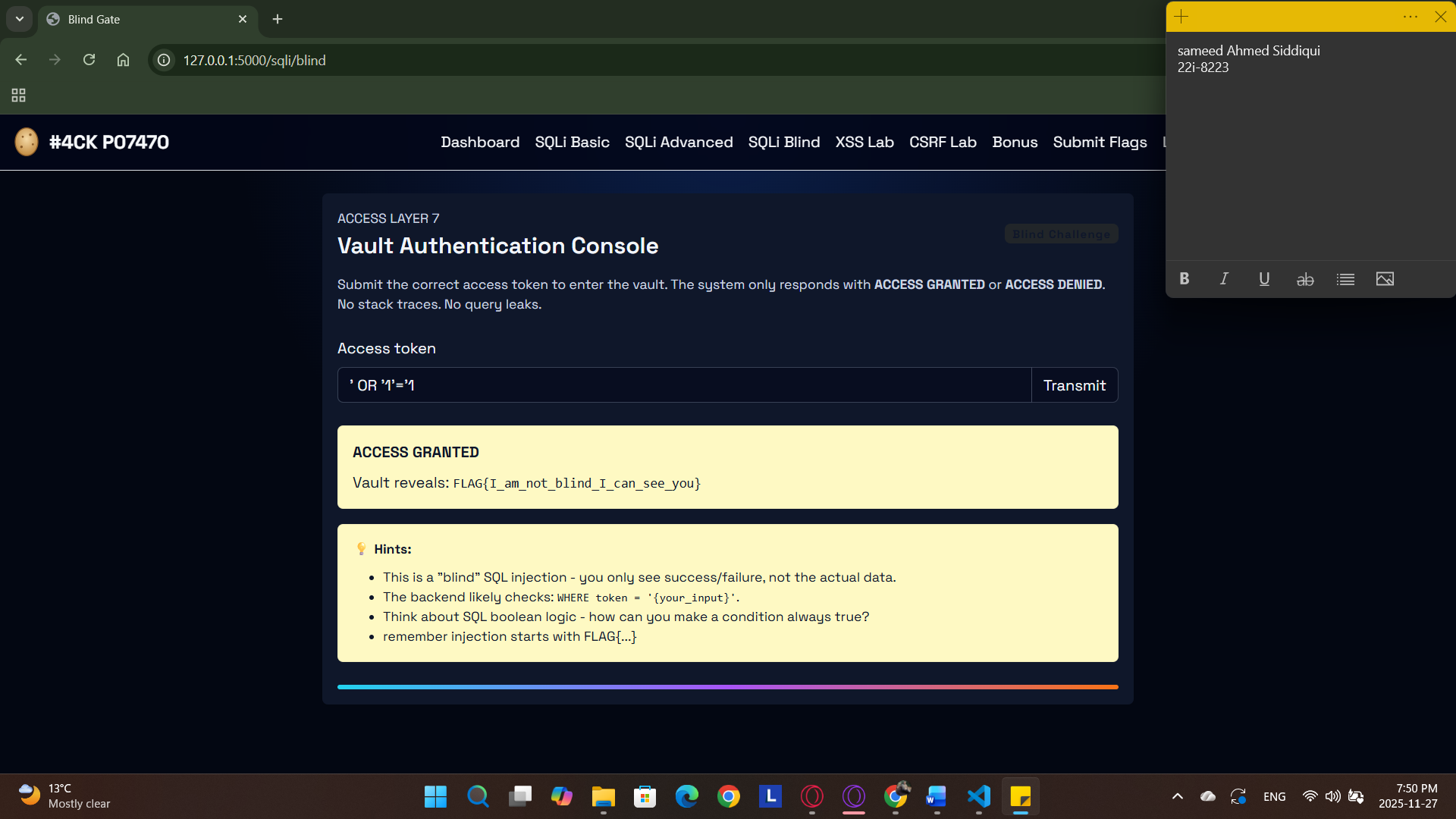




Used sqlite\_master to get table names and structure of client\_vault table, after that used the columns found to find the hidden flag.

Q3)

Screenshots:

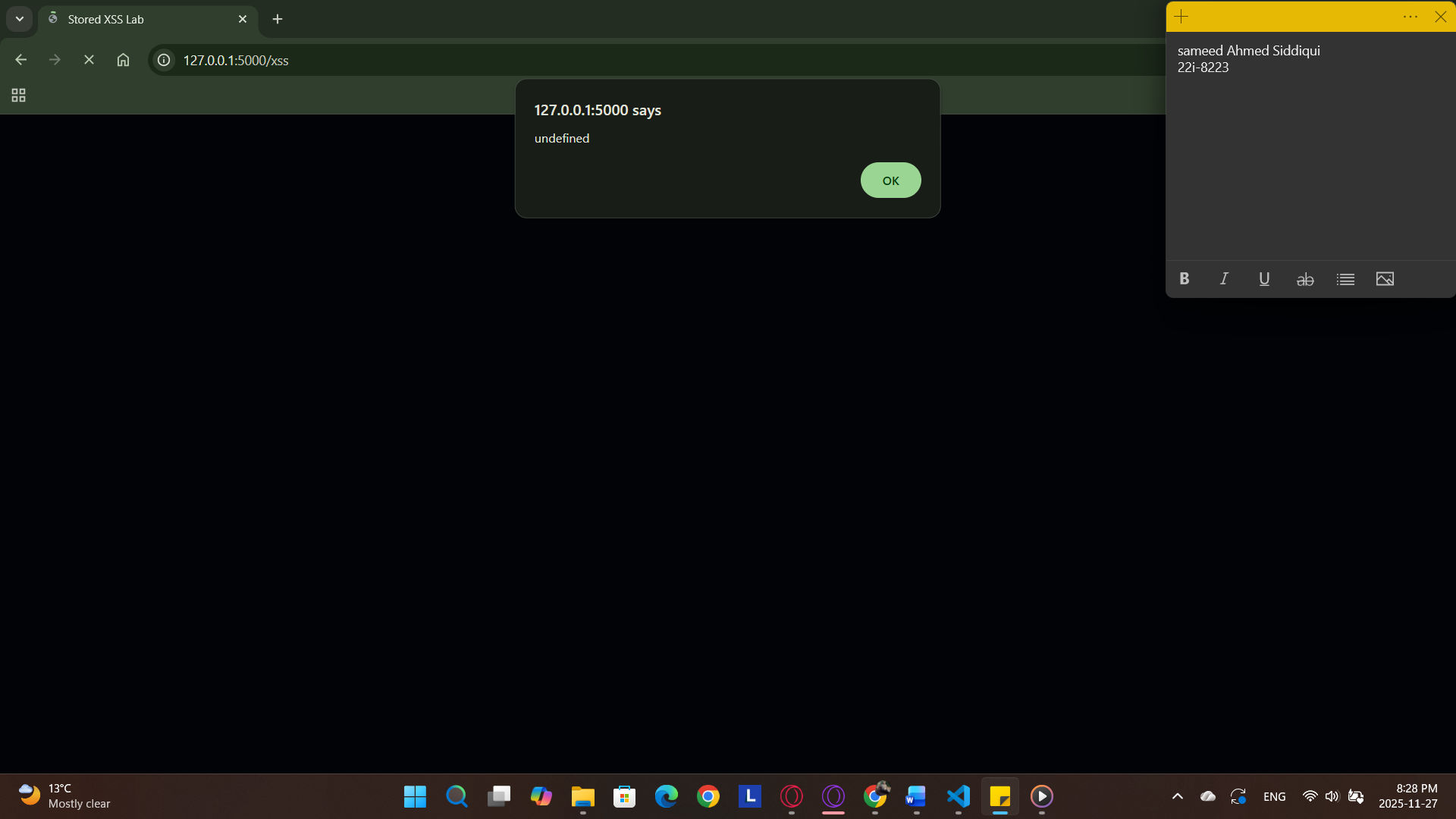


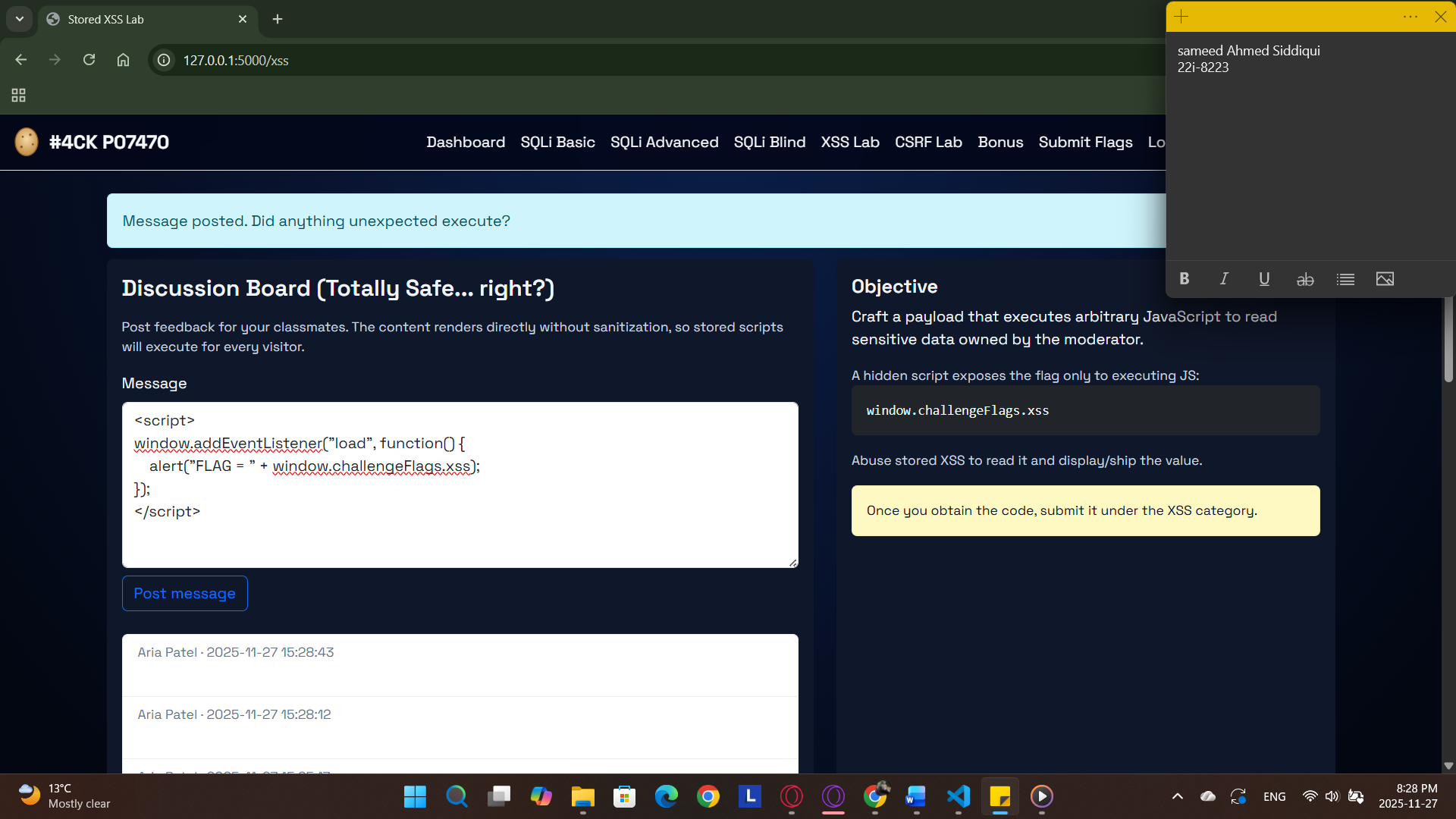
Used a simple Boolean query with one open quote at end to take into account the query used. Tried multiple queries to get access. The query ending with ‘--’ do not work as query breaks.

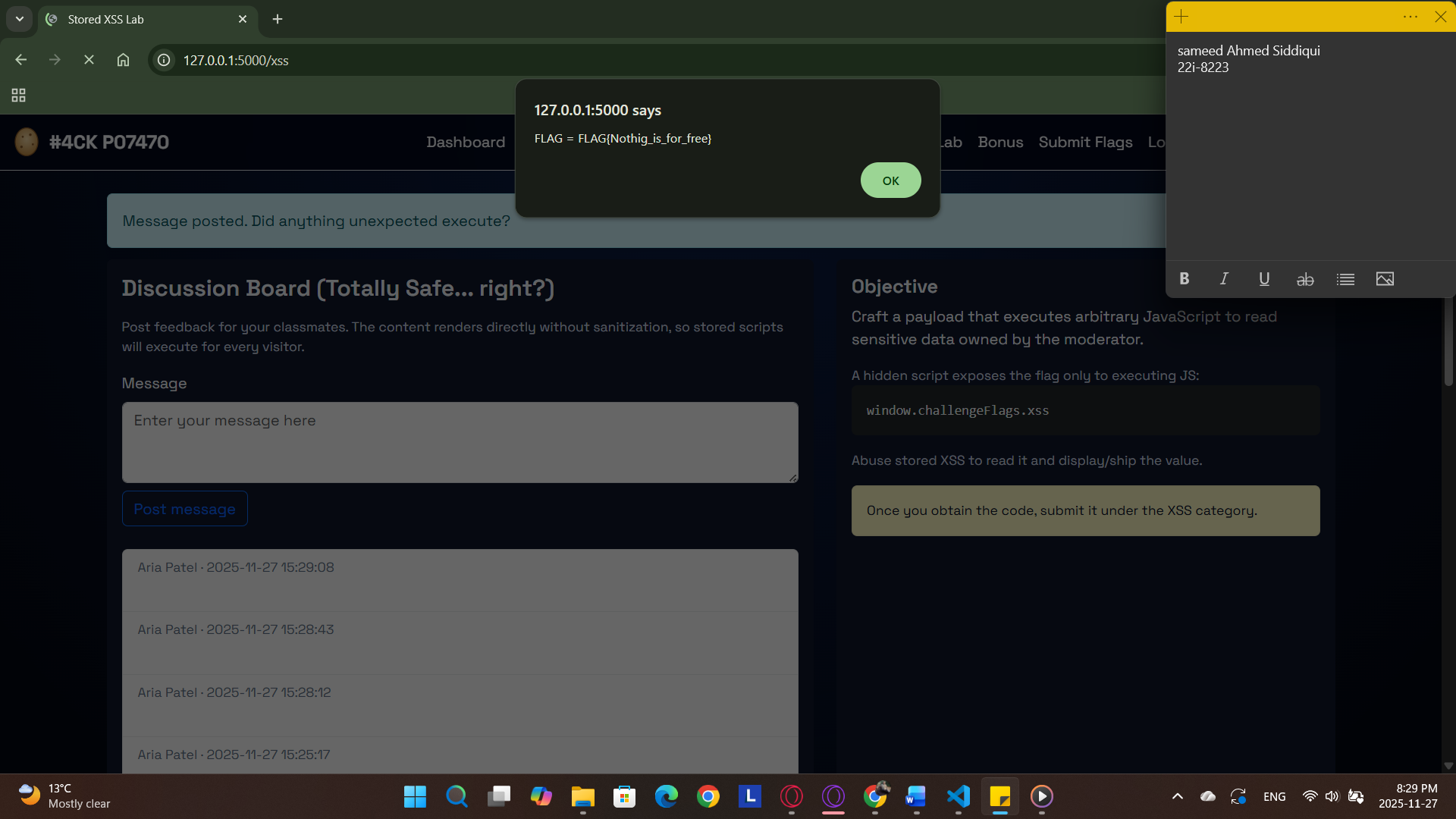
Q4)

Screenshots:





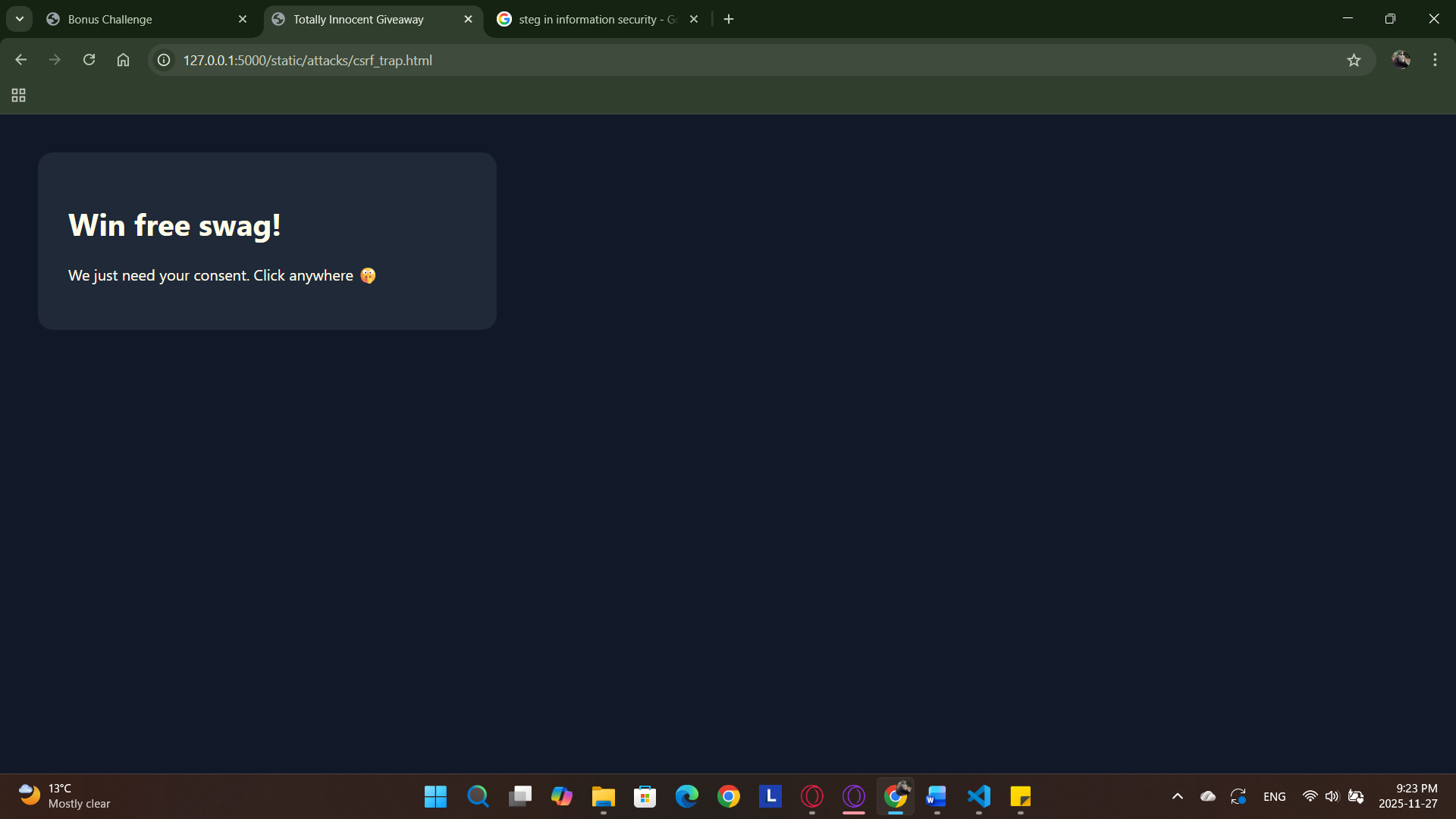




First created a script for this to get the window.challengeFlags.xss and pop it in an alert. The problem faced was the alert popped before the page loaded. To counter this added an event listner to only get the flag after page loaded.

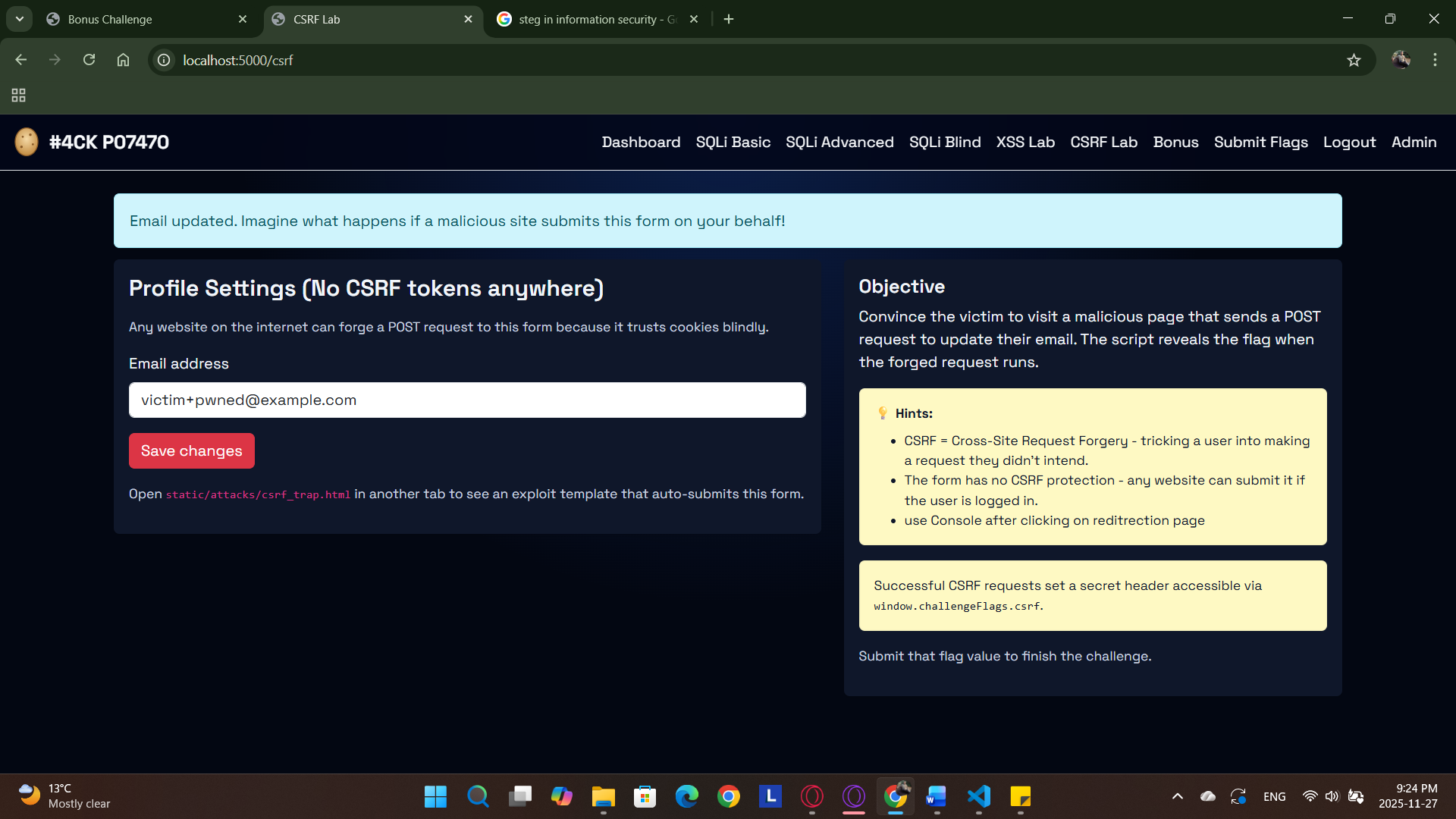
Q5)

Screenshots:



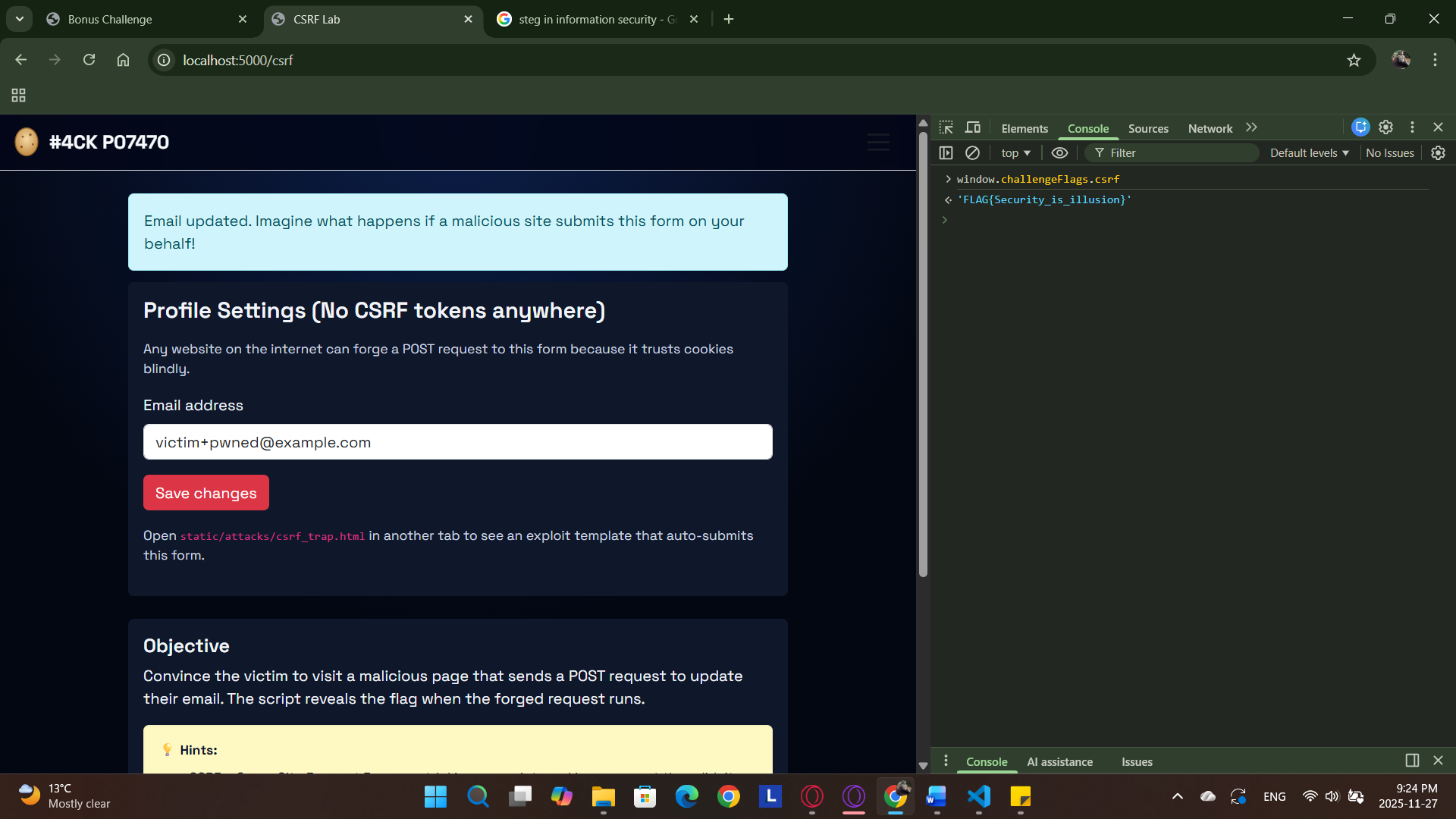
Sameed Ahmed Siddiqui

22i-8223



Sameed Ahmed Siddiqui

22i-8223



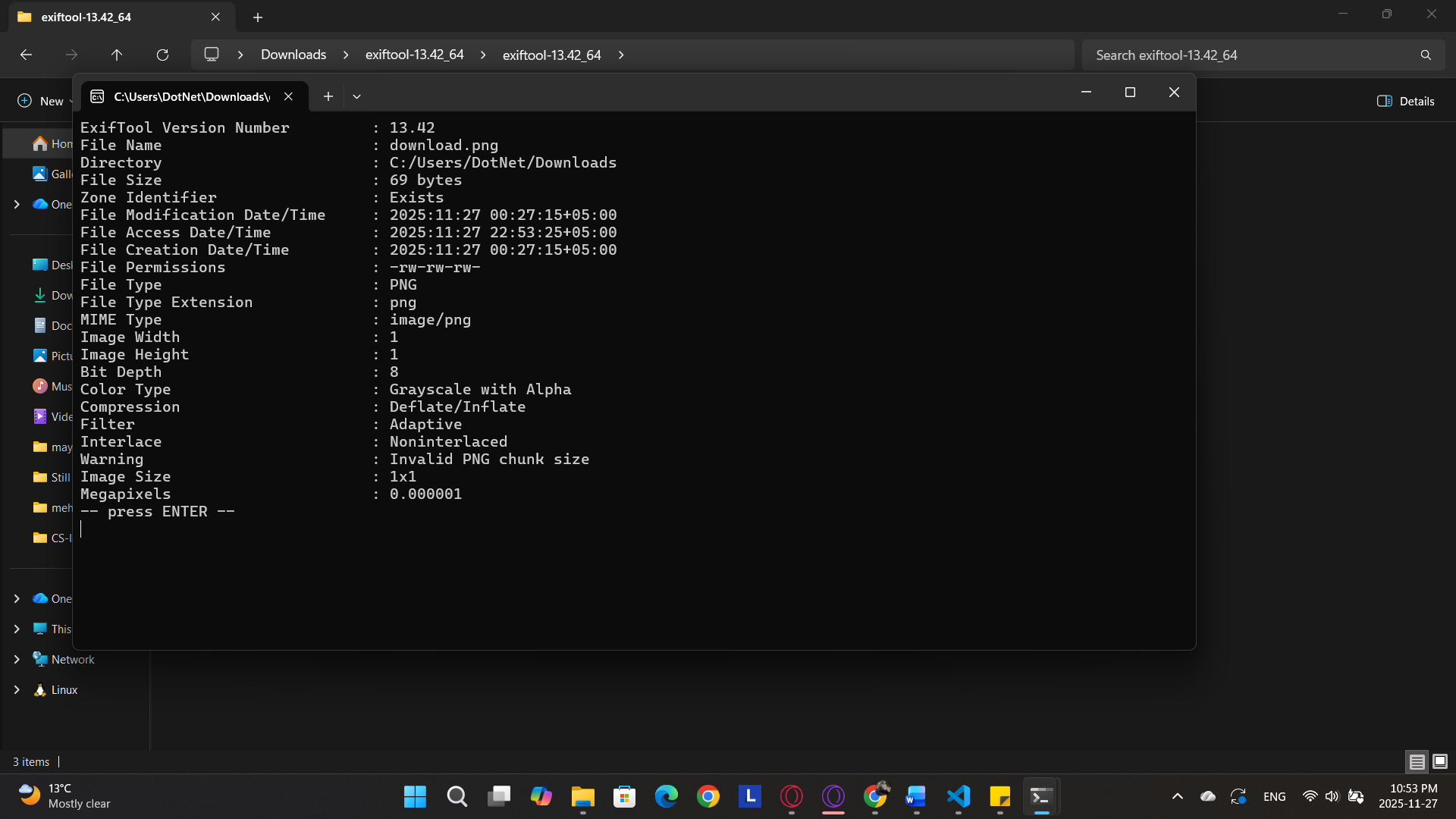
Sameed Ahmed Siddiqui

22i-8223

In a separate browser tab, I opened the csrf\_trap.html file. After clicking I was prompted to login, after logging in re entered the same URL and clicking anywhere, I used console to get the csrf flag.

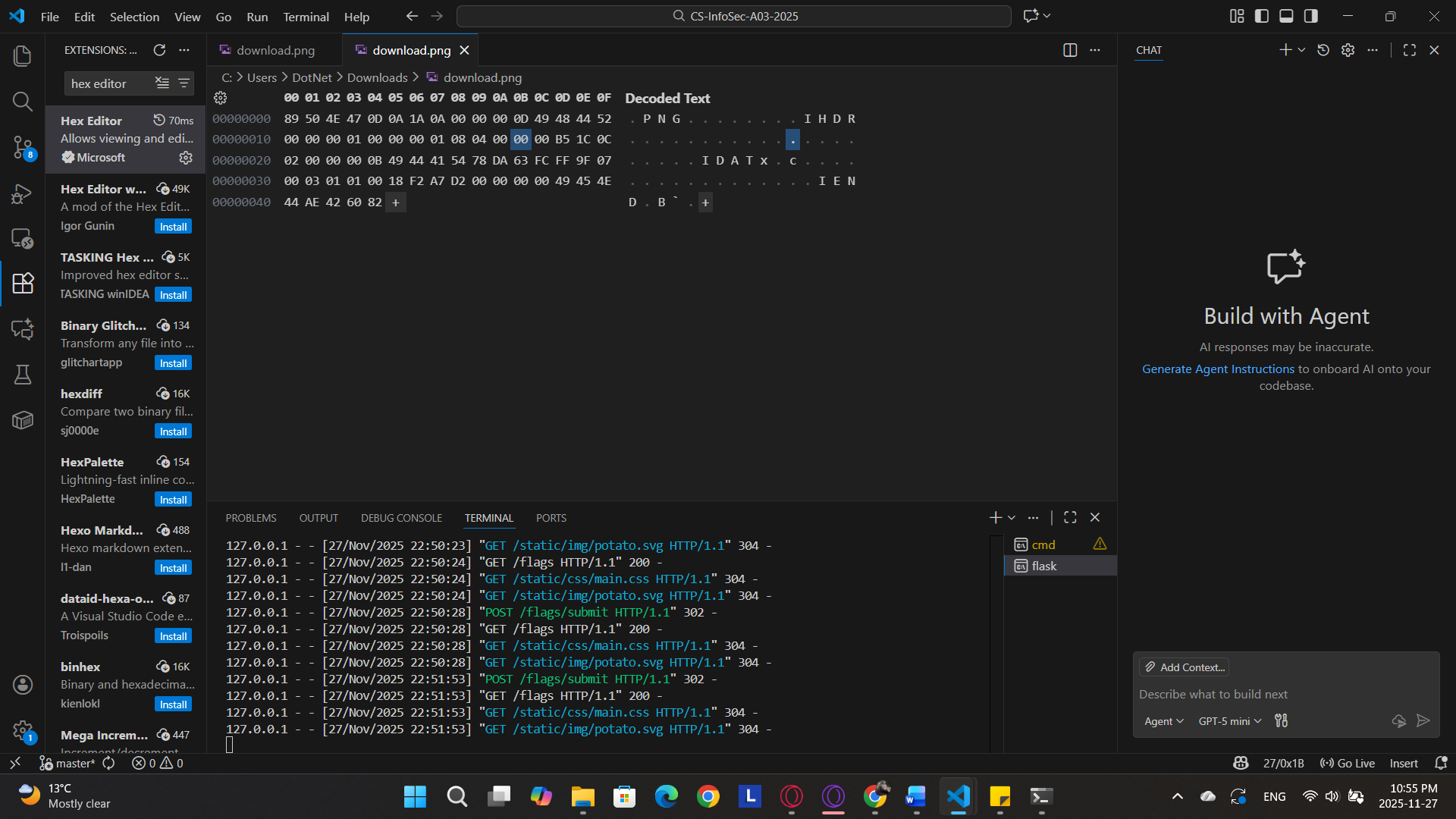
Q6)

Screenshots:



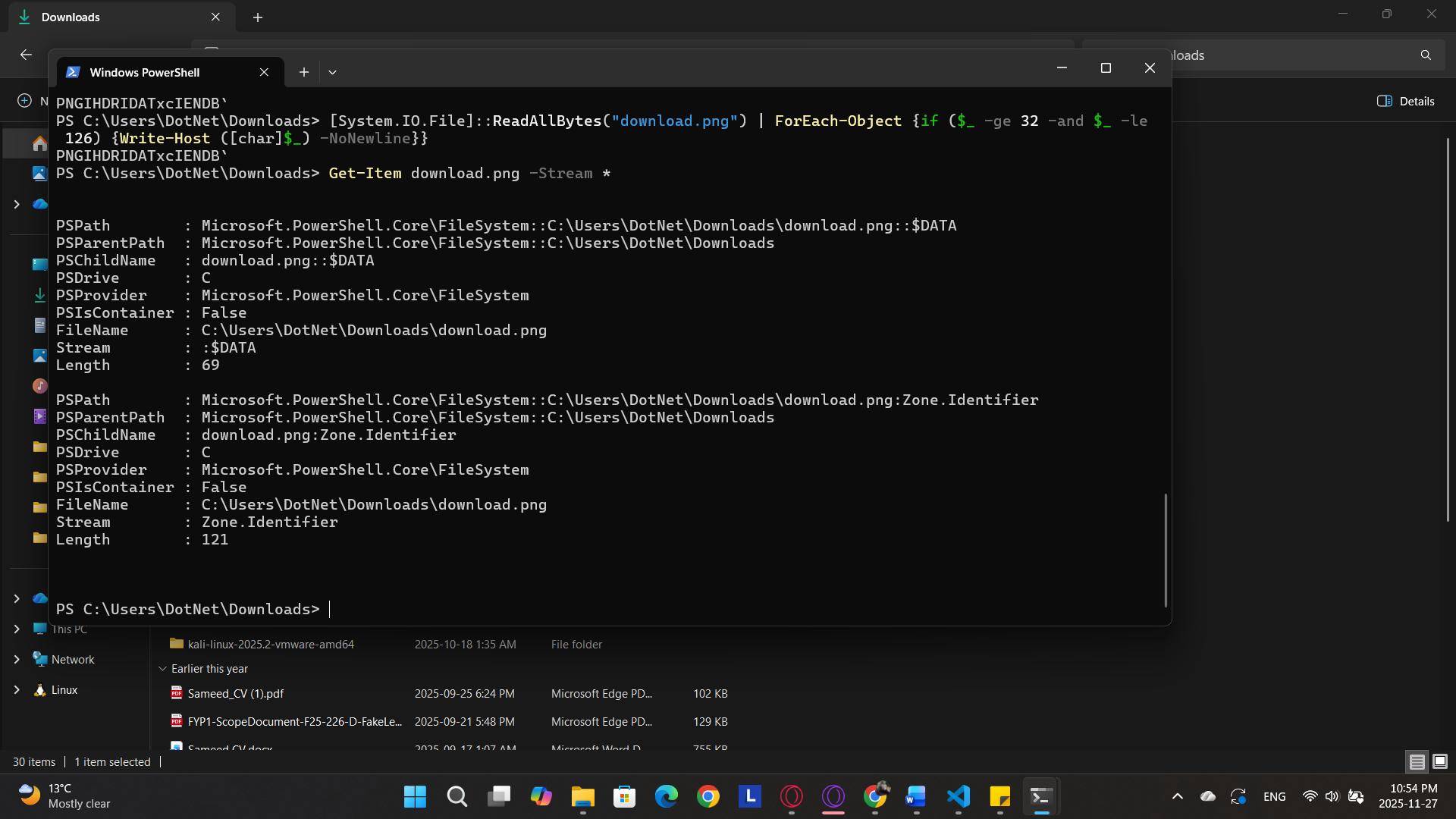
Sameed Ahmed Siddiqui

22i-8223



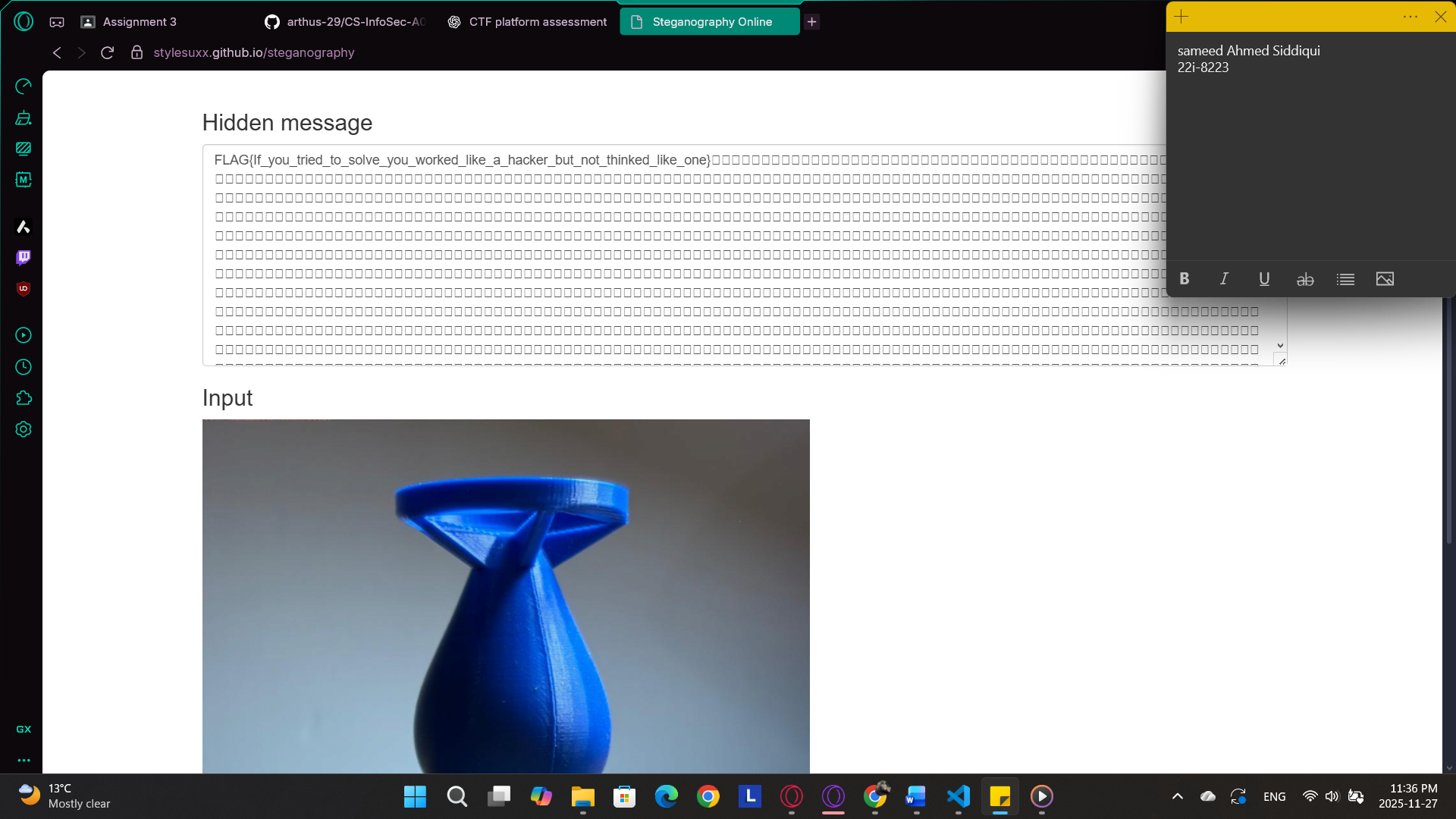
Sameed Ahmed Siddiqui

22i-8223



Sameed Ahmed Siddiqui

22i-8223



Downloaded the image from bonus window, after that used exifool and hex extension in vscode to try to find the flag. However, after multiple effort came to conclusion that the image downloaded was a red hearing, then used an online steg tool to find flag in a different image(‘Bomb.png’), found the flag in that image.