

Dylan Ramdhan

CS 357, Prof. Goldberg

Login Authentications Challenges: Challenge 5

Nov 3, 2023

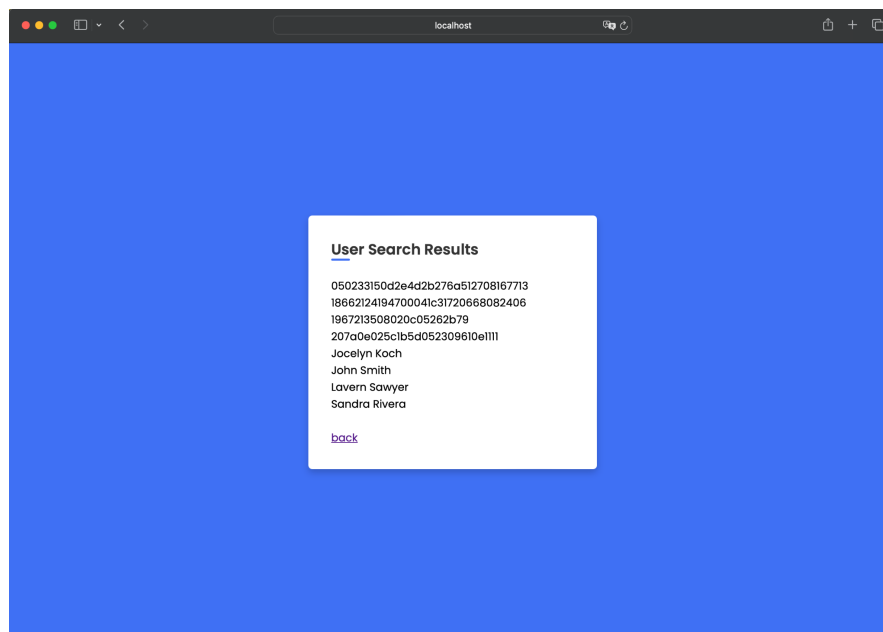
Login Authentication Challenges Report: Challenge #5

Step #1:

When conducting this challenge, I realized that I must register first, find the decryption of my own password, and apply this to find the credentials of the admin's login information. To first initialize the beginning of the attack, I must first insert the SQL code:

" UNION SELECT password FROM users –

After pasting the SQL code into the search link (localhost:8080/search) we would be able to view the database (1).

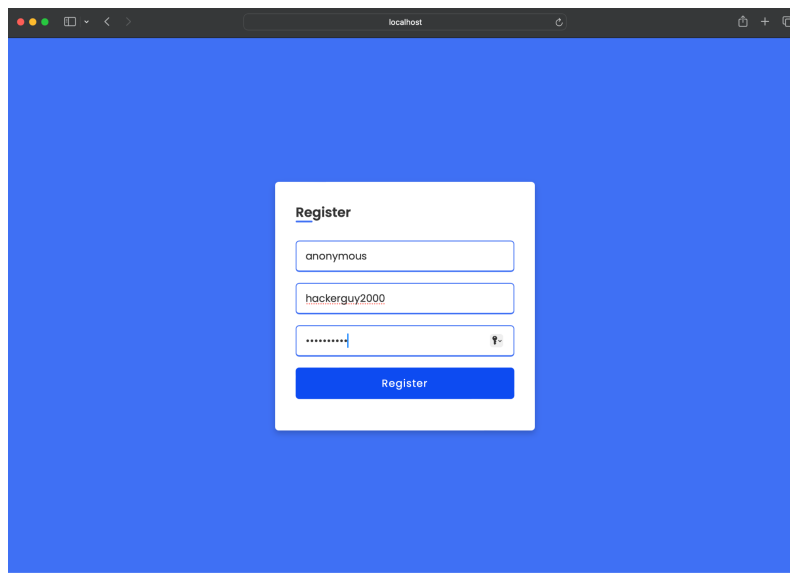


1. SQL Database

Seeing the database, we notice the possibility of enacting an attack onto the server.

Step #2:

We continue the process of attacking the server by simply registering (localhost:8080/register) for our own account, with an username and password (2).

*2. Setting Up Test Account*

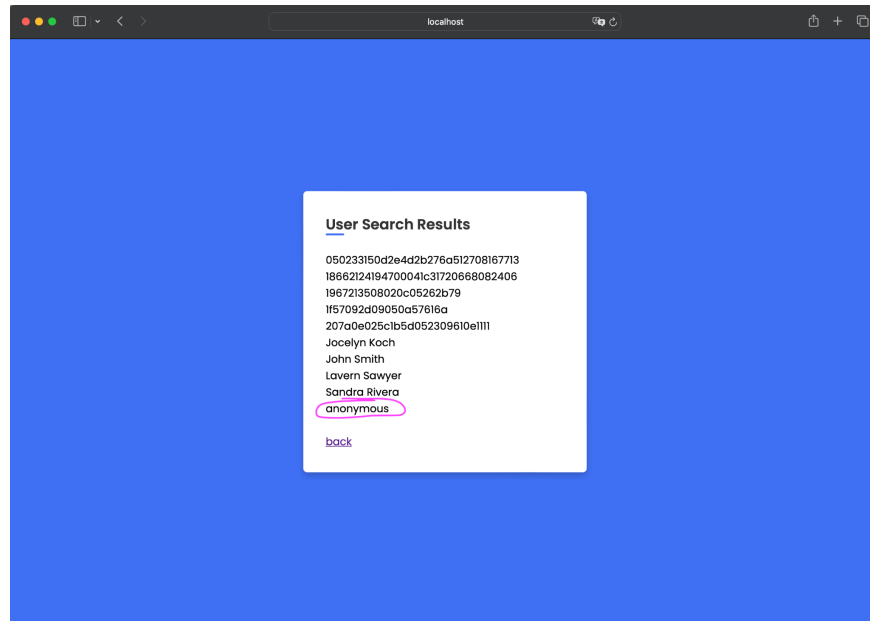
Username: *hackerguy2000*

Password: *hacker2023*

After creating the account, we would then go back to the search page (localhost:8080/search) and insert the same SQL code from the previous step (3):

" UNION SELECT password FROM users –

By doing this we would be able to view the accounts that have already been registered, including the account that I had recently made, named '**anonymous**' (3).



3. Accounts in the Database

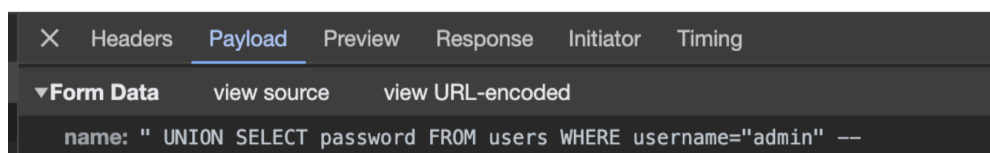
Step #3:

After viewing this, we would insert the encrypted password into the Python file. By inserting the password into the code, we would make this hexadecimal encryption into ASCII string. This will allow us to find the secret key by XORing both the password (password: hacker2023) and the ASCII string of the encrypted hexadecimal.

Step #4:

Once acquiring the secret key, I find the admin's encrypted password by utilizing the SQL code again:

" UNION SELECT password FROM users WHERE username="admin" --



4. Inserting SQL Code for Encrypted Password

By inserting this, we would be able to view the admin's encrypted password (4). Finding the credential, I would then run this into the XOR again for the admin's ASCII, which reveals the encrypted hex string and secret key, thus revealing the admin's password.