

Dylan Ramdhan

CS 357, Prof. Goldberg

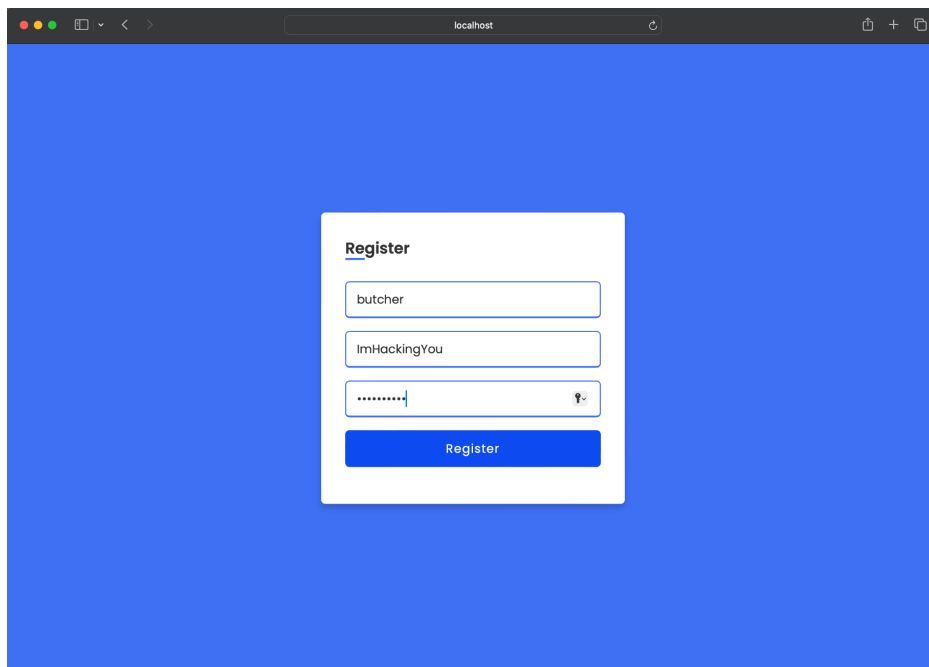
Login Authentications Challenges: Challenge 6

Nov 3, 2023

Login Authentication Challenges Report: Challenge #6

Step #1:

In this challenge, we mostly see that it is similar to the previous challenge, Challenge 5. In this challenge we first begin the attack by making an account (1).



The screenshot shows a web browser window with a blue background. In the center, there is a white rectangular form titled "Register". The form contains three input fields: the first is labeled "Name" and contains the text "butcher"; the second is labeled "Username" and contains the text "ImHackingYou"; the third is labeled "Password" and contains masked characters ".....". Below the input fields is a blue button with the text "Register".

Name: butcher

Username: ImHackingYou

Password: hacking101

Step #2:

Next we begin by encoding the password to a SHA256 encryption. Utilizing an SHA256 encryption generator, we are able to generate an SHA256 code (2).

SHA256 Generator

GENERATE A SHA256 HASH

Input value

hacking101

Generate

SHA256 HASH

a28e11932990cf64ed370ac0ec9ccddd51eabca40b444fd4de2e85ce5ba4b6f

2. Generating SHA256 Generator

SHA256 Code: a28e11932990cf64ed370ac0ec9ccddd51eabca40b444fd4de2e85ce5ba4b6f

(Sources: <https://tools.keycdn.com/sha256-online-generator>)

Step #3:

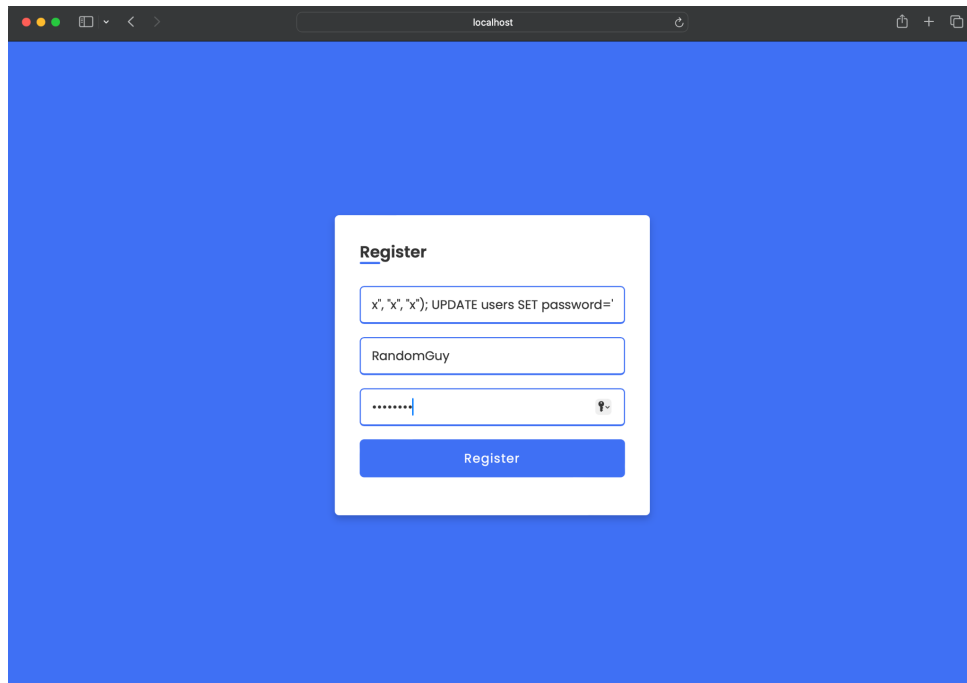
We return back to the registration page (localhost:8080/register) and enter in the new information. For the username, this would be the insertion of SQL code:

x", "x", "x"); UPDATE users SET

password='a28e11932990cf64ed370ac0ec9ccddd51eabca40b444fd4de2e85ce5ba4b6f' WHERE

username='admin'; --

As for the password, we can randomly insert anything as this information is not needed in accessing the admin's credentials (3).



The screenshot shows a web browser window with a blue background. In the center is a white 'Register' form. The form has three input fields and a 'Register' button. The first input field contains the SQL payload: `x', 'x', 'x'); UPDATE users SET password='`. The second input field contains the username: `RandomGuy`. The third input field contains masked characters: `.....`. The 'Register' button is blue with white text.

3. Registering the Account with the New Credentials.

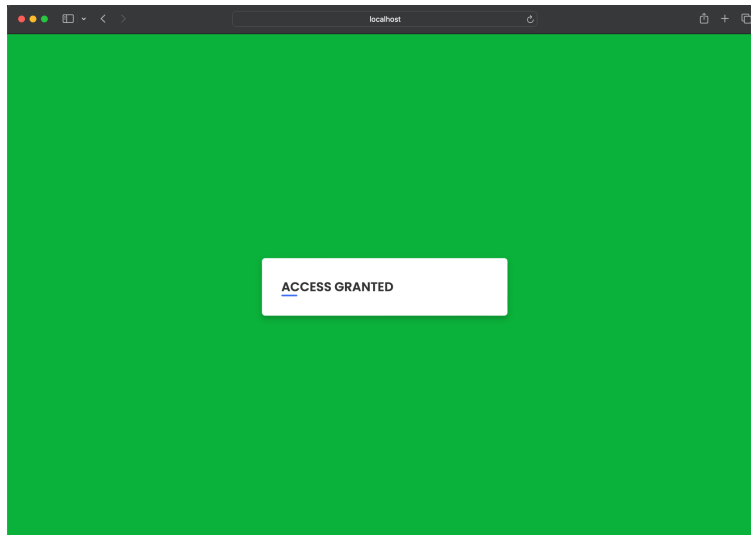
Username: [insertion of SQL code]

Name: RandomGuy

Password: hacker

Step #4:

Lastly, we can now insert these credentials into the login page (localhost:8080). By inserting the username: *admin*, and the password: *hacking101*, we are able to gain the entire full access into the admin's account (4).



4. Full Access into the Admin's Account!