Elinor Holt

Prof. Goldberg

CS 357

Nov 1, 2024

Challenge 4: Collisions

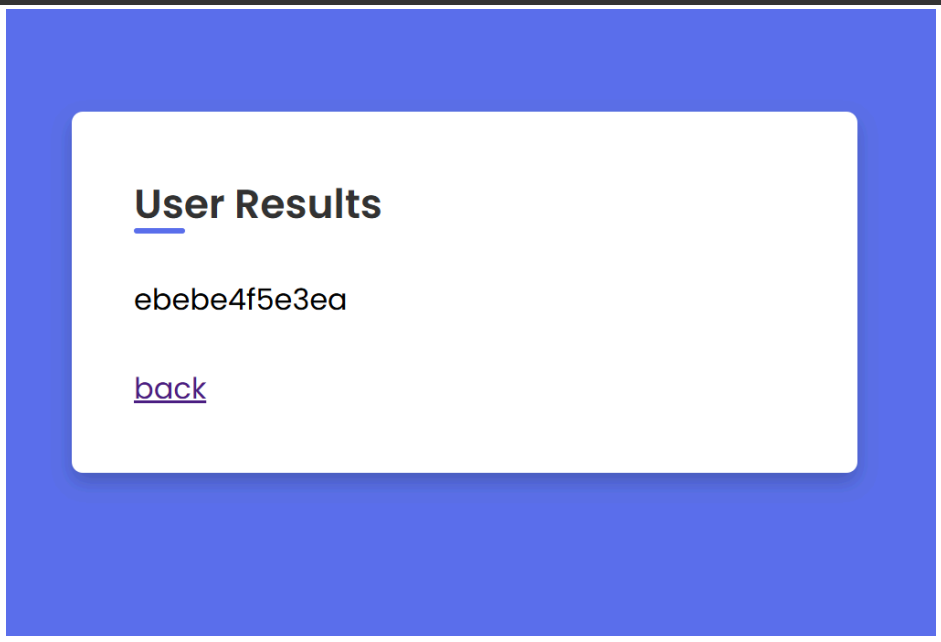
A. Recon:

   a. I used the same methods from Challenge 3 to find the table and column names in the database.

B. Exploit Instructions (Automated in code):

   a. I reused the exploit method from the search page to find the password hash associated with the admin account by submitting the following SQL query:

```
hello" union select password_hash from members where username =
"admin"; --
```

   b. 

c. This query retrieves the password_hash for the member with the username "admin." Starting the query with a unique string (not found in any member names) simplifies the output, so the results display only the password_hash.

d. The cleartext password is XORed byte by byte with the hex value 0xa5 to produce the hash, so we can recover it by reapplying the XOR operation on the hashed password. Using Python's built-in function, I XORed the password hash with 0xa5a5a5a5a5a5 and printed the resulting password.

e. The printed password can be used to log into the admin account.

C. References:

a. https://www.geeksforgeeks.org/get-the-logical-xor-of-two-variables-in-python/

b. https://stackoverflow.com/questions/11119632/bitwise-xor-of-hexadecimal-numbers