Om Khadka, U51801771
Sources: Properties of the Vigenere cipher, Vigenere Cipher Tool
Collabs: N/A

Challenge 6

This hack exploited a design flaw where the passwords were stored encrypted rather than hashed, using a Vigenère cipher with a recoverable secret key. The attack compromised the admin account through a known plaintext attack that allowed the derivation of the encryption key.

Vulnerability

The following flaws allowed this hack to work:

- Encrypted rather than hashed passwords, making them reversible
- Vigenère cipher implementation is a weak classical cipher vulnerable to cryptanalysis
- SQL injection vulnerability; the /search endpoint allows extraction of encrypted passwords
- The same secret key is used for all users

Attack

The script for this attack does the following:

1. Extract **admin_ciphertext** from /search endpoint using SQL injection.
    a. " UNION SELECT password_hash FROM members WHERE username='admin'--
    b. The ciphertext is fully uppercase of length **x**.
2. Register a new account.
    a. Name/username doesn't matter, what matters is the password.
    b. **test_password** must be 1) the same length as **admin_ciphertext** 2) All set to 'A'
3. Extract **test_ciphertext** by using the same method as in **1**
    a. " UNION SELECT password_hash FROM members WHERE username='**test_username**'--
4. Applied Vigenere cipher mathematics to derive the secret key, **key**
    a. (**test_ciphertext - test_password**) mod 26
5. Used **key** to decrypt **admin_ciphertext**
    a. admin_password = (**admin_ciphertext - key**) mod 26
6. Logged in as admin with the following form

    username : admin
    name : om khadka
    password : **admin_password**

Om Khadka, U51801771
Sources: Properties of the Vigenere cipher, Vigenere Cipher Tool
Collabs: N/A

Vigenere

The Vigenere cipher works as follows:

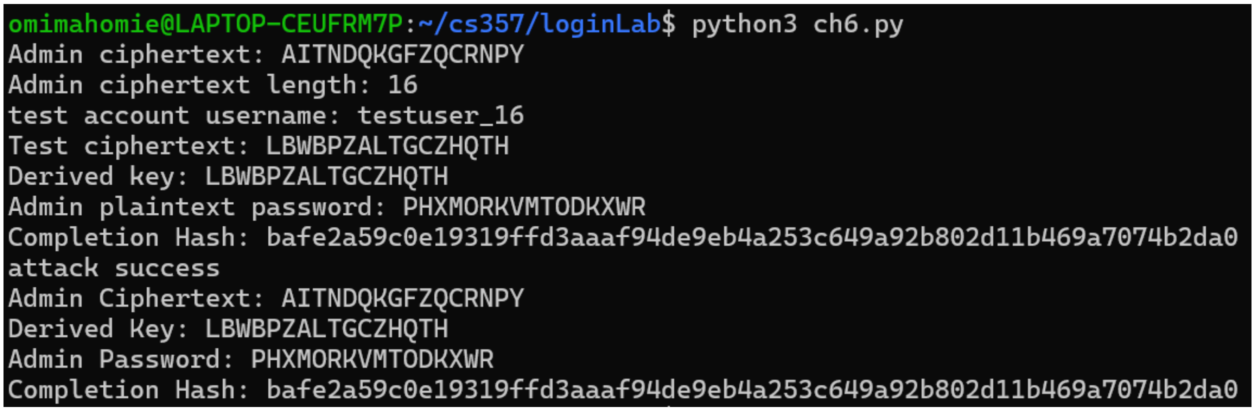
For each character position i:
C_i = (P_i + K_i) mod 26   // Encryption
P_i = (C_i - K_i) mod 26   // Decryption
K_i = (C_i - P_i) mod 26   // Key derivation

All operations are mod 26 since there are 26 letters in the alphabet.

The reason why the test user's password was all A's was that **A = 0** in this cipher:

K_i = (C_i - P_i) mod 26
K_i = (C_i - 0) mod 26
K_i = C_i mod 26

The key is essentially the ciphertext.



```
omimahomie@LAPTOP-CEUFRM7P:~/cs357/loginLab$ python3 ch6.py
Admin ciphertext: AITNDQKGFZQCRNPY
Admin ciphertext length: 16
test account username: testuser_16
Test ciphertext: LBWBPZALTGCZHQTH
Derived key: LBWBPZALTGCZHQTH
Admin plaintext password: PHXMORKVMTODKXWR
Completion Hash: bafe2a59c0e19319ffd3aaaf94de9eb4a253c649a92b802d11b469a7074b2da0
attack success
Admin Ciphertext: AITNDQKGFZQCRNPY
Derived Key: LBWBPZALTGCZHQTH
Admin Password: PHXMORKVMTODKXWR
Completion Hash: bafe2a59c0e19319ffd3aaaf94de9eb4a253c649a92b802d11b469a7074b2da0
```

Hash: bafe2a59c0e19319ffd3aaaf94de9eb4a253c649a92b802d11b469a7074b2da0