Task 4: Password Security & Authentication Analysis

1. How Passwords Are Stored:

Passwords are not stored in plain text. Instead, they are converted into hash values using hashing algorithms. Hashing changes a password into a fixed-length code, which improves security.

2. Hashing vs Encryption:

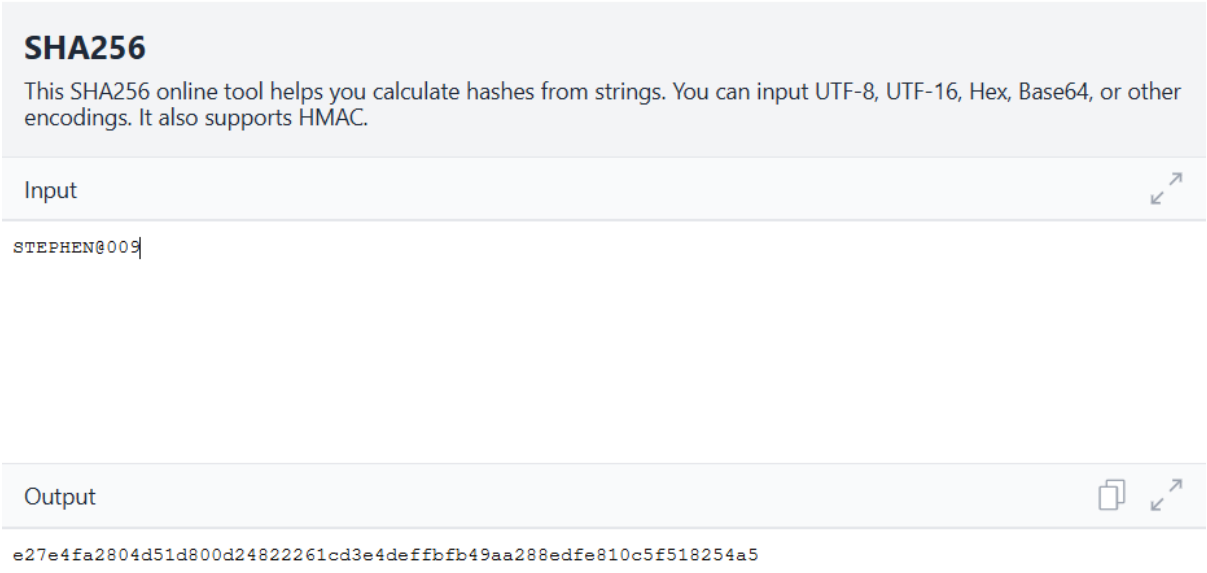
- Hashing: One-way process, cannot be reversed easily (used for passwords).
- Encryption: Two-way process, original data can be recovered using a key.

3. Types of Password Hashes:

Common hash types studied include:

- MD5
- SHA-1
- bcrypt

Stronger algorithms like bcrypt provide better protection.



4. Password Cracking Methods:

Weak passwords can be cracked using:

- Dictionary attacks (using common password lists)
- Brute-force attacks (trying all possible combinations)

5. Why Weak Passwords Fail:

- Weak passwords are often found in common wordlists, making them easy to crack.
- Short passwords reduce the number of possible combinations.
- Passwords without symbols, numbers, or uppercase letters are predictable.
- Reused passwords can expose multiple accounts if one is compromised.
- Weak hashing algorithms combined with weak passwords increase risk.

6. Multi-Factor Authentication (MFA):

- MFA requires two or more verification factors.
- Even if a password is stolen, MFA can prevent unauthorized access.
- Common MFA methods include OTP, mobile apps, biometrics, and security keys.
- MFA reduces the impact of phishing and password-cracking attacks.
- It significantly improves overall account security.

7. Importance of Strong Passwords:

- Strong passwords are harder to guess and crack.
- Long passwords increase security by expanding possible combinations.
- Using a mix of uppercase, lowercase, numbers, and symbols improves strength.
- Unique passwords prevent multiple account compromises.
- Strong passwords combined with MFA provide maximum protection**.**

8. Recommendations for Strong Authentication:

- Use long and complex passwords.
- Avoid common words and personal information.
- Do not reuse passwords across accounts.
- Enable Multi-Factor Authentication (MFA).
- Use secure authentication methods and tools.