Task 6: Create a Strong Password and Evaluate Its Strength

1.Objective

Understand what makes a password strong and test it against password strength tools.

---

2. Tools Used

- Password Manager for Testing: Bitwarden (for secure password generation and evaluation)

Passwords Tested and Results

Password	Strength (Rating)	Estimated Time to Crack	Feedback from Tool
password	Very Weak	Less than 1 second	Common password; lacks symbols and complexity
Kshitij@123	Moderate to Strong	12 days	Includes symbol and numbers; still somewhat guessable
K$h1t1j@2025!	Strong	31 years	Good length, randomness, and complexity
!A1b2C3d4E5f6G7h8	Strong	21 years	Excellent length and mix of all character types

---

3. Evaluation and Observations

Strong Password Characteristics:

- Length: More than 12 characters.
- Complexity: Combination of:
    - Uppercase and lowercase letters
    - Numbers
    - Special characters (e.g., !@#$)
- Unpredictability: Avoidance of dictionary words or personal information.

Weak Password Characteristics:

- Short passwords (under 8 characters).
- Use of common words (e.g., password, admin).
- Lack of diversity in character types.
- Predictable or reused formats.

---

4. Tips Learned from Evaluation

1. Length matters: Longer passwords are significantly harder to crack.
2. Symbols help: Adding even one special character greatly boosts strength.
3. Avoid patterns: Predictable sequences (like 1234) reduce effectiveness.
4. Substitution improves strength: Replacing characters (s → $, i → 1) adds entropy.
5. Passphrases are useful: Combinations of unrelated words with symbols work well (e.g., C0ffee@Rain+Storm2025).
6. Use a Password Manager: Tools like Bitwarden or LastPass help generate and store strong passwords safely.

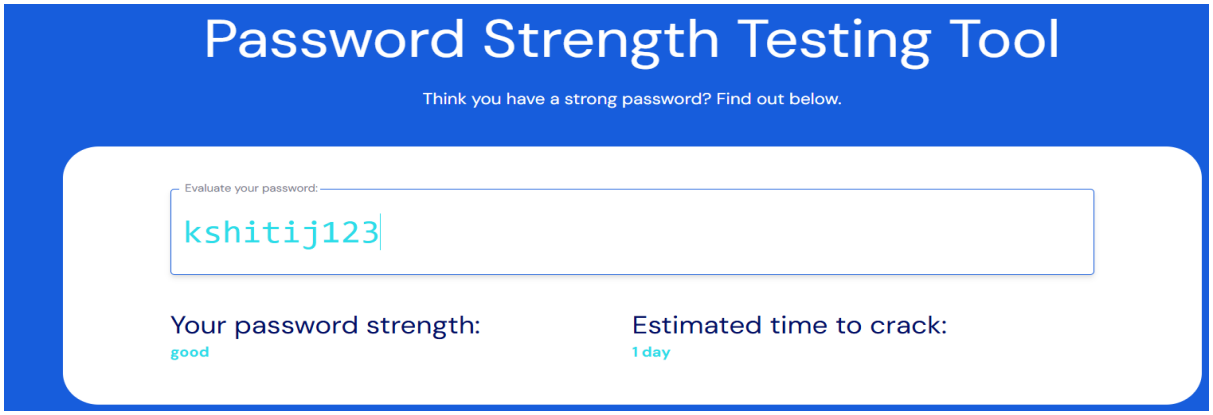
5.Common Password Attacks (Researched)

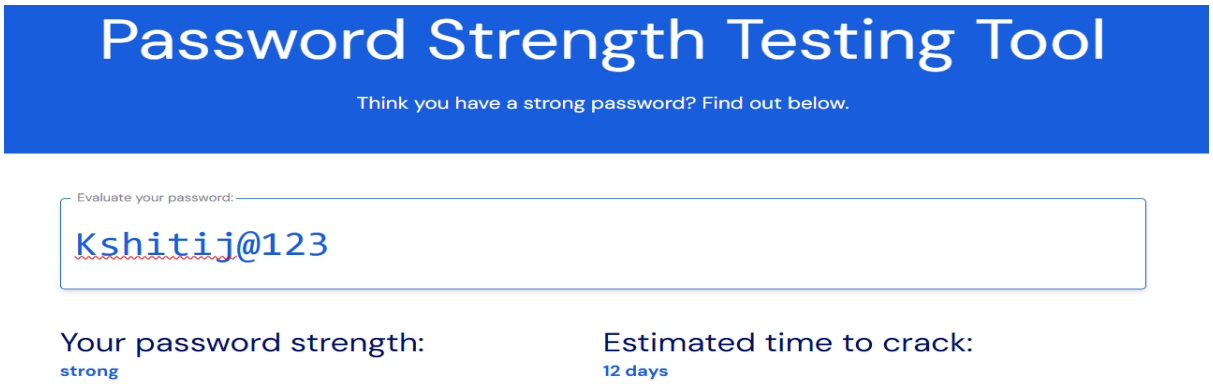
1. Brute Force Attack
    - Tries all combinations.
    - Very effective against short or simple passwords.
2. Dictionary Attack
    - Uses precompiled lists of common words and passwords.
    - Exploits predictable human choices like 123456 or password1.
3. Credential Stuffing
    - Applies leaked username-password pairs on other sites.
    - Dangerous if passwords are reused.

Conclusion

Through this exercise, the importance of password complexity and unpredictability became evident. Passwords like password are practically useless, while structured, randomized passwords offer strong defense against common attacks. Users should always aim to create complex passwords and use trusted password managers for maintaining them securely.

Screenshots





Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

K$h1t1j@2025!

Your password strength:
strong

Estimated time to crack:
31 years

Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

!A1b2C3d4E5f6G7h8

Your password strength:
strong

Estimated time to crack:
21 years

Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

password

Your password strength:
very weak

Estimated time to crack:
less than a second