Password Strength Evaluation

Objective:

The objective of this task is to understand what makes a password strong or weak by testing various passwords of different complexity levels using an online password strength checking tool. This helps develop awareness about secure password practices and protection against common password based attacks like brute-force and dictionary attacks.

Tool Used: HowSecureIsMyPassword.net

- This tool estimates how long it would take a computer to crack your password using brute force techniques.
- It does **not save or transmit** your password.
- The results depend on:
    - Length of the password
    - Use of uppercase and lowercase letters
    - Inclusion of numbers and special characters
    - Randomness and unpredictability

Passwords Tested and Their Results:

Password	Estimated Time to Crack
cracked	200 milliseconds
Cracked	25 seconds
Cracked@12	5 years
Cracked@2564	34 thousand years
CrA@86keD02#It	200 million years

Analysis of Results:

- **Short and simple passwords** are extremely easy to crack.
- Adding **capital letters** increases the time moderately.
- Including **numbers and special characters** makes the password much harder to guess.
- A **long and random password** is nearly impossible to crack with current computing power.
- Complexity significantly increases password security.

Best Practices for Creating Strong Passwords:

- Use at least **12 characters**.
- Combine **uppercase**, **lowercase**, **numbers**, and **symbols**.
- Avoid personal information like names or birthdates.
- Don't reuse passwords across multiple sites.
- Use a **password manager** to create and store passwords.
- Consider using **passphrases** (e.g : Coffee@Rain7&Books!)

Common Password Attacks:

1. **Brute-force Attack**: Tries every possible combination of characters until the correct one is found.
2. **Dictionary Attack**: Tries a list of known or commonly used passwords.
3. **Credential Stuffing**: Uses leaked username-password combinations from previous breaches.

Role of Multi-Factor Authentication (MFA):

Even if a password is compromised, MFA adds a **second layer of protection**. Examples include:

- OTPs sent to phones
- Authenticator apps (e.g, Google Authenticator)
- Fingerprint or face ID

MFA significantly increases the difficulty of unauthorized access.

Real-Life Example: LinkedIn Breach (2012):

- 6.5 million hashed passwords leaked.
- Many users had weak passwords like 123456, linkedin, and password.
- Attackers used dictionary and brute-force methods to crack them.

This breach highlights the importance of complex, unique passwords.

Conclusion:

Creating strong, unique passwords is one of the simplest and most effective ways to protect digital accounts. Tools like howsecureismypassword.net help users visually understand the strength of their credentials.