Password Strength Evaluation Report

Objective:

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

Tools Used:

Online free password strength checkers (e.g., passwordmeter.com)

Methodology :

1. Created multiple passwords with varying complexity.
2. Used combinations of uppercase, lowercase, numbers, symbols, and different lengths.
3. Tested each password on a password strength checker.
4. Noted scores and feedback from the tool.
5. Identified best practices for creating strong passwords.
6. Documented tips learned from the evaluation.
7. Researched common password attacks (brute force, dictionary).
8. Analyzed how password complexity affects security.

Observations

- Short & simple passwords (like 'password') are the weakest. They are vulnerable to dictionary attacks because they are common words.
- Adding numbers (e.g., 'Password123') improves strength slightly but still predictable.
- Substitutions (like 'P@ssw0rd') help but attackers often guess these patterns.
- A mix of uppercase, lowercase, numbers, and symbols makes passwords much harder to crack.
- Length is the biggest factor — longer passwords exponentially increase brute force difficulty.

Common Password Attacks

- Brute Force Attack: Tries every possible combination until the password is found. Long and complex passwords resist brute force.
- Dictionary Attack: Uses common words or leaked password lists. Simple passwords like 'password123' fall instantly.
- Phishing & Social Engineering: Even strong passwords can be stolen if a user is tricked into revealing them.
- Credential Stuffing: Attackers reuse leaked usernames/passwords from past breaches.

Passwords Tested & Results:

Password | Complexity | Strength Score | Notes / Feedback

Password123	Low	Weak	Too common, easily guessable
P@ssw0rd!23	Medium	Moderate	Improved with symbols and numbers
7G!m@#9vK$2q	High	Strong	Strong combination, difficult to guess

Best Practices Learned:

- Use a mix of uppercase, lowercase, numbers, and symbols.
- Avoid common words or sequential patterns.
- Longer passwords are stronger.
- Unique passwords for different accounts.
- Regularly update passwords.

Conclusion:

Password complexity significantly improves security against attacks such as brute force or dictionary attacks.

Strong passwords are long, unique, and include varied characters.