



Task 6: Create a Strong Password and Evaluate Its Strength

Objective

To understand what makes a password strong by creating various passwords with varying complexity, testing them using free online password strength checkers, and analyzing the results.

Methodology

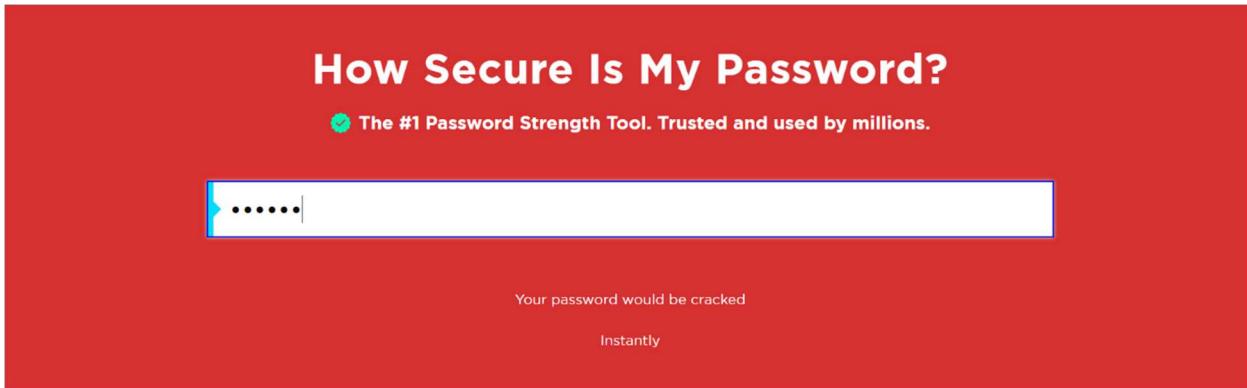
1. Password Creation Criteria:

- Length: Minimum 8–16 characters
- Includes: Uppercase, lowercase, numbers, special characters
- Avoid: Dictionary words, personal info

2. Passwords Tested:

Password	Score (%)	Time to Crack (Est.)	Verdict
password123	26%	< 2 seconds	 Weak
P@ssw0rd123	54%	~1 hour	 Medium
Th!sIsStr0ng#9	100%	34 thousand years	 Very Strong
aBc\$983#LpQ!	100%	8 million years	 Very Strong

1. Weak Password



2. Strong Password



📌 Learnings & Tips for Strong Passwords

✓ Best Practices:

- Use at least 12 characters
- Combine letters (upper & lower), numbers, symbols
- Avoid real words and common phrases
- Do not reuse passwords
- Consider using a **password manager**

⌚ Common Mistakes:

- Using personal info (e.g., names, birthdays)

- Reusing passwords across sites
 - Using sequential or repeated characters (e.g., 123456, aaaaaa)
-

Understanding Common Attacks

Attack Type	Description
Brute Force	Tries every possible combination until it finds the correct one
Dictionary	Uses common words or phrases to guess passwords
Credential Stuffing	Tries known breached usernames/passwords from data leaks

Key Takeaways

- **Password complexity = security:** Every added character or symbol increases difficulty to crack.
 - **Length > complexity:** A long passphrase can be stronger than a short complex password.
 - **Passphrases** like HOrse\$Battery\$Staple2025 are easy to remember and secure.
 - **Multi-Factor Authentication (MFA)** adds another strong layer of defense.
 - **Password Managers** help generate and store unique, secure passwords.
-

Conclusion

A strong password is essential in protecting personal and organizational data. Through this task, I understood the technical and strategic importance of secure password practices and how to evaluate them using real tools.