# Task 6: Create a Strong Password and Evaluate Its Strength

Submitted by: Sivamani Achanta

Date: 01/07/2025

## Objective

To understand the key elements of a strong password, evaluate various password combinations using online password strength checkers, and learn best practices to protect against password-related attacks.

## Tools Used

• https://passwordmonster.com – Online password strength testing tool

## Passwords Tested and Strength Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Characters Used | Strength | Time to Crack | Feedback Summary |
| password123 | Lowercase + Numbers (11 characters) | Very Weak | 0 seconds | Common pattern, easy to guess, offers no security |
| p@ssw0rd! | Lowercase + Symbols (9 characters) | Very Weak | 0 seconds | Contains dictionary word, predictable substitutions |
| 123456 | Numbers only (6 characters) | Very Weak | 0 seconds | Extremely weak, widely used password |
| MyC@t$Eat5Fi$h | Upper, Lower, Symbols, Numbers (14 char) | Very Strong | 4 years | Excellent use of passphrase and complexity |
| !QAZ2wsx#EDC4rfv | Upper, Lower, Symbols, Numbers (16 char) | Very Strong | 112 years | Highly secure, complex, and random |

## Tips Learned from Evaluation

• Longer passwords significantly increase strength and resistance to brute-force attacks.  
• Avoid using dictionary words and predictable patterns like 'password123'.  
• Include a mix of uppercase, lowercase, numbers, and special symbols.  
• Passphrases like 'MyC@t$Eat5Fi$h' are easy to remember and hard to crack.  
• Password strength tools help visualize how secure a password is.

## Common Password Attacks Researched

1. Brute Force Attack:  
 - Tries every possible combination. Short and simple passwords are cracked quickly.

2. Dictionary Attack:  
 - Uses known words from dictionaries or common password lists. `p@ssw0rd` is easily guessed this way.

3. Credential Stuffing:  
 - Tries usernames and passwords leaked from other sites. Password reuse makes you vulnerable.

## Summary: How Complexity Affects Security

• Adding just 1 symbol or number greatly increases the time it takes to crack.  
• Passphrases with 12+ characters are much harder to break than short, complex ones.  
• Password strength = length × randomness × character diversity.

## Conclusion

This task highlighted the importance of password complexity and uniqueness. Strong passwords act as the first line of defense in cybersecurity. Regular password reviews and use of password managers are recommended for optimal security.