Password Strength Evaluation

This document explains how password complexity affects security.
We used an online password strength checker to test multiple passwords with varying complexity.

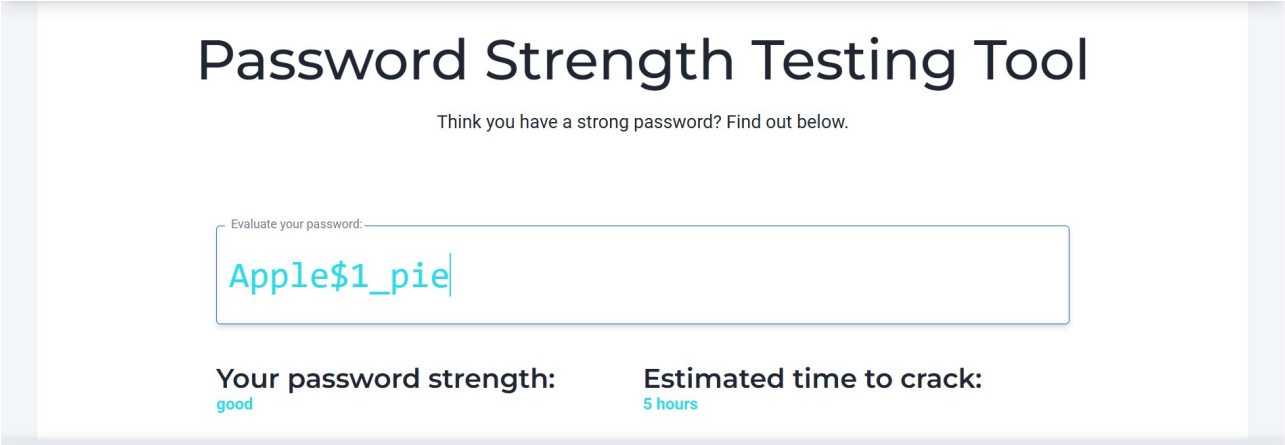
Platform Used: Security.org Password Strength Checker

Steps Performed:

1. Created multiple passwords with different levels of complexity (uppercase, lowercase, numbers, symbols, length).
2. Tested each password using the online tool.
3. Collected scores and feedback.
4. Analyzed the results to identify best practices for creating strong passwords.
5. Researched common password attacks (brute force, dictionary) to understand the importance of password strength.

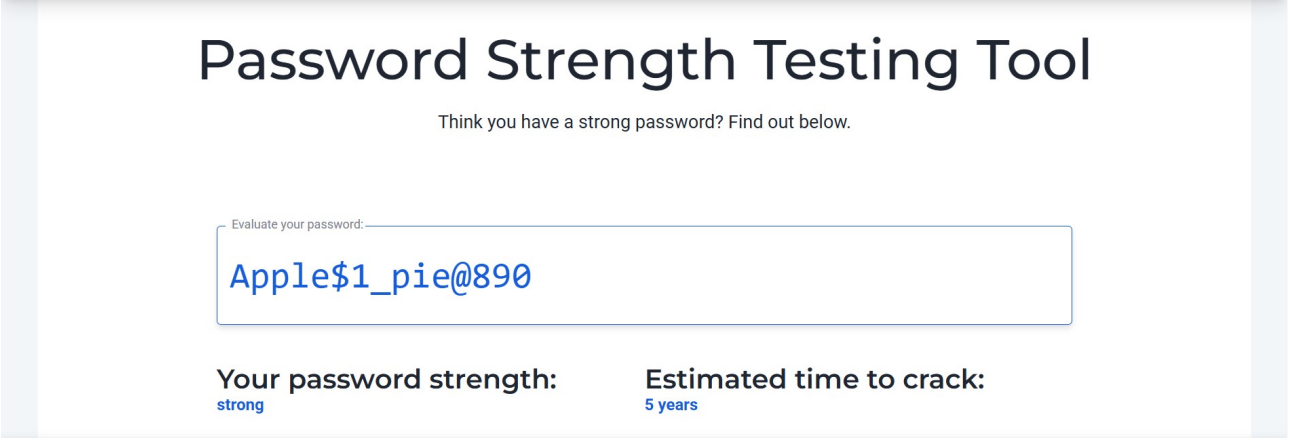
Below are screenshots and analysis for each tested password.

Good Password



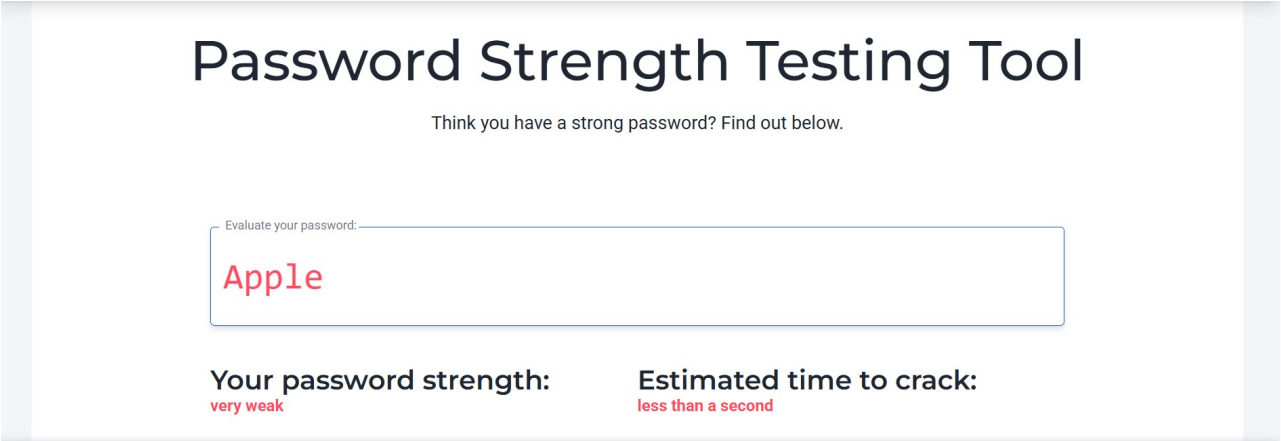
This password meets most security recommendations, including length, uppercase, lowercase, numbers, and symbols. It is resistant to most basic attacks.

Strong Password



This password is very strong with high complexity, making it extremely difficult for brute force or dictionary attacks.

Very Weak Password



This password is short and lacks complexity, making it very easy to crack using automated tools.