Task 6: Password Strength Evaluation Report

# Objective

To create and evaluate multiple passwords with different complexity levels using a password strength checker tool, and to understand best practices and the importance of strong password creation.

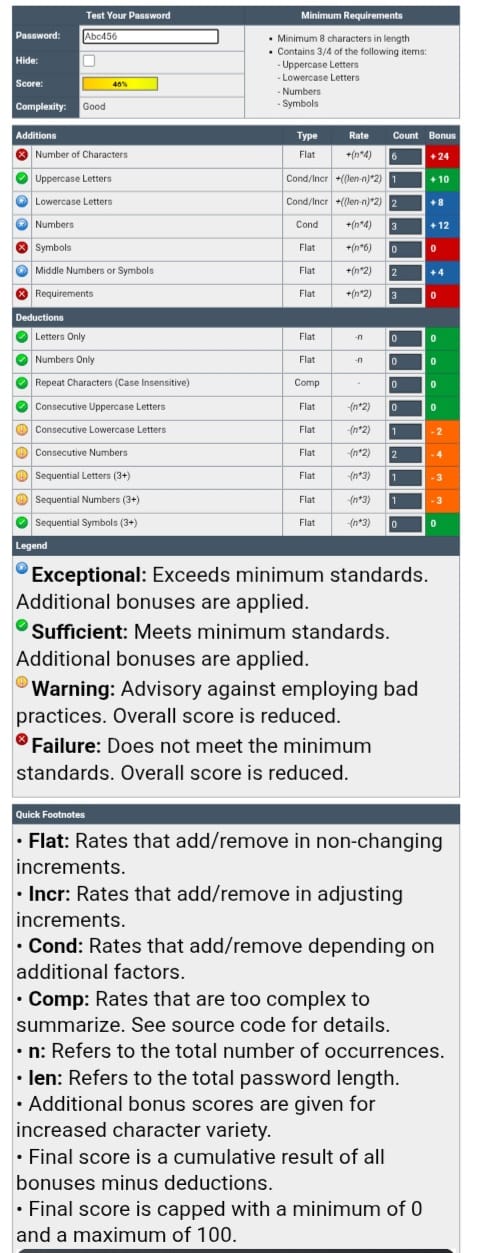
# Password Test Results

Two passwords were tested:

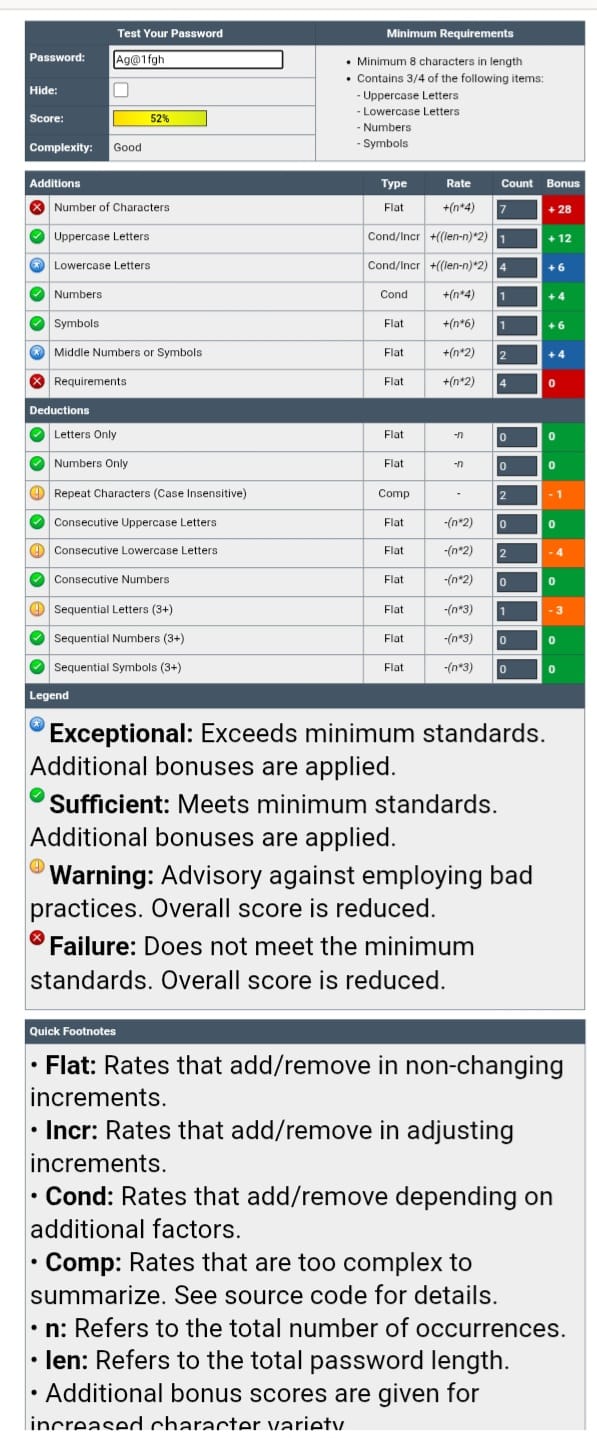
1. Abc456 – A mix of uppercase, lowercase, and numbers.

2. Ag@1fgh – Includes uppercase, lowercase, number, and symbol.

Password Strength Result for Abc456:



Password Strength Result for Ag@1fgh:



# Observations and Feedback

The first password 'Abc456' scored 40% with good complexity but did not meet the minimum requirement of 8 characters.  
The second password 'Ag@1fgh' scored 52% and met more criteria including the presence of a symbol, but it was still under the ideal length of 8 characters.  
Both tests highlight the impact of character variety and length on password strength.

# Tips for Creating Strong Passwords

- Use a mix of uppercase, lowercase, numbers, and symbols

- Ensure your password is at least 12 characters long

- Avoid dictionary words, common patterns, and personal information

- Use passphrases or password managers for better memorability and storage

# Common Password Attacks and the Role of Complexity

Brute Force Attacks: Attackers try every possible combination. Stronger passwords take exponentially more time to crack.  
Dictionary Attacks: Use precompiled lists of common passwords. Complex and unique passwords reduce the effectiveness.  
Password complexity directly increases resistance against these attacks, especially when combined with length.