Password Strength Raw Results

This document presents the raw results of testing different passwords using a password strength meter. The objective was to observe how variations in length, character diversity, and complexity affect the strength score and overall classification of a password. By analyzing results from very weak to very strong, we can understand what factors make a password secure.

Password	Score (%)	Complexity
****************	0%	Very Weak
rosemary	9%	Very Weak
rosemary00	36%	Weak
rosemary00@	58%	Good
Rosemary00	66%	Strong
Rosemary00@	84%	Very Strong
y4lAk*6P@?72&83oM2Fh	100%	Very Strong

Analysis of Results: • Passwords with only lowercase letters (e.g., 'rosemary') scored poorly. • Adding numbers improved scores slightly, but repetition reduced strength. • Including uppercase letters and symbols significantly improved ratings. • Longer and more complex passwords (e.g., 'y4lAk*6P@?72&83oM2Fh') achieved the highest strength. Conclusion: Password strength is directly related to both length and complexity. A diverse mix of characters is essential for resisting brute-force and dictionary attacks.