Password Strength Evaluation Report

Author: Yuvateja

Date: October 2025

📘 Introduction

This report explores password strength by testing various password samples using online tools like PasswordMeter.com. It also summarizes best practices and common attack types to strengthen cybersecurity awareness and prepare for interviews.

🧪 Password Samples & Evaluation

Password	Complexity Level	Score (%)	Feedback Summary
password123	Weak	26%	Predictable, lacks symbols
Pass123!	Medium	58%	Moderate strength
P@ssW0rd2025	Strong	84%	Good mix of characters
T3j@Yuv@#Secure2025	Very Strong	100%	Excellent length and complexity

🖼️ Screenshots from PasswordMeter.com are included in the GitHub repository.

✅ Best Practices for Strong Passwords

- Use 12+ characters

- Mix uppercase, lowercase, numbers, and symbols
- Avoid dictionary words and personal info
- Dont reuse passwords across platforms
- Use passphrases and password managers

🔓 Common Password Attacks

Attack Type	Description
Brute Force	Tries every possible combination; longer passwords resist better
Dictionary Attack	Uses known words and common passwords; weak passwords fall quickly
redential Stuffing	Uses leaked passwords from other sites; reused passwords are vulnerable