Password Strength Checker Report

Cyber Security Internship – CodeAlpha

Name: Shishidhar Kompulira Kuttappa
Domain: Cyber Security
Project: Password Strength Checker
Date: (today's date)

Introduction
Passwords are one of the most important components of cybersecurity. Weak passwords make systems vulnerable to brute-force attacks, credential stuffing, and unauthorized access. This project focuses on analyzing password strength based on common security standards.

Password Strength Criteria
1. Length: Passwords should be at least 8 characters long.
2. Uppercase Letters: Inclusion of capital letters improves strength.
3. Lowercase Letters: Helps increase character variety.
4. Numbers: Adds complexity and resistance to guessing.
5. Special Characters: Symbols significantly improve password security.

Strength Evaluation Examples
Weak Password:
Example: password123
Reason: No uppercase letters or special characters.

Medium Password:
Example: Password123
Reason: Includes uppercase letters and numbers but lacks special characters.

Strong Password:
Example: P@ssw0rd!2024
Reason: Contains uppercase, lowercase, numbers, special characters, and sufficient length.

Conclusion
Strong passwords play a crucial role in protecting user accounts and sensitive information. By following good password practices and using strong combinations of characters, users can significantly reduce the risk of cyberattacks. This project highlights the importance of password awareness in cybersecurity.