

Evaluating Password Security: Strengths and Common Vulnerabilities

Bruno De Cesar Faria, Emmanuel D, Dalamo Jr, Bhavesh Kumar Sharma

B.Sc. Computer Science – Semester IV

Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, India

Abstract: Passwords have long served as the cornerstone of digital authentication, safeguarding sensitive data, financial information, and personal communication. However, as cyber threats evolve, the effectiveness of traditional password-based systems is increasingly questioned. This project aims to evaluate password security by analyzing both strengths and common vulnerabilities associated with password usage. Through a review of password creation practices, password strength estimation tools (such as zxcvbn), and simulated brute-force/cracking scenarios, this study highlights why weak and reused passwords remain a critical vulnerability in modern cybersecurity. The findings indicate that while strong, unique passwords significantly reduce risk, human behavior—including poor memory, convenience, and negligence—often undermines security. The project also emphasizes the role of multi-factor authentication (MFA) and password managers as supplementary defenses. Ultimately, the study concludes that while passwords are not obsolete, their security depends on a combination of robust policies, user awareness, and complementary authentication mechanisms.

Keywords: Passwords, Cybersecurity, Authentication, Vulnerabilities, Password Strength, Data Breaches

