Report: Password Strength Evaluation and Analysis

By : Pranav Vijayakumar

Objective

To understand what makes a password strong by creating and evaluating various passwords using online strength-checking tools, and to identify best practices for password creation and security.

Table of content

1. Introduction

Passwords are one of the most critical layers of digital security. With the growing sophistication of cyber threats, creating and maintaining strong passwords is essential to protect sensitive data and user accounts. This report explores the characteristics of strong passwords, evaluates various password examples using online password strength tools, and provides guidelines for creating robust credentials.

2. Tools Used

To evaluate password strength, the following free online tools were used:

- **PasswordMeter.com:** Offers a detailed scoring system based on password length, character types, and common patterns.
- **HowSecureIsMyPassword.net:** Estimates how long a password would take to crack using brute force.
- **NordPass Password Strength Checker:** Provides strength feedback and recommendations.

3. Passwords Created

To understand the effect of different parameters, multiple passwords were created with varying lengths and complexities:

Password	Length	Components Used	Notes
apple123	8	Lowercase, digits	Simple and commonly used
Apple123!	9	Uppercase, lowercase, digits, symbol	Basic complexity
@PpL3!9rB#	10	Mixed characters	Randomized and strong
XkT#82!qrPl9	12	Mixed characters	Long, randomized, very strong
P@ssw0rd	8	Common password pattern	Predictable, unsafe

4. Password Strength Evaluation

4.1 Results Table

Password	PasswordMeter Score	Crack Time (HowSecureIsMyPassword)	NordPass Feedback
apple123	27% (Weak)	2 minutes	Too simple, lacks complexity
Apple123!	76% (Medium)	3 days	Medium strength, still guessable
@PpL3!9rB#	98% (Strong)	3,000 years	Excellent complexity and randomness
XkT#82!qrPl9	100% (Very Strong)	34 trillion years	Highly secure, excellent entropy
P@ssw0rd	45% (Weak)	10 minutes	Predictable variation of common term

4.2 Analysis of Results

- **Length and complexity** directly improve password strength.
- **Substituting characters** (like @ for a) in common words does not make them secure.
- **Random combinations** of characters with no dictionary patterns provide the best resistance to attacks.
- **Passwords ≥ 12 characters** with varied character types score the highest.

5. Password Attack Methods

Understanding how passwords are attacked helps in crafting defenses:

Attack Type	Description	Countermeasures
Brute Force	Systematically tries every possible combination of characters	Long, complex passwords
Dictionary	Uses lists of common passwords and words	Avoid real words and common patterns

Attack Type	Description	Countermeasures
Phishing	Tricks users into revealing passwords through fake websites/emails	Educate users, use MFA
Keylogging	Captures keystrokes via malware	Anti-malware tools, secure input mechanisms

6. Best Practices for Strong Passwords

Based on analysis and tool feedback, the following practices are recommended:

Use a combination of:

- **Uppercase and lowercase letters**
- **Numbers**
- **Special symbols** (@, #, !, etc.)
- **12+ character length**

Avoid:

- Personal information (birthdays, names)
- Common words or phrases (e.g., password, admin)
- Sequential characters (12345, abcdef)
- Keyboard patterns (qwerty, asdf)

Recommendations:

- Use a **password manager** to generate and store strong, unique passwords.
- Enable **multi-factor authentication (MFA)** wherever possible.
- **Do not reuse passwords** across different sites or platforms.

7. Conclusion

Password security is a vital aspect of protecting digital identities. Through this evaluation, we found that strong passwords are typically long, random, and diverse in character composition. Online tools offer valuable insights into password strength and crack resistance, allowing users to make informed decisions.

By adhering to best practices and understanding the risks of weak credentials, users can significantly reduce their exposure to common password-based attacks.

8. References

- PasswordMeter: https://www.passwordmeter.com
- HowSecureIsMyPassword: https://howsecureismypassword.net
- NordPass Checker: https://nordpass.com/password-strength-checker/
- OWASP Password Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html