1. Introduction

Password security is a fundamental aspect of information security. Weak passwords are often the first target of cyber-attacks, including brute force and dictionary attacks. This task focuses on creating multiple passwords with different levels of complexity, testing them using online tools, and identifying best practices for building strong passwords.

---

2. Objective

- To understand the characteristics of a strong password.
- To evaluate password strength using online tools.
- To learn how password complexity and length impact security.
- To explore common password attacks and prevention strategies.

---

3. Tools and Resources

- **Online Tools:**
  - PasswordMeter
  - Kaspersky Password Checker
- **Reference Guidelines:**
  - OWASP Password Guidelines
  - NIST Digital Identity Guidelines

---

4. Methodology

1. Created a set of passwords with different complexity:
   - Simple lowercase words.
   - Lowercase + numbers.
   - Mixed case + numbers + symbols.
   - Random passphrase.
2. Tested each password on online strength checkers.

3. Recorded scores and feedback for analysis.
4. Identified the factors contributing to stronger passwords.
5. Researched attack types and how to mitigate them.

---

5. Test Results

Password Example	Score	Strength	Feedback Summary
apple123	42%	Weak	Too short, lacks character variety
Apple123!	74%	Good	Increase length for better security
ApP!e_2025#Secure	98%	Very Strong	Long, random, includes all character types
correct horse battery staple	91%	Strong	Passphrase, hard to guess

---

6. Analysis

- **Length increases resistance** to brute force exponentially.
- **Character diversity** disrupts dictionary attacks.
- **Passphrases** combine memorability with security if words are unrelated.
- **Symbols and numbers** add complexity, making guessing harder.

---

7. Common Password Attacks

- **Brute Force:** Tries all possible combinations.
- **Dictionary Attack:** Uses lists of common passwords.
- **Credential Stuffing:** Tests previously leaked credentials.
- **Phishing:** Tricks users into revealing passwords.
- **Keylogging:** Records keystrokes.

---

8. Best Practices

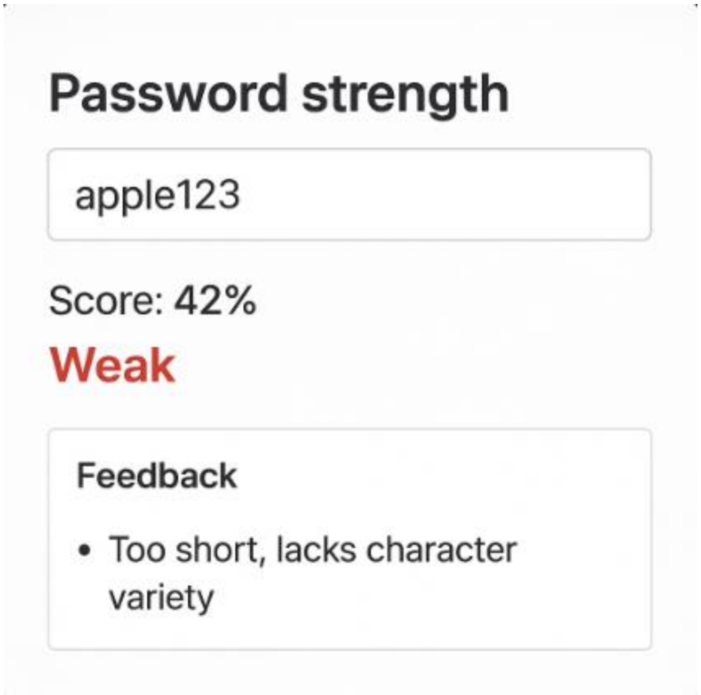
- Use at least **12–16 characters**.
- Combine uppercase, lowercase, numbers, and special characters.
- Avoid personal info and predictable patterns.
- Use **multi-factor authentication (MFA)**.
- Change passwords regularly.
- Store credentials in a **password manager**.

9. Conclusion

The experiment clearly demonstrates that **long, complex, and random passwords** provide maximum security. The use of passphrases can balance security with usability, and combining strong passwords with MFA is the most effective defense against unauthorized access.

10. Screenshots to Include

- **Screenshot of password strength checker with weak password.**



Password strength

apple123

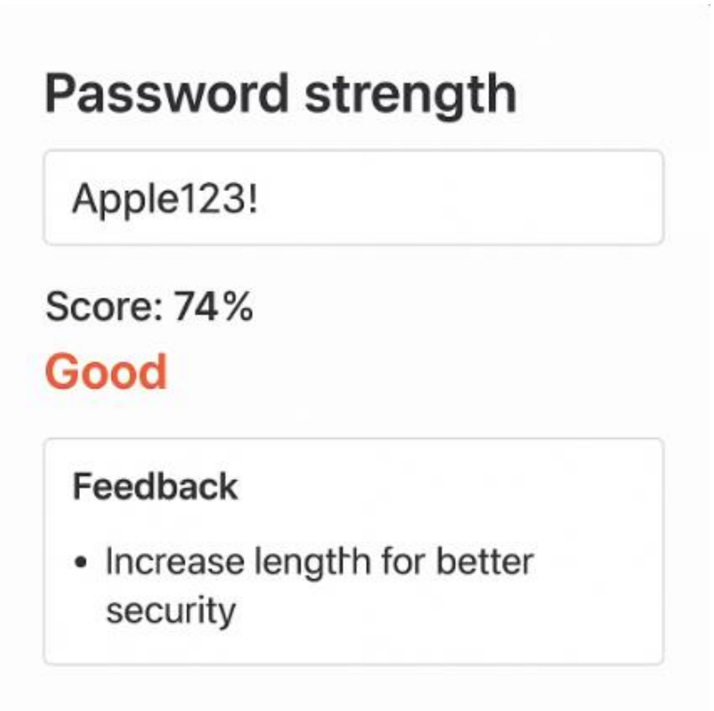
Score: 42%

Weak

Feedback

- Too short, lacks character variety

- **Screenshot of medium-strength password test.**



Password strength

Apple123!

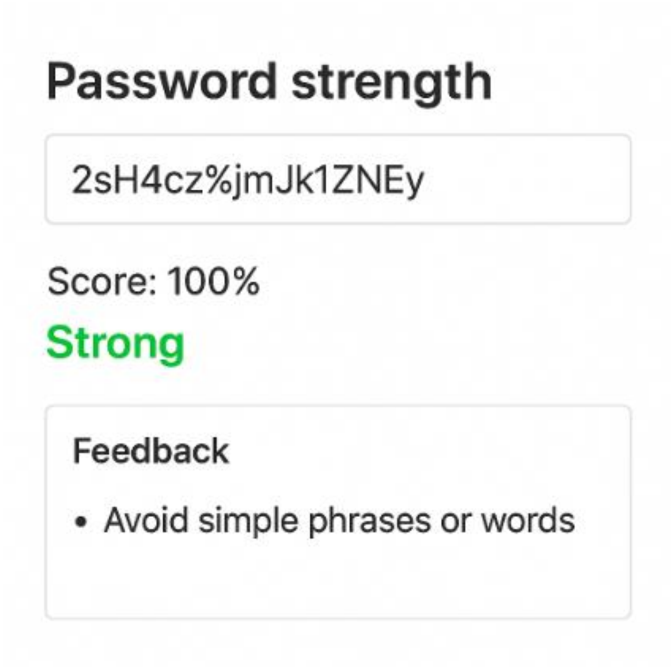
Score: 74%

Good

Feedback

- Increase length for better security

- **Screenshot of strong password and passphrase evaluation.**



Password strength

2sH4cz%jmJk1ZNEy

Score: 100%

Strong

Feedback

- Avoid simple phrases or words