Task 6: Create a Strong Password and Evaluate Its Strength

🎯 Objective

To create multiple passwords of varying complexity, evaluate their strength using an online password checker, and understand best practices for creating secure passwords.

🛠️ Tools Used

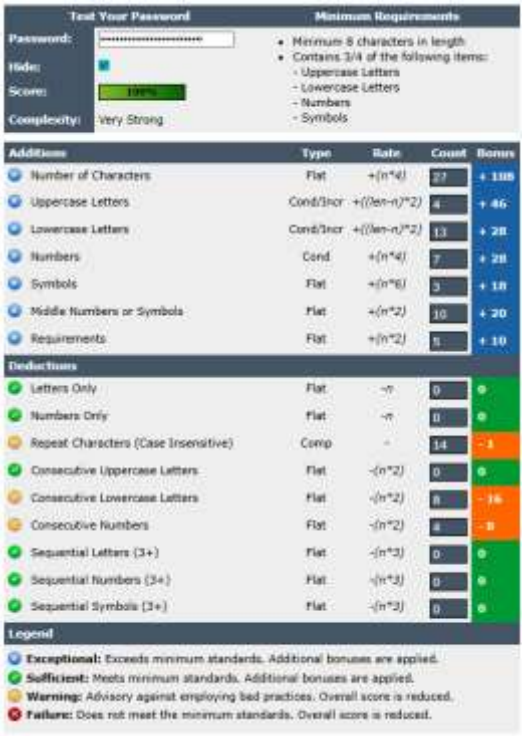
- Password Meter
- How Secure Is My Password

🧪 Steps Performed

1. **Created Multiple Passwords**
    - Designed four different passwords ranging from weak to very strong.
2. **Tested Password Strength**
    - Used password strength checker tools to evaluate score, time to crack, and security feedback.
3. **Documented Results**
    - Recorded results in a table for comparison.
4. **Researched Common Password Attacks**
    - Reviewed brute force, dictionary, and phishing attacks.
5. **Identified Best Practices**
    - Listed key guidelines for creating strong and secure passwords.

📊 Password Strength Results

Password	Score (%)	Time to Crack	Feedback
apple123	37%	Less than a second	Too short, contains dictionary word
Apple@123	81%	Few minutes	Medium complexity, could be longer
P@ssw0rd!2025	100%	Hours	Strong but contains common word pattern
Gr33n$PineAppl3!2025#Secure	100%	Centuries	Very strong, good mix of characters



⚠️ Common Password Attacks

- **Brute Force Attack** – Trying every possible character combination until the password is found.
- **Dictionary Attack** – Using a list of common words, phrases, or leaked passwords to guess the password.
- **Phishing** – Trick users into revealing their password via fake login pages or malicious links.

✅ Best Practices for Strong Passwords

- Minimum **12–16 characters**
- Include **uppercase, lowercase, numbers, and special symbols**
- Avoid **personal information** (name, DOB, etc.)
- Use **passphrases** (e.g., CorrectHorseBatteryStaple!)
- Enable **Multi-Factor Authentication (MFA)** for extra security

📌 Outcome

This exercise demonstrated the importance of using complex, unpredictable passwords to protect against common cyber attacks. Strong passwords greatly increase the time and effort required for an attacker to compromise an account.