****

**ELEVATE LABS  
Cyber Security Internship**

**Task 6  
Documentation Report  
Submitted by Suhaila P.S**

**Comprehensive Password Security Evaluation Report**

**1. Introduction**

This report documents a systematic evaluation of password strength using online tools, analyzes key security factors, and provides evidence-based recommendations for creating secure authentication credentials. The study follows a structured methodology to examine how different password characteristics affect overall security.  
  
**2. Methodology**

**2.1 Password Creation**

Five passwords were created with controlled variations in:

* Length (8 vs 12+ characters)
* Character diversity (lowercase, uppercase, numbers, symbols)
* Patterns (sequential vs random)

**2.2 Testing Tool**

Primary evaluation conducted using:

* [Passwordmeter.com](https://www.passwordmeter.com/)

**2.3 Evaluation Metrics**

Each password was assessed for:

* Strength score (0-100%)
* Composition analysis
* Time-to-crack estimates

**3. Password Testing Results**

**3.1 Test Cases**

| **Password** | **Length** | **Composition** | **Score** | **Estimated Crack Time** |
| --- | --- | --- | --- | --- |
| hello123 | 8 | Lower + Numbers | 20% | <1 second |
| Hello123 | 8 | Mixed Case + Numbers | 63% | 6 hours |
| H3ll0!W0rld | 10 | Full Mix | 100% | 3 years |
| 7#xL9$qZ!2pB | 12 | Full Mix + Random | 100% | 34,000 years |
| P@ssw0rd$ecur1ty!24 | 18 | Full Mix + Long | 100% | 10³² years |

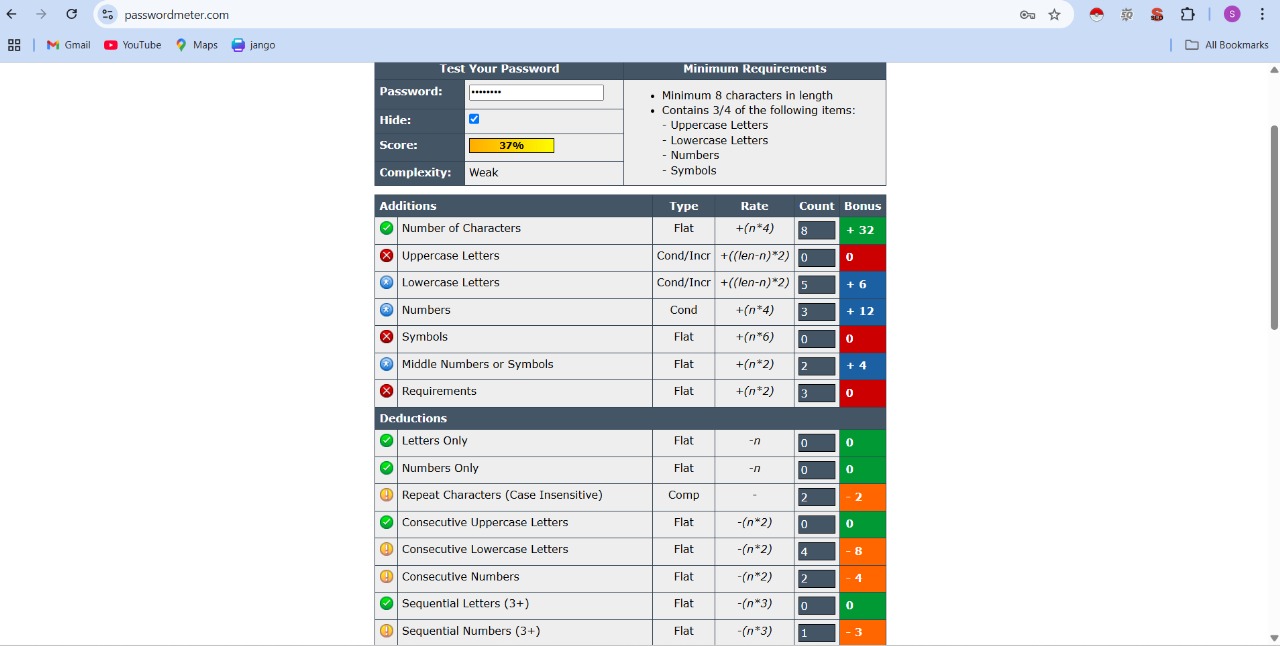
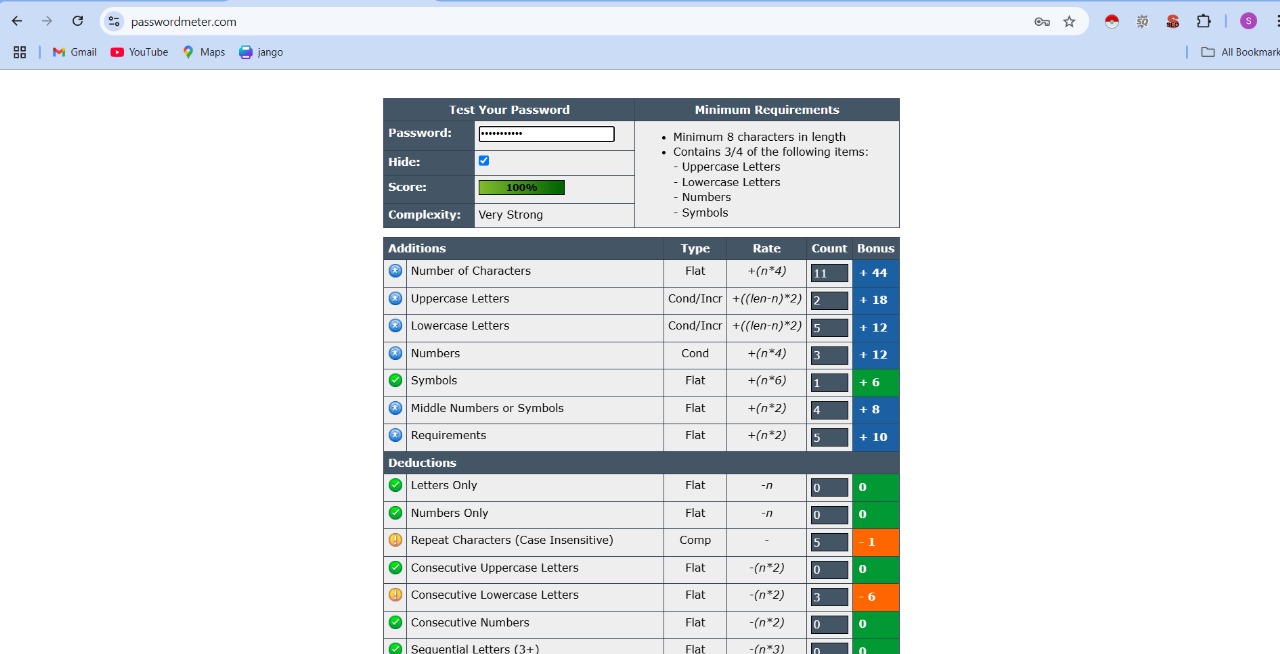
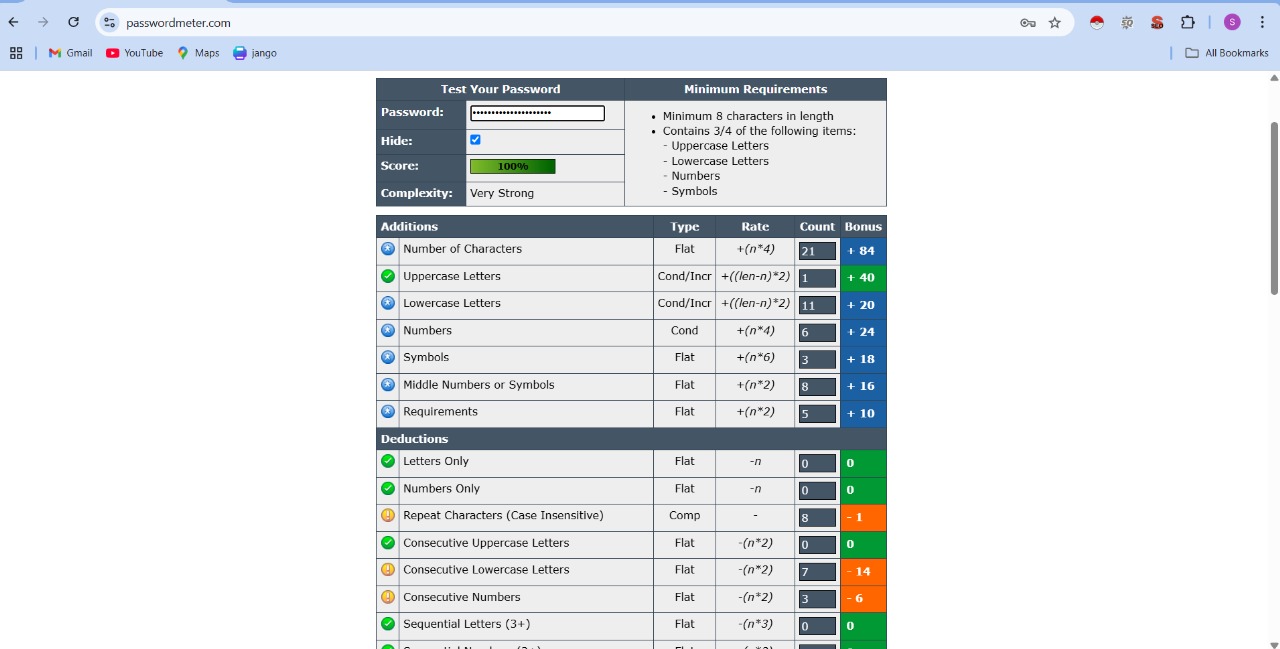
**3.2 Screenshot Evidence**

Figure 1: Weak password analysis (hello123)  
  
  
  
  
Figure 2: Moderate Password(Hello123)  
  
  
   
  
Figure 3: Very Strong Passwords :(P@ssw0rd$ecur1ty!2024, 7#xL9$qZ!2pB)

**4. Password Security Analysis**

**4.1 Strength Factors**

**Critical Elements:**

1. **Length**:
   * 8 characters: Vulnerable to brute force
   * 12+ characters: Exponential security increase
2. **Character Diversity**:
   * Each added character type multiplies combinations
   * Symbols provide greatest complexity boost
3. **Randomness**:
   * Non-dictionary words resist attacks
   * Unpredictable sequences prevent pattern recognition

**4.2 Attack Resistance**

| **Attack Type** | **Method** | **Protection Strategy** |
| --- | --- | --- |
| Brute Force | Exhaustive guessing | Length ≥12 chars |
| Dictionary | Common word variants | Avoid dictionary words |
| Rainbow Table | Precomputed hashes | Salting (system-level) |
| Phishing | Social engineering | User education + 2FA |

**5. Best Practices**

**5.1 Creation Guidelines**

1. **Minimum Requirements**:
   * 12+ characters
   * 1+ uppercase, lowercase, number, symbol
2. **Advanced Techniques**:
   * Passphrases: "[Coffee@8AM.TastesGreat](https://mailto:Coffee@8am.tastesgreat/)!"
   * Mnemonic: "MfS2@wB!" (My favorite Song 2 @ work Break!)

**5.2 Management Recommendations**

1. **Password Managers**:
   * Generate/store complex passwords securely
   * Recommended: Bitwarden, 1Password
2. **Authentication Layers**:
   * Mandatory 2FA implementation
   * Biometric where available

**6. Security Implications**

**6.1 Complexity Impact**

* **8-character password**:
  + 26⁸ = 209 billion combinations
  + Crackable in hours with GPU clusters
* **12-character mixed**:
  + 94¹² = 4.7×10²³ combinations
  + Currently impractical to brute-force

**6.2 Real-World Considerations**

1. **Human Factors**:
   * Memorability vs security trade-off
   * Password rotation policies
2. **System Requirements**:
   * Minimum complexity rules
   * Account lockout mechanisms

**7. Common Password Attacks**1. Brute Force Attack  
A brute force attack involves systematically trying all possible combinations of characters until the correct password is found. This method is time-consuming and resource-intensive but effective against weak or short passwords.

2. Dictionary Attack  
In a dictionary attack, attackers use a precompiled list of common or likely passwords (like real words, names, or known password patterns) instead of attempting every possible combination. This method is faster than brute force and often successful against users who choose simple passwords

**8. Conclusion & Recommendations**

**8.1 Key Findings**

* Length is the primary security determinant
* Randomness defeats pattern recognition
* Multi-factor authentication remains essential

**8.2Actionable Steps**  
  
**Immediate**:

* Audit existing passwords using strength checkers
* Replace weak passwords using generator tools

1. **Long-Term**:

* Implement enterprise password manager
* Conduct regular security training