# Cyber Security Internship – Task 6

## Task Name: Create a Strong Password and Evaluate Its Strength

**Name:** Dhruvik Variya
**Date:** 30 June 2025

---

## Objective

To understand what makes a password strong by creating multiple passwords with varying complexity, testing them using an online password strength checker, analyzing feedback, and learning best practices to avoid weak passwords and common attacks like brute force or dictionary attacks.

---

## Tools Used

- Website: https://passwordmeter.com
- Screenshots captured from each test
- Manual review of security feedback

---

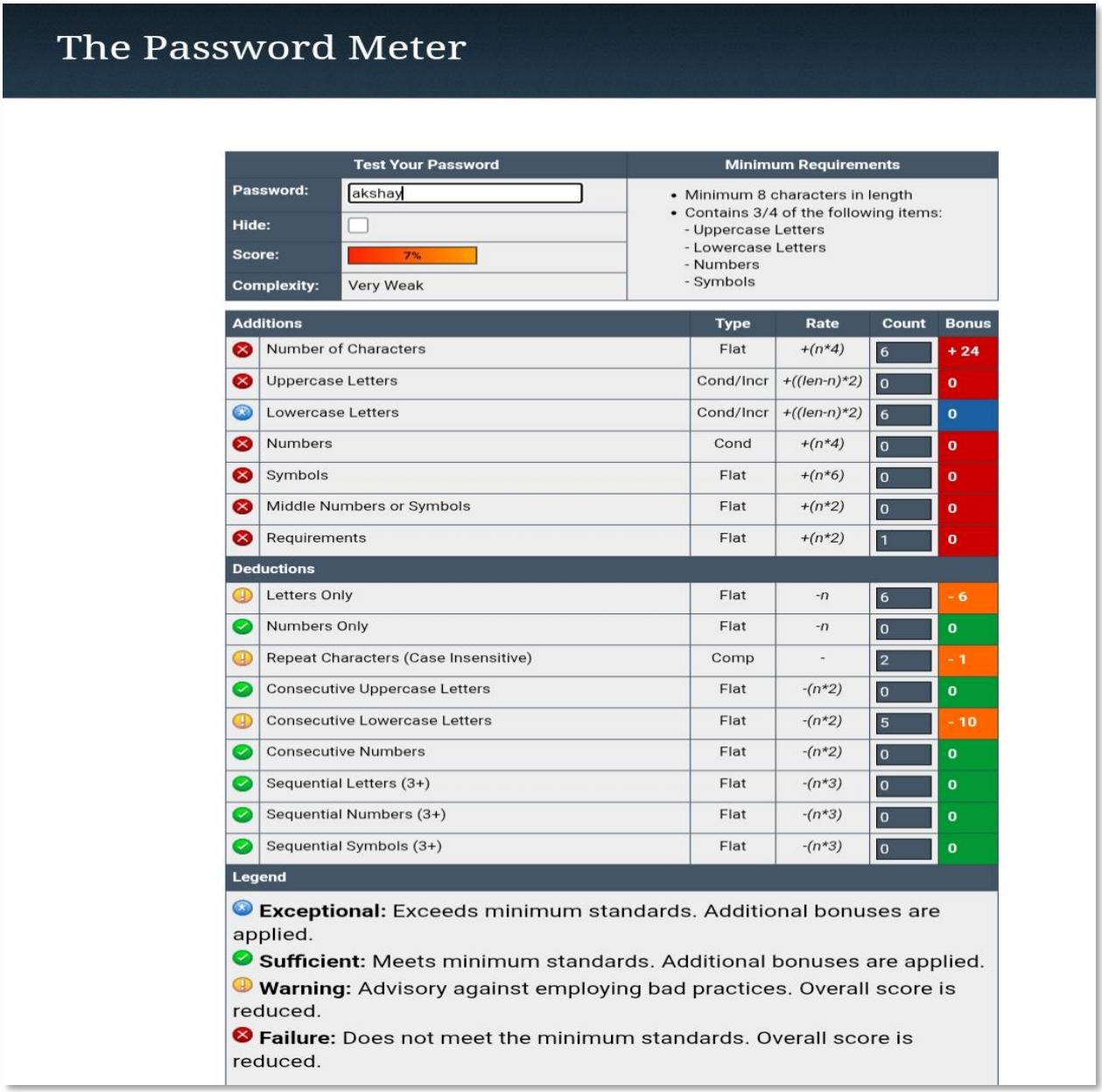
## Password Testing and Evaluation

I created and tested five different passwords ranging from very weak to very strong. Below are the full details:

---

## 1. Password: `akshay`

- **Score:** 7%
- **Complexity:** Very Weak
- **Feedback:**
  - Only lowercase letters
  - Too short (6 characters)
  - No numbers, uppercase, or special characters



The Password Meter

| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | akshay | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | ☐ | |
| Score: | 7% | |
| Complexity: | Very Weak | |

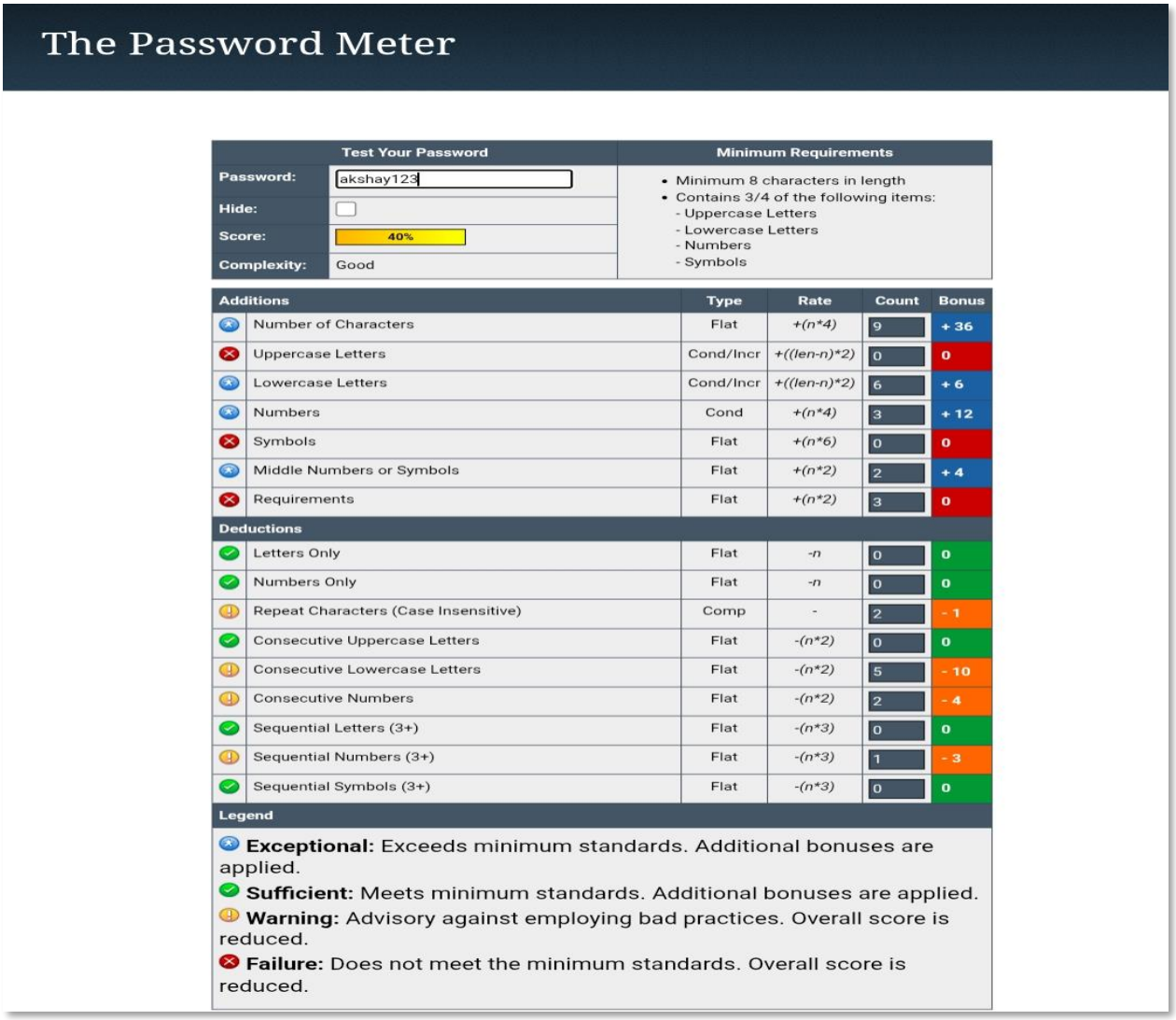
| Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|
| Number of Characters | Flat | +(n*4) | 6 | + 24 |
| Uppercase Letters | Cond/Incr | +((len-n)*2) | 0 | 0 |
| Lowercase Letters | Cond/Incr | +((len-n)*2) | 6 | 0 |
| Numbers | Cond | +(n*4) | 0 | 0 |
| Symbols | Flat | +(n*6) | 0 | 0 |
| Middle Numbers or Symbols | Flat | +(n*2) | 0 | 0 |
| Requirements | Flat | +(n*2) | 1 | 0 |
| **Deductions** | | | | |
| Letters Only | Flat | -n | 6 | - 6 |
| Numbers Only | Flat | -n | 0 | 0 |
| Repeat Characters (Case Insensitive) | Comp | - | 2 | - 1 |
| Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Lowercase Letters | Flat | -(n*2) | 5 | - 10 |
| Consecutive Numbers | Flat | -(n*2) | 0 | 0 |
| Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Numbers (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

**Legend**

**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
**Sufficient:** Meets minimum standards. Additional bonuses are applied.
**Warning:** Advisory against employing bad practices. Overall score is reduced.
**Failure:** Does not meet the minimum standards. Overall score is reduced.

- **Result:** ❌ Failed basic password standards
- **Conclusion:** Easily guessable and vulnerable to brute force attacks

## 2. Password: `akshay123`



The Password Meter

| Test Your Password | |
|---|---|
| Password: | akshay123 |
| Hide: | ☐ |
| Score: | 40% |
| Complexity: | Good |

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

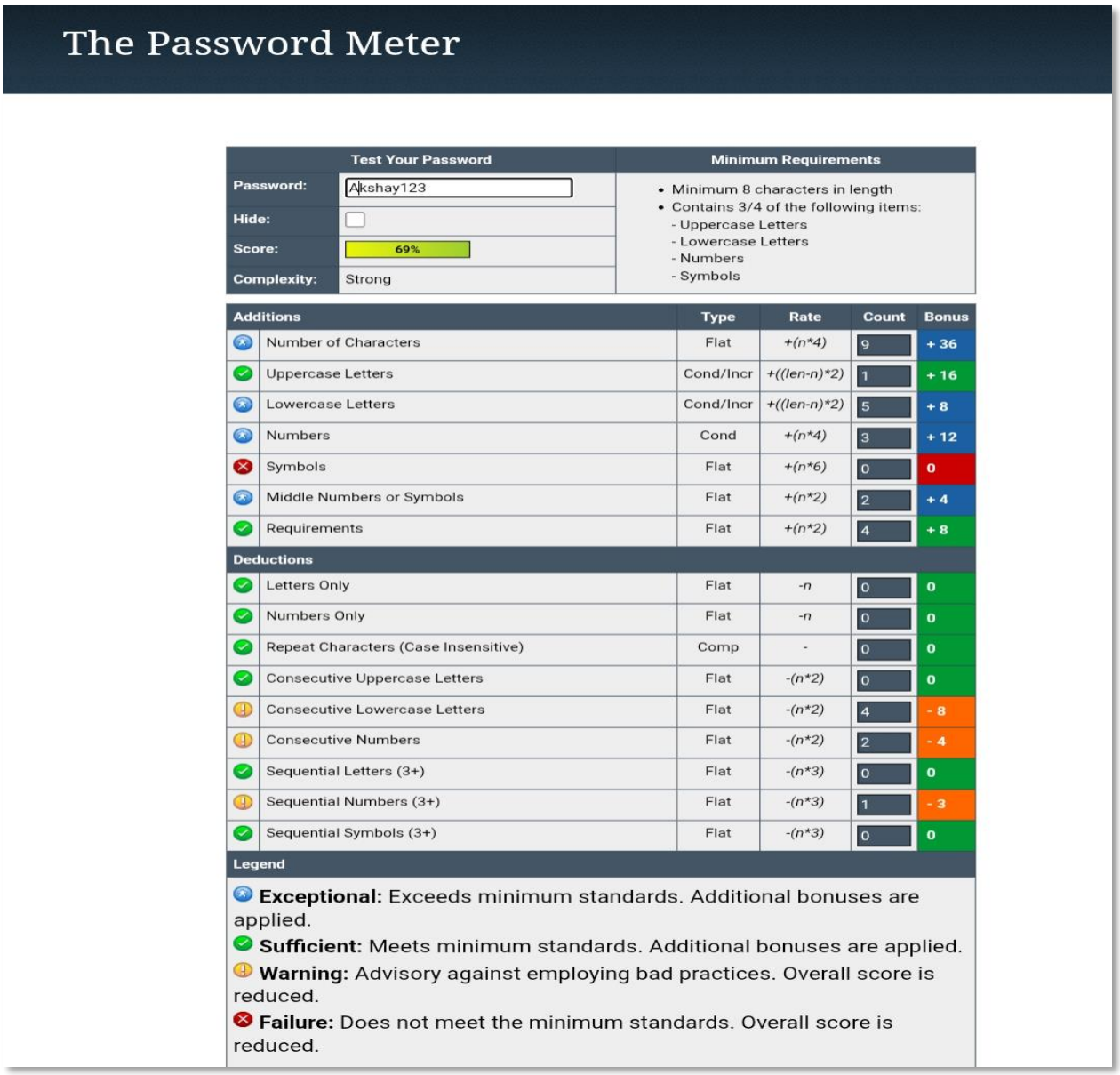
| Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|
| Number of Characters | Flat | +(n*4) | 9 | + 36 |
| Uppercase Letters | Cond/Incr | +((len-n)*2) | 0 | 0 |
| Lowercase Letters | Cond/Incr | +((len-n)*2) | 6 | + 6 |
| Numbers | Cond | +(n*4) | 3 | + 12 |
| Symbols | Flat | +(n*6) | 0 | 0 |
| Middle Numbers or Symbols | Flat | +(n*2) | 2 | + 4 |
| Requirements | Flat | +(n*2) | 3 | 0 |
| **Deductions** | | | | |
| Letters Only | Flat | -n | 0 | 0 |
| Numbers Only | Flat | -n | 0 | 0 |
| Repeat Characters (Case Insensitive) | Comp | - | 2 | - 1 |
| Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Lowercase Letters | Flat | -(n*2) | 5 | - 10 |
| Consecutive Numbers | Flat | -(n*2) | 2 | - 4 |
| Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Numbers (3+) | Flat | -(n*3) | 1 | - 3 |
| Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

**Legend**

**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
**Sufficient:** Meets minimum standards. Additional bonuses are applied.
**Warning:** Advisory against employing bad practices. Overall score is reduced.
**Failure:** Does not meet the minimum standards. Overall score is reduced.

- **Score:** 40%
- **Complexity:** Good
- **Feedback:**
  - Includes numbers
  - Still missing uppercase and symbols
  - Repeated/consecutive lowercase letters and numbers
- **Result:** Slightly better, but still weak against dictionary attacks
- **Conclusion:** Needs more variation in character types

## 3. Password: `Akshay123`



The Password Meter

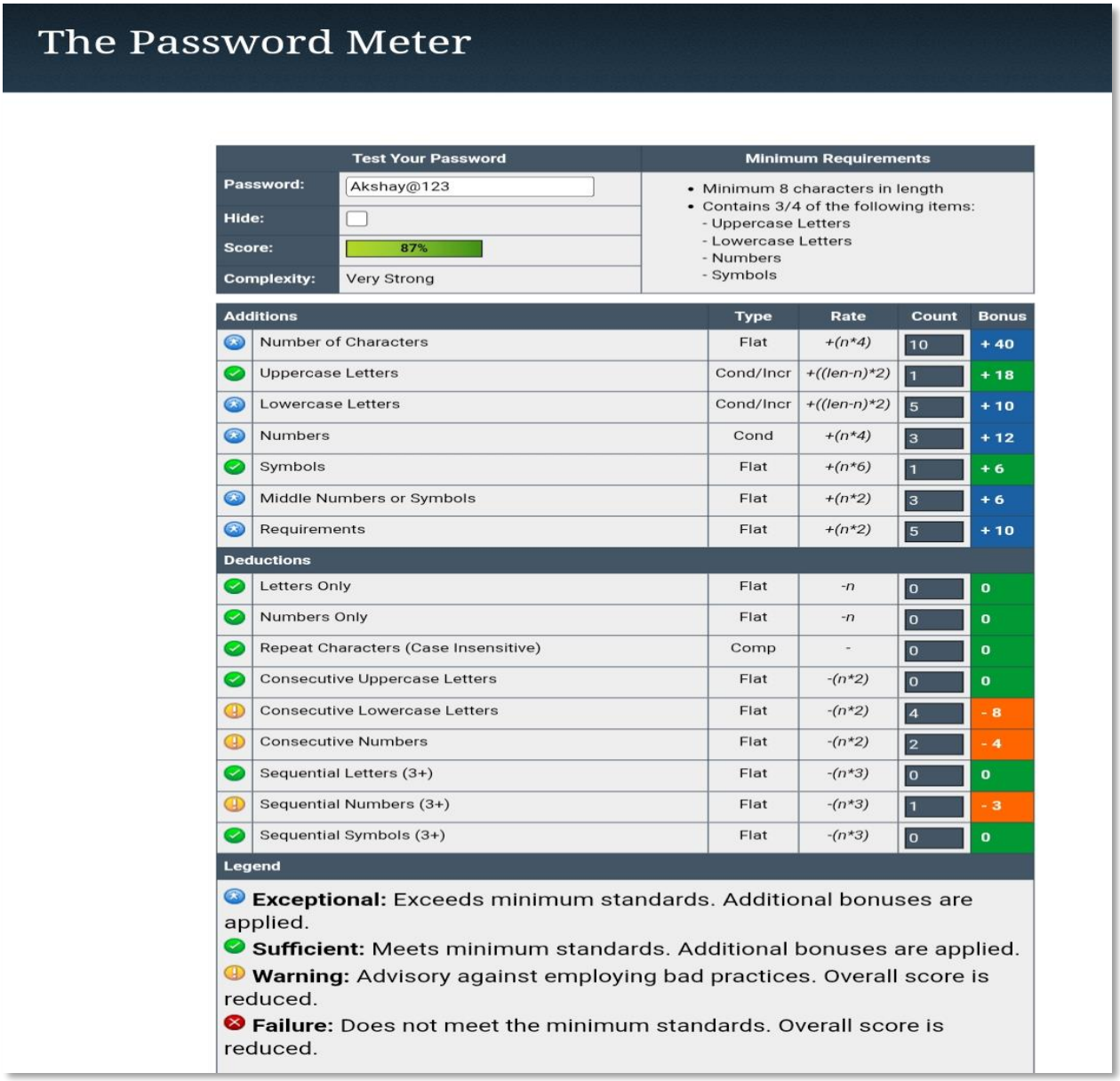
| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | Akshay123 | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | ☐ | |
| Score: | 69% | |
| Complexity: | Strong | |

| Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|
| Number of Characters | Flat | +(n*4) | 9 | + 36 |
| Uppercase Letters | Cond/Incr | +((len-n)*2) | 1 | + 16 |
| Lowercase Letters | Cond/Incr | +((len-n)*2) | 5 | + 8 |
| Numbers | Cond | +(n*4) | 3 | + 12 |
| Symbols | Flat | +(n*6) | 0 | 0 |
| Middle Numbers or Symbols | Flat | +(n*2) | 2 | + 4 |
| Requirements | Flat | +(n*2) | 4 | + 8 |
| **Deductions** | | | | |
| Letters Only | Flat | -n | 0 | 0 |
| Numbers Only | Flat | -n | 0 | 0 |
| Repeat Characters (Case Insensitive) | Comp | - | 0 | 0 |
| Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Lowercase Letters | Flat | -(n*2) | 4 | - 8 |
| Consecutive Numbers | Flat | -(n*2) | 2 | - 4 |
| Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Numbers (3+) | Flat | -(n*3) | 1 | - 3 |
| Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

**Legend**

**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
**Sufficient:** Meets minimum standards. Additional bonuses are applied.
**Warning:** Advisory against employing bad practices. Overall score is reduced.
**Failure:** Does not meet the minimum standards. Overall score is reduced.

- **Score:** 69%
- **Complexity:** Strong
- **Feedback:**
  - Includes uppercase, lowercase, and numbers
  - No special characters
- **Result:** Acceptable for low-sensitivity accounts
- **Conclusion:** Stronger due to uppercase, but still not ideal without a symbol



The Password Meter

| Test Your Password | |
|---|---|
| Password: | Akshay@123 |
| Hide: | ☐ |
| Score: | 87% |
| Complexity: | Very Strong |

**Minimum Requirements**

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

| Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|
| Number of Characters | Flat | +(n*4) | 10 | + 40 |
| Uppercase Letters | Cond/Incr | +((len-n)*2) | 1 | + 18 |
| Lowercase Letters | Cond/Incr | +((len-n)*2) | 5 | + 10 |
| Numbers | Cond | +(n*4) | 3 | + 12 |
| Symbols | Flat | +(n*6) | 1 | + 6 |
| Middle Numbers or Symbols | Flat | +(n*2) | 3 | + 6 |
| Requirements | Flat | +(n*2) | 5 | + 10 |
| **Deductions** | | | | |
| Letters Only | Flat | -n | 0 | 0 |
| Numbers Only | Flat | -n | 0 | 0 |
| Repeat Characters (Case Insensitive) | Comp | - | 0 | 0 |
| Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Lowercase Letters | Flat | -(n*2) | 4 | - 8 |
| Consecutive Numbers | Flat | -(n*2) | 2 | - 4 |
| Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Numbers (3+) | Flat | -(n*3) | 1 | - 3 |
| Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

**Legend**

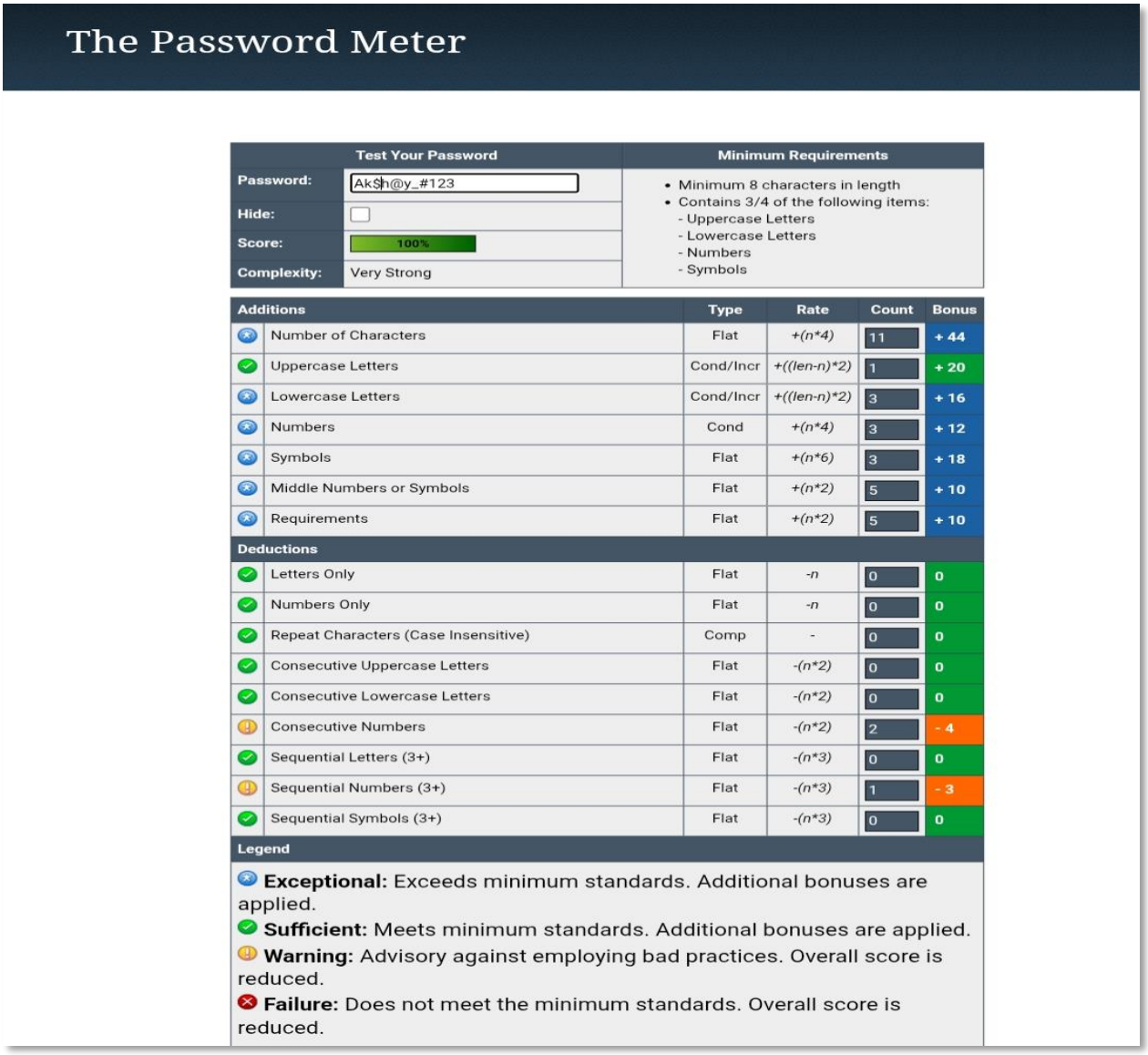
**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
**Sufficient:** Meets minimum standards. Additional bonuses are applied.
**Warning:** Advisory against employing bad practices. Overall score is reduced.
**Failure:** Does not meet the minimum standards. Overall score is reduced.

## 4. Password: `Akshay@123`

- **Score:** 87%
- **Complexity:** Very Strong
- **Feedback:**
  - Meets most criteria: length, uppercase, lowercase, number, and one symbol
- **Result:** Excellent and secure for most services
- **Conclusion:** Balanced structure, a good example of a strong, usable password

## 5. Password: `Ak$h@y_#123`

- **Score:** 100%
- **Complexity:** Very Strong
- **Feedback:**



The Password Meter

| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | Ak$h@y_#123 | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | ☐ | |
| Score: | 100% | |
| Complexity: | Very Strong | |

| Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|
| Number of Characters | Flat | +(n*4) | 11 | + 44 |
| Uppercase Letters | Cond/Incr | +((len-n)*2) | 1 | + 20 |
| Lowercase Letters | Cond/Incr | +((len-n)*2) | 3 | + 16 |
| Numbers | Cond | +(n*4) | 3 | + 12 |
| Symbols | Flat | +(n*6) | 3 | + 18 |
| Middle Numbers or Symbols | Flat | +(n*2) | 5 | + 10 |
| Requirements | Flat | +(n*2) | 5 | + 10 |
| **Deductions** | | | | |
| Letters Only | Flat | -n | 0 | 0 |
| Numbers Only | Flat | -n | 0 | 0 |
| Repeat Characters (Case Insensitive) | Comp | - | 0 | 0 |
| Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Lowercase Letters | Flat | -(n*2) | 0 | 0 |
| Consecutive Numbers | Flat | -(n*2) | 2 | - 4 |
| Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| Sequential Numbers (3+) | Flat | -(n*3) | 1 | - 3 |
| Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

**Legend**

**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
**Sufficient:** Meets minimum standards. Additional bonuses are applied.
**Warning:** Advisory against employing bad practices. Overall score is reduced.
**Failure:** Does not meet the minimum standards. Overall score is reduced.

  - Long length (11 characters)
  - Contains all types: uppercase, lowercase, numbers, and multiple symbols
- **Result:** ✅ Ideal password for sensitive accounts
- **Conclusion:** Excellent complexity; resistant to brute-force and dictionary attacks

---

## 📊 Summary Table

| Password | Score | Complexity | Strength Notes |
|---|---|---|---|
| `akshay` | 7% | Very Weak | Only lowercase, too short |
| `akshay123` | 40% | Good | Lacks uppercase & symbols |
| `Akshay123` | 69% | Strong | Missing symbol, decent structure |
| `Akshay@123` | 87% | Very Strong | Secure and well-balanced |
| `Ak$h@y_#123` | 100% | Very Strong | Excellent mix of all character types and length |

---

## 🧠 Key Tips Learned from Evaluation

- Always use a **minimum of 8–12 characters** for strength.
- Mix **uppercase, lowercase, numbers, and special characters**.
- Avoid using personal names or easily guessed combinations.
- **Passphrases** like `Sunny@Night#2025` are easy to remember yet secure.
- **Avoid repeating characters** or common patterns (e.g., `123`, `abc`).
- Password strength greatly improves with **symbol placement and randomness**.

---

## 🔒 Common Password Attacks

---

### 1. 💣 Brute Force Attack

**Definition:**
A brute force attack systematically tries **every possible combination** of characters until it finds the correct password.

**How it works:**

- Attackers use automated scripts or tools (like Hydra, John the Ripper, or Hashcat).
- It tries `a`, then `aa`, `ab`, `abc`, and so on until the correct password is found.
- Short and simple passwords are cracked **very quickly**.

**Defence:**

- Use **long and complex passwords** (e.g., 12+ characters).
- Implement **account lockouts** after failed login attempts.
- Enable **multi-factor authentication (MFA)**.

---

## 2. 📚 Dictionary Attack

**Definition:**
This attack uses a predefined **list of commonly used words or leaked passwords** to guess a password.

**How it works:**

- The attacker tries passwords like `password`, `123456`, `welcome`, `qwerty`, etc.
- They use large "dictionary files" created from real leaked databases.

**Defense:**

- Avoid using **common words, names, or patterns**.
- Don't use simple variations like `Password123!`.
- Use **randomized characters or passphrases** instead.

---

## 🔐 How Password Complexity Affects Security – Summary

Password complexity plays a **crucial role** in protecting against cyberattacks like brute force, dictionary attacks, and credential stuffing. A complex password is harder to guess, slower to crack, and less likely to be found in leaked databases.

---

### 🧠 Key Factors of Complexity:

1. **Length:**
   - Longer passwords take exponentially more time to crack.
   - Minimum recommended: **12+ characters**.
2. **Character Variety:**
   - Use a mix of:
     - ✅ Uppercase (A–Z)
     - ✅ Lowercase (a–z)
     - ✅ Numbers (0–9)
     - ✅ Symbols (@, #, $, etc.)

- Increases the number of possible combinations.

3. **Unpredictability:**
   - Avoid names, dictionary words, and keyboard patterns.
   - Use **random phrases** or symbol substitutions (e.g., `@` for `a`).

---

## 🛡️ Why Complexity Matters:

| Without Complexity | With Complexity |
|---|---|
| **Easy to guess/crack** | Difficult to guess or automate |
| **Vulnerable to dictionary attacks** | Resistant to brute force |
| **Found in leaked data** | Unique and safer |

---

## ✅ Example:

- **Weak:** `password123` (easy to guess, short, common)
- **Strong:** `T!m3@R!ver_2025` (long, complex, unique)

---

## ✅ Conclusion

This task helped me understand how small changes in a password's structure (length, character variety, and symbols) drastically affect its strength. Tools like PasswordMeter give great feedback on password quality, and this evaluation reinforced why **strong passwords are critical to cyber defence**.

Now I can confidently:

- Build secure passwords
- Analyse weaknesses
- Educate others about password safety
- Avoid common traps that lead to credential leaks

---