**Task 6 : Create a Strong Password and Evaluate Its Strength.**

**Objective:** Understand what makes a password strong and test it against password strength tools.

**Tools:** Online free password strength checkers (e.g., passwordmeter.com).

**Deliverables:** Report showing password strength results and explanation.

1. **Create multiple passwords with varying complexity.**

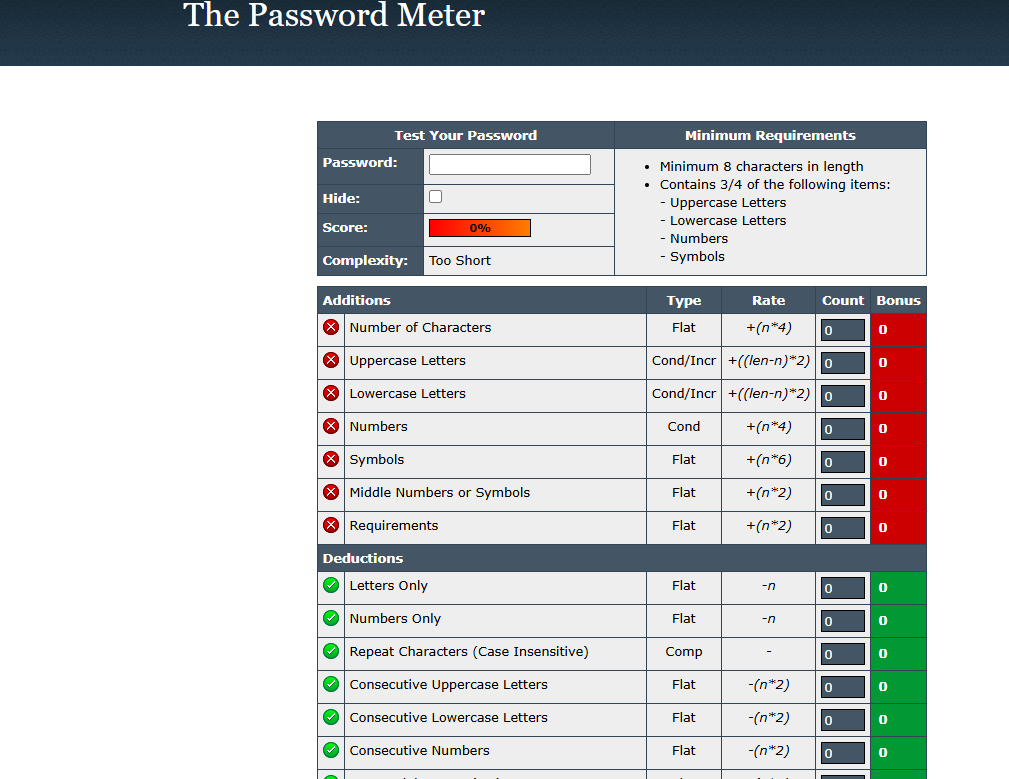
**2. Use uppercase, lowercase, numbers, symbols, and length variations.**

a) elevatelabsinternship

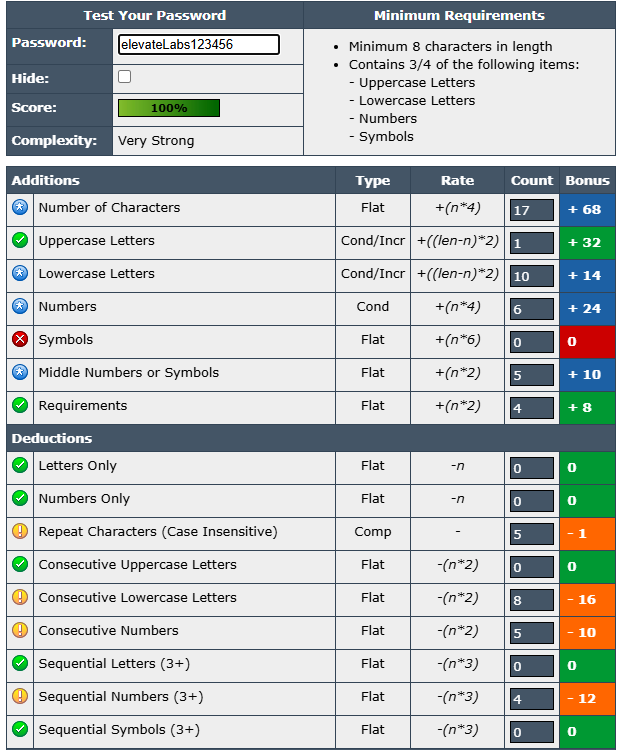
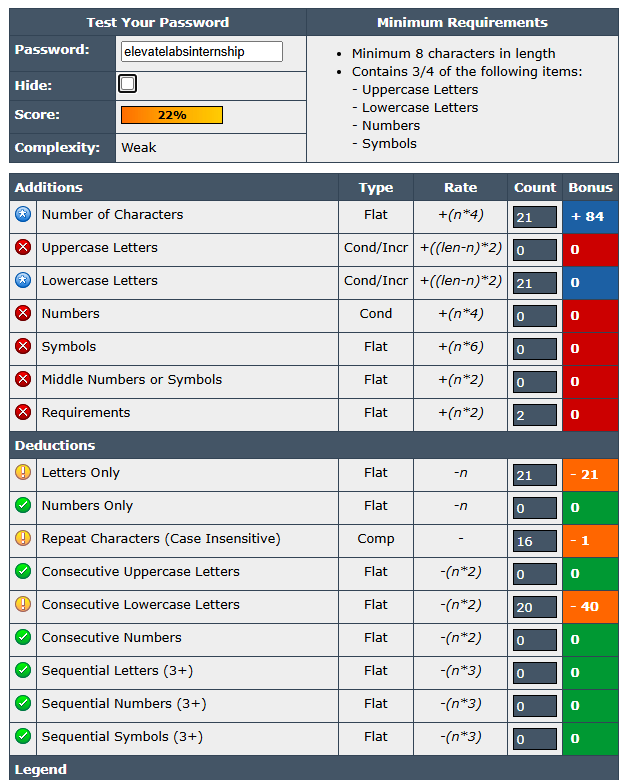
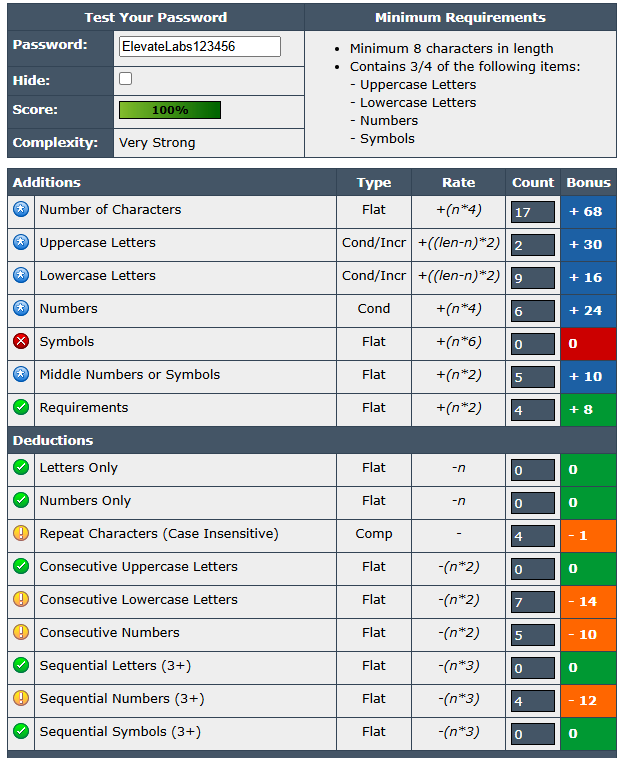
b) elevateLabs123456

c) ElevateLabs123456

d) ElevateLabs\*##&123456

**3. Test each password on password strength checker.**

**4. Note scores and feedback from the tool.**



**5. Identify best practices for creating strong passwords.**

To create a strong password, aim for a password that is at least 12 characters long, uses a combination of uppercase and lowercase letters, numbers, and symbols, and avoids personal information or easily guessable words and patterns.

**Here's a more detailed breakdown:**

**1) Length:**

* Aim for a password that is at least 12 characters long.
* The longer the password, the more difficult it is to crack.
* Consider passwords of 14 or more characters for even greater security.

**2) Complexity:**

* Include a mix of uppercase and lowercase letters, numbers, and symbols.
* Using a combination of these character types makes the password harder to guess through brute-force attacks.

**3) Uniqueness:**

* Avoid using the same password for multiple accounts.
* If a hacker gains access to one account with the same password, they could potentially access other accounts.

**4) Personal Information:**

* Avoid using personal information like your name, birthday, or phone number.
* This information can be easily found online and used to guess your password.

**5) Common Words and Patterns:**

* Avoid using common words, phrases, or easily guessable patterns.
* Hackers may use dictionary-based attacks to try and guess your password.

**6) Memorable Passwords:**

* Consider using a memorable phrase or a phrase that has some meaning to you.
* You can then use the first letter of each word in the phrase to create a password.
* For example, you could use the phrase "I love to eat pizza every Friday night" and create the password "Il2ep3Fn!".

**7) Password Generators:**

* Consider using a password generator tool to create random, complex, and unique passwords.
* Password managers can also generate strong passwords for you and store them securely.

**6. Write down tips learned from the evaluation.**

Tips are as follows:

1. Use a password that is at least 12 characters long.

1. Include a mix of uppercase and lowercase letters, numbers, and symbols.
2. Avoid using the same password for multiple accounts.
3. Avoid using personal information like your name, birthday, or phone number.
4. Avoid using common words, phrases, or easily guessable patterns.
5. Consider using memorable phrase/ phrase that has some meaning to you.
6. Consider using a password generator tool to create random, complex, and unique passwords.

**7. Research common password attacks (brute force, dictionary).**

**🔐 Brute Force Attack**

This attack tries all possible combinations of characters until the correct password is found.

It is time-consuming and computationally intensive but guarantees success eventually.

Brute force tools can automate the process and target weak passwords easily.

Using complex passwords and account lockout mechanisms helps prevent it.

**📖 Dictionary Attack**

It uses a predefined list of likely passwords (dictionary) to guess the correct one.

The attack relies on users choosing common or simple passwords found in the list.

It is faster than brute force but limited to the words in the dictionary.

To defend against it, users should avoid predictable or common passwords.

**8. Summarize how password complexity affects security.**

Password complexity, which refers to the difficulty in guessing or cracking a password, directly impacts security.

More complex passwords, characterized by length, variety of characters (uppercase, lowercase, numbers, symbols), and unpredictability, are significantly harder to crack using brute force or dictionary attacks.

This increased difficulty translates to better security, making it more challenging for unauthorized individuals to access accounts and data