**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 Used:**

* Online Password Strength Checker: <https://passwordmeter.com>

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

### Step-by-Step Summary Based on Guidelines:

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

* Weak Password Tested: “abcd”
* Medium Password Tested: “abcdefgh123”
* Strong Password Tested: “Abcdefg123$Xy”

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

* Weak: Only lowercase, short (4 characters), no numbers/symbols.
* Medium: Lowercase and numbers, longer (11 characters), no symbols/uppercase.
* Strong: Includes uppercase, lowercase, numbers, symbols; length is 13 characters.

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

* Weak Password Score: 34% (Weak)
* Medium Password Score: 43% (Good)
* Strong Password Score: 100% (Very Strong)

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

* Weak password lacked complexity (no uppercase, symbols, short length).
* Medium password met length but missed uppercase and symbols.
* Strong password fulfilled all requirements (length, complexity, diversity).

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

* Include all character types: uppercase, lowercase, numbers, symbols.
* Use at least 12–14 characters.
* Avoid repetition and sequential characters.
* Place numbers/symbols in the middle.

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

* Password strength depends heavily on diversity and position of characters.
* Short passwords, even with some variety, are not secure.
* Repeated or sequential characters reduce password strength.

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

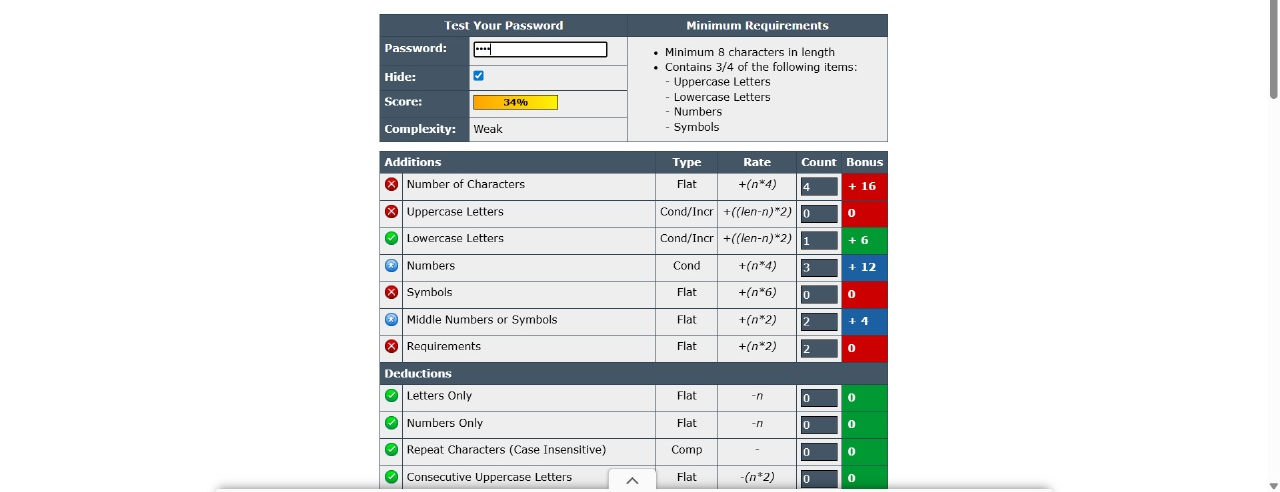
* **Brute Force:** Tries all possible combinations; longer, complex passwords resist it.
* **Dictionary Attacks:** Use common words; random and diverse characters defend against it.

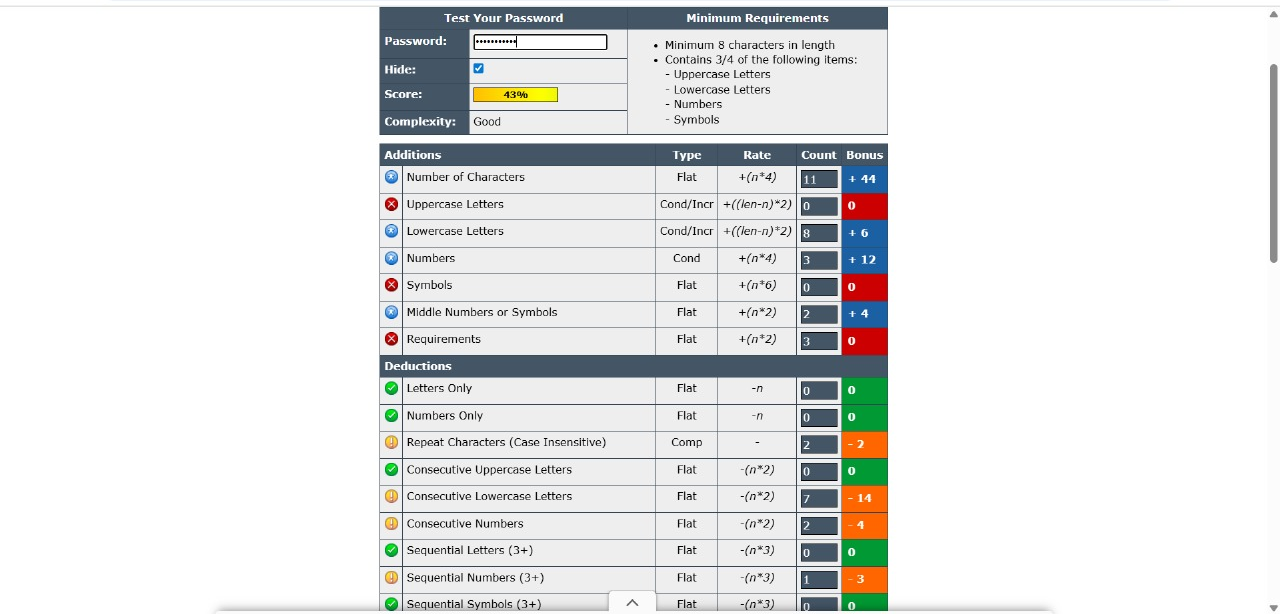
**8. Summarize how password complexity affects security:**

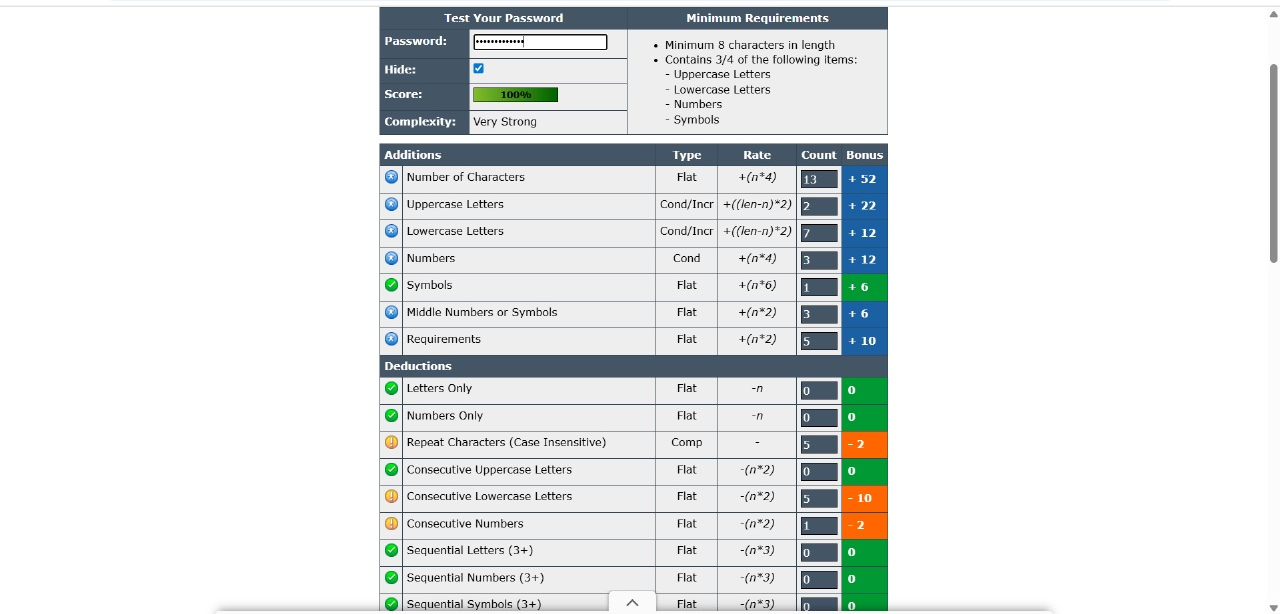
* Higher complexity (length, varied characters) increases resistance to attacks.
* Meeting complexity requirements helps in achieving strong ratings and real security.
* Strong passwords reduce vulnerability to automated and manual attacks.

**Screenshots:**

* **Weak Password Test Result:** Weak Password



* **Medium Password Test Result:** Medium Password
* **Strong Password Test Result:** Strong Password



**Conclusion:** Creating strong passwords involves using a mix of character types, avoiding patterns, and ensuring sufficient length. Regular testing and awareness of attack types support stronger personal security practices.