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).

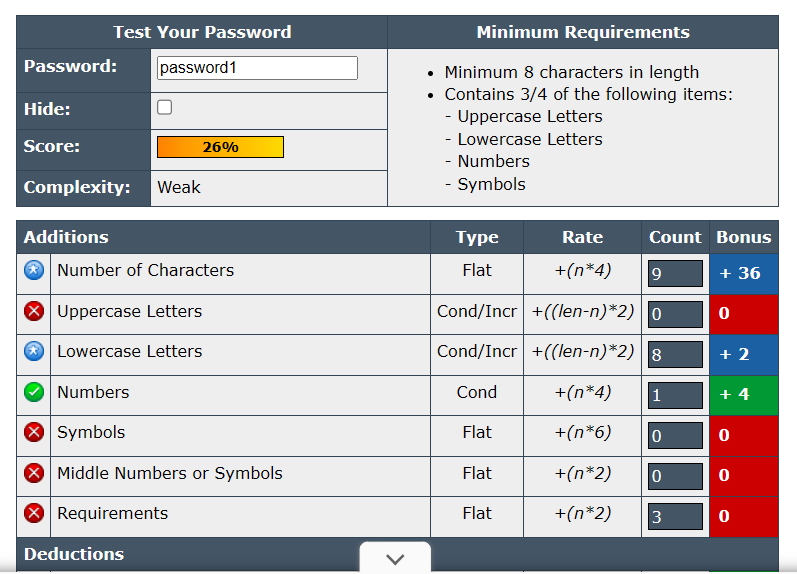
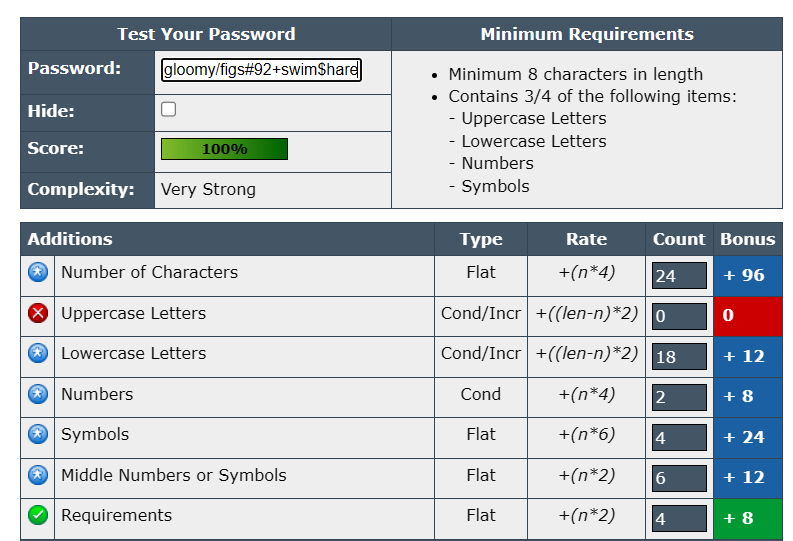
**Deliverables**: Report showing password strength results and explanation.

Step-by-Step Configuration :

Step-1: Create Multiple Password

|  |  |  |
| --- | --- | --- |
| **Complexity Level** | **Example** | **Reason** |
| Weak | password1 | Commman Word + Number |
| Medium | Password1 | Capitalized + number |
| Strong | P@ssw0rd! | Leetspeak,but predictable |
| Stronger | S!mpleYetLong123 | Long,mix case,digit,symbol |
| Very Strong | glacier-harp7!Paper | Passphrase with symbols & mixed case |
| Extreme | gloomy/figs#92+swim$hare | Long, complex, high entropy |

Step-2 : Check Password Strength using tool

* <https://passwordmeter.com>
* <https://www.security.org/how-secure-is-my-password/>

Step-3 : Test Each Password

For each password:

1. Go to the **first** checker, enter the password, note:
   * **Score** (percentage or rating)
   * **Feedback** (suggestions for improvement)
   * **Estimated crack time** (if shown)
2. Repeat with the **second** checker.
3. Record results in a table (paper, doc, or spreadsheet).

Step-4 : Research Common Password Attacks

Summarize in your own words:

* **Brute Force:** Tries every possible combination.
* **Dictionary Attack:** Uses lists of common words/phrases.
* **Credential Stuffing:** Uses stolen passwords from breaches.
* **Password Spraying:** Tries common passwords across many accounts.