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

**Objective:**

* To understand what makes a password strong and to test multiple passwords using an online strength checker.

**Method:**

* Four passwords with different complexity levels were created and tested using passwordmeter.com. Scores and feedback were recorded for analysis.

**Results:**

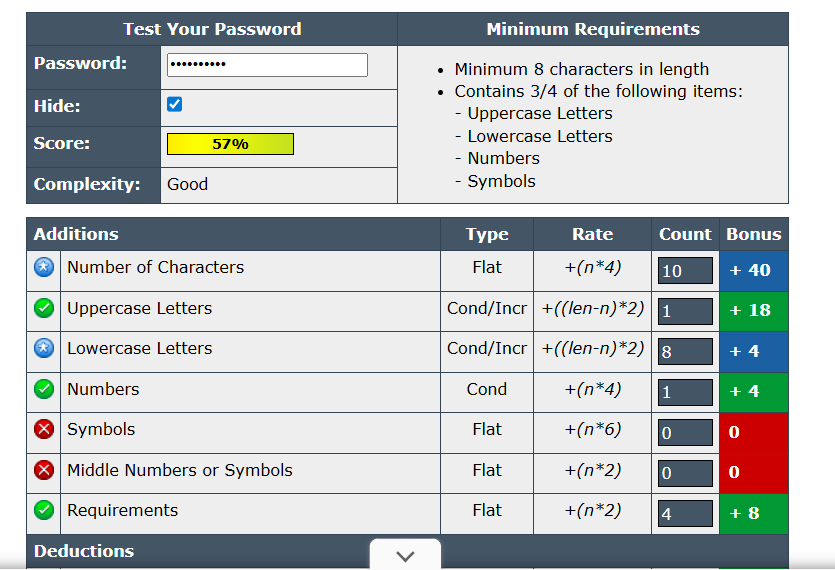
|  |  |  |  |
| --- | --- | --- | --- |
| Password | Score (%) | Feedback from Tool | Strength Level |
| sunshine123 | 28% | Too short, no symbols, predictable pattern | Weak |
| Summer2025 | 48% | Add symbols, increase length | Medium |
| S@f3H0u$e!2025 | 88% | Very strong, minor improvement: longer length | Strong |
| R#9x!q@72Lz$B8vM | 100% | Excellent: mix of all types, long length | Very Strong |

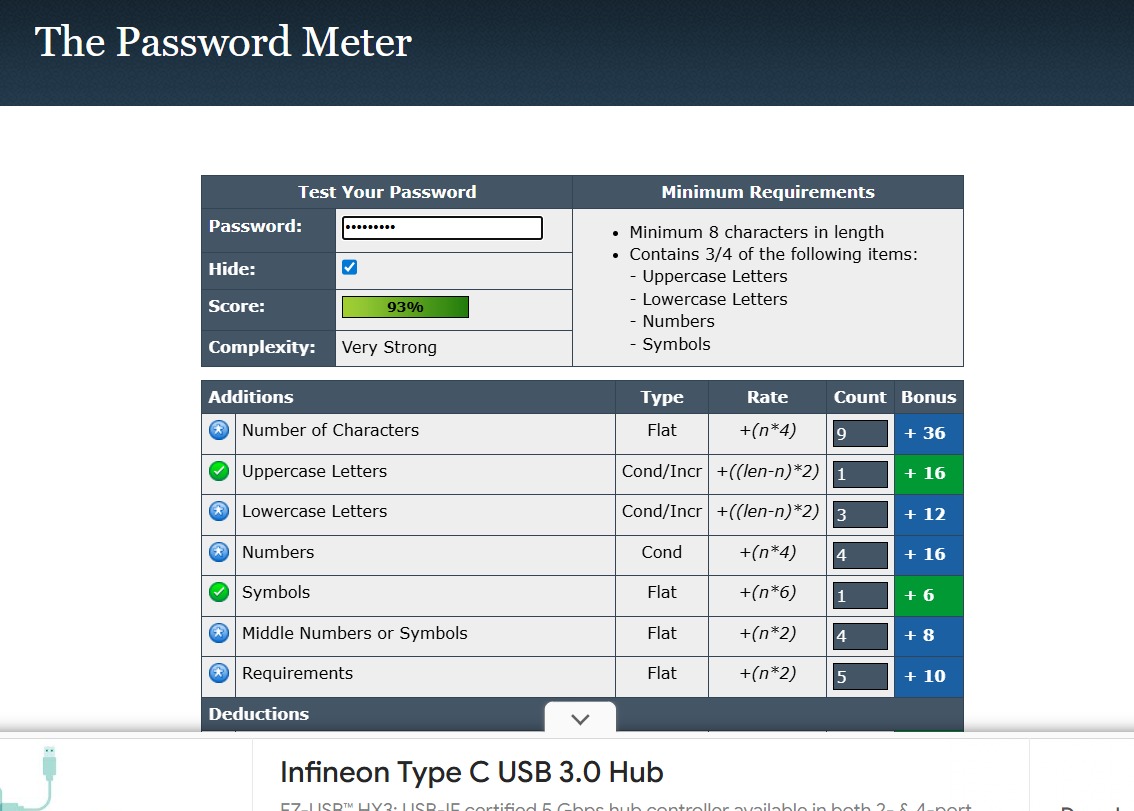
**Best Practices Learned:**

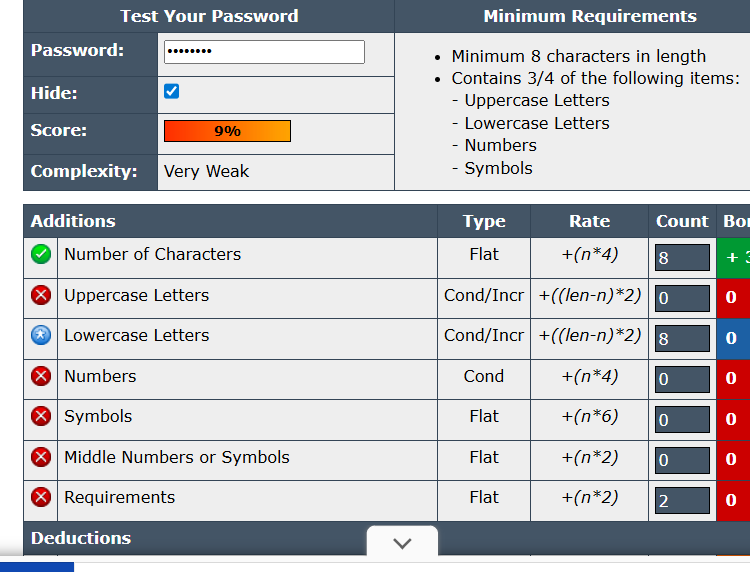
* Minimum length 12-16 characters.
* Use uppercase, lowercase, numbers, and special characters
* Avoid dictionary words and personal info
* Use random sequences or passphrases

**Common Password Attacks**

1. Brute Force: Tries all combinations  
2. Dictionary Attack: Tries common words/passwords  
3. Credential Stuffing: Reuses leaked passwords





****

**Conclusion:**

Complexity greatly increases security by making it harder and slower for attackers to crack a password. Using long, random, and mixed-character passwords is the most effective defense against password-related attacks.