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

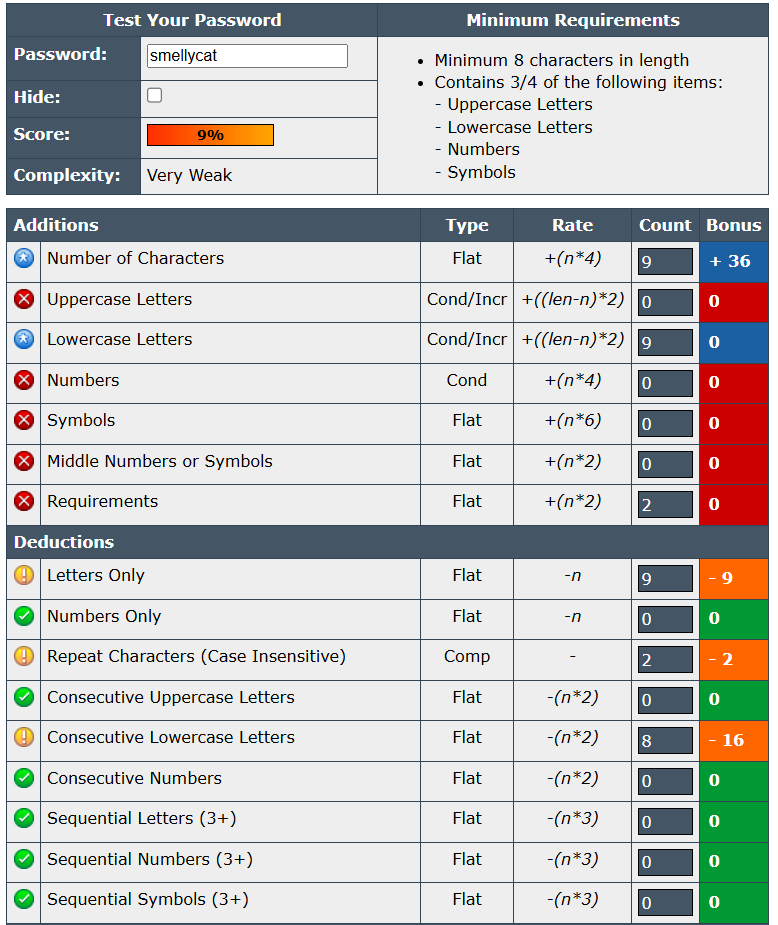
**Step 1: Passwords Created**

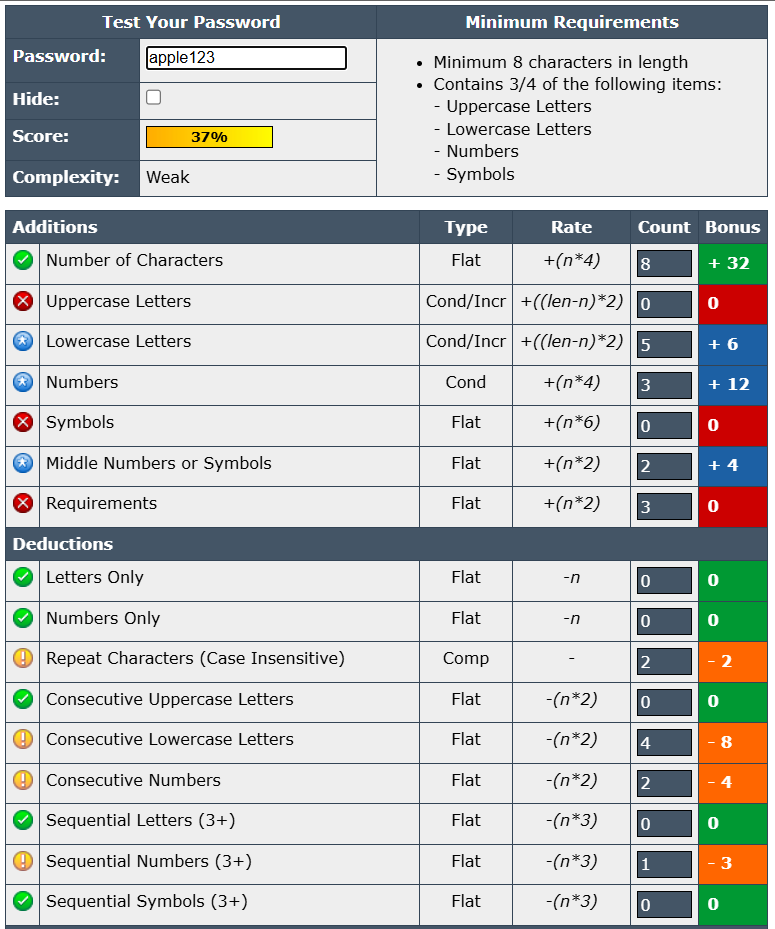
Five passwords were created with varying complexity to analyze how length, character types, and randomness affect overall strength.

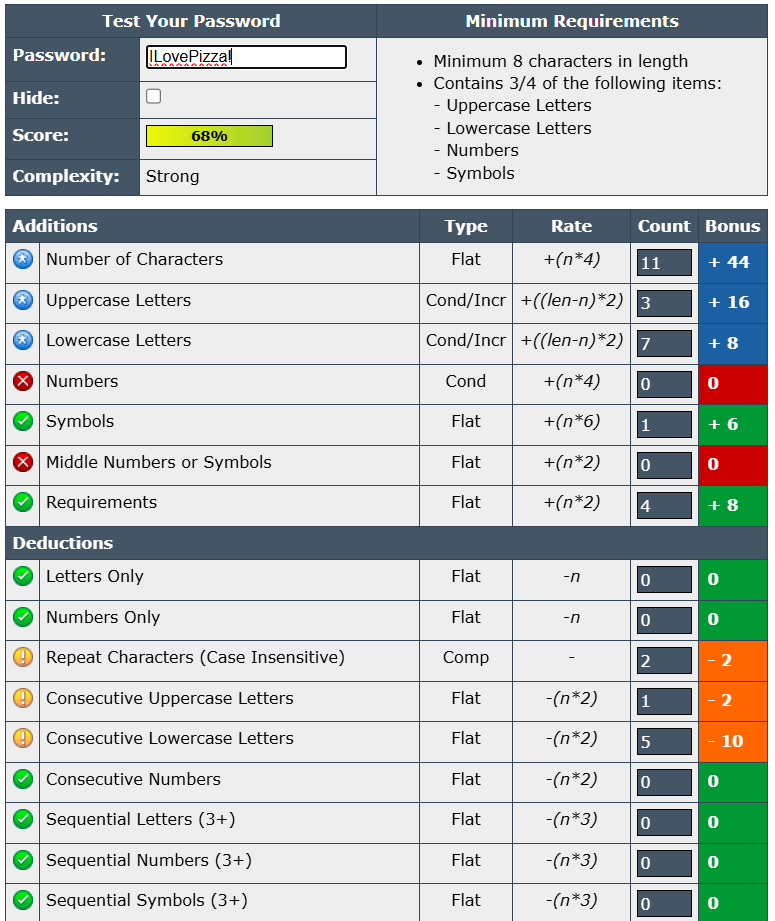
|  |  |  |
| --- | --- | --- |
| **No.** | **Password** | **Description** |
| 1 | smellycat | Simple lowercase word (no numbers or symbols). |
| 2 | apple123 | Lowercase word + numbers (common pattern). |
| 3 | ILovePizza! | Mixed case + symbol, moderate length. |
| 4 | \_HorsePurpleHatRun\_ | Long passphrase (multiple words, one symbols). |
| 5 | cXmnZK65rf\*&DaaD | Random string with upper/lowercase, numbers, and symbols. |

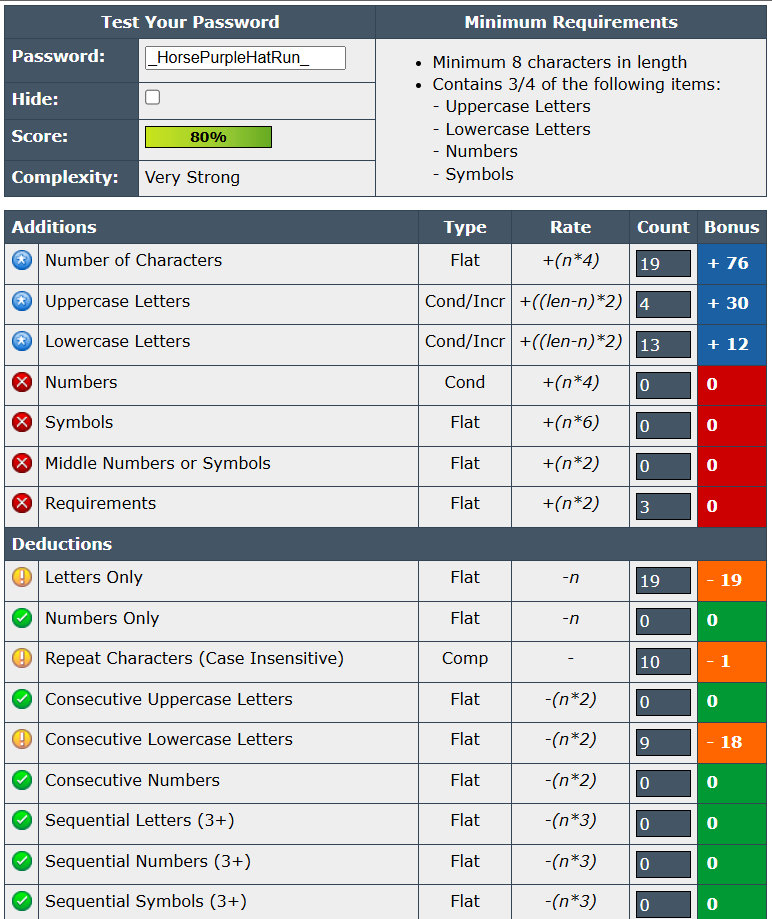
**Step 2: Test Results from** [**PasswordMeter.com**](https://www.passwordmeter.com/)

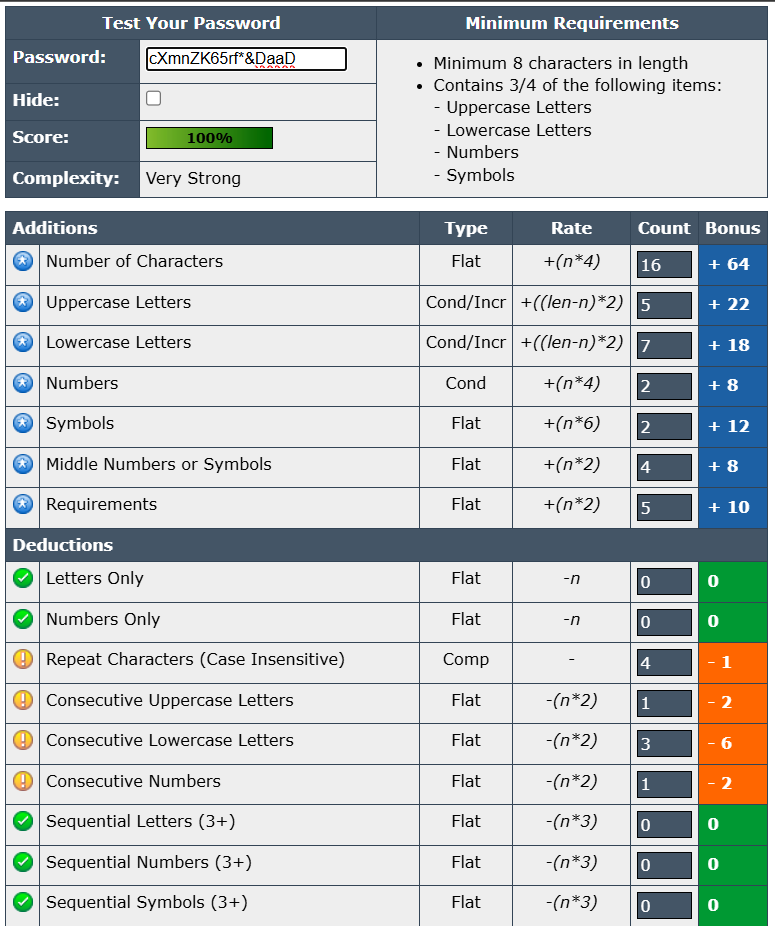
|  |  |  |
| --- | --- | --- |
| **Password** | **Score (%)** | **Tool Feedback** |
| smellycat | 9% (Very Weak) | Only lowercase letters; short and based on a dictionary word. |
| apple123 | 37% (Weak) | Adds numbers but still predictable and common. |
| ILovePizza! | 68% (Fair) | Good mix of uppercase, lowercase, and symbol; still uses dictionary words. |
| \_HorsePurpleHatRun\_ | 80% (Strong) | Long length with one symbol improves strength; passphrase style; lacks numbers. |
| cXmnZK65rf\*&DaaD | 100% (Excellent) | High entropy; includes all character types; long and fully random. |

****

****

****

****

****

**Step 3: Best Practices Identified**

From the testing and feedback, these best practices were observed:

1. Length is crucial - strength increases dramatically beyond 12–14 characters.
2. Combine character types - uppercase, lowercase, digits, and symbols.
3. Avoid common words or predictable patterns like “apple123” or “password2024”.
4. Use random or passphrase-style passwords for better entropy.
5. Avoid personal details (names, birthdays, or favorite words).
6. Place numbers/symbols in the middle, not just at the end.
7. Use unique passwords per account and never reuse.
8. Use a password manager to store and generate strong, unique passwords.

**Step 4: Tips Learned from Evaluation**

* Even simple additions (like capital letters or symbols) only moderately improve weak passwords.
* Length with a symbol alone (like in \_HorsePurpleHatRun\_) can create a strong password.
* Random combinations with all character types (like cXmnZK65rf\*&DaaD) reach near-perfect scores.
* Human-created passwords often follow patterns - using password generators or passphrases helps avoid predictability.
* Balanced complexity and memorability are key: strong doesn’t have to mean impossible to remember.

**Step 5: Research on Common Password Attacks**

|  |  |  |
| --- | --- | --- |
| **Attack Type** | **Description** | **Prevention** |
| Brute Force Attack | Systematically tries every possible combination. | Use long, random passwords (12+ characters). |
| Dictionary Attack | Uses common words and variations (like “apple”, “qwerty”). | Avoid real words or phrases; use symbols and mixed case. |
| Credential Stuffing | Attackers reuse leaked credentials across sites. | Never reuse passwords; enable MFA. |
| Phishing | Tricks users into revealing credentials. | Verify links before entering passwords; use password managers. |

**Step 6: Summary - How Password Complexity Affects Security**

* Complexity and randomness directly improve password strength.
* Length increases the total number of possible combinations, making brute-force attacks impractical.
* Character diversity (upper, lower, symbols, numbers) adds entropy, reducing predictability.
* Dictionary words make passwords much weaker, even if they include numbers or symbols.
* Completely random or long passphrases offer the strongest defense against automated attacks.

**Step 7: Conclusion**

Passwords that are long, random, and diverse in character types are exponentially more secure. Weak passwords like smellycat can be cracked in seconds, while complex ones like cXmnZK65rf\*&DaaD would take millions of years with brute-force methods. Using length, unpredictability, and multiple character sets is the key to building truly strong passwords. Combining this with multi-factor authentication (MFA) provides the best real-world protection.