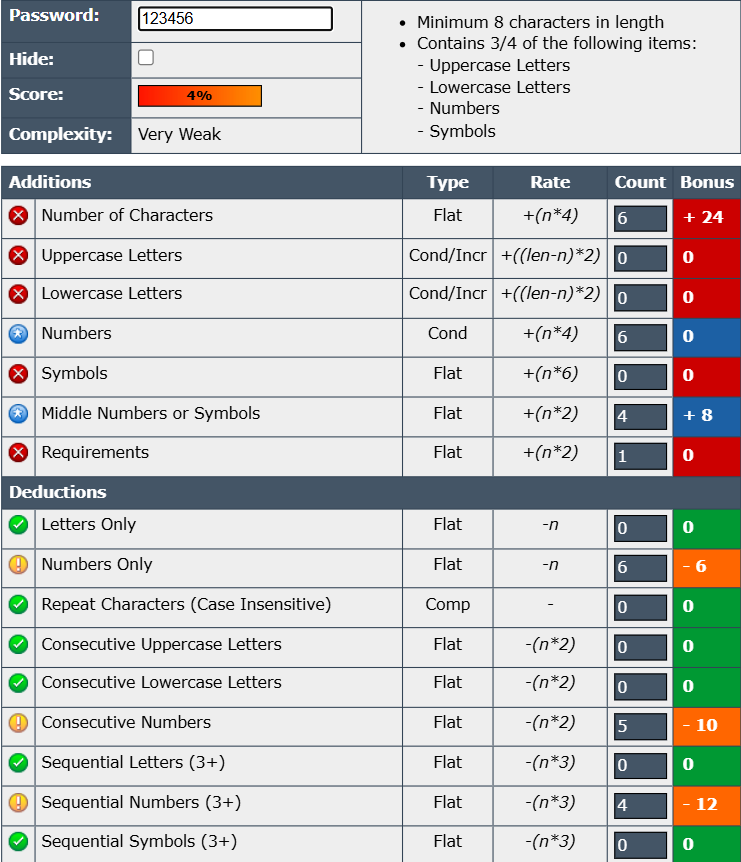
Password Strength Evaluation Report

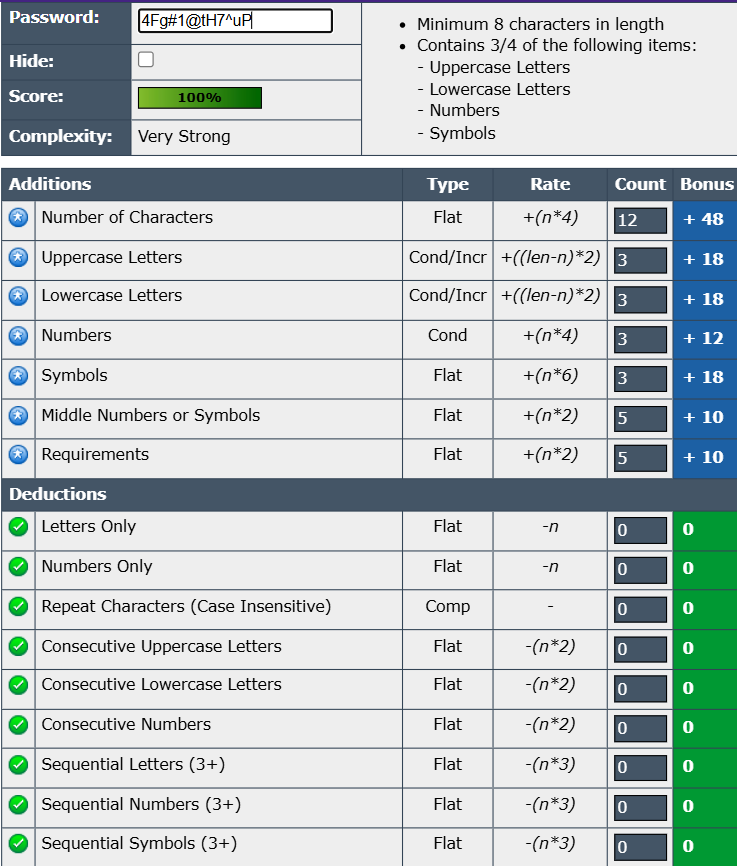
# 1. Introduction

This report evaluates the strength of different types of passwords using an online password strength checker. The goal is to understand what makes a password secure and how complexity and randomness protect against common password attacks.

# 2. Passwords Tested and Results

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Description | Score | Feedback |
| 123456 | Common numeric password | 0% | Very weak. Too short and predictable. |
| Password123 | Simple word + number | 33% | Weak. Contains dictionary word. |
| P@ssw0rd! | Word with symbol and number | 75% | Moderate. Still includes common word patterns. |
| XyT9@!zLw3 | Randomized characters, 10 length | 82% | Strong. Complex and unpredictable. |
| 4Fg#1@tH7^uP | Complex mix, 12 characters | 100% | Very strong. Excellent length and variety. |





# 3. Analysis

Strong passwords use random combinations of letters, numbers, and symbols, and are at least 12–16 characters long. Weak passwords contain common patterns, dictionary words, or are too short.

# 4. Tips for Strong Passwords

* Use 12 or more characters
* Mix upper/lowercase, numbers, and symbols
* Avoid dictionary words and personal info
* Use a password manager
* Enable two-factor authentication

# 5. Common Attacks and Why Complexity Matters

Brute Force: Tests all combinations; long passwords take longer to crack.

Dictionary Attack: Tries common words - avoid real words.

Credential Stuffing: Reusing passwords makes you vulnerable.

# 6. Conclusion

Strong passwords are essential for protecting digital identities. Using long, complex, and unique passwords helps prevent common attacks. Following best practices and using tools like password strength checkers helps users build better security habits.