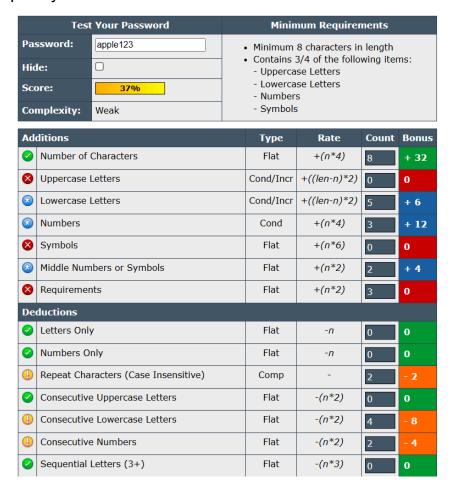
# Task 6: Create a Strong Password and Evaluate Its Strength.

# 1. Passwords Created for Testing:

Password: apple123

Complexity Details: Lowercase + numbers



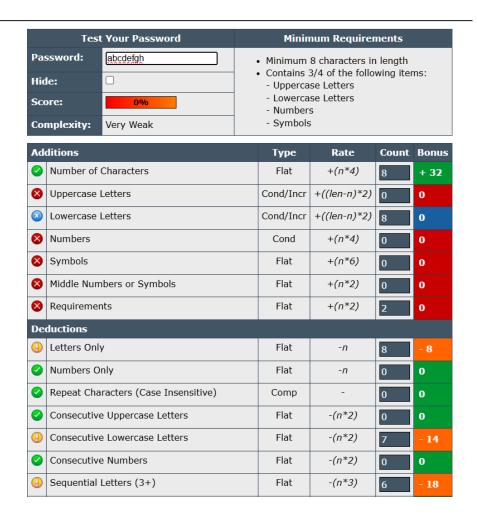
Password: Apple@123
Complexity Details: Uppercase + lowercase + numbers + symbol



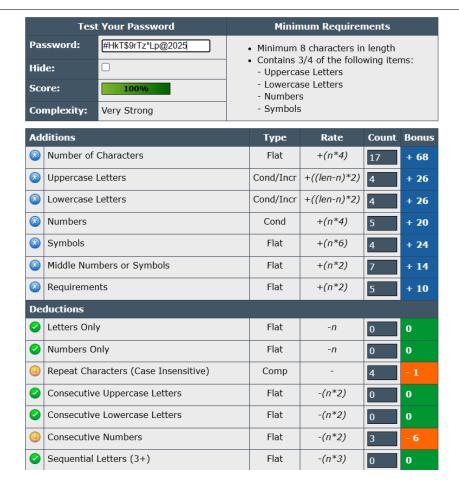
Password: P@ssW0rd2025!
Complexity Details: Mixed case + symbols + numbers (12 characters)

Test Your Password		Minimum Requirements			
Password:		Minimum 8 characters in length Contains 3/4 of the following items: Uppercase Letters Lowercase Letters Numbers Symbols			
Additions		Туре	Rate	Count	Bonus
Number of Characters		Flat	+(n*4)	13	+ 52
② Uppercase Letters		Cond/Incr	+((len-n)*2)	2	+ 22
Lowercase Letters		Cond/Incr	+((len-n)*2)	4	+ 18
Numbers	Numbers		+(n*4)	5	+ 20
Symbols		Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols		Flat	+(n*2)	6	+ 12
Requirements		Flat	+(n*2)	5	+ 10
Deductions					
✓ Letters O	Letters Only		-n	0	0
Numbers	Numbers Only		-n	0	0
Repeat Ch	Repeat Characters (Case Insensitive)		-	6	- 2
✓ Consecution	Consecutive Uppercase Letters		-(n*2)	0	0
Onsecution	ive Lowercase Letters	Flat	-(n*2)	2	- 4
Onsecution	ive Numbers	Flat	-(n*2)	3	- 6
✓ Sequentia	al Letters (3+)	Flat	-(n*3)	0	0
Sequentia	al Numbers (3+)	Flat	-(n*3)	0	0

Password:abcdefgh
Complexity Details: All lowercase, simple



Password:#HkT\$9rTz\*Lp@2025
Complexity Details: 16 chars, uppercase, lowercase, symbols, numbers



#### **Observations and Best Practices:**

- Length matters: Longer passwords significantly increase strength.
- Use all character types: A strong password should include uppercase, lowercase, numbers, and special symbols.
- Avoid common words or sequences: Even with complexity, predictable patterns like "P@ssw0rd" are discouraged.
- Unique and random is key: The more random and unique a password, the stronger it is.

### Tips Learned from Evaluation:

- Aim for passwords that are at least 12 characters long.
- Combine letters (both cases), numbers, and symbols in unpredictable ways.
- Avoid dictionary words, dates, or names.
- Consider using passphrases with random words + symbols for both security and memorability.
- Use password managers to store complex passwords safely.

### Researched common password attacks:

1. Attack by Brute Force

Attempts to guess a password by attempting every character combination.

Automated tools try each combination until they find the right one.

Make use of CAPTCHAs, enable account lockout, and create lengthy, complicated passwords

#### 2. Dictionary Attack:

This method guesses the password by using a list of real words and popular passwords.

Finds matches, tools iterate through wordlists (such as 123456, gwerty, and password).

Use complex and one-of-a-kind passwords; stay away from real words and recurring patterns.

3. Stuffing Credentials

Attempts to access several websites using previously compromised username-password combinations.

Exploits reused credentials from data breaches to access other accounts.

Never reuse passwords; use unique ones for every site and enable multi-factor authentication (MFA).

## **How Password Complexity Affects Security:**

- Simple passwords (e.g., "password123") can be cracked in seconds by dictionary attacks.
- Complex passwords with randomness and length can take years or decades to crack using brute force.
- Higher complexity increases entropy, reducing the success rate of automated guessing attacks.
- Password complexity delays or defeats cracking attempts, especially if used with multi-factor authentication.