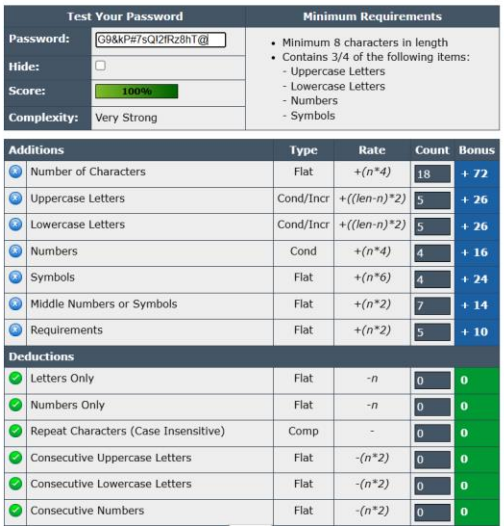
Task 6: Create a Strong Password and Evaluate Its Strength

Objective: Understand what makes a password strong and test it against password strength tools.

- **Step 1: Create multiple passwords with varying complexity**
- Examples (don't actually use these, just for testing):
  - Simple: apple123
  - Medium: Appl3Tree!
  - Strong: M@ngo!SunR1se2025
  - Very strong: G9&kP#7sQ!2fRz8hT@
- **Step 2: Use uppercase, lowercase, numbers, symbols, and length variations**
  - **Lowercase only:** passwordtest
  - **Mixed case:** SecureTest
  - **Case + numbers:** Secur3Pass
  - **Case + numbers + symbols:** S3cur3!Pass#
  - **Long passphrase:** BlueElephantsDanceAtMidnight2025!
- Step 3: Test each password on a password strength checker

Test Your Password		Minimum Requirements
Password:	apple123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	37%	
Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 6
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	2	- 4



Test Your Password		Minimum Requirements
Password:	G9&kP#7sQ!2fRz8hT@	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	18	+ 72
Uppercase Letters	Cond/Incr	+((len-n)*2)	5	+ 26
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 26
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	4	+ 24
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	0	0

- **4. Note scores and feedback from the tool**

• **Password**	• **Strength Score**	• **Feedback Example**
• apple123	• Weak	• Too short, common word
• Appl3Tree!	• Medium	• Better, but still somewhat guessable
• M@ngo!SunR1se2025	• Strong	• Long and diverse
• G9&kP#7sQ!2fRz8hT@	• Very Strong	• Extremely hard to crack

Password	Strength Score	Feedback Example
BlueElephantsDance…	Very Strong	Secure due to length & randomness

- **Step 5: Identify best practices for creating strong passwords**
- From testing, you'll notice:
  - Length **matters more** than just complexity.
  - Random words/phrases are harder to crack than short, complex ones.
  - Avoid dictionary words or personal info.
  - Use **symbols, numbers, and case variation**.
  - Consider using a **passphrase** (long + memorable)
- **Step 6: Write down tips learned**
  - Aim for **at least 12–16 characters**.
  - Mix **uppercase, lowercase, numbers, and symbols**.
  - Avoid patterns (e.g., 123456, Qwerty@2025).
  - Use a **password manager** to store unique passwords for each account.
  - Enable **multi-factor authentication (MFA)** for extra security.
- **Step 7: Research common password attacks**
  - **Brute force:** Tries all possible combinations until it finds the correct one.
  - **Dictionary attack:** Uses a precompiled list of common words and passwords.
  - **Credential stuffing:** Uses leaked usernames/passwords from other breaches.
  - **Phishing:** Tricks you into revealing passwords.
  - **Keylogging:** Malware records keystrokes.

- **Step 8: Summarize how password complexity affects security**
  - **Short/simple passwords** are cracked in seconds using brute force or dictionary attacks.
  - **Medium complexity** adds resistance but still guessable if reused or too short.
  - **Long + complex (16+ chars)** passwords are highly resistant to brute force.
  - **Passphrases** (random words + symbols/numbers) are both secure and easier to remember.
  - Overall: **Length + randomness = strongest defense.**