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

Here we evaluate password strength by passwordmeter.com

We use password like

1. V\*123@@321

2. 123@@321

3. 123456789

Here I tried 3 different password having different strength

Below are the image of try password



| **Score Range** | **Rating** |
| --- | --- |
| 0 - 19 | Very Weak |
| 20 - 39 | Weak |
| 40 - 59 | Reasonable |
| 60 - 79 | Strong |
| 80 - 100 | Very Strong |

**🔐 Common Password Attacks**

**1. 🧱 Brute-Force Attack**

* **What it is**: The attacker tries every possible combination of characters until the correct password is found.
* **Target**: Usually short or simple passwords.
* **Speed**: Very slow for complex passwords, but fast for simple or short ones.
* **Defense**:
  + Use long, complex passwords
  + Enable account lockouts after failed attempts
  + Implement rate limiting and CAPTCHA

**2. 📖 Dictionary Attack**

* **What it is**: Tries passwords from a predefined list of common passwords (like 123456, password, qwerty).
* **Faster than brute-force** because it targets likely candidates.
* **Defense**:
  + Avoid using common or predictable passwords
  + Use password managers to generate unique passwords

**🔐 Summary: How Password Complexity Affects Security**

**Password complexity directly increases security** by making passwords harder to guess, crack, or brute-force. Here's how:

**🧠 1. Increases Brute-Force Resistance**

* More possible combinations = more time and computing power needed to guess.
* Example:
  + abc123 (low complexity) can be cracked in seconds.
  + T9$kL@8zQ1! (high complexity) may take centuries.

**🔢 2. Reduces Success of Dictionary & Guessing Attacks**

* Complex passwords avoid common words, names, or keyboard patterns (qwerty, 123456), which are easy targets.
* Attackers rely on these patterns in dictionary and credential stuffing attacks.

**🔄 3. Minimizes Repetition & Predictability**

* Strong passwords avoid repeated characters or predictable substitutions (like P@ssw0rd), which attackers often anticipate.

**🔒 4. Supports Secure Multi-Factor Authentication**

* Complex passwords are harder to compromise, making the first layer of MFA more secure.

**📉 Weak Password Example:**

* summer2024
  + Common word, predictable number, no symbols — easily cracked.

**📈 Strong Password Example:**

* Xz@91v!#Lq
  + Mix of uppercase, lowercase, numbers, and symbols — high entropy.

**✅ Best Practices**

* Use **12+ characters** with a mix of **upper/lowercase, numbers, symbols**
* Avoid personal info or common patterns
* Use a **password manager** to create and store complex passwords

**In short:**  
🔑 **Complex passwords make unauthorized access exponentially harder, defending against most automated and manual password attacks.**