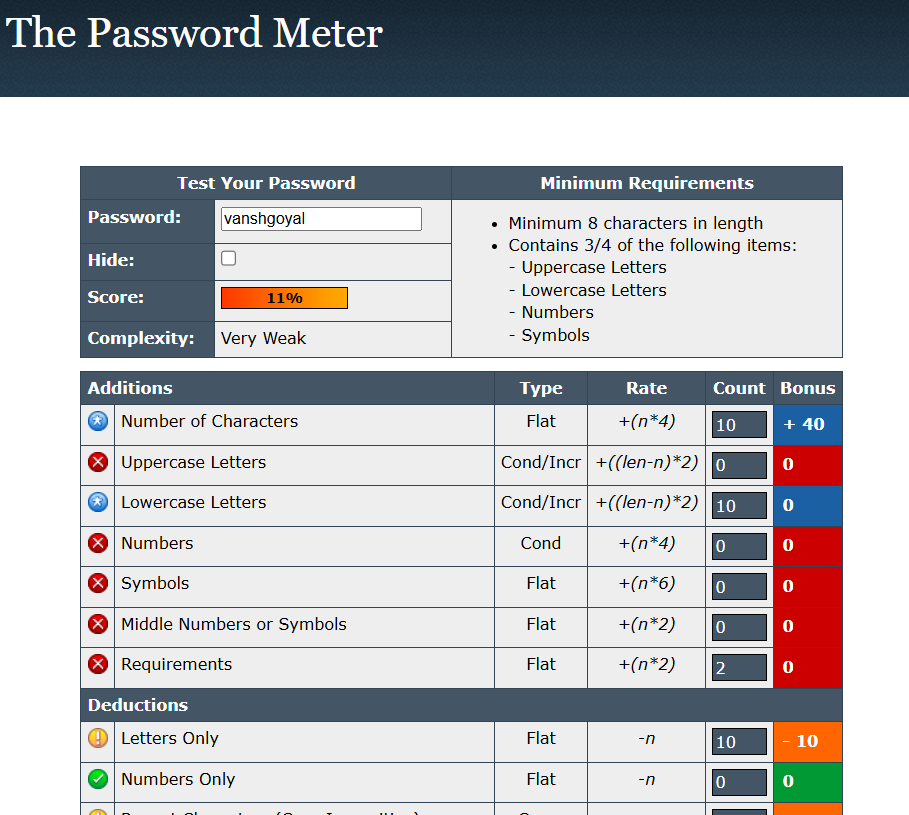
Create a Strong Password and Evaluate Its Strength



**Password Evaluation Summary (Password: vanshgoyal)**

* **Score:** 11%
* **Complexity:** Very Weak
* The password **fails to meet minimum security standards**, despite being 10 characters long.

**Major Weaknesses Identified:**

| **Criteria** | **Status** | **Comment** |
| --- | --- | --- |
| **Uppercase Letters** | ❌ Missing | Only lowercase used |
| **Numbers** | ❌ Missing | No numeric characters present |
| **Symbols** | ❌ Missing | No special characters like @, #, etc. |
| **Diversity of Characters** | ❌ Lacking | Only lowercase letters used |
| **Middle Numbers/Symbols** | ❌ None | No non-letter characters in the middle |
| **Requirements Met** | ❌ Only 2 | Needs at least 3 of 4 types (Upper, Lower, Number, Symbol) |

**Deductions:**

* **Letters Only:** −10 points because the password contains **only letters**.
* **No other deductions** for numbers or repeated characters — but only because those elements are missing.

**What Worked:**

* **Length:** 10 characters (+40 bonus) — this is the only strength.

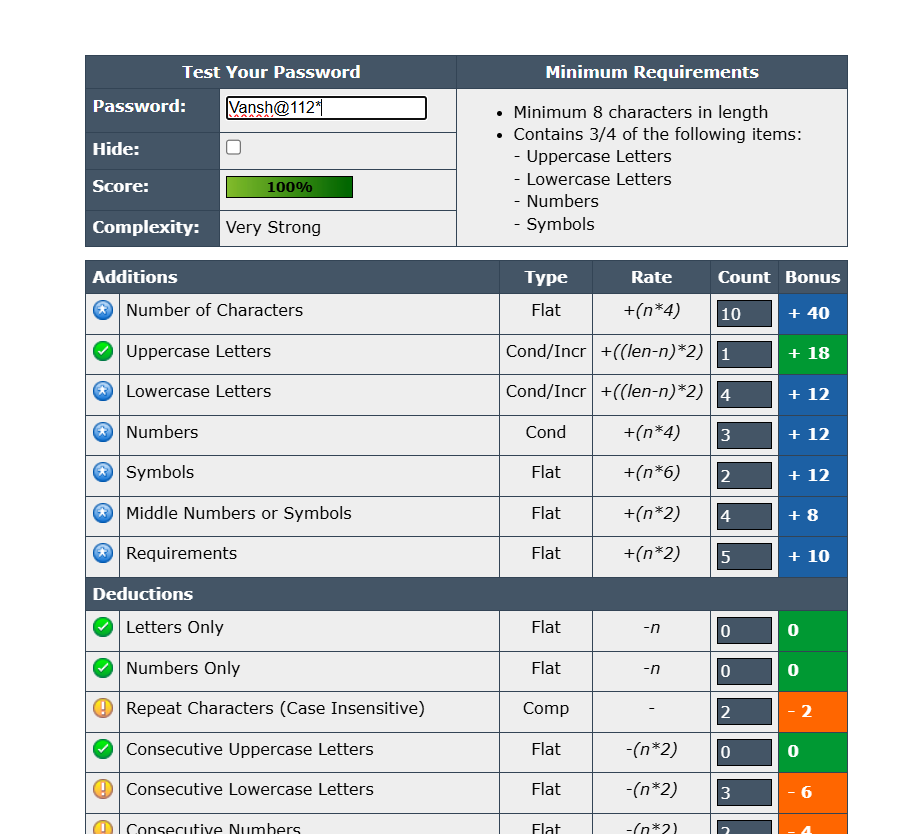
**Tips Learned from This Evaluation:**

1. **Use Character Variety:**  
   Add **uppercase letters, numbers, and symbols** to increase complexity.
2. **Avoid “Letters Only” Passwords:**  
   Passwords made up entirely of letters are penalized and are highly insecure.
3. **Meet All Minimum Requirements:**  
   Use at least **3 of the 4**: uppercase, lowercase, number, and symbol.
4. **Add Middle Characters (Numbers/Symbols):**  
   Avoid predictable formats like starting or ending with a capital letter or number.
5. **Long is Not Enough Alone:**  
   Even a 10-character password is **weak** if it lacks diversity.

**Suggested Strong Version:**

**V@nshG0yal!**

* Adds uppercase V, number 0, symbol @ and !
* Meets all 4 complexity criteria
* Much stronger security rating



From the password evaluation shown in the screenshot, here are several important tips learned about creating a strong password:

**Password Evaluation Summary (Password: Vansh@112)**

* **Score: 100%**
* **Complexity: Very Strong**
* **This password is well-balanced, meeting all complexity and strength criteria.**

**Strengths (Additions):**

| **Criteria** | **Count** | **Bonus** | **Comments** |
| --- | --- | --- | --- |
| **Length (10 characters)** | **10** | **+40** | **Good overall length** |
| **Uppercase Letters** | **1** | **+18** | **At least one uppercase included** |
| **Lowercase Letters** | **4** | **+12** | **Satisfies lowercase requirement** |
| **Numbers** | **3** | **+12** | **Enhances entropy** |
| **Symbols** | **2** | **+12** | **Special characters improve strength** |
| **Middle Numbers/Symbols** | **4** | **+8** | **Less predictable structure** |
| **Meets All Requirements** | **5 types** | **+10** | **Passes all 4 required character types** |

**Minor Weaknesses (Deductions):**

| **Deduction** | **Count** | **Penalty** | **Comment** |
| --- | --- | --- | --- |
| **Repeat Characters** | **2** | **−2** | **Repeated characters (e.g., 1)** |
| **Consecutive Lowercase Letters** | **3** | **−6** | **e.g., ans in the password** |
| **Consecutive Numbers** | **2** | **−4** | **11 or 12 sequence** |

**Tips Learned:**

1. **Use All Character Types:  
   Including uppercase, lowercase, numbers, and symbols boosts strength and meets all requirements.**
2. **Length Helps:  
   10 characters significantly improves the score.**
3. **Avoid Repetition & Sequences:  
   Repeating or consecutive characters slightly reduce score — mix things up for better security.**
4. **Middle Placement Matters:  
   Placing numbers or symbols in the middle improves complexity.**

**Final Verdict:**

**This is a strong password.  
It’s secure against common attacks like brute force and dictionary attacks. Minor improvements can be made by avoiding consecutive/repeated characters, but overall, this password is excellent.**

Research Common Password Attacks

**1. Brute Force Attack**

* **What it is:**  
  A method where attackers try all possible combinations of characters until the correct password is found.
* **Tools used:**  
  Automated tools like **Hydra**, **John the Ripper**, or **Hashcat**.
* **Weakness it exploits:**  
  Short, simple, or predictable passwords.
* **Prevention tips:**
  + Use **long passwords** (10+ characters).
  + Include **uppercase, lowercase, numbers, and symbols**.
  + Implement **account lockout** after failed attempts.
  + Use **multi-factor authentication (MFA)**.

**2. Dictionary Attack**

* **What it is:**  
  Attackers use a precompiled list of common or leaked passwords (like “123456” or “password”) to guess the password.
* **Tools used:**  
  Dictionary files (e.g., rockyou.txt) with tools like **Medusa** or **John the Ripper**.
* **Weakness it exploits:**  
  Passwords based on words or patterns commonly used by humans.
* **Prevention tips:**
  + Avoid **common words** or names in passwords.
  + Don’t use **dictionary-based passwords** with simple substitutions (like "Pa$$word").
  + Use a **random password generator** or passphrase system (e.g., Diceware).

**3. Credential Stuffing**

* **What it is:**  
  Attackers use leaked username-password pairs from other breaches to log in to other sites.
* **Weakness it exploits:**  
  Reusing the **same password across multiple services**.
* **Prevention tips:**
  + Never reuse passwords.
  + Use a **password manager** to manage unique passwords.
  + Enable **MFA** wherever possible.

**4. Social Engineering / Phishing**

* **What it is:**  
  Tricks users into revealing their passwords (e.g., via fake login pages or emails).
* **Weakness it exploits:**  
  Human trust and poor security awareness.
* **Prevention tips:**
  + Train users to recognize phishing.
  + Use anti-phishing tools and email filters.
  + Verify suspicious communications independently.

**5. Hybrid Attack**

* **What it is:**  
  Combines dictionary attacks with slight variations (e.g., adding numbers or symbols).
* **Tools used:**  
  Custom wordlists with **rules** applied in tools like Hashcat.
* **Prevention tips:**
  + Avoid **predictable modifications** like “Password123!”.
  + Use truly **random and long** passwords.

**Summary Table:**

| **Attack Type** | **Description** | **Preventive Measures** |
| --- | --- | --- |
| **Brute Force** | Tries all combinations | Use long/complex passwords; lockouts |
| **Dictionary** | Uses common password lists | Avoid common/real words |
| **Credential Stuffing** | Tries reused credentials | Use unique passwords; enable MFA |
| **Phishing** | Tricks user into giving password | Awareness training; anti-phishing tools |
| **Hybrid** | Tries modified dictionary words | Use random, complex passwords |

**How Password Complexity Affects Security – Summary**

Password complexity significantly increases **resistance to attacks** by making it harder for attackers to guess or crack passwords using automated methods.

**Key Factors of Password Complexity:**

1. **Length**
   * Longer passwords exponentially increase the number of possible combinations.
   * Example: A 12-character password is vastly stronger than an 8-character one.
2. **Character Variety**
   * Using a mix of:
     + Uppercase (A-Z)
     + Lowercase (a-z)
     + Numbers (0-9)
     + Symbols (!@#$%)
   * Prevents attackers from succeeding with basic dictionary or brute-force attacks.
3. **Unpredictability**
   * Avoids patterns, sequences, and common substitutions (e.g., P@ssw0rd is predictable).
   * Random, unique characters make hybrid or rule-based attacks less effective.

**Weak Password Example:**

Password123

* Short (11 characters)
* Uses predictable pattern and dictionary word
* Easily cracked by dictionary or hybrid attack

**Strong Password Example:**

hG!9t@zQ2#eL

* 12 characters
* Mix of upper, lower, numbers, and symbols
* Random and unpredictable

**Complexity vs. Common Attacks:**

| **Attack Type** | **Complexity Benefit** |
| --- | --- |
| Brute Force | Slows down or prevents successful guesses |
| Dictionary Attack | Invalidates common/simple words |
| Hybrid Attack | Renders rule-based variations ineffective |
| Credential Stuffing | Irrelevant if each password is unique |

**Bottom Line:**

**Higher password complexity = stronger defense against automated and manual attacks.**  
For best results:

* Use at least **12 characters**
* Include **all character types**
* Avoid **common patterns**
* Use a **password manager** for secure storage