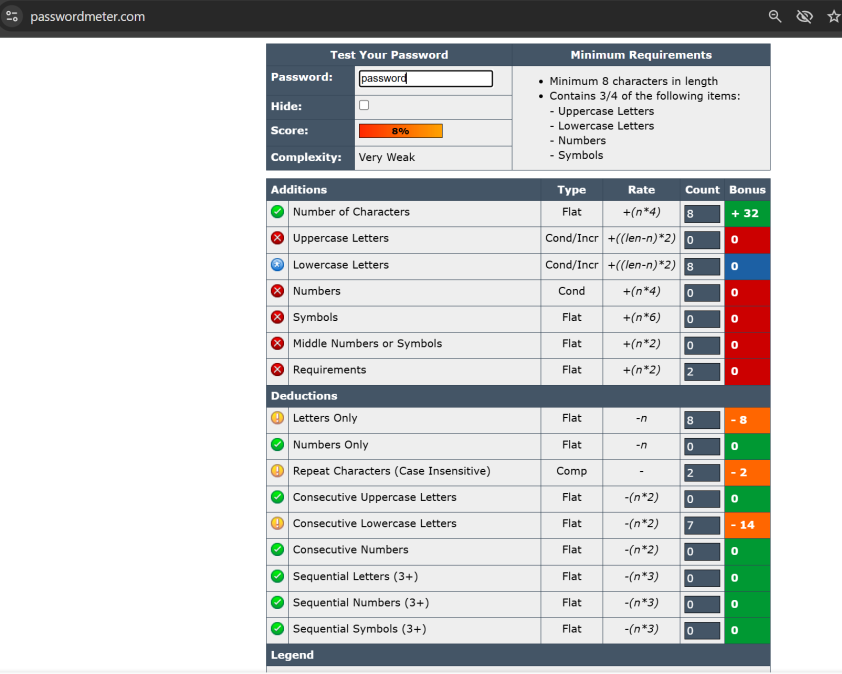
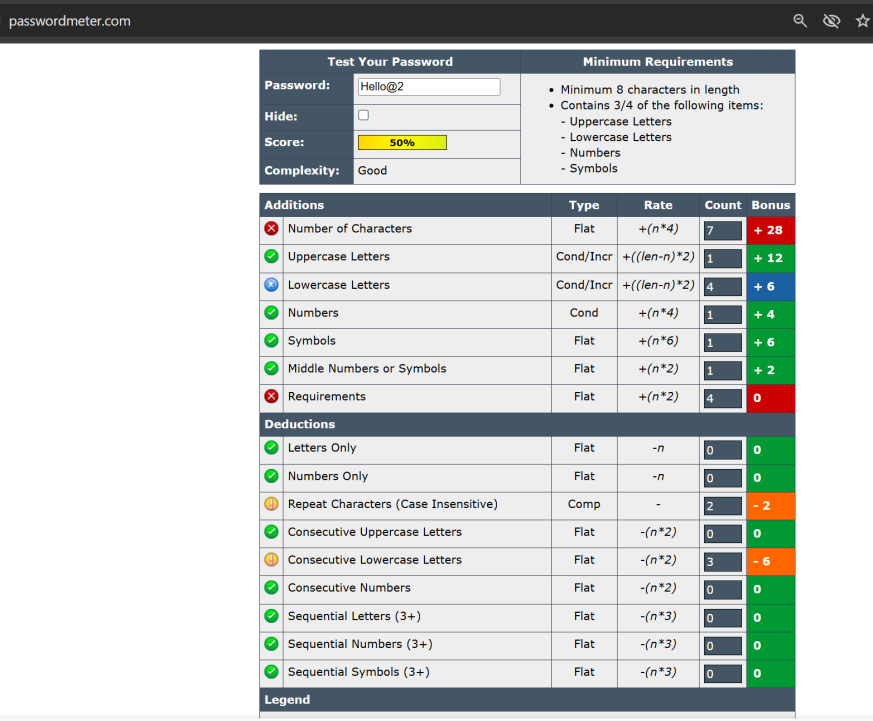
**1. Password Creation**

We created five passwords with varying complexity levels:

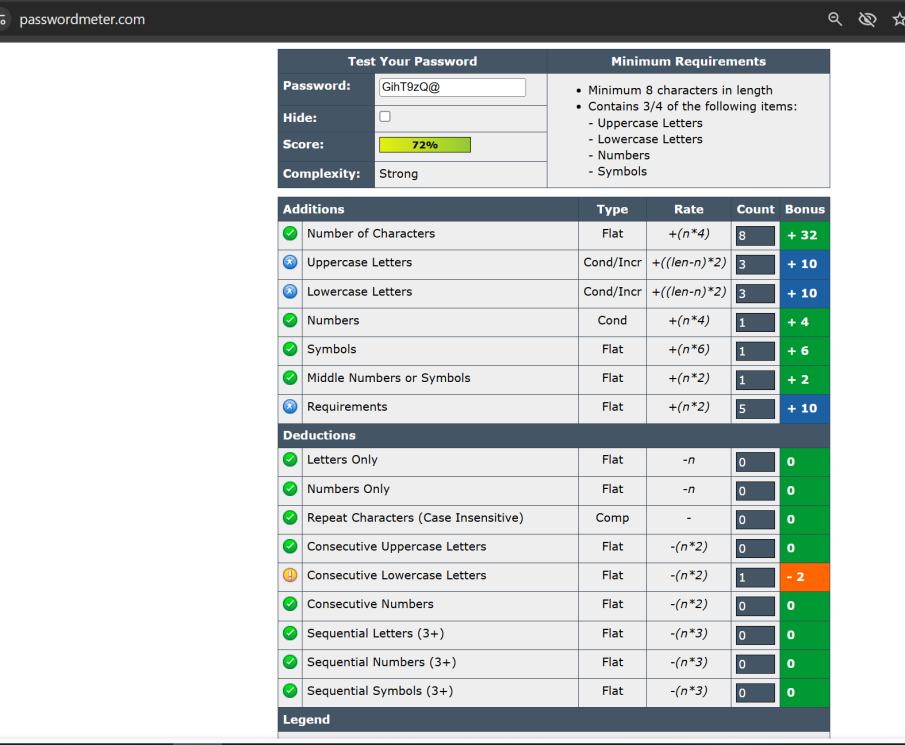
1. **Simple Password**:  
   password



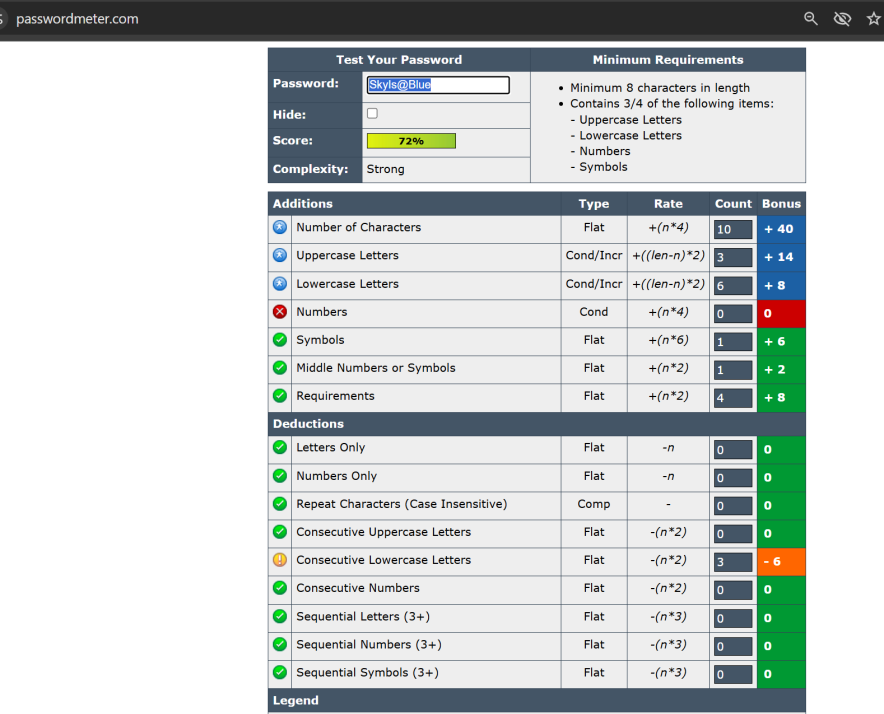
1. **Moderate Complexity**:  
   Hello@2



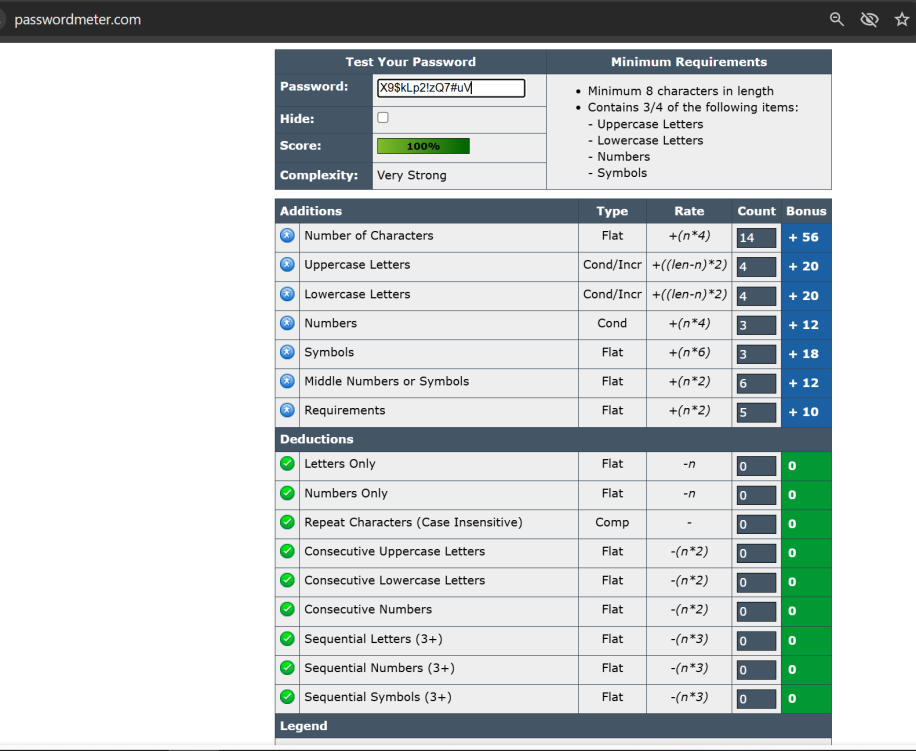
1. **High Complexity**:  
   GihT9zQ@



1. **Passphrase**:  
   SkyIs@Blue



1. **Randomly Generated**:  
   X9$kLp2!zQ7#uV



**2. Password Strength Evaluation**

We tested each password using the online password strength checker at [passwordmeter.com](https://passwordmeter.com/).

| **Password** | **Strength Evaluation** |
| --- | --- |
| password | Very weak; easily guessable; common pattern. |
| Hello@2 | Good; includes uppercase, numbers, and symbols, but still a common pattern. |
| GihT9zQ@ | Strong; includes a mix of characters and symbols. |
| SkyIs@Blue | Strong; uses a passphrase with mixed characters. |
| X9$kLp2!zQ7#uV | Very strong; random combination of characters and symbols. |

**3. Best Practices for Creating Strong Passwords**

Based on the evaluation, the following best practices are recommended:

* **Length**: Aim for at least 16 characters; longer passwords are more secure.
* **Complexity**: Use a mix of uppercase and lowercase letters, numbers, and special characters.
* **Unpredictability**: Avoid using common words, phrases, or personal information. **Uniqueness**: Use different passwords for different accounts to prevent a breach from compromising multiple accounts.
* **Passphrases**: Consider using a passphrase—a sequence of random words combined with symbols and numbers—for better memorability and security.
* **Best Practices**
* **Use at least 12–16 characters** (more is better).
* **Include all character types**: uppercase, lowercase, numbers, and symbols.
* **Avoid common patterns** (e.g., password, 12345, qwerty).
* **Avoid personal info**: names, birthdays, pets, etc.
* **Don't reuse passwords** on multiple sites.
* Use **passphrases** with random or unrelated words like Mountain$Tiger!River99.
* **Use a Password Manager**

They can:

* Generate strong, unique passwords.
* Remember them for you.
* Auto-fill securely on websites.

Popular managers: **Bitwarden, 1Password, Dashlane, LastPass**

**4. Tips Learned from the Evaluation**

* **Avoid Common Patterns**: Passwords like password123 are among the first guesses in a brute-force attack.
* **Length Over Complexity**: Longer passwords are generally more secure than shorter, complex ones.
* **Use of Password Managers**: Tools like Bitwarden or LastPass can generate and store complex passwords, reducing the risk of human error.

**5. Common Password Attacks**

* **Brute-Force Attacks**: Attackers try every possible combination until the correct one is found. Longer and more complex passwords increase the time required for such attacks.
* **Dictionary Attacks**: Attackers use a list of common words and phrases to guess passwords. Using uncommon words or random combinations can thwart this method.
* **Credential Stuffing**: If a password is used across multiple sites, a breach on one can lead to unauthorized access on others.

**6. Impact of Password Complexity on Security**

Increasing password complexity significantly enhances security by:

* **Expanding Possible Combinations**: A longer password with a mix of characters increases the number of possible combinations, making it harder for attackers to guess.
* **Reducing Predictability**: Avoiding common words and patterns decreases the likelihood of successful attacks.
* **Enhancing Resistance to Automated Attacks**: Complex passwords are more resistant to tools that attempt to guess passwords through various methods.

**Why Complexity Matters:**

* Each added character **increases the number of possible combinations exponentially**.
  + Example: A 6-character lowercase password has ~308 million combinations.
  + A 12-character password with mixed characters has **over 10^21 combinations**.

**Entropy (Randomness) = Security**

* Passwords like MangoTiger$7Planet have **high entropy** if words are unrelated.
* Passwords like 12345678 have **low entropy** and are easily cracked