**CYBER SECURITY INTERNSHIP IN ELEVATE LABS**

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

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

1. Create multiple passwords with varying complexity.

2. Use uppercase, lowercase, numbers, symbols, and length variations.

We’ll make four sample passwords with varying complexity

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **Sl. No.** | **Password** | **Type** | **Reason for Choice** | | 1 | sumathi12 | Weak | Common word + numbers | | 2 | njsr962 | Simple | Mixed word + numbers | | 3 | NjsR!456 | Moderate | Mixed case + symbol + numbers | | 4 | Fr45$unboss@ | Strong | Uncommon words, numbers as letters, special char | | 5 | N2k@s!z9#Rf6 | Very Strong | Random, long, high complexity | | | |  |  |
|  |  |

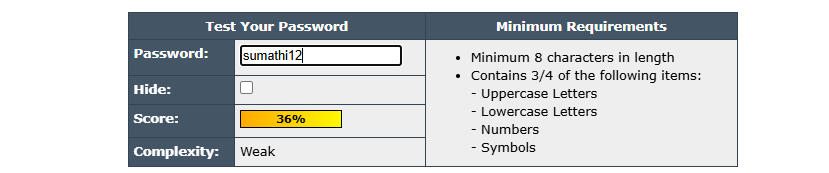
3. Test each password on password strength checker.

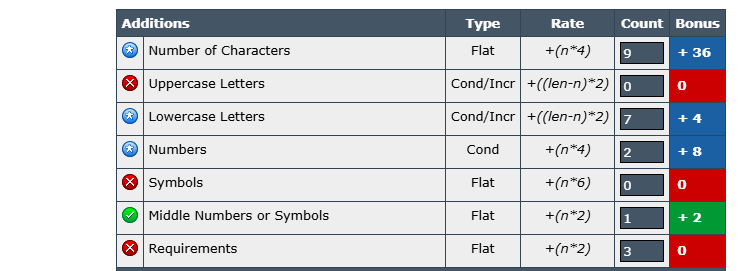
4. Note scores and feedback from the tool.

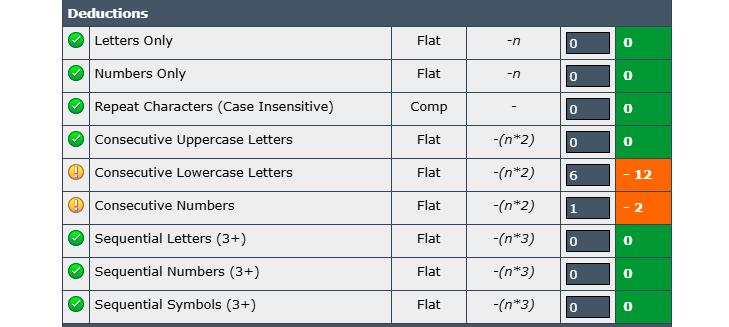
Password meter is a simple online evaluation tool used to determine the relative strength of passwords.

**Sample 1: sumathi12**



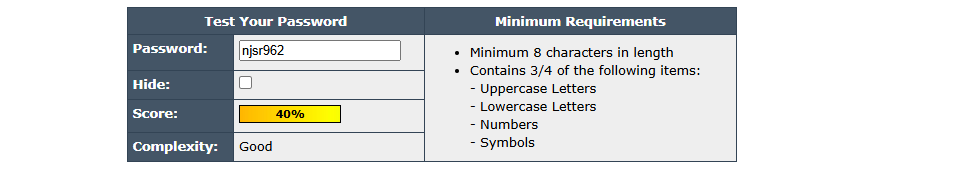


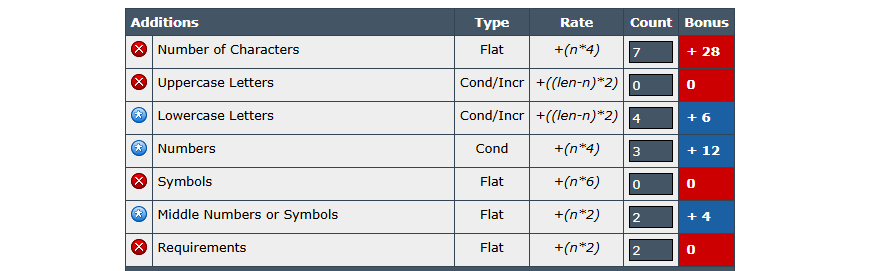


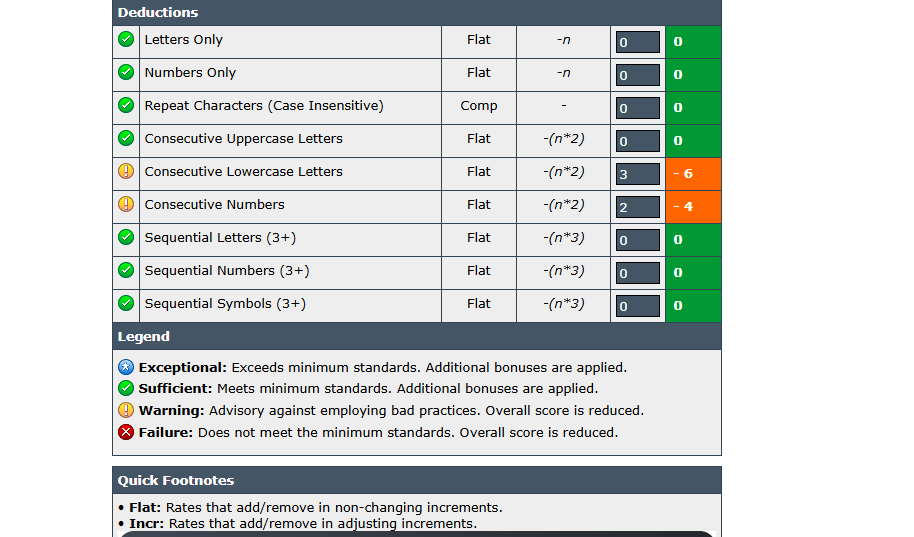


**Sample 2: njsr962**



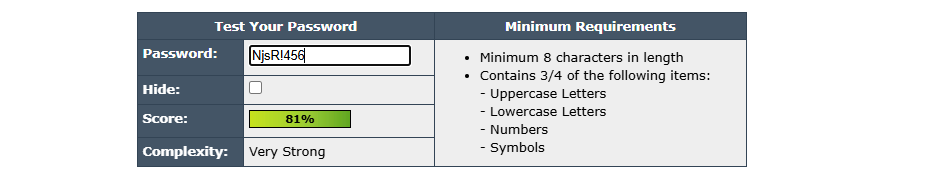






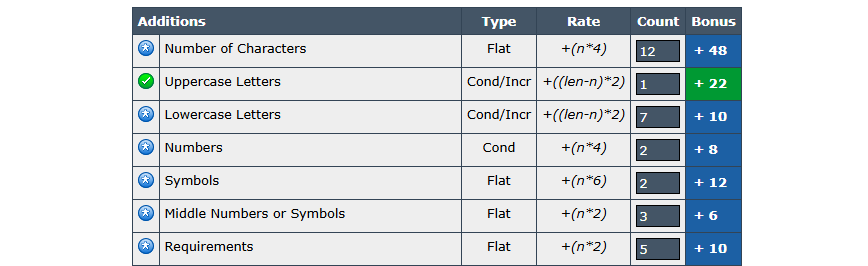
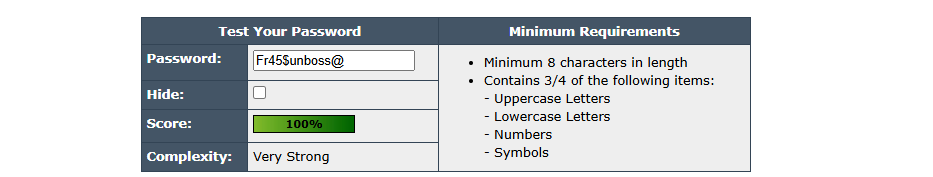
**Sample 3: NjsR!456**

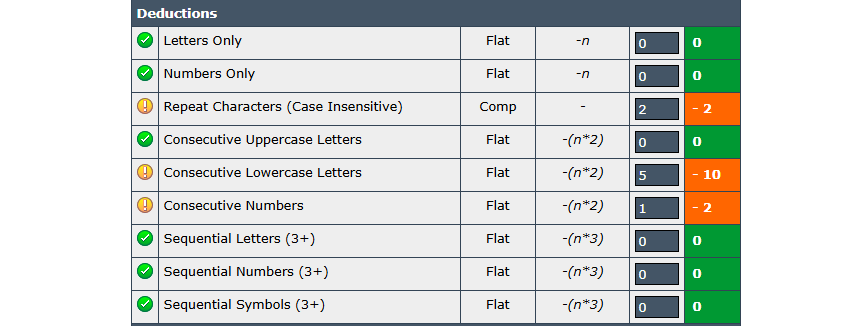






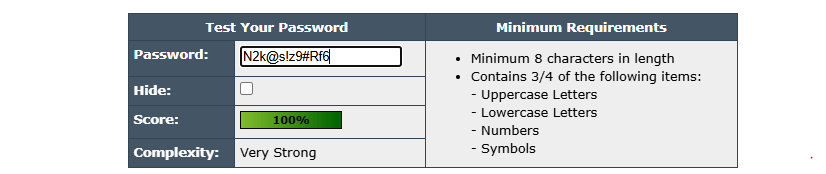
**Sample 4: Fr45$unboss@**

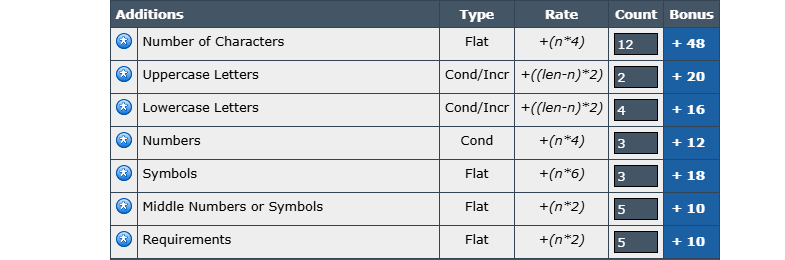


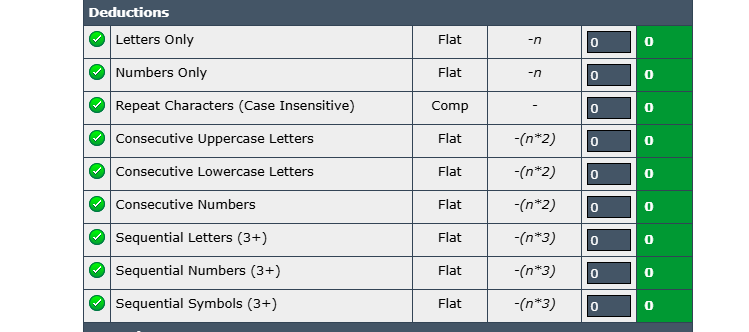


**Sample 5: Fr45$unboss@**









Example using passwordmeter.com — actual scores will vary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl. No. | **Password** | **Score** | **Strength** | **Feedback** |
| 1 | sumathi12 | ~36% | Weak | Too short, dictionary word, predictable |
| 2 | njsr962 | ~40% | Good | Too short, mixed characters |
| 3 | NjsR!456 | ~81% | Strong | Better mix, still short |
| 4 | Fr45$unboss@ | ~100% | Very Strong | Long, mixed characters, but some dictionary words |
| 5 | N2k@s!z9#Rf6 | ~100% | Very Strong | High complexity, no patterns, long length |

5. Identify best practices for creating strong passwords.

* Length matters: 12+ characters is ideal.
* Mix it up: Use uppercase, lowercase, numbers, and symbols.
* Avoid dictionary words: Easy targets for dictionary attacks.
* No patterns: Avoid predictable sequences like 1234 or qwerty.
* Passphrases work well: Combine unrelated words with symbols/numbers.

**1. Make it long enough to resist guessing**

* Aim for at least **12–16 characters**.
* Longer passwords are exponentially harder to brute-force.

**2. Use a mix of character types**

* Include **uppercase**, **lowercase**, **numbers**, and **special characters**.
* Example format: N2k@s!z9#Rf6 (but avoid predictable substitutions like P@ssw0rd!).

**3. Avoid personal or obvious information**

* Do not use your name, birthdate, username, pet’s name, or simple patterns like 123456 or qwerty.

**4. Use passphrases instead of single words**

* Combine random, unrelated words into a sentence-like structure.
* Example: BluePiano7!DrinksMango — easier to remember, hard to guess.

**5. Make it unique for every account**

* Reusing passwords means if one is breached, all are at risk.

**6. Avoid dictionary words or common phrases**

* Hackers use “dictionary attacks” that try common words and leaked password lists.

**7. Consider using a password manager**

* Generates and stores complex, unique passwords for you.
* This avoids the need to memorize them all.

**8. Enable multi-factor authentication (MFA)**

* Even the strongest password can be stolen — MFA adds an extra barrier.

**9. Update passwords after a breach**

* If a service you use is hacked, change your password immediately.

6. Write down tips learned from the evaluation.

**Tips Learned from the Evaluation**

1. Length matters – Aim for at least 12–16 characters for strong protection.
2. Mix character types – Use uppercase, lowercase, numbers, and special symbols.
3. Avoid personal info – Don’t use names, dates, or easily guessed details.
4. Use passphrases – Combine random words into a memorable but unpredictable phrase.
5. Make each password unique – Never reuse passwords across accounts.
6. Avoid common patterns – Stay away from sequences like 1234, abcd, or keyboard patterns.
7. Use a password manager – To store and generate complex passwords securely.
8. Turn on MFA – Add extra security beyond just the password.
9. Change passwords after a breach – Act quickly if your account might be compromised.

7. Research common password attacks (brute force, dictionary).

**1. Brute Force:** Tries all possible combinations.

* Complexity and length increase attack time exponentially.

**2. Dictionary Attack:** Tries known words and common passwords.

* Avoid real words or common phrases.

**3. Credential Stuffing:** Uses leaked username-password pairs.

* Always use unique passwords for each site.

**4. Crunch Command:** is a Linux tool

* Used to generate custom wordlists for password cracking, testing, or brute-force attacks.

8. Summarize how password complexity affects security.

The strongest passwords are long, random, and unpredictable. Testing in tools like PasswordMeter highlights weaknesses you may not notice. A good approach is to create random passphrases or long strings and store them in a password manager.

Password complexity directly increases security by making it harder for attackers to guess or crack the password through brute force, dictionary, or social engineering attacks. Complex passwords use a mix of uppercase and lowercase letters, numbers, and special symbols, which expands the number of possible combinations an attacker must try. This significantly increases the time and computing power required to break them. When combined with sufficient length and uniqueness, high complexity helps protect against both automated attacks and password reuse risks, thereby strengthening overall account security.