Task – 6 Create a Strong Password and Evaluate Its Strength

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

Tools: Online free password strength checker

(https://www.passwordmonster.com/)

Procedure

In this activity, I aim to explore and evaluate the effectiveness of various password combinations in terms of strength and resistance to cracking attempts.

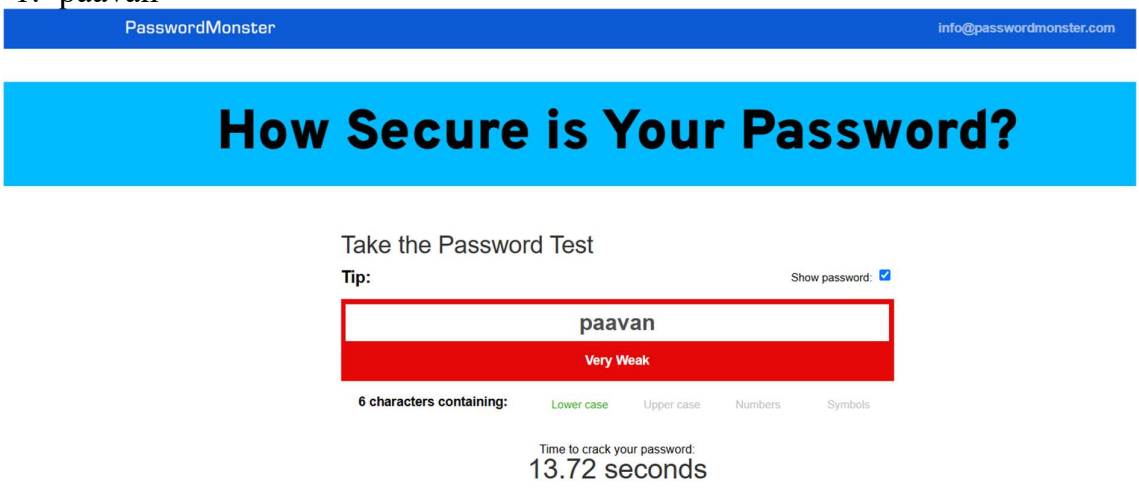
To conduct this experiment, I've prepared a custom list of sample passwords. These were designed with increasing complexity to observe how each modification impacts their overall security.

The sample passwords used for testing are as follows:

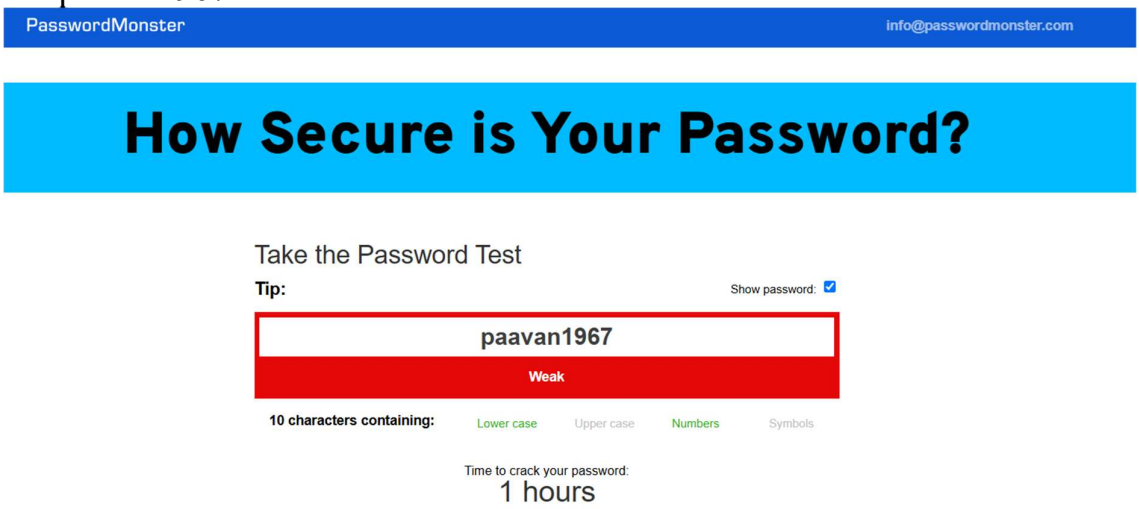
- **paavan**
- **paavan1967**
- **paavan*1967**
- **p#aa*10van@#sh20**

Each password builds upon the previous one, adding elements like numbers, uppercase letters, and special characters to increase complexity.

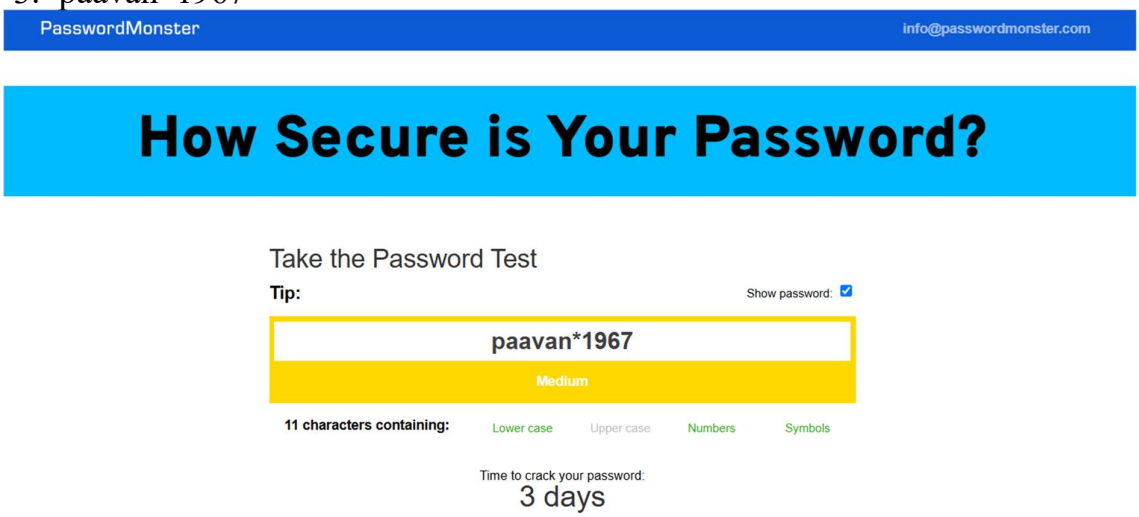
1. paavan



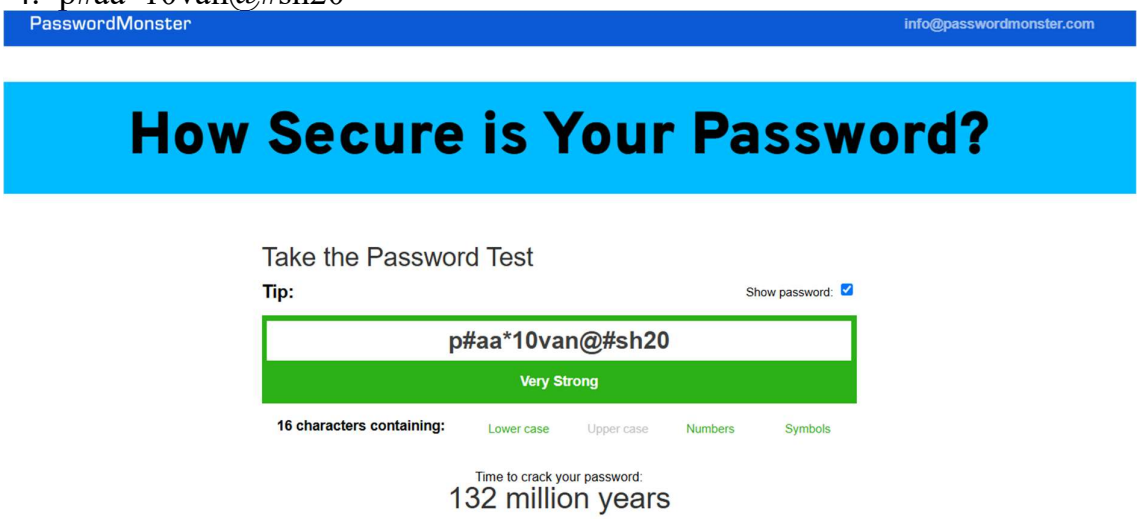
2. paavan1967



3. paavan*1967



4. p#aa*10van@#sh20



Analysis of Password Strength

This particular password is considered highly secure due to several key features that increase its complexity and resistance to brute-force or dictionary attacks.

Firstly, there is a deliberate alteration in the structure of the username—where a letter within the name has been substituted (e.g., replacing "a" with "X"). This small but effective change adds unpredictability to the password pattern. Additionally, the inclusion of an uppercase letter within the modified section further complicates any guessing attempts, as it forces attackers to consider both lowercase and uppercase variants during their attempts.

Moreover, the password incorporates a well-balanced mix of elements:

- **Numerical digits placed randomly**
- **Uppercase and lowercase character blend**
- **Extended character length**
- **Use of a special symbol ($)**

This combination significantly enhances the password's entropy, making it much more resistant to modern cracking techniques—even those utilizing automated tools. Such complexity ensures that even with the use of advanced algorithms, the password remains difficult to decipher.

- Its time to try a password that Google Password Suggestion feature suggests us and check it strength and analyze what makes that password much stronger than the one we created.

Effective Strategies for Creating Strong Passwords

To safeguard your digital identity, it’s essential to build passwords that are resilient against cracking attempts. Here are some important strategies to follow:

- Mix **uppercase** and **lowercase** characters to reduce predictability.
- Incorporate **digits** and **special characters** (like @, #, !, $, etc.).
- Ensure your password has a **minimum length of 12–16 characters**.
- Avoid any **personal identifiers** such as your name, date of birth, or popular words.
- Create passwords with **nonsensical combinations** that don't form recognizable words.
- Use a **password manager** to generate and store complex, unique passwords for every platform.

Paavan Shastri

💡 Key Takeaways from Password Strength Testing

After analyzing multiple sample passwords with varying levels of complexity, several important lessons were observed:

- **Stay away from simplicity**: Short, name-based, or real-word passwords are highly vulnerable.
- **Length adds security**: A longer password means exponentially more combinations for an attacker to guess.
- **Embrace randomness**: Mixing unrelated characters, numbers, and symbols enhances protection.
- **Avoid predictable changes**: Swapping ‘a’ with ‘@’ is helpful, but truly random modifications are far stronger.
- **Don’t use personal data**: Birth years, usernames, and common patterns make passwords easier to guess.

🛠️ Popular Techniques Used in Password Cracking

Cybercriminals utilize a variety of methods to try to uncover user passwords. Here are two widely used approaches:

- **Brute-Force Attack**: This method involves systematically checking every possible character combination until the correct one is found. It becomes feasible against short or simple passwords.
- **Dictionary Attack**: Attackers use a predefined list of commonly used words or known passwords to attempt quick matches. If your password includes regular phrases, it becomes easier to crack.

Both methods can be executed using automated software that tests **millions of guesses per second**, making password strength critical.

🔍 Impact of Password Complexity on Security

The more intricate your password is, the more challenging it becomes to break. A complex password typically includes:

- A mix of uppercase and lowercase letters
- Numbers

Paavan Shastri

- Special characters
- No meaningful or guessable patterns
- A long string length

In essence, increasing a password's complexity increases the total number of possible combinations an attacker must try, which in turn delays or prevents successful cracking using brute-force or dictionary attacks.