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/)

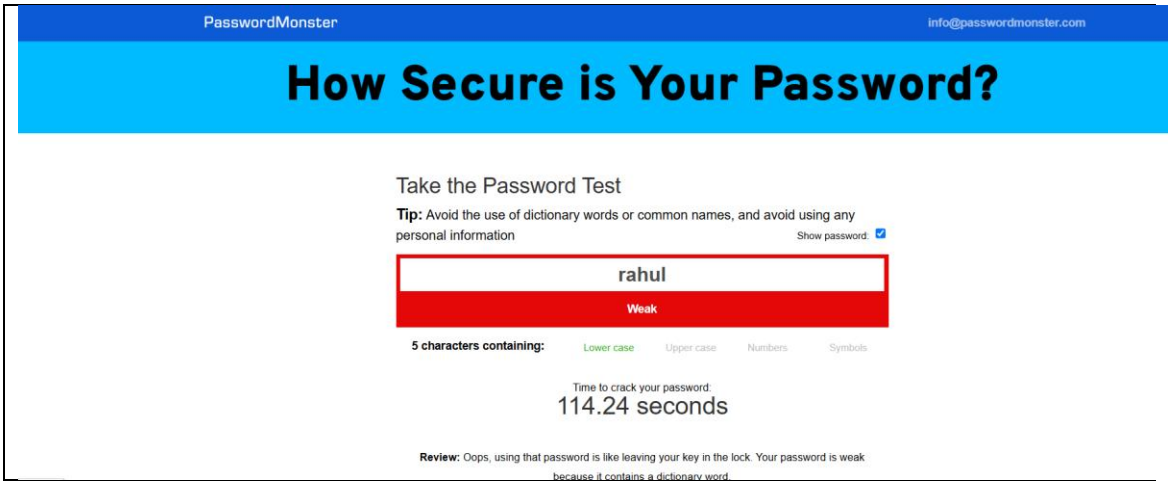
Step-by-Step Procedure

- To test and understand what makes a password strong we will be taking a list of passwords that I have created for testing purpose of how easily a password can be cracked and identified.

- The list of passwords are :
  - rahul
  - rahulshah
  - rahul1284shah
  - rXhul1284shah
  - rXhuL$1284shah

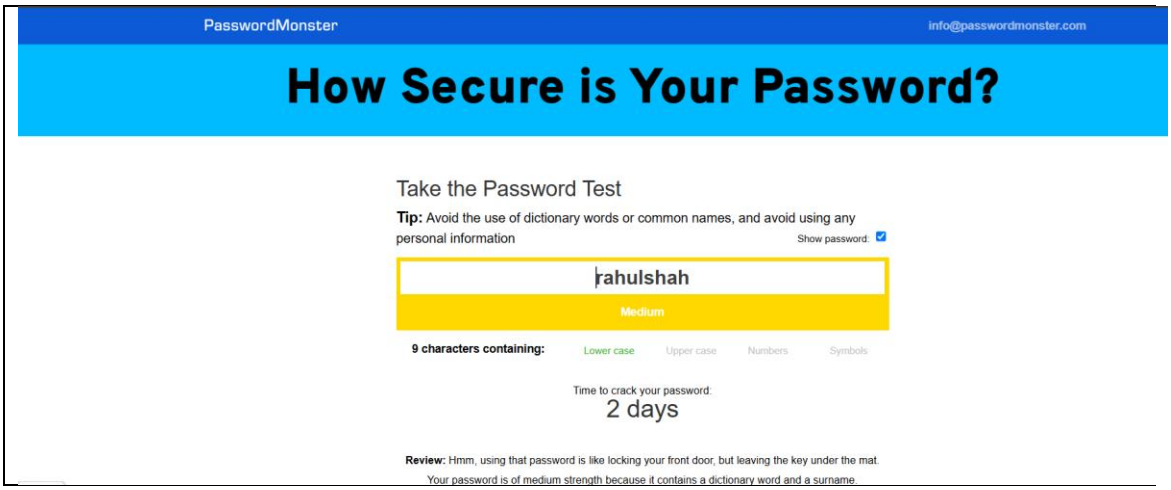
- At end I will also be using Google's Password Suggestion feature to create a strong password and tests its strength.

1. rahul



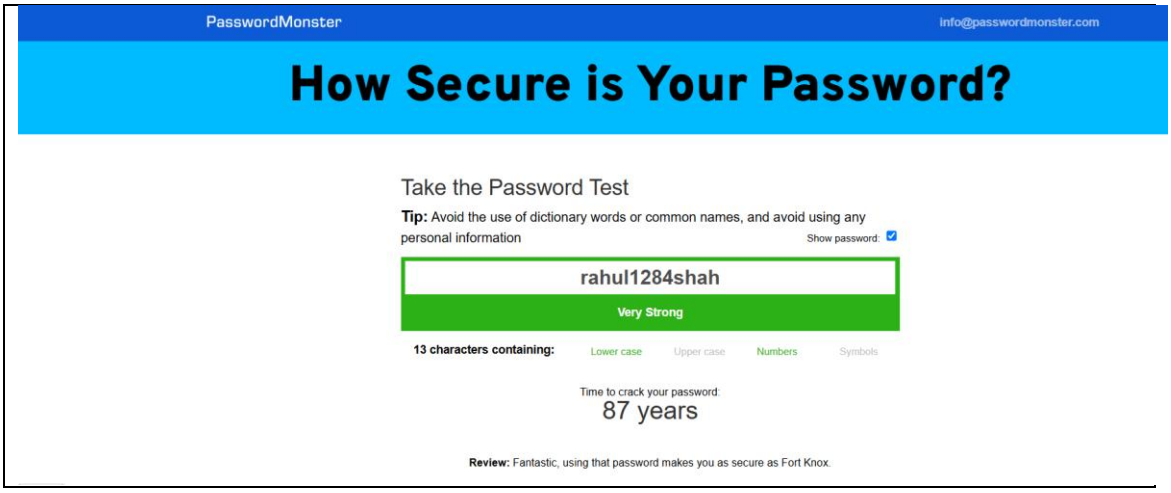
- The reason for this password being weak is that it contains just the simple name of the person or the user which is way too easy for an attacker to identify.

2. rahulshah



- The reason for this password having medium strength is its length and has a extended surname of user, but still it is easier for the attacker to crack this password if he/she knows the whole name of the user.

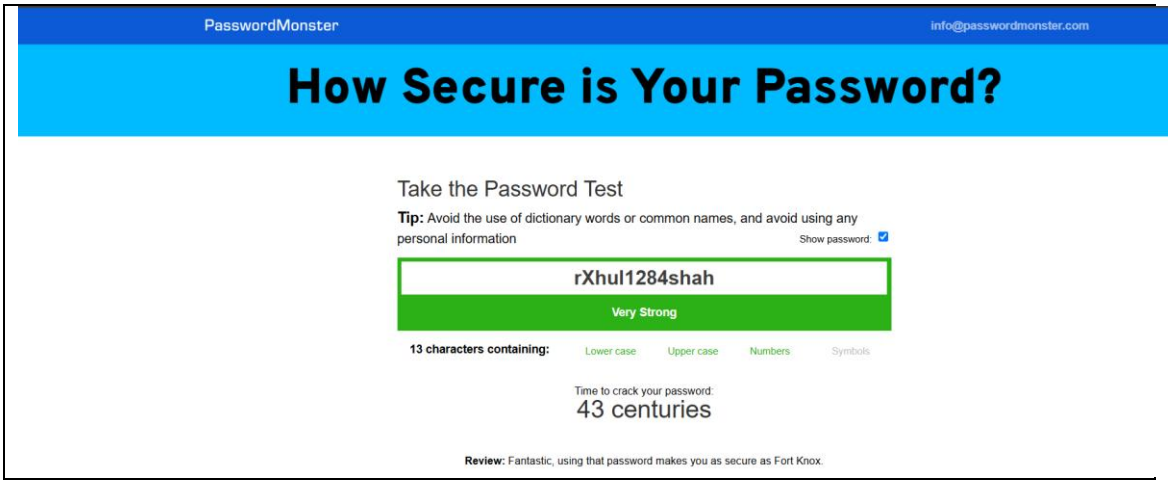
3. rahul1284shah



- The reason for this password being very strong is that it contains the full name of the person with addition of some **random digits** in the between.

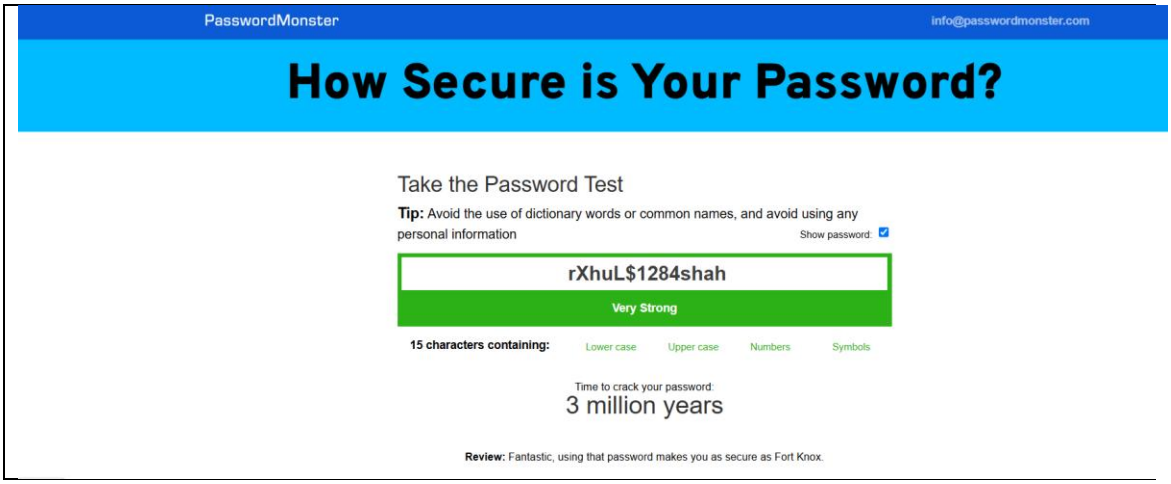
- But still it not hard for the attacker to get used to this pattern as he/she can use automated tools for random digits and through continuous brute force of different combinations of passwords, the real one can be identified.

4. rXhul1284shah



- The reason for this password being very strong is that though it contains the random digits and the name of the user but it also contains a character mismatch in the name itself (i.e. ‘a’ is replaced with ‘X’) with a upper case letter which makes it difficult for the attacker to crack because he/she has to iterate a multiple amount of alphabets both upper case and lower case to know the real-one used in the password.

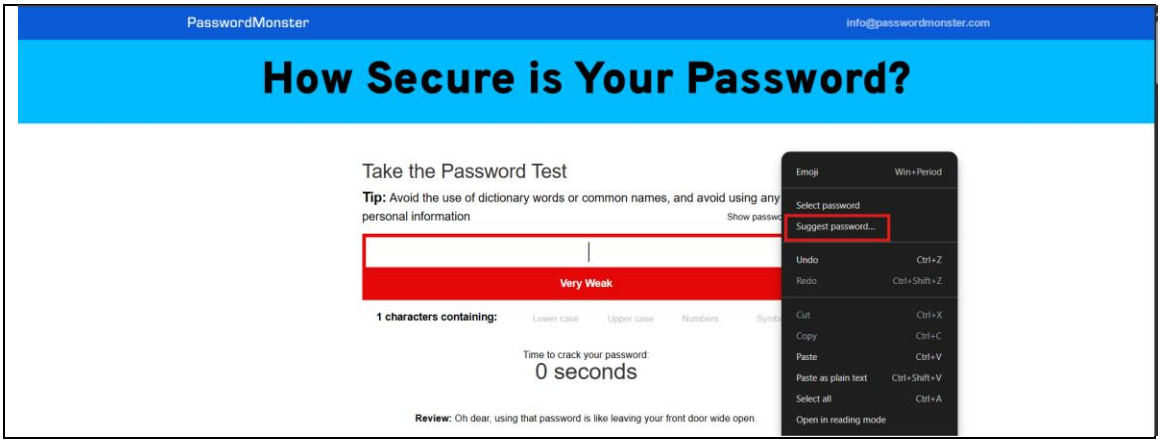
5. rXhuL$1284shah

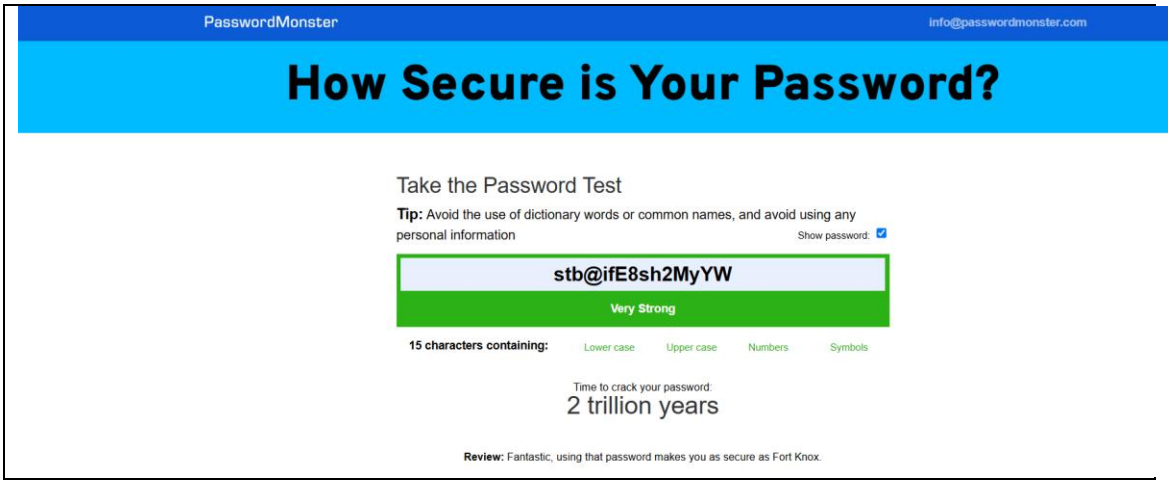


- The reason for this password being very strong is that it contains
  - Random digits
  - Upper case letters
  - Length
  - Lower case Letters
  - Special Character($)

- This combination of letters, numbers and special character makes it much tough for the attacker to crack the password even though using automated tools for password cracking.

6. 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.





- The reason for this password being very strong and making it nearly impossible for an attacker to crack is :
  - Lower case letters
  - Upper case Letter
  - Random Digits
  - Special Characters
  - Length
- What makes this password unique and strong from previous passwords?
  - This password contains random arrangement of letters, numbers and special characters in such a way that it does not have any meaning or any relation with the user.
  - In previous password the user included his/her name with random digits and special characters but still it had chances to be cracked.

- But in this case the password does not have any connectivity with the users name or any personal information.
  It is the just the random arrangement of every aspect what is required to make a **Strong Password.**

Best Practices for Creating Strong Passwords

When creating a strong password, follow these best practices to ensure maximum security:

- Use a combination of **uppercase and lowercase letters**.
- Include **numbers** and **special characters** (like `@`, `#`, `$`, `%`, etc.).
- Make the password **at least 12–16 characters** long.
- Avoid using **personal information** such as names, birthdays, or common phrases.
- Use **unpredictable combinations** of characters that have no dictionary meaning.
- Consider using a **password manager** to generate and store strong, unique passwords for each site.

Tips Learned from the Evaluation

From evaluating the different passwords and their strength, we can derive the following key tips:

- **Avoid simplicity**: Short passwords with dictionary words or names are the easiest to crack.
- **Length matters**: The longer the password, the harder it is to brute force.
- **Randomization is key**: A password that mixes unrelated characters, digits, and symbols significantly increases strength.
- **Avoid patterns**: Predictable substitutions (like replacing `a` with `@`) are better than nothing, but random substitutions are more secure.
- **Personal info is risky**: Including your name, birth year, or common sequences makes a password vulnerable to social engineering.

Common Password Attacks

Attackers use various methods to try and crack passwords. Two of the most common are:

- **Brute Force Attack**: In this method, the attacker tries every possible combination of characters until the correct password is found. This attack is more successful against short or simple passwords.
- **Dictionary Attack**: The attacker uses a list of common words and phrases (a "dictionary") to guess the password. This method is effective against passwords that use real words or common patterns.

Both attacks can be automated using tools that test millions of combinations per second, which is why strong and complex passwords are crucial.

How Password Complexity Affects Security

Password complexity directly impacts how difficult it is for an attacker to crack it. The more complex a password is—by including uppercase and lowercase letters, numbers, symbols, and using longer lengths—the more combinations an attacker has to try. This dramatically increases the time and computing power needed for a successful attack.

In simple terms, **complex passwords are more resistant to brute-force and dictionary attacks**. A random, complex password that lacks recognizable patterns or personal info is significantly harder to crack than one based on names or common phrases.