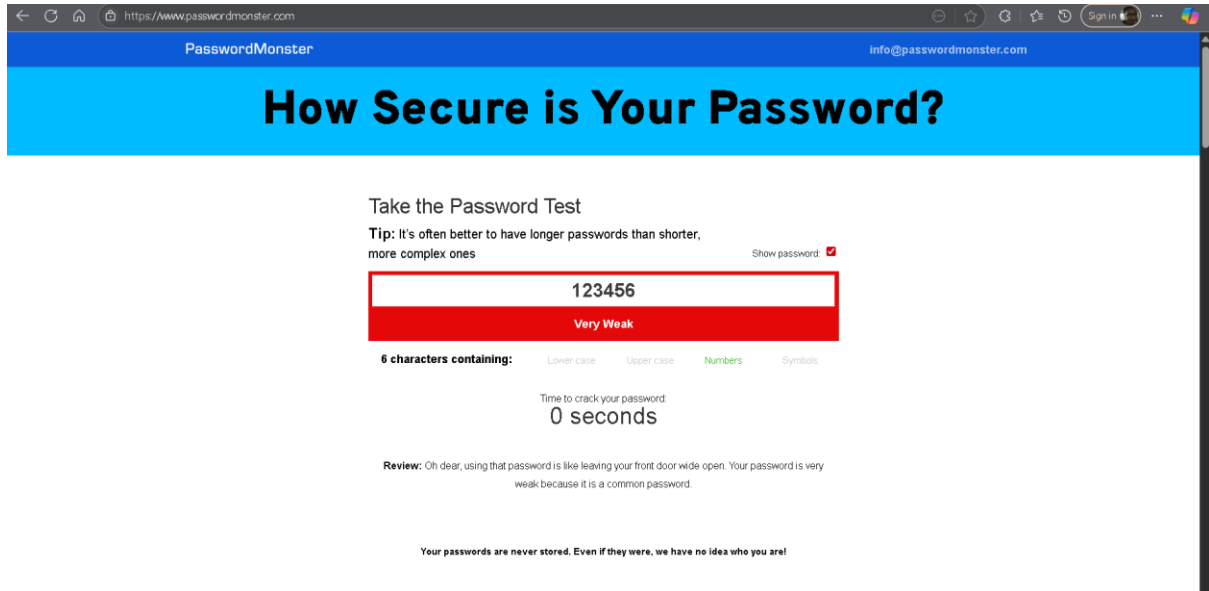


# Task 6:

By: Niranjan Manoj

Using a site known as password monster we evaluate the strength of various types of passwords:



The screenshot shows the PasswordMonster website interface. At the top, there's a blue header with the site name and email. Below it, a large blue banner asks 'How Secure is Your Password?'. The main content area is white and titled 'Take the Password Test'. It includes a tip about longer passwords, a 'Show password' checkbox, and a password input field containing '123456'. Below the input field, a red bar indicates the password is 'Very Weak'. A breakdown shows '6 characters containing: Lower case, Upper case, Numbers, Symbols'. The estimated cracking time is '0 seconds'. A review message states: 'Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password.' At the bottom, a note says 'Your passwords are never stored. Even if they were, we have no idea who you are!'.

The website suggests us to use all the different types of characters such as numbers, symbols, upper and lower case. It also shows the time it would take for the password to be cracked.

## Take the Password Test

**Tip:** It's often better to have longer passwords than shorter, more complex ones

Show password: ☒



The form shows a password input field with the text 'Xyz@123'. Below the input field, a red bar indicates the password is 'Weak'.

**7 characters containing:** Lower case Upper case Numbers Symbols

Time to crack your password:  
**42.87 minutes**

**Review:** Oops, using that password is like leaving your key in the lock. Your password is weak because it contains a dictionary word and a sequence of characters.

The website also suggests to not use dictionary words as it makes it easier to crack

## Take the Password Test

**Tip:** It's often better to have longer passwords than shorter, more complex ones

Show password: ☒

eL@vA!E@734|

Very Strong

**11 characters containing:**

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

45 years

**Review:** Fantastic, using that password makes you as secure as Fort Knox.

Increasing the no of characters as well including a variety of characters makes our password a lot more stronger

Some common password attacks are as follows:

- a)Bruteforce: where every possible combination is tried out until success
- b) Dictionary Attack: where common words and variations are tried out
- c)keylogging: where a malware records our keystrokes

To conclude the higher the complexity and length of the password the harder it is to any form of attack and weak passwords such as names and dictionary words should be avoided