Task 6

Today's task is simple but very important to understand as every person needs to understand the value of having strong passwords which can save them from soo much trouble. So let's understand how to create a strong password and what is the definition of a strong password:

1. Firstly let's create multiple random passwords for me the examples would be:
   - password123
   - Password@123
   - Tr33H!v3$L!ghT
   - !Qw9@Er7#Zx2&Ty1
   - Admin2024
   - G#7mP%u6v!rL^9aD
2. Now we have a simple list of passwords that we can compare to see which one is a better password.
   3. To do this we need to check these against some online tools I mainly use " passwordmeter.com " so lets check some passwords in the website like in fig1:

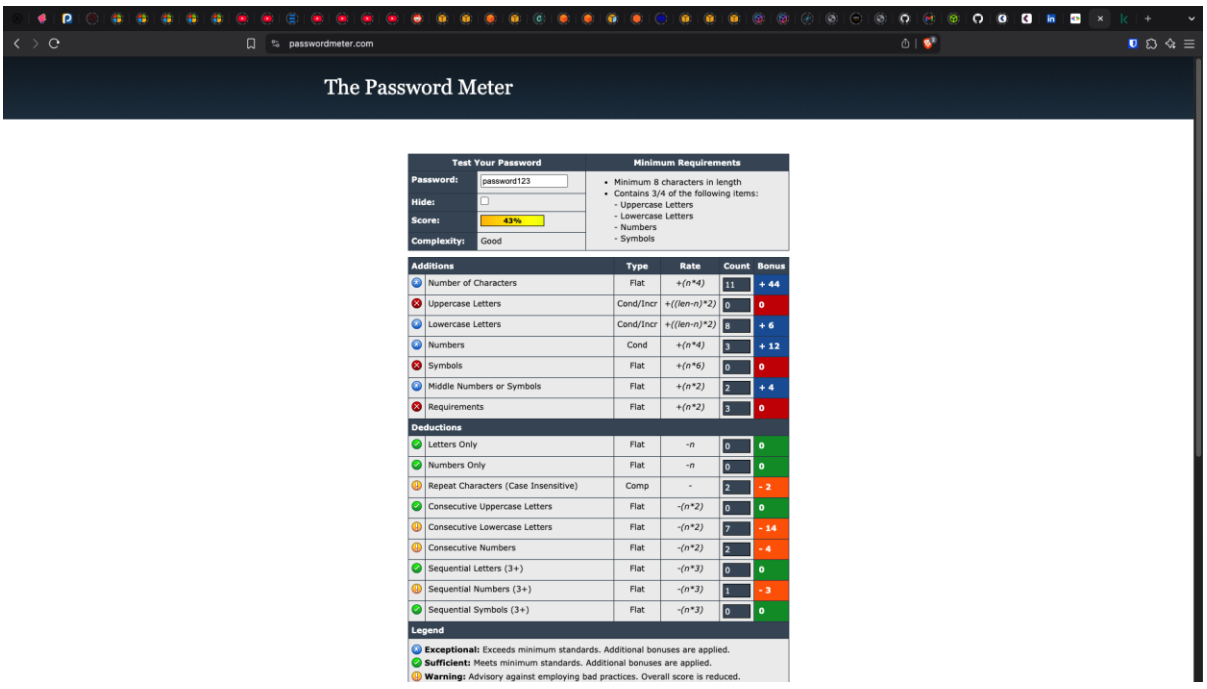

fig1

4. Just like in fig 1 lets check all the other passwords and check the scores:
   - Password123: 43%
   - Password@123: 65%

- Tr33H!v3$L!ghT: 100%
- !Qw9@Er7#Zx2&Ty1: 100%
- Admin2024: 75%
- G#7mP%u6v!rL^9aD: 100%

5. Now let's understand how to make a strong password
   To make a strong password there are 5 main key factors:
   - Use a minimum of 12–16 characters.
   - Include a mix of uppercase, lowercase, numbers, and special characters.
   - Avoid dictionary words, names, or repeated patterns.
   - Don't reuse passwords across accounts.
   - Use passphrases or random word combinations for memorability (e.g., Horse-Battery!Staple$123).
6. Now this is the information I found out while reading a blog post on password complexity which was realy informative and helpfull in this task.
7. Now lets see what I learned from this evalation :
   - Firstly the more complex your password is the morescore you are gonna get on password checking websites
   - Adding symbols and increasing the length has the most noticeable effect for strong passwords
   - Using predictable patters like "chinmay + 1234" is the reciepe to create a weak password, AVOID IT.
   - Most tools use comparison techniques from already available data sets which can lead to false possitives its the passwords is not avalable on the dataset but still could be a weak password.
8. Now see come of the password related cyber attacks and how to prevent them:
   - Brute force: the attacker tries every possible combination to try and force his way through by just guessing or using automated tools.
   - Dictionary: the attacker used common but predictable words like qwerty and admin123 to try and get the login.
   - Credential stuffing: The attacker uses leaked passwords from other breaches to try and guess one from them is yours.
   - Phishing: The attacker tricks you into telling him your password or take subtle hints by keeping a relationship with you.

Now you must be thinking the scores aren't soo bad but in this category anything below 100% is bad because the passwords which are low scored are generally prone to be breached easily like for example Password@123 might have gotten a score of 65% but it

still is one of the most common passwords on the planet which is not a good case if you it set as your password and someone tries to brute force your account. So the simple key security advise is to trn on MFA on everything that requires a login.