ELEVATE LABS CYBERSECURITY INTERNSHIP

Task-6:

1)

12345678 - Very weak

Elevatelabs- Weak

ElevateLabs@2005 - Good

El@2ev00atela5bs - Strong

/wv5G*]mZe*oy),sw - Very Strong

2)

Lets compare the above passwords with respect to Numbers, Uppercase, Lowercase, symbols, and length variations used

Password

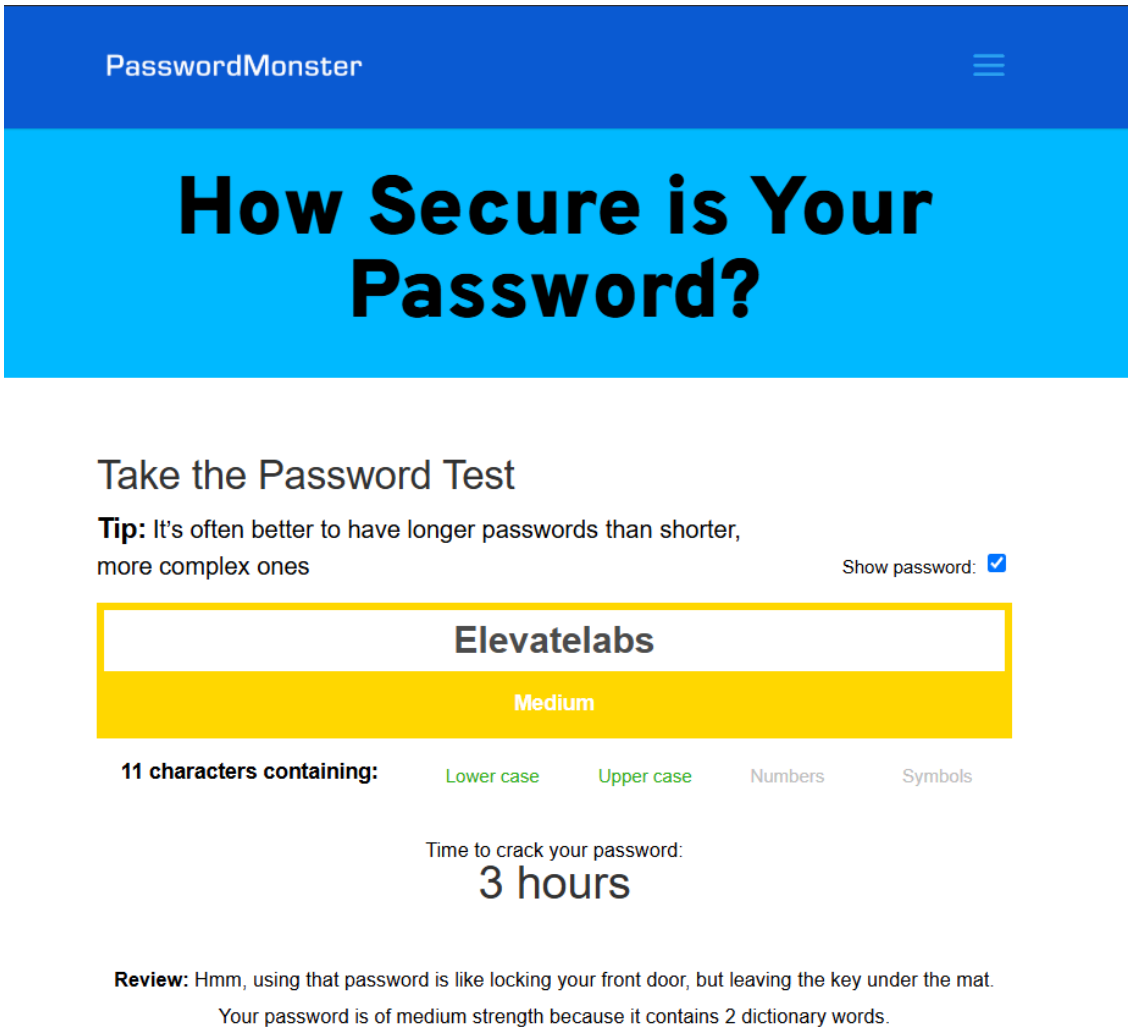
Password	Uppercase	Lowercase	Symbols	Numbers	Length
12345678	NO	NO	NO	YES	8
Elevatelabs	YES	YES	NO	NO	15
Elevatelabs@2005	YES	YES	YES	YES	16
El@2ev00atela5bs	YES	YES	YES	YES	16
/wv5G*]mZe*oy),sw	YES	YES	YES	YES	17

3,4)

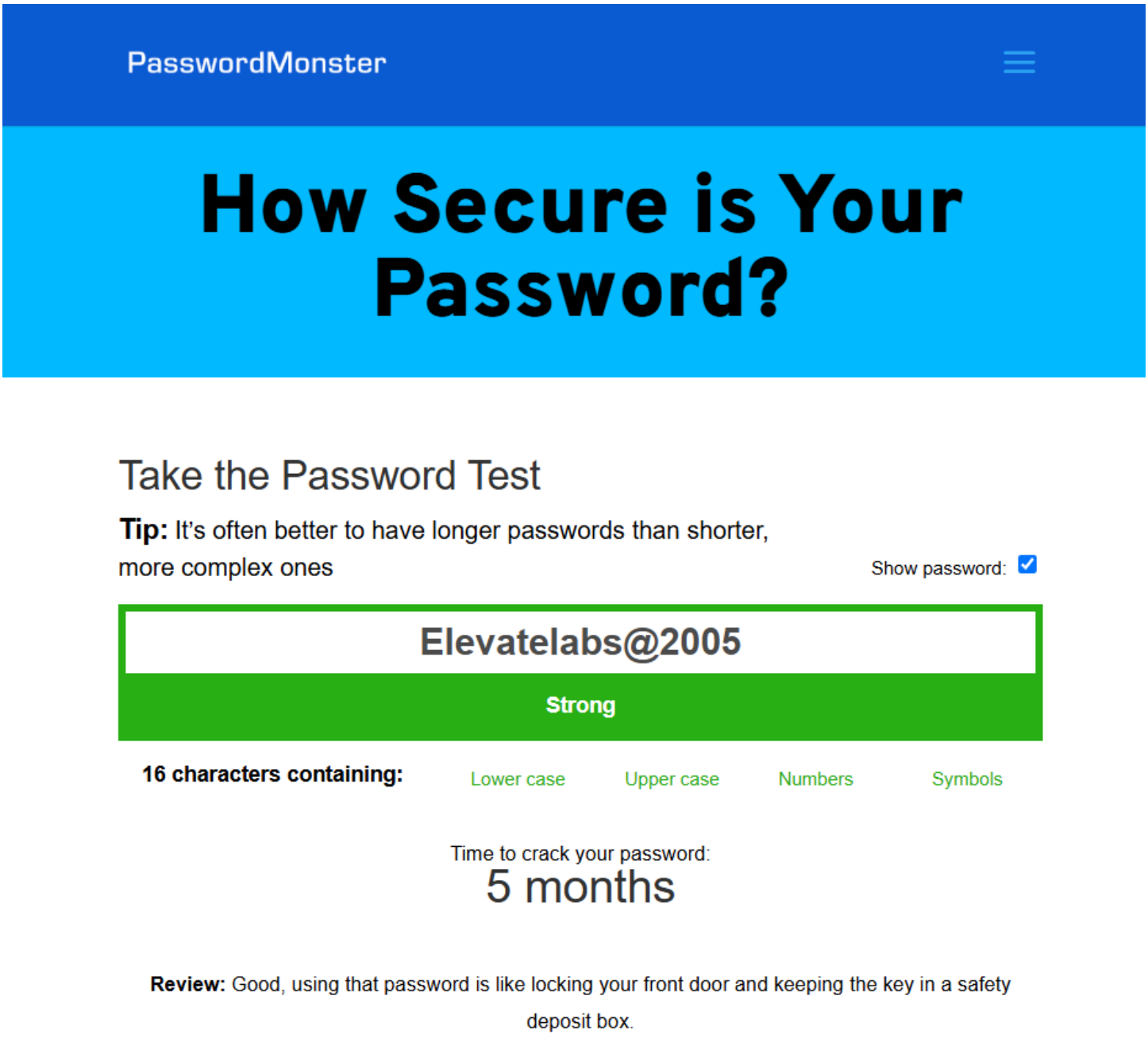
Using Password Strength Meter checking the strength of passwords created also scores and feedbacks can be observed

Password:12345678

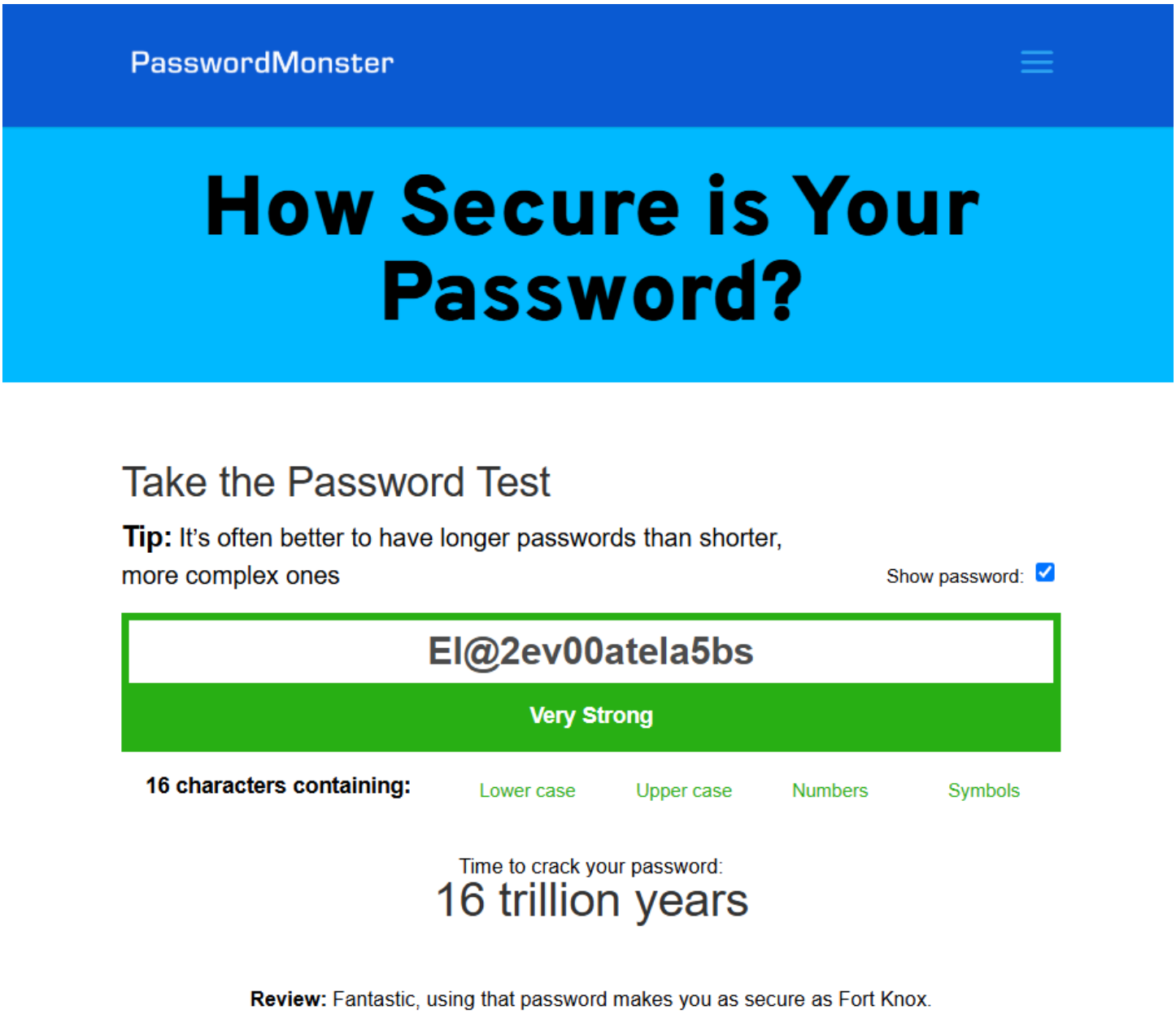
Password:Elevatelabs



Password:Elevatelabs@2005



Password:El@2ev00atela5bs



Password:/wv5G*]mZe*oy),sw

5)

Use at least 12–16 characters

Mix uppercase, lowercase, numbers, and symbols

Avoid dictionary words and common phrases

Do not reuse passwords across different accounts

Use a password manager to store and generate passwords

There are also some tools such as 🌐 Create strong passwords for free | F-Secure and also google password generator to generate very strong passwords

6)

A password like Elevatelabs@2005 is decent but not enough for high-value accounts

Complexity must be combined with length (16+ characters ideal)

Avoid patterns like Name + Year or Word + Number

Passwords should be randomly generated if possible

Adding multiple symbol types improves score significantly

7)

Brute Force:

Tries every possible combination until the correct one is found effective against short, simple passwords

Dictionary Attack:

Uses common words or phrases from a predefined list very effective on passwords like Elevatealabs

Credential Stuffing:

Uses leaked username password pairs on multiple sites prevented by using unique passwords for each account so instead of using same password across multiple platforms use various passwords and try to change password in fixed intervals

8)

Low complexity : susceptible to quick dictionary/brute force attacks easy to crack using existing state of art tools

Medium complexity : delays attackers not effectively but for a short amount of time not preferable to use where privacy matters the most.

High complexity + length : Very tough to crack even with the state of art tools that are present the more complex and lengthy the password is the more difficult for it to get cracked.

So choosing password wisely with higher complexity is a better choice to do else passwords alone not going to help to keep our details in applications secure enough.