Task 6

Password Strength Evaluation Report

Objective:

To understand what makes a password strong by testing multiple passwords of varying complexity using online password strength checkers, and analyzing the results.

Passwords Tested and Evaluation

1. Password: MaximumHello@#87894885
   - Strength: Very Strong
   - Reason: Long, includes uppercase, lowercase, numbers, and symbols.

2. Password: myname777@#

- Strength: Medium
- Reason: Good use of characters but relatively short.

3. Password: adminadmin12

- Strength: Weak
- Reason: Predictable word (admin) and lacks symbols.

4. Password: admin admin

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with   Show password: ☑

adminadmin
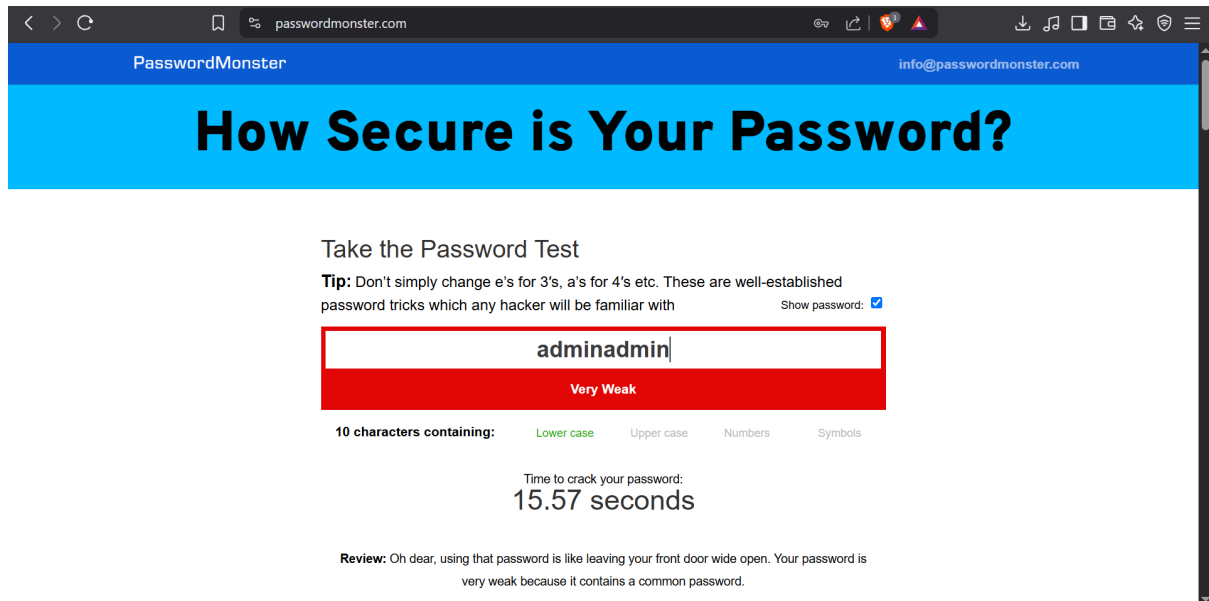
Very Weak

10 characters containing: Lower case   Upper case   Numbers   Symbols

Time to crack your password:
15.57 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password.

    - Strength: Very Weak
    - Reason: Common word, has a space, no numbers or symbols, very guessable.

What Makes a Password Strong?
- At least 12–14 characters.
- Mix of uppercase, lowercase, numbers, and special characters.
- Avoid common words like 'admin', 'password', or '123456'.
- No reuse across accounts.
- Not based on personal information (name, birthdate, etc.).

Tips Learned from Evaluation:
1. Use passphrases or a mix of unrelated words and symbols (e.g., RedTiger#Skate44!).
2. Avoid patterns like 'adminadmin', 'qwerty', or repeating numbers.
3. Use a password manager to store and generate secure passwords.
4. Enable Two-Factor Authentication (2FA) wherever possible.

Tools Used
- passwordmonster.com