

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



The screenshot shows the PasswordMonster website interface. At the top, there's a blue header with 'PasswordMonster' and 'info@passwordmonster.com'. Below this is a large blue banner with the text 'How Secure is Your Password?'. The main content area has a white background. It starts with the heading 'Take the Password Test' followed by a tip: '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'. There's a 'Show password:' checkbox which is checked. Below this is a green-bordered box containing the password 'MaximumHello@#87894885'. Underneath the box is a green bar with the text 'Very Strong'. Below that, it says '22 characters containing:' followed by four green bars representing 'Lower case', 'Upper case', 'Numbers', and 'Symbols'. Further down, it says 'Time to crack your password:' followed by '12 thousand years'. At the bottom, there's a 'Review:' section that says 'Fantastic, using that password makes you as secure as Fort Knox.'

1. Password: MaximumHello@#87894885

- Strength: Very Strong
- Reason: Long, includes uppercase, lowercase, numbers, and symbols.

2. Password: myname777@#

passwordmonster.com

PasswordMonster info@passwordmonster.com

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: ☒

myname777@#

Medium

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
7 hours

Review: Hmm, using that password is like locking your front door, but leaving the key under the mat. Your password is of medium strength because it contains 3 dictionary words.

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

3. Password: adminadmin12

passwordmonster.com

PasswordMonster info@passwordmonster.com

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: ☒

adminadmin12

Weak

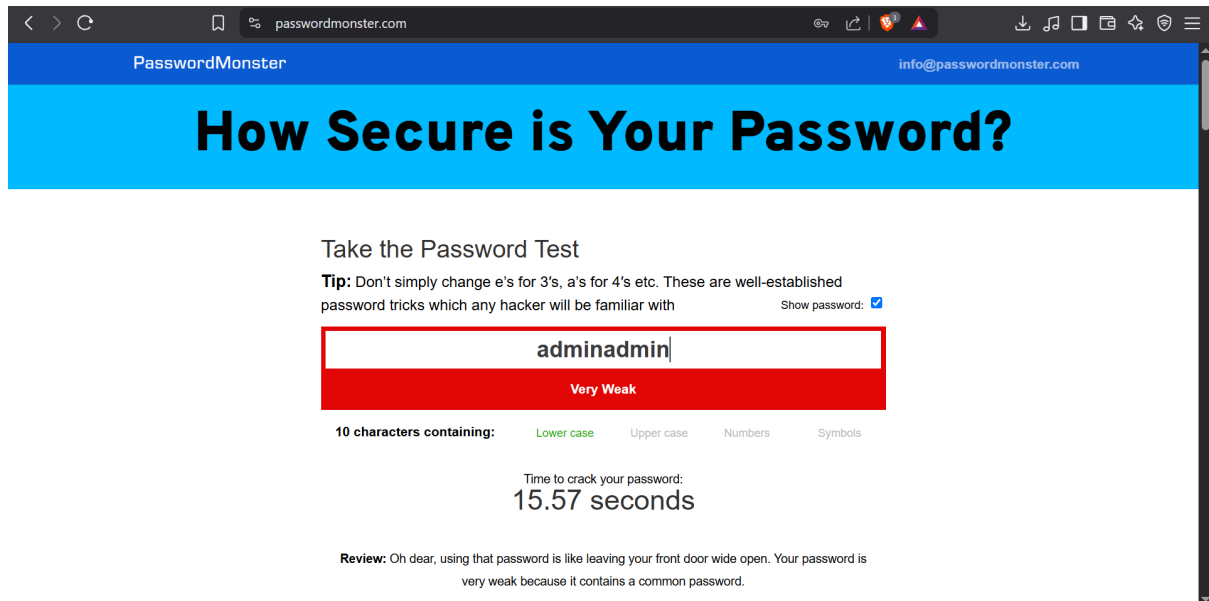
12 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
1 hours

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

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

4. Password: admin admin



- 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