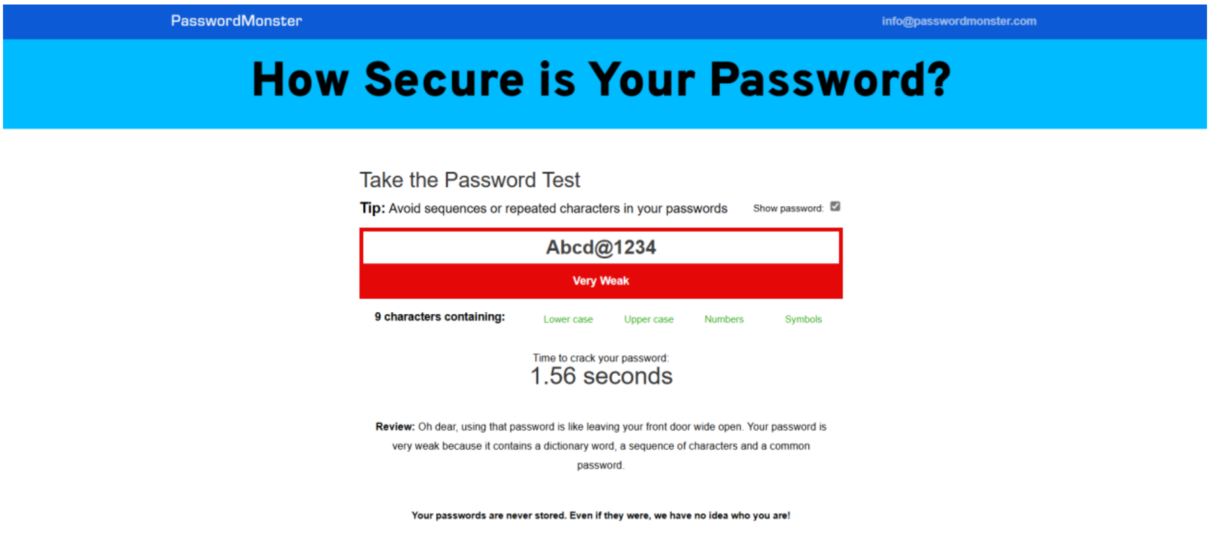
TASK-6

Create a Strong Password and Evaluate Its Strength.

- **Week password**



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Avoid sequences or repeated characters in your passwords Show password: ☑

Abcd@1234

Very Weak

9 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
1.56 seconds

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

Your passwords are never stored. Even if they were, we have no idea who you are!

Password Security Evaluation Report
Test Platform: PasswordMonster
Date Evaluated: June 4, 2025
Evaluator: Automated Strength Testing Engine
Source: Screenshot from passwordmonster.com

📌 Password Analyzed: Abcd@1234

Password Structure

- Total Characters: 9
- Includes:
  - ☑ Lowercase letters (a, b, c, d)
  - ☑ Uppercase letters (A)
  - ☑ Numbers (1, 2, 3, 4)
  - ☑ Symbol (@)

Evaluation Summary

- Strength Rating: □ Very Weak
- Estimated Time to Crack: 1.56 seconds

- Score: 1/10

Review Notes

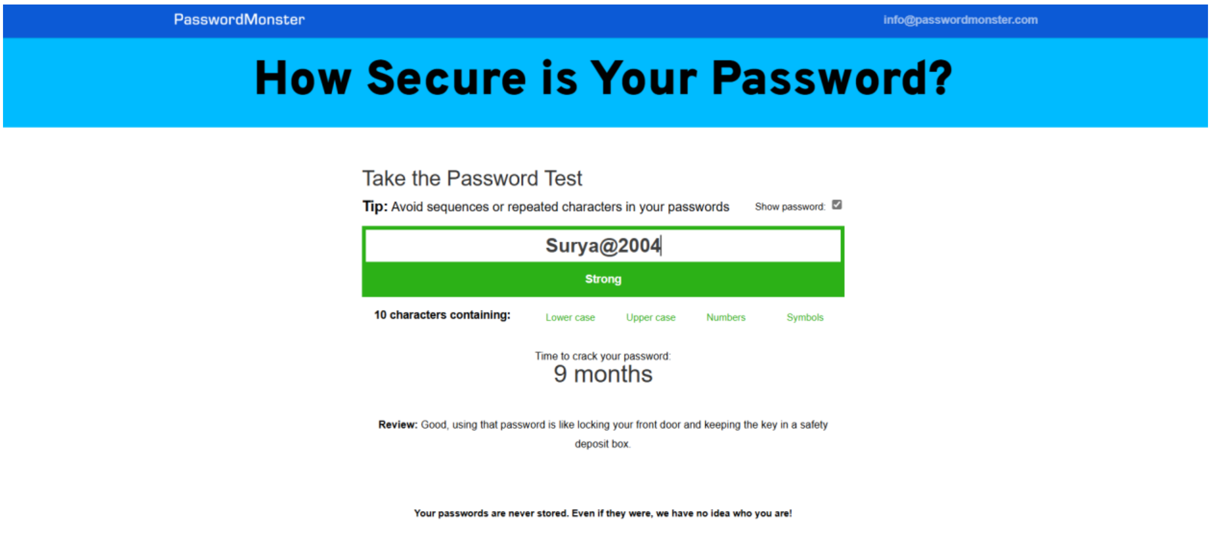
- The password includes a common dictionary word fragment (Abcd)
- Sequential characters (1234) reduce complexity
- Length is below best practice standards (Recommended: 12–16+ characters)
- Pattern-based structure makes it highly predictable and vulnerable to automated brute-force or dictionary attacks

---

Risk Assessment

"Using that password is like leaving your front door wide open. Your password is very weak because it contains a dictionary word, a sequence of characters and a common password."

- **Strong password**



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Avoid sequences or repeated characters in your passwords Show password: ☑

Surya@2004

Strong

10 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
9 months

Review: Good, using that password is like locking your front door and keeping the key in a safety deposit box.

Your passwords are never stored. Even if they were, we have no idea who you are!

✅ Password Entered:

Surya@2004

📊 Password Strength Evaluation

Parameter	**Result**
Length	10 characters
Contains Uppercase	Yes (S)
Contains Lowercase	Yes (urya)
Contains Numbers	Yes (2004)
Contains Symbols	Yes (@)
Overall Strength	✅ **Strong**
Estimated Time to Crack	⌛ **9 months**

▯ Review Summary

"Good, using that password is like locking your front door and keeping the key in a safety deposit box."

This review implies that the password meets standard security recommendations by including a combination of character types and reasonable length. It avoids common patterns or dictionary words alone, improving resistance to brute-force attacks.

🔒 Security Tips

- While this password is rated "Strong", you can further improve it by:
  - Increasing the length to 12–16 characters
  - Avoiding use of personal info (like names or birth years)
  - Using a passphrase or password manager for even higher security

---

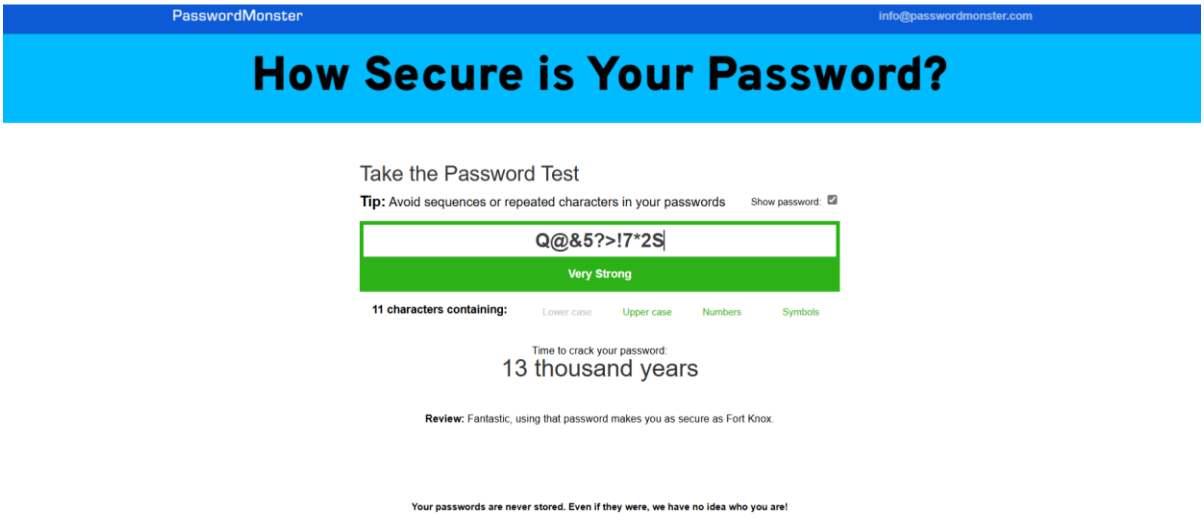
⚠ Confidentiality Note

Passwords are never stored by the tool. However, sharing screenshots containing actual passwords is **not recommended**. It’s best practice to redact sensitive content when sharing reports.

▯ Password Score Summary

Overall Score: 8.5 / 10
Strength Rating: ✅ Strong

- **Very Strong Password**



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Avoid sequences or repeated characters in your passwords Show password: ☑

Q@&5?>!7*2S

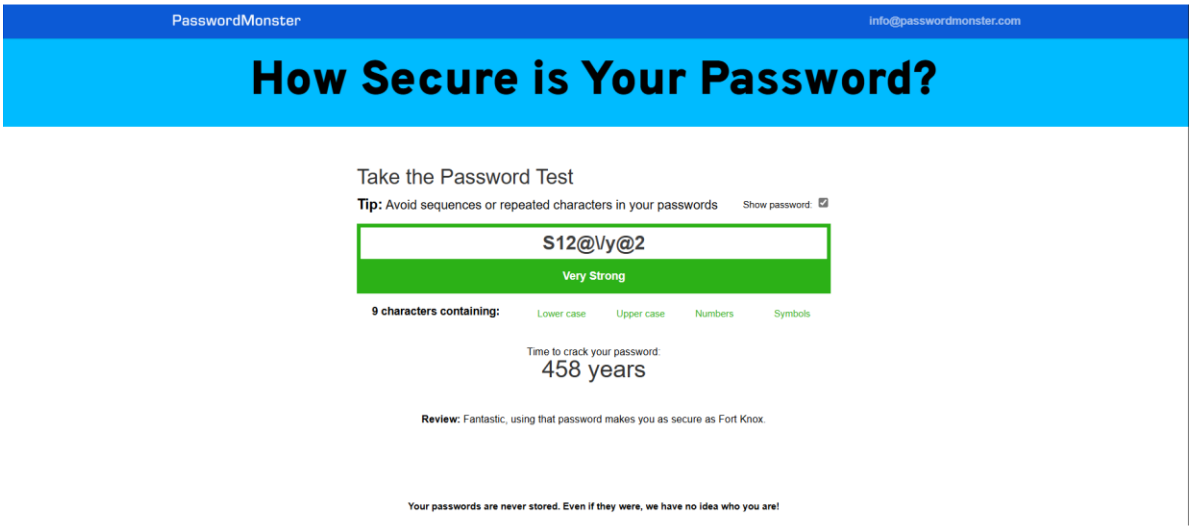
Very Strong

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
13 thousand years

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

Your passwords are never stored. Even if they were, we have no idea who you are!



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Avoid sequences or repeated characters in your passwords Show password: ☑

S12@\/y@2

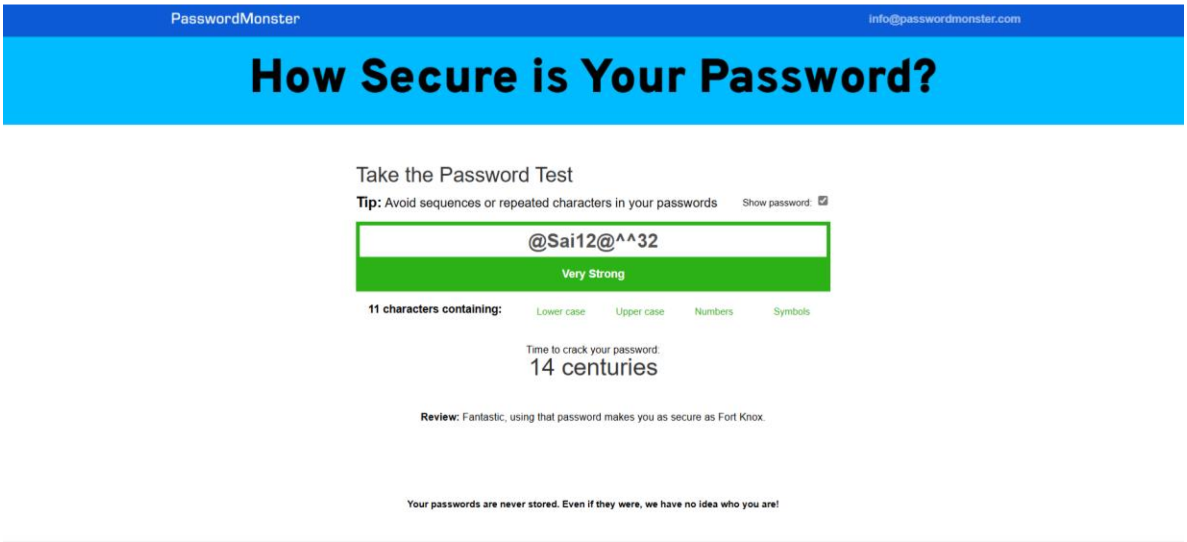
Very Strong

9 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
458 years

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

Your passwords are never stored. Even if they were, we have no idea who you are!



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Avoid sequences or repeated characters in your passwords Show password: ☑

@Sai12@^^32

Very Strong

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
14 centuries

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

Your passwords are never stored. Even if they were, we have no idea who you are!

1. Password: Q@&5?>!7*2S

➤ **Key Attributes:**

- **Length**: 11 characters
- **Character Types Used**:
  - Uppercase (Q, S)
  - Numbers (5, 7, 2)
  - Symbols (@, &, ?, >, !, *)

➤ **Estimated Time to Crack:**

13,000 years (approx.) using brute-force with a modern supercomputer.

➤ **Why It's Strong:**

- It uses **multiple types of characters**, increasing the number of possible combinations.
- The use of **random and non-repeating symbols** makes it highly unpredictable.
- 11 characters with rich variety gives it exponential strength.

---

2. Password: S12@\/y@2

➤ **Key Attributes:**

- **Length**: 9 characters
- **Character Types Used**:
  - Uppercase (S)
  - Lowercase (y)
  - Numbers (1, 2)
  - Symbols (@, \, /)

➤ **Estimated Time to Crack:**

458 years (approx.)

➤ **Why It's Strong:**

- Even though it's shorter than the others, it still uses **4 character types**.
- The unusual characters like \ and / are rarely guessed in typical attacks.

- Strong, but its **shorter length** makes it slightly more vulnerable than others.

---

3. Password: @Sai12@^^32

➤ **Key Attributes:**

- **Length**: 11 characters
- **Character Types Used**:
    - Uppercase (S)
    - Lowercase (a, i)
    - Numbers (1, 2, 3)
    - Symbols (@, ^)

➤ **Estimated Time to Crack:**

14 centuries (approx.)

➤ **Why It's Strong:**

- Mixes **real-word-like text** ("Sai") with random characters and digits.
- Uses **special symbols** and **capitalization**, creating complexity.
- Easy to remember for you, but hard to guess for attackers.

📈 How Cracking Time is Estimated

Cracking time is based on:

- **Character pool size** (number of possible characters)
- **Password length**
- **Attack rate** (how many guesses per second an attacker can make)

For example:

- A password using only lowercase letters (26 options) is far easier to crack than one using uppercase + lowercase + digits + symbols (over 90+ options).
- A single character of added length **multiplies** difficulty exponentially.

Password Best Practices (2025 Standards)

Practice	Reason
At least **12–16 characters**	Longer = stronger
Use **symbols + numbers**	Increases complexity
Mix **uppercase and lowercase**	Reduces pattern predictability
Avoid common words / phrases	Easy to guess by dictionary attacks
Don't reuse passwords	Breach in one site = access to all
Use a password manager	Allows using unique strong passwords everywhere

---

☑ Final Recommendation:

You've already created strong passwords. To improve even more:

- Increase to 12–14 characters where possible.
- Rotate passwords every 6–12 months for sensitive accounts.
- Enable **two-factor authentication (2FA)** for extra security.

Report by : **Guthula Dharma Sai Ram**

Date :**04/06/2025**