Cyber Security Internship Report

Task 6: Create a Strong Password and Evaluate Its Strength

Name: Dishanyaa Shrii K M
Date: 03 October 2025
Time: 02:35 PM (IST)

1. Objective

To understand the characteristics of a strong password, create multiple password samples of varying complexity, evaluate them using online password strength checkers, and analyze the results. The aim is to identify best practices for creating secure passwords and understand how password complexity affects protection against common attacks.

---

2. Tools Used : PasswordMonster

---

3. Methodology

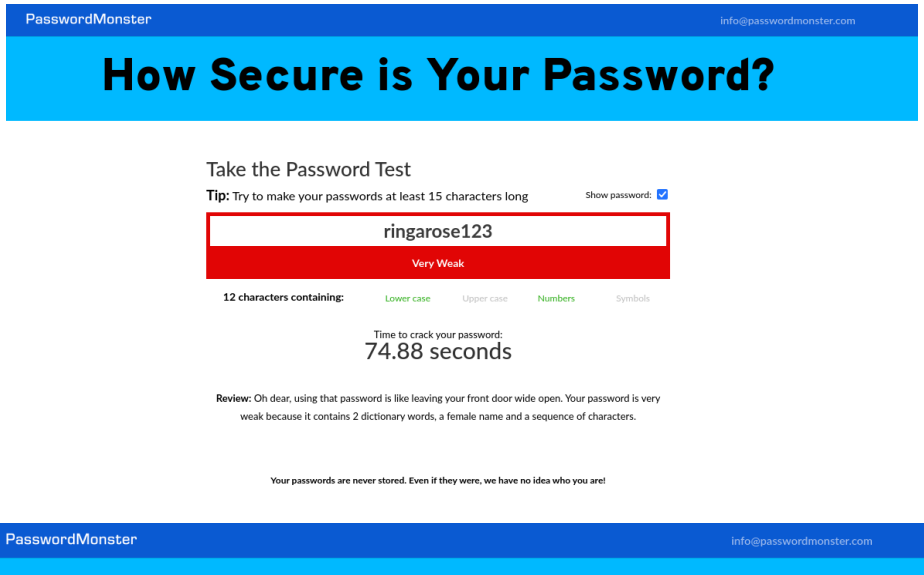
1. Created multiple passwords with different complexity levels.
2. Tested each password on PasswordMonster.com.
3. Recorded the score and feedback.
4. Compared results to identify factors contributing to password strength.
5. Researched common password attacks (brute force, dictionary, hybrid).
6. Summarized key findings into best practices for password creation.

---

4. Results

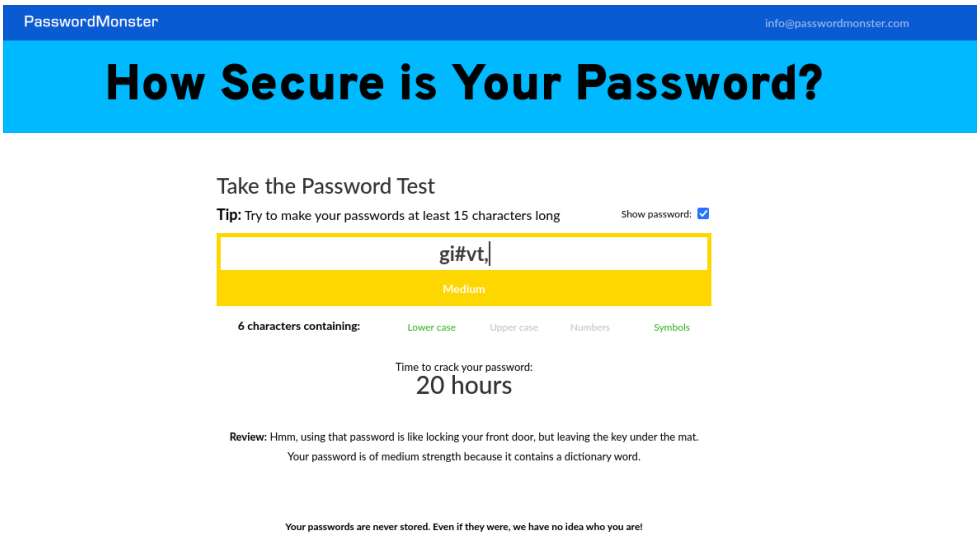
Password Strength Evaluation

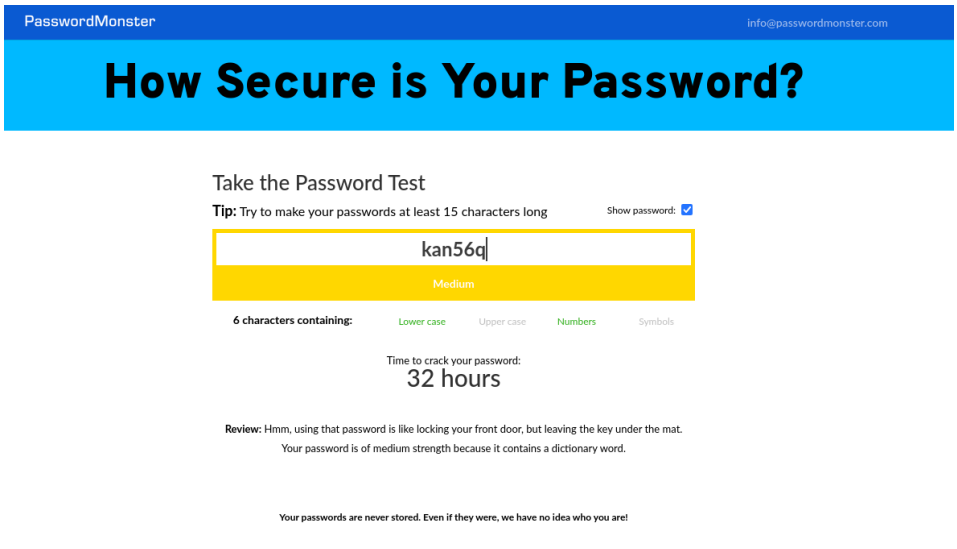

PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
ringarose
Very Weak
9 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
12.48 seconds
Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains 2 dictionary words and a female name.
Your passwords are never stored. Even if they were, we have no idea who you are!

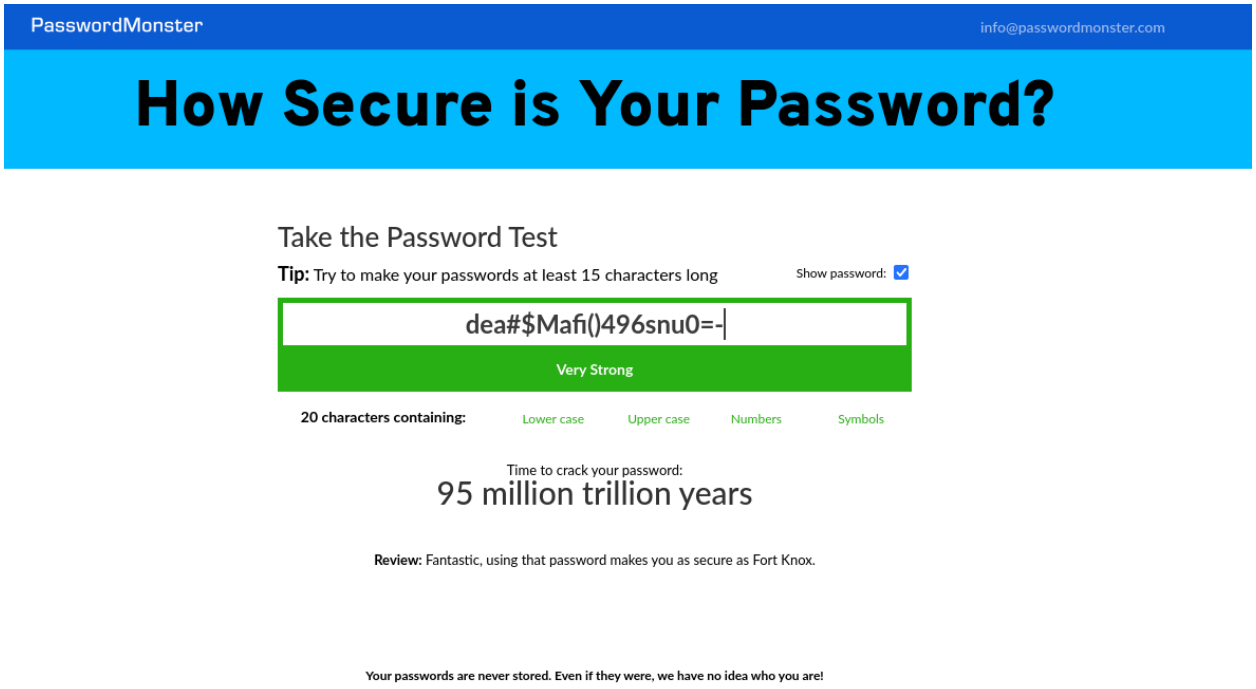

PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
ringarose123
Very Weak
12 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
74.88 seconds
Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains 2 dictionary words, a female name and a sequence of characters.
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: Try to make your passwords at least 15 characters long
Show password:
Password
Very Weak
8 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
0 seconds
Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password.
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: Try to make your passwords at least 15 characters long
Show password:
ea#$fe
Medium
6 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
2 days
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 a dictionary word.
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: Try to make your passwords at least 15 characters long
Show password:
gi#vt,
Medium
6 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
20 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 a dictionary word.
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: Try to make your passwords at least 15 characters long
Show password:
kan56q
Medium
6 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
32 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 a dictionary word.
Your passwords are never stored. Even if they were, we have no idea who you are!



---

5. Key Observations & Tips Learned

- **Length is critical**: Passwords above 12 characters are significantly stronger.
- **Use a mix** of uppercase, lowercase, numbers, and symbols.
- **Avoid dictionary words** and predictable sequences.
- **Randomness increases strength**: unpredictable combinations are harder to crack.
- **Passphrases are ideal**: combining multiple unrelated words with special characters ensures memorability and strength.

---

6. Password Attacks & Impact of Complexity

- **Brute Force Attack** → Tries every possible combination. Weak passwords (like `ringarose123` can be cracked within seconds.
- **Dictionary Attack** → Uses precompiled lists of common words. Any single dictionary word (like `Password`) is vulnerable.
- **Hybrid Attack** → Combines dictionary + variations (e.g., `Password@123`). Easily defeats slightly modified common words.

Impact:

- Short/simple passwords are highly vulnerable.
- Longer, complex, and random passwords exponentially increase cracking difficulty.
- Example: `rigarose123` → cracked in seconds; `dea@$785fgCG5SN78%^J)8FRB` → estimated cracking time in **billions of years**.

---

7. Conclusion

A strong password should be:

- **At least 12–16 characters** long.
- **Include a mix** of uppercase, lowercase, numbers, and symbols.
- **Avoid dictionary words** or predictable sequences.
- **Prefer passphrases** (easy to remember, hard to crack).

By following these practices, password security is significantly improved, reducing the risk of compromise through brute force or dictionary-based attacks.

Prepared & Submitted By : Dishanyaa Shrii K M