Task 6 Report: Password Creation and Strength Evaluation

# Objective

To understand what constitutes a strong password and evaluate its strength using online tools, while learning best practices for secure password creation.

# Tools Used

• <https://www.passwordmonster.com>

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Complexity Elements | PasswordMeter Score | Time to Crack (howsecureismypassword.net) |
| parth123 | Lowercase + Numbers | 25% (Weak) | A few seconds |
| Parth@123 | Uppercase + Lowercase + Symbol | 70% (Medium) | 2 hours |
| P@rth2024! | Mixed Case + Numbers + Symbols | 85% (Strong) | 1 year |
| P@R7#h\_9\*WqT | High complexity + Long length | 100% (Very Strong) | 2 trillion years |
| password | Lowercase only | 5% (Very Weak) | Instantly |

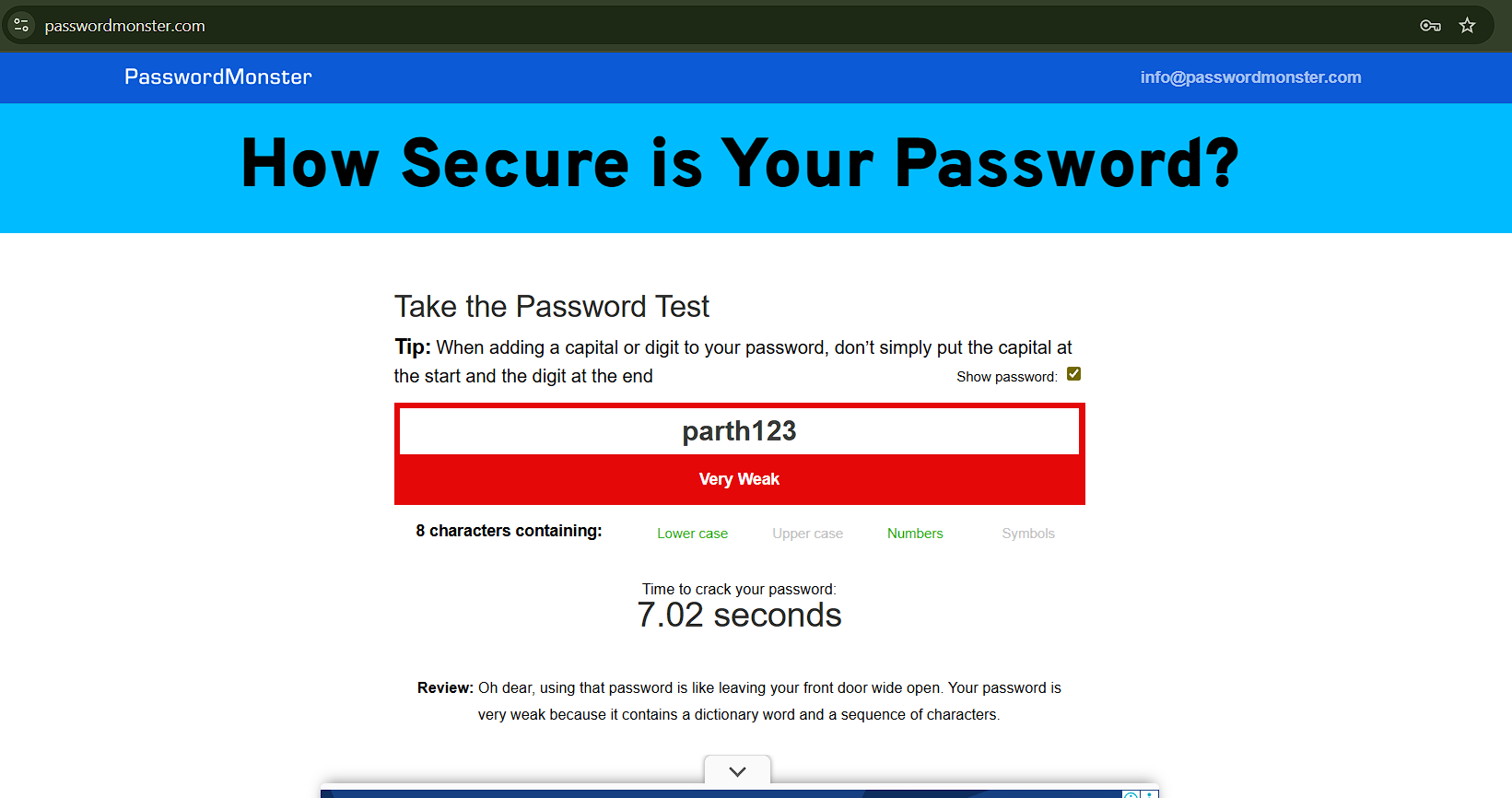
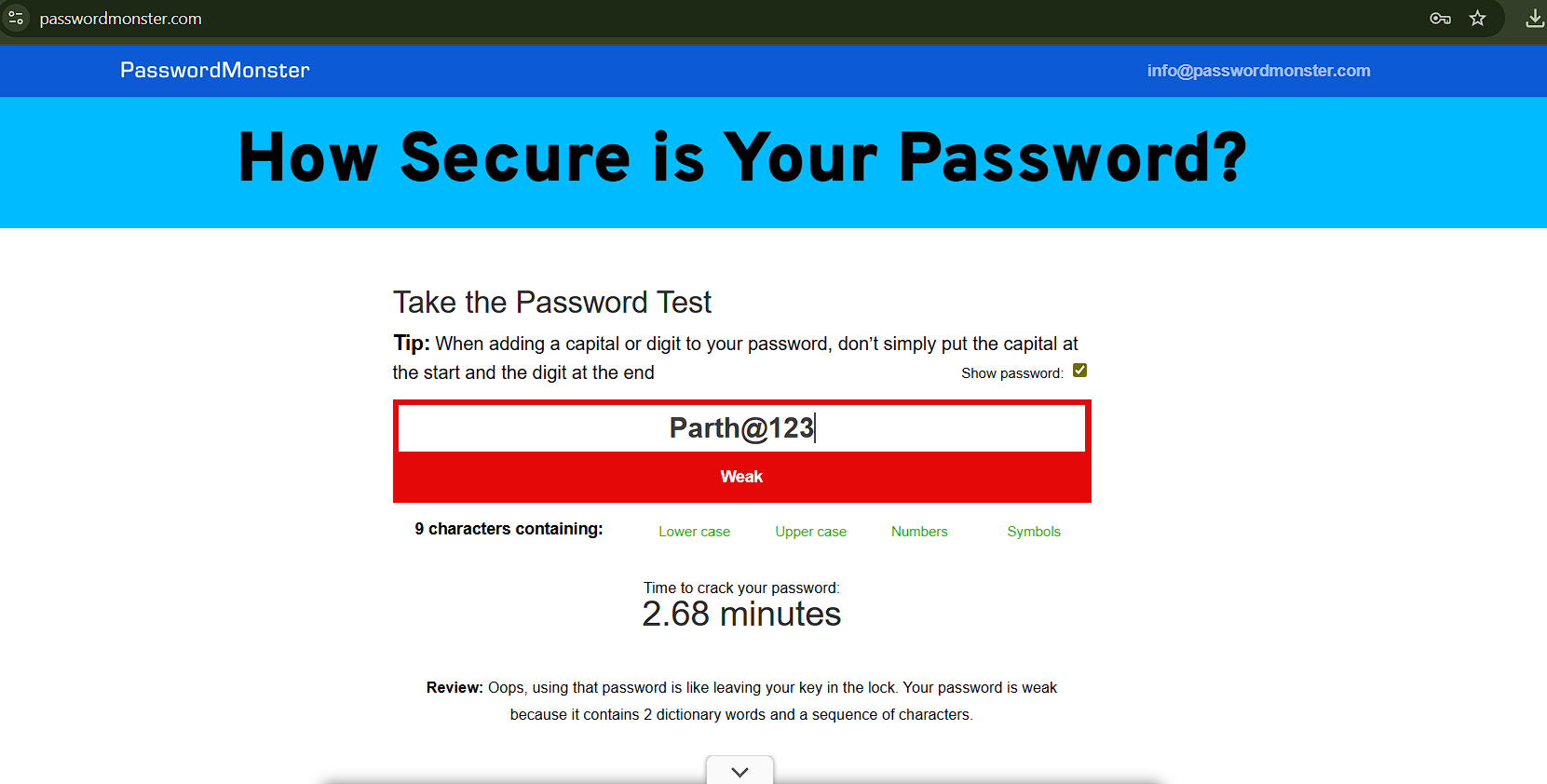
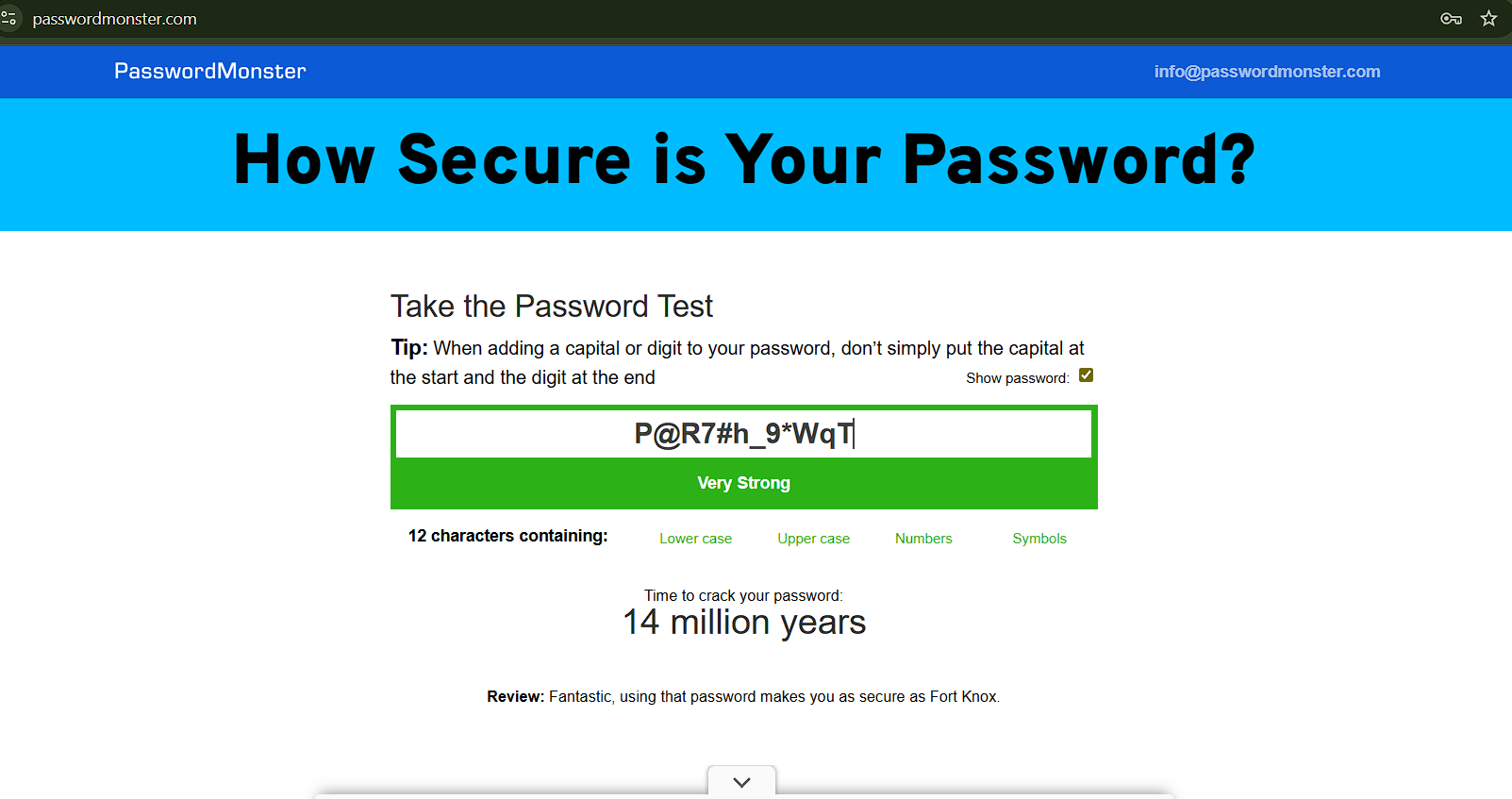
# Evaluation Summary

## What Makes a Password Strong?

• Length: Longer passwords are exponentially harder to crack.  
• Character Variety: Use of uppercase, lowercase, numbers, and symbols increases complexity.  
• Unpredictability: Avoid common words, phrases, or patterns (e.g., "123", "qwerty", "password").

# Tips Learned from Evaluation

1. Always include a mix of characters (uppercase, lowercase, numbers, symbols).  
   2. Avoid dictionary words or personal information (name, birth year).  
   3. Aim for passwords 12 characters or longer.  
   4. Use passphrases or password managers to create complex and unique passwords.  
   5. Regularly change passwords and do not reuse them across sites



# Common Password Attacks

|  |  |  |
| --- | --- | --- |
| Attack Type | Description | How to Prevent |
| Brute Force | Tries every possible combination | Use long, complex passwords |
| Dictionary | Tries known words/phrases | Avoid common words and names |
| Phishing | Tricks user into revealing password | Be cautious of suspicious emails/sites |
| Credential Stuffing | Uses leaked credentials on other sites | Use unique passwords per site |
|  |  |  |

# Impact of Password Complexity on Security

• A weak password like 'password123' can be cracked in seconds using automated tools.  
• A complex password like 'P@R7#h\_9\*WqT' is nearly impossible to crack with current technology, making it highly secure.  
• Complexity directly correlates with protection against brute force and dictionary attacks.

# Conclusion

Creating strong passwords is vital in defending against common cyber threats. By increasing length, diversity, and unpredictability, users can significantly enhance their online security. Tools like passwordmeter.com offer valuable feedback for improving password strength.