# 🔐 Password Strength Evaluation Report

## 1. Objective

The purpose of this activity is to understand what makes a password strong, test different passwords using online password strength checkers, and identify best practices for creating secure passwords.

## 2. Tools Used

- Password Strength Checker: passwordmeter.com

- Browser: (Write which browser you used, e.g., Chrome/Edge/Firefox)

## 3. Methodology

1. Created multiple passwords with different complexity levels.
2. Used variations in uppercase, lowercase, numbers, symbols, and length.
3. Tested each password on the online tool.
4. Collected feedback and strength scores.
5. Researched common password attacks (brute force, dictionary).
6. Summarized how password complexity improves security.

## 4. Test Passwords & Results

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Complexity Level | Tool Score/Feedback | Notes |
| hello123 | Low | Weak – common & short | Easy to guess, dictionary word |
| Hello123! | Medium | Fair – better but predictable | Slightly stronger |
| He!!o\_1234 | Strong | Good – includes symbols & numbers | Still short |
| Myp@ssW0rd!2025 | Very Strong | Strong – long + variety | Difficult to brute force |
| Xy#92kLm!Zp8& | Very Strong+ | Excellent – high entropy | Hard to crack |

## 5. Best Practices Identified

* Use long passwords (12+ characters).
* Mix uppercase, lowercase, numbers, and symbols.
* Avoid dictionary words or common substitutions (e.g., 'Password123').
* Use passphrases (e.g., random but memorable sentence).
* Never reuse passwords across accounts.
* Consider using a password manager.

## 6. Common Password Attacks

* Brute Force Attack: Tries all possible combinations until correct password is found.
* Dictionary Attack: Uses lists of common words/phrases to guess passwords.
* Credential Stuffing: Uses leaked passwords from other sites.

## 7. Conclusion

From the evaluation, it is clear that:  
- Password strength increases with length, randomness, and character variety.  
- Weak/simple passwords are highly vulnerable to attacks.  
- Following best practices significantly improves password security.  
  
Outcome: Gained practical understanding of password security and best practices.