PASSWORD STRENGTH EVALUATION REPORT

Cyber Security Internship – Task 6 Elevate Labs | Ministry of MSME, Government of India

Submitted by: Tayyeba Ali **Date:** 01/07/2025

1. Objective

To understand the characteristics of strong passwords, evaluate password strength using online tools, and identify best practices and vulnerabilities through testing and research.

2. Tools Used

- **PasswordMeter, Bitwarden**- for evaluating password strength
- Screenshot tool for documentation
- **GitHub**- for final report submission

3. Tested Passwords & Strength Evaluation

Password	Score (out of 100)	Estimated Time To Crack	Additions Observed	Deductions Noted	Strength Tier
`sEek@1#MnC@8p`	100	9 years	Mixed case, multiple symbols, long	Minimal deductions	**Very Strong**
`Pass@78@#12`	100	2 days	Uppercase, lowercase, numbers, symbols	Repeated symbols, minor patterning	**Strong**
`Ab@B1_66`	88	3 hours	Uppercase letters, lowercase letter, numbers, symbols, middle symbol placement, all four character types present	Repeated characters, consecutive numbers, predictable structure	**Strong**
`nIcE_GUY_1`	73	4 days	Mixed case, underscore, number	Short length, lack of middle symbols	**Moderate**
`11234ab`	48	28 seconds	Numbers, lowercase	Sequential numbers, weak length & variety	**Very Weak**

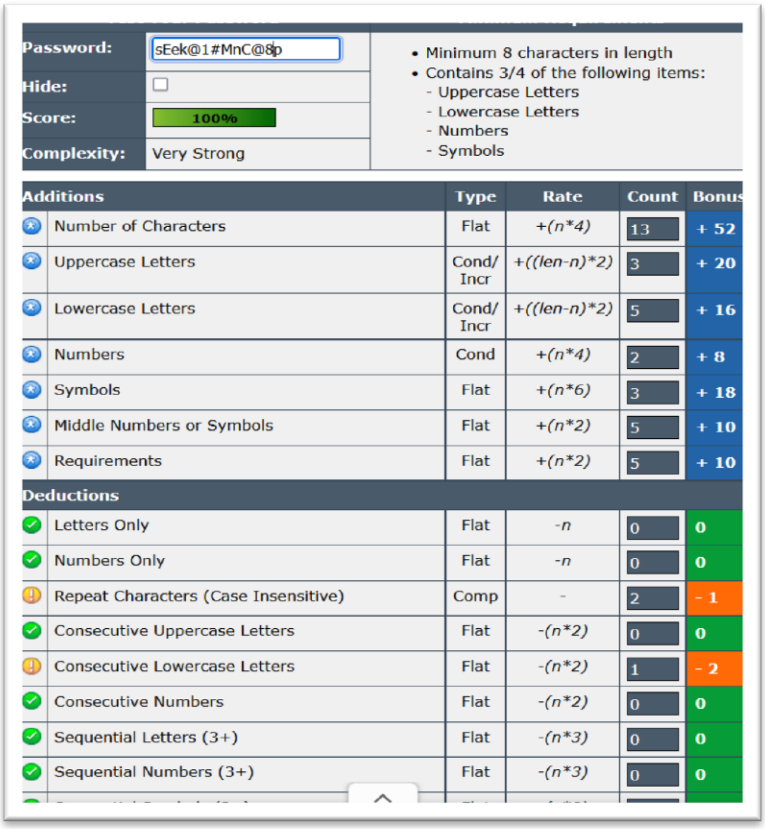
Each password was tested on both PasswordMeter, Bitwarden and evaluated based on character, variety, sequence, symbol placement, length and estimated cracking time.

4. Screenshots

Below are the evaluation results for each of the tested passwords, including screenshots from both **PasswordMeter** and **Bitwarden**.

1. **sEek@1#MnC@8p:**

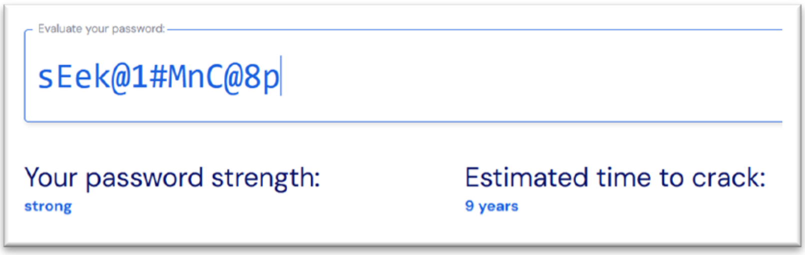
- **PasswordMeter:**



Password:	sEek@1#MnC@8p	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	100%	
Complexity:	Very Strong	

	Additions	**Type**	**Rate**	**Count**	**Bonus**
●	Number of Characters	Flat	+(n*4)	13	+ 52
●	Uppercase Letters	Cond/ Incr	+((len-n)*2)	3	+ 20
●	Lowercase Letters	Cond/ Incr	+((len-n)*2)	5	+ 16
●	Numbers	Cond	+(n*4)	2	+ 8
●	Symbols	Flat	+(n*6)	3	+ 18
●	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
●	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0

- **Bitwarden:**



Evaluate your password:

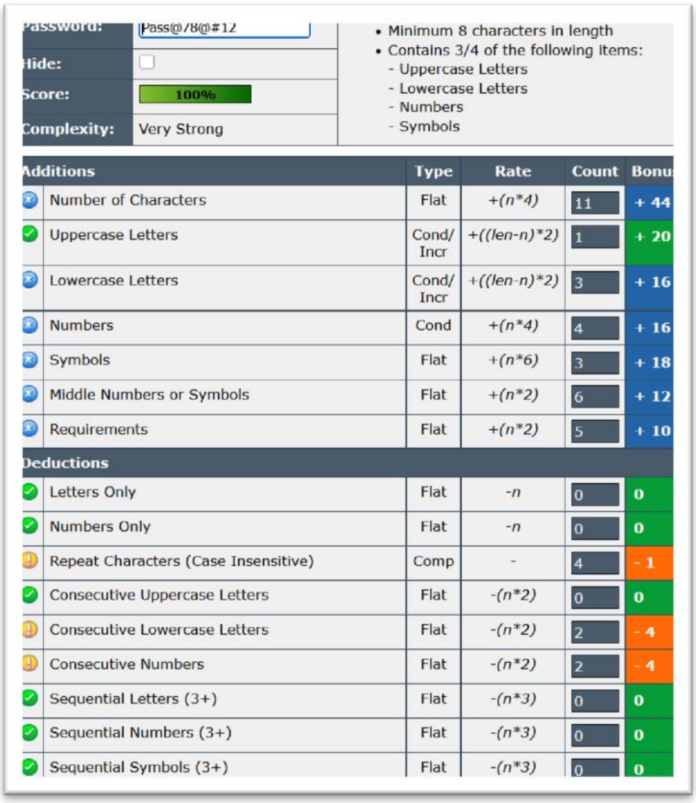
sEek@1#MnC@8p

Your password strength:
strong

Estimated time to crack:
9 years

2. **Pass@78@#12:**

- **PasswordMeter:**

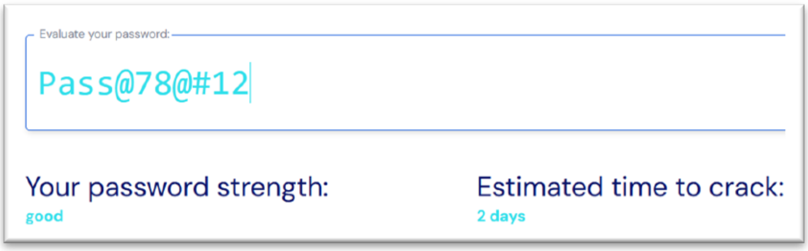


Password:	Pass@78@#12
Hide:	□
Score:	100%
Complexity:	Very Strong

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonu
●	Number of Characters	Flat	+(n*4)	11	+ 44
✓	Uppercase Letters	Cond/ Incr	+((len-n)*2)	1	+ 20
●	Lowercase Letters	Cond/ Incr	+((len-n)*2)	3	+ 16
●	Numbers	Cond	+(n*4)	4	+ 16
●	Symbols	Flat	+(n*6)	3	+ 18
●	Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
●	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
⚠	Repeat Characters (Case Insensitive)	Comp	-	4	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
⚠	Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
⚠	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

- **Bitwarden:**



Evaluate your password:

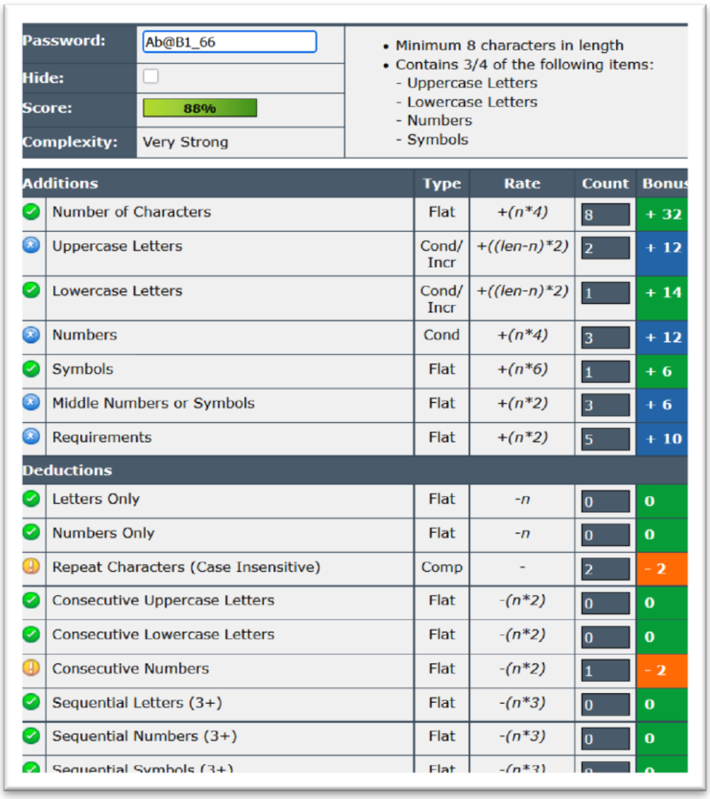
Pass@78@#12

Your password strength:
good

Estimated time to crack:
2 days

3. **Ab@B1_66:**

- **PasswordMeter:**

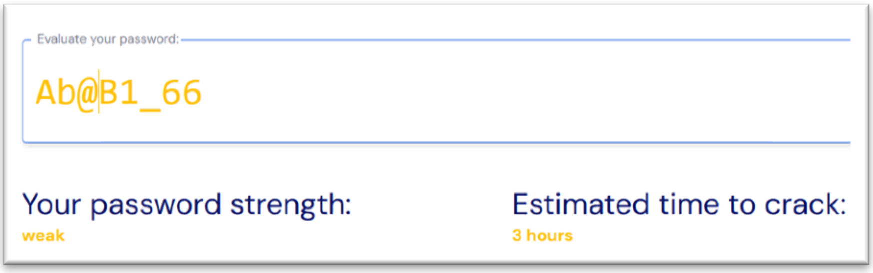


Password:	Ab@B1_66
Hide:	□
Score:	88%
Complexity:	Very Strong

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	**Type**	**Rate**	**Count**	**Bonus**
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✪	Uppercase Letters	Cond/ Incr	+((len-n)*2)	2	+ 12
✓	Lowercase Letters	Cond/ Incr	+((len-n)*2)	1	+ 14
✪	Numbers	Cond	+(n*4)	3	+ 12
✓	Symbols	Flat	+(n*6)	1	+ 6
✪	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✪	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 2
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	1	- 2
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

- **Bitwarden:**



Evaluate your password:

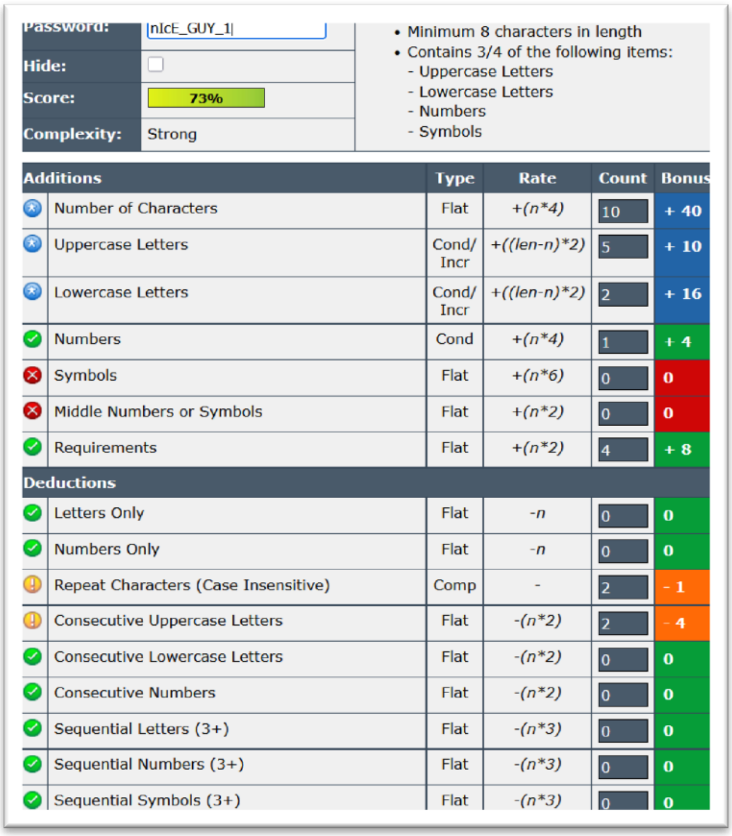
Ab@B1_66

Your password strength:
weak

Estimated time to crack:
3 hours

4. nIcE_GUY_1:

- **PasswordMeter:**

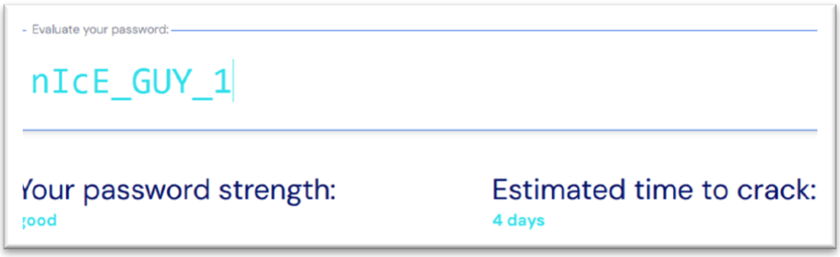


Password:	nIcE_GUY_1
Hide:	□
Score:	73%
Complexity:	Strong

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	10	+ 40
★	Uppercase Letters	Cond/ Incr	+((len-n)*2)	5	+ 10
★	Lowercase Letters	Cond/ Incr	+((len-n)*2)	2	+ 16
✓	Numbers	Cond	+(n*4)	1	+ 4
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✓	Requirements	Flat	+(n*2)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 1
!	Consecutive Uppercase Letters	Flat	-(n*2)	2	- 4
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

- **Bitwarden:**



Evaluate your password:

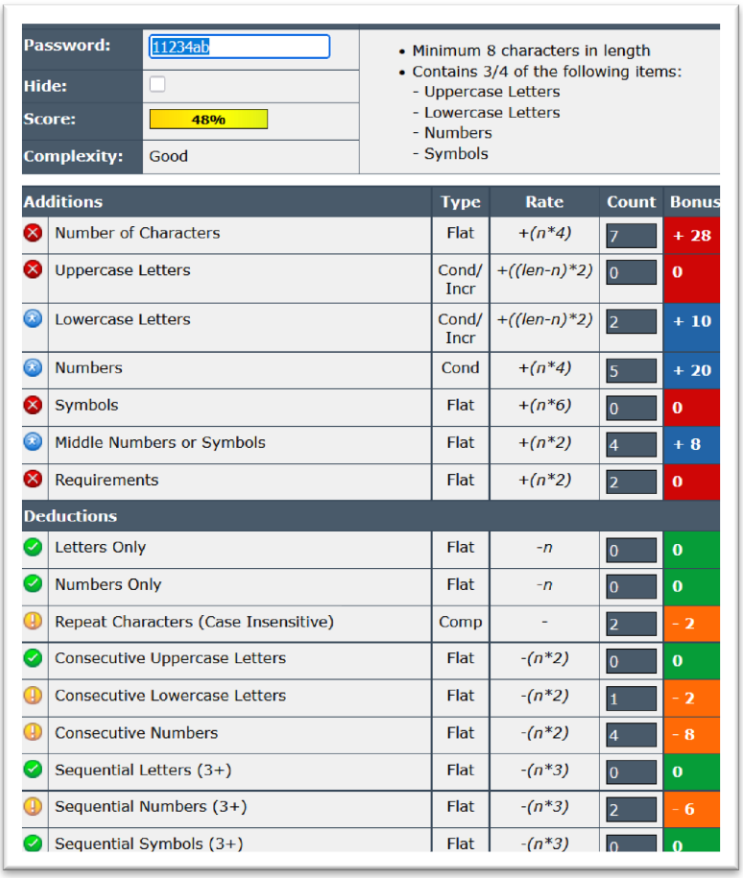
nIcE_GUY_1

Your password strength:
good

Estimated time to crack:
4 days

5. **11234ab:**

- **PasswordMeter:**

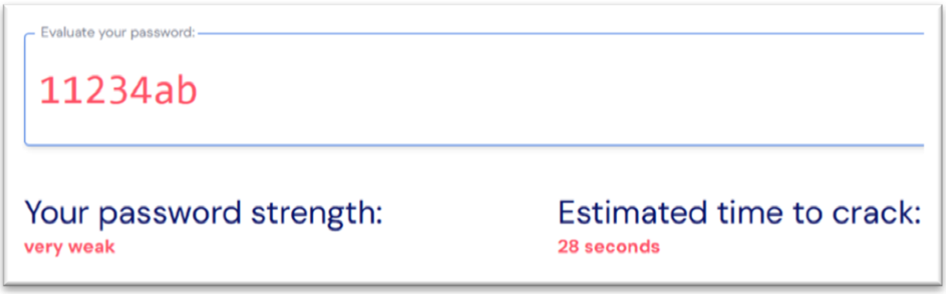


Password:	11234ab
Hide:	□
Score:	48%
Complexity:	Good

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Additions	Type	Rate	Count	Bonus
✗ Number of Characters	Flat	+(n*4)	7	+ 28
✗ Uppercase Letters	Cond/ Incr	+((len-n)*2)	0	0
★ Lowercase Letters	Cond/ Incr	+((len-n)*2)	2	+ 10
★ Numbers	Cond	+(n*4)	5	+ 20
✗ Symbols	Flat	+(n*6)	0	0
★ Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
✗ Requirements	Flat	+(n*2)	2	0
Deductions				
✓ Letters Only	Flat	-n	0	0
✓ Numbers Only	Flat	-n	0	0
! Repeat Characters (Case Insensitive)	Comp	-	2	- 2
✓ Consecutive Uppercase Letters	Flat	-(n*2)	0	0
! Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
! Consecutive Numbers	Flat	-(n*2)	4	- 8
✓ Sequential Letters (3+)	Flat	-(n*3)	0	0
! Sequential Numbers (3+)	Flat	-(n*3)	2	- 6
✓ Sequential Symbols (3+)	Flat	-(n*3)	0	0

- **Bitwarden:**



Evaluate your password:

11234ab

Your password strength:
very weak

Estimated time to crack:
28 seconds

4. Tips & Best Practices Learned

- Use **a mix of character types**- uppercase, lowercase, numbers, and symbols to increase complexity.
- **Avoid sequential patterns** like 1234 or abcd, which are easily guessed.
- **Middle placement of numbers or symbols** is more effective than placing them only at the ends.
- **Longer passwords** (10+ characters) are exponentially harder to crack, even if they look simple.
- Create **unpredictable structures**, avoid common casing-symbol-number combos (e.g., Ab@B1) that tools may recognize.
- **Repeating characters** (e.g., 66) and character type clustering lower randomness and reduce real-world strength.
- Always test passwords using **multiple tools**—PasswordMeter focuses on structural rules, while Bitwarden estimates actual time to crack based on entropy.
- **Passphrases** with unrelated words and minor complexity (e.g., Mountain@River_Planet42) are both strong and memorable.
- Don't reuse passwords, even if they're slightly modified. Credential stuffing attacks exploit variations.
- Enable **multi-factor authentication (MFA)** to add a second layer of defense.

5. Comparative Analysis: *PasswordMeter v/s Bitwarden*

During this task, I evaluated each password using two different tools: **PasswordMeter** and **Bitwarden** and noticed some key differences in how they rate password strength:

- **PasswordMeter** focuses on structural complexity. It assigns scores based on the presence of uppercase, lowercase, numbers, symbols, length, and their placement (e.g., symbols in the middle).
- **Bitwarden**, on the other hand, estimates **how long it would take to crack** the password using brute-force techniques, factoring in **entropy and randomness**.

For example, my password: *Ab@B1_66* received **88% (Very Strong)** on PasswordMeter but was rated **Weak (3 hours to crack)** on Bitwarden. This revealed that while the password met structural rules (variety and pattern), it lacked enough **unpredictability** to resist real-world attacks.

Key Insight: Scoring high on a rule-based tool doesn't always mean a password is secure. It's equally important to consider entropy and crack time when evaluating real-world strength.

Using both tools side-by-side gave me a better understanding of what truly makes a password resilient- **not just variety, but unpredictability and non-patterned structure**.

6. Common Password Attacks

- **Brute Force Attack**: This method involves trying all possible combinations of characters until the correct password is found. The shorter and simpler the password, the quicker it is to crack. For example, an 8-character password using only lowercase letters can be broken in seconds.
- **Dictionary Attack:** This technique uses a predefined list of common passwords or real words like *password123* or *qwerty* to guess login credentials. Passwords that resemble dictionary words or follow common patterns are especially vulnerable.

Both these methods are automated and rely heavily on predictable or weak password structures, which is why length, variety, and randomness are critical to defense.

7. Conclusion

This task clearly showed me how crucial password complexity is in protecting against common attack methods. Strong passwords aren't just about meeting character requirements, they also need to be unpredictable and free from patterns. The more complex and random a password is, the longer it takes to crack with brute-force or dictionary-based tools. Length, mixed character types, and entropy all play a vital role in strengthening password security.

By testing my passwords on multiple platforms and evaluating real-world cracking estimates, I've gained a deeper understanding of how attackers operate—and how to build defenses that hold up against them.