Task 6: Strong Password Creation and Evaluation

1. Objective

The aim of this task was to create multiple passwords of varying complexity, test their strength using an online password checker, analyse the results, and identify best practices for creating strong passwords.

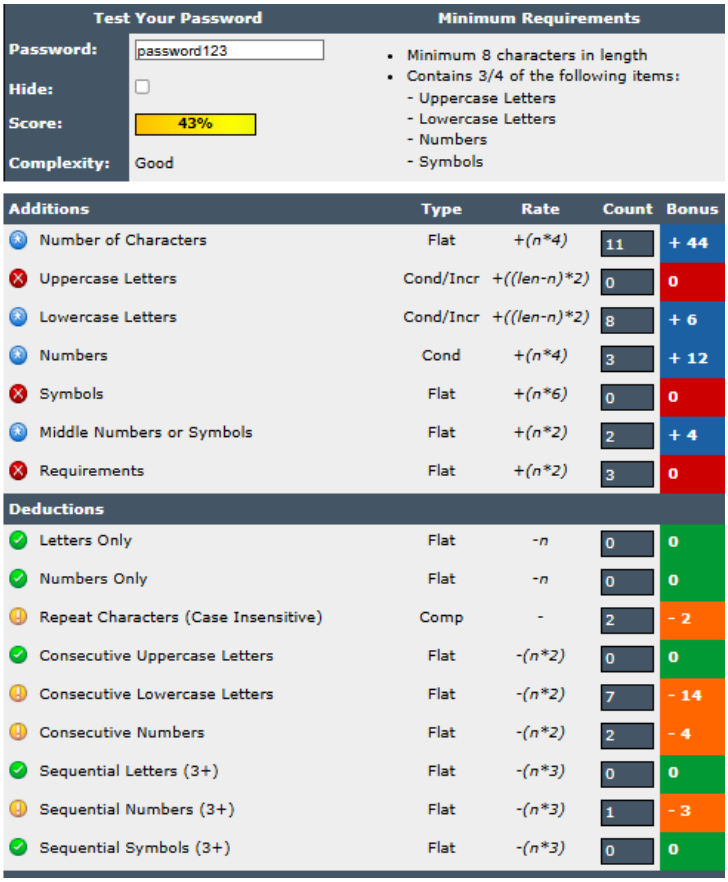
2. Tools Used

- Password strength checker:
  - https://passwordmeter.com
  - https://bitwarden.com/password-strength/
- Word document for recording results and notes
- Screenshot tool (Snipping Tool) for capturing test results

3. Passwords Created for Testing

A set of five passwords was created with varying levels of complexity to test their strength:

1. password123 - common word with numbers; weak.



Test Your Password		Minimum Requirements
Password:	password123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	43%	
Complexity:	Good	

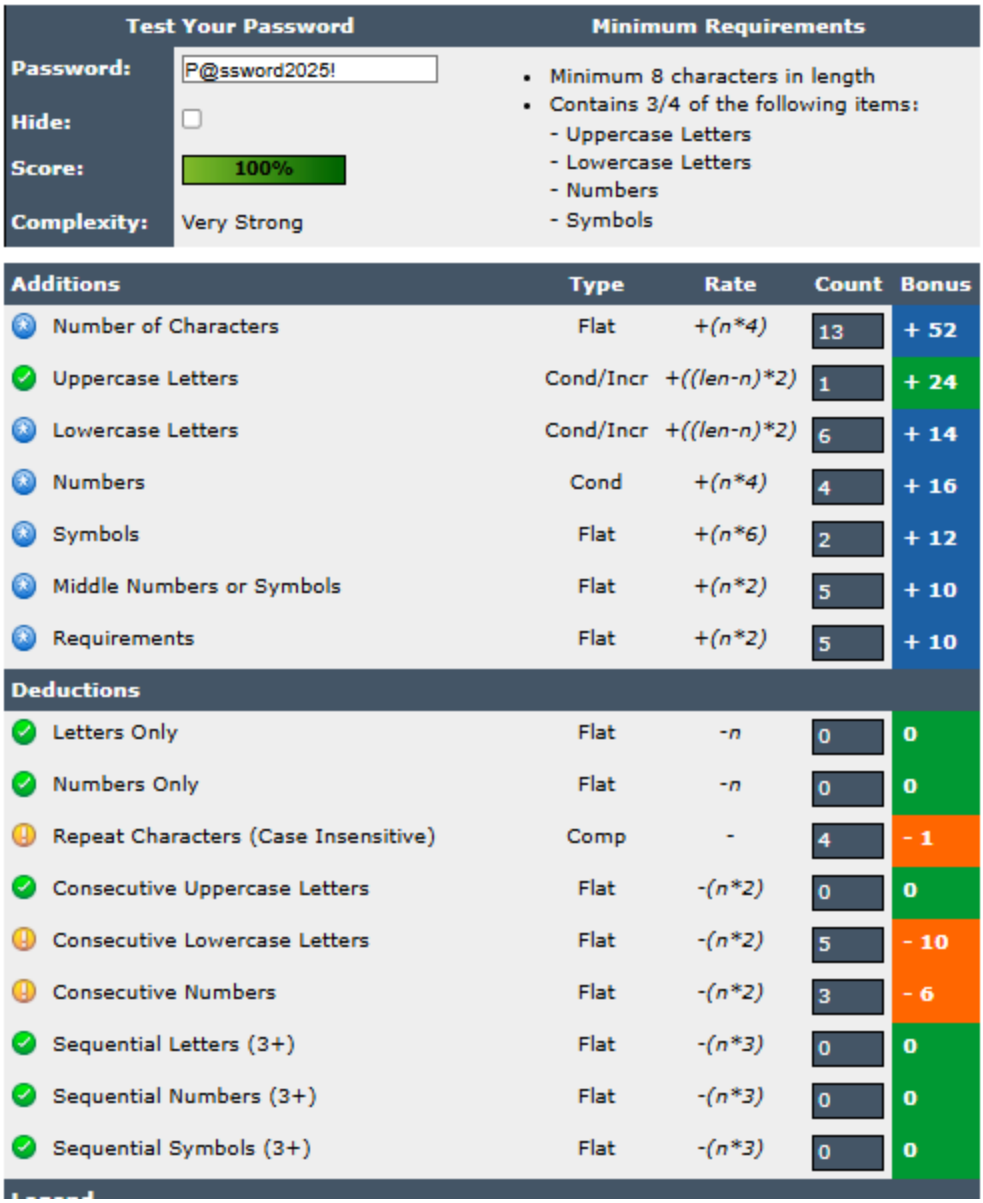
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	11	+ 44
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 6
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	3	0
Deductions				
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)	7	- 14
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

2. 123456 - short numeric only; very weak.

Test Your Password		Minimum Requirements
Password:	123456	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	4%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	6	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	1	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	6	- 6
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	5	- 10
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	4	- 12
Sequential Symbols (3+)	Flat	-(n*3)	0	0

3. P@ssword2025! - mix of uppercase, lowercase, numbers, and symbols; medium strong.



Test Your Password		Minimum Requirements
Password:	P@ssword2025!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

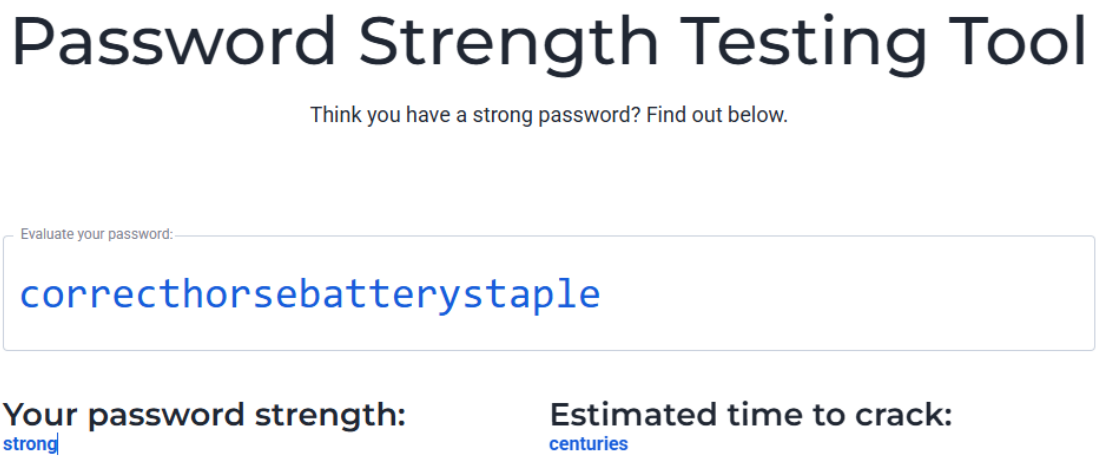
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	13	+ 52
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 14
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
Consecutive Numbers	Flat	-(n*2)	3	- 6
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

4. Th!sIsAStr0ngP@ssw0rd! - long, highly complex, mixed characters; very strong.

Test Your Password		Minimum Requirements
Password:	Th!sIsAStr0ngP@ssw0rd!	• 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)	22	+ 88
Uppercase Letters	Cond/Incr	+((len-n)*2)	5	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	12	+ 20
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	10	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	1	- 2
Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
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
Legend				

5. correcthorsebatterystaple - long passphrase of unrelated words; strong and memorable.



4. Password Strength Testing Results

Each password was tested using an online password strength checker. The table below shows scores, and feedback provided.

Password	Score	Feedback
password123	**43%**	Common, predictable; insufficient complexity.
123456	**4%**	Very short, numbers only; widely used and easy to guess.
P@ssword2025!	**100%**	Strong mix of character types; resistant to simple attacks.
Th!sIsAStr0ngP@ssw0rd!	**100%**	Long, diverse characters; highly resistant to brute force.
correcthorsebatterystaple	**100%**	Long passphrase; strong but may be vulnerable to dictionary phrases.

5. Best Practices for Strong Passwords

- Use **at least 12 characters** (longer is better).
- Combine **uppercase letters**, **lowercase letters**, **numbers**, and **symbols**.
- Avoid common words, keyboard patterns, and predictable sequences.
- Don't just replace letters with common substitutions (e.g., P@ssw0rd).
- Consider a **passphrase** of multiple unrelated words for memorability and strength.
- Use a **password manager** to store unique passwords for each account.

6. Common Password Attacks and How Strong Passwords Help

- **Brute Force Attack** - tries all possible combinations; strong, long passwords make this process take an impractically long time.
- **Dictionary Attack** - uses lists of common/stolen passwords; random, unique passwords prevent success.
- **Credential Stuffing** - tests leaked credentials on other sites; using unique passwords for each account stops it.
- **Rainbow Table Attack** - uses precomputed hash lists; complex passwords and salted hashes reduce effectiveness.

7. Conclusion

This task confirmed that password strength is influenced primarily by **length**, **character diversity**, and **randomness**. Weak passwords, especially short or common ones, can be guessed quickly by attackers. Strong, unique passwords significantly reduce the likelihood of successful compromise, especially when paired with good account security practices.