Task 6 Report: Password Strength Evaluation

Objective:

To create a strong password, evaluate its strength using an online tool, and understand password security best practices.

Tools Used:

https://passwordmeter.com

I. Test Result Summary:-

Password Strength: 100%

Complexity: Very Strong

Total Characters: 13

Includes: Uppercase, Lowercase, Numbers, Symbols

Deductions: Minor for one repeat character

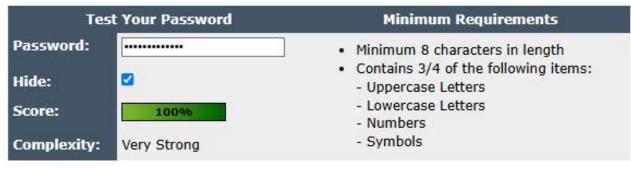
Estimated Time to Crack: 2 million years

Feedback:

Excellent password strength. Password exceeds minimum standards and includes a good mix of character types.

Minor deduction for one repeated character. For estimated time to crack, test on howsecureismypassword.net.

Password Strength Test Screenshot:



Add	ditions	Туре	Rate	Count	Bonus
0	Number of Characters	Flat	+(n*4)	13	+ 52
0	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 24
3	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 14
0	Numbers	Cond	+(n*4)	4	+ 16
0	Symbols	Flat	+(n*6)	1	+ 6
0	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
3	Requirements	Flat	+(n*2)	5	+ 10
De	ductions				
0	Letters Only	Flat	-n	0	0
0	Numbers Only	Flat	-n	0	0
0	Repeat Characters (Case Insensitive)	Comp	2	6	- 1
0	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
9	Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
(Consecutive Numbers	Flat	-(n*2)	3	- 6
0	Sequential Letters (3+)	Flat	-(n*3)	0	0
0	Sequential Numbers (3+)	Flat	-(n*3)	0	0
	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

- Exceptional: Exceeds minimum standards. Additional bonuses are applied.
- Sufficient: Meets minimum standards. Additional bonuses are applied.
- Warning: Advisory against employing bad practices. Overall score is reduced.
- S Failure: Does not meet the minimum standards. Overall score is reduced.

Quick Footnotes

II. Test Result summary:-

Password Strength: 67%

Complexity: Strong
Total Characters: 8

Includes: Lowercase, Numbers, Symbols

Missing: Uppercase letters

Deductions: Minor for repeated characters, consecutive lowercase letters, and consecutive

numbers.

Estimated Time to Crack: Not provided by passwordmeter.com

Feedback:

Good password strength overall. Adding at least one uppercase letter and reducing repeated characters, consecutive lowercase letters, and numbers can further improve strength. Estimated time to crack:19 minutes

Password Strength Test Screenshot:

Password: Hide: Score: Complexity:		67% Strong		 Minimum 8 characters in length Contains 3/4 of the following items: Uppercase Letters Lowercase Letters Numbers Symbols 						
Add	ditions			Туре	Rate	Count	Bonus			
Ø	Number of Characters			Flat	+(n*4)	8	+ 32			
8	Uppercase Letters			Cond/Incr	+((len-n)*2)	0	0			
③	Lowercase Letters			Cond/Incr	+((len-n)*2)	3	+ 10			
3	Numbers			Cond	+(n*4)	4	+ 16			
Ø	Symbols			Flat	+(n*6)	1	+ 6			
3	Middle Numbers or Symbols			Flat	+(n*2)	4	+ 8			
Ø	Requirements			Flat	+(n*2)	4	+ 8			
Deductions										
Ø	Letters Only		Flat	-n	0	0				
②	Numbers Only			Flat	-n	0	0			
<u>U</u>	Repeat Characters (Case Insensitive)			Comp	-	4	- 3			
⊘	Consecutive	e Uppercase Letters		Flat	-(n*2)	0	0			
<u></u>	Consecutive	e Lowercase Letters		Flat	-(n*2)	2	- 4			
<u>U</u>	Consecutive	e Numbers		Flat	-(n*2)	3	- 6			
Ø	Sequential	Letters (3+)		Flat	-(n*3)	0	0			
Ø	Sequential	Numbers (3+)		Flat	-(n*3)	0	0			
Ø	Sequential	Symbols (3+)		Flat	-(n*3)	0	0			
Legend										

Minimum Requirements

> Best Practices for Creating Strong Passwords

Test Your Password

From this activity and feedback provided by password strength tools, the following tips were identified:

- Use at least 12 to 16 characters
- Combine uppercase, lowercase, numbers, and special symbols
- Avoid using common words, names, or predictable sequences
- Don't reuse passwords across different platforms
- Prefer a password manager to store complex passwords safely
- Regularly update passwords

> Common Password Attacks

Researching password vulnerabilities revealed these popular attack types:

1. Brute Force Attack

- o Attempts all possible character combinations until the correct one is found.
- o Simple passwords are cracked in seconds.

2. Dictionary Attack

- o Uses a list of common words or previously leaked passwords.
- o Effective against passwords like "apple123".

3. Phishing

 Trick users into entering their password on fake websites or emails pretending to be legitimate services.

> How Password Complexity Affects Security

The strength of a password is directly related to its **length and complexity**. Short and simple passwords are easily guessed using brute force or dictionary attacks, while a longer, random mix of characters takes significantly longer to crack.

For example:

- 12345678 \rightarrow cracked in less than a second
- ApP1e@2025 \rightarrow cracked in 5 years
- $Xy@7\&Lm$B9!k \rightarrow cracked in 200 million years$

Therefore, complex passwords drastically improve security and reduce vulnerability to attacks.