Task 4: Create a Strong Password and Evaluate Its Strength

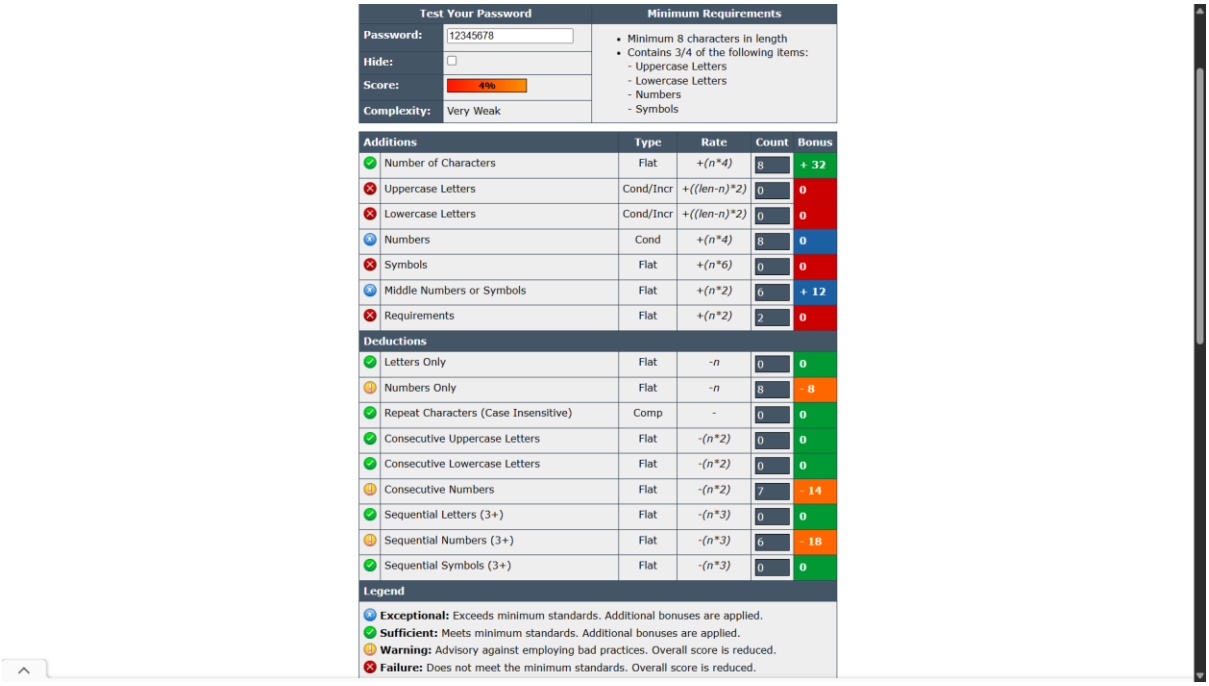
Objective: Understand what makes a password strong and test it against password strength tools.

Before we Directly Dive into Checking Passwords Strength lets understand how creating a complex password helps us being secure in this Digital World.
Let first Understand how passwords are Hacked and how creating a complex password can actually help us to stay secure.
To understand that we need to know what does a hacker does to get the Password.
Following is some of the Common Password Attacks which a Hacker Can Try:

Attack Type	Description	How Complexity Helps
Brute Force	Tries all possible combinations.	Longer and more complex passwords take significantly more time to crack.
Dictionary Attack	Uses lists of common words/passwords.	Random and complex passwords avoid matches in dictionary files.
Credential Stuffing	Reuses known breached passwords across multiple accounts.	Unique passwords for each site mitigate this risk.
Social Engineering	Tricks users into revealing passwords.	Not directly affected by complexity, but avoid personal info.

Now We know How Complexity Works Lets Check out How we Can Increase Complexity.

First Let's Start with very Common Password which can be brute forced in seconds.



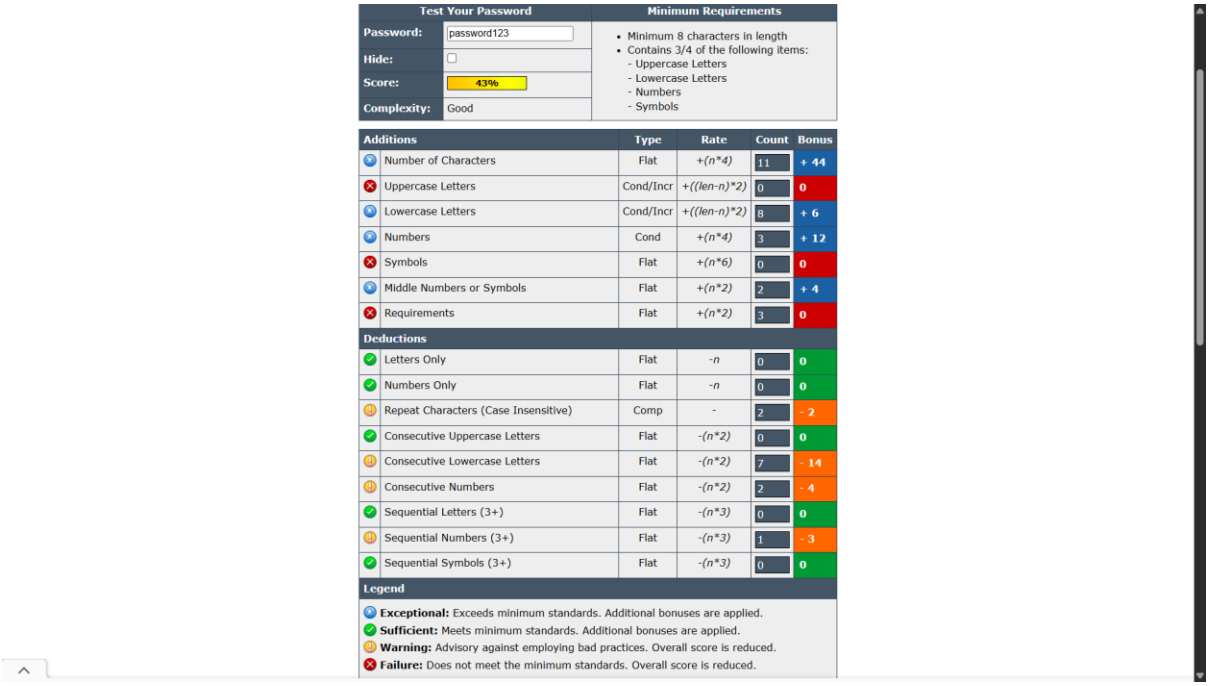
Test Your Password		Minimum Requirements
Password:	12345678	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	4%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	8	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
Requirements	Flat	+(n*2)	2	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	8	- 8
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)	7	- 14
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	6	- 18
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.
Failure: Does not meet the minimum standards. Overall score is reduced.

Now let's try a longer version of This:



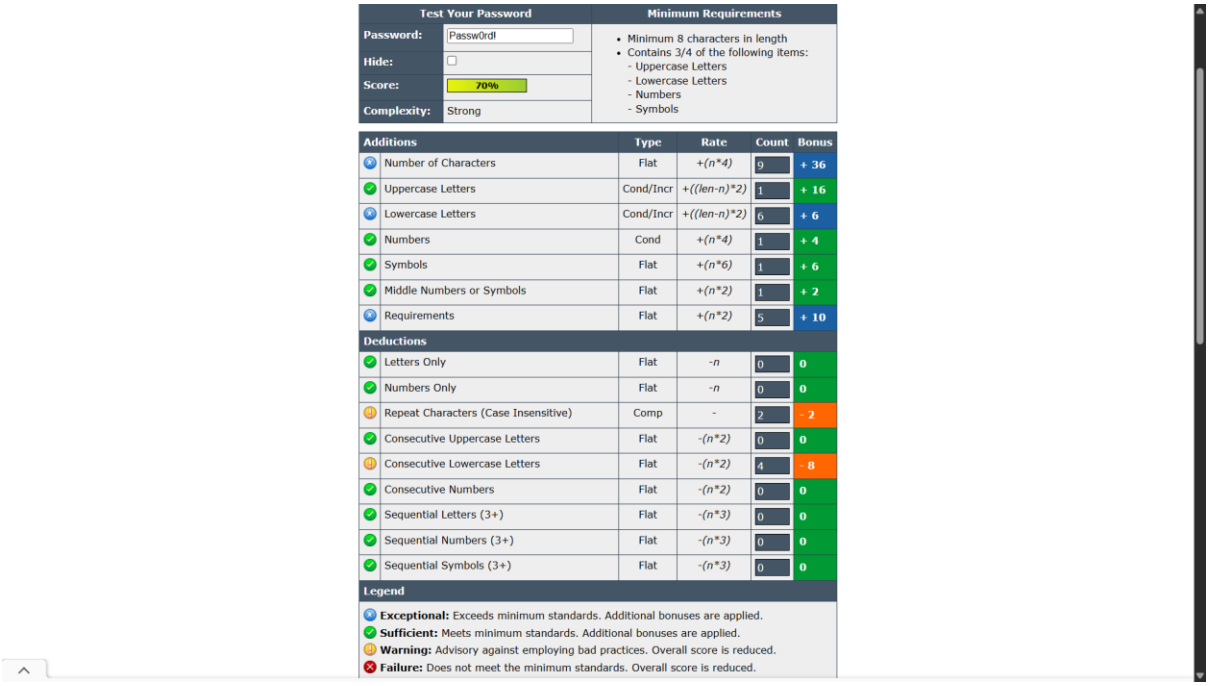
Test Your Password		Minimum Requirements
Password:	password123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	43%	
Complexity:	Good	

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

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.
Failure: Does not meet the minimum standards. Overall score is reduced.

Now let’s try to add a special character in there:



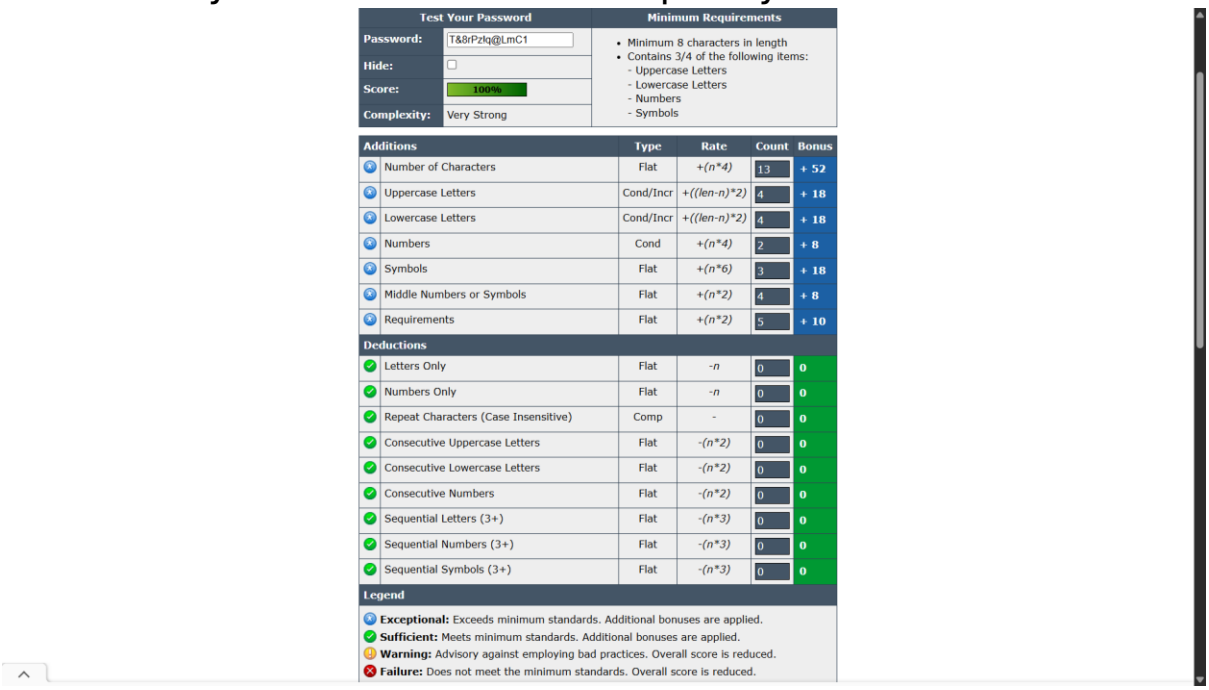
Test Your Password		Minimum Requirements
Password:	Passw0rd!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	70%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 6
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
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)	4	- 8
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

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.
Failure: Does not meet the minimum standards. Overall score is reduced.

Now let’s try to add some more complexity:



Test Your Password		Minimum Requirements
Password:	T&8rPzkq@LmC1	• 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)	4	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 18
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	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
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

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.
Failure: Does not meet the minimum standards. Overall score is reduced.

Let’s try to Evaluate the Result:

Password	Strength	Feedback
12345678	4%	Very Weak: Easily guessable

Password123	43%	Too common: lacks symbols, predictable
Passw0rd!	70%	Moderate: weak length, common pattern
T&8rPz!q@LmC1	100%	Very Strong: high entropy and length

What we Learn from this:

- **Longer passwords** (12+ characters) are exponentially stronger.
- **Mix character types**: Include upper & lower case letters, numbers, and symbols.
- **Avoid dictionary words** or common substitutions (e.g., P@ssw0rd is still predictable).
- **Avoid reused passwords**: Use a password manager to store complex passwords.
- **Avoid sequences and patterns** (e.g., 123456, qwerty, abcdef).

Conclusion

A strong password is:

- At least **12–16 characters** long
- Contains **uppercase, lowercase, numbers, and symbols**
- **Avoids dictionary words**, personal info, or predictable patterns

Best Example:

T&8rPz!q@LmC1 — Rated 100% strength. Balanced length, randomness, and character diversity.