Task 6: Create a Strong Password and Evaluate Its Strength.

1. **Create multiple passwords with varying complexity.**

For this task, we will create five different passwords with varying degrees of complexity. Each password will use different techniques to test how its strength can be affected by length, complexity, and randomness.

Password 1: Weak Password (Low Complexity)

A weak password is easy to guess and often used by people who want something simple to remember. However, it is vulnerable to common attacks.

- **Password**: password123

Password 2: Medium Complexity

This password has some improvements by adding a special character and a number. It's harder to guess but still fairly common and vulnerable to attacks.

- **Password**: Secure1$@

Password 3: High Complexity

This password is much stronger as it contains a mixture of uppercase, lowercase, numbers, and special characters. However, it's still not fully random.

- **Password**: !M3ssyF@nt@stic#12

Password 4: Very Complex

This password is much longer and incorporates a mix of everything, including symbols, numbers, uppercase letters, and lowercase letters. The additional length significantly improves the password's security.

- **Password**: #M$18cPz!_B3xL1qX8

Password 5: Extremely Complex (Highly Secure)

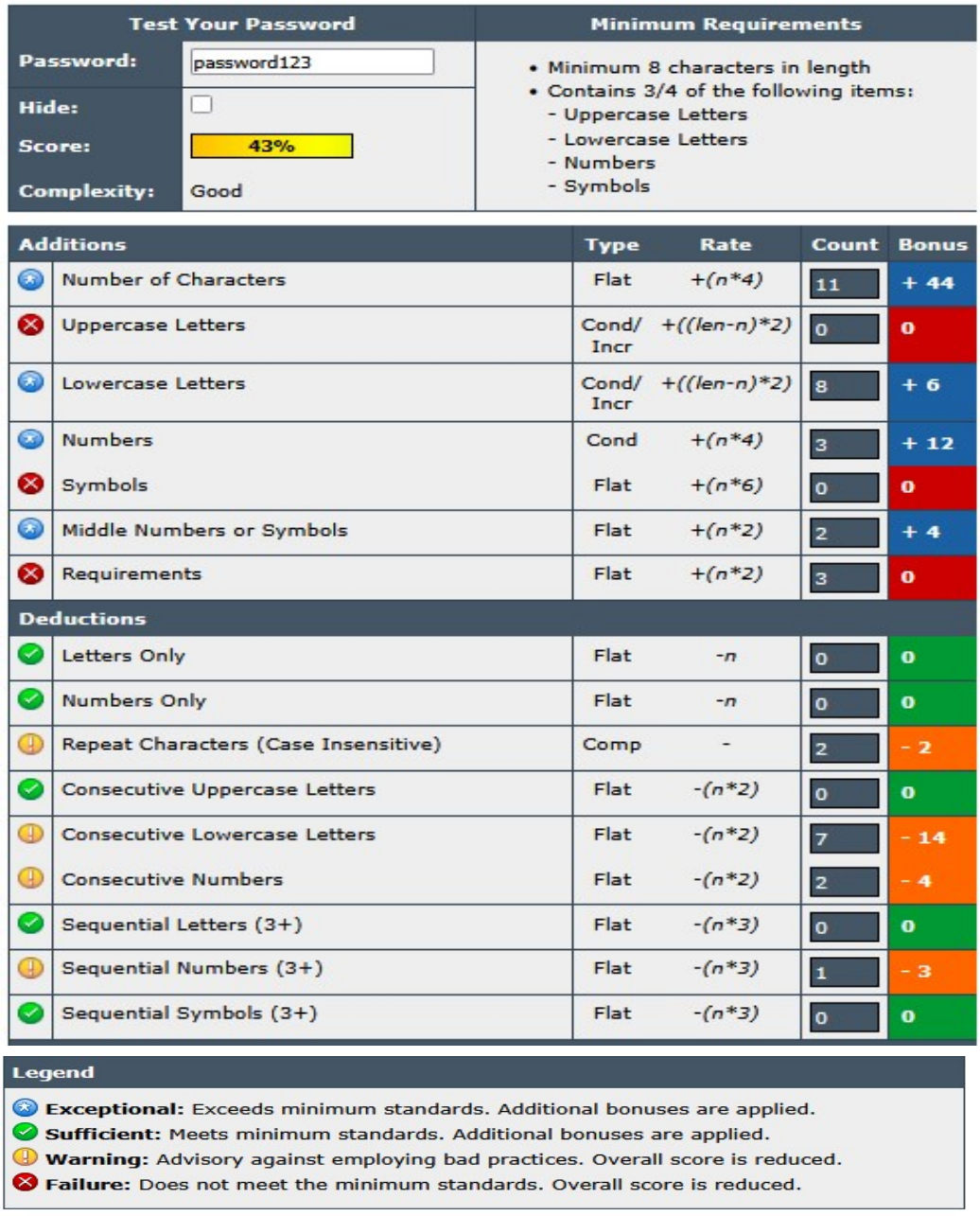
This is the most secure password, combining length, randomness, and diversity of character types, making it difficult for brute force or dictionary attacks to succeed.

- **Password**: h8@j6T&lU3w@zP0b3m#u1Rf!

2. **Testing each password on password strength checker with scores and feedback from the tool (passwordmeter.com).**

Password 1: password123

- **Score**: 43/100
- **Feedback**: This password is weak and should be avoided. It is vulnerable to brute force attacks and dictionary attacks. Try making the password longer and using a mix of characters.



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	

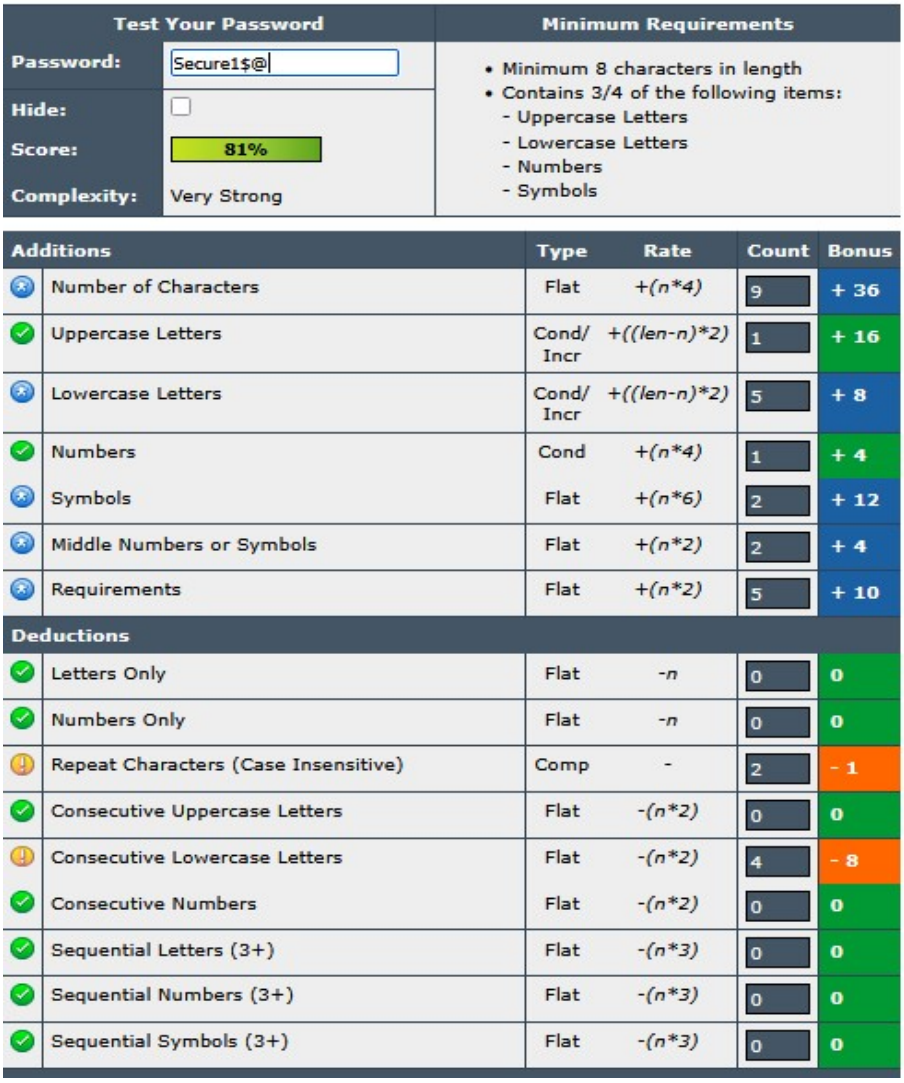
Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	11	+ 44
✗	Uppercase Letters	Cond/ Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/ Incr	+((len-n)*2)	8	+ 6
✓	Numbers	Cond	+(n*4)	3	+ 12
✗	Symbols	Flat	+(n*6)	0	0
✓	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✗	Requirements	Flat	+(n*2)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

Password 2: Secure1$@

- **Score**: 81/100
- **Feedback**: This is a medium-to-strong password. It uses uppercase and lowercase letters, numbers, and special characters, which is great. However, it could be stronger if it were longer or more random. It’s still vulnerable to dictionary attacks because "secure" is a commonly used word.



Test Your Password		Minimum Requirements
Password:	Secure1$@	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	81%	
Complexity:	Very Strong	

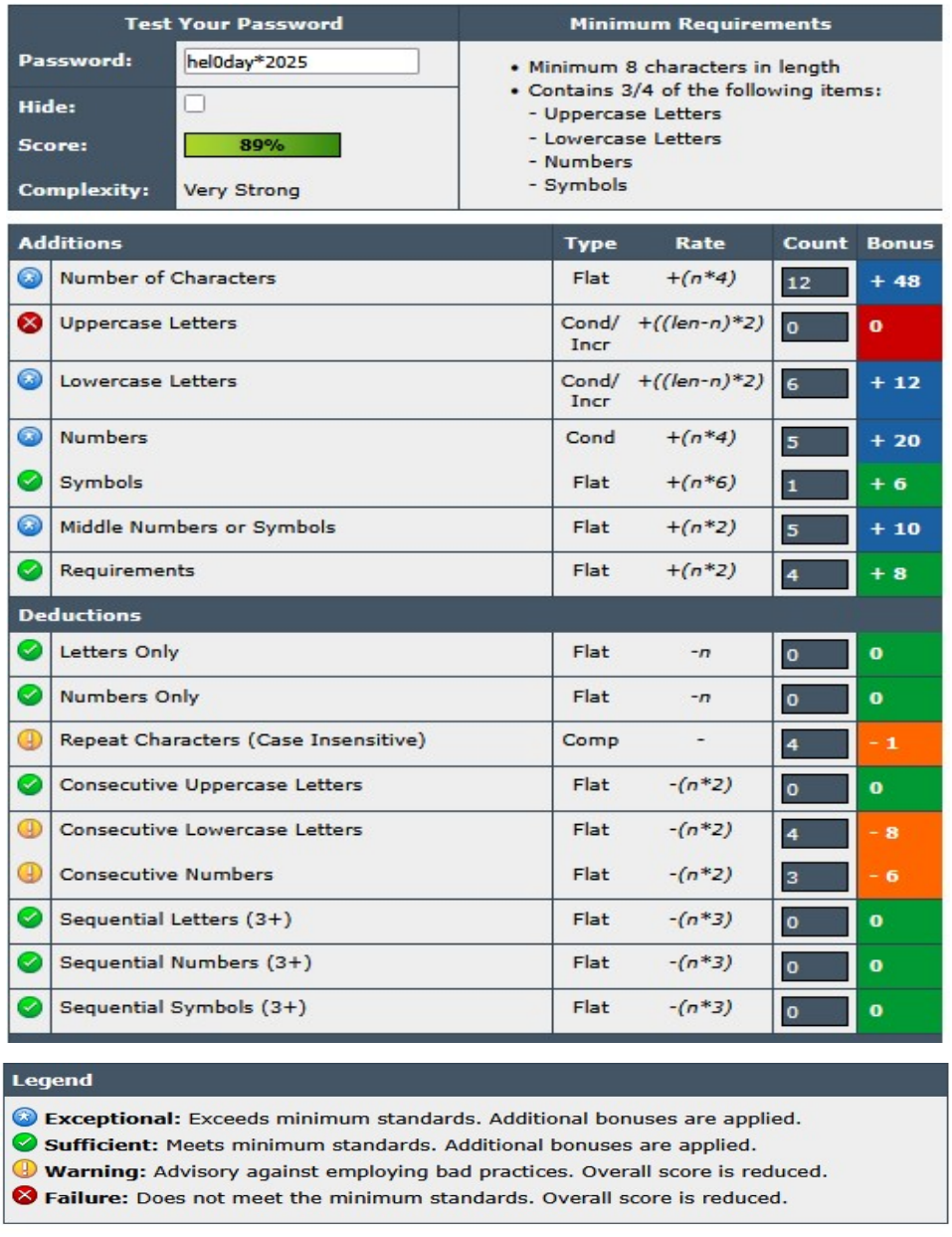
Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	9	+ 36
✓	Uppercase Letters	Cond/ Incr	+((len-n)*2)	1	+ 16
✓	Lowercase Letters	Cond/ Incr	+((len-n)*2)	5	+ 8
✓	Numbers	Cond	+(n*4)	1	+ 4
✓	Symbols	Flat	+(n*6)	2	+ 12
✓	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✓	Requirements	Flat	+(n*2)	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)	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.

Password 3: hel0day*2025

- **Score**: 89/100
- **Feedback**: This password is stronger than the first two because it includes a mix of numbers, letters, and a special character. However, the word "day" is still a common word, which lowers the score slightly. Despite this, it's significantly stronger than a simple word-based password. This would be harder to crack than password123 than but not as strong as the more complex ones.



Test Your Password		Minimum Requirements
Password:	hel0day*2025	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	89%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
⊛	Number of Characters	Flat	+(n*4)	12	+ 48
✗	Uppercase Letters	Cond/ Incr	+((len-n)*2)	0	0
⊛	Lowercase Letters	Cond/ Incr	+((len-n)*2)	6	+ 12
⊛	Numbers	Cond	+(n*4)	5	+ 20
✓	Symbols	Flat	+(n*6)	1	+ 6
⊛	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
✓	Requirements	Flat	+(n*2)	4	+ 8
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)	4	- 8
!	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

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.

Password 4: b3@ut1fUlk3y#078,^4!

- **Score**: 100/100
- **Feedback**: b3@ut1fUlk3y#078,^4! is a strong password with a solid mix of uppercase, lowercase, numbers, and special characters. However, the use of a modified version of "beautifulkey" still makes it somewhat vulnerable to dictionary or pattern-based attacks—increasing randomness would further enhance its strength.

Test Your Password		Minimum Requirements
Password:	b3@ut1fUlk3y#078,^4!	• 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)	20	+ 80
✓	Uppercase Letters	Cond/ Incr	+((len-n)*2)	1	+ 38
✓	Lowercase Letters	Cond/ Incr	+((len-n)*2)	7	+ 26
✓	Numbers	Cond	+(n*4)	7	+ 28
✓	Symbols	Flat	+(n*6)	5	+ 30
✓	Middle Numbers or Symbols	Flat	+(n*2)	11	+ 22
✓	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)	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

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.

Password 5: P#7zL8m@D2w5X!r9Q

- **Score**: 100/100
- **Feedback:** P#7zL8m@D2w5X!r9Q is highly secure due to its randomness, length, and the lack of predictable patterns or dictionary words. It's resistant to both dictionary attacks and brute-force methods.

Test Your Password		Minimum Requirements
Password:	P#7zL8m@D2w5X!r9Q	• 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)	17	+ 68
✓	Uppercase Letters	Cond/ Incr	+((len-n)*2)	5	+ 24
✓	Lowercase Letters	Cond/ Incr	+((len-n)*2)	4	+ 26
✓	Numbers	Cond	+(n*4)	5	+ 20
✓	Symbols	Flat	+(n*6)	3	+ 18
✓	Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
✓	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.