Password Creation and Evaluation

Task Name: Task 6 – Create and Evaluate Strong Passwords

Tools Used: passwordmeter.com, security.org password checker, online password generator

Passwords Tested: 4 (simple, moderate, strong, very strong)

OBJECTIVE

The aim of this task was to understand how to create strong passwords and evaluate their strength using online tools. It focused on identifying what makes a password secure and how various attack methods can exploit weak ones.

1. Creating Passwords with Varying Complexity

I started by creating several example passwords with different levels of complexity:-

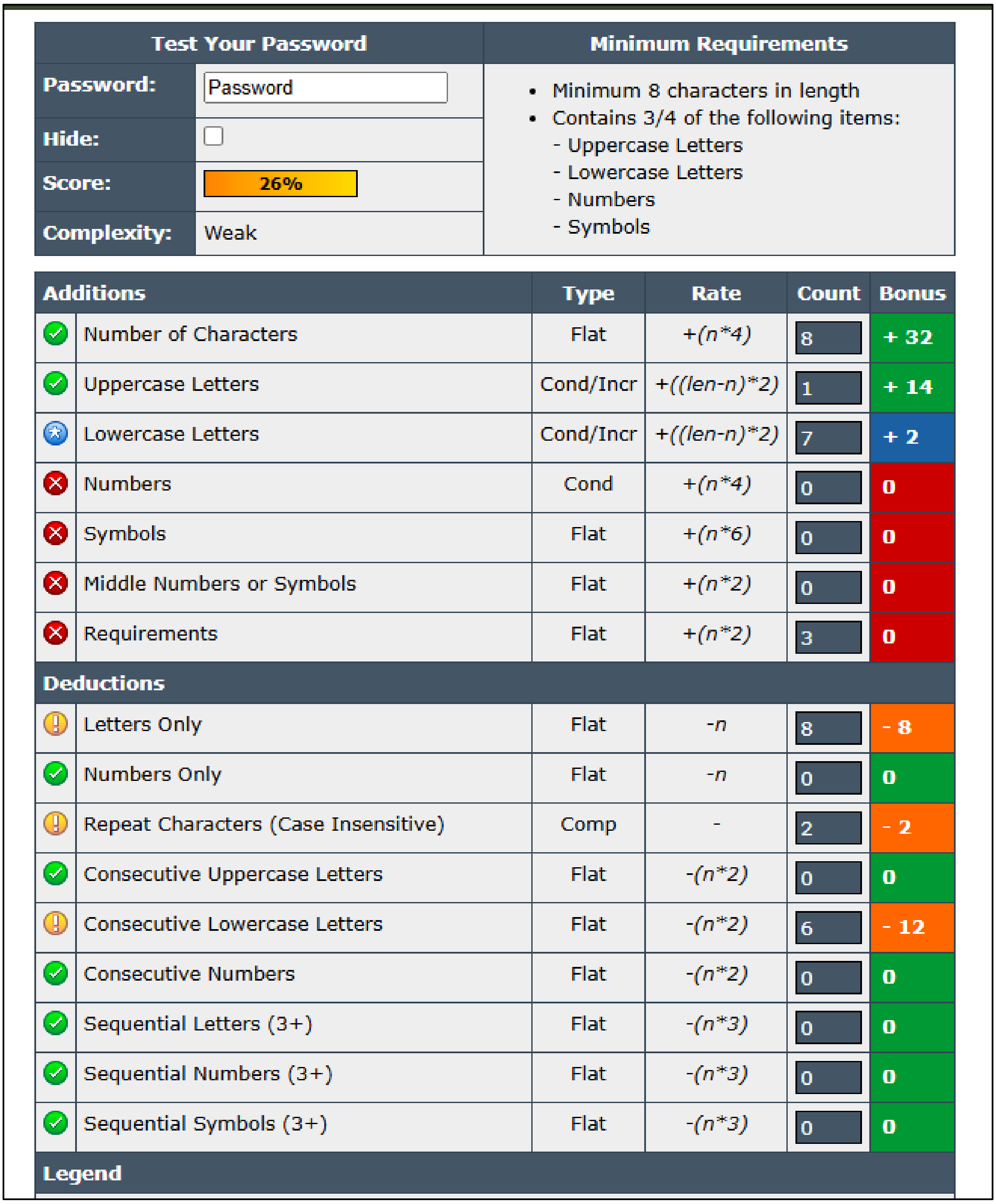
- A simple, commonly used password:-
  - password
- A slightly improved version with some symbol:-
  - P@ssword
- A longer, more personalized password:-
  - SummerTrip@Italy2025!
- A fully randomized and complex password:-
  - W7x$eL@9pQ!zR

Each one reflected a different style and strength level, allowing a clear comparison of what improves or weakens a password.

2. Testing Password Strength Using Online Tools

For this i am testing the password strengths using “passwordmeter”

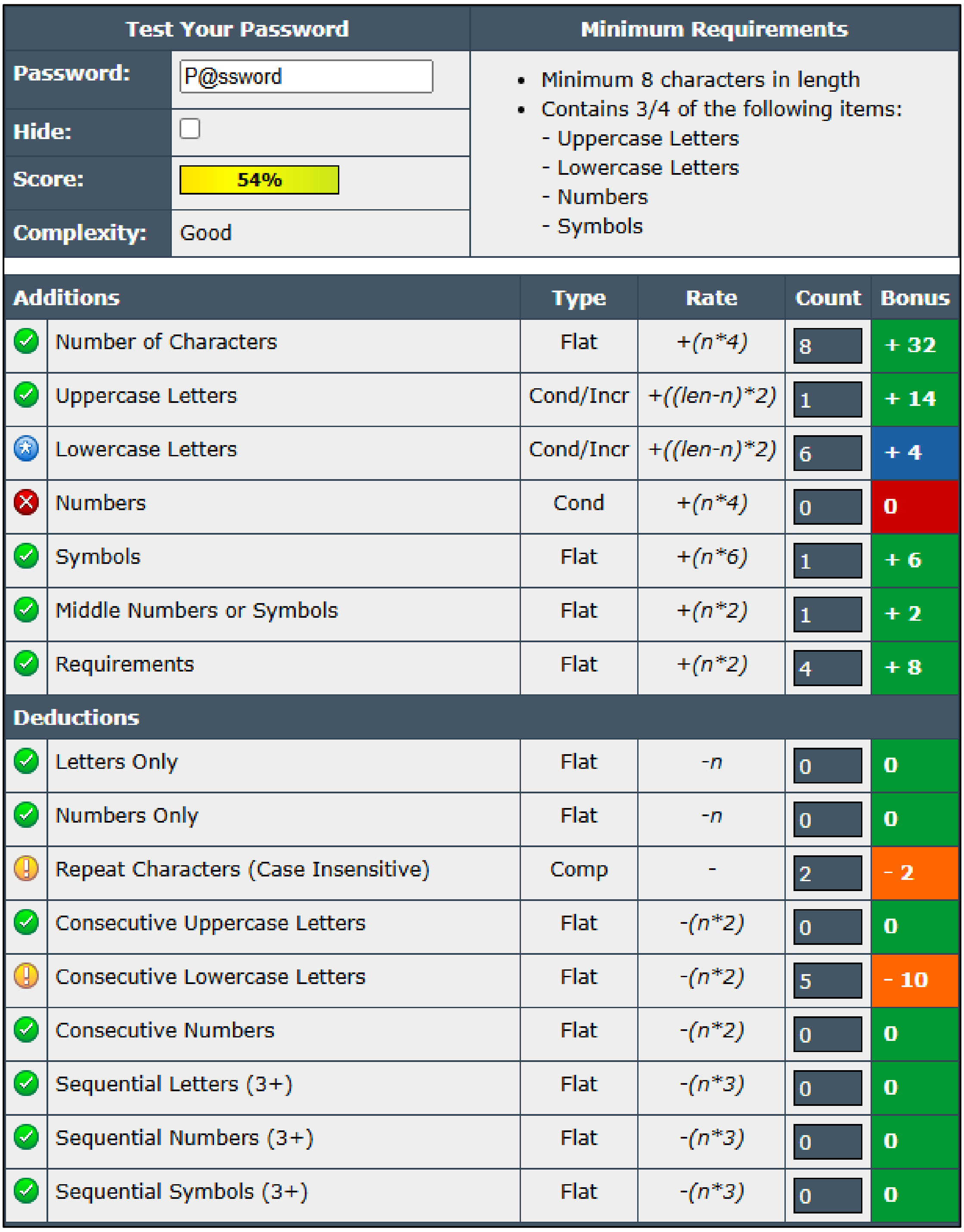
- A simple, commonly used password:-
    - password



Test Your Password		Minimum Requirements
Password:	Password	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	26%	
Complexity:	Weak	

	Additions	Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 2
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	3	0
	Deductions				
!	Letters Only	Flat	-n	8	- 8
✓	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)	6	- 12
✓	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				

- A slightly improved version with some symbol:-
    - P@ssword



Test Your Password	
Password:	P@ssword
Hide:	□
Score:	54%
Complexity:	Good

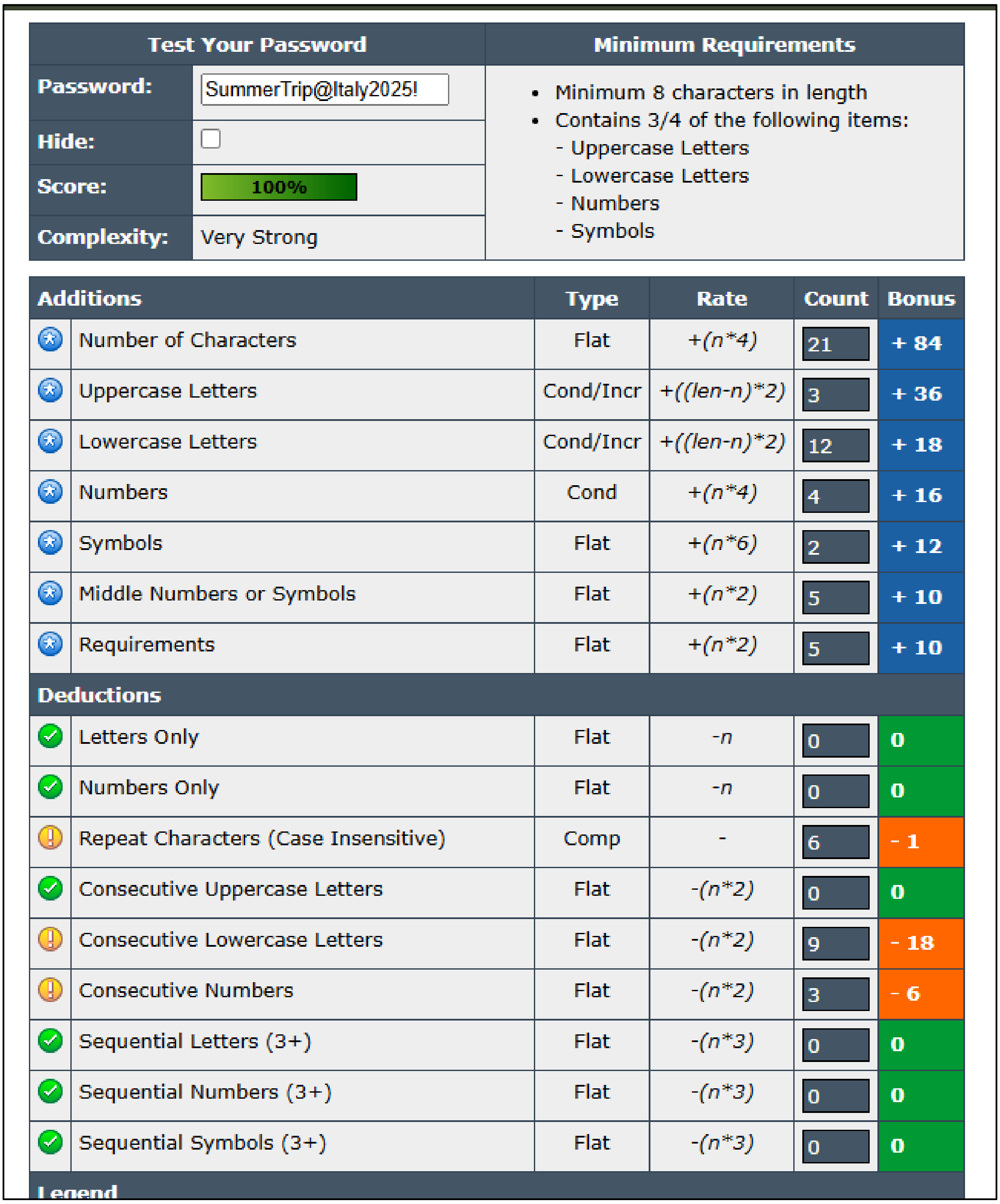
Minimum Requirements

- 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)	1	+ 14
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 4
✗	Numbers	Cond	+(n*4)	0	0
✓	Symbols	Flat	+(n*6)	1	+ 6
✓	Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
✓	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	- 2
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	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

- A longer, more personalized password:-
  - SummerTrip@Italy2025!



Test Your Password	
Password:	SummerTrip@Italy2025!
Hide:	☐
Score:	100%
Complexity:	Very Strong

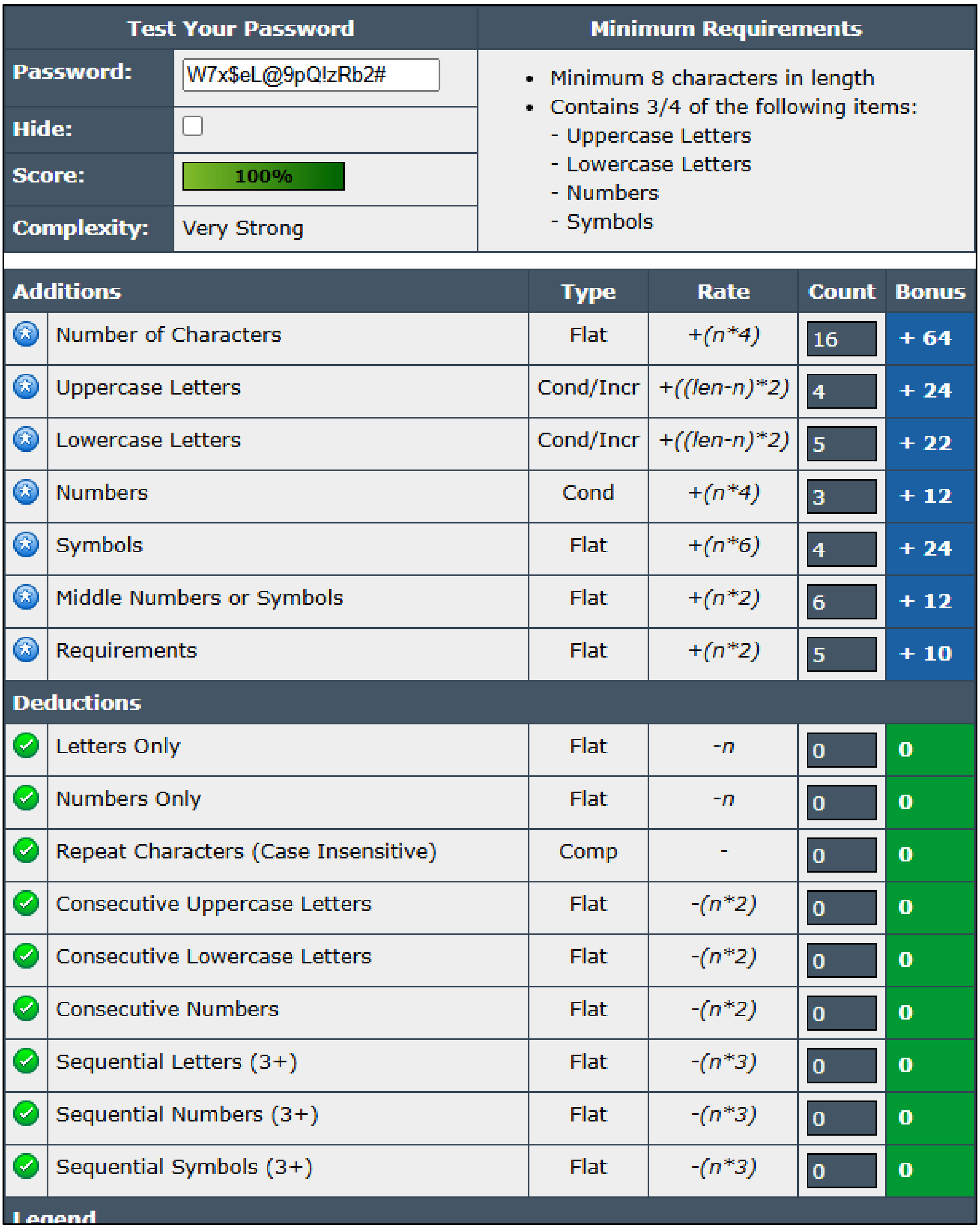
Minimum Requirements

- 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)	21	+ 84
✪	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 36
✪	Lowercase Letters	Cond/Incr	+((len-n)*2)	12	+ 18
✪	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	-	6	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
⚠	Consecutive Lowercase Letters	Flat	-(n*2)	9	- 18
⚠	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

- A fully randomized and complex password:-
    - W7x$eL@9pQ!zRb2#



Test Your Password		Minimum Requirements
Password:	W7x$eL@9pQ!zRb2#	• 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)	16	+ 64
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 24
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 22
★	Numbers	Cond	+(n*4)	3	+ 12
★	Symbols	Flat	+(n*6)	4	+ 24
★	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	-	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

3. Observations from the Results

After testing the four sample passwords using online tools, I noted their scores, strength levels, and feedback. This helped highlight how factors like length, symbol use, and randomness affect overall password security.

Here's the analysis report:

Password	**Score**	**Strength**	**Feedback**
password	26%	Weak	Commonly used, no symbols or variety
P@ssword	54%	Moderate	Better due to symbol but still predictable
SummerTrip@Italy2025!	100%	Strong	Long, personalized, good mix of characters
W7x$eL@9pQ!zRb2#	100%	Very Strong	Fully random, excellent complexity and length

This comparison made it clear that longer passwords with more variety or randomness are significantly harder to crack. Personal passphrases and completely random strings both performed very well in the tests.

4. Key Practices for Creating Strong Passwords

From the results, these important points stood out:

- Short or common passwords like "password" are extremely weak and easy to guess.
- Adding symbols such as @, !, or # does improve strength, but if the pattern is predictable, it can still be cracked.
- Personalized passphrases that include numbers and symbols tend to perform much better and are easier to remember.
- Fully random and long strings are the strongest, as their unpredictability makes them very hard to break.

5. Understanding Common Password Attacks

To better understand why strong passwords are important, I explored a few common ways attackers try to steal or crack them:

Brute Force

This method tries every possible combination of characters until the correct password is found. It’s like trying to unlock a door by turning every key on a keychain one by one. Tools like Hydra, John the Ripper, and Medusa are often used for this. Short and simple passwords can be cracked in seconds using this method.

Dictionary Attack

Instead of guessing random combinations, this attack tries common words and phrases like "password", "123456", or "qwerty". It uses pre-made lists of popular passwords (called wordlists) and checks them quickly. Tools like Hashcat or John the Ripper with dictionary files such as rockyou.txt are commonly used. If your password is based on real words, this method can break it fast.

Credential Stuffing

In this case, attackers take leaked username and password combinations from past data breaches and try them on other websites. Since many people reuse the same password across multiple sites, it often works. Automated tools like Sentry MBA or Snipr are used to test thousands of accounts in minutes.

Phishing

This attack tricks users into giving away their password by sending fake emails or creating fake websites that look real. When someone enters their password on these fake sites, it goes straight to the attacker. Tools like Gophish and Evilginx are used to create these fake login pages and capture user input.

Weak or reused passwords are easy targets for all of these attack methods. That’s why using strong, unique passwords for each account is one of the best ways to protect yourself online.

6. Summary: Why Password Complexity Matters

This task helped me understand how important password complexity really is. Simple passwords like password or 123456 offer almost no protection and can be guessed very quickly using common tools.

In contrast, longer passwords that mix uppercase and lowercase letters, numbers, and special symbols are much harder to break. Random strings or unique passphrases that do not follow common patterns add even more strength.

Attackers use tools that try weak and common passwords first, so the more complex and unique a password is, the less likely it is to be cracked. This shows that strong passwords are one of the simplest and most effective ways to protect your online accounts.