Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

TASK – 6 CREATING A STRONG PASSWORD AND EVALUATING ITS STRENGTH

Tools used: Passwordmeter.com, ChatGPT.

INTRODUCTION:

In today's digital world, passwords remain the primary method of securing personal and sensitive information across various platforms. However, not all passwords provide equal protection. The strength of a password determines how resistant it is to cyberattacks such as brute force and dictionary attacks. This task focuses on understanding what makes a password strong by creating multiple passwords with varying complexity and evaluating their strength using online tools. The objective is to analyze the factors influencing password strength, learn best practices for creating robust passwords, and recognize common attack techniques that exploit weak passwords. This knowledge is crucial for improving cybersecurity and safeguarding digital identities effectively.

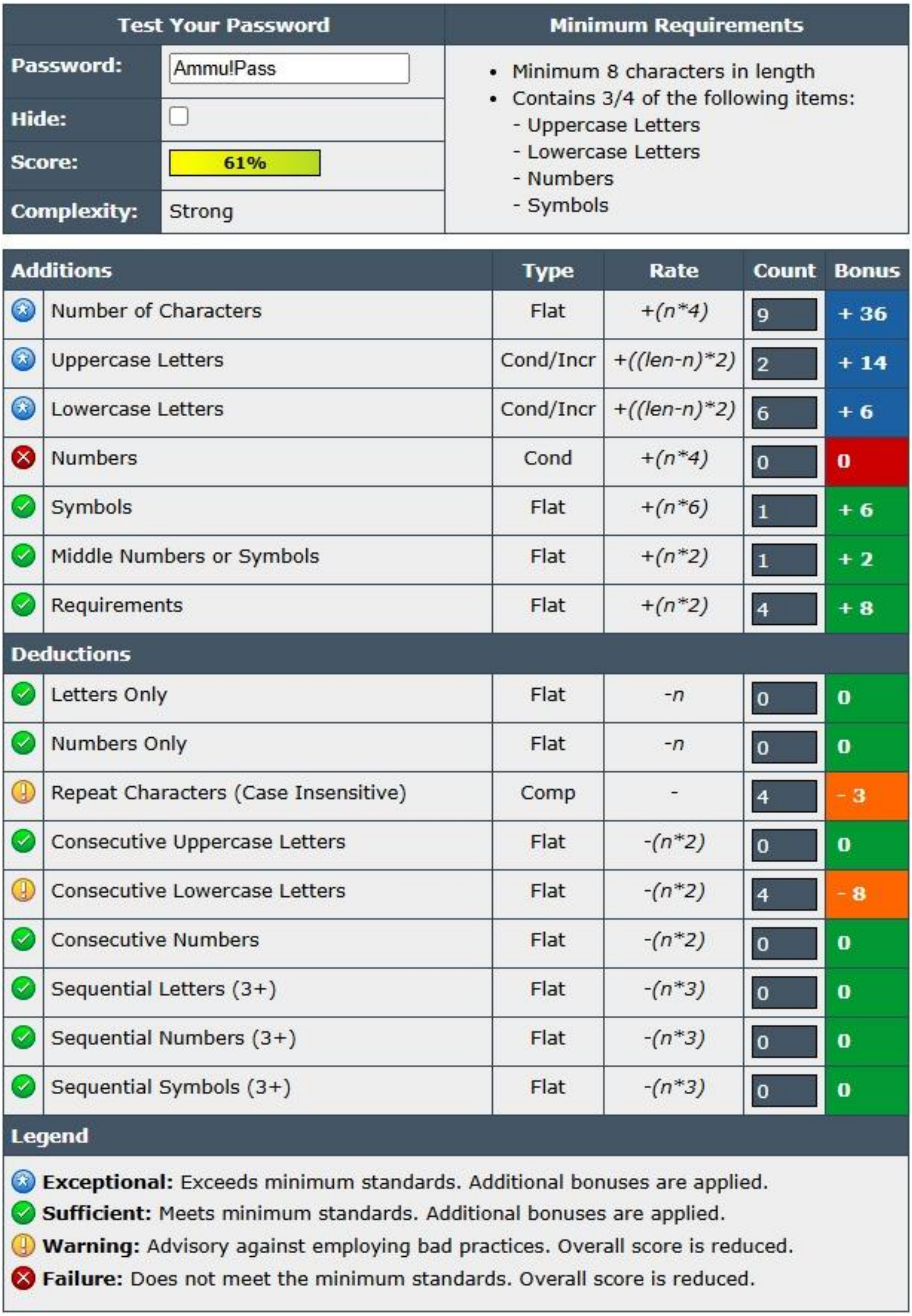
PASSWORD STRENGTH:

Password strength is a measure of how effective a password is at resisting guessing or brute-force attacks. It estimates how many attempts an attacker would need on average to correctly guess the password. The strength depends mainly on three factors: length, complexity, and unpredictability of the password.

→ **Length:** Longer passwords provide exponentially more possible combinations, making them harder to crack.
→ **Complexity:** Using a mix of uppercase and lowercase letters, numbers, and special characters increases the number of possible character combinations and makes the password harder to guess.
→ **Unpredictability:** Avoiding common words, predictable patterns, or personal information makes passwords less vulnerable to attacks.

Strong passwords typically take years or centuries to guess using current technologies, while weak ones might be cracked in a few tries. Password strength is essential for safeguarding against attacks like brute-force and dictionary attacks, as well as reducing the risk of unauthorized access to accounts.

Here are the screenshots from passwordmeter.com where I tested a few passwords.



Test Your Password	
Password:	Ammu!Pass
Hide:	□
Score:	61%
Complexity:	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)*	9	+ 36
★	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	2	+ 14
★	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	6	+ 6
✗	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	-	4	- 3
✓	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

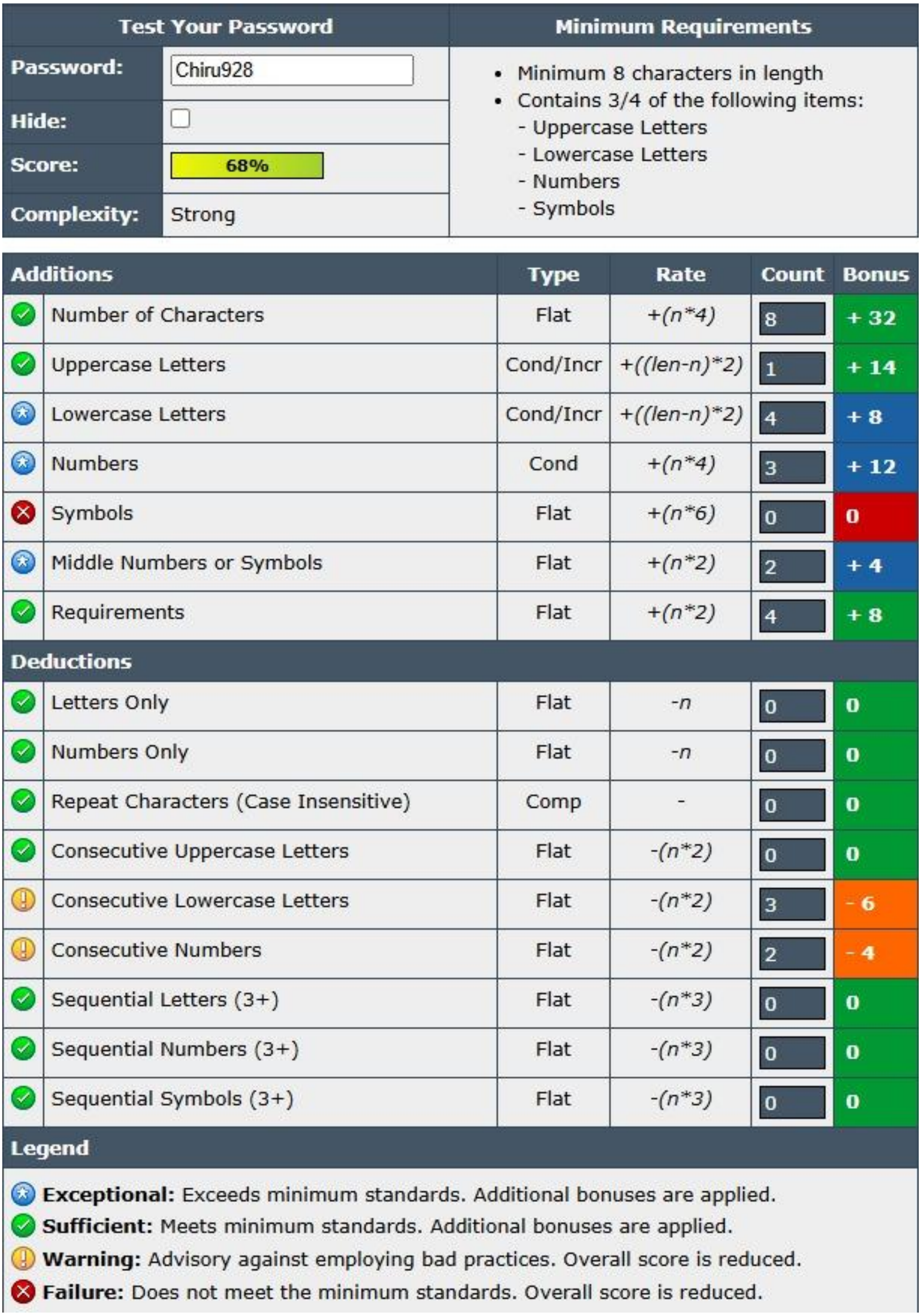
★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.

✓ **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.

SCREENSHOT 1



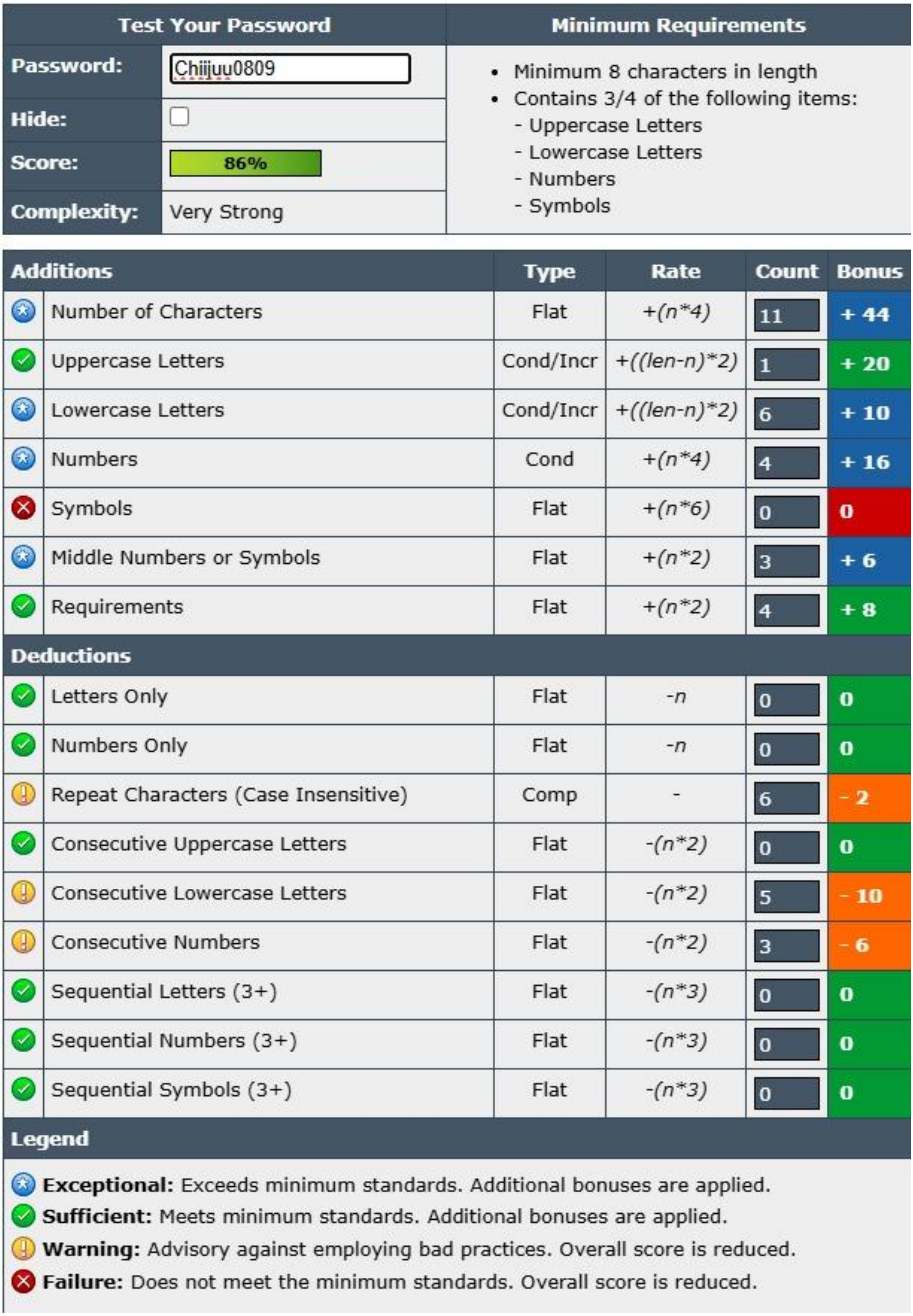
Test Your Password		Minimum Requirements
Password:	Chiru928	- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	68%	
Complexity:	Strong	

	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)	4	+ 8
★	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)	4	+ 8
	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)	3	- 6
!	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.

SCREENSHOT 2



Test Your Password	
Password:	Chiijuu0809
Hide:	□
Score:	86%
Complexity:	Very Strong

Minimum Requirements

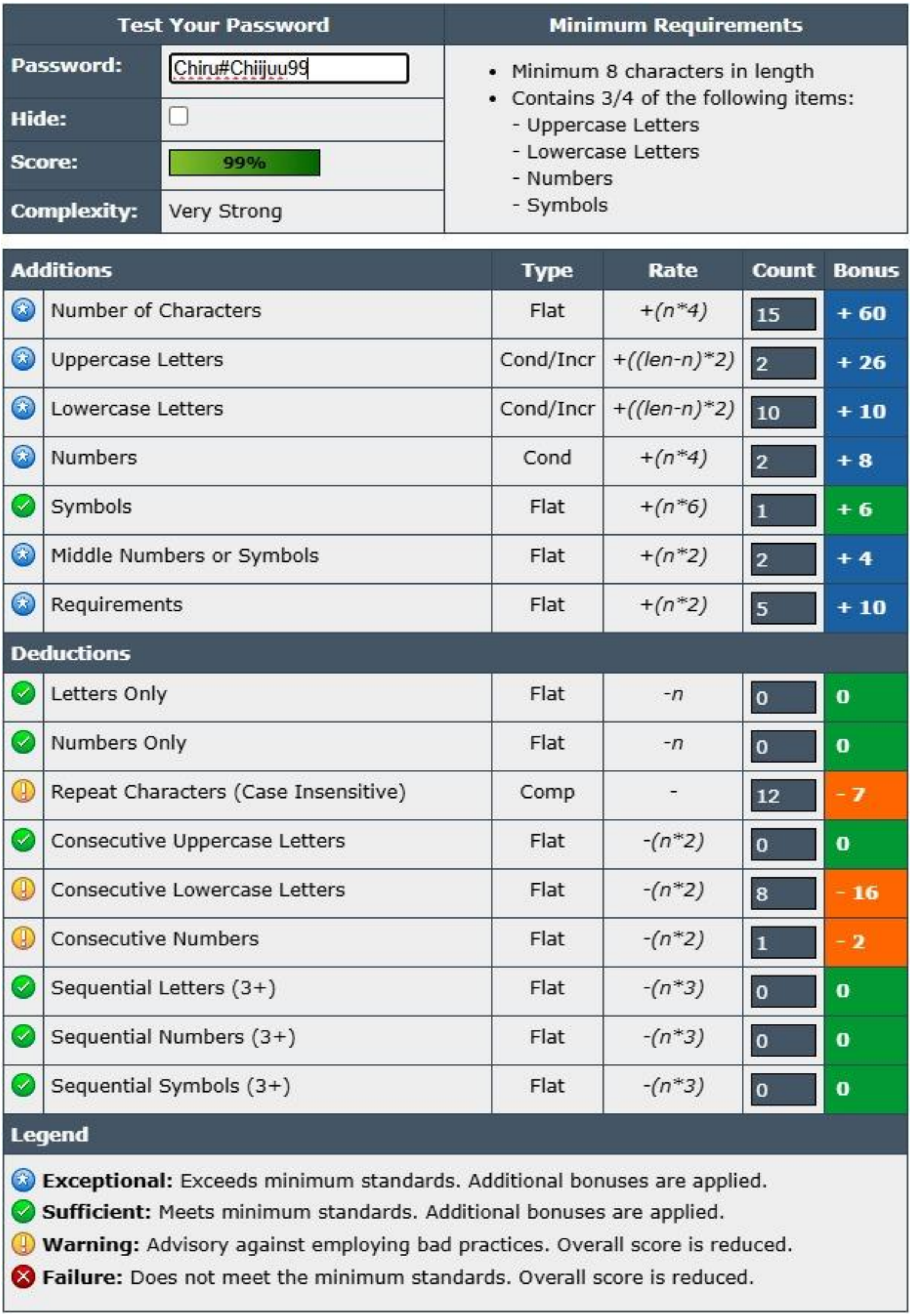
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
✪	Number of Characters	Flat	+(n*4)	11	+ 44
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 20
✪	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 10
✪	Numbers	Cond	+(n*4)	4	+ 16
✗	Symbols	Flat	+(n*6)	0	0
✪	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✓	Requirements	Flat	+(n*2)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	6	- 2
✓	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

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.

SCREENSHOT 3



Test Your Password	
Password:	Chiru#Chiijuu99
Hide:	□
Score:	99%
Complexity:	Very Strong

Minimum Requirements

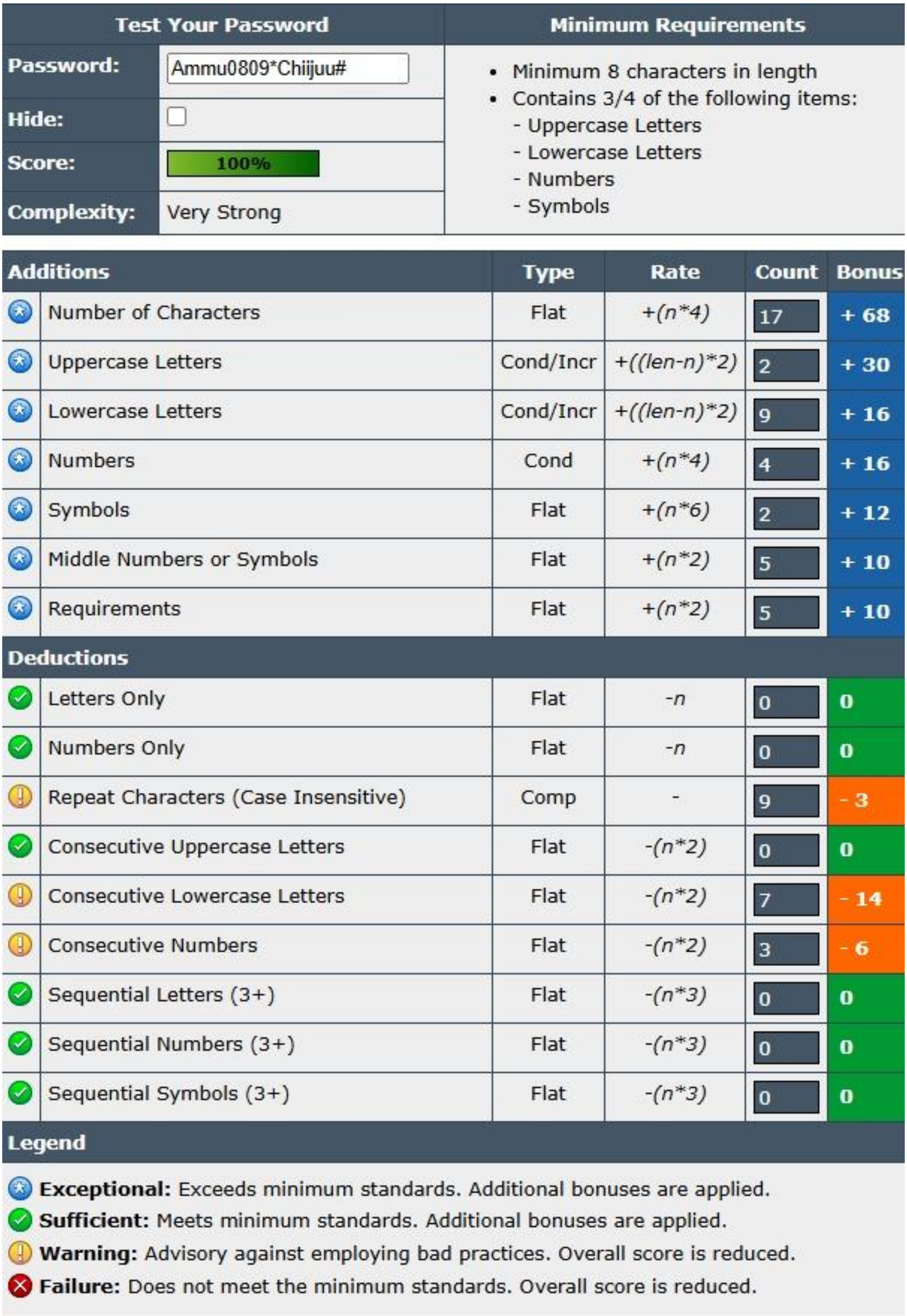
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
✪	Number of Characters	Flat	+(n*4)	15	+ 60
✪	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 26
✪	Lowercase Letters	Cond/Incr	+((len-n)*2)	10	+ 10
✪	Numbers	Cond	+(n*4)	2	+ 8
✓	Symbols	Flat	+(n*6)	1	+ 6
✪	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	-	12	- 7
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
⚠	Consecutive Lowercase Letters	Flat	-(n*2)	8	- 16
⚠	Consecutive Numbers	Flat	-(n*2)	1	- 2
✓	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.

SCREENSHOT 4



Test Your Password	
Password:	Ammu0809*Chiijuu#
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)	17	+ 68
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 30
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 16
★	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	-	9	- 3
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	7	- 14
!	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.

SCREENSHOT 5

SCREENSHOT 1:

Password: Ammu!Pass

- **Score:** 61%, Complexity: Strong
- **Explanation:** This password has 9 characters with uppercase, lowercase, and one symbol. Lack of numbers and presence of repeated characters (-3) and consecutive lowercase (-8) reduce strength. Despite meeting basic criteria, it ranks lower due to limited length and complexity.

SCREENSHOT 2:

Password: Chiru928

- **Score:** 68%, Complexity: Strong
- **Explanation:** This password is shorter (8 characters) and lacks symbols, resulting in a lower score. It benefits from some uppercase (+14), lowercase (+8), and numbers (+12) but loses points due to consecutive lowercase (-6), numbers (-4), and no symbols. The overall strength is strong but weaker compared to longer complex passwords.

SCREENSHOT 3:

Password: Chiijuu0809

- **Score:** 86%, Complexity: Very Strong
- **Explanation:** The 11-character password includes uppercase, lowercase, and numbers but no symbols, which limits its bonus points. Deductions come from repeated characters (-2), consecutive lowercase (-10), and numbers (-6), reducing the score but keeping it high due to length and required character types.

SCREENSHOT 4:

Password: Chiru#Chiijuu99

- **Score:** 99%, Complexity: Very Strong
- **Explanation:** This password has 15 characters, including uppercase and lowercase letters, numbers, and symbols. It scores high due to the mix of character types (+60 for length, +26 uppercase, +10 lowercase, +8 numbers, +6 symbols). There are some repeated characters (-7) and consecutive lowercase letters (-16), but the overall complexity remains very strong.

SCREENSHOT 5:

Password: Ammu0809*Chiijuu#

- **Score:** 100%, Complexity: Very Strong
- **Explanation:** With 17 characters combining uppercase, lowercase, numbers, and symbols, this password meets all complexity criteria. It gains bonuses for middle numbers/symbols (+10) and satisfies all minimum requirements.

Minor deductions for repeated characters (-3), consecutive lowercase (-14), and numbers (-6) do not significantly affect the strength.

BRUTE FORCE ATTACK:

A brute force attack is a cyberattack technique where the attacker attempts to gain unauthorized access to an account or system by systematically and exhaustively trying every possible combination of passwords or encryption keys until the correct one is found. This attack method usually utilizes automated software to rapidly generate and test millions of password combinations.

The success of a brute force attack largely depends on the complexity and length of the password. Simple passwords like “Chiru928” (68% strength) or “Ammu!Pass” (61% strength) have lower complexity scores, making them more vulnerable to brute force cracking. In contrast, more complex passwords like “Chiru#Chiijuu99” (99% strength) and “Ammu0809*Chiijuu#” (100% strength) with a mix of uppercase letters, lowercase letters, numbers, and symbols have higher complexity and resist brute force attacks far better.

Above screenshots demonstrate how including a combination of character types and increasing password length boosts the score and complexity rating, significantly enhancing security. The use of symbols, numbers in the middle, and avoiding repeated or consecutive characters further strengthen the password, reducing the likelihood that a brute force attack will succeed quickly.

To mitigate brute force attacks, it is recommended to:

- Use long passwords with mixed character types.
- Avoid simple, predictable words or patterns.
- Implement account lockouts or rate limits on login attempts.
- Use multi-factor authentication to add extra security layers.

This methodical approach to password creation makes brute force attacks impractical by increasing the number of possible combinations exponentially.

DICTIONARY ATTACK:

Dictionary attacks exploit the tendency of users to choose passwords based on common words or simple phrases. As seen in the screenshots you shared, passwords that use common words, repeated characters, or predictable patterns tend to have lower strength scores and are thus vulnerable.

In a dictionary attack, an attacker uses precompiled lists— “dictionaries”—of commonly used passwords, words, or leaked passwords and systematically tries each against a target account. For example, a password like “Chiru928” scores 68% strength partly due to the presence of common words and predictable sequences, making it susceptible to dictionary-based guesses.

Above screenshots demonstrate the importance of using complex passwords rich in mixed characters (letters, numbers, symbols) and avoiding predictable words or repeated patterns to defend against such attacks.

Thus, dictionary attacks succeed against weak passwords by focusing on likely guesses rather than random combinations, making password complexity and unpredictability critical for security.

AUTHENTICATION BEST PRACTICES:

To secure user accounts and protect sensitive information, it is essential to follow authentication best practices:

- Use Strong Passwords and Policies: Encourage the creation of complex, unique passwords that combine uppercase and lowercase letters, numbers, and symbols. Enforce minimum length and avoid common or reused passwords.

- Multi-Factor Authentication (MFA): Require users to verify their identity using multiple factors, such as a password plus a one-time code or biometric verification, to add a second layer of security.

- Secure Transmission: Ensure authentication credentials are transmitted over encrypted channels such as HTTPS/TLS to prevent interception.

- Password Storage: Store passwords securely using strong hashing algorithms with added salt to protect against database breaches.

- Account Lockout and Rate Limiting: Implement limits on failed login attempts to prevent brute force attacks by locking accounts temporarily or slowing response times.

- Session Management: Use secure, time-limited sessions and require reauthentication for sensitive actions to prevent session hijacking.

- Regular Audits and Monitoring: Continuously audit authentication systems for vulnerabilities and monitor login activities for suspicious behavior.

- Least Privilege Principle: Limit user access rights to only what is necessary, reducing the risk of unauthorized actions.

Adhering to these practices enhances security, reduces vulnerabilities, and protects against common cyber threats such as brute force attacks, phishing, and credential theft.

My password strength test results show how different factors influence strength scores:

→ Passwords like “Chiru#Chiijuu99” and “Ammu0809*Chiijuu#” scored 99% and 100%, rated as “Very Strong,” because they have sufficient length (15-17 characters), a good mix of uppercase and lowercase letters, numbers, and symbols, and relatively few repeated or sequential characters.

→ Simpler passwords such as “Chiru928” (68%) and “Ammu!Pass” (61%) scored lower because of shorter length, fewer symbols, and presence of repeated and consecutive characters that reduce complexity.

→ The password strength meter also accounts for factors such as the position of numbers and symbols (middle placement adds to strength) and penalizes repeated characters or sequences.

Overall, passwords with higher length and diverse character types rank stronger and are harder to crack, thereby providing better security against brute force and dictionary attacks.

CONCLUSION:

This task emphasized the critical role of password strength in protecting digital information from unauthorized access. By creating and evaluating multiple passwords with varying characteristics, it became evident that password strength increases significantly with greater length, a mix of uppercase and lowercase letters, numbers, and special symbols. Passwords that incorporate diverse characters and avoid predictable patterns or repeated sequences are much harder for attackers to crack through common techniques like brute force or dictionary attacks. The analysis highlights best practices for creating strong passwords, which are essential to enhancing cybersecurity and safeguarding personal and organizational data. Applying these principles can significantly reduce the risk of password-related breaches and improve overall digital security posture.

****