Cybersecurity Internship – Task 6

Create a Strong Password and Evaluate Its Strength

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

Name : Bogi Arun

Date : 12/08/2025

Tools: Online free password strength checkers

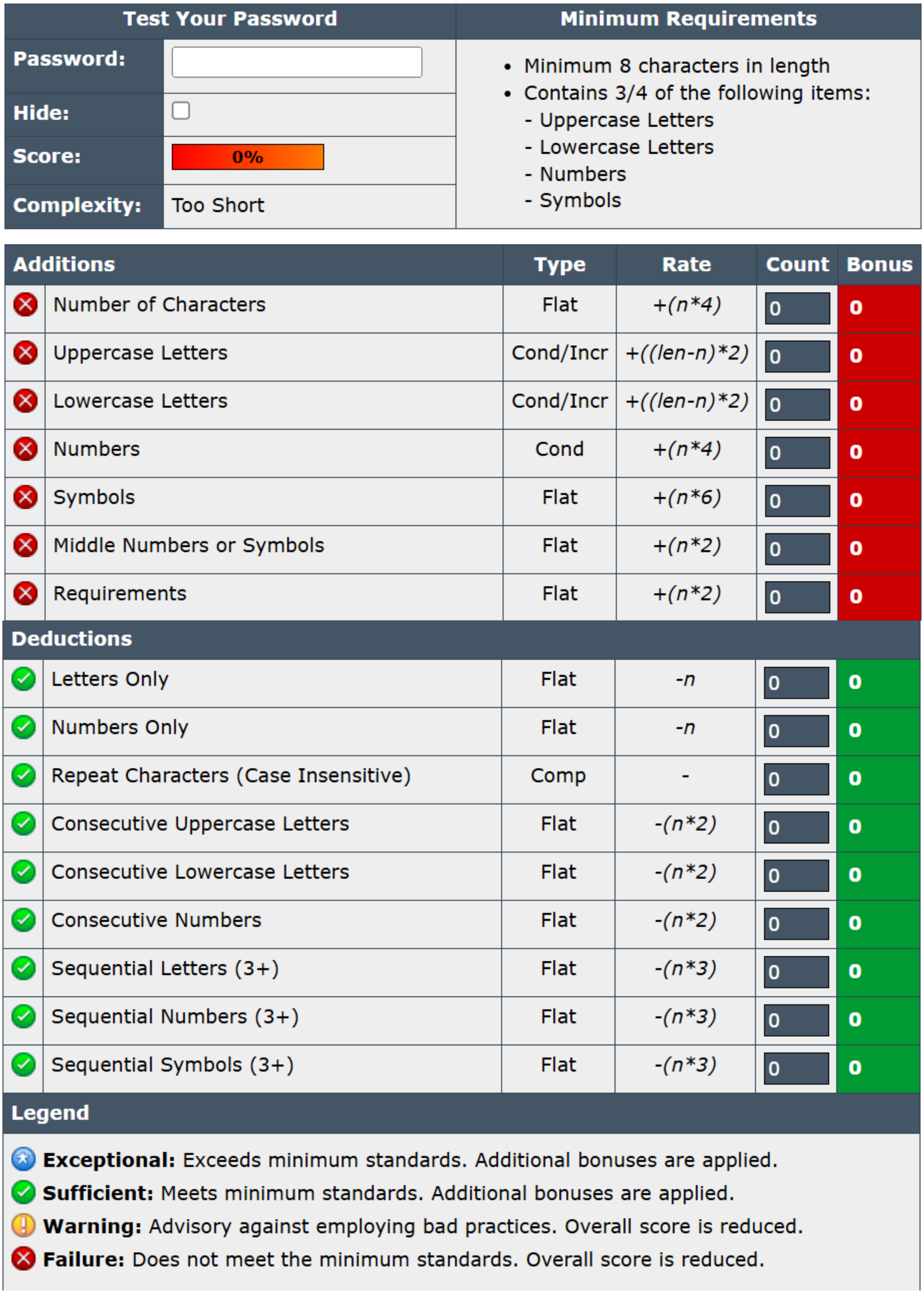
Introduction

Passwords are the first line of defense in protecting sensitive information, online accounts, and digital identities. A weak password can be easily guessed or cracked, making systems vulnerable to cyberattacks such as brute force or dictionary attacks. This task focuses on understanding the characteristics of a strong password, testing its strength using online tools, and identifying best practices for secure password creation. By creating and evaluating multiple passwords with varying complexities, learners will gain practical knowledge of password security, the importance of complexity and length, and methods to defend against common password-based attacks.

Step-by-Step Guide:

1. Create Multiple Passwords:
- Make at least 4–5 passwords with different complexity levels:
  Weak example: arun123
  Medium example: Arun@1234
  Strong example: @R!un#2025$
  Passphrase example: BlueSky!Run@Fast2025
- Use uppercase, lowercase, numbers, symbols, and at least 12 characters for strong ones.

2. Test Passwords with Strength Checker:
- Use free password strength checkers:
  https://passwordmeter.com/
  https://www.security.org/how-secure-is-my-password/
- Enter each password and note score, estimated time to crack, and feedback



Test Your Password	
Password:	
Hide:	☐
Score:	0%
Complexity:	Too Short

Minimum Requirements

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

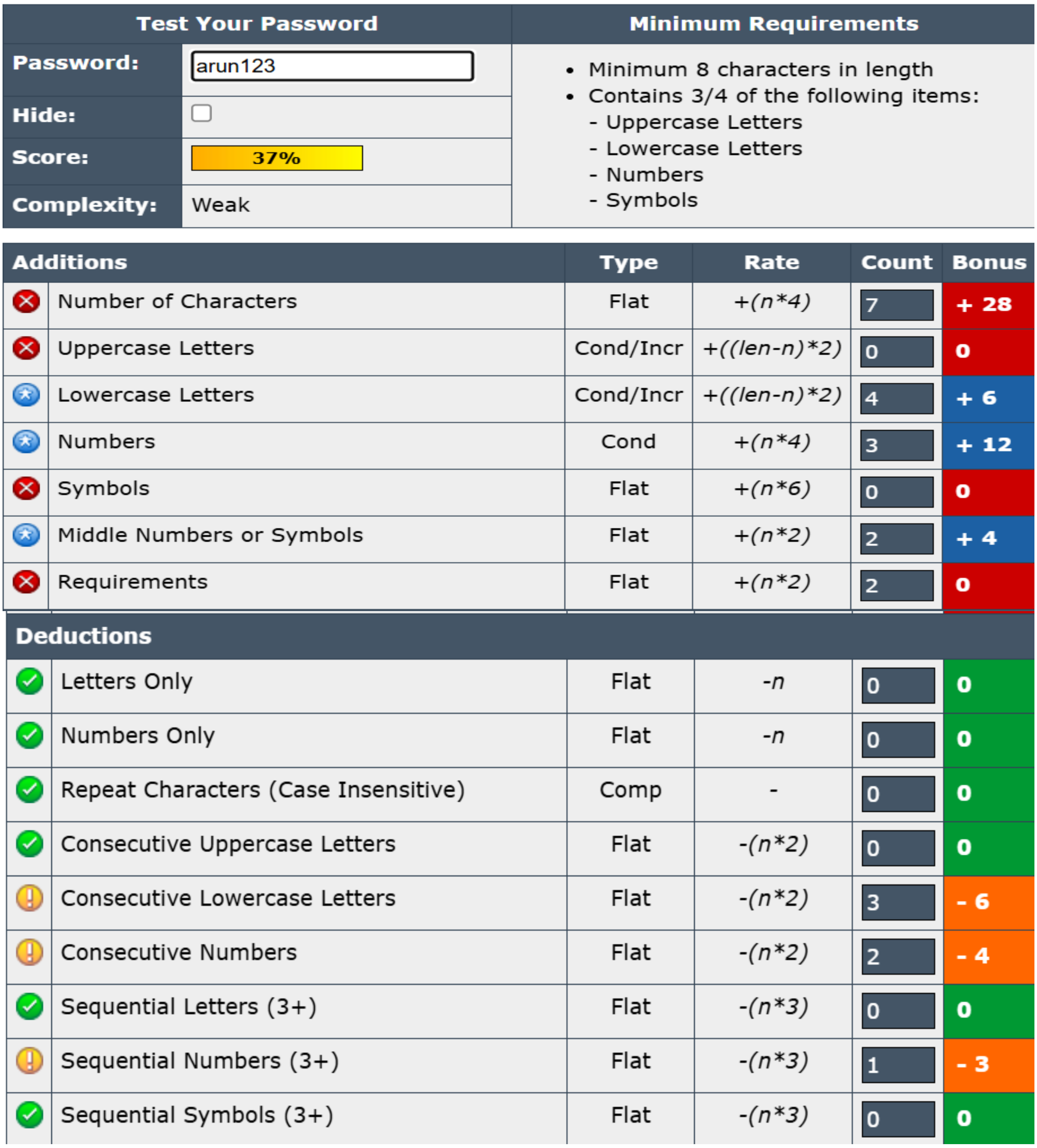
	Additions	Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	0	0
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	0	0
	Deductions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

Document the Results

Password	Strength Score	Time to Crack	Feedback from Tool
arun123	Weak	Few seconds	Too short, no special characters
Arun@1234	Medium	Minutes	Add more characters and special symbols
@R!un#2025$	Strong	Centuries	Meets all complexity rules
BlueSky!Run@Fast2025	Very Strong	Centuries+	Excellent length & complexity



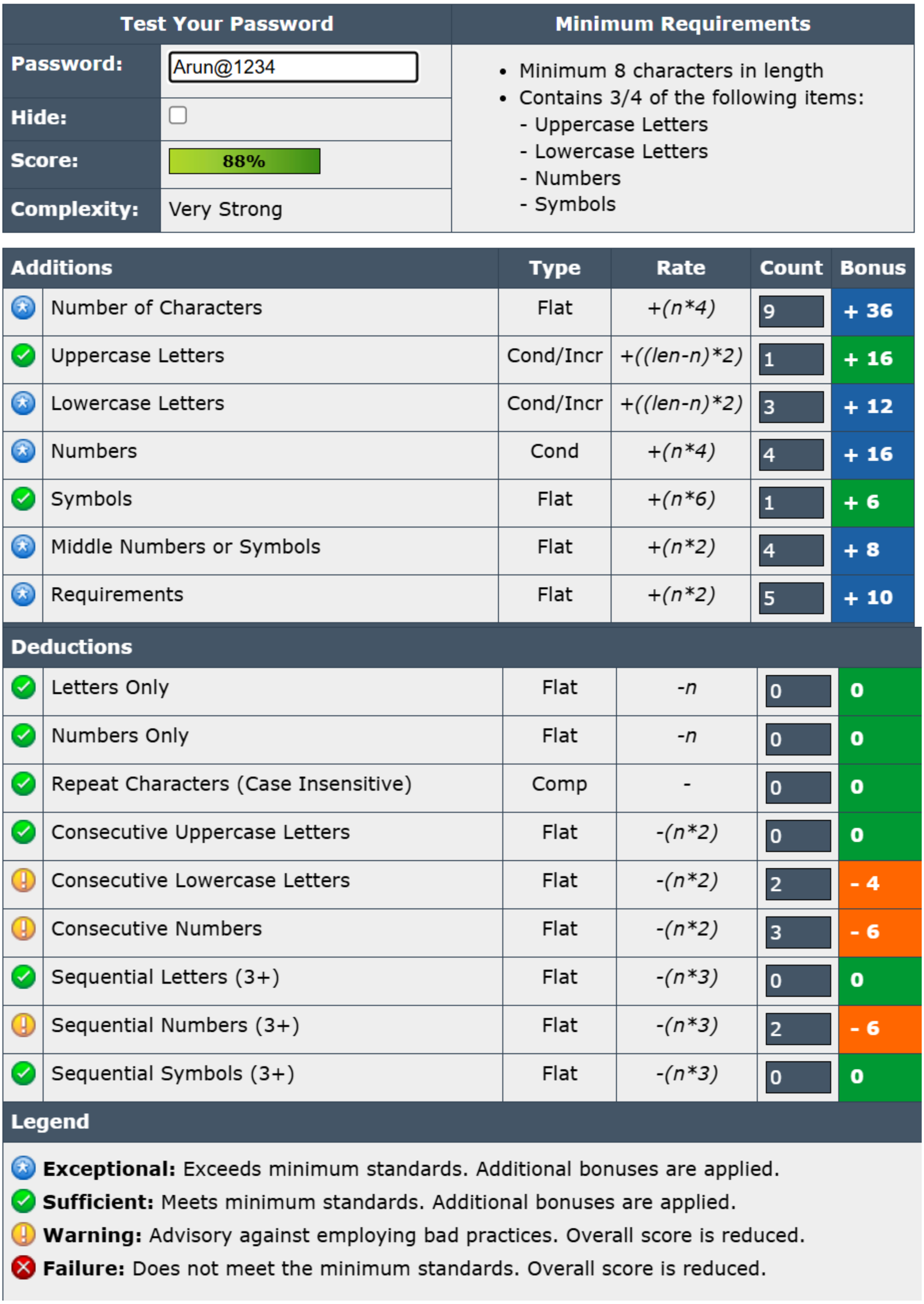
Test Your Password	
Password:	arun123
Hide:	□
Score:	37%
Complexity:	Weak

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)	7	+ 28
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 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)	2	0

	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)	1	- 3
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0



Test Your Password	
Password:	Arun@1234
Hide:	□
Score:	88%
Complexity:	Very Strong

Minimum Requirements

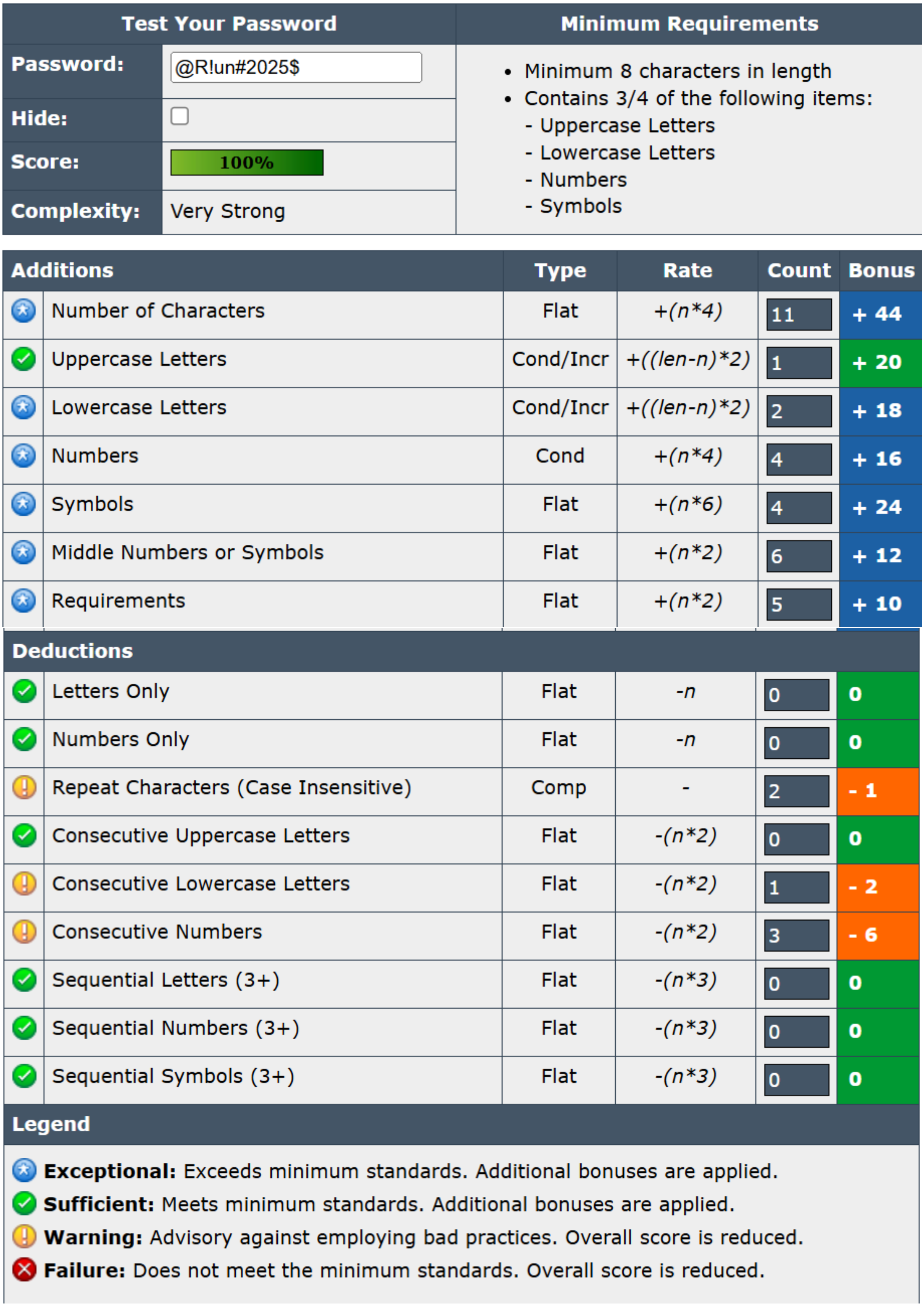
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	9	+ 36
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 12
★	Numbers	Cond	+(n*4)	4	+ 16
✓	Symbols	Flat	+(n*6)	1	+ 6
★	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)	2	- 4
!	Consecutive Numbers	Flat	-(n*2)	3	- 6
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	2	- 6
✓	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.



Test Your Password		Minimum Requirements
Password:	@R!un#2025$	- 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)*	11	+ 44
✓	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	1	+ 20
★	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	2	+ 18
★	Numbers	Cond	*+(n*4)*	4	+ 16
★	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	-	2	- 1
✓	Consecutive Uppercase Letters	Flat	*-(n*2)*	0	0
⚠	Consecutive Lowercase Letters	Flat	*-(n*2)*	1	- 2
⚠	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

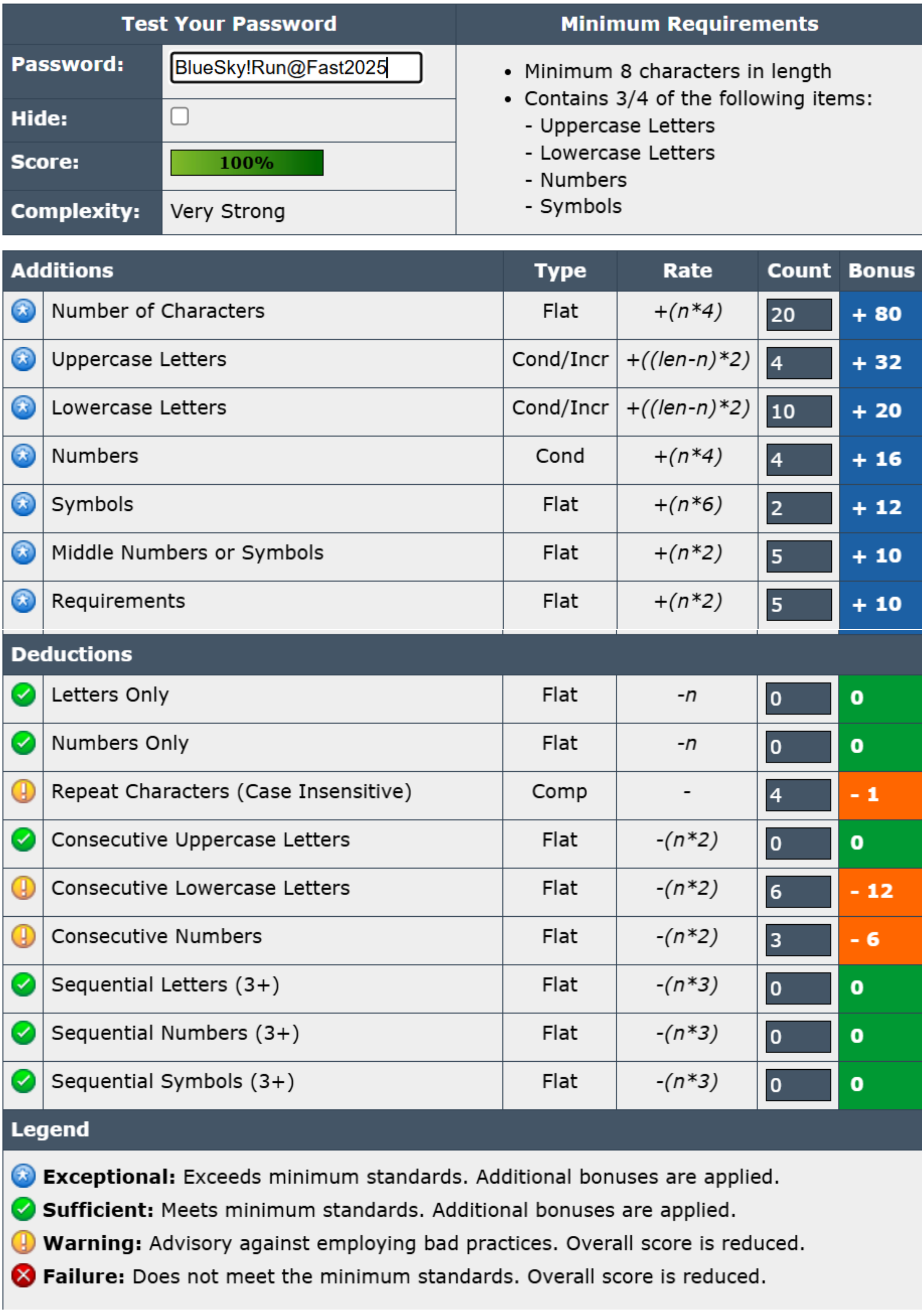
Legend

★ **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.



Test Your Password		Minimum Requirements
Password:	BlueSky!Run@Fast2025	- 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)	4	+ 32
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	10	+ 20
★	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	-	4	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
⚠	Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
⚠	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.

Summarize Best Practices:
- Use at least 12–16 characters
- Include uppercase, lowercase, numbers, and symbols
- Avoid dictionary words or personal info
- Use passphrases for better memory
- Change passwords regularly
- Enable Multi-Factor Authentication (MFA)
- Consider a password manager

Common Password Attacks

1. **Brute Force Attack**
    - In a brute force attack, the attacker tries **every possible combination** of characters until the correct password is found.
    - The time required depends on password length, complexity, and computing power.
    - Example: Trying a, b, c … all the way to zZ9@! until the right one is found.
2. **Dictionary Attack**
    - Uses a **predefined list of words** (like a dictionary or common password list) to guess the password.
    - Works well against weak passwords containing common words, phrases, or simple variations.
    - Example: Guessing from a list like password, 123456, qwerty, admin123.
3. **Phishing Attack** *(optional addition)*

- Tricks the user into revealing their password via fake websites, emails, or messages.
- Example: A fake login page that captures your entered credentials.

4. **Credential Stuffing** *(optional addition)*

- Attackers use leaked username–password pairs from one breach to try logging into other accounts, exploiting reused credentials.

How Password Complexity Affects Security

Password complexity plays a crucial role in protecting accounts and systems from unauthorized access. A complex password — one that combines uppercase and lowercase letters, numbers, special symbols, and sufficient length — greatly increases the number of possible combinations an attacker must try. This makes brute force and dictionary attacks significantly more time-consuming and resource-intensive. Simple or predictable passwords can be cracked in seconds, while highly complex ones may take years or even centuries to break with current technology. Therefore, increasing complexity directly enhances resistance to common password attacks and improves overall security.

Conclusion

This task demonstrated the importance of creating and maintaining strong, complex passwords to safeguard personal and organizational data. Through practical testing with password strength tools, it became clear that longer passwords with a mix of characters significantly increase resistance against brute force and dictionary attacks. The evaluation reinforced best practices such as avoiding common words, using passphrases, and enabling multi-factor authentication. By applying these strategies, users can greatly enhance their password security and reduce the risk of unauthorized access.