Task 6 Report – Password Strength Evaluation

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

1. Introduction

Passwords are the first line of defense against unauthorized access to accounts and systems. Weak passwords are easy targets for attackers using techniques such as brute force or dictionary attacks. This task aims to explore password complexity by testing different passwords and analyzing their strength.

2. Methodology

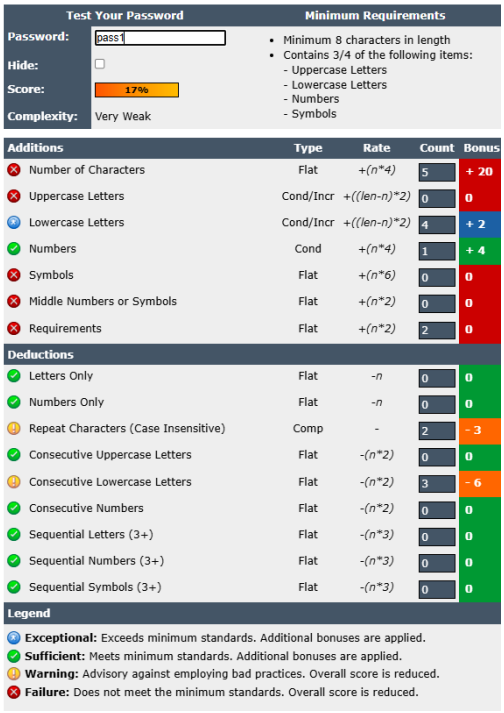
1. Created five passwords with varying complexity:
   - Very weak
   - Weak
   - Medium strength
   - Strong
   - Very strong
2. Tested each password using [Tool Name, e.g., passwordmeter.com].
3. Recorded the strength score and tool feedback for each.
4. Analyzed results to determine best practices for creating strong passwords.

3. Results

Password	Tool Rating / Score	Feedback from Tool
pass1	Very Weak	Too short, only lowercase letters and numbers
test12	Weak	Needs uppercase and symbols, longer length recommended
password123	Weak / Medium	Common word detected, predictable pattern
ASDFGHJKL;'	Strong	Long length, contains uppercase and symbols, lacks lowercase and numbers
@Artist23Here!	Very Strong	Long, contains uppercase, lowercase, numbers, and symbols

4. Screenshots

Screenshot for `pass1`:



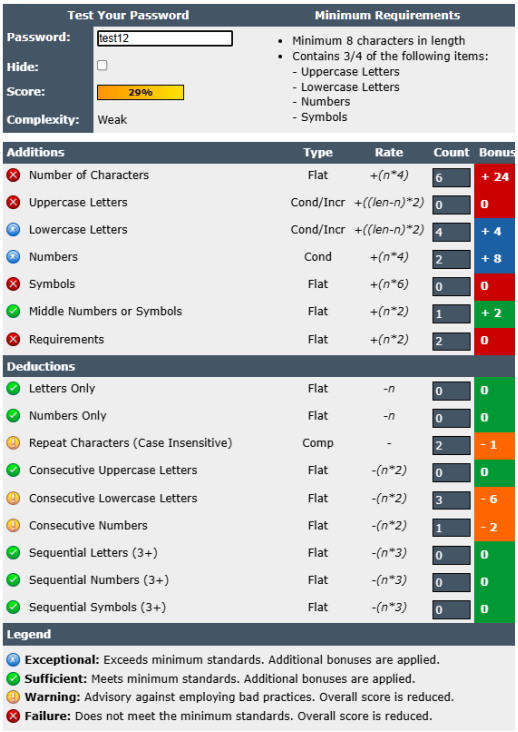
Test Your Password		Minimum Requirements
Password:	pass1	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	17%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	5	+ 20
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 2
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	2	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 3
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
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 for `test12`:



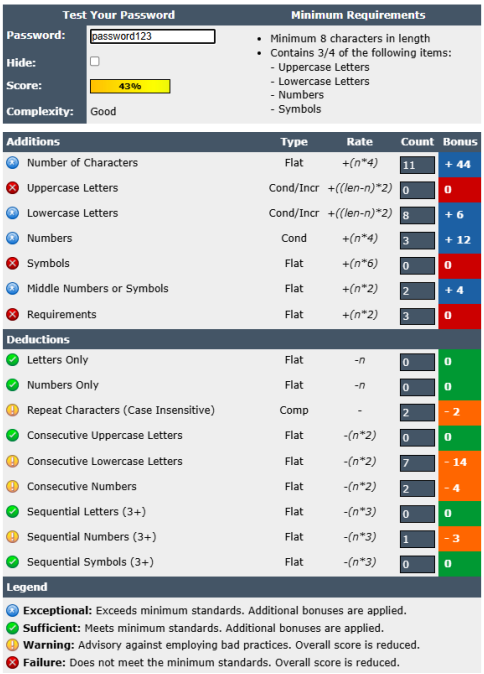
Test Your Password		Minimum Requirements
Password:	test12	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	29%	
Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 4
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	2	0
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)	3	- 6
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 for `password123`:



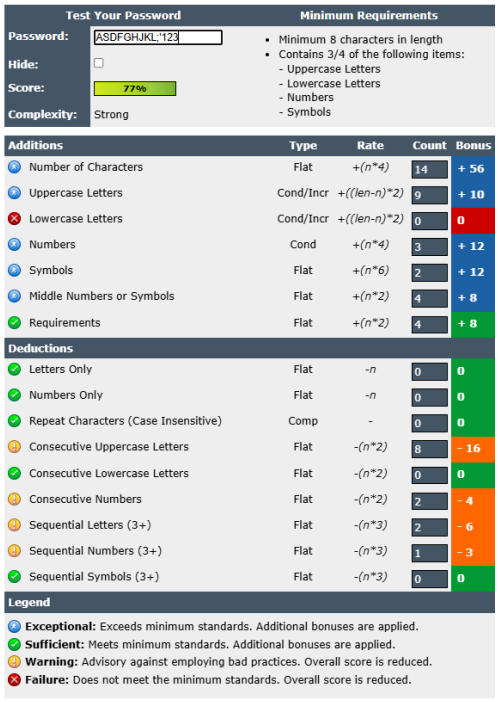
Test Your Password		Minimum Requirements
Password:	password123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	43%	
Complexity:	Good	

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.

Screenshot for `ASDFGHJKL;'`:



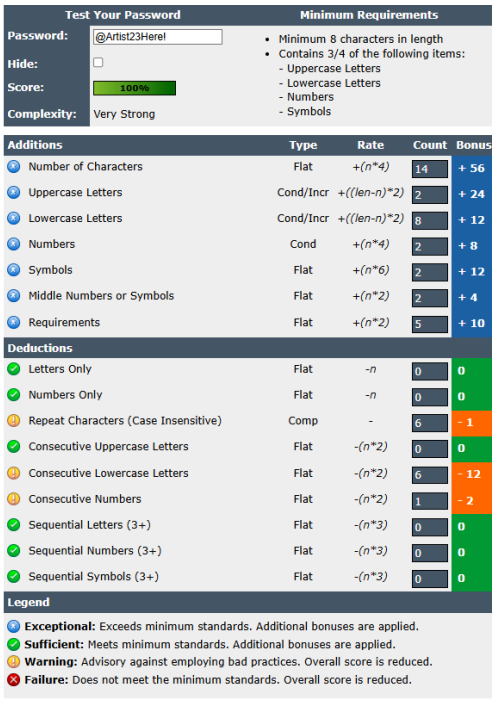
Test Your Password		Minimum Requirements
Password:	ASDFGHJKL;'123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	77%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	9	+ 10
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
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)	8	- 16
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	2	- 6
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.

Screenshot for `@Artist23Here!`:



Test Your Password		Minimum Requirements
Password:	@Artist23Here!	• 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)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 12
Numbers	Cond	+(n*4)	2	+ 8
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	-	6	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
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.

5. Observations

- Short passwords with only lowercase letters and numbers score poorly.
- Adding uppercase letters, numbers, and symbols increases the strength.
- Common words like 'password' reduce the score even if length is sufficient.
- Random placement of symbols and mixed character types produces the highest strength scores.

6. Best Practices for Creating Strong Passwords

- Use at least 12–16 characters.
- Include uppercase, lowercase, numbers, and special symbols.
- Avoid dictionary words or predictable patterns (e.g., '12345', 'qwerty').
- Use random combinations rather than meaningful phrases.
- Do not reuse passwords across different accounts.
- Consider using a password manager for storage.

7. Common Password Attacks

1. Brute Force Attack
Attempts every possible combination until the correct password is found. Short and simple passwords are cracked quickly.

2. Dictionary Attack
Uses precompiled lists of common passwords or words to guess passwords. Weak passwords like 'password123' are highly vulnerable.

8. Conclusion

This evaluation shows that password complexity significantly improves resistance to attacks. The more diverse and longer a password is, the harder it becomes for attackers to guess it using automated methods. Complex passwords like '@Artist23Here!' can take years or even centuries to crack, while simple ones like 'pass1' can be broken almost instantly.