

Password Strength Analysis Report

Cybersecurity Internship Task 6

Student Name: V. Prem Sai

Date: September 30, 2025

Task: Create a Strong Password and Evaluate Its Strength

Tool Used: passwordmeter.com

Executive Summary

This report presents a comprehensive analysis of password strength testing conducted using passwordmeter.com, examining four different password combinations to understand their security effectiveness against common cyber attacks. The study demonstrates how password complexity and length directly impact resistance to brute force and dictionary attacks.

Password Testing Results

The following passwords were tested using passwordmeter.com with detailed scoring breakdowns:

Passwords Tested:

amrutha\$2L1 Length: 11 characters)

Prem#5so0 Length: 9 characters)

Maha@401126 Length: 11 characters)

Prem@sa Length: 7 characters)

Test Results Summary:

Password	Estimated Score	Complexity Level	Character Mix	Security Assessment
amrutha\$2L1	Very Strong	Excellent	Upper, Lower, Numbers, Symbols	High security due to length and mixed characters
Prem#5so0	Strong	Good	Upper, Lower, Numbers, Symbols	Moderate security with decent complexity
Maha@401126	Very Strong	Excellent	Upper, Lower, Numbers, Symbols	High security with optimal length
Prem@sa	Moderate	Fair	Upper, Lower, Symbols	Limited security due to short length

Test Your Password		Minimum Requirements	
Password: Hide: Score: Complexity:	<input type="text" value="amrutha\$2L1"/> <input type="checkbox"/> <div>87%</div> Very Strong	<ul style="list-style-type: none"> Minimum 8 characters in length Contains 3/4 of the following items: <ul style="list-style-type: none"> 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	$+(len-n)*2$	7	+ 8
★ 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	-	2	- 1
✔ 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
★ 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

Password:

Hide:
☐








Score:










82%

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	$+(n*4)$	<input type="text" value="9"/>	+ 36
 Uppercase Letters	Cond/Incr	$+\left((len-n)*2\right)$	<input type="text" value="1"/>	+ 16
 Lowercase Letters	Cond/Incr	$+\left((len-n)*2\right)$	<input type="text" value="5"/>	+ 8
 Numbers	Cond	$+(n*4)$	<input type="text" value="2"/>	+ 8
 Symbols	Flat	$+(n*6)$	<input type="text" value="1"/>	+ 6
 Middle Numbers or Symbols	Flat	$+(n*2)$	<input type="text" value="2"/>	+ 4
 Requirements	Flat	$+(n*2)$	<input type="text" value="5"/>	+ 10

Deductions	Type	Rate	Count	Bonus
 Letters Only	Flat	$-n$	<input type="text" value="0"/>	0
 Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0
 Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="0"/>	0
 Consecutive Uppercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
 Consecutive Lowercase Letters	Flat	$-(n*2)$	<input type="text" value="3"/>	- 6
 Consecutive Numbers	Flat	$-(n*2)$	<input type="text" value="0"/>	0
 Sequential Letters (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
 Sequential Numbers (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
 Sequential Symbols (3+)	Flat	$-(n*3)$	<input type="text" value="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:

Maha@401126

Hide:

☐








Score:










100%

Complexity:


Very Strong


- 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	$+(len-n)*2$	3	+ 16
 Numbers	Cond	$+(n*4)$	6	+ 24
 Symbols	Flat	$+(n*6)$	1	+ 6
 Middle Numbers or Symbols	Flat	$+(n*2)$	6	+ 12
 Requirements	Flat	$+(n*2)$	5	+ 10


Deductions	Type	Rate	Count	Bonus
 Letters Only	Flat	$-n$	0	0
 Numbers Only	Flat	$-n$	0	0
 Repeat Characters (Case Insensitive)	Comp	-	4	- 2
 Consecutive Uppercase Letters	Flat	$-(n*2)$	0	0
 Consecutive Lowercase Letters	Flat	$-(n*2)$	2	- 4
 Consecutive Numbers	Flat	$-(n*2)$	5	- 10
 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:	<input type="text" value="Prem@sa"/>	<ul style="list-style-type: none"> Minimum 8 characters in length Contains 3/4 of the following items: <ul style="list-style-type: none"> Uppercase Letters Lowercase Letters Numbers Symbols 			
Hide:	<input type="checkbox"/>				
Score:	<div>58%</div>				
Complexity:	Good				

Additions	Type	Rate	Count	Bonus
✓ Number of Characters	Flat	$+(n*4)$	<input type="text" value="8"/>	+ 32
✓ Uppercase Letters	Cond/Incr	$+(len-n)*2$	<input type="text" value="1"/>	+ 14
⚡ Lowercase Letters	Cond/Incr	$+(len-n)*2$	<input type="text" value="6"/>	+ 4
✗ Numbers	Cond	$+(n*4)$	<input type="text" value="0"/>	0
✓ Symbols	Flat	$+(n*6)$	<input type="text" value="1"/>	+ 6
✓ Middle Numbers or Symbols	Flat	$+(n*2)$	<input type="text" value="1"/>	+ 2
✓ Requirements	Flat	$+(n*2)$	<input type="text" value="4"/>	+ 8

Deductions				
✓ Letters Only	Flat	$-n$	<input type="text" value="0"/>	0
✓ Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0
✓ Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="0"/>	0
✓ Consecutive Uppercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
⚠ Consecutive Lowercase Letters	Flat	$-(n*2)$	<input type="text" value="4"/>	- 8
✓ Consecutive Numbers	Flat	$-(n*2)$	<input type="text" value="0"/>	0
✓ Sequential Letters (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
✓ Sequential Numbers (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
✓ Sequential Symbols (3+)	Flat	$-(n*3)$	<input type="text" value="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.

Research: Brute Force Attacks

Definition and Mechanism

A brute force attack is a systematic cyber attack method where attackers attempt to crack passwords, login credentials, or encryption keys through exhaustive trial and error¹. This approach involves testing every possible combination of characters until the correct password is discovered, relying on computational "force" rather than sophisticated techniques².

Types of Brute Force Attacks

Simple Brute Force Attacks: Manual or automated attempts to guess credentials without sophisticated tools, typically targeting weak passwords like "password123"³.

Dictionary-Enhanced Brute Force: Combines systematic character testing with common word patterns, making attacks more efficient against predictable passwords⁴.

Reverse Brute Force: Starts with known passwords from data breaches and tests them against multiple usernames⁵.

Hybrid Attacks: Combines dictionary words with character variations, targeting passwords like "NewYork1993" or "Password@123"⁶.

Attack Process

Brute force attacks follow a systematic approach:

- Target selection and reconnaissance
- Tool deployment (John the Ripper, Hashcat, Hydra)
- Systematic password generation and testing
- Success confirmation and system access⁷

Time Requirements

The effectiveness of brute force attacks depends exponentially on password complexity:

- 4-character password: Under 1 minute
- 6-character password: Approximately 1 hour
- 8-character complex password: Several days
- 11+ character complex password: Months to years

Research: Dictionary Attacks

Definition and Operation

A dictionary attack is a password-cracking technique that utilizes predefined lists of common words, phrases, and previously compromised passwords⁹. Unlike brute force attacks that test every possible character combination, dictionary attacks focus on likely password candidates, making them more time-efficient¹⁰.

Attack Methodology

Dictionary attacks operate through a structured four-step process:

Wordlist Compilation: Attackers create comprehensive lists containing common passwords, dictionary words, names, and character substitution variations¹¹.

Target Acquisition: The attacker identifies password hashes or login systems to compromise¹².

Systematic Testing: Each word from the dictionary is systematically tested against the target system¹³.

Pattern Variations: Advanced attacks include common transformations like replacing "o" with "0" or adding numbers and symbols¹⁴.

Dictionary Types

Basic Dictionary Attack: Uses static lists of common words and phrases from actual dictionaries and popular password lists.

Hybrid Dictionary Attack: Combines dictionary words with transformations including character substitutions, case changes, and number/symbol additions.

Rainbow Table Attack: Employs precomputed hash tables for rapid password matching, though salt-protected systems resist this approach.

Common Tools

Popular dictionary attack tools include:

- **John the Ripper:** Versatile password recovery tool supporting multiple hash formats¹⁸.
- **Hydra:** Fast parallel brute-force tool for network services¹⁹.
- **Aircrack-ng:** Specialized Wi-Fi password recovery tool²⁰.
- **Medusa:** Modular authentication brute-forcer²¹.

Password Complexity Impact on Security

Character Diversity Benefits

Password complexity significantly enhances security by exponentially increasing the search space that attackers must explore^[22]. Each additional character type (uppercase letters, lowercase letters, numbers, symbols) multiplies possible combinations, making brute force attacks substantially more resource-intensive^[23].

Length vs. Complexity Analysis

Recent cybersecurity research indicates that **password length provides greater security benefits than complexity alone**^[24]. While complex passwords containing various character types strengthen security, longer passwords offer exponentially superior protection:

- 8-character complex password: 6.6×10^{15} combinations
- 12-character simple password: 4.7×10^{16} combinations
- 12-character complex password: 7.2×10^{23} combinations^[25]

Entropy and Unpredictability

Password complexity contributes to higher entropy—a measure of randomness and unpredictability^[26]. Complex passwords avoiding common words, predictable patterns, and personal information demonstrate significantly greater resistance to both dictionary and brute force attacks^[27].

Security Effectiveness

The testing results demonstrate clear security patterns:

High-Security Passwords (amrutha\$2L1, Maha@401126 Achieved excellent ratings through optimal length 11+ characters) combined with full character diversity.

Moderate-Security Passwords Prem#5so0 Demonstrated good security with balanced length and complexity.

Lower-Security Passwords Prem@sa): Limited effectiveness due to insufficient length despite character mixing.

Modern Security Recommendations

Current cybersecurity standards emphasize:

- **Minimum 12-character length** for optimal protection^[28]
- **Character diversity** including uppercase, lowercase, numbers, and symbols^[29]
- **Unpredictable patterns** avoiding dictionary words and personal information^[30]
- **Multi-factor authentication** as complementary protection^[31]

Analysis of Test Results

Security Pattern Analysis

The password testing revealed distinct security effectiveness patterns:

Length Dominance: Passwords exceeding 10 characters consistently achieved higher security ratings, regardless of complexity variations.

Character Mixing Impact: Passwords incorporating all four character types (uppercase, lowercase, numbers, symbols) demonstrated superior resistance to dictionary attacks.

Predictability Risks: Passwords containing recognizable names or patterns showed vulnerability despite meeting technical complexity requirements.

Practical Security Implications

amrutha\$2L1 and **Maha@401126** represent optimal password design, combining sufficient length with comprehensive character diversity. These passwords would require extensive computational resources for successful brute force attacks.

Prem#5so0 demonstrates acceptable security for most applications but could benefit from additional length for enhanced protection.

Prem@sa illustrates the security limitations of shorter passwords, even with symbol inclusion.

Security Recommendations

Based on the analysis findings, the following password security practices are recommended:

Individual Users

Prioritize length: Target minimum 12-character passwords

Implement character diversity: Include uppercase, lowercase, numbers, and symbols

Avoid predictable patterns: Eliminate dictionary words, names, and sequential characters

Enable multi-factor authentication: Add secondary verification layers

Use password managers: Generate and store complex, unique passwords

Organizations

Enforce comprehensive password policies emphasizing length over complexity alone

Implement account lockout mechanisms to prevent automated attacks

Deploy breach password monitoring to identify compromised credentials

Provide security awareness training on password best practices

Consider passwordless authentication for enhanced security

Conclusion

This password strength analysis demonstrates the critical importance of balancing length, complexity, and unpredictability in password security. The testing results confirm that passwords exceeding 10 characters with mixed character types provide superior protection against both brute force and dictionary attacks.

The research reveals that while complexity rules contribute to security, **password length provides the most significant protection enhancement**. Organizations and individuals should prioritize comprehensive password policies that emphasize length requirements while maintaining character diversity standards.

Modern cybersecurity requires understanding both attack methodologies and defensive strategies. The evolution of password-cracking techniques necessitates continuous adaptation of security practices, with multi-factor authentication and passwordless solutions representing the future of secure authentication.

Screenshot evidence of password testing from passwordmeter.com validates these findings, demonstrating the practical application of password security principles in real-world scenarios.