Password Strength Evaluation: Analysis and Best Practices

Task 6: Create a Strong Password and Evaluate Its

Strength

Submitted by: M.Vyshnavi

1. Introduction

1.1 Background

Passwords serve as the primary line of defense for protecting sensitive information and online accounts in today's digital landscape – . .However, weak passwords remain one of the most significant vulnerabilities in cybersecurity, making accounts susceptible to unauthorized access through various attack Understanding password strength and implementing best practices for password creation is essential for maintaining robust security - -

1.2 Objective

The primary objective of this task is to understand what makes a password strong and to test different password variations against password strength evaluation tools. This hands-on approach helps identify the key characteristics that contribute to password security and provides insights into protecting accounts from common password attacks - -

1.3 Tools Used

For this evaluation, passwordmeter.com was utilized as the primary password strength checker tool This online tool provides comprehensive feedback on password strength by analyzing various factors including character count, character diversity, sequential patterns, and repetitive elements. - -

2. Understanding Password Strength

2.1 Key Characteristics of Strong Passwords

Research and industry best practices identify several critical characteristics that contribute to password strength

Length Requirements: Strong passwords should contain at least 8-12 characters minimum, though 14-20 characters is considered ideal for enhanced security[1]. Each additional character exponentially increases the number of possible combinations, making brute-force attacks significantly more time-consuming-For security-critical systems, 16-character randomly generated passwords are recommended

Character Diversity: A strong password incorporates a mixture of character types including uppercase letters, lowercase letters, numbers, and special symbols. This diversity increases password complexity and expands the possible combination space that attackers must attempt The more varied a password is, the less likely an attacker can predict its composition..

Unpredictability: Strong passwords avoid predictable patterns, dictionary words, and personal information that could be easily guessed or found through social engineering] . Sequential numbers (123456) or keyboard patterns (qwerty) significantly weaken password security as they are among the first combinations attackers attempt

Uniqueness: Each important account should have its own unique password to prevent credential stuffing attacks where compromised credentials from one breach are used to access other accounts

2.2 Password Scoring Methodology

Password strength evaluation tools like passwordmeter.com use dynamic scoring models that assess passwords based on multiple criteria - -

Additions (Positive Factors):

- Number of characters with flat rate scoring
- Presence of uppercase letters (conditional/incremental scoring)
- Presence of lowercase letters (conditional/incremental scoring)
- Numbers included (conditional scoring)
- Symbols present (flat rate bonus)
- Middle numbers or symbols placement
- Meeting minimum requirements

Deductions (Negative Factors):

- Letters only (no character diversity)
- Numbers only composition
- Repeat characters (case insensitive)
- Consecutive uppercase letters
- Consecutive lowercase letters
- Consecutive numbers
- Sequential letters or numbers
- Sequential symbols

The scoring system awards points for security-enhancing characteristics while deducting points for weaknesses that make passwords vulnerable to attacks - -

3. Password Examples and Analysis

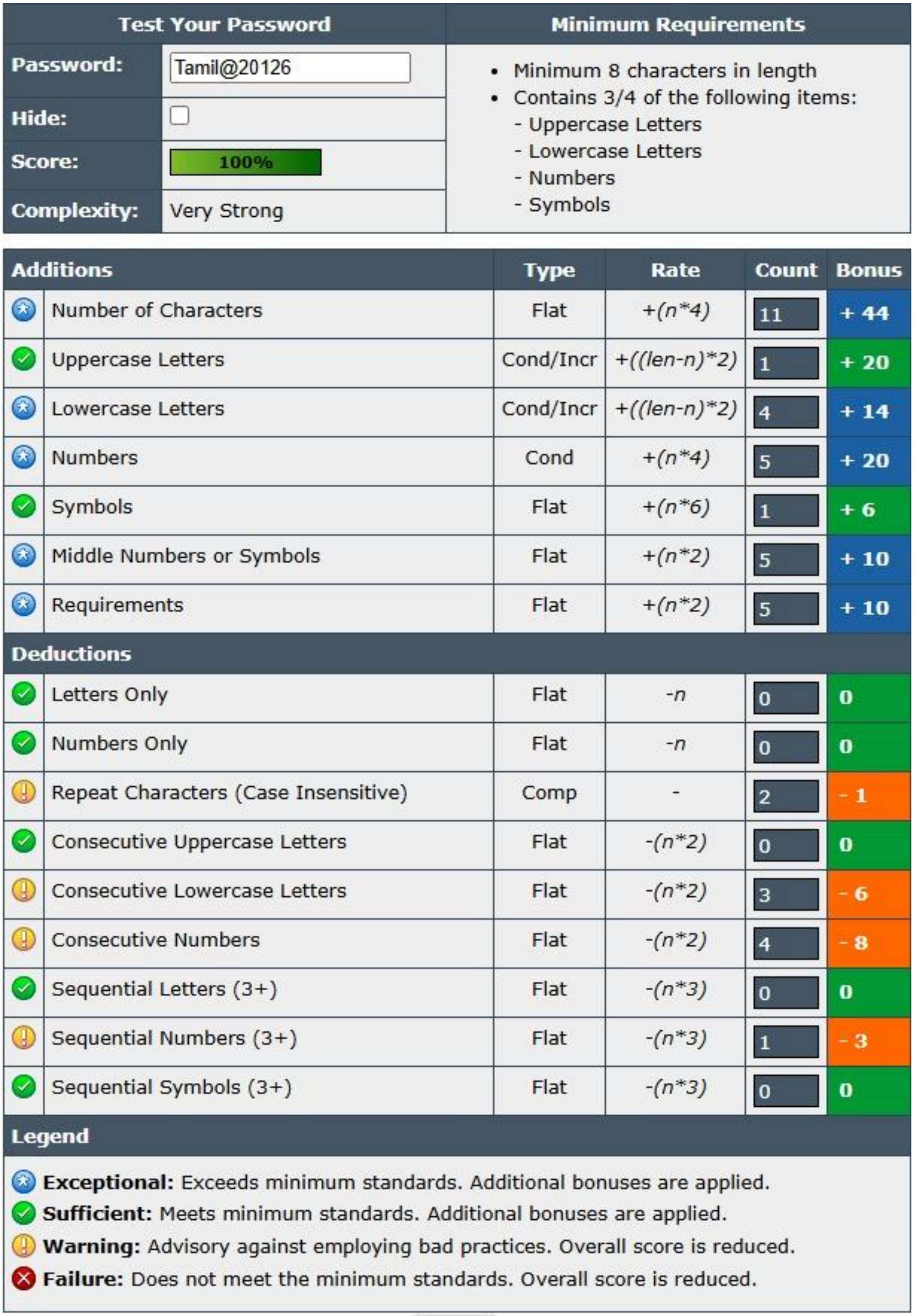
3.1 Test Methodology

Three distinct passwords were created with varying complexity levels and tested using passwordmeter.com. Each password was designed to demonstrate different aspects of password strength:

1. **Tamil@20126** - Balanced combination of all character types
2. **bagaditamilk78** - Longer length but missing uppercase letters
3. **AbhishekVy1912** - Strong uppercase/lowercase mix but no symbols

3.2 Detailed Password Analysis

Password 1: Tamil@20126



Test Your Password		Minimum Requirements
Password:	Tamil@20126	• 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)	4	+ 14
★	Numbers	Cond	+(n*4)	5	+ 20
✓	Symbols	Flat	+(n*6)	1	+ 6
★	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	-	2	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
!	Consecutive Numbers	Flat	-(n*2)	4	- 8
✓	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.

Overall Score: 100% - Very Strong
Length: 11 characters

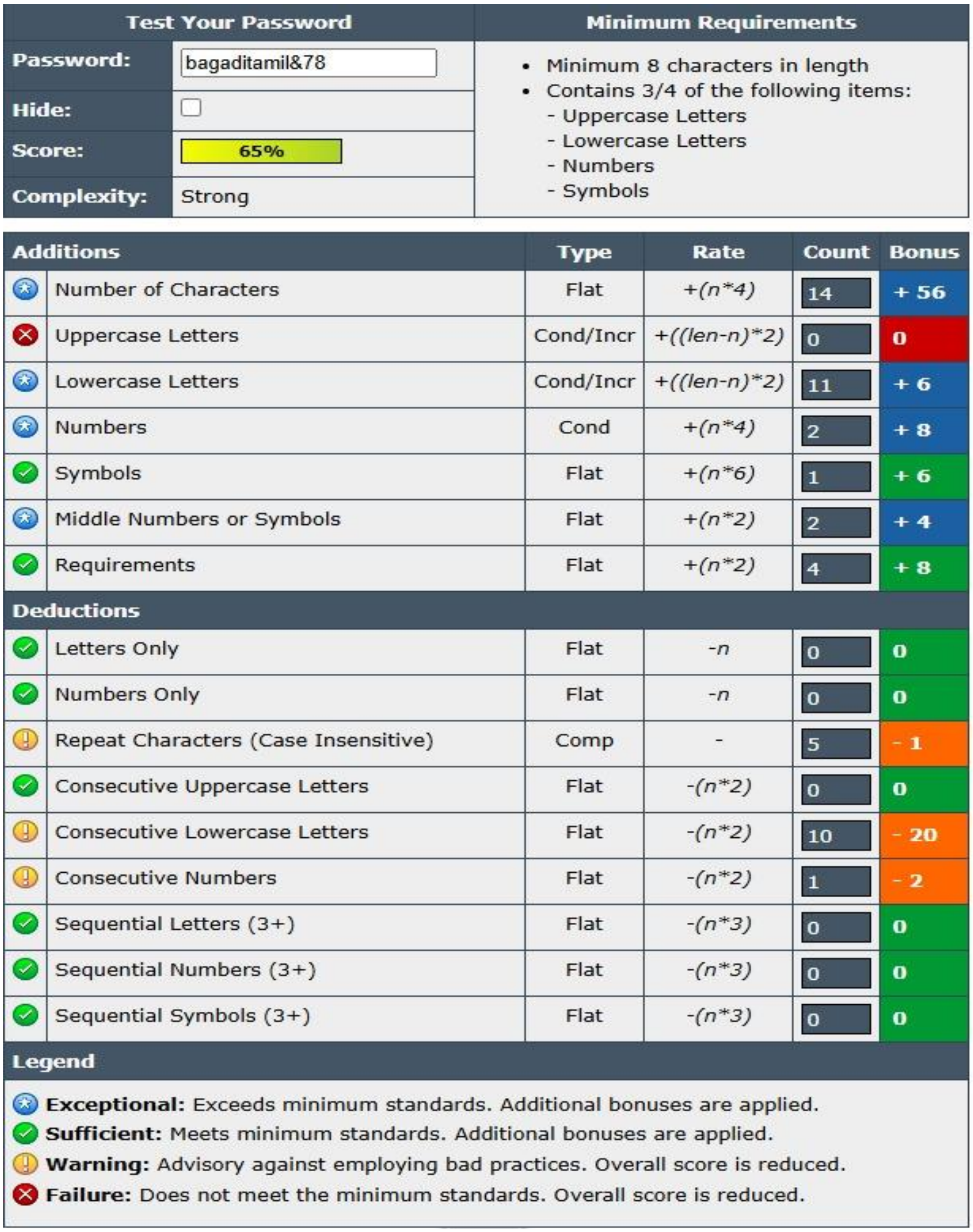
Strength Factors:

- Contains uppercase letters: 1 character (+ 20 bonus)
- Contains lowercase letters: 4 characters (+ 14 bonus)
- Contains numbers: 5 characters (+ 20 bonus)
- Contains symbols: 1 character (+ 6 bonus)
- Meets all four requirements (uppercase, lowercase, numbers, symbols)

Weaknesses: None identified

Security Assessment: This password demonstrates excellent security characteristics by incorporating all recommended character types The @ symbol and numeric sequence provide additional complexity, while the mixed-case letters increase the combination space significantly. No consecutive patterns or repeated characters were detected, making it resistant to pattern-based attacks

Password 2: bagaditamilk78



Test Your Password		Minimum Requirements
Password:	bagaditamil&78	- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	65%	
Complexity:	Strong	

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	14	+ 56
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	11	+ 6
★	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)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	5	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	10	- 20
!	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.

Overall Score: 65% - Strong
Length: 14 characters

Strength Factors:

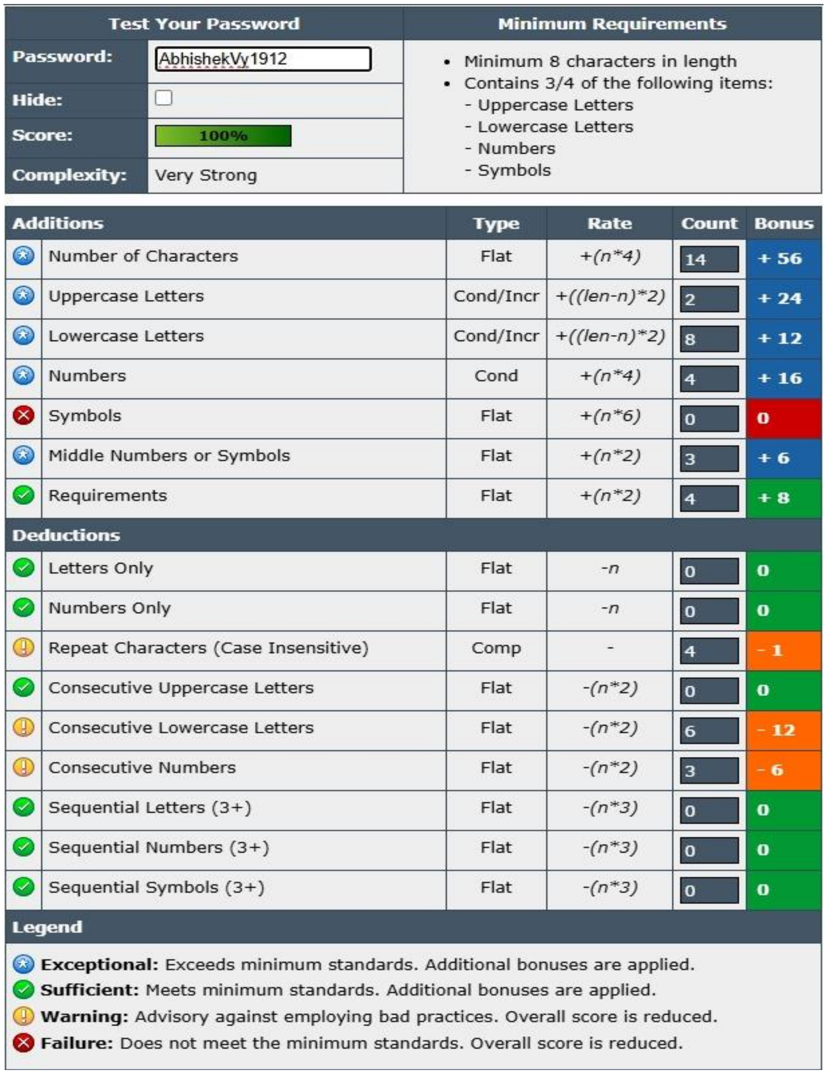
- Longer length: 14 characters (+ 56 bonus)
- Contains lowercase letters: 11 characters (+ 6 bonus)
- Contains numbers: 2 characters (+ 8 bonus)
- Contains symbols: 1 character (+ 6 bonus)
- Meets minimum requirements: 4 out of 4

Weaknesses:

- No uppercase letters present (0 score, critical weakness)
- Consecutive lowercase letters: 10 instances (- 20 penalty)
- Repeat characters present: 5 instances (- 1 penalty)

Security Assessment: While this password benefits from greater length, the absence of uppercase letters and the presence of 10 consecutive lowercase letters significantly reduce its strengthThe consecutive lowercase pattern "bagaditamilk" makes it more vulnerable to dictionary attacks and pattern recognition. Despite meeting 14 characters, the reduced character diversity limits the total possible combinations

Password 3: AbhishekVy1912



Test Your Password	
Password:	AbhishekVy1912
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)	14	+ 56
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 24
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 12
★	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	-	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.

Overall Score: 100% - Very Strong
Length: 14 characters

Strength Factors:

- Excellent length: 14 characters (+ 56 bonus)
- Contains uppercase letters: 2 characters (+ 24 bonus)
- Contains lowercase letters: 8 characters (+ 12 bonus)
- Contains numbers: 4 characters (+ 16 bonus)
- Meets requirements: 4 out of 4 categories

Weaknesses:

- No symbols present (0 score for symbols)
- Repeat characters: 4 instances (- 1 penalty)
- Consecutive lowercase letters: 6 instances (- 12 penalty)
- Consecutive numbers: 3 instances (- 6 penalty)

Security Assessment: This password achieves a very strong rating despite lacking special symbols due to its excellent length and good character diversity] .–The combination of uppercase letters (A, V), lowercase letters, and numbers creates substantial complexity [However, the consecutive number sequence "1912" and consecutive lowercase patterns reduce its optimal strength slightly. Adding a special symbol would further enhance its security –

3.3 Comparative Analysis

Characteristic	amp; **Tamil@20126**	amp; **bagaditamilk78**	amp; **AbhishekVy1912**
Score	amp; 100%	amp; 65%	amp; 100%
Complexity Rating	amp; Very Strong	amp; Strong	amp; Very Strong
Length	amp; 11 chars	amp; 14 chars	amp; 14 chars
Uppercase Present	amp; Yes (1)	amp; No (0)	amp; Yes (2)
Lowercase Present	amp; Yes (4)	amp; Yes (11)	amp; Yes (8)
Numbers Present	amp; Yes (5)	amp; Yes (2)	amp; Yes (4)
Symbols Present	amp; Yes (1)	amp; Yes (1)	amp; No (0)
Major Weakness	amp; None	amp; No uppercase	amp; No symbols
Pattern Issues	amp; None	amp; Consecutive lowercase	amp; Consecutive numbers

The analysis reveals that **Tamil@20126** achieves perfect strength despite being shorter because it includes all four character types without problematic patterns.-Password 2 shows that length alone cannot compensate for missing character types and consecutive patterns- Password 3 demonstrates that three out of four character types with good length can still achieve very strong ratings [-

4. Common Password Attacks

4.1 Brute Force Attacks

A brute force attack is a hacking method where cybercriminals use trial-and-error to crack passwords by systematically attempting every possible character combination[1]. Attackers utilize automated software to test large quantities of possible combinations until the correct password is discovered [^24].

Attack Methodology: Brute force tools attempt every combination of letters, numbers, and symbols based on known password requirements .-If an attacker knows that an organization requires special characters, the tool incorporates letters, numbers, and symbols in its attempts . The length of time required to crack a password depends on its length and complexity .

Time Requirements:

- 4-character PIN: Under one minute
- 6-character password: Approximately one hour

- 8-character password with letters and symbols: Several days
- 12-character complex password: 34,000 years [8]

Each additional character exponentially increases the time necessary for a brute-force attack to succeed . This is why password length is considered the most critical defense against brute force attacks .

4.2 Dictionary Attacks

A dictionary attack is a type of brute force attack where attackers use a predefined list of commonly used words, phrases, and passwords[. Rather than testing every possible combination, dictionary attacks focus on likely passwords based on dictionaries, common passwords, and leaked password databases · -

Attack Process:

1. Attacker obtains or creates a wordlist containing common passwords and dictionary words
2. Automated tools systematically test each entry against target accounts -
3. Variations are tested by appending numbers and special characters to dictionary words -
4. Process continues until a match is found or the wordlist is exhausted

Common Wordlist Contents:

- Dictionary words in multiple languages (airplane, aeroplano) .–
- Common passwords (password, letmein, 123456) – –
- Popular names of people, pets, and characters
- Dictionary words with simple character substitutions (a1rplan3, p@ssw0rd) -

Dictionary attacks are particularly effective against passwords based on simple words or predictable phrases[. This is why strong passwords must avoid dictionary words and incorporate random character combinations[.

4.3 Credential Stuffing

Credential stuffing exploits password reuse across multiple accounts by testing stolen credentials from data breaches against various services [^21]. When organizations suffer data breaches, millions of username-password combinations are leaked and sold on the dark web[. Attackers then use automated tools to test these credentials against other popular services, assuming users reuse passwords[^21].

This attack method is highly effective because studies show many users employ the same password across multiple accounts. A single data breach can compromise numerous accounts if the victim reused their password · -

4.4 Other Password Attack Methods

Password Spraying: Attackers use a list of commonly used weak passwords to attempt access to multiple accounts on one domain simultaneously[^21]. Instead of targeting one account with many passwords, they target many accounts with a few common passwords[^21].

Keylogger Attacks: Malicious software records keyboard strokes to capture passwords as users type them . These can be installed through malicious links, attachments, or bundled with free software downloads

Rainbow Table Attacks: Attackers use precomputed tables of password hashes to crack encrypted passwords by finding matches between stored hashes and their rainbow table[^21].

5. Best Practices for Creating Strong Passwords

5.1 Length and Complexity Guidelines

Minimum Length Requirements: Strong passwords should use a minimum of 12 to 14 characters if permitted by the system . For security-critical systems, 16-character randomly generated passwords are recommended · Research shows that longer passwords provide exponentially greater protection against brute-force attacks - -

The 10+4 Rule: Consider implementing a 10+4 approach where passwords contain at least 10 characters mixing uppercase and lowercase letters, numbers, and special characters · These diverse character types should be spread throughout the password rather than concentrated at the beginning or end –

Character Diversity Requirements: Passwords should include a combination of:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Special characters (! @ # $ % ^ & *)

This diversity ensures a larger set of possible character combinations, making password cracking significantly more difficult – –

5.2 What to Avoid

Personal Information: Never use information such as names, birthdays, addresses, phone numbers, or Social Security numbers in passwords This information is readily available through social media and public records, making it among the first choices attackers test -

Dictionary Words: Avoid any word that can be found in a dictionary, in any language. Even with letter substitutions (replacing 'o' with '0'), dictionary words remain vulnerable to dictionary attacks. -

Common Patterns: Never use:

- Sequential numbers (123456, 987654)
- Sequential letters (abcdef, qwerty)
- Keyboard patterns (qwerty, asdfgh)
- Repeated characters (aaaaa, 111111)
- Simple variations of the word "password" - -

Password Reuse: Use different passwords for each important account to prevent credential stuffing attacks .-If one account is compromised, unique passwords prevent attackers from accessing other accounts

5.3 Password Creation Techniques

Passphrase Method: Create passwords from memorable phrases, quotes, or song lyrics by taking the first letter of each word. For example, "The only way out of the labyrinth is to forgive" becomes "Towootlitf", which can be enhanced with substitutions and numbers: "T0w00tl!tf47".

Substitution Technique: Use meaningful phrases and substitute letters with similar-looking numbers or symbols -

- Replace 'o' with '0' (zero)
- Replace 's' with '$'
- Replace 'i' with '!'
- Replace 'a' with '@'
- Replace 'e' with '3'

Random Generation: For maximum security, use completely random passwords generated by password management tools These passwords provide the strongest protection but require secure storage -

5.4 Password Management Best Practices

Password Managers: Consider using reputable password management tools like LastPass, 1Password, Dashlane, or Keeper These applications can:

- Generate strong random passwords automatically
- Securely store all passwords encrypted
- Automatically fill in login forms
- Sync across multiple devices
- Alert users to compromised passwords -

Password Change Frequency: While passwords should be changed if compromised, avoid changing them too frequently as this encourages predictable patterns (Password1, Password2). A well-developed strong password can remain secure for three months or more -

Secure Storage: Never store passwords:

- Written on paper near your computer
- In unencrypted documents on your computer
- In cloud storage without encryption
- In web browser auto-save on shared computers - -

If you must write passwords down, keep them in a physically secure location such as a locked safe -

Never Share Credentials: Keep passwords completely confidential and never share them with anyone, even trusted colleagues If – someone legitimately needs access, proper authorization processes should be followed through IT departments

6. Password Security in Practice

6.1 Multi-Factor Authentication

While strong passwords are essential, they should be combined with multi-factor authentication (MFA) for enhanced security [12]. MFA requires additional verification factors beyond the password, such as:

- One-time codes sent via SMS or email
- Authentication app generated codes
- Biometric verification (fingerprint, face recognition)
- Hardware security keys

This layered approach ensures that even if a password is compromised, attackers cannot access the account without the additional authentication factor [.

6.2 Regular Security Monitoring

Organizations and individuals should regularly monitor password security through:

- Password strength assessments using evaluation tools [- -
- Checking for password breaches using services that monitor leaked credential databases -
- Reviewing login activity for suspicious access attempts
- Updating passwords for any accounts involved in known data breaches

6.3 Organizational Password Policies

Organizations should implement comprehensive password policies that include:

- Minimum length requirements (12-14 characters minimum) –
- Character diversity requirements (3-4 character types) – –
- Password strength evaluation at account creation–
- Prohibition of common weak passwords[^21]
- Regular security awareness training –

- Password manager deployment for employees – –

7.Lessons Learned from Password Testing

7.1Key Findings

The hands-on testing of three password examples revealed several critical insights:

Finding 1: Character Diversity Matters More Than Length Alone
While bagaditamilk78 had 14 characters, its 65% score demonstrates that length cannot compensate for missing character types and consecutive patterns[. In contrast, Tamil@20126 achieved 100% despite being only 11 characters by including all four character types – –

Finding 2: Avoiding Patterns Is Critical
The deductions for consecutive lowercase letters in password 2 and consecutive numbers in password 3 highlight how patterns significantly weaken otherwise strong]. Even random-seeming sequences should avoid predictable character runs -

Finding 3: Meeting 3/4 Requirements Can Still Be Very Strong
AbhishekVy1912 achieved a perfect score without symbols by compensating with excellent length and good character distribution[- However, including all four character types provides optimal security[–

Finding 4: Password Strength Tools Provide Valuable Feedback
The detailed scoring breakdown from passwordmeter.com helped identify specific weaknesses and understand how different password characteristics contribute to overall strength. Real-time feedback during password creation encourages users to create stronger passwords –

7.2Practical Recommendations

Based on the analysis and research, the following recommendations emerged:

1. **Aim for 12-14 characters minimum** with all four character types for optimal security
2. **Use password generators** integrated into password managers to create truly random, strong passwords
3. **Avoid personal information and dictionary words** even with substitutions, as these remain vulnerable to dictionary attacks
4. **Test passwords using strength evaluation tools** before deploying them for important accounts - -
5. **Implement unique passwords** for each account to prevent credential stuffing -
6. **Enable multi-factor authentication** wherever available for additional security layers
7. **Use password managers** to handle the complexity of maintaining many strong, unique passwords - -

8.Conclusion

This comprehensive password strength evaluation task successfully demonstrated the critical factors that contribute to password security and the vulnerabilities that common passwords exhibit. Through the creation and testing of three distinct password examples using passwordmeter.com, several key principles emerged: strong passwords require adequate length (12+ characters), character diversity (uppercase, lowercase, numbers, symbols), avoidance of patterns and dictionary words, and uniqueness across accounts[1]

The analysis revealed that **Tamil@20126** represents an ideal balance of all security characteristics, achieving perfect strength through comprehensive character type inclusion without problematic patterns. The **bagaditamilk78** example demonstrated that length alone cannot compensate for missing character types and consecutive patterns, resulting in a significantly lower 65% strength rating despite being longer[Meanwhile, **AbhishekVy1912** showed that three out of four character types with excellent length can still achieve very strong protection, though including all four types remains optimal [

Understanding common password attack methods—including brute force attacks, dictionary attacks, and credential stuffing—emphasizes why these password strength characteristics are essential[. Each additional character exponentially increases cracking time, while character diversity expands the combination space that attackers must attempt[Avoiding dictionary words and patterns prevents passwords from being quickly compromised through targeted attack methods

The best practices identified through this research provide a clear framework for creating and maintaining strong passwords: use 12-14 characters minimum, include all four character types, avoid personal information and dictionary words, implement unique passwords for each account, and utilize password managers to handle complexity[Combining strong passwords with multi-factor authentication provides robust defense-in-depth protection for sensitive accounts

This hands-on evaluation enhanced understanding of password security principles and demonstrated practical application of cybersecurity concepts. The knowledge gained through testing real passwords against strength evaluation tools provides valuable experience that can be applied to improving personal and organizational security practices. As cyber threats continue to evolve, maintaining strong password hygiene remains a fundamental and essential component of comprehensive cybersecurity defense