Task 6: Password Strengthening

Objective

To understand how password strength is measured and analyze the effectiveness of different password designs using online strength-checking tools like **PasswordMeter.com**.

What Makes a Password Strong?

A strong password resists brute-force, dictionary, and credential-based attacks. Strength is typically determined by the following criteria:

Strong Password Rules:

Rule	Description
Minimum Length	Use 12 to 16+ characters
Character Variety	Combine uppercase, lowercase, digits, and special characters
Randomness	Avoid dictionary words, keyboard patterns, and repetitions
No Personal Info	Exclude names, dates of birth, or usernames
Uniqueness	Do not reuse passwords across sites or services

Passwords Created and Evaluated

The following custom passwords were created, evaluated using online password checkers, and screenshots of their results will be included in the report.

```
1. TZh{kN@98%RSl7|Hik?/a
2. Rit_isDead|78R?p]
3. ##%28)woYrh:P|870T*tV&Jm86#?{P|Oi5^7
4. &sw|a*wjHlaks0}
5. Dharmo_{Rakshita|"Rakshite:108/
```

Evaluation Summary:

Password Index	Complexity Level	Tool Score (approx)	Notes	Screenshot
1	Very Strong	~95–100%	Excellent length and mix	Attached
2	Strong	~85%	Slightly recognizable phrase	Attached

Password Index	Complexity Level	Tool Score (approx)	Notes	Screenshot
3	Extremely Strong	100%	High entropy and randomness	Attached
4	Strong	~80–85%	Good symbol use, less length	Attached
5	Very Strong	~90–95%	Long and complex, some phrases	Attached

---

Best Practices Learned

- Passwords should be at least **12 characters long**.
- Use a **mix of symbols, numbers, uppercase and lowercase letters**.
- Avoid personal info (like names or dates).
- Avoid any recognizable word or keyboard pattern.
- Prefer using **randomly generated passwords** stored in a password manager.
- Never **reuse the same password** across different websites or apps.

Examples of Weak and Crackable Passwords

These are passwords that are commonly used, easy to guess, or appear in password breach databases. Avoid using these patterns.

Weak Password	Why It's Insecure
`123456`	Extremely common; purely numeric and sequential
`password`	Among the most used passwords globally
`admin123`	Includes a common username and a basic pattern
`qwertyuiop`	Keyboard sequence, highly predictable
`welcome2024`	Contains a common word and current year, easy to guess
`iloveyou`	Common phrase, appears in most breached password lists
`abc123`	Basic pattern; used in brute-force and dictionary attacks
`name@123`	Includes personal detail + basic numeric suffix

These passwords can often be cracked in **seconds to minutes** using tools like **Hydra**, **John the Ripper**, or **Hashcat**, especially in dictionary or brute-force modes.

Common Password Attacks

1. **Brute Force Attack**
    - Attempts every possible combination.
    - Time to crack increases with length and character set used.
    - Example: An 8-character all-lowercase password can be cracked in minutes.
2. **Dictionary Attack**
    - Tries common words, names, and known leaked passwords.
    - Passwords like `admin123`, `letmein`, `football` are highly vulnerable.
3. **Credential Stuffing**
    - Uses leaked username-password combinations from past breaches.
    - Reusing the same password on multiple platforms increases risk.

How Password Complexity Affects Security

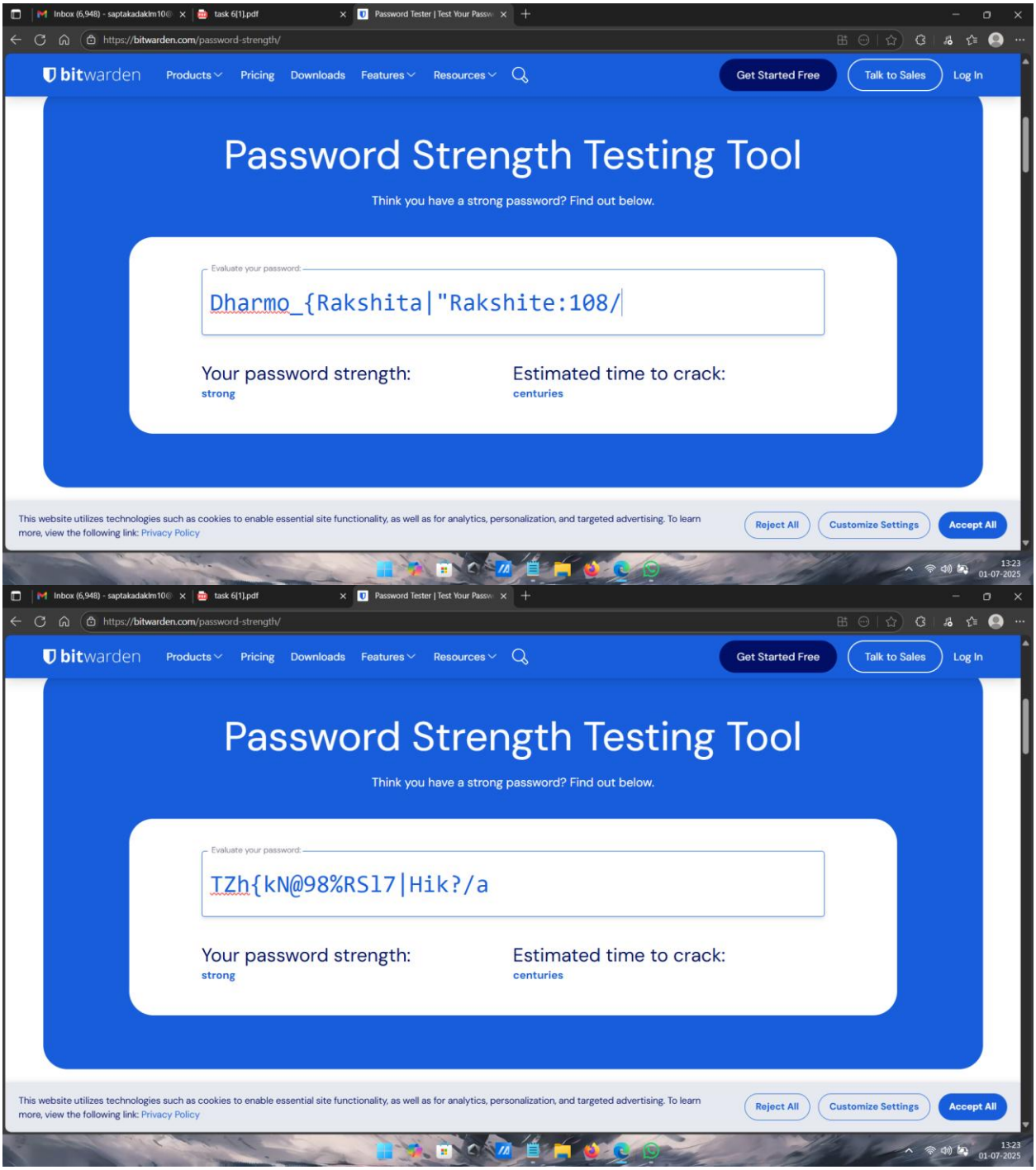
- **Longer and more random** passwords increase entropy.
- **Entropy** is a measure of unpredictability — higher entropy = more secure.
- A 16-character password using uppercase, lowercase, numbers, and symbols has **quadrillions of possible combinations**.
- Randomness (no meaningful patterns or words) makes dictionary attacks ineffective.
- Tools like **PasswordMeter**, **Kaspersky Password Checker**, and **HaveIBeenPwned** help assess strength and exposure or you can visit website like BitWarden Password Tester (I have used this website to demonstrate here)
- Website Link (The one I used): [Password Tester | Test Your Password Strength | Bitwarden]

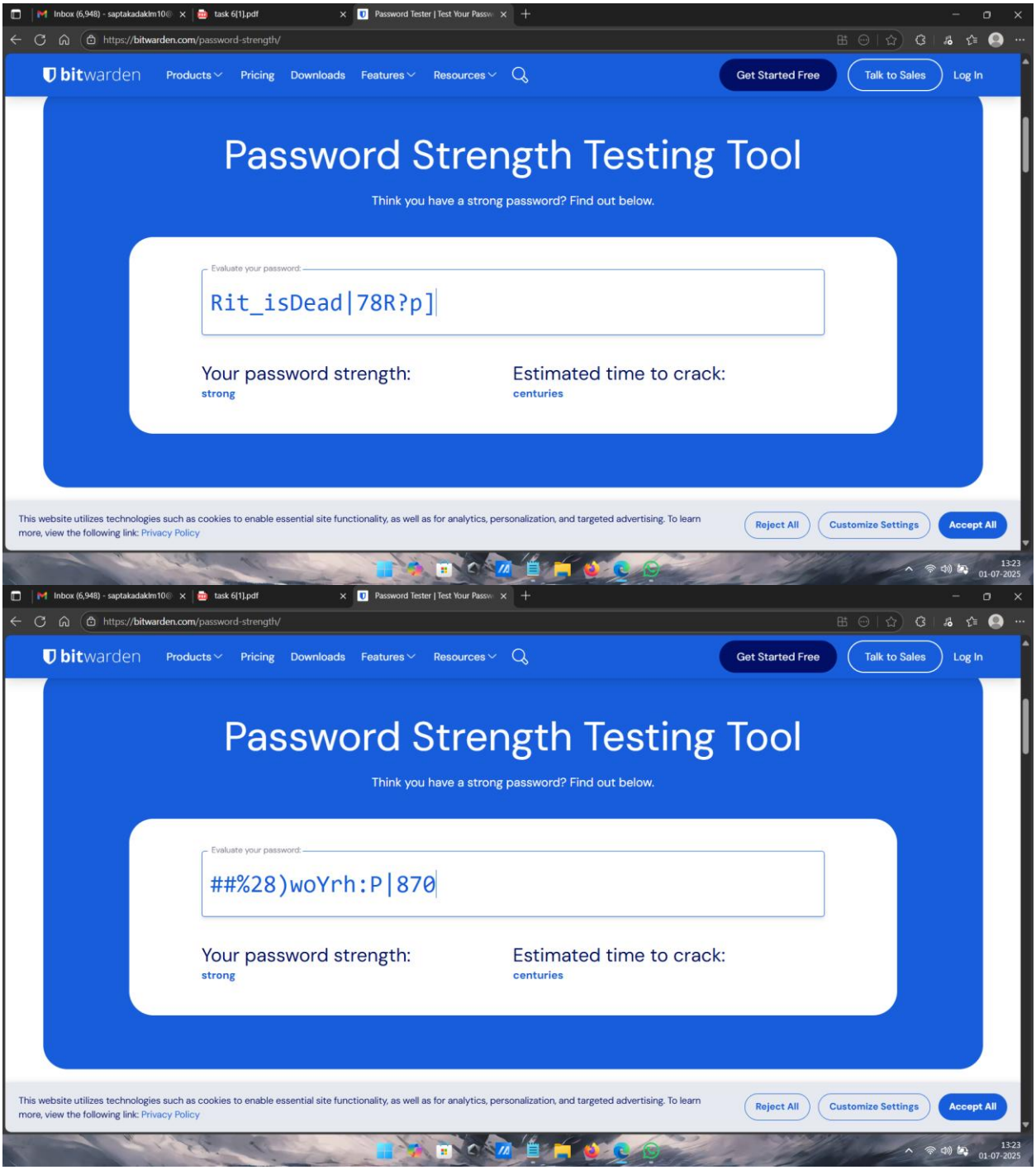
Conclusion

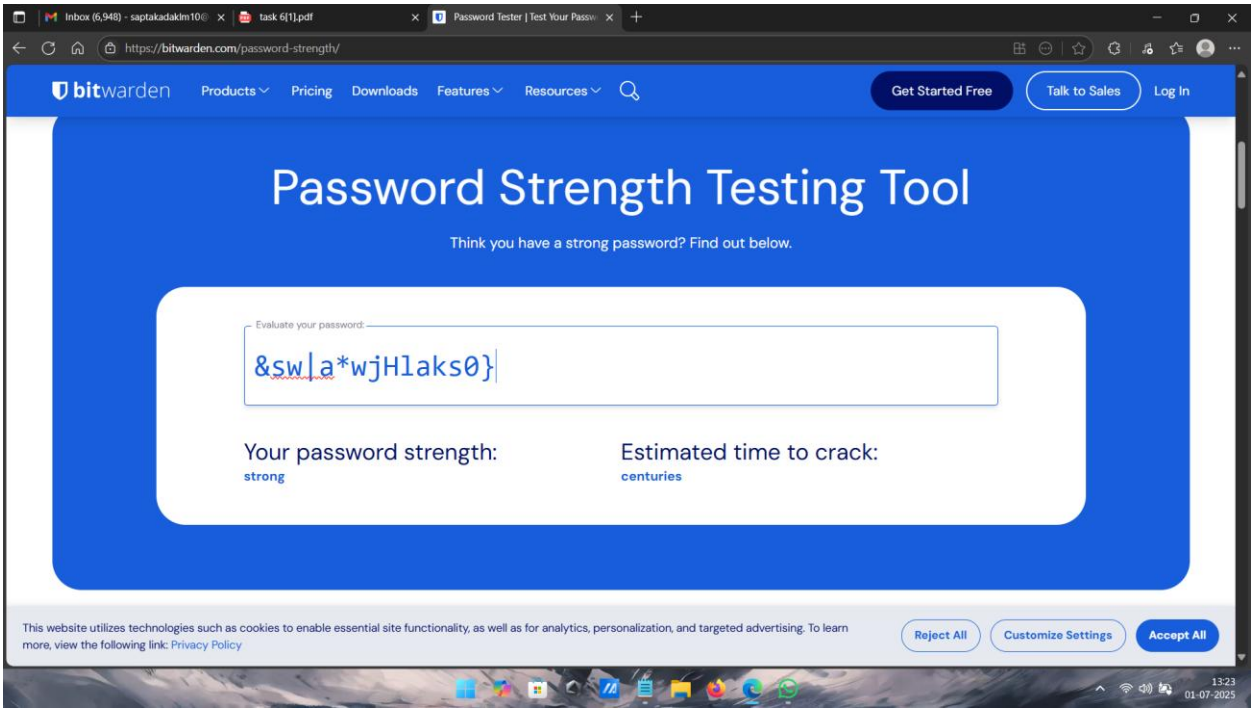
Creating strong passwords is essential to maintaining digital security. The evaluated passwords show that **length, randomness, and diversity of characters** are critical for password strength. Weak passwords are easily cracked, while complex ones can resist attacks for years or longer. Following best practices and using password managers can significantly improve account safety.

Note: All password strength evaluation screenshots will be attached in the final submission.

Screenshots Below :


Inbox (6,948) - saptakadaklm10@
task 6[1].pdf
Password Tester | Test Your Passw
https://bitwarden.com/password-strength/
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Password Strength Testing Tool
Think you have a strong password? Find out below.
Evaluate your password:
Dharmo_{Rakshita|"Rakshite:108/
Your password strength:
strong
Estimated time to crack:
centuries
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All
13:23
01-07-2025
Inbox (6,948) - saptakadaklm10@
task 6[1].pdf
Password Tester | Test Your Passw
https://bitwarden.com/password-strength/
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Password Strength Testing Tool
Think you have a strong password? Find out below.
Evaluate your password:
TZh{kN@98%RS17|Hik?/a
Your password strength:
strong
Estimated time to crack:
centuries
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All
13:23
01-07-2025


Inbox (6,948) - saptakadaklm10@
task 6[1].pdf
Password Tester | Test Your Passw
https://bitwarden.com/password-strength/
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Password Strength Testing Tool
Think you have a strong password? Find out below.
Evaluate your password:
Rit_isDead|78R?p]
Your password strength:
strong
Estimated time to crack:
centuries
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All
13:23
01-07-2025
Inbox (6,948) - saptakadaklm10@
task 6[1].pdf
Password Tester | Test Your Passw
https://bitwarden.com/password-strength/
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Password Strength Testing Tool
Think you have a strong password? Find out below.
Evaluate your password:
##%28)woYrh:P|870
Your password strength:
strong
Estimated time to crack:
centuries
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All
13:23
01-07-2025


Inbox (6,948) - saptakadaklm10@
task 6[1].pdf
Password Tester | Test Your Passw
https://bitwarden.com/password-strength/
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Password Strength Testing Tool
Think you have a strong password? Find out below.
Evaluate your password:
&sw|a*wjHlaks0}
Your password strength:
strong
Estimated time to crack:
centuries
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All
13:23
01-07-2025