

TASK-7

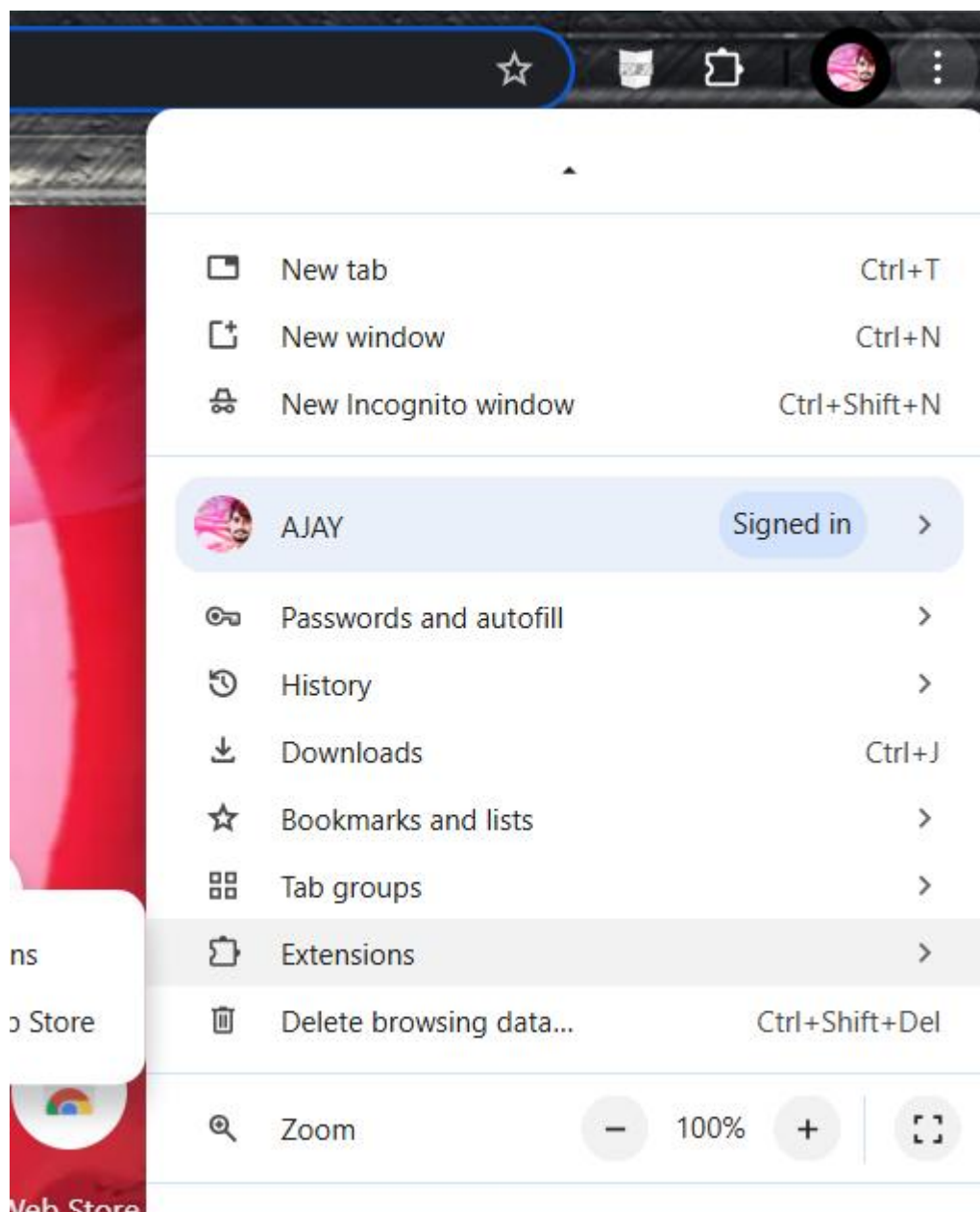
THESE EXTENSIONS ARE USED TO ENHANCE THE WORK AND SIMPLY THE WORK TO SURF OVER THE INTERNET

AND THESE ALSO TAKE CERTAIN PERMISSIONS WHICH WE ARE UNAWARE SOMETIMES


DUE TO THIS MANY PRIVACY COMPLICATIONS TAKE PLACE

WHERE IT MAY LEAD TO EVEN STEALING OF PERSONAL DATA AND STEALING CREDENTIALS ALSO

BELOW ATTACHED SCREENSHOTS ARE THE BROWSER EXTENSIONS WHICH I AM USING AND WHAT PERMISSIONS I GIVE TO THEM




All extensions



AdBlock — block ads across the web
Block ads on YouTube and your favorite sites for free

Details Remove


On



ChatGPT search
Change default search engine to ChatGPT search.

Details Remove


Off



Chrome Remote Desktop
Chrome Remote Desktop extension

Details Remove


On



Google Docs Offline
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.

Details Remove


On



Open in Firefox™ Browser
Open current page, link, or all tabs in the Firefox browser with a left-click or through right-click context menu.

Details Remove


On



PDF Viewer
Uses HTML5 to display PDF files directly in the browser.

Details Remove

On

←  **AdBlock — block ads across the web**

On On

Description
Block ads on YouTube and your favorite sites for free

Version
6.23.0


Size
266 MB

Permissions

- Read and change all your data on all websites
- Display notifications

Site access

Allow this extension to read and change all your data on websites that you visit: ? On all sites

Site settings 

Pin to toolbar Off

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable Off

Resources

The Cyber Scheme

JavaScript Obfuscator

Caesar Cipher Shift

CyberChef

Google dork cheats

Shodan Account

Shodan Account

All Bookmarks

Extensions

My extensions

Keyboard shortcuts

Discover more extensions and themes on the [Chrome Web Store](#)

Search extensions

Chrome Remote Desktop

On

Description
Chrome Remote Desktop extension

Version
2.1

Size
< 1 MB

Permissions

- Manage your downloads
- Communicate with cooperating native applications

Site access
This extension has no additional site access

Site settings

Pin to toolbar

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable

Developer mode

Search extensions

PDF Viewer

On

Description
Uses HTML5 to display PDF files directly in the browser.

Version
4.6.129

Size
8.4 MB

Permissions

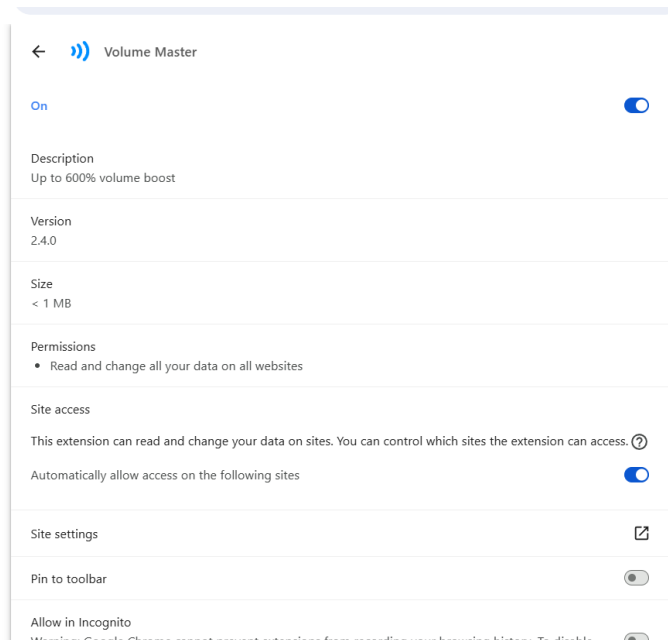
- Read your browsing history

Site access
Allow this extension to read and change all your data on websites that you visit: ? On all sites

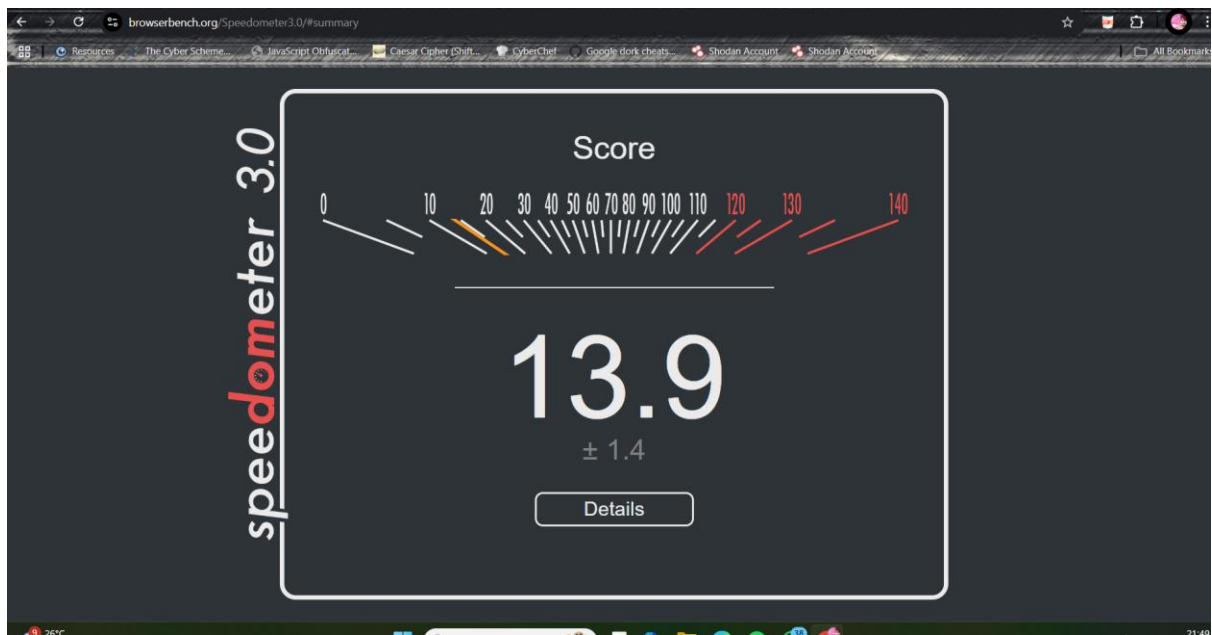
Site settings

Pin to toolbar

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.



BROWSER SPEED CHECKING AFTER INSPECTING ALL THE EXTENSIONS



Interview Questions:

1. How can browser extensions pose security risks?
2. What permissions should raise suspicion?
3. How to safely install browser extensions?
4. What is extension sandboxing?
5. Can extensions steal passwords?
6. How to update extensions securely?
7. Difference between extensions and plugins?
8. How to report malicious extensions?

1. How can browser extensions pose security risks?

As a Cyber Security student, I understand that browser extensions can act as potential attack vectors. Malicious extensions may access sensitive data such as browsing history, cookies, login credentials, and even inject scripts into webpages. If not properly vetted, they can be used for data exfiltration, surveillance, or launching phishing attacks.

2. What permissions should raise suspicion?

Suspicious permissions include access to:

- All website data (Read and change all your data on the websites you visit)
 - Clipboard access
 - Background activity
 - Access to tabs and browsing activity
 - Downloads or file system access
- Such permissions, especially when unrelated to the extension's core function, may indicate malicious intent.
-

3. How to safely install browser extensions?

To install browser extensions safely:

- Only use official web stores (like Chrome Web Store or Mozilla Add-ons).
 - Check developer reputation and reviews.
 - Review the requested permissions.
 - Avoid installing too many extensions.
 - Regularly audit and remove unused or outdated ones.
-

4. What is extension sandboxing?

Extension sandboxing is a security mechanism that isolates extensions from each other and from sensitive browser functions. It limits their access to system resources and user data unless explicitly granted, reducing the impact of a compromised or malicious extension.

5. Can extensions steal passwords?

Yes, if an extension is malicious or poorly designed, it can potentially access and exfiltrate passwords by:

- Reading input fields on login pages
 - Accessing the clipboard if passwords are copied
 - Capturing keystrokes
- Hence, it's crucial to minimize permissions and use password managers with autofill protection.
-

6. How to update extensions securely?

Secure updating involves:

- Enabling auto-updates from official extension stores
 - Avoiding third-party sources or sideloading
 - Regularly checking changelogs and developer authenticity
 - Using browsers that validate extension updates via signatures
-

7. Difference between extensions and plugins?

- **Extensions** are JavaScript-based and run within the browser, enhancing user experience (e.g., ad blockers, password managers).
 - **Plugins** are external components that handle special content types like Flash or Java, and are now largely deprecated due to security risks.
-

8. How to report malicious extensions?

To report a malicious extension:

- Use the browser's official reporting tools (e.g., "Report abuse" option in Chrome Web Store).
 - Provide a detailed explanation and screenshots if needed.
 - Notify your organization's security team if installed on a corporate device.
 - Optionally, report it to CERT or similar cyber response teams if it's part of a larger attack.
-