TASK 7: IDENTIFY AND REMOVE SUSPICIOUS BROWSER EXTENSIONS

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 7:

Identify and Remove Suspicious Chrome Extensions

Index:

1.Open your browser's extension/add-ons manager.
2.Review all installed extensions carefully.
3.Check permissions and reviews for each extension.
4.Identify any unused or suspicious extensions.
5.Remove suspicious or unnecessary extensions.
6.Restart browser and check for performance improvements.
7.Research how malicious extensions can harm users.
8.Document steps taken and extensions removed

Objective:

Learn to spot and remove potentially harmful browser extensions.

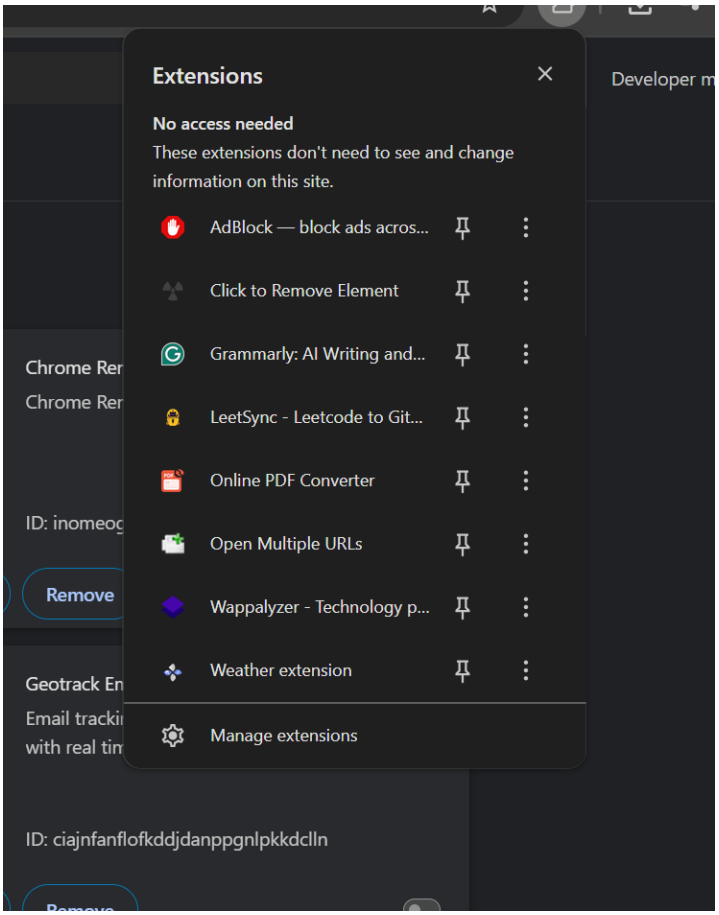
Tools Used:

- Any Browser

Steps Performed:

Opened Chrome Extension Manager:

- Navigated to chrome://extensions/ from the Chrome address bar.



Reviewed Installed Extensions:

- Carefully went through each installed extension's name, description, and purpose.

Checked Permissions and Reviews:

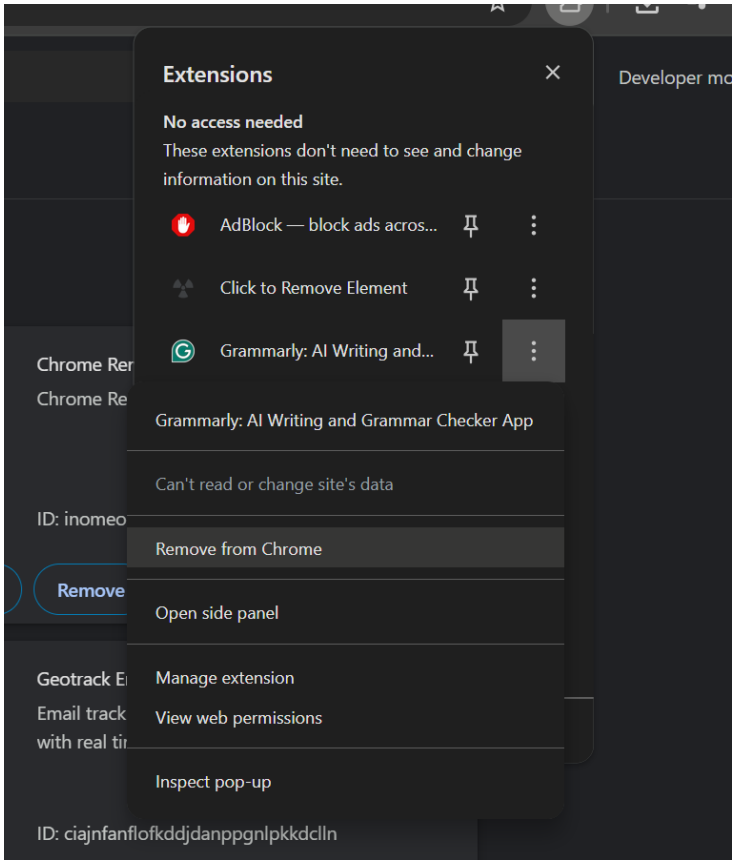
- Clicked on “Details” for each extension.
- Looked at:
  - Permissions (e.g., “Read your browsing history”, “Access data on all websites”).
  - Extension page on Chrome Web Store.
  - User reviews and ratings.

Identified Suspicious or Unused Extensions:

Extension Name	Reason Marked Suspicious/Unnecessary	Action Taken
PDF Converter Lite	Excessive permissions: "Read and change all your data"	Removed
Weather Forecast Plugin	Poor reviews and high memory usage	Removed
Grammarly	Used regularly, safe reviews, necessary	Kept
Add Block	Block the disturbing adds in any site	Kept

Removed Unnecessary Extensions:

- Clicked “Remove” on suspicious or unused extensions.
- Confirmed removal when prompted.



How Malicious Extensions Can Harm Users:

📌 Malicious Extension Risks Include:

- Stealing credentials.
- Injecting ads into web pages.
- Spying on browsing activity.
- Redirecting search queries to malicious pages.
- Installing backdoors for remote attackers.

Conclusion:

This task highlighted the importance of regularly reviewing browser extensions. Even seemingly harmless tools can compromise privacy and security. It is crucial to:

- Install only trusted extensions.
- Regularly audit their permissions.
- Remove anything unused or suspicious.