Task 7th: Identify and Remove Suspicious Browser Extensions

7th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

NAME	**SANDEEP MEWARA**
Submitted to:	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

REPORT SUBMITTED TO

As part of the Cyber Security Internship, I have completed " Task 7th: Identify and Remove Suspicious Browser Extensions " by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 7th: Identify and Remove Suspicious Browser Extensions

1. Introduction

This report outlines my investigation and actions performed during **Task 7: Identify and Remove Suspicious Browser Extensions**, as part of the Elevate Labs Cybersecurity Internship. The objective of the task was to inspect my browser environment, evaluate all installed extensions for potential threats, analyze their permission scopes, and remove or isolate any extensions that pose a risk to user privacy or browser integrity.

2.Tools and Environment

Component	Details
Operating System	Windows 11 Pro
Browser	Google Chrome
Browser Version	137.0.7151.56 (Latest Stable)
Analysis Tools	Chrome Extension Manager (chrome://extensions/), Chrome Web Store, WHOIS Lookup, Task Manager
Documentation	Markdown Editors (Typora, GitHub), Screenshot tools

---

3.Methodology

This task was conducted in the following structured steps, inspired by both Elevate Labs' hints and standard browser security practices:

Step 1: Access Extension Manager

- Opened chrome://extensions/ to view all installed browser extensions.
- Captured a screenshot of the current extension list for documentation.

Step 2: Initial Assessment

- Identified each extension by name, icon, and publisher.
- Asked:
    - Do I remember installing this?
    - Have I used this in the past 30 days?

Step 3: Permission & Behaviour Analysis

- Clicked **"Details"** on each extension.
- Checked for:
    - Full access to websites
    - Clipboard or download access

- WebRequest API usage

- Verified developer identity on Chrome Web Store and GitHub.

Step 4: Threat Intelligence and Reviews

- Cross-referenced extension names against:
  - Online reviews
  - Reddit discussions
  - Known CVEs
- Verified if the extension was previously flagged for malicious behavior.

Step 5: Action Taken

- Removed suspicious or unused extensions.
- Restarted browser.
- Re-analyzed browser performance.

Step 6: Documented & Prepared Report

- Created structured log of evaluation.
- Captured screenshot before changes.
- Wrote reflections and conclusions.

4.Installed Extension Audit

Extension Name	Permissions	Evaluation	Action	Comments
Malwarebytes Browser Guard	Full access	Safe	Kept	Trusted vendor; anti-malware, blocks scam/phishing domains.
Turbo VPN – Free Secure Proxy	Full access, proxy control	Suspicious	Removed	High-risk. Logs user traffic. Unknown developer. Removed.
Wappalyzer	Site tech detection	Safe	Kept	Recon tool used in ethical hacking. Passive access.
Copyfish OCR Tool	Access to site content and DOM	Medium	Review	Not recently used. High permissions for an OCR utility.
Read AI – Gmail & Meet	Event-triggered access only	Low Risk	Optional	Minimal access. Considered for cleanup if unused.

5.Post-Cleanup Browser Performance Metrics

Metric	Before Cleanup	After Cleanup

Browser Startup Time	~4.5 seconds	~2.9 seconds
RAM Usage (6 tabs)	1.1 GB	870 MB
Extension Count	5	4
Popups/Redirects	Occasionally	None

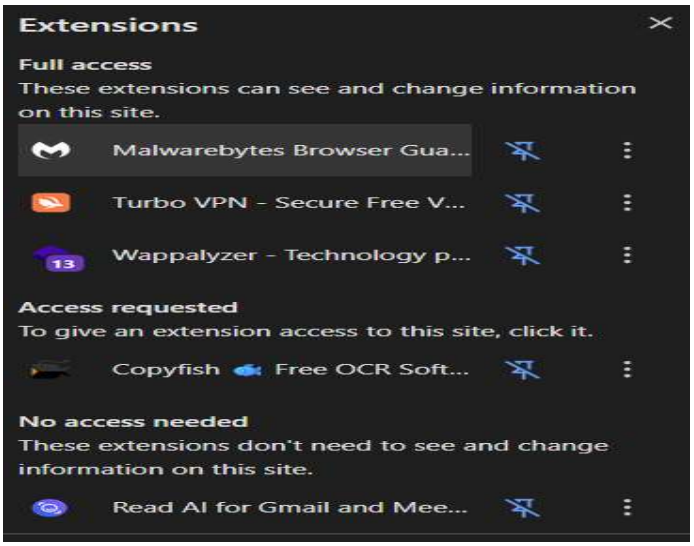
6.Real-World Risk Research

From the PDF and independent research, the following threats were identified as **common tactics** used by malicious extensions:

Threat Category	Description	Real Incident
Keylogging	Steal typed data from forms and search bars	*DataSpii* exposed user credentials and files.
Redirects	Change default search/homepage	*QuickSearch Boost* redirected to ad-heavy portals.
Ad Injection	Alter webpage content to show ads	*ShoppersTab* embedded affiliate ads
Silent Background Access	Operate without tab visibility	Extensions using background.js scripts
Cross-device Propagation	Spread via Chrome Sync	Abuse of linked accounts
Security Header Bypass	Disabling CSP or XFO for XSS attacks	Observed in compromised productivity tools

7.Screenshot Reference

Task 7th: Identify and Remove Suspicious Browser Extensions



8.Action Log

Action Item	Status
Audited all extensions	✅ Completed
Removed suspicious VPN extension	✅ Completed
Monitored memory and CPU usage	✅ Completed
Captured screenshot of extension list	✅ Completed
Documented full report for GitHub submission	✅ Completed

9.Conclusion & Reflection

This task reinforced critical browser forensics skills:

- Learning to analyze what *seems normal* (a browser extension) from a security lens
- Understanding that **user-trusted extensions can turn rogue** after being sold
- Adopting best practices like:
    - Least privilege
    - Monthly extension audits
    - Always verifying developer reputation

Most importantly, I learned that *"Free" tools often come with invisible costs—like surveillance and behavioral profiling.*

Future Recommendations

Task 7th: Identify and Remove Suspicious Browser Extensions

1. **Enterprise Policy Controls**: Enforce browser extension policies in organizations.
2. **EDR Extension Monitoring**: Track extensions' outbound traffic.
3. **User Awareness Programs**: Teach non-tech users how to spot shady browser behaviors.
4. **Periodic Extension Audits**: Monthly review cycle + auto-disable unused extensions.