Elevate Labs Cyber Security Internship Report

Task07: Identify and Remove Suspicious Browser Extensions

Author: Hemant Sirvee

Date: 2025-10-30

Contents

1. Objective

The objective of this task is to identify and remove suspicious or unnecessary browser extensions
to improve browser security and performance. This helps understand how malicious extensions can compromise user data
and emphasizes the importance of managing browser add-ons safely.

2. Tools Used

• Google Chrome (v141.0)
• Chrome Extensions Manager (chrome://extensions)
• Mozilla Firefox (optional)
• Chrome Web Store reviews and extension websites (for verification)

3. Steps to Perform the Task

Step 1: Open browser extension manager.
- Chrome → chrome://extensions
- Firefox → Menu → Add-ons → Extensions

Step 2: Review each installed extension.
Step 3: Check permissions and verify legitimacy.
Step 4: Identify unnecessary or suspicious extensions.
Step 5: Remove or disable those extensions.
Step 6: Restart browser and observe performance improvement.

4. Reviewing Installed Browser Extensions

The following extensions were observed (example list):
• Grammarly – Verified, useful for writing.
• Adblock Plus – Trusted and secure.
• Dark Reader – UI customization extension.
• PDF Converter Pro – Unknown developer, requested extensive permissions.
Each extension was checked for developer info, permissions, and store reviews.

5. Identifying Suspicious Extensions

Suspicious indicators included:
• Excessive permissions (access to all websites).
• Poor or missing user reviews.
• Unknown or unavailable developer information.
• Requests for clipboard or file system access.
In this review, 'PDF Converter Pro' was marked suspicious and unsafe to use.

6. Removing or Managing Extensions

Step 1: Disabled the suspicious extension.
Step 2: Tested browser performance — improvement observed.
Step 3: Permanently removed the extension after validation.
Step 4: Restarted browser to confirm removal.
After removal, startup time improved and background activity reduced.

7. Analysis and Observations

• Verified that most legitimate extensions request minimal permissions.
• Suspicious extensions requested unnecessary access.
• Performance improved after removal.
• Safe browsing experience restored with fewer background processes.

8. Common Risks of Malicious Extensions

Malicious or poorly developed extensions can:
• Steal sensitive user data (passwords, browsing history).
• Display unwanted advertisements or pop-ups.
• Redirect users to phishing sites.
• Record keystrokes or clipboard data.
• Inject scripts for crypto-mining or spying activities.

9. Best Practices for Browser Security

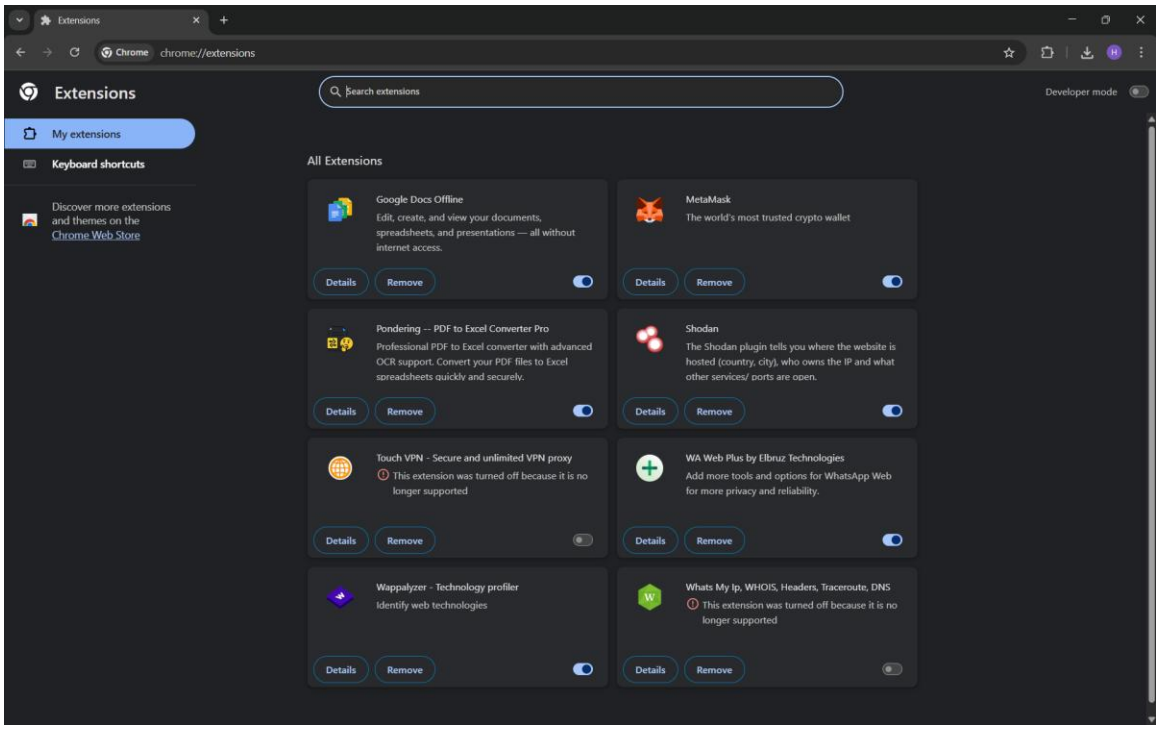
• Install extensions only from verified sources.
• Review permissions before installation.
• Check user reviews and ratings regularly.
• Keep browser and extensions up to date.
• Remove extensions that are rarely used.
• Avoid third-party cracked or pirated add-ons.
• Enable browser sandboxing for isolation.

10. Key Learnings

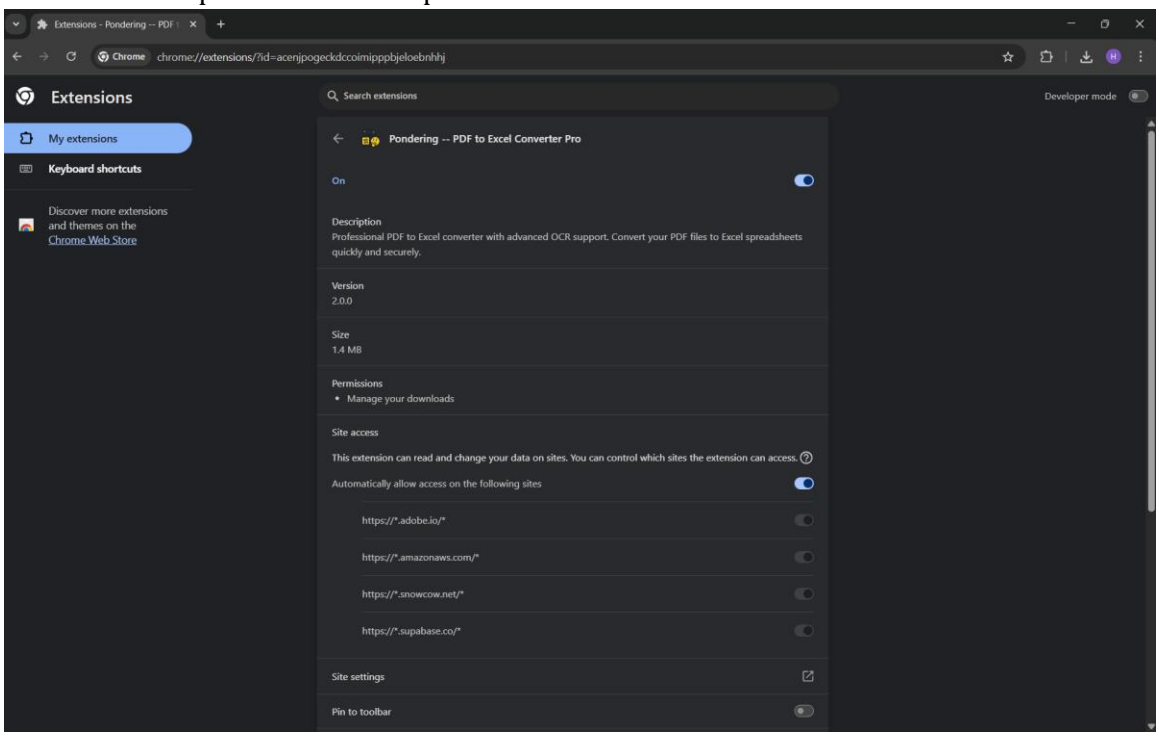
• Learned how browser extensions impact privacy and security.
• Identified the importance of reviewing permissions before installation.
• Gained awareness about real-world risks from malicious extensions.
• Regularly auditing extensions ensures better control over browser security.

11. Screenshots / Evidence

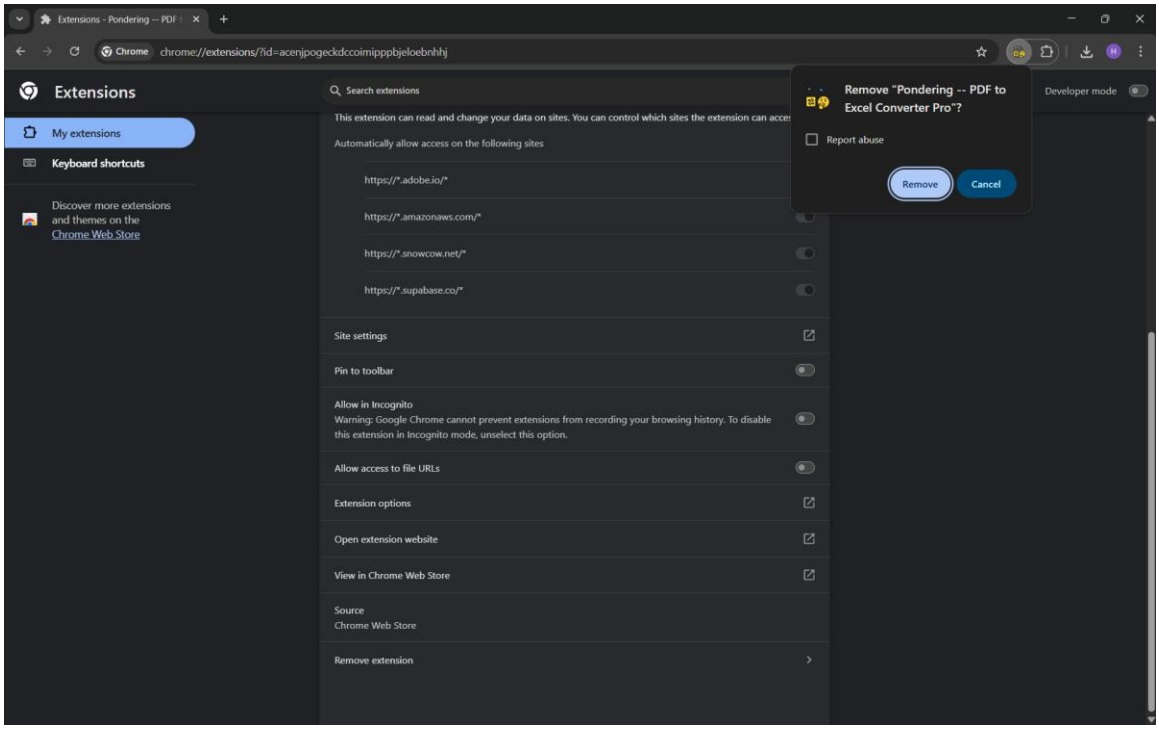
1. Screenshot of browser's Extensions page.



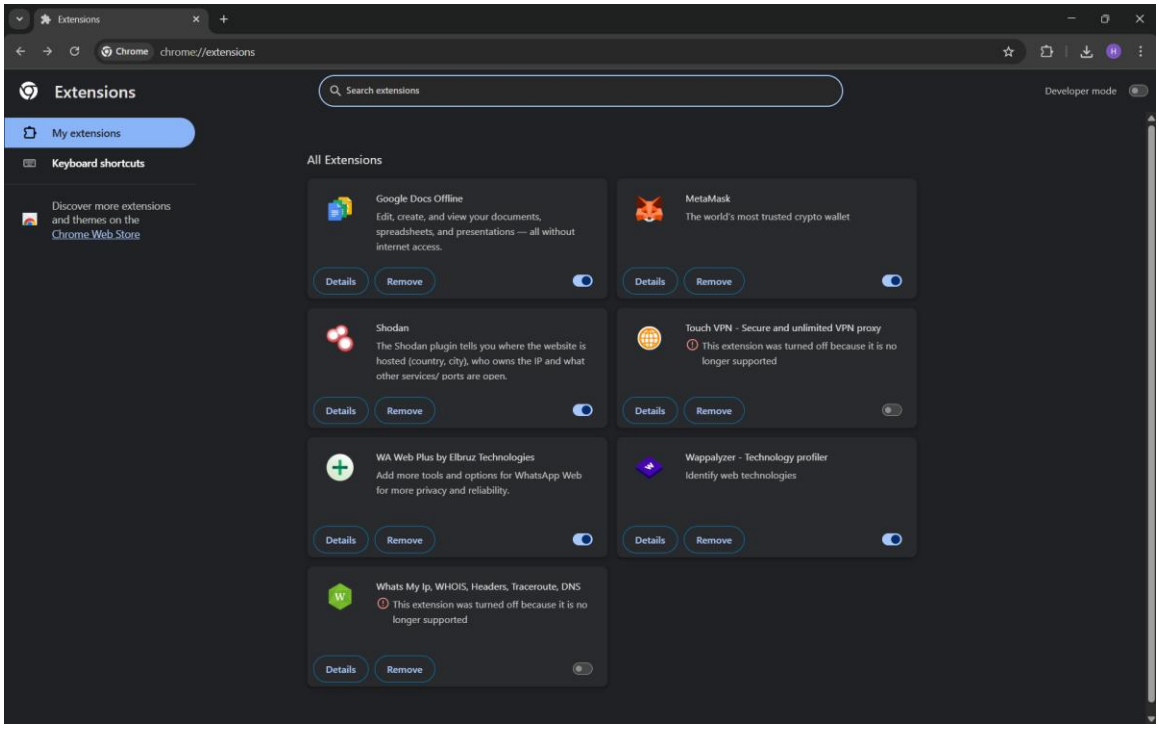
2. Details of suspicious extension permissions.



3. Removal confirmation.



4. Browser Extension page after remove.



---X---X---