Task 7 – Detecting and Uninstalling Harmful Browser Add-ons

🎯 Objective:

Develop the ability to identify and eliminate browser extensions that may pose security or privacy risks.

🧰 Tools Used:

Web Browser – Google Chrome (or any other browser like Firefox)

🛠 Procedure

1. **Navigating to Installed Extensions:**

   To begin, I accessed the extensions dashboard in Google Chrome to inspect all currently active plugins. This was done by:

   - Clicking the three-dot menu in the top-right corner
   - Navigating to **Extensions > Manage Extensions**,
   - Or directly entering: chrome://extensions/ in the address bar.

   Here, I examined each extension, focusing on those requesting broad or potentially unnecessary permissions that could lead to vulnerabilities or performance issues.

---

2. **Analysis of Installed Extensions:**

   Upon reviewing, I noticed some extensions were primarily for UI customization, while others served productivity purposes like AI support.

   Interestingly, Chrome had automatically disabled two extensions that were outdated and no longer maintained. As a best practice, I proceeded to uninstall these to keep the browser clean and secure.

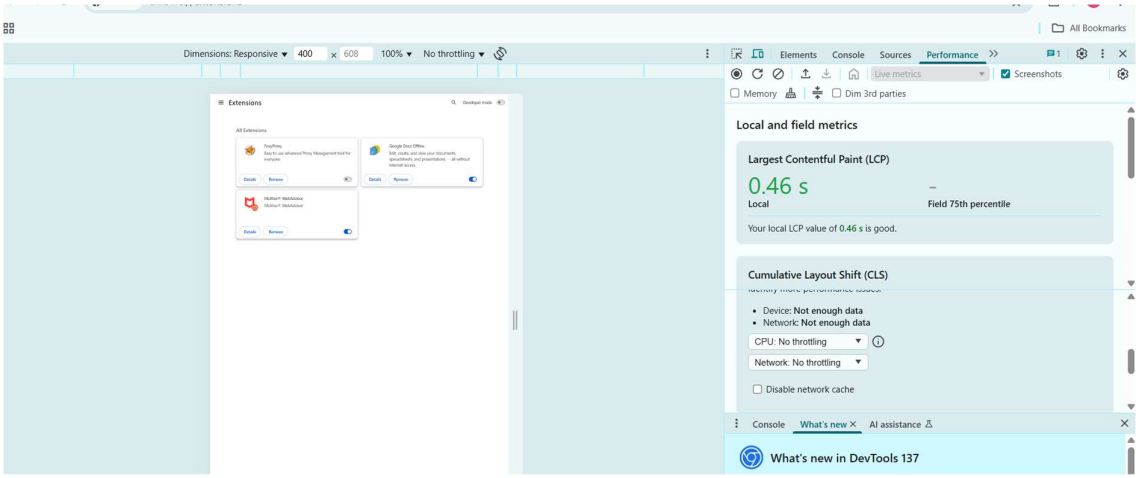
---

3. **Performance Comparison (Before vs. After Cleanup):**

   After capturing screenshots of browser performance before and after removing unused extensions, I observed the following metrics:

📊 **Before Removing Extensions (Screenshot 1):**

- **LCP (Largest Contentful Paint):** 0.46 seconds – Excellent load speed
- **CLS (Cumulative Layout Shift):** 0.00 – No unexpected layout shifts
- **INP (Interaction to Next Paint):** 32 ms – Very responsive



Final Analysis:

- **Screenshot 1** demonstrated faster initial loading (LCP).
- Both setups maintained perfect layout consistency (CLS = 0).

Conclusion:
While Screenshot 1 had marginally faster load speed, Screenshot 2 improved interactivity, making it more fluid for real-world use. Both setups were well-optimized, but a cleaner browser slightly improved the experience.

⚠ Risks of Malicious Extensions

Malicious extensions can pose serious threats to both privacy and device performance. Here's how:

1. **Information Theft:**
   - Can capture login credentials, stored data, credit card details, and more via keylogging or unauthorized access.
2. **Browser Hijacking:**
   - Alter homepages or redirect search results to malicious sites to generate revenue or conduct phishing attacks.

Paavan Shastri

3. **Unwanted Ads:**
    - Injects pop-ups or ads into web pages, sometimes leading to scams or malware.
4. **Excessive Permissions:**
    - May request the ability to "read and modify all your data on the websites you visit," which is a red flag.
5. **Performance Issues:**
    - Can slow down browsing or hog system resources by running hidden background scripts.

🛡 **Tips to Stay Secure**

- Always download extensions from reputable sources.
- Check user reviews, update history, and required permissions before installing.
- Regularly audit and remove extensions that are unused or suspicious.