Task 7 --

Identify and remove suspicious browser entension

General Signs of a Suspicious Browser Extension:

- **Unwanted ads:** Seeing pop-ups, banners, or in-text ads on websites that usually don't have them.
- **Redirects:** Your browser automatically redirects you to unfamiliar websites.
- **Changed homepage or search engine:** Your default homepage or search engine has been altered without your permission.
- **Slow browser performance:** Your browser becomes unusually slow or crashes frequently.
- **New toolbars you didn't install:** Unfamiliar toolbars appearing in your browser.
- **Requests for unusual permissions:** An extension asking for broad permissions that seem unnecessary for its stated function (e.g., a simple weather extension asking to read all your Browse data).
- **Difficulty uninstalling:** The extension keeps reappearing after you try to remove it.
- **Negative reviews/unknown developer:** Little-known extensions with many negative reviews or from an unfamiliar developer.

How to Identify and Remove Suspicious Extensions (Step-by-Step for Major Browsers):

1. Google Chrome:

- **Identify:**
    1. Open Chrome.
    2. Type chrome://extensions in the address bar and press Enter, or click the three vertical dots (Menu) in the top right corner, then go to Extensions > Manage Extensions.
    3. Review the list of extensions. Look for any you don't recognize, didn't intentionally install, or that seem to be causing problems.
    4. Pay attention to the permissions requested by each extension. You can click on the "Details" button for each extension to see more information and its permissions.
- **Remove:**
    1. On the chrome://extensions page, for each suspicious extension, toggle off the switch to disable it first.

2. Then, click the Remove button to uninstall it.
3. Confirm by clicking Remove again in the pop-up.

2. Mozilla Firefox:

- **Identify:**
    1. Open Firefox.
    2. Click the three horizontal lines (Menu) in the top right corner, then click Add-ons and themes, or type about:addons in the address bar and press Enter.
    3. In the left sidebar, click Extensions.
    4. Examine the list for unfamiliar or suspicious extensions.
- **Remove:**
    1. On the about:addons page, locate the suspicious extension.
    2. Click the three horizontal dots next to the extension's name.
    3. Select Remove.
    4. Confirm the removal if prompted.

3. Microsoft Edge:

- **Identify:**
    1. Open Edge.
    2. Click the three horizontal dots (Settings and more) in the top right corner, then select Extensions, or type edge://extensions in the address bar and press Enter.
    3. Browse the list of installed extensions.
- **Remove:**
    1. On the edge://extensions page, find the extension you want to remove.
    2. Toggle off the switch to disable it.
    3. Click the Remove button below the extension's name.
    4. Confirm by clicking Remove in the dialog box.

4. Safari (macOS):

- **Identify:**
    1. Open Safari.

2. Click Safari in the menu bar at the top of the screen, then select Settings (or Preferences on older macOS versions).
3. Click the Extensions tab.
4. Review the list of installed extensions.

- **Remove:**
    1. In the Extensions tab, select the suspicious extension from the left sidebar.
    2. Click the Uninstall button on the right.
    3. You may need to confirm the removal by clicking Show in Finder and then dragging the extension to the Trash.

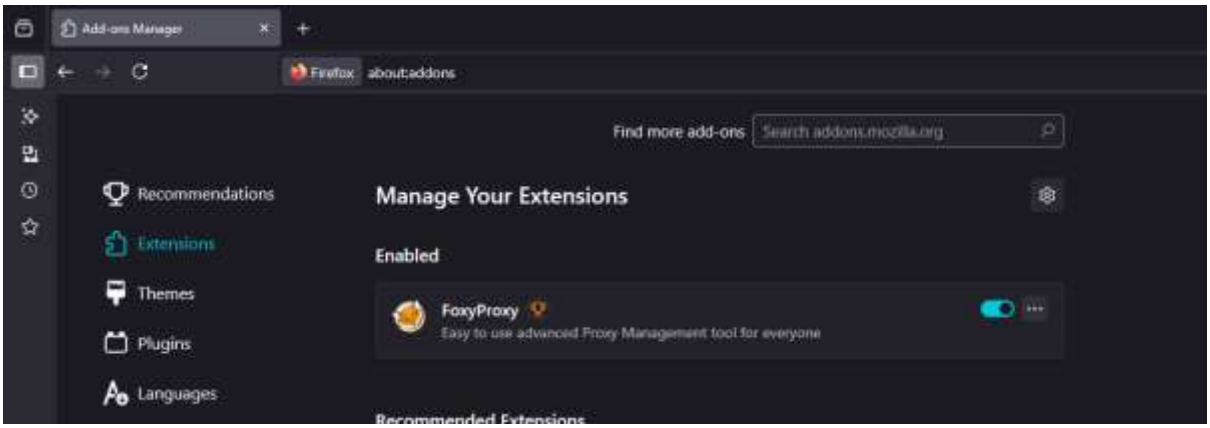
Additional Steps After Removing Suspicious Extensions:

1. **Run a Malware Scan:** After removing extensions, it's highly recommended to run a full scan with a reputable antivirus/anti-malware program (e.g., Windows Defender, Malwarebytes, Avast, AVG) to ensure no lingering threats are on your system.
2. **Reset Browser Settings (Optional but Recommended):** If problems persist, consider resetting your browser settings to their default. This will usually reset your homepage, new tab page, search engine, and disable all extensions (you can re-enable trusted ones later).
    - **Chrome:** chrome://settings/reset
    - **Firefox:** about:support (then click "Refresh Firefox")
    - **Edge:** edge://settings/resetProfileSettings
    - **Safari:** Safari doesn't have a direct "reset" option. You might need to clear history and website data, and manually check other settings.
3. **Check for Unwanted Programs:** Sometimes, suspicious extensions are installed as part of a larger unwanted program. Go to your computer's Control Panel (Windows) or Applications folder (macOS) and uninstall any programs you don't recognize.
4. **Change Passwords:** If you suspect any sensitive information might have been compromised, change important passwords (especially for email, banking, and social media).
5. **Be Cautious in the Future:**
    - Only install extensions from official browser web stores (Chrome Web Store, Firefox Add-ons, Microsoft Edge Add-ons, Safari Extensions Gallery).

- Read reviews and check the developer's reputation before installing.
- Be wary of extensions that ask for excessive permissions.
- Avoid clicking on suspicious links or downloading software from untrustworthy sources.

Each extension listens for page changes in the browser, and each time the user navigates to a new page, the extension sends the page URL to a remote server to check if affiliate revenue code can be injected. Many sites (including How-To Geek) include affiliate code in links to shopping websites, which sometimes provides them with a small cut of revenue. However, most of the offending extensions are not related to buying items at all, and they are injecting the code for all possible pages. McAfee also found evidence that some of the extensions wait 15 days after they are installed to start injecting affiliate code, presumably to avoid initial detection.

I have check my computer system there is no any harmful extension installed



Only testing purpose Foxy Proxy installed for burp suite.