TASK-7
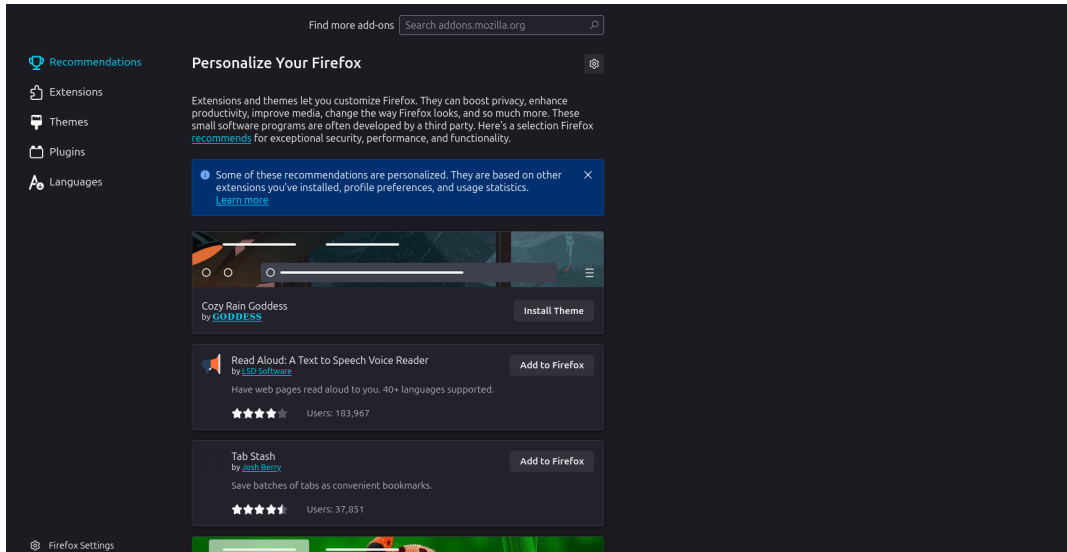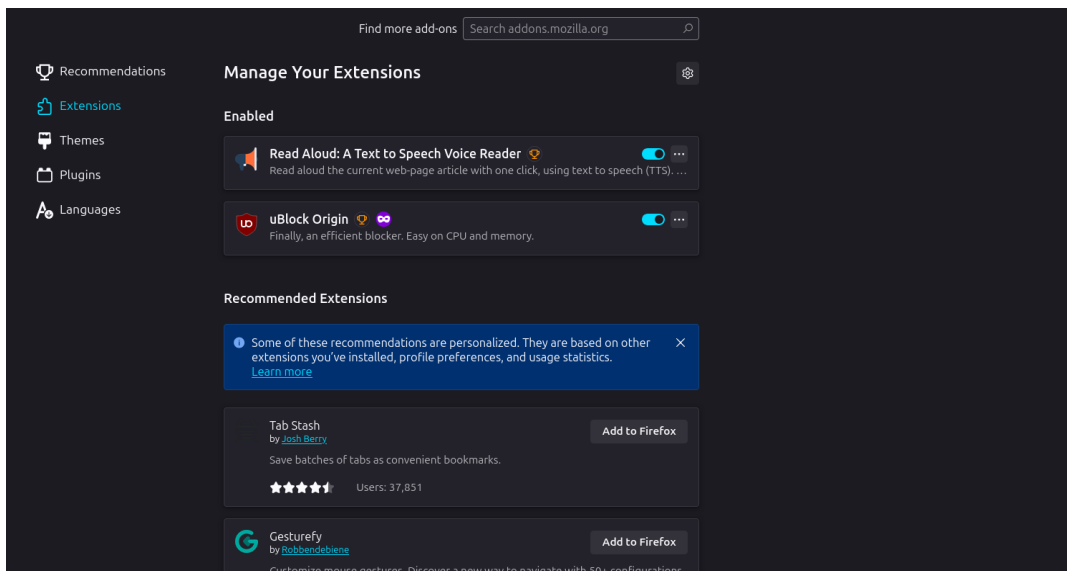# IDENTIFY AND REMOVE SUSPICIOUS BROWSER EXTENSIONS
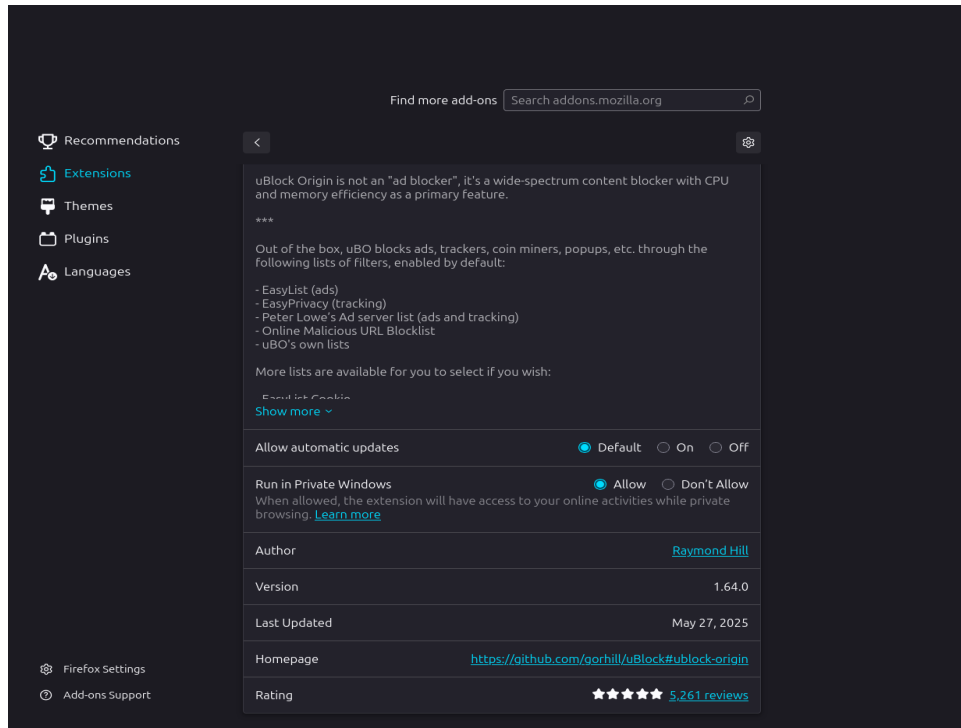
1.OPENING THE ADS-ON MANAGER: Click the **three-line menu (☰) → Add-ons and themes → Extensions.**
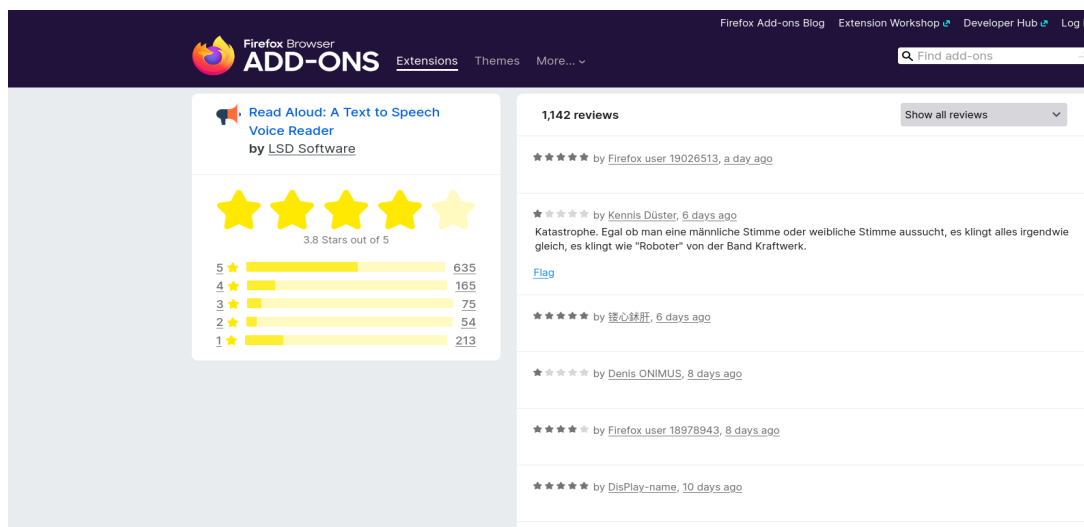

2.VIEWING THE INSTALLED EXTENSIONS: Click **"Extensions"** on the left sidebar.

3.CHECKING EXTENSION DETAILS: For each extension, click the **3-dot menu (⋯)** next to it → click **"Manage"**
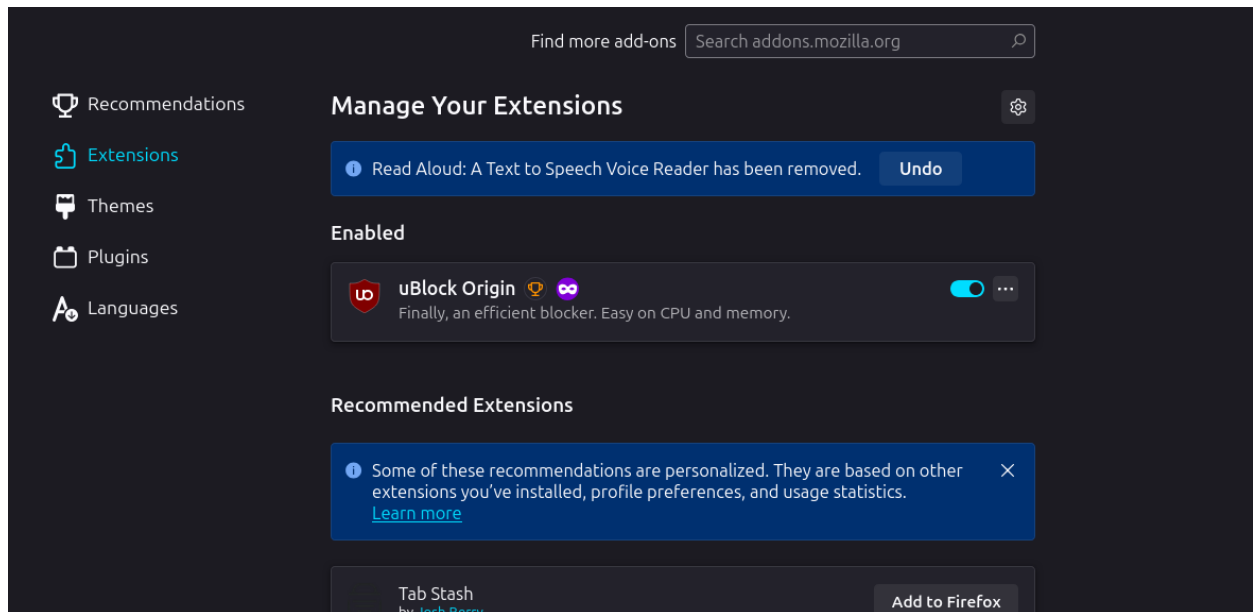

4.CHECKING FOR REVIEWS: In the **"Manage"** page, click **"More Options"** → "**View on Firefox Add-ons site".**

5.REMOVING UNNECESSARY EXTENSIONS: Removing **Read Aloud** extension
Click the **3-dot menu (···)** → **Remove**

6.RESTARTING FIREFOX: Close and **Reopen** firefox.

7.CONCLUSION: Regularly reviewing your Firefox extensions is an essential part of maintaining your browser's security and performance. By checking installed add-ons, verifying their permissions and reputation, and removing those that are suspicious or unnecessary, you reduce the risk of privacy breaches, malware infections, and unwanted behavior such as ad injection or data tracking. Restarting your browser after making changes ensures all updates take effect smoothly. Staying informed about how malicious extensions operate empowers you to browse more safely and maintain better control over your online experience.

HOW MALICIOUS EXTENSIONS CAN HARM YOU:

- Track Your Browsing: They may log websites you visit and sell your data.

- Steal Personal Info: Some can capture login credentials or autofill data.

- Inject Ads/Redirects: They can display unwanted ads or redirect you to malicious sites.

- Install Malware: They may download other harmful files in the background.

- Hijack Browser Settings: Change your homepage or search engine to ad-filled ones.

SIGNS AN EXTENSION MIGHT BE MALICIOUS:

- You don't remember installing it.

- It asks for unnecessary permissions (e.g., access to all websites).

- It has very few or fake-looking reviews.

- It causes pop-ups, redirects, or changes your search engine/homepage.