Task - 7

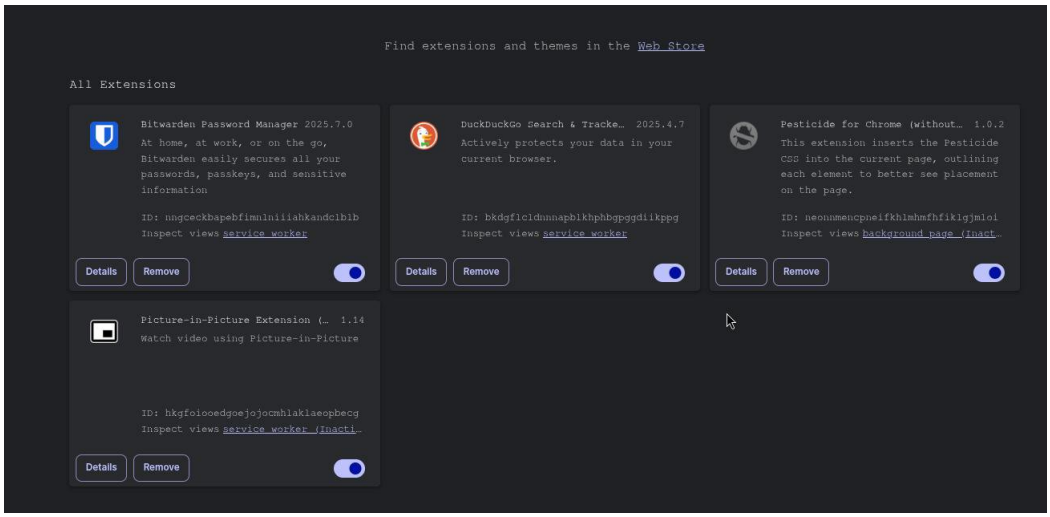
Browser extension Analysis

Objective: Learn to spot and remove potentially harmful browser extensions.

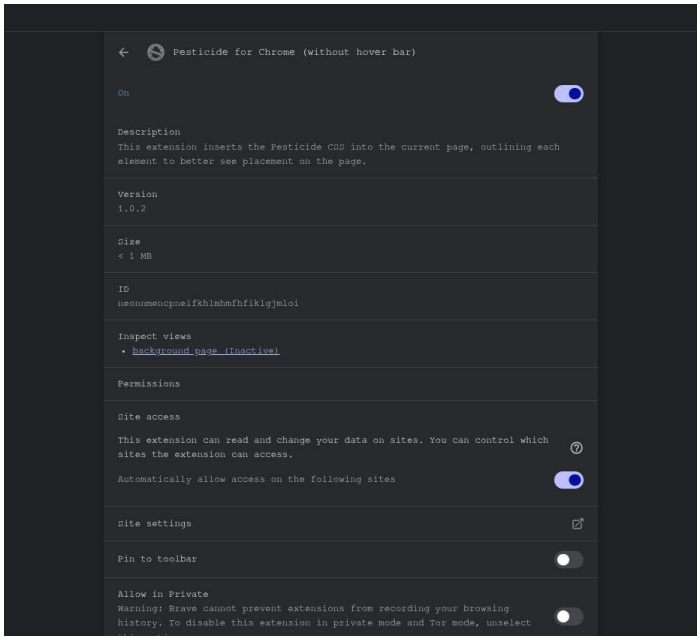
Tools: Any web browser

There is no suspicious extensions , had not found but there is a extension i haven't used for a long time

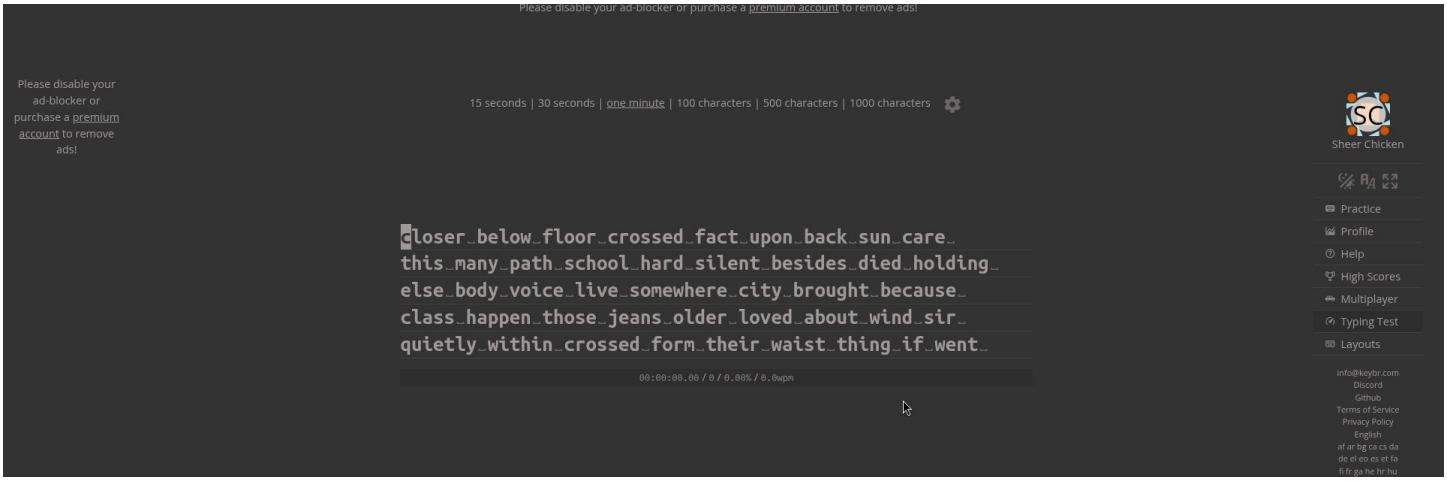
Called pesticide , which is a Developer tool, for CSS debugging tool, which i am going to investigate

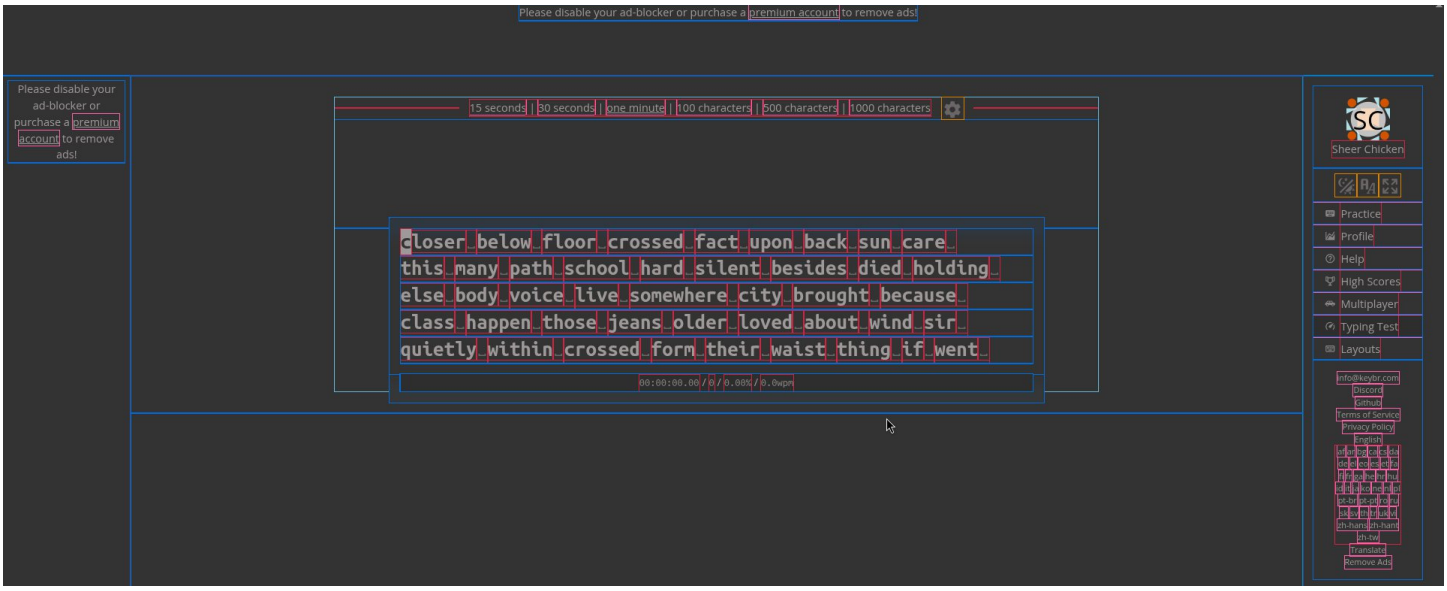


These are the all extensions have installed in my brave browser, all though some of them are not using from a long time, like pesticide, and picture-in-picture,

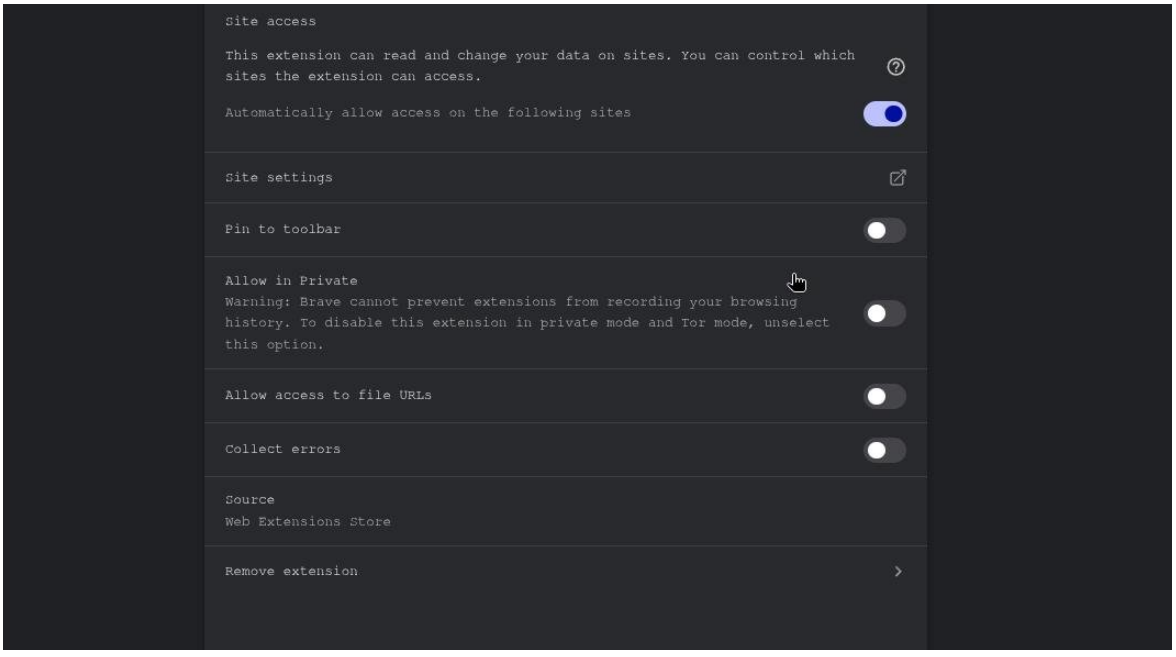


as you can see below image is the details of the pesticide extension in my browser, it describes that it injects its CSS to the existing page css like this





But when i see the permissions of this extension i saw a awkward permission



this has the permission to automatically access to read and change on sites data

These are some threats of the Malicious Browser extensions:

Malicious browser extensions are software add-ons designed to compromise security, privacy, or system performance. They can harm users in several ways:

Data Theft: Such extensions often request broad permissions, allowing them to access or steal sensitive data like login credentials, cookies, browsing history, and even financial information.

User Tracking & Surveillance: They may record keystrokes, take screenshots, monitor browsing habits, or access camera and microphone.

Session Hijacking & Account Takeover: By stealing session tokens or cookies, attackers can impersonate users and access their accounts.

Malware Delivery: Extensions can install additional malware, including ransomware or spyware, to compromise devices.

Content Manipulation: Malicious plugins may inject ads, change search results, or redirect users to phishing sites, misleading or defrauding users.

Persistence and Obfuscation: Advanced extensions can disable security settings, reinstall themselves, and avoid detection, making removal difficult.