Browser Extension to Block Trackers

Introduction

In the current digital age, user privacy is often compromised by hidden trackers embedded in websites. These trackers collect personal data without explicit consent. To address this issue, we developed a lightweight, privacy-focused browser extension aimed at blocking known tracking scripts to improve online anonymity and security.

Abstract

This project delivers a browser extension for Chrome and Firefox that automatically blocks web requests to known tracking domains. By leveraging browser APIs and predefined tracker lists, the extension identifies and prevents data transmission to third-party trackers. It includes a real-time counter to show blocked attempts and supports user-managed whitelists and blacklists for customizable privacy control.

Tools Used

- Languages: JavaScript, HTML, CSS
- APIs & Frameworks: Chrome/Firefox Extensions API (Manifest v3), webRequest API
- Tracker List: DuckDuckGo Tracker Radar (open-source dataset)

Steps Involved in Building the Project

1. Setup Manifest File (v3):

Defined metadata, permissions (webRequest, storage), background service worker, and popup UI files.

2. Integrated Tracker List:

Imported DuckDuckGo's open-source tracker domains list to filter requests.

3. Intercept Web Requests:

Used the chrome.webRequest.onBeforeRequest listener to check outgoing requests against the

tracker list and block them if matched.

4. Badge Counter for Analytics:

Implemented a dynamic badge counter to display the number of blocked requests per session.

5. Popup UI:

Built a simple popup using HTML/CSS to show analytics and provide toggle options for enabling/disabling blocking on specific sites.

6. Whitelist/Blacklist Feature:

Allowed users to manually manage domains using Chrome's storage.sync API, so exceptions can be maintained per user preference.

7. Testing & Deployment:

Tested the extension on multiple tracker-heavy websites and validated functionality across Chrome and Firefox browsers.

Conclusion

The extension effectively blocks tracking scripts in real-time, empowering users to browse with enhanced privacy. It remains lightweight and customizable, ensuring a balance between security and usability. Future improvements may include adding a visual log of blocked domains and cloud sync for user settings. This project demonstrates the practical application of JavaScript and browser APIs to solve real-world privacy concerns.