📄 Cyber Security Internship – Task 7 Report

Task Title: Identify and Remove Suspicious Browser Extensions
Objective: Strengthen browser security by detecting and removing potentially harmful or unnecessary extensions.
Tools Used: Google Chrome / Mozilla Firefox Extension Manager

1. Introduction

Browser extensions add useful functionalities, but they can also introduce severe security risks if misused. This task focuses on auditing installed extensions, identifying suspicious or unused ones, and removing them to minimize attack vectors.

2. Methodology

The following steps were taken:

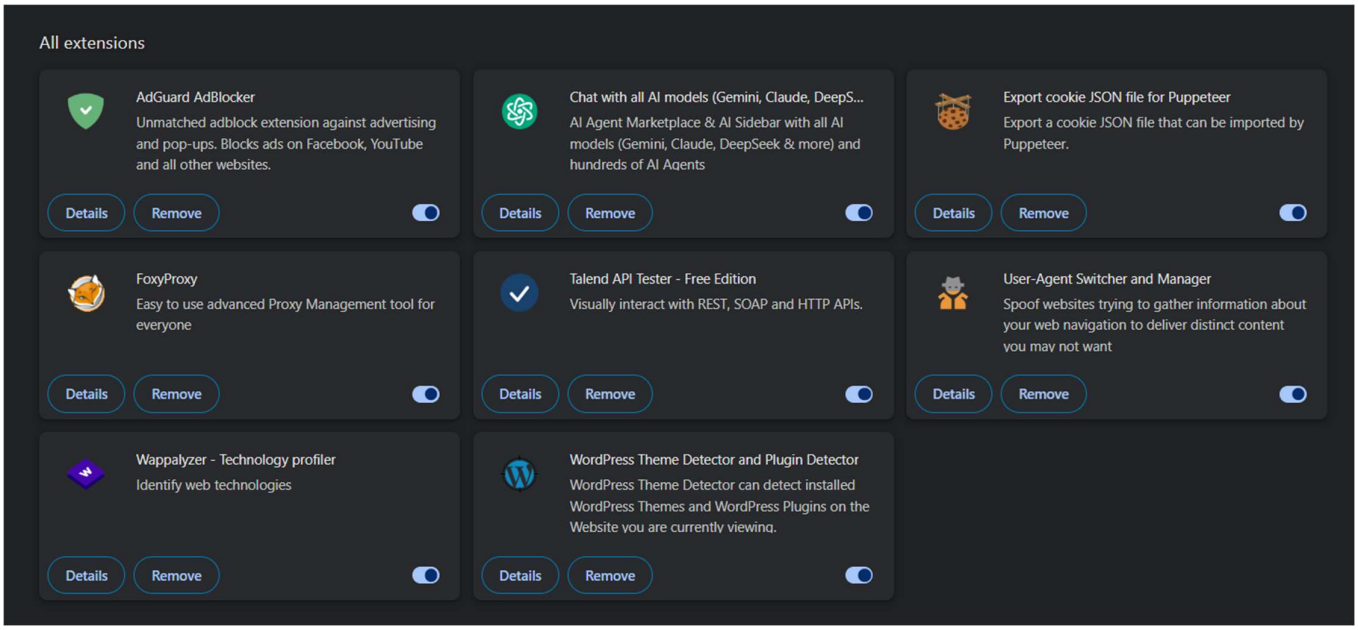
1. **Opened Extension Manager** – Accessed browser's extension/add-ons page.
2. **Listed All Installed Extensions** – Created an inventory of active and inactive extensions.
3. **Analysed Permissions** – Reviewed requested permissions, especially high-risk ones such as:
    - Access to all websites
    - Reading browsing history
    - Accessing cookies and passwords
4. **Checked Reputation** – Looked at developer details, ratings, and last update dates.
5. **Removed Suspicious/Unused Extensions** – Unnecessary add-ons were deleted or disabled.
6. **Restarted Browser** – Verified performance improvements and reduced risk exposure.

3. Findings

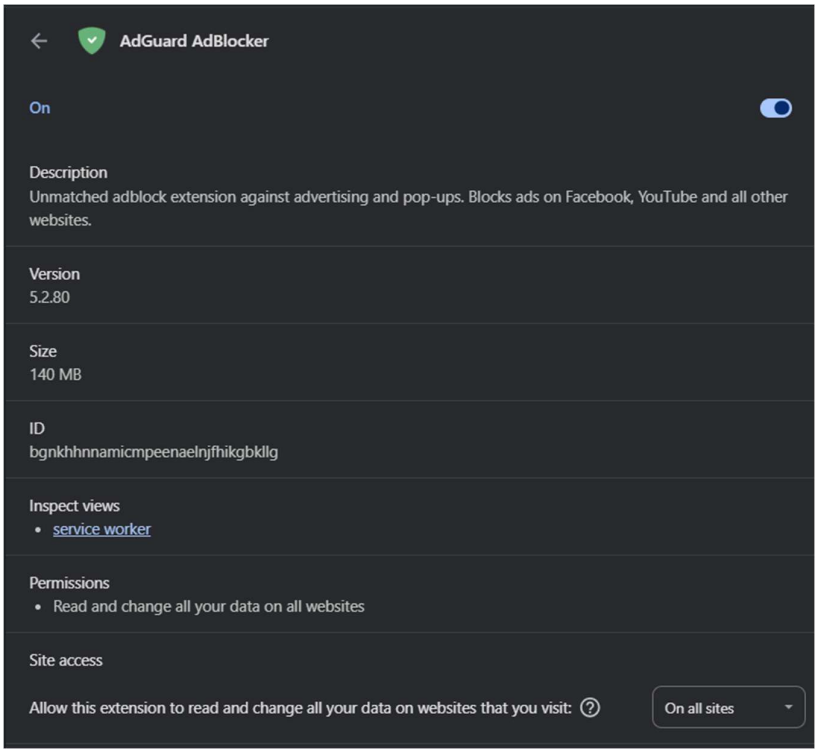
During the audit, multiple extensions were evaluated. Some were kept due to trusted sources and legitimate functionality, while others were flagged as suspicious due to outdated versions, excessive permissions, or lack of necessity.

4. Screenshots (Evidence)

4.1 Before Audit



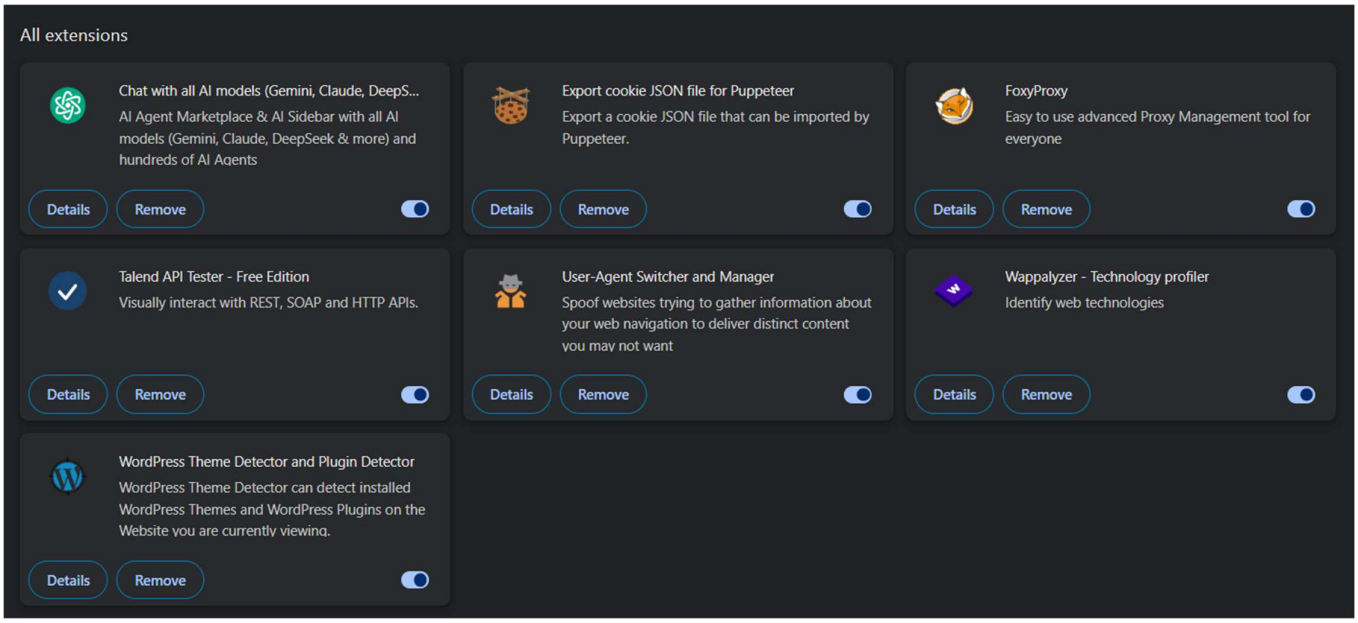
4.2 Permission Analysis



Extension: AdGuard Adblocker
Requested Permission: “Read and change all your data on all websites”
Analysis:
The requested permission may initially seem suspicious, as it grants the extension the ability to view and modify content on any website. In general, extensions with such permissions could potentially:

- Steal sensitive information such as login credentials or cookies.
- Modify webpages to inject advertisements, phishing links, or malicious scripts.
- Track user activity across multiple websites.

4.3 After Audit



5. Security Risks of Suspicious Extensions

- **Data Theft:** Unauthorized access to passwords, browsing history, or personal information.
- **Privacy Invasion:** Hidden tracking and profiling of user behavior.
- **Browser Hijacking:** Altering search engine settings, homepage, or injecting ads.
- **System Exploits:** Exploiting outdated extensions to execute malicious code.

6. Best Practices for Safe Extension Management

- Install extensions only from official stores.
- Regularly review and audit installed add-ons.
- Avoid extensions requesting excessive permissions.
- Keep extensions updated or remove outdated ones.
- Follow the *principle of least privilege* when granting permissions.

7. Audit Summary Table

Extension Name	Permissions Requested	Status	Action Taken
Chat with all AI models	Access to browsing history, all sites	Suspicious	Removed
Export Cookie JSON	Access browsing history	Safe	Kept
Foxy Proxy (For Bug Bounty)	Read and Change data on all sites Manage Downloads	High Risk	Kept if you used for security researcher
User-Agent Switcher	NA	Safe	Kept
Wappalyzer	Read browsing history	Safe	Kept

(This table can be filled with actual extensions from your system for authenticity.)

8. Conclusion

The audit revealed that not all installed browser extensions are safe. By removing suspicious and unused extensions, the overall security and performance of the browser improved significantly. This task highlighted the importance of regular extension reviews as part of personal and organizational cybersecurity hygiene.