**Task 7 : Identify and Remove Suspicious Browser Extensions**

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

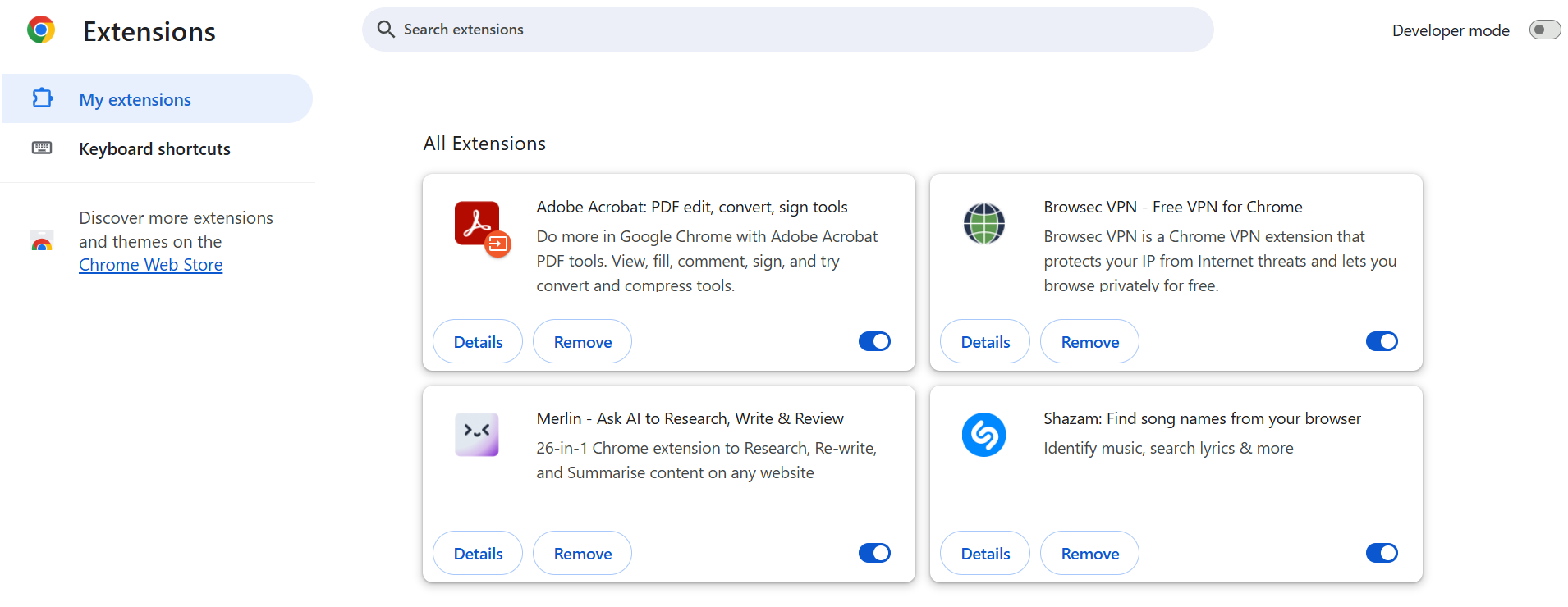
**Tools:** Any web browser (Chrome, Firefox)

**Deliverables:** List of suspicious extensions found and removed (if any)

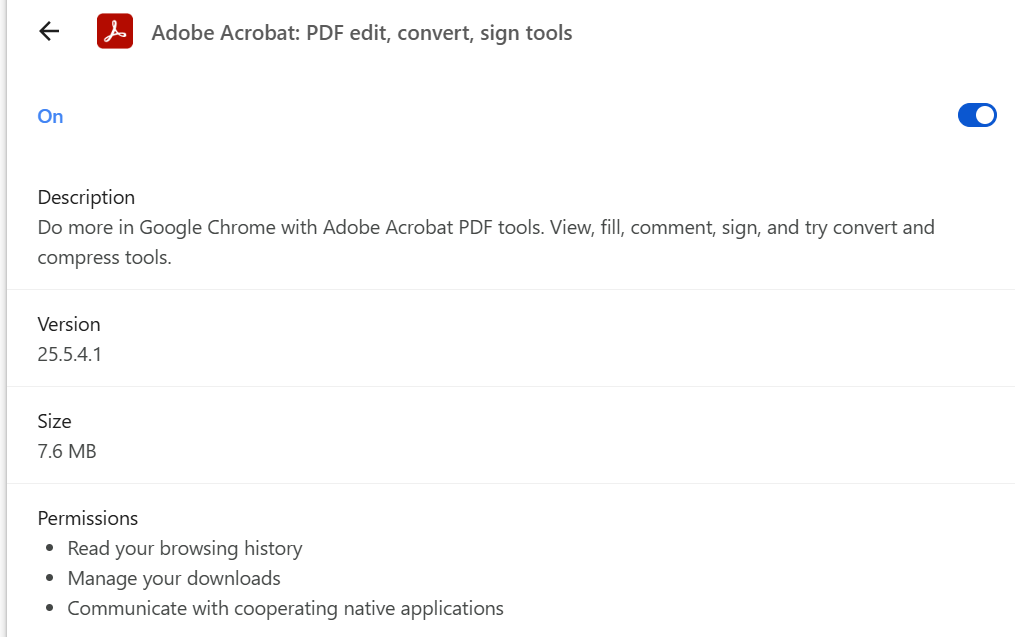
1. **Opened our browser’s extension/add-ons manager.**



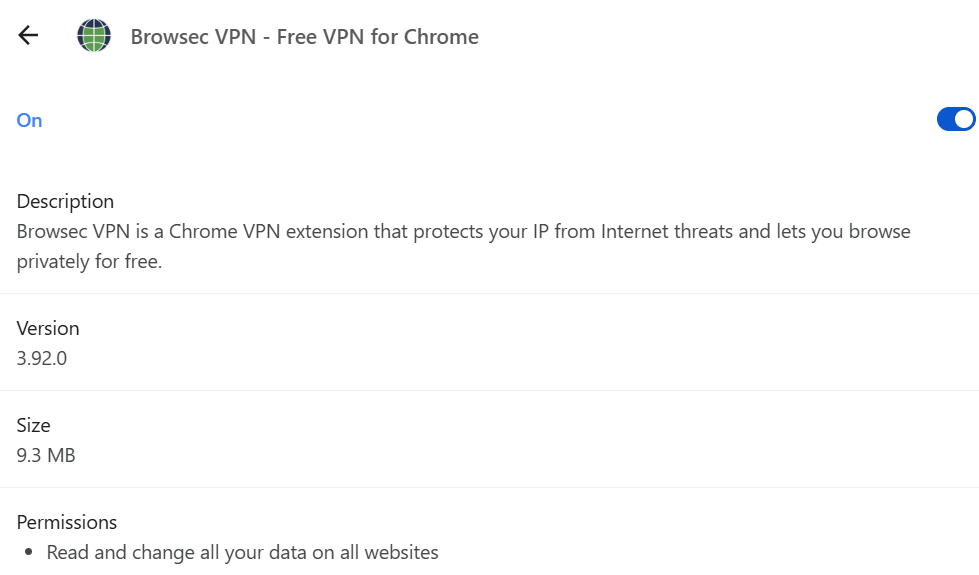
1. **Review all installed extensions carefully.**

****

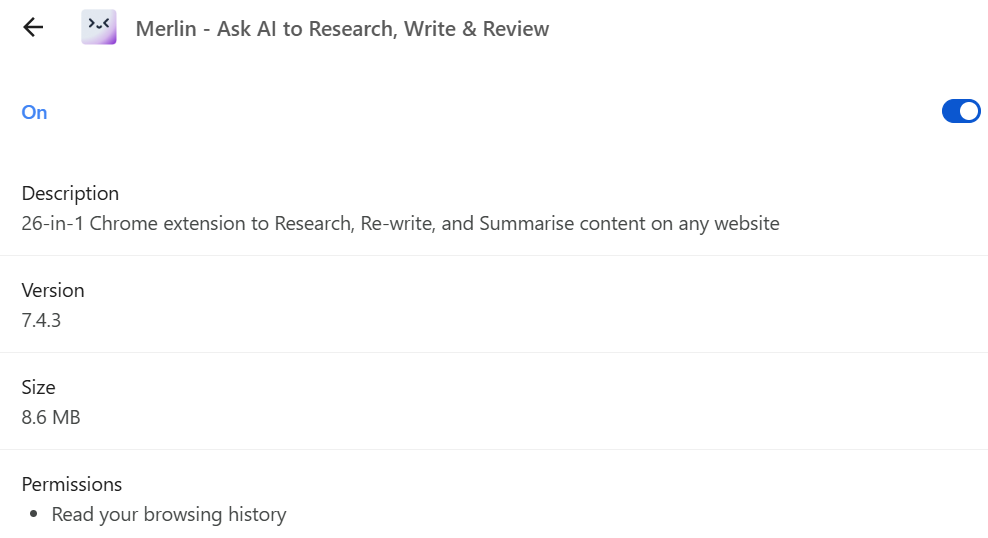
1. **Check permissions and reviews for each extension.**

**Permission for “Adobe Acrobat” extension:**

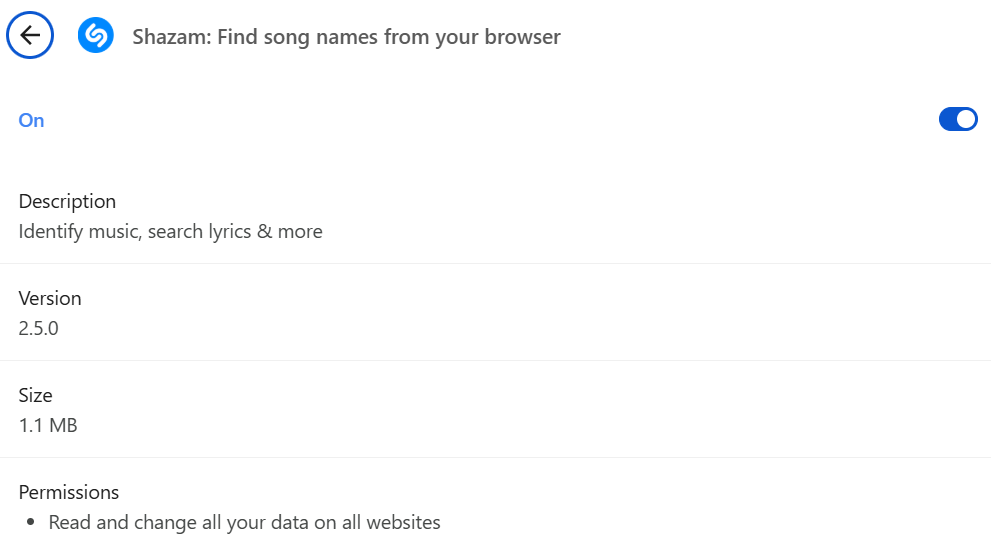
**Permission for “Browsec VPN” extension:**

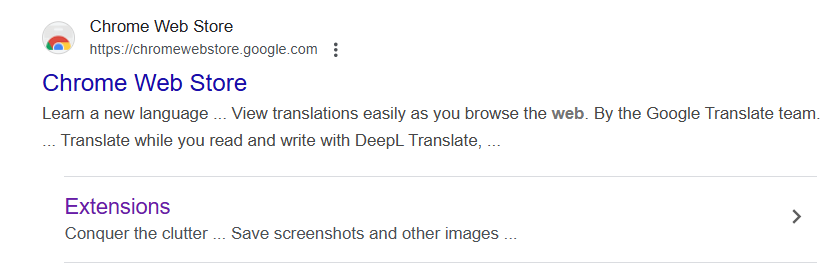
****

**Permission for “Merlin Ai” extension :**

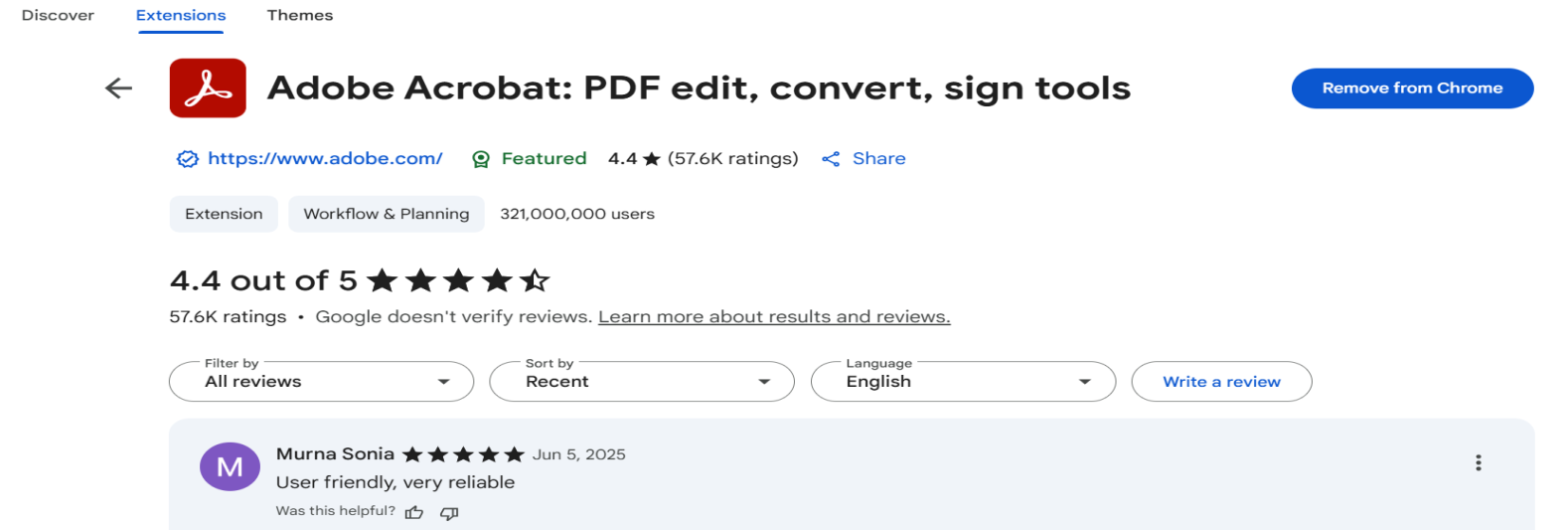
****

**Permission for “Shazam” extension :**

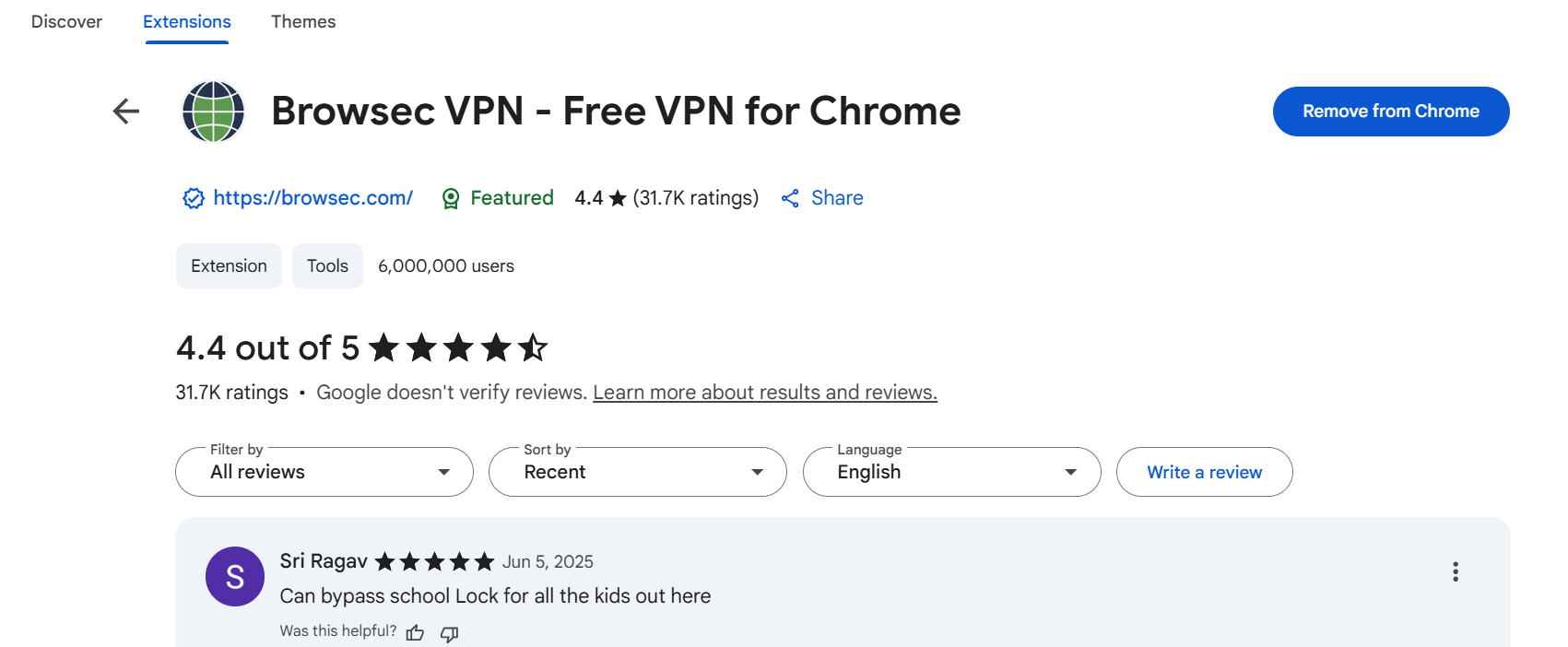
****

**To get the reviews for each extension, we visited “Chrome Web Store”:**   


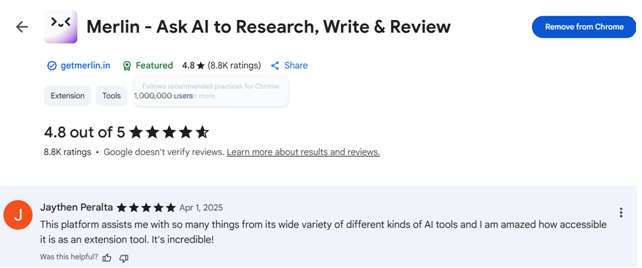
We got the following reviews:

**For Adobe Acrobat:**  


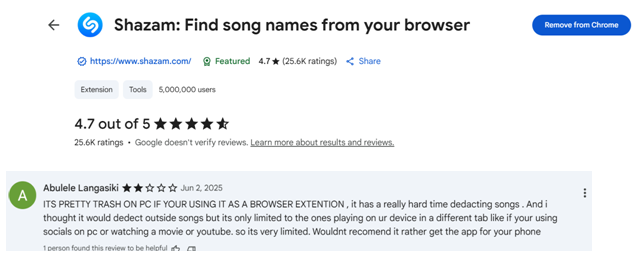
**For Browsec VPN:**

****

**For Merlin Ai:**

****

**For Shazam:**

****

1. **Identify any unused or suspicious extensions.**

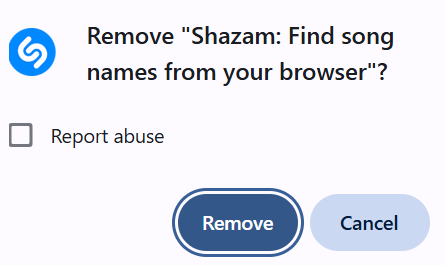
So, through our research and analysis:  
**1. Adobe Acrobat:** Got good reviews and is used by thousands of people with no such security issues or any other grievance, so, this is considered safe for usage.  
**2. Browsec VPN:** Good for use, on point functioning, thus, safe to use.

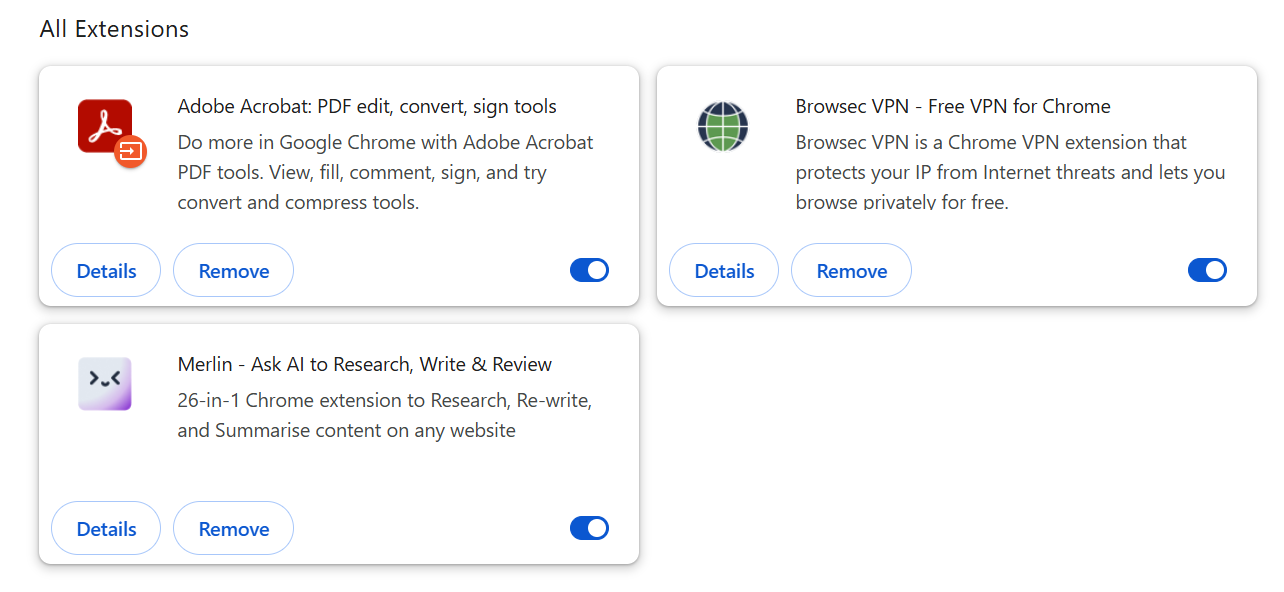
**3. Merlin Ai:** Great reviews, everyone appreciating this extension (me personally too) , no security issues faced whatsoever, thus, makes it significant extension for usage.   
**4. Shazam:** Although, the reviews are mixed, but the security levels and functioning of this extension is not upto-date or trustworthy. Thus we consider this suspicious.

**5. Remove suspicious or unnecessary extensions.**

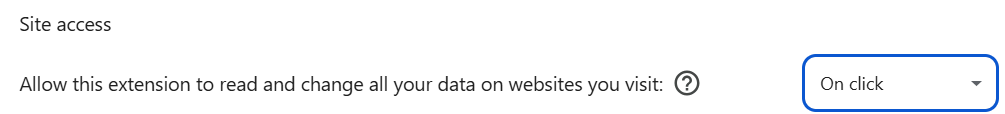
So, as from above analysis, we did the following steps:

**Shazam:**  



**Adobe Acrobat:**

Changed the site access to “on click” from “all sites” which changes automatically in the other two too, i.e., Merlin AI and Browsec VPN ****

1. **Restart browser and check for performance improvements.**

After removing a suspicious Chrome extension and restarting the chrome web-browser can lead to noticeable performance improvements, including:

1. faster website loading times,
2. less memory usage, and
3. a smoother overall browsing experience.

Malicious extensions can drain resources and slow down the browser, so removing them can significantly enhance your online experience.

1. **Research how malicious extensions can harm users.**

According to research, Specific Ways Malicious Extensions Can Harm Users:

* + **Data Theft:**

Malicious extensions can access a wide range of user data, including browsing history, login credentials, payment information, and personal details, which can be used for identity theft or other malicious purposes.

* + **Tracking and Surveillance:**

These extensions can track user activities, collect information about browsing habits, and even monitor user keystrokes.

* + **Malicious Code Injection:**

Malicious extensions can inject harmful code into websites, potentially modifying the content of web pages, redirecting users to phishing sites, or stealing sensitive information.

* + **Phishing Attacks:**

Malicious extensions can mimic legitimate extensions or inject fake prompts to trick users into revealing their personal information.

* + **Performance Issues:**

Some extensions can consume significant system resources, slowing down the browser and potentially impacting overall system performance.

* + **Installation of Malware/Spyware:**

Malicious extensions can install malware or spyware on the user's device, leading to further security vulnerabilities and privacy breaches.

1. **Document steps taken and extensions removed.**
2. Opened our browser’s extension/add-ons manager.
3. Reviewed all installed extensions carefully. (chrome web browser)
4. Checked permissions and reviews for each extension. (chrome web store)
5. Identified any unused or suspicious extensions.
6. Removed suspicious or unnecessary extensions. (Shazam Extension)
7. Restarted browser and check for performance improvements. (faster loading and less memory usage)
8. Researched how malicious extensions can harm users.

*Data Theft, Tracking, Keylogging, Phishing, Performance issues, Malware distribution.*