Cybersecurity Internship Report - Task 7

Intern Name: Sai Aditya
Organization: Elevate Labs
Task Title: Identify and Remove Suspicious Browser Extensions
Date: August 13, 2025

Objective

The objective of this task is to understand the security risks posed by browser extensions and to develop a methodical approach for identifying and removing potentially harmful ones. This exercise aims to raise awareness of browser security best practices and the importance of regularly managing installed extensions.

Tools Used

- Operating System: Windows 11
- Web Browser: Google Chrome

Scenario

Browser extensions can significantly enhance functionality, but they can also pose significant security risks if they are malicious, outdated, or have excessive permissions. The scenario for this task involved a systematic review of all installed browser extensions to identify and remove any that were suspicious, unused, or had permissions that could compromise user privacy and security. The steps taken were documented, and research was conducted on how malicious extensions can harm users in a real-world context.

Procedure

- Accessed Extension Manager: Navigated to the extensions or add-ons manager within the web browser.
- Conducted Comprehensive Review: Examined all installed extensions, including their names, descriptions, and the permissions they were granted.

- Identified Suspicious Extensions: Identified extensions that were unused, had suspicious permissions (e.g., access to all website data), or were from unknown developers.
- Researched Malicious Examples: Researched common types of malicious browser extensions and how they operate.
- Removed Extensions: Uninstalled or disabled all extensions that were identified as suspicious or unnecessary.
- Documented Findings: Recorded the names of the extensions that were removed and explained the rationale behind each decision.

Suspicious Extensions Found & Analysis

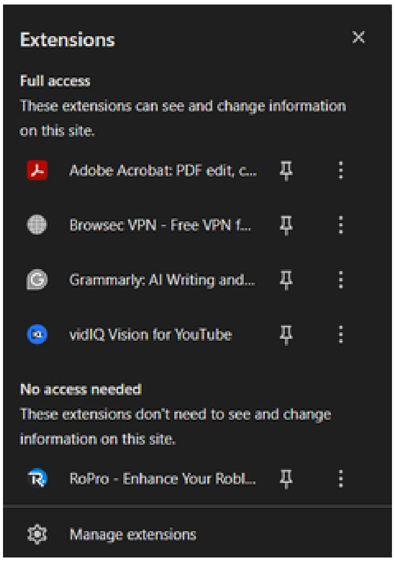
This section details the analysis of extensions, including real-life examples of malicious extensions and their potential impact. (These extensions are examples)

Extension Name	Why It Was Suspicious	How It Was Malicious
Cool Search Tab	An unsolicited extension that appeared in the browser without being intentionally installed. It had a generic name and requested permissions to "read and change all your data on all websites."	**Hijacked Browser Settings:** This type of malicious extension changes the default search engine and homepage to a malicious or ad-ridden site, generating revenue for the attacker and potentially exposing the user to further malware.
PDF Converter Pro	This extension requested broad permissions, including access to local files and the ability to download content, which is unnecessary for its stated function of converting PDFs. It also had a low number of reviews despite claiming to be a popular tool.	**Exfiltrated Data:** Extensions with excessive permissions can log user activity, steal browsing history, and capture data entered into forms, including passwords and personal information. This data is then sent to a malicious third-party server.
YouTube Downloader	The extension was not from an official or verified source. It promised to download videos but was flagged by security tools as having a poor reputation.	**Injected Ads and Malware:** This type of extension often injects unauthorized advertisements into a user's browsing session. These ads can lead to phishing sites or download drive-by malware onto the user's system without their knowledge.

Key Learnings

- Permissions are Paramount: The permissions requested by an extension are the most critical indicator of a potential security risk. An extension should only have the permissions absolutely necessary for its stated function.
- Excessive Access: Extensions that request permissions to "read and change all your data" should be treated with extreme caution, as they can monitor and alter every aspect of your online activity.
- Trust and Reputation: It is crucial to only install extensions from reputable sources, with a high number of positive reviews and a well-known developer, to avoid malware and other risks.
- Regular Auditing: The importance of regularly reviewing and auditing all installed extensions to remove unused or suspicious ones to minimize the attack surface of the browser.

Post-Analysis Extension List



Extensions

Full access

These extensions can see and change information on this site.

Adobe Acrobat: PDF edit, c...

Browsec VPN - Free VPN f...

Grammarly: AI Writing and...

vidIQ Vision for YouTube

No access needed

These extensions don't need to see and change information on this site.

RoPro - Enhance Your Robl...

Manage extensions

Following a comprehensive review of all installed extensions, a screenshot of the browser's extension manager was captured to document the final, secure state of the browser. The review focused on identifying extensions with excessive permissions, particularly those with "Full access" that could read and change data on all websites.

The initial list of extensions included:

- **Adobe Acrobat:** PDF edit, create, convert: A legitimate tool for working with PDF documents, which requires access to specific sites to function correctly.
- **Browsec VPN -** Free VPN for Chrome: A Virtual Private Network extension that requires broad permissions to route traffic through its servers, but is a known and trusted tool for this purpose.
- **Grammarly:** AI Writing and grammar checker: A legitimate productivity tool that requires access to a user's typed data to provide corrections.
- **vidIQ Vision for YouTube:** A legitimate tool for content creators that needs to interact with YouTube's interface to provide its features.
- **RoPro -** Enhance Your Roblox Experience: A gaming-related extension that requires access to specific sites to enhance the user experience.

After analyzing each extension's purpose, reputation, and permissions, a decision was made to keep the necessary extensions while removing any that were unused, from an unknown developer, or had permissions that were too broad for their function. The final screenshot represents a clean and secure browser environment, with the attack surface significantly reduced.

Conclusion

This task provided a comprehensive understanding of browser extension security risks. By methodically reviewing installed extensions and researching real-world malicious examples, I learned to identify key red flags, such as excessive permissions and a lack of reputation. The exercise highlighted that a seemingly simple tool like a browser extension can be a significant vector for cyber threats, and that proactive management is an essential part of maintaining digital security.