CYBER SECURITY INTERNSHIP

Task-7

Identify and Remove Suspicious Browser Extensions

Information

Name: K. Vamsi

Institution: Kalasalingam Academy of Research and Education

Internship Role: Cybersecurity Intern

Submission Date: 14/08/2025

1. Introduction

Browser extensions enhance functionality but can also pose significant security risks. Some appear safe at first but later turn malicious through updates, earning the name **"sleeper agents."** These compromised extensions may track browsing activity, steal sensitive data, or redirect users to harmful sites. Even official web store extensions are not always completely safe. Regularly reviewing installed extensions is essential to maintaining browser security. This report covers the identification and removal of suspicious extensions from the Brave browser.

2. Tools

Browsers

- Brave
- Microsoft Edge
- Google Chrome

3. Methodology

- Browser extensions enhance user functionality but can also be exploited by cybercriminals.
- Even extensions from official web stores can become compromised after an update, allowing malicious actors to.
- Track browsing history.
- Steal sensitive data.
- Redirect traffic to unwanted sites.

When activated, malicious extensions may:

- Capture the URL of every page visited.
- Send it to a remote server along with a unique identifier for tracking.
- Receive redirect instructions from a Command & Control (C&C) server.
- Redirect the browser to attacker-controlled sites.

4. Known Malicious Extensions

The following extensions have been identified as suspicious:

Google Chrome:

- Emoji keyboard online
- Free Weather Forecast
- Unlock Discord
- Dark Theme
- Volume Max
- Unblock TikTok
- Unlock YouTube VPN
- Geco colorpick
- Weather

Microsoft Edge:

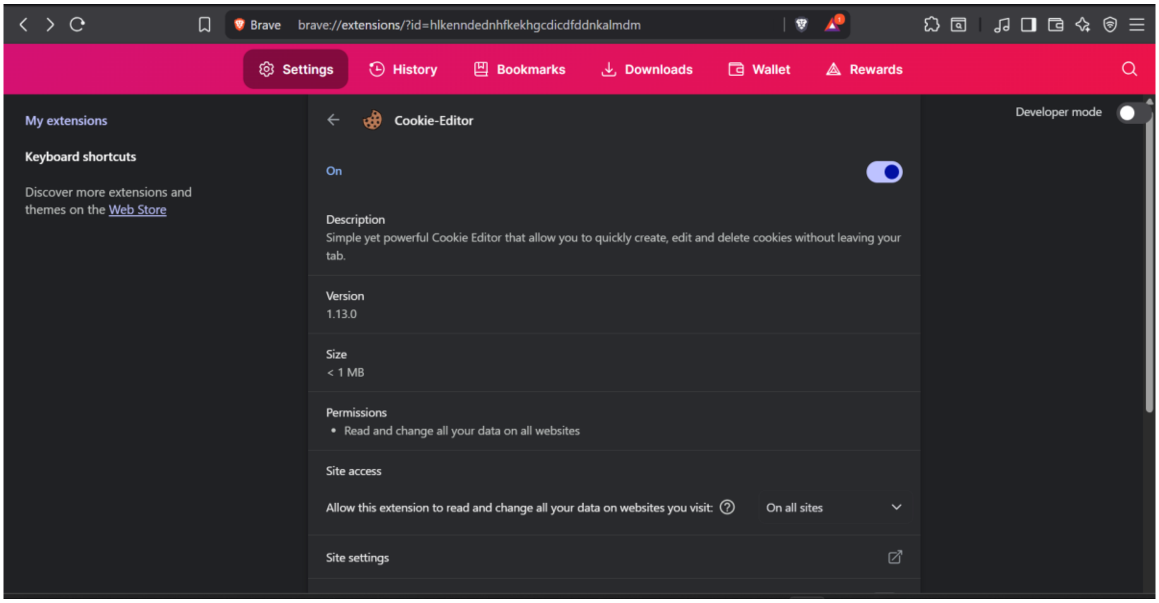
- Unlock TikTok
- Volume Booster
- Web Sound Equalizer
- Header Value
- Flash Player
- Youtube Unblocked
- SearchGPT
- Unlock Discord

1. Open **Brave Browser**.
2. Navigated to brave://extensions/ to view installed extensions.
3. Reviewed each installed extension and compared them with the known malicious list.
4. Checked extension permissions for any unusual or excessive requests.
5. Removed any extensions deemed suspicious.

5. Findings

Installed Extensions in Brave:

1. Cookies Editor



brave://extensions/?id=hlkenndednhfkekhgcdicdfddnkalmdm

Discover more extensions and themes on the Web Store

Cookie-Editor

On

Description
Simple yet powerful Cookie Editor that allow you to quickly create, edit and delete cookies without leaving your tab.

Version
1.13.0

Size
< 1 MB

Permissions
- Read and change all your data on all websites

Site access

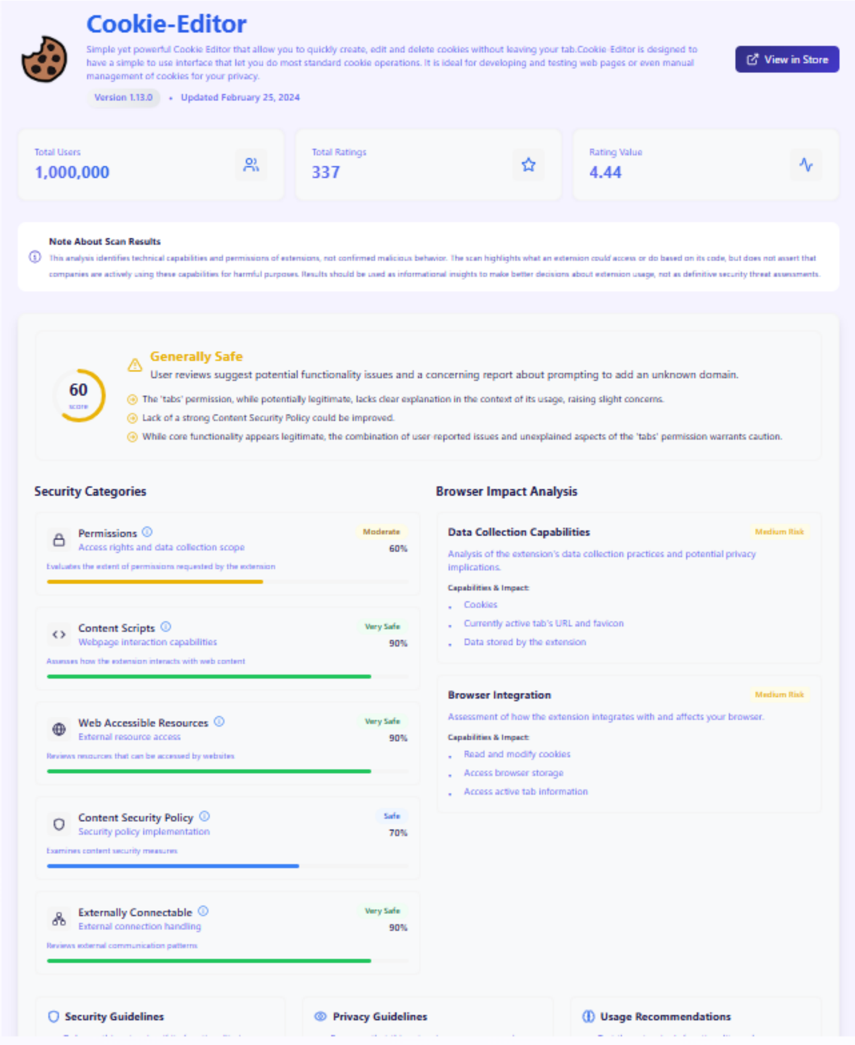
Allow this extension to read and change all your data on websites you visit: On all sites

Site settings

Fig (1): Cookie-Editor

- Open the website: https://crxplorer.com
- Enter the extension ID in the search box.
- If results show excessive permissions or connections to suspicious domains → mark as **Suspicious**.
- If no issues are found mark as **Safe**.

Scan results



Cookie-Editor

Simple yet powerful Cookie Editor that allow you to quickly create, edit and delete cookies without leaving your tab.Cookie-Editor is designed to have a simple to use interface that let you do most standard cookie operations. It is ideal for developing and testing web pages or even manual management of cookies for your privacy.

Version 1.13.0 • Updated February 25, 2024

Total Users 1,000,000

Total Ratings 337

Rating Value 4.44

Note About Scan Results

This analysis identifies technical capabilities and permissions of extensions, not confirmed malicious behavior. The scan highlights what an extension could access or do based on its code, but does not assert that companies are actively using these capabilities for harmful purposes. Results should be used as informational insights to make better decisions about extension usage, not as definitive security threat assessments.

60 score

Generally Safe

User reviews suggest potential functionality issues and a concerning report about prompting to add an unknown domain.

- The 'tabs' permission, while potentially legitimate, lacks clear explanation in the context of its usage, raising slight concerns.
- Lack of a strong Content Security Policy could be improved.
- While core functionality appears legitimate, the combination of user-reported issues and unexplained aspects of the 'tabs' permission warrants caution.

Security Categories

Permissions — Access rights and data collection scope — Moderate 60%
Evaluates the extent of permissions requested by the extension

Content Scripts — Webpage interaction capabilities — Very Safe 90%
Assesses how the extension interacts with web content

Web Accessible Resources — External resource access — Very Safe 90%
Reviews resources that can be accessed by websites

Content Security Policy — Security policy implementation — Safe 70%
Examines content security measures

Externally Connectable — External connection handling — Very Safe 90%
Reviews external communication patterns

Browser Impact Analysis

Data Collection Capabilities — Medium Risk

Analysis of the extension's data collection practices and potential privacy implications.

Capabilities & Impact:

- Cookies
- Currently active tab's URL and favicon
- Data stored by the extension

Browser Integration — Medium Risk

Assessment of how the extension integrates with and affects your browser.

Capabilities & Impact:

- Read and modify cookies
- Access browser storage
- Access active tab information

Security Guidelines

Privacy Guidelines

Usage Recommendations

Fig (2): Scan Results

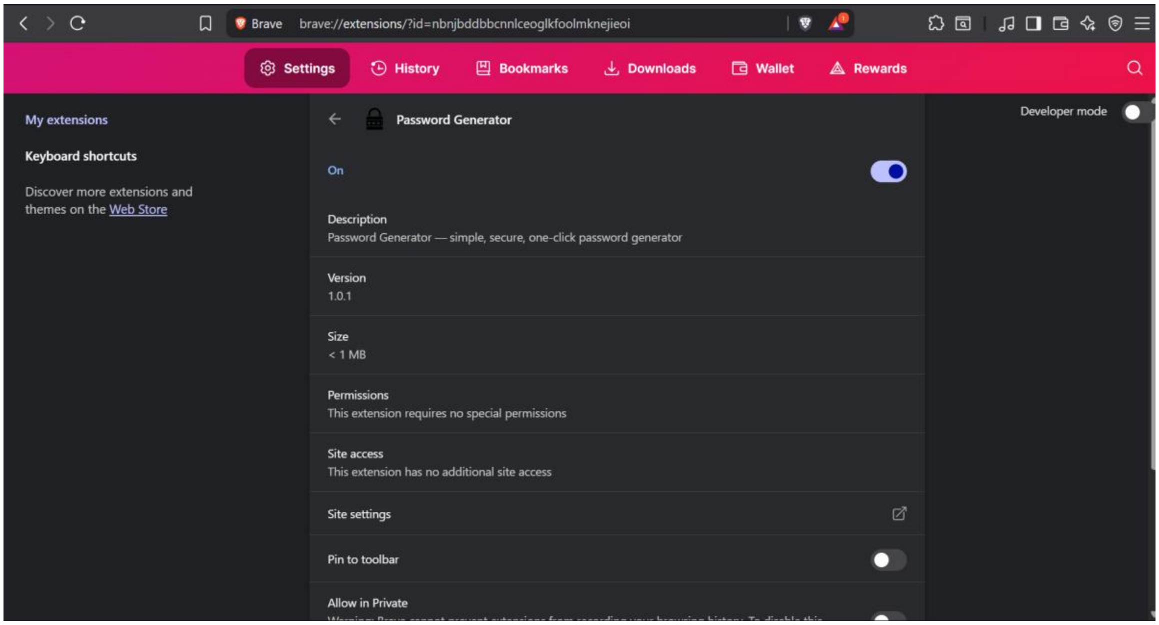
Review the scan results for

- Permissions requested
- External scripts loaded
- Update history
- Any reported security issues

Malicious Extensions Found:

- 60% only safe try to avoid these extension.

2. Password Generator


Brave
brave://extensions/?id=nbnjbddbbcnnlceoglkfoolmknejieoi
Settings
History
Bookmarks
Downloads
Wallet
Rewards
My extensions
Keyboard shortcuts
Discover more extensions and themes on the Web Store
Developer mode

Password Generator

On

Description
Password Generator — simple, secure, one-click password generator

Version
1.0.1

Size
< 1 MB

Permissions
This extension requires no special permissions

Site access
This extension has no additional site access

Site settings

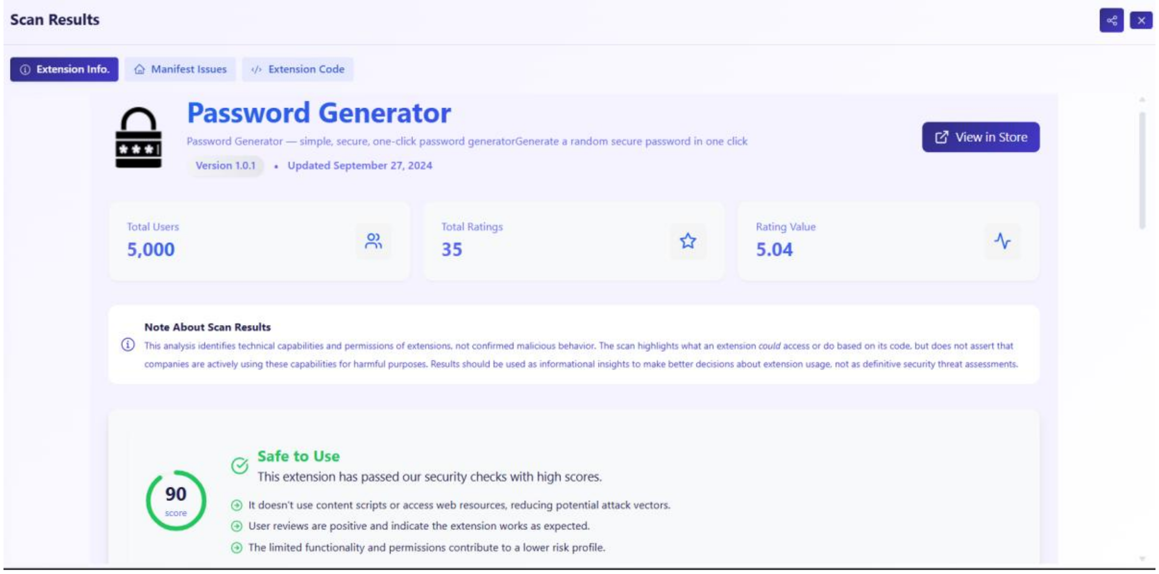
Pin to toolbar

Allow in Private

Fig (3): Password Generator

- Open the website: https://crxplorer.com
- Enter the extension ID in the search box.
- If results show excessive permissions or connections to suspicious domains → mark as **Suspicious**.
- If no issues are found mark as **Safe**.

Scan results



Password Generator

Password Generator — simple, secure, one-click password generatorGenerate a random secure password in one click

Version 1.0.1 • Updated September 27, 2024

Total Users
5,000

Total Ratings
35

Rating Value
5.04

Note About Scan Results

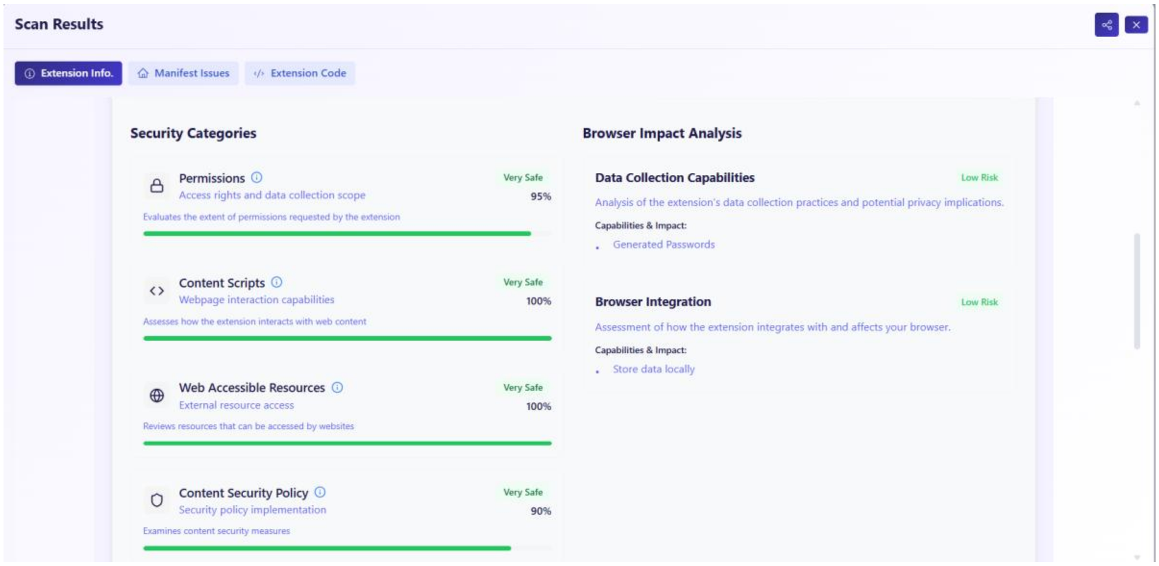
This analysis identifies technical capabilities and permissions of extensions, not confirmed malicious behavior. The scan highlights what an extension *could* access or do based on its code, but does not assert that companies are actively using these capabilities for harmful purposes. Results should be used as informational insights to make better decisions about extension usage, not as definitive security threat assessments.

90
score

Safe to Use

This extension has passed our security checks with high scores.

- It doesn't use content scripts or access web resources, reducing potential attack vectors.
- User reviews are positive and indicate the extension works as expected.
- The limited functionality and permissions contribute to a lower risk profile.



Scan Results

Security Categories

Permissions
Access rights and data collection scope
Very Safe
95%
Evaluates the extent of permissions requested by the extension

Content Scripts
Webpage interaction capabilities
Very Safe
100%
Assesses how the extension interacts with web content

Web Accessible Resources
External resource access
Very Safe
100%
Reviews resources that can be accessed by websites

Content Security Policy
Security policy implementation
Very Safe
90%
Examines content security measures

Browser Impact Analysis

Data Collection Capabilities
Low Risk
Analysis of the extension's data collection practices and potential privacy implications.
Capabilities & Impact:
- Generated Passwords

Browser Integration
Low Risk
Assessment of how the extension integrates with and affects your browser.
Capabilities & Impact:
- Store data locally

Fig (4): Scan Results

Review the scan results for

- Permissions requested
- External scripts loaded
- Update history
- Any reported security issues

Malicious Extensions Found:

- None detected.

Recommendations

- Only install extensions from trusted sources.
- Regularly review installed extensions.
- Check extension permissions after updates.
- Enable two-factor authentication for critical accounts.
- Run periodic security scans using tools like Malwarebytes.