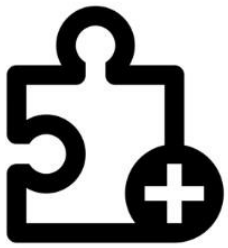


ABOUT BROWSER EXTENSIONS & BCBE

By
ABHINAV KHANNA

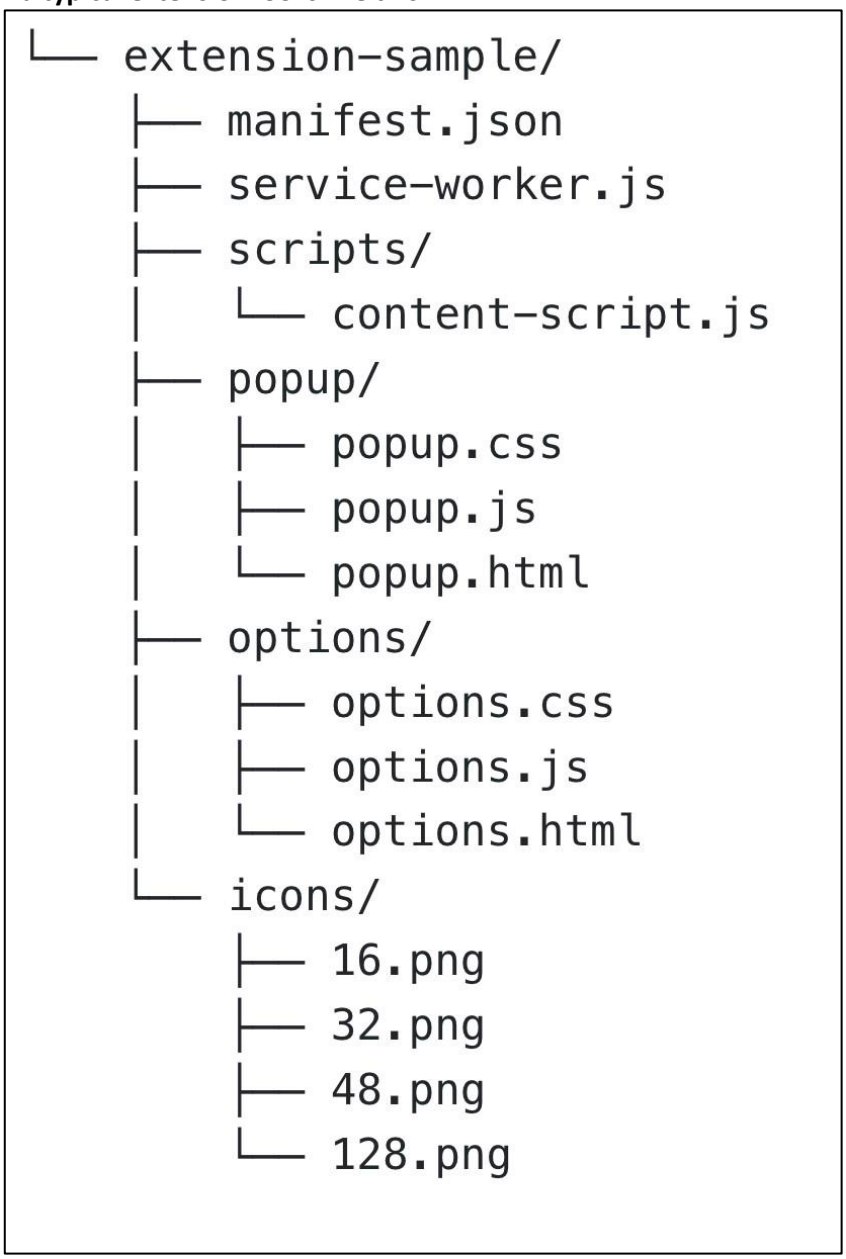
What are Browser Extensions?

Browser extensions are software programs that can be installed within a web browser to enhance its functionality and customize the browsing experience. These extensions are designed to provide additional features, tools, and capabilities to the browser, to improve productivity, or convenience for users.

Some Popular Browser Extensions are:

- Wappalyzer
- Grammarly
- AdBlock
- LastPass

The structure of a typical extension looks like this:



- **Manifest.json**: This is a mandatory file that provides metadata and configuration information about the extension. It defines details like the extension's name, version, permissions, icons, background scripts, content scripts, and more.

- **Popup**: This folder contains files related to the extension's popup, which is a small window that appears when the user clicks the extension icon in the browser's toolbar. The popup can provide a user interface for quick actions or information display.

- **Content scripts**: Content scripts are JavaScript files that can be injected into web pages to interact with and modify their content. They can be used to enhance or alter the behaviour of specific websites.

- **Icons**: This folder contains different sizes of icons used to represent the extension in the browser's user interface. Icons are usually provided in various resolutions to accommodate different display sizes.

- **Background**: This folder contains background scripts that run in the background of the browser, even when the extension's popup or content scripts are not active. Background scripts can be used for tasks like handling events, managing data, and maintaining the extension's state.

- **Matches**: It is a regular expression that defines which URLs or web pages the extension's content script should be injected into. Matches can be found in manifest.json file.

Some Known permissions of chrome extensions:

Permission Name	Description
activetab	Allows the extension to read the content of the currently active tab and interact with it.
storage	Enables the extension to store and retrieve data locally, such as preferences or user settings.
cookies	Grants access to browser cookies, allowing the extension to read, create, modify, and delete cookies.
history	Provides access to the user's browsing history, allowing the extension to query and manipulate the user's browsing history.
unlimitedStorage	Increases the amount of storage that the extension can use without requesting additional storage permissions.
bookmarks	Allows the extension to manage the user's bookmarks, create new bookmarks, and modify existing ones.
tabs	Enables the extension to query and manipulate browser tabs, including opening, closing, and reloading tabs.
Alarms	Allows the extension to schedule and manage alarms, which can trigger events at specific times.
notifications	Enables the extension to display desktop notifications to the user.
downloads	Grants the extension the ability to interact with the browser's download manager and manage downloaded files.

How to load an extension in chrome Browser?

- Open **chrome://extensions**
- Turn on **Developer mode**
- Click on **Load unpacked** and upload the extension

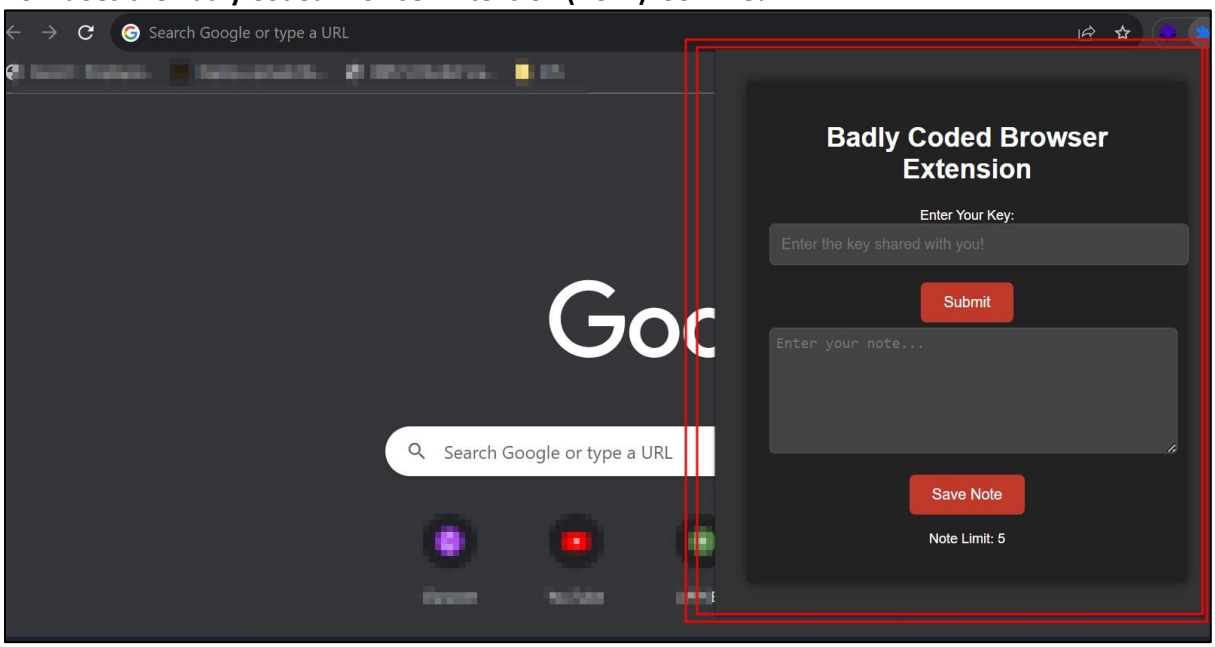
What is Badly Coded Browser Extension (BCBE) and what does it do?

BCBE is a chrome extension designed to show the vulnerabilities in browser extensions. This extension serves as a hands-on learning tool for developers and security professionals. Upon installation of BCBE, users experience simulated vulnerabilities firsthand, highlighting the potential vulnerabilities found in poorly written extensions.

BCBE educates by demonstrating the tangible consequences of unpatched code, overreaching permissions, and improper data handling. Through interactive exercises, users will understand secure development practices, permissions management, and secure data handling for extensions.

By practicing on BCBE, users will be to understand how to perform Browser Extension Security Assessments.

How does the Badly Coded Browser Extension (BCBE) look like?



Some tools that can be used for Extension Assessments:

- ExtAnalysis
- Tarnish
- DoubleX
- CRXcavator
- Burp Suite
- Process Hacker
- JSHint
- BeeF
- Chrome DevTools