

# BROWSER EXTENSION SECURITY PART II






---





**WHY  
BROWSER  
EXTENSION  
SHOULD BE  
SECURED?**

## **BROWSER EXTENSIONS SHOULD BE SECURED FOR SEVERAL REASONS**

-  **Protection against malicious attacks**
-  **User data privacy**
-  **Prevention of unauthorized modifications**
-  **Mitigation of phishing attacks**
-  **Reputation and trust**

# BROWSER SECURITY EXTENSIONS







Windows Defender



BROWSER  
GUARD



1Password



Adblock**Plus**

ExpressVPN

# **USECASES FOR CREATING BROWSER EXTENSION**

**PRODUCTIVITY TOOLS** : Create custom tools to boost productivity,such as to-do lists or note-taking

**WEB DEVELOPMENT** : Build extensions that aid web developers by providing additional debugging tools or code analysis or performance monitoring

**PRIVACY AND SECURITY** : Implement password managers or tools that help users manage their online privacy settings

**CONTENT CUSTOMIZATION** : Customize the appearance and layout of website according to user preferences

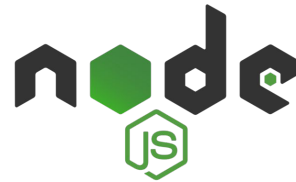
**E-COMMERCE AND PRICE TRACKING** : Build extensions that assist users with online shopping,such as price comparison tools, automatic coupon finders or wish list

**SOCIAL MEDIA ENHANCEMENT** : Develop extensions that enhance online learning experience on social media platforms, like adding extra features ,analytics , or customization options

# LANGUAGES USED IN BACK-END



**PYTHON**





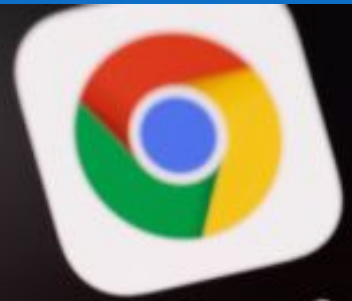
# TYPES OF BROWSERS AND ITS EXTENSIONS



Safari



Edge



Chrome



Firefox



Opera

## CHROME EXTENSIONS(.crx)

- Used in Google Chrome
- Also compatible with chromium-based Browsers like Microsoft Edge, Opera and others.



chrome

Extensions



GRAMMARLY



TODOIST



DARK READER



POCKET



MOMENTUM

## FIREFOX ADD-ONS(.xpi)

- ➔ Used in Mozilla Firefox
- ➔ Some Firefox extensions may also work in browsers based on the Firefox engine





Firefox Browser

# ADD-ONS

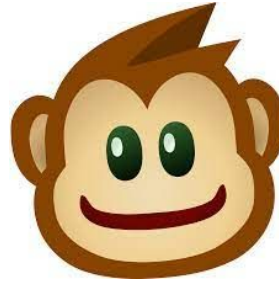
Extensions

Themes

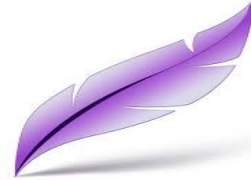
More... ▾



COOKIE AUTO DELETE  
FACEBOOK  
CONTAINER



GREASE  
MONKEY



LIGHT SHOT



COLORZILLA



## EDGE EXTENSIONS(.msix)

- Used in Microsoft Edge
- Microsoft Edge is now built on the Chromium engine, so many Chrome extensions are also compatible







HELPER BIRD

MICROSOFT  
EDITOR

HONEY

GLOOM  
DARK MODEPRESTO MAP  
LEAD  
EXTRACTOR



### **SAFARI EXTENSION(.safariextz)**

- ➔ Used in Apple Safari
- ➔ Safari extensions are designed specifically for the Safari browser on macOS.





## OPERA EXTENSIONS (.oex or .nex)

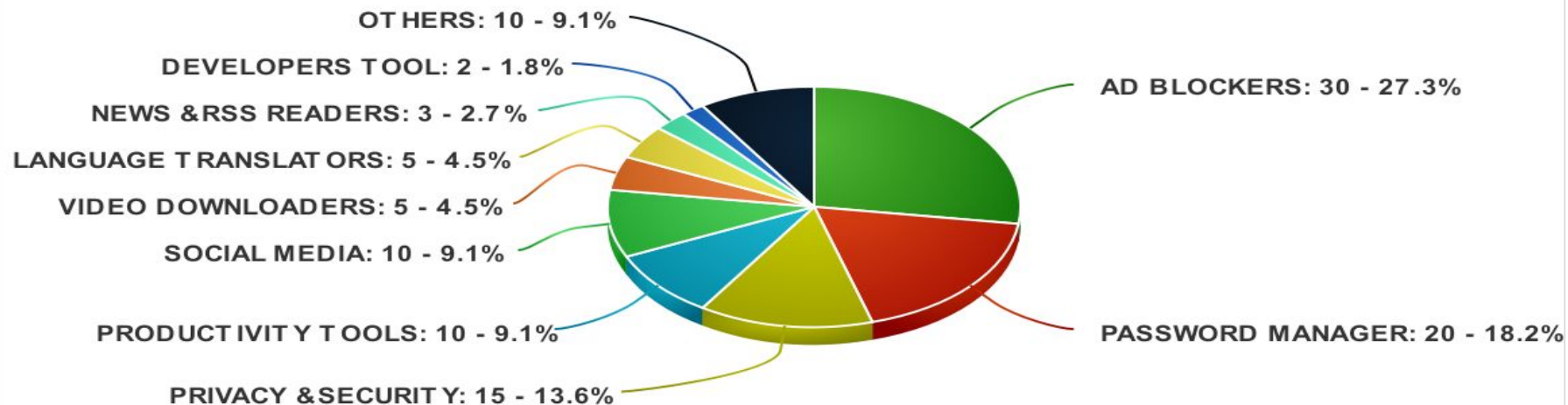
- ➡ Used in the Opera Browser
- ➡ Opera also supports Chrome extensions  
Since its built on the Chromium engine



## **BRAVE EXTENSIONS(.crx)**

- ➡ Used in the Brave Browser
- ➡ Brave supports Chrome extensions due to its Chromium foundation.

## COMMON BROWSER EXTENSIONS USED IN DIFFERENT BROWSERS





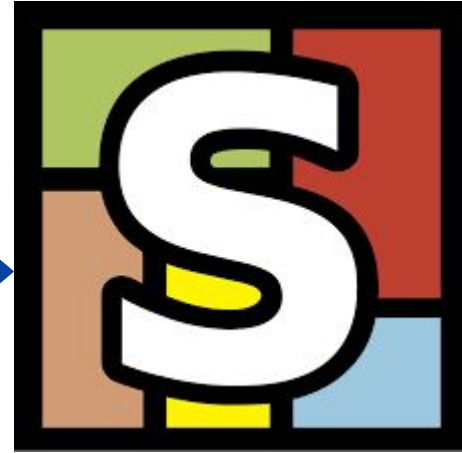
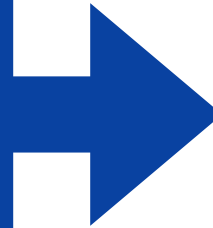
**CASE STUDIES AND  
REAL WORLD  
EXAMPLES  
HIGHLIGHTING THE  
IMPORTANCE OF  
BROWSER  
EXTENSION  
SECURITY**

1. The Web of Trust (WOT) Debacle:  
In 2016, the popular browser extension Web of Trust, which claimed to warn users of potentially malicious websites, was found to be collecting and selling user browsing history without proper anonymization. This breach compromised the privacy of over 140 million users. This incident raised awareness about the need for robust security measures in browser extensions and the importance of vetting trusted developers.

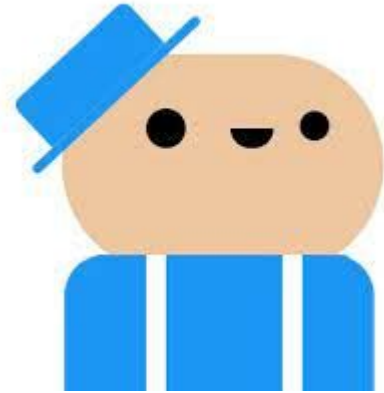


## 2. Stylish Extension Data Leak:

Stylish, a browser extension that let users customize the appearance of websites, was discovered in 2018 to collect and transmit users' browsing history to an external server without their knowledge or consent. This revealed the vulnerability of browser extensions in collecting sensitive user information, emphasizing the importance of transparency and proper permissions for data access.



3. The Great Suspender Incident:  
The Great Suspender, a popular Chrome extension designed to improve browser performance, was sold in 2021 to an unknown entity. Shortly after the acquisition, users reported concerns about suspicious behavior and potential data collection. This incident underlined the need for users to exercise caution when extensions change ownership or undergo significant updates.



#### 4. Microsoft Edge Extension Vulnerability:

In 2019, a vulnerability was discovered in the Microsoft Edge browser that allowed an attacker to bypass security measures and install malicious extensions without user consent. This case highlighted the importance of robust security measures within browsers to prevent unauthorized installations and ensure the integrity of extensions.

