# Identify and Remove Suspicious Browser Extensions

## Objective

To identify, evaluate, and understand the risks associated with browser extensions and ensure that only safe and legitimate extensions remain installed.

## Tools Used

- **Browsers:** Google Chrome, Mozilla Firefox

## Steps Taken

1. **Opened the browser's extension/add-on manager:**
    - **Chrome:** chrome://extensions/
    - **Firefox:** about:addons
2. **Reviewed installed extensions carefully.**
    - Checked names, developers, and installation sources.
3. **Checked permissions and legitimacy.**
    - Verified extension descriptions and reviews on the Chrome Web Store and Mozilla Add-ons page.
4. **Identified potential risks.**
    - Looked for unnecessary permissions such as "Read and change all your data on all websites."
5. **Decided whether to keep or remove each extension.**
    - All installed extensions were found to be legitimate and useful for cybersecurity learning purposes, so none were removed.
6. **Restarted browsers to check for performance.**
    - No performance issues detected.
7. **Researched how malicious extensions can harm users.**
    - Malicious extensions can steal cookies, passwords, or browsing data.
    - They can redirect traffic, inject ads, or track user behavior.
8. **Enabled automatic updates and security checks for extensions.**
    - Ensured that all extensions are set to update automatically to receive the latest security patches and bug fixes.
    - Verified that no third-party or developer mode extensions are enabled to minimize security risks.

**Extensions Reviewed**

**Google Chrome**

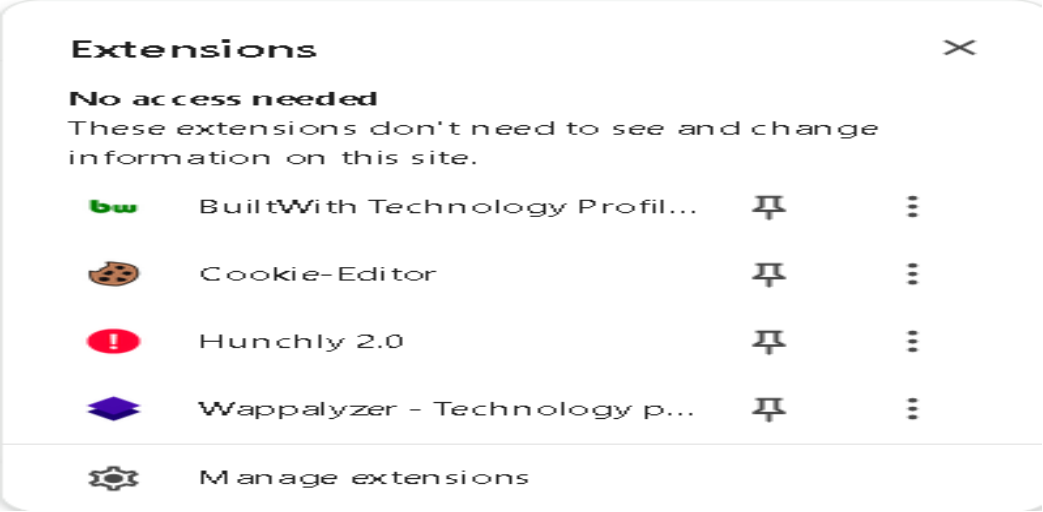
| Extension Name | Purpose | Legitimacy | Action |
|---|---|---|---|
| Cookie-Editor | Used to view, edit, and manage browser cookies for web testing and cybersecurity labs. | ✓ Safe and legitimate. | **Kept** |
| Hunchly 2.0 | Used for web capture and OSINT investigations. | ✓ Safe (official tool). | **Kept** |
| Wappalyzer - Technology Profiler | Identifies website technologies (CMS, frameworks, analytics tools). | ✓ Safe and legitimate. | **Kept** |
| BuiltWith Technology Profiler | Similar to Wappalyzer; detects technologies used by websites. | ✓ Safe but redundant. | **Kept** |

**Mozilla Firefox**

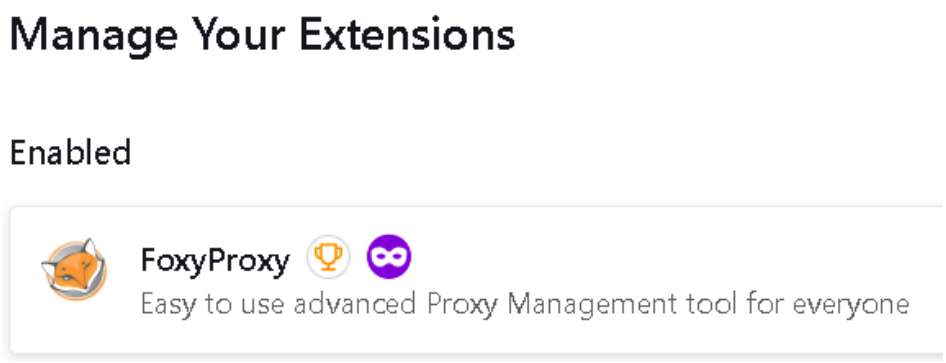
| Extension Name | Purpose | Legitimacy | Action |
|---|---|---|---|
| FoxyProxy | Used to manage proxies during penetration testing and cybersecurity analysis. | ✓ Safe and legitimate. | **Kept** |

**Screenshots**

Chrome Extensions:



Firefox Add-ons:




**Findings**

- All installed extensions are verified and legitimate.
- None show signs of suspicious activity or excessive permissions.
- Browser performance remains stable after review.

**Risks of Malicious Browser Extensions**

- Can **steal sensitive data** such as cookies, passwords, or browsing history.
- May **inject advertisements or malicious code** into websites.
- Can **redirect users** to phishing or scam pages.
- Might **track user behavior** without consent.

**Outcome**

- Gained awareness of how to identify and verify browser extensions.
- Confirmed that all extensions currently installed are safe and necessary for cybersecurity learning.
- Improved understanding of how malicious extensions can compromise browser security.

**Conclusion**

- No suspicious extensions were found.
  All installed extensions are legitimate, educational, and useful for cybersecurity purposes.
  Browser security awareness improved after completing this task.