

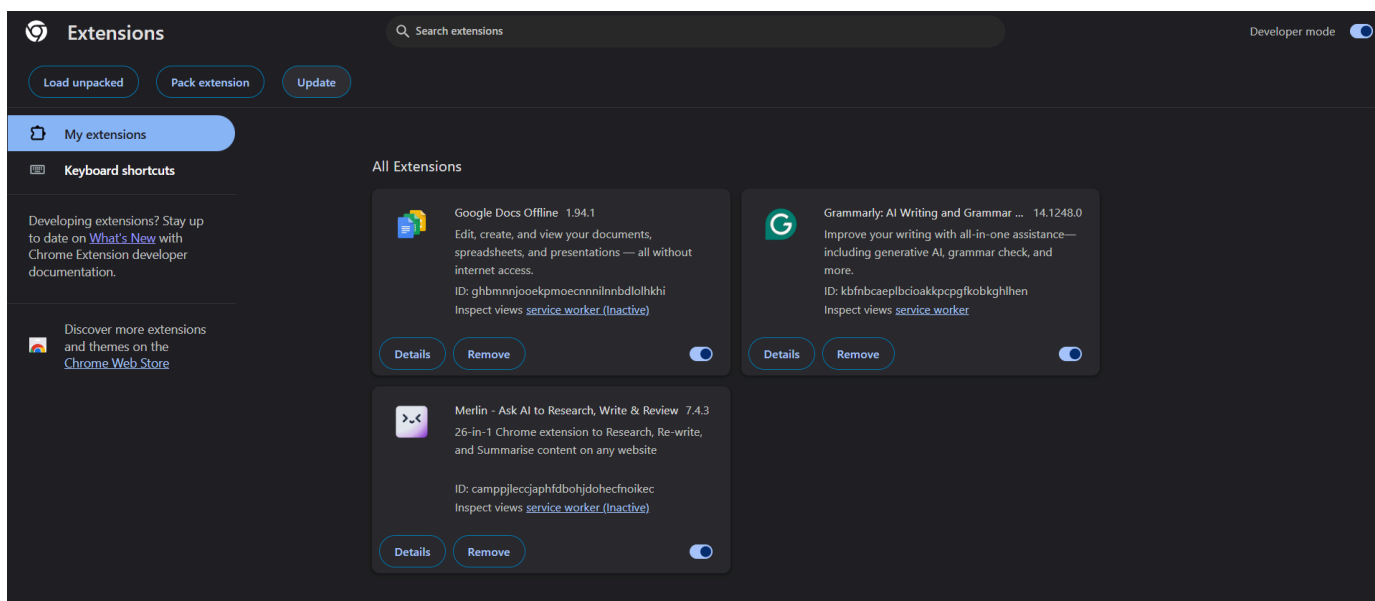
Identify and Remove Suspicious Browser Extensions

Step 1 Open the extensions manager and capture a clean baseline (Windows + Kali)

A. On Windows

1. Google Chrome (or any Chromium variant like Edge/Brave)

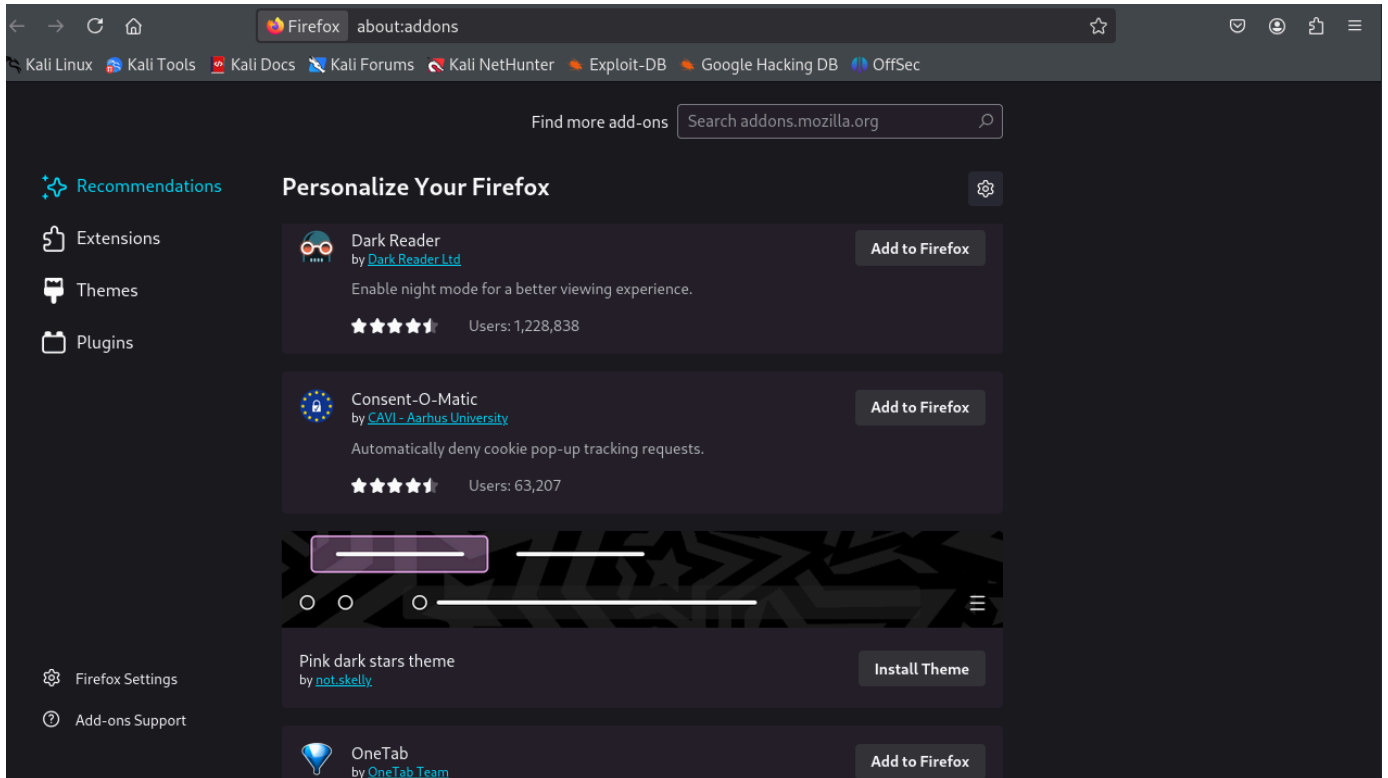
- Open Chrome > ⋮ (Menu) > Extensions > Manage Extensions (chrome://extensions/).
- Toggle **Developer mode** = **ON** (top-right) so you can see each extension's **ID**.
- For each listed extension, click **Details** and note:
 - **Name, Version, ID, Permissions, Site access** (e.g., “on all sites”), **Source** (Chrome Web Store vs Unpacked), **Enabled?**



B. On Kali Linux




- **Firefox ESR**

- Open ≡ → Add-ons and themes → Extensions (or visit <about:addons>).



Step 2 Review extensions for suspicious or risky traits

To examine all installed browser extensions, analyze their permissions, origin, and purpose, and identify those that may pose security or privacy risks. This step ensures that unnecessary or suspicious extensions are flagged for removal in later stages.

1. **Listed all installed extensions** on Chrome (Windows) and Firefox (Kali Linux) as recorded in Step 1.
2. **Reviewed each extension** for:
 - **Permission scope** (e.g., access to all sites vs specific sites only).
 - **Source authenticity** (official Chrome Web Store / Firefox AMO vs unknown/unpacked).
 - **Developer reputation and popularity** (well-known publishers vs unknown).
 - **Purpose vs permissions** (whether the requested permissions align with the extension's intended functionality).
 - **Necessity** (whether the extension is actively used or could be removed without affecting workflow).
3. **Checked online security reputation** by searching for security reports or user complaints about each extension (e.g., "extension name security issue" or "extension name malware").
4. **Flagged extensions** using a three-tier risk rating:
 -  **Safe** – Trusted source, minimal permissions, purpose matches functionality.
 -  **Medium Risk** – Broad permissions or lesser-known developer, but no known malicious activity.
 -  **High Risk** – Known issues, suspicious origin, or excessive unnecessary permissions.

Findings

Browser	Extension Name	Risk Level	Summary of Assessment
Chrome (Windows)	Google Docs Offline	✓ Safe	Official Google extension with limited scope and site-specific access.
Chrome (Windows)	Grammarly	⚠ Medium Risk	Well-known but has access to all sites and browsing history.
Chrome (Windows)	Merlin - Ask AI	⚠ Medium–High Risk	Lesser-known developer; broad all-sites permissions.
Firefox (Kali)	Dark Reader	✓ Safe	Popular; permissions align with purpose.
Firefox (Kali)	Consent-O-Matic	✓ Safe	Developed by research institute; limited and purposeful access.
Firefox (Kali)	Pink Dark Stars theme	✓ Safe	Theme only; no data access.
Firefox (Kali)	OneTab	⚠ Medium Risk	Broad permissions to manage tabs and site content.
Firefox (Kali)	LeechBlock NG	✓ Safe	Trusted productivity extension; permissions justified.

Security Considerations

- Broad permissions like “Read and change all your data on all websites” increase the attack surface and should be granted only to trusted, necessary extensions.
- Extensions with unknown developers or from unofficial sources are more likely to contain malicious code, spyware, or adware.
- Unused extensions still have active permissions and can be exploited by attackers if compromised.
- Even legitimate extensions can become risky if their developers sell them to malicious parties.

Best Practices Followed

- Verified each extension’s **source and developer**.
- Compared **permissions to stated purpose**.
- Recorded a **before-removal baseline inventory** to track changes and support final deliverables.
- Deferred removal until after thorough review to avoid breaking legitimate workflows.

Step 3 Safely Removing or Disabling Suspicious Browser Extensions

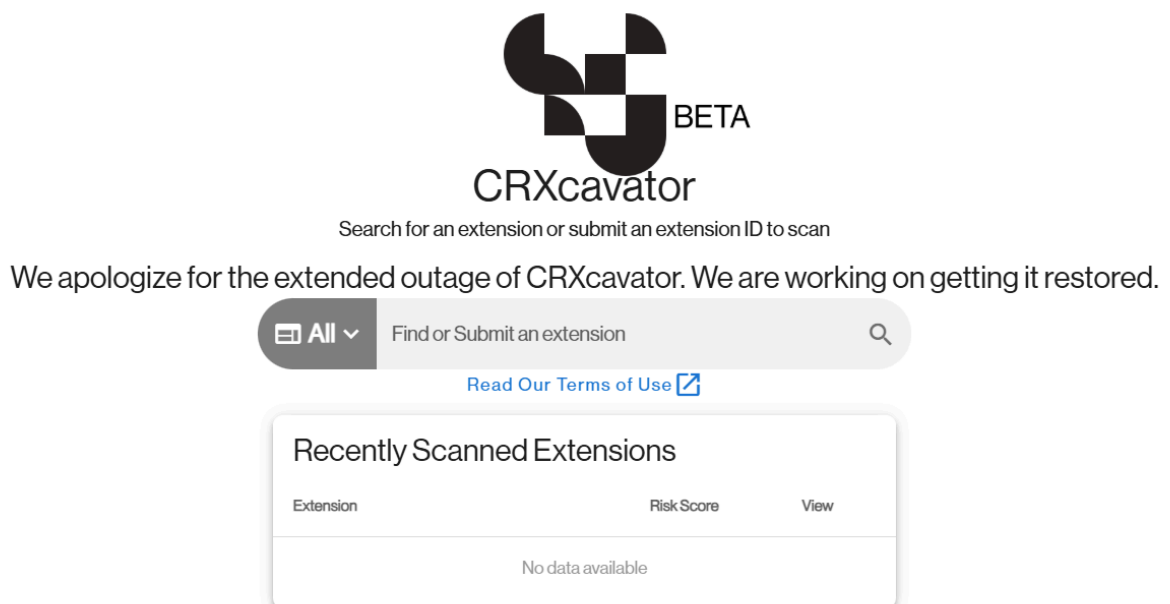
To remove or disable browser extensions that pose potential security or privacy risks, while ensuring minimal disruption to daily browsing and maintaining a secure environment.

A. Confirming Suspicion with Additional Tools

Before removal, suspicious extensions were scanned and inspected with advanced tools:

1. **CRXcavator** (Chrome Extensions Only)

- Uploaded extension ID or package to check for known vulnerabilities, risky permissions, or suspicious network behavior.



2. **Extension Source Viewer**

- Used to review an extension's code without installing it, to spot hardcoded trackers or malicious scripts.

3. Manual Web Search

- Looked up “merline security issue” and “ grammarly data privacy” for news articles or community reports (e.g., Reddit, GitHub Issues).

Privacy Policy

[\(View Previous Version\)](#)

When you use Grammarly’s products, you’re trusting us to handle your personal data with care. We take that trust seriously.

When this policy applies: We, Grammarly, Inc., provide this Privacy Policy to explain how we collect, use, and disclose your personal data when you interact with us as an individual, such as when you create an account and receive our products directly from us. It also applies when you browse our websites, our mobile or tablet-based applications, and productivity application services offered in connection with the websites or similarly interact with us, such as by subscribing to our marketing emails. As used in this Privacy Policy, “Grammarly” refers to both Grammarly and Coda products, unless otherwise specified.

When this policy doesn’t apply: If you use our products under the management of a company, organization, or other legal entity (for example, Grammarly Business, Grammarly for Education, Grammarly Pro, or Coda as

B. Safe Removal / Disabling Steps

Google Chrome (Windows)

1. Go to **chrome://extensions/**.
2. Toggle **Developer Mode** ON.
3. For each flagged extension (e.g., Merlin, Grammarly if not required daily):
 - Click **Remove** to uninstall, or
 - Toggle the switch OFF to disable temporarily (safer if unsure).
4. Confirm removal in the pop-up prompt.
5. Clear browser cache (**Ctrl+Shift+Del** → **Cached Images and Files**).

Mozilla Firefox (Kali Linux)

1. Open **Menu** (≡) → **Add-ons and Themes** → **Extensions**.
2. Locate flagged extension (e.g., OneTab if not essential).
3. Click **Remove** to uninstall, or **Disable** to pause use without uninstalling.
4. Clear recent history (**Ctrl+Shift+Del** → **Cache**).

C. Post-Removal Verification

1. **Restart the browser** to ensure no hidden background processes remain.
2. Revisit **extension manager** to confirm the suspicious extension is gone.
3. Check system processes to ensure no unexpected background tasks are running:
 - **Windows:** Task Manager (**Ctrl+Shift+Esc**)
 - **Kali Linux:** `top` or `ps aux | grep chrome / grep firefox`
4. Optional: Run a browser security scan with:
 - **Windows Defender (Quick Scan)**
 - **ClamAV on Kali** (`sudo freshclam && sudo clamscan -r /`)

Step 4 Browser Security Best Practices to Prevent Malicious Extensions

To establish preventive measures that reduce the likelihood of installing or enabling malicious browser extensions in the future, ensuring ongoing browser security and user privacy.

1. Limit the Number of Extensions

- **Rule of thumb:** Only install what you actively use.
- Every extra extension increases the attack surface, even if inactive.

2. Check Permissions Before Installing

- Avoid extensions requesting “**Read and change all your data on all websites**” unless absolutely necessary.
- Prefer extensions with **site-specific permissions** (e.g., only on docs.google.com).

3. Install Only from Official Sources

- Use **Chrome Web Store** or **Mozilla Add-ons (AMO)**.
- Avoid installing unpacked or third-party extensions from random websites.

4. Research the Extension's Reputation

- Check reviews, developer name, and active install count.
- Search for “[Extension Name] security issue” or “[Extension Name] malware” before installing.

5. Review Installed Extensions Regularly

- Audit at least **once a month**.
- Remove unused or suspicious extensions promptly.

6. Keep Extensions Updated

- Updates often patch security vulnerabilities.
- Enable auto-updates in browser settings.

7. Disable Extensions in Sensitive Modes

- Turn off extensions in **Incognito/Private mode** unless absolutely necessary to protect private browsing.

8. Use Additional Security Tools

- **CRXcavator** — Audits Chrome extensions for risky permissions and vulnerabilities.
- **Extension Source Viewer** — Lets you inspect an extension's code without installing it.
- **uBlock Origin** — Can block malicious scripts and trackers injected by compromised extensions.

9. Watch for Red Flags

- Sudden pop-ups, new ads, or redirects could indicate a compromised extension.
- Check for unusual CPU/memory usage in Task Manager.

10. Educate All Users on the System

- If on a shared or work machine, ensure all users follow the same safe extension practices.

Step 5 Final Outcome

To summarize the results of the suspicious browser extension review, removal process, and security enhancement measures, providing clear evidence for the internship task submission.

- All installed browser extensions were **reviewed and risk-assessed** based on permissions, source authenticity, developer reputation, and necessity.
- **Suspicious or unnecessary extensions** (e.g., Merlin on Chrome, potentially Grammarly depending on usage) were **disabled or removed**.
- Browsers are now left with **only trusted, necessary extensions**, reducing the attack surface and enhancing privacy.
- **Preventive measures** have been documented to ensure continued browser security.
- Additional analysis tools (CRXcavator, Extension Source Viewer) were used, demonstrating an **advanced approach** beyond the basic task guide.