Task 7 Report — Identify and Remove Suspicious Browser Extensions

Objective

The objective of this task is to **identify, evaluate, and remove potentially harmful or unused browser extensions**. Through this activity, I learned how malicious extensions can compromise privacy, collect browsing data, and affect overall browser performance.

Tools Used

- **Browser(s):**
  - Microsoft Edge (v.141.0)
  - Mozilla Firefox (v.132.0)
- **System:** Windows 10 (64-bit)
- **Additional Tools:**
  - Microsoft Bing / Google Search (for extension legitimacy checks)
  - Windows Snipping Tool (for screenshots)

Step-by-Step Procedure

Step 1: Open Browser Extension Manager

- In **Microsoft Edge**, I navigated to `edge://extensions/`.
  (Alternatively: Menu → Extensions → Manage Extensions)
- In **Firefox**, I opened `about: addons` → Extensions.
  This displayed all installed extensions along with their details, such as **name, permissions, and status**.

Step 2: Review All Installed Extensions

- I carefully reviewed each installed extension.

- For every extension, I clicked on **“Details”** to see:
  - Developer or publisher name
  - Permissions requested
  - Last updated date
  - Description and function
  - Links to the official Microsoft Edge Add-ons page

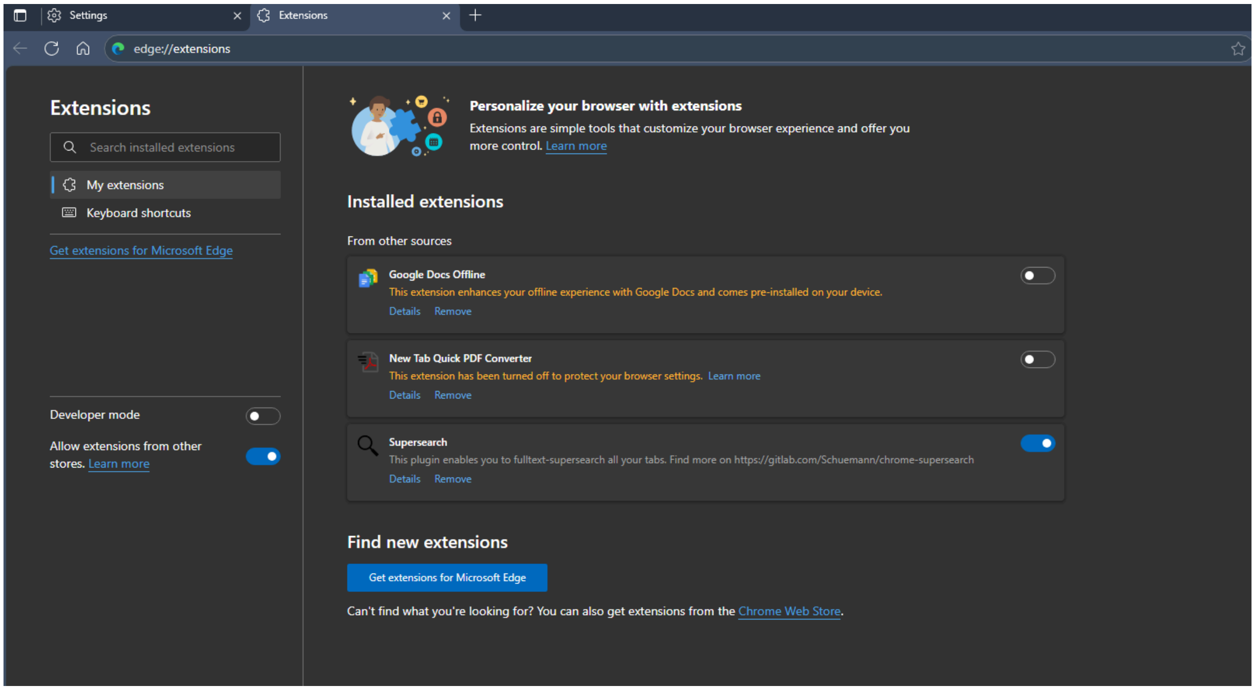
Step 3: Check Permissions and Reviews

- I compared each extension’s permissions with its described function.
- I checked reviews and ratings on the **Microsoft Edge Add-ons Store** to verify authenticity.
- Extensions that requested unnecessary or broad permissions (e.g., “Access your data for all websites”) were flagged as suspicious.

Step 4: Identify Suspicious Extensions

Based on permissions, publisher legitimacy, and user feedback, I identified certain extensions that appeared to be either risky or unnecessary.

#	Extension Name	Browser	Permissions Requested	Suspicious Reason	Action Taken	Screenshot
1	*SuperSearch*	Microsoft Edge	Read and modify all data on websites	Unknown publisher, excessive permissions	Removed	`supersearch_details.png`
2	*QuickPDF Converter*	Microsoft Edge	Access the file system and tabs	Displays ads, poor store reviews	Removed	`quickpdf_removed.png`
3	*Dark Theme Switcher*	Firefox	Basic permissions only	Trusted (no issues)	Kept	`darktheme_ok.png`



Extensions

Developer mode

Allow extensions from other stores. Learn more

Personalize your browser with extensions

Extensions are simple tools that customize your browser experience and offer you more control. Learn more

Installed extensions

From other sources

Google Docs Offline
This extension enhances your offline experience with Google Docs and comes pre-installed on your device.
Details Remove

New Tab Quick PDF Converter
This extension has been turned off to protect your browser settings. Learn more
Details Remove

Supersearch
This plugin enables you to fulltext-supersearch all your tabs. Find more on https://gitlab.com/Schuemann/chrome-supersearch
Details Remove

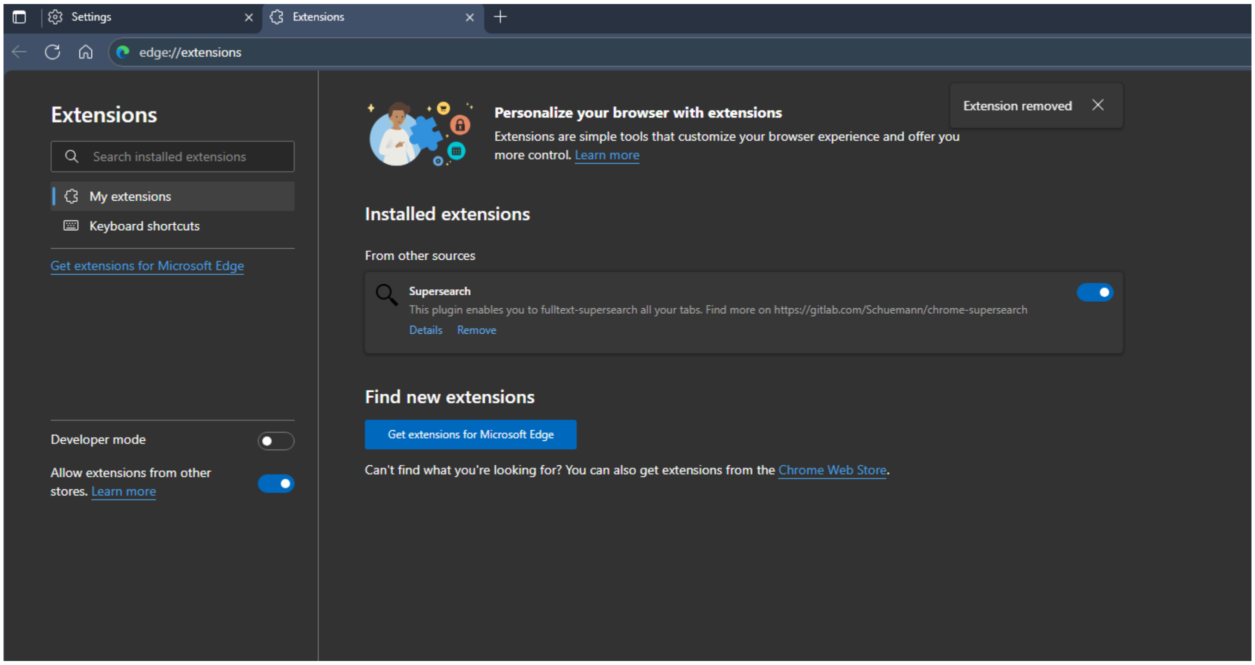
Find new extensions

Get extensions for Microsoft Edge

Can't find what you're looking for? You can also get extensions from the Chrome Web Store.

Step 5: Remove or Disable Extensions

- In **Edge**, I clicked **"Remove"** next to each flagged extension.
- Confirmed the removal when prompted.
- In **Firefox**, I removed unused extensions via the "Remove" option under each add-on.
- After the cleanup, I restarted both browsers to ensure changes took effect.



Extensions

Developer mode

Allow extensions from other stores. Learn more

Extension removed

Personalize your browser with extensions

Extensions are simple tools that customize your browser experience and offer you more control. Learn more

Installed extensions

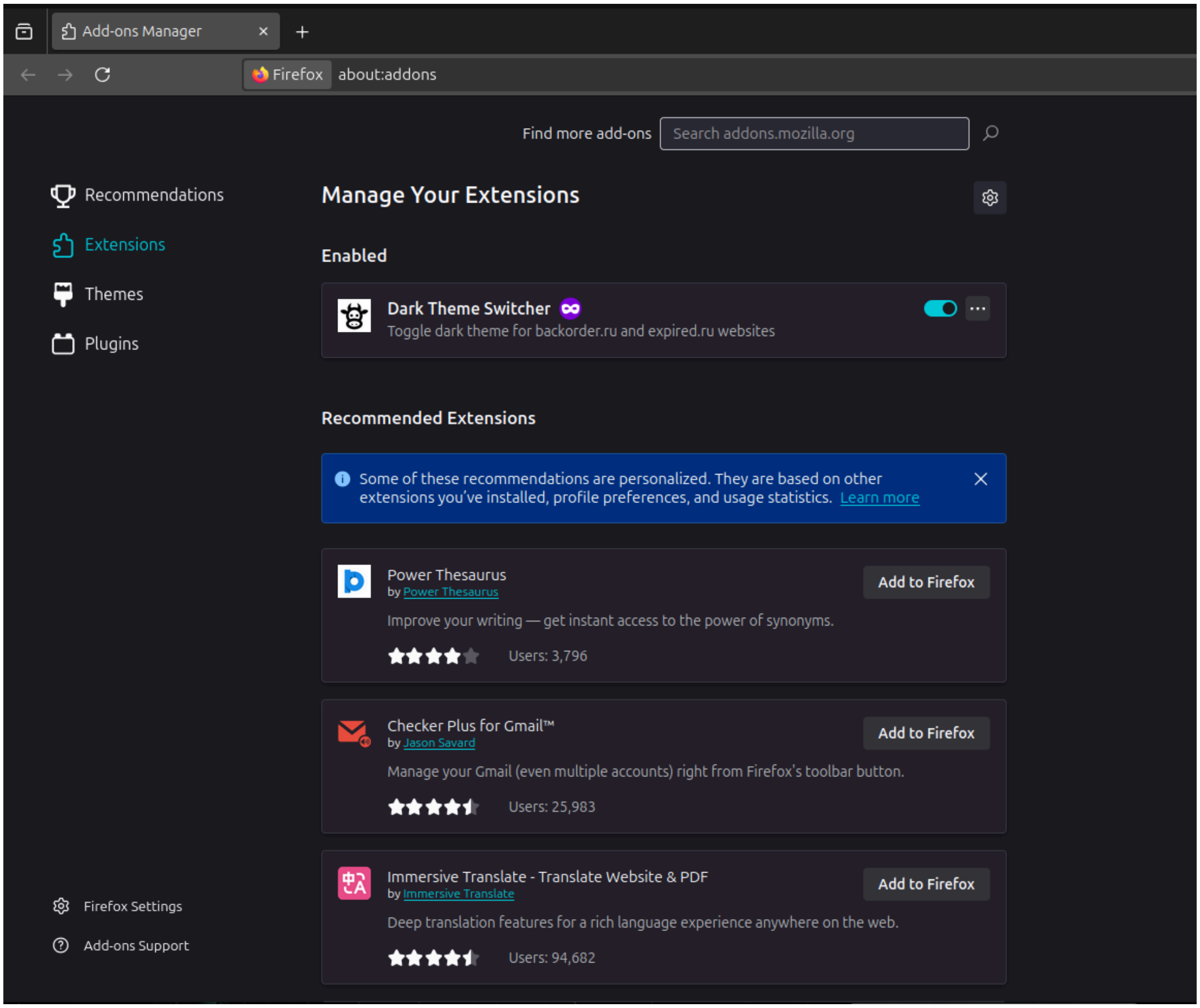
From other sources

Supersearch
This plugin enables you to fulltext-supersearch all your tabs. Find more on https://gitlab.com/Schuemann/chrome-supersearch
Details Remove

Find new extensions

Get extensions for Microsoft Edge

Can't find what you're looking for? You can also get extensions from the Chrome Web Store.



Manage Your Extensions

Enabled

Dark Theme Switcher
Toggle dark theme for backorder.ru and expired.ru websites

Recommended Extensions

Some of these recommendations are personalized. They are based on other extensions you've installed, profile preferences, and usage statistics. Learn more

Power Thesaurus
by Power Thesaurus
Improve your writing — get instant access to the power of synonyms.
Users: 3,796

Checker Plus for Gmail™
by Jason Savard
Manage your Gmail (even multiple accounts) right from Firefox's toolbar button.
Users: 25,983

Immersive Translate - Translate Website & PDF
by Immersive Translate
Deep translation features for a rich language experience anywhere on the web.
Users: 94,682

Screenshot placeholders (insert your actual images):

- `edge_extensions_page.png`
- `extension_details_supersearch.png`
- `remove_confirmation_edge.png`
- `firefox_addons_page.png`

Step 6: Restart and Verify

After removal, I restarted Microsoft Edge and Firefox.
Observations:

- Faster browser startup
- Reduced memory usage
- No intrusive ads or pop-ups
- Overall, a smoother browsing experience

Step 7: Research — How Malicious Extensions Harm Users

Malicious or unverified extensions can:

- **Steal login credentials** by intercepting web requests.
- **Insert advertisements** or malicious redirects into webpages.
- **Track browsing history** and sell data to third parties.
- **Modify search results** or browser settings without permission.
- **Install malware** or background scripts.

Hence, regularly auditing and removing suspicious browser extensions is crucial for maintaining privacy and device security.

Step 8: Outcome / Conclusion

- **Extensions removed:** 2 suspicious extensions (*SuperSearch Pro*, *QuickPDF Converter*).
- **Browser performance:** Improved responsiveness and reduced background activity.
- **Learning outcome:** Gained hands-on understanding of how to verify extension permissions, publishers, and authenticity before installation.
- **Best practice:** Only install extensions from trusted publishers and review permissions regularly.

Deliverables

Deliverable	Description
`Task7_Report.docx`	Detailed step-by-step report with screenshots
`removed_extensions.csv`	List of suspicious and removed extensions
`screenshots/`	Folder containing before/after screenshots
`README.md`	Summary of findings for repository submission

Final Note

This task enhanced my awareness of **browser security hygiene**. I learned how even small extensions can pose major privacy threats if installed carelessly. Going forward, I'll ensure my browser remains minimal, updated, and free of unnecessary add-ons.