Task 7 :Identify and Remove Suspicious Browser Extensions

Objective: Learn to spot and remove potentially harmful browser extensions.

Tools: Any web browser (Chrome, Microsoft Edge)
Operating System: Windows 10/11
Internet Access for researching suspicious extensions
Security Check Platforms:
1. Chrome Web Store
2. Firefox Add-ons

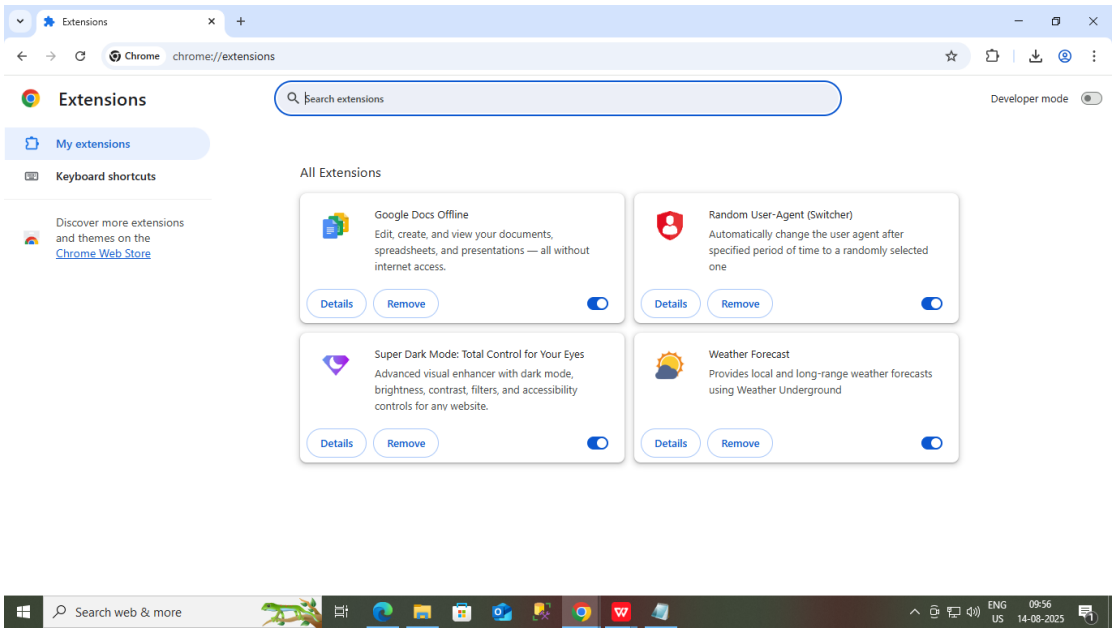
Steps Included:

1. Google Chrome Browser

➢ Opening Extension Manager

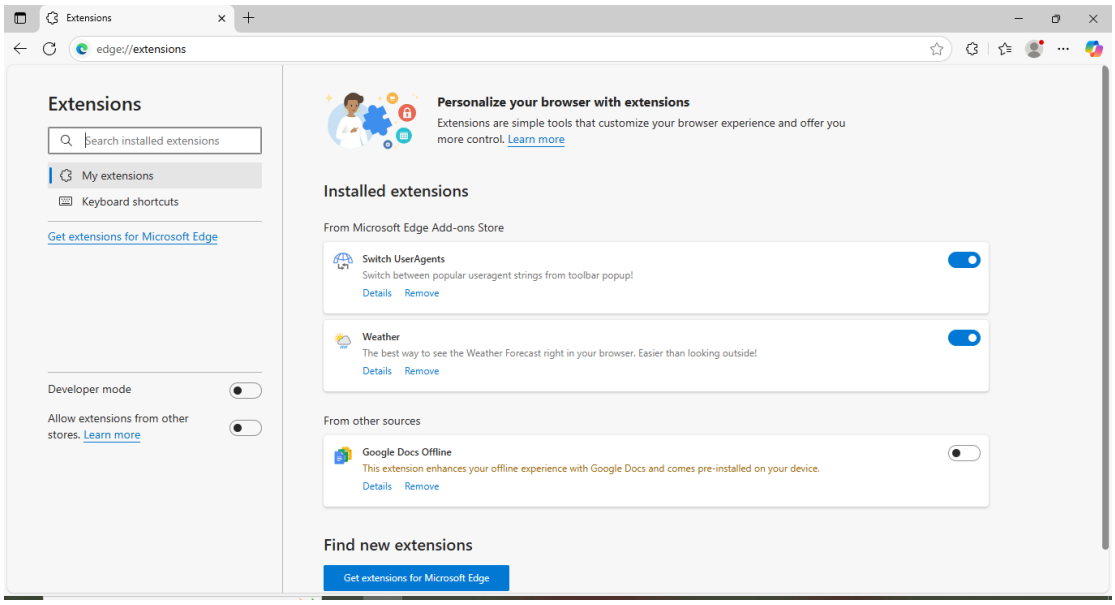
Steps:

Click Menu (⋮) → More Tools → Extensions
(Shortcut: chrome://extensions/)



2. **Microsoft Edge Browser**

Click Menu (⋯) → Extensions → Manage Extensions
(Shortcut: edge://extensions/)



Documented Installed Extensions

Browser	Extension Name	Publisher	Permissions Granted	Status
Microsoft Edge	Switch UserAgents	Microsoft Edge Add-ons Dev	Switch between popular user-agent strings from toolbar popup	Removed (test)
Microsoft Edge	Weather	Microsoft Edge Add-ons Dev	Provide weather forecast info, may request location access	Removed (test)
Microsoft Edge	Google Docs Offline	Google LLC	Enhance offline experience with Google Docs	Kept
Google Chrome	Random User-Agent (Switcher)	Chrome Web Store Developer	Automatically change user-agent per selected period	Removed (test)
Google Chrome	Super Dark Mode: Total Control	Chrome Web Store Developer	Modify appearance of all websites, apply dark mode	Removed (test)
Google Chrome	Weather Forecast	Chrome Web Store Developer	Provide weather forecast info, may request location access	Removed (test)
Google Chrome	Google Docs Offline	Google LLC	Edit, create, and view Google Docs, Sheets, and Slides offline	Kept

Identifying & Researching Suspicious Indicators:

Microsoft Edge

A. Switch UserAgents

Risk:

1. Can disguise the browser identity, potentially bypassing site restrictions.

2. May be abused to impersonate other devices, which could be used for malicious activities like evading security filters.

3. Requires all-site access, which could allow interception or manipulation of website data.

B. Weather

Risk:

1. Requests location access — this could be misused for tracking user movements.

1. Might collect browsing patterns alongside location to profile the user.

2. Some weather extensions have been reported to inject ads or redirect to affiliate links.

C. Google Docs Offline (Kept)

Risk:

1. Developed by Google, minimal risk, but still has access to offline documents.

2. If compromised, could expose stored offline document data.

Google Chrome

A. Random User-Agent (Switcher)

Risk:

1. Similar risks to Switch UserAgents — can bypass detection, but if abused, could facilitate malicious browsing behavior.

2. All-site access means it can monitor or alter traffic.

B. Super Dark Mode: Total Control

Risk:

1. Requires permission to modify the content of all websites to apply dark mode.

2. This capability could be exploited to inject malicious scripts or ads.

3. Some dark mode extensions have been caught mining cryptocurrency in the background.

C. Weather Forecast

Risk:

1. Same as the Edge “Weather” extension — location tracking risk.

2. Could collect and sell geolocation data to third parties.

3. Potential for injecting ads in forecast pages.

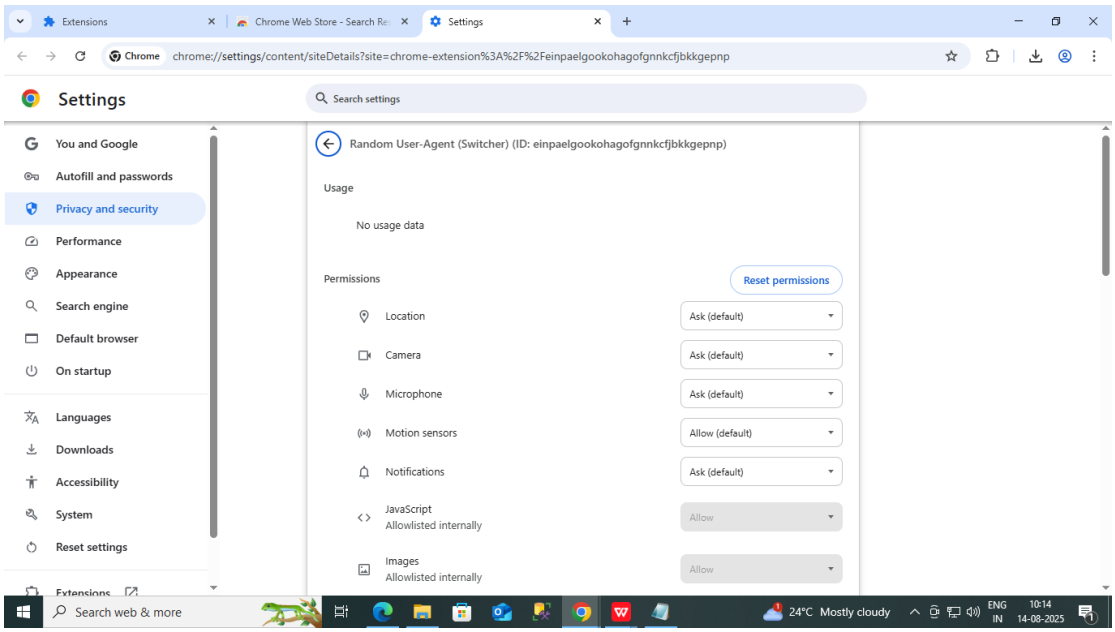
D. Google Docs Offline (Kept)

Risk:

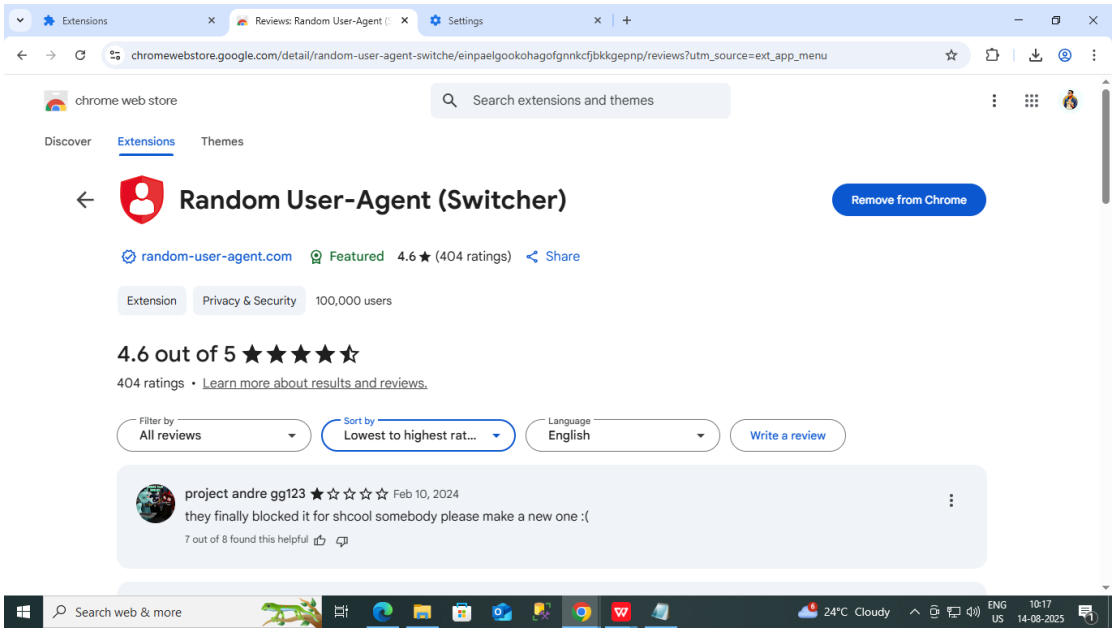
1. Trusted source, but same minimal risk of offline document exposure if browser or extension is compromised.

❖ Researching the Extension

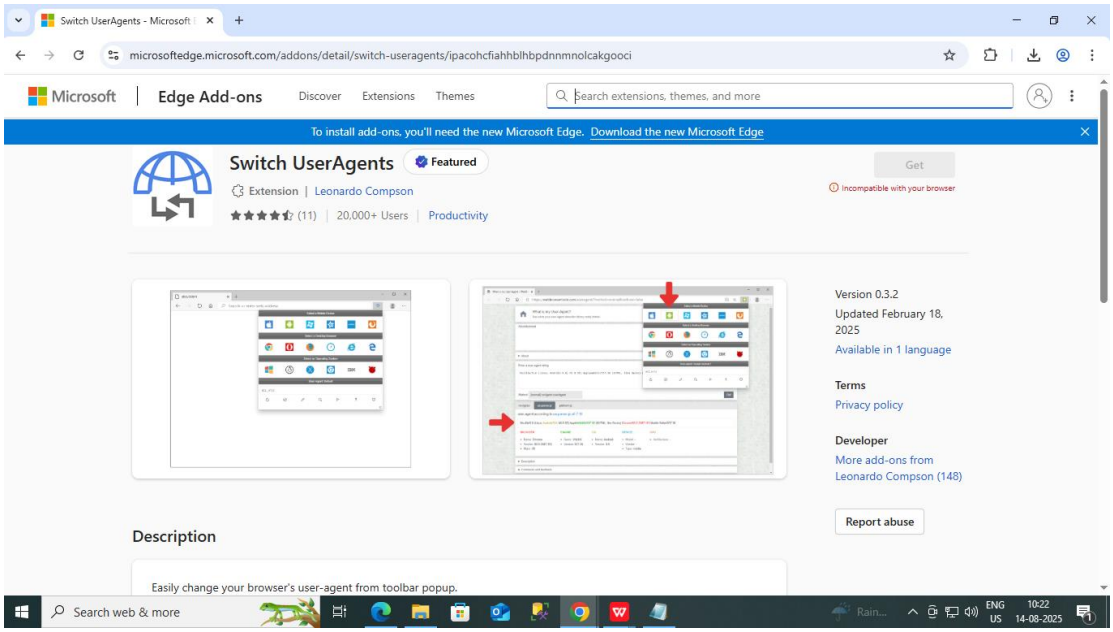
Checking Permission for Each Extension:



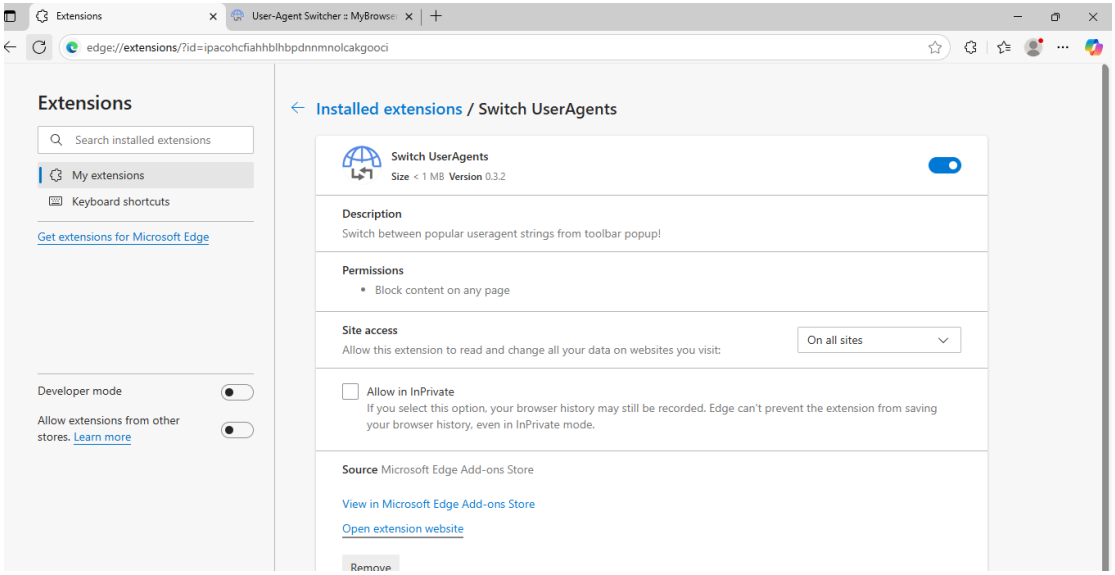
Checking Reviews on Chrome Web Store:



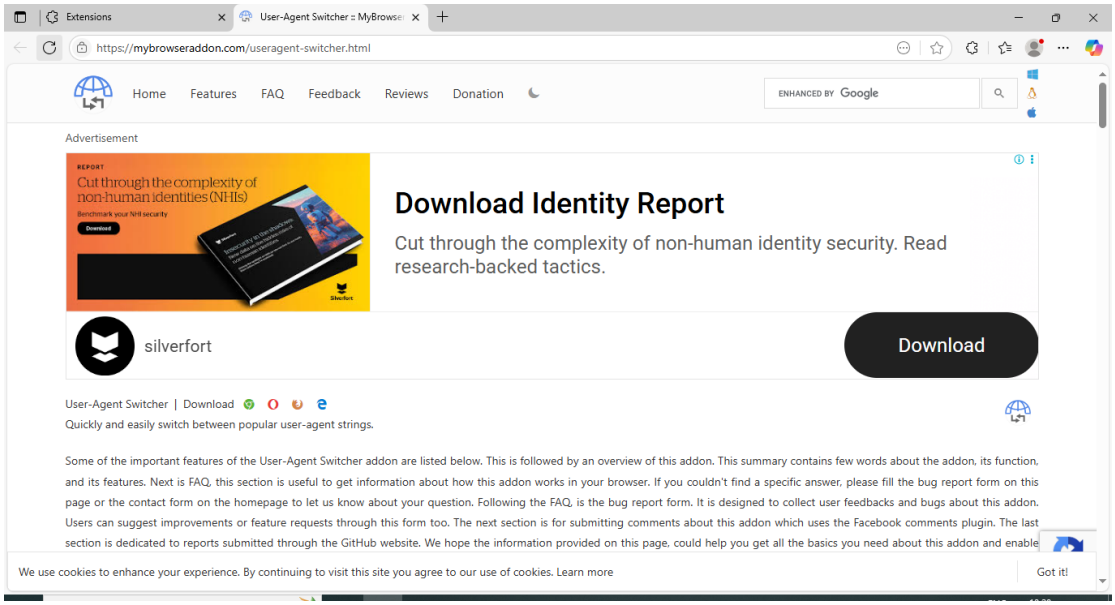
Checking Extension & Reviews on Edge Add Ons:



Checking Extension Permission on Microsoft Edge Extension Manager:

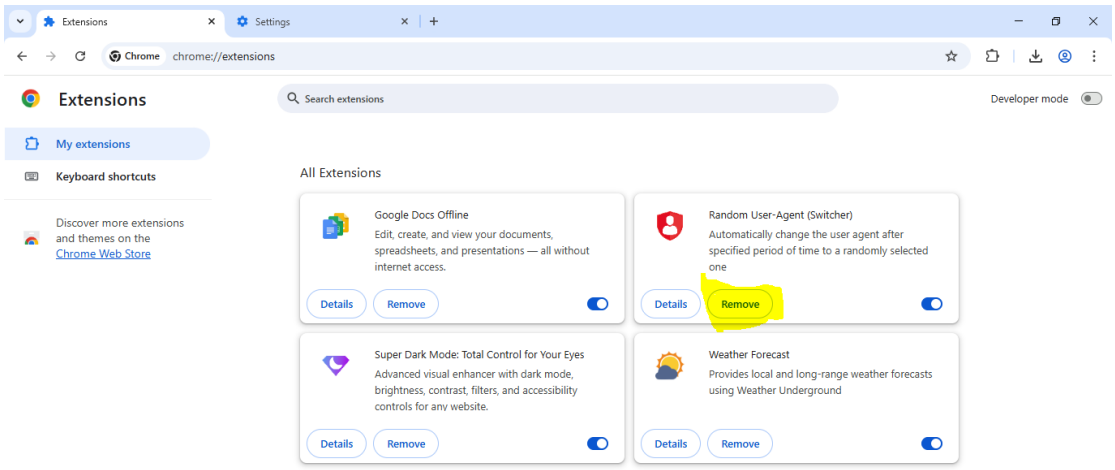


Visiting Extension Website:

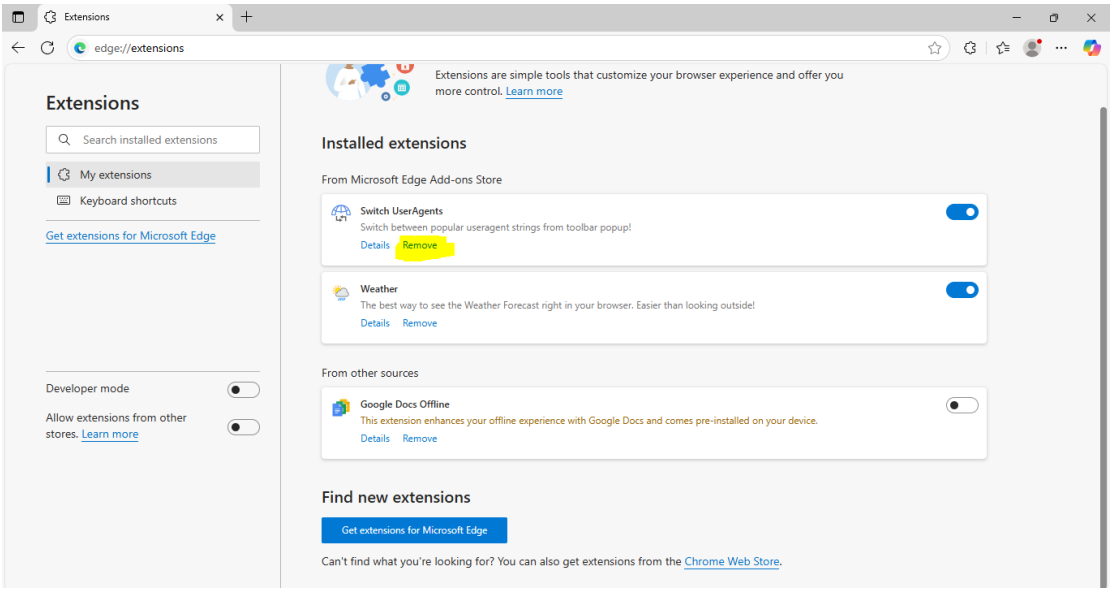


❖ Removing Suspicious/Unused Extensions

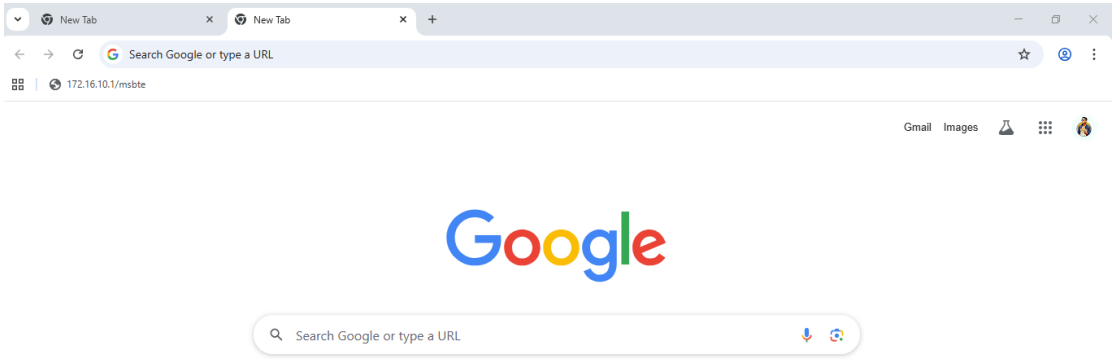
Google Chrome Browser



Microsoft Edge



❖ **Restarting Browser after removing unsafe & unused extension:**



Learning from Research

1. Malicious browser extensions can:

2. Steal login credentials & personal data.

3. Track browsing history without consent.

4. Inject pop-up ads or redirect you to phishing pages.

5. Install additional hidden malware.