Task 7: Identify and Remove Suspicious Browser Extensions

Objective:

To identify potentially harmful or unnecessary browser extensions in Firefox and remove them to enhance security and performance.

Step-by-Step Process:

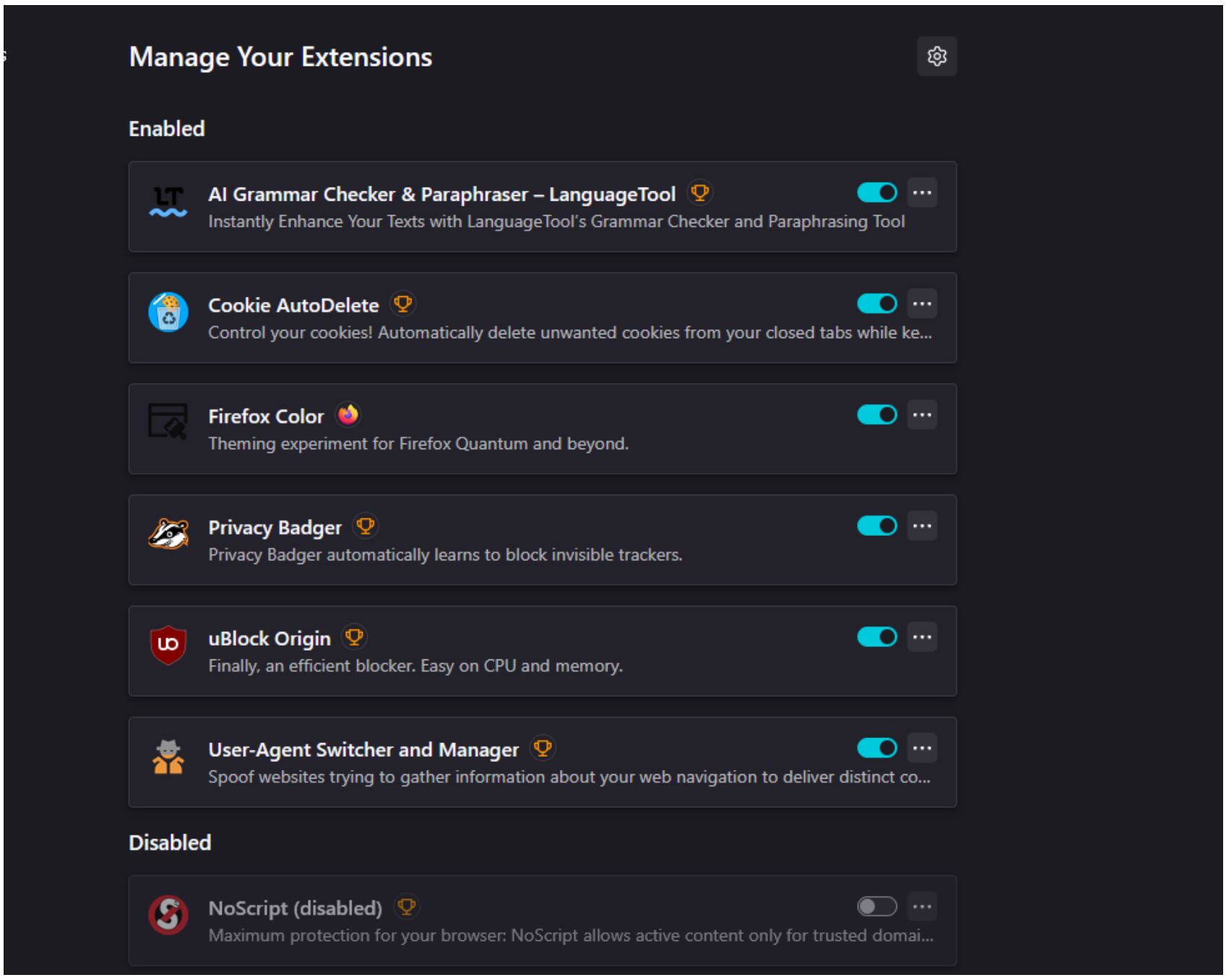
1. Opened Browser's Extension Manager

I accessed the Firefox extension page by entering "about:addons" in the URL bar. This displayed a full list of installed extensions.

2. Reviewed Installed Extensions

Here's what I found:

Extension	**Status**	**Purpose / Notes**
AI Grammar Checker (LanguageTool)	Enabled	Helpful but requires deep permissions
Cookie AutoDelete	Enabled	Secure … clears cookies after tab closure
Firefox Color	Enabled	Safe
Privacy Badger	Enabled	Trusted… blocks trackers
uBlock Origin	Enabled	Efficient ad/tracker blocker
User-Agent Switcher	Enabled	Can spoof browser info suspicious potential
NoScript	Disabled	High-security tool but caused access issues



What Caused Issues:

The browser became unusable I couldn't open github, WhatsApp, or other websites.

Real cause: NoScript Extension.

It blocks active scripts by default, even on safe sites, which broke website functionality.

Action Taken:

- Disabled NoScript**.**
- Restarted Firefox.
- Everything worked instantly again.

How Malicious Browser Extensions Can Harm Users:

Malicious browser extensions might *look* harmless, but they can be used to:

1. **Steal Data** – They can access everything you type in your browser, including passwords, credit card info, and emails.

2. **Spy on Browsing Activity** – Track every website you visit and sell that data to shady third parties.
3. **Inject Ads & Redirects** – Forcefully display popups, ads, or redirect you to dangerous phishing sites.
4. **Take Over Accounts** – Some can hijack your browser sessions and control logged-in accounts.
5. **Install Malware** – They can download malware or ransomware silently.
6. **Bypass Security** – Some extensions disable safe browsing features or tamper with firewalls.
7. **Act as Backdoors** – Give attackers remote access to your browser or device.

Lessons Learned:

- Even trusted extensions like NoScript can break browser access if misconfigured.
- Some privacy tools (like User-Agent Switcher) may interfere with site rendering or fingerprinting checks.
- Always audit extension permissions, disable what you don't need, and test performance after changes.
- Even a single shady extension can be enough to ruin your digital life. That's why auditing extensions regularly is so important.

Conclusion:

I reviewed all extensions, disabled the problematic one, and confirmed that the browser now works without issues. I now understand how extensions can affect security and usability and how to control them better.