# Task 7: Identify and Remove Suspicious Browser Extensions

## Objective:

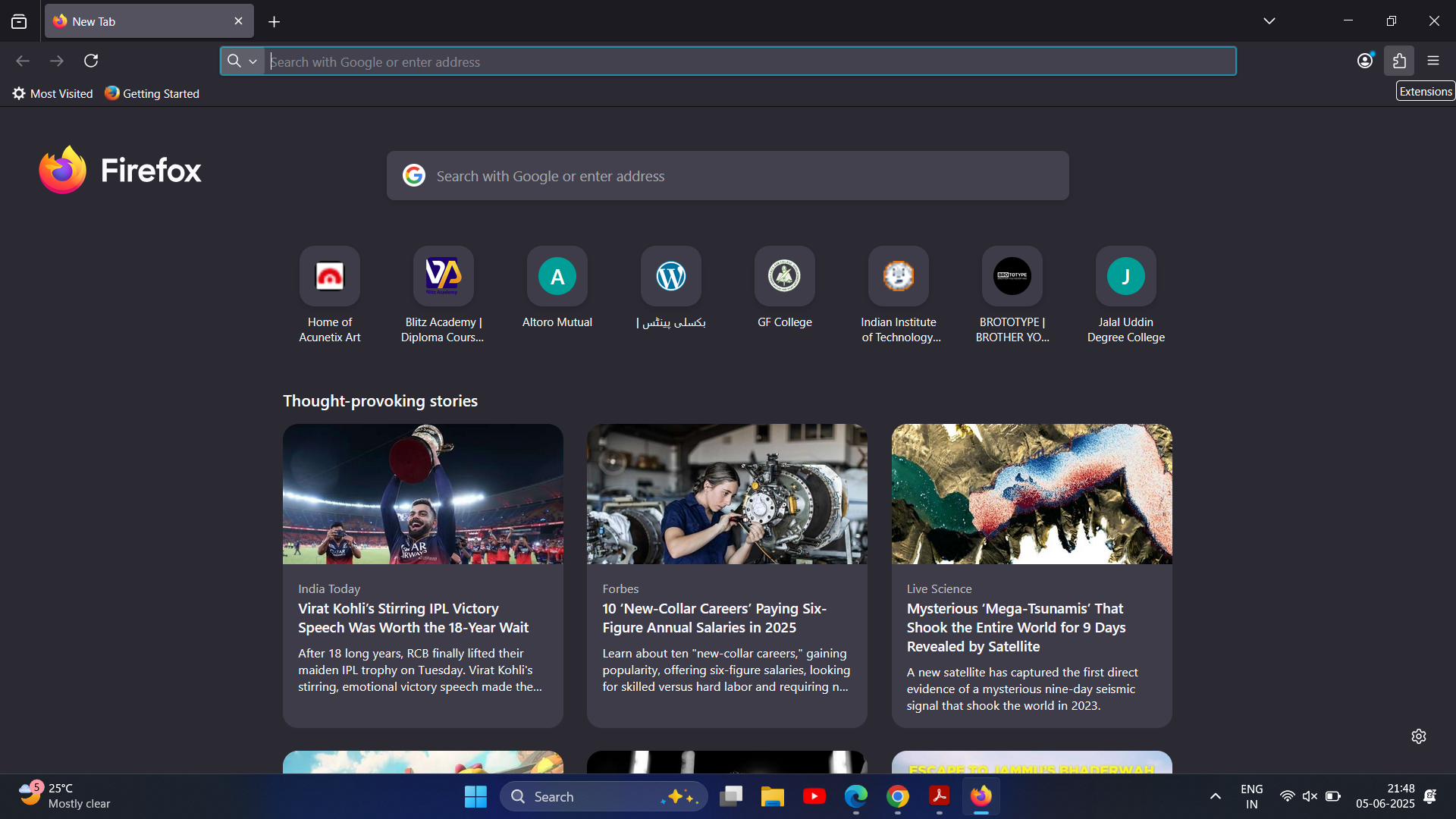
To learn how to spot and remove potentially harmful browser extensions.

## Tools Used:

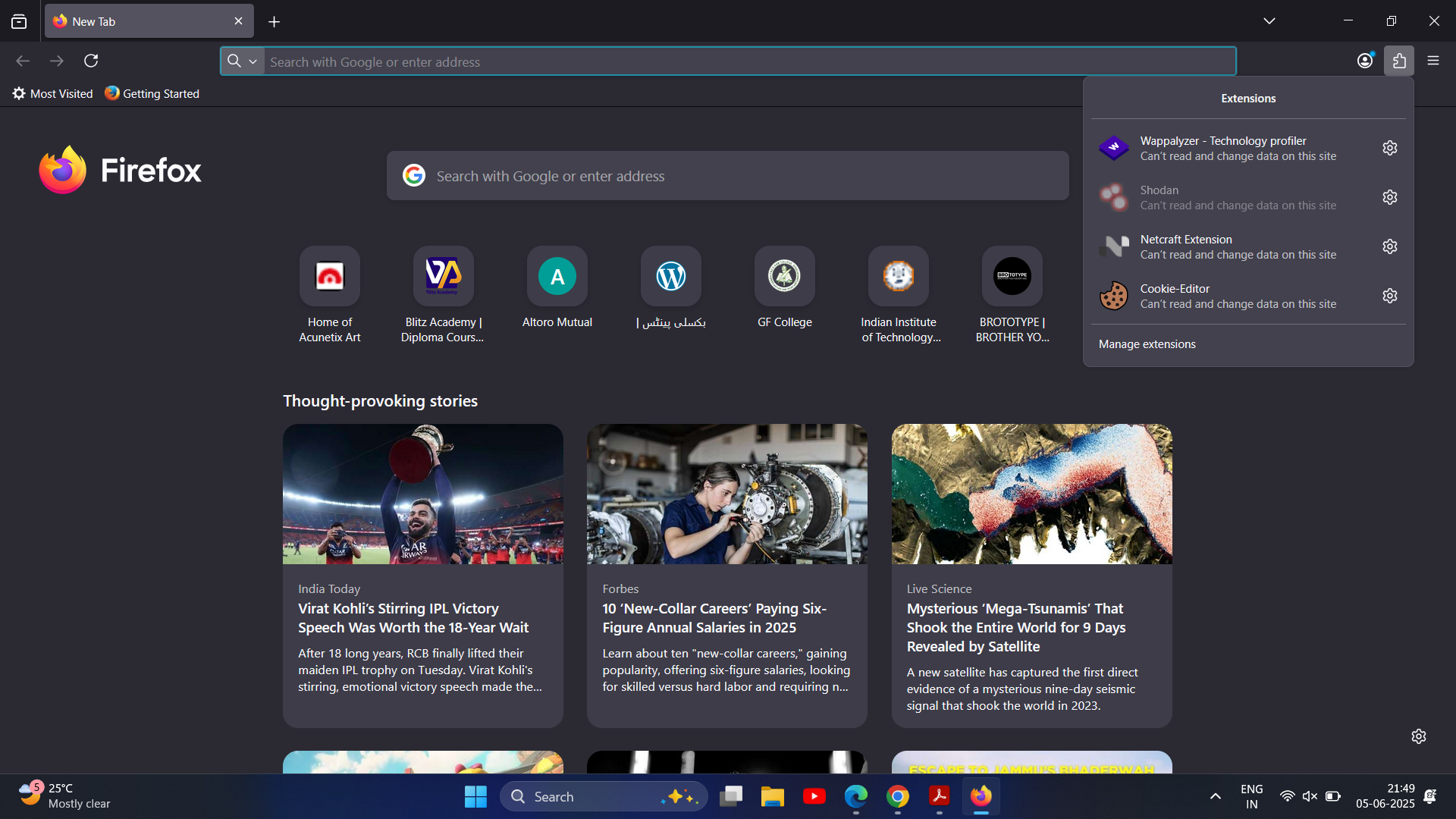
Browser: Google Chrome (same process applies for Firefox/Edge)

## Steps Taken:

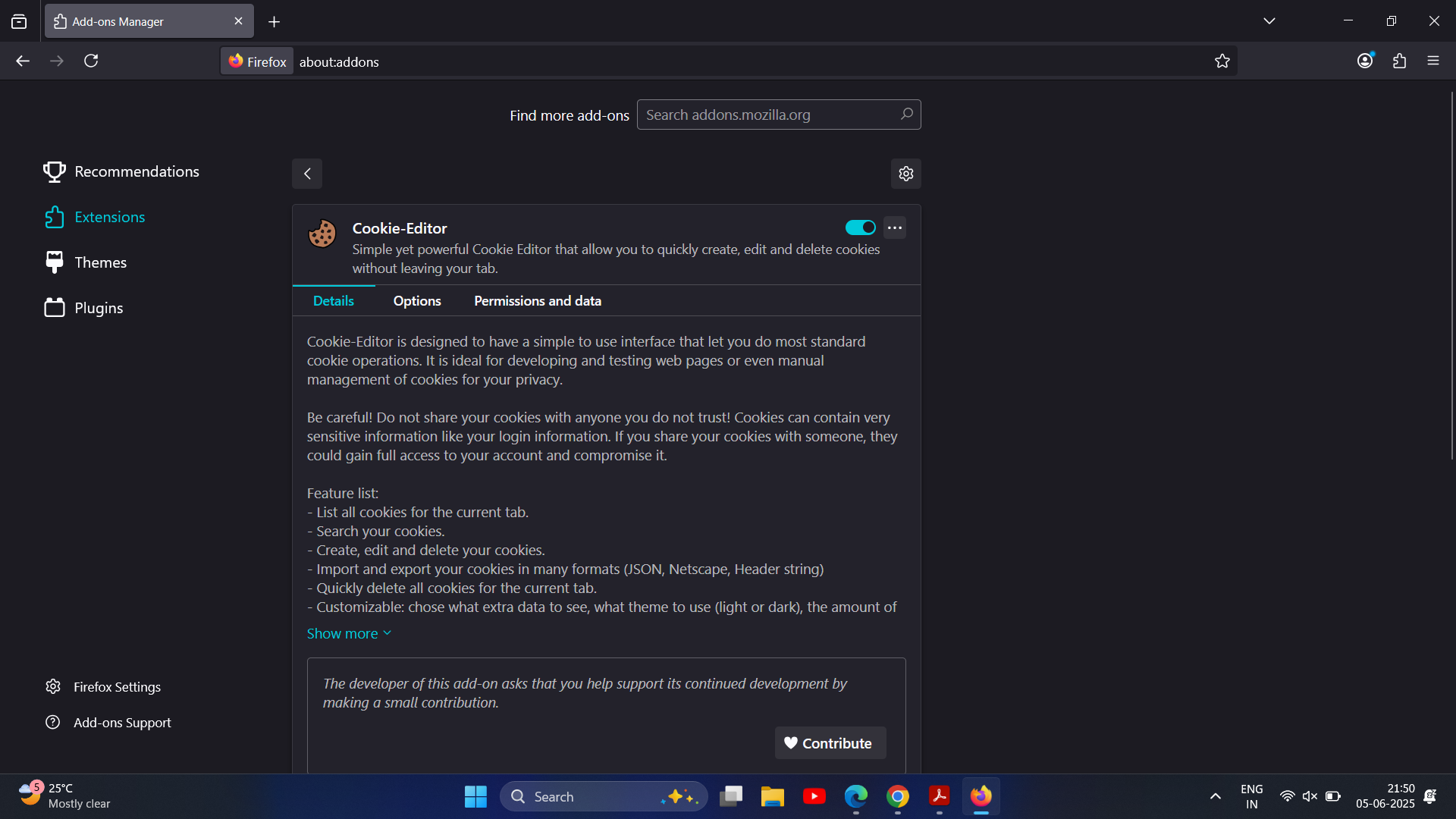
1. Opened the Browser's Extension Manager:  
   - Navigated to chrome://extensions/.



1. Reviewed All Installed Extensions:  
   - Manually inspected each extension’s name, source, and description.



1. Checked Permissions and Reviews:  
   - Clicked 'Details' on each extension.  
   - Verified permissions, developer, and user reviews.



1. Searched for Suspicious or Unused Extensions:  
   - Looked for unknown tools, broad permissions, and inactive extensions.
2. Conclusion:  
   - No suspicious or unknown extensions were found.  
   - All installed extensions are frequently used and from trusted sources.
3. Restarted Browser:  
   - No issues noted, browser performance remained good.
4. Researched Potential Risks of Malicious Extensions:  
   - Learned about risks like tracking, ads injection, search redirection, and credential theft.
5. Documented Findings:  
   - This report summarizes the steps taken and confirms a clean extension environment.

## Outcome:

No action needed regarding extensions.  
Improved awareness of extension security.  
Confirmed a clean and safe browser setup.