Elevate Labs (Cyber-Security Internship)

Task 7: Identify and Remove Suspicious Browser Extensions

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

Tools: Any web browser (**Chrome, Firefox**)

Deliverables: List of suspicious extensions found and removed (IF ANY)

Report (Browser Extension):

List of Browser-Extension Used:

1. FoxyProxy: FoxyProxy is owned and developed consistently by the same few people since 2006. It has never been sold and never will.

WHAT IS IT?
FoxyProxy is a Firefox and Chrome extension that switches an internet connection across one or more proxy servers. Proxies can be switched by:

- Point-And-Click of coloured icons in a popup menu
- URL - define URL patterns with wildcards or regular expressions
- browser tab - set individual proxies per tab!
- Firefox container or Private Browsing windows - define different proxies for each container

2. HackBar: A Browser Extension for Penetration Testing.

3. Wappalyzer – Technology Profiler: Wappalyzer is a browser extension that uncovers the technologies used on websites. It detects content management systems, eCommerce platforms, web servers, JavaScript frameworks, analytics tools and many more.

Extension Name	Browser	Reasons Suspicious	Action Taken
FoxyProxy	Firefox	Kown-Safe	Kept
HackBar	Firefox	Kown-Safe	Kept
Wappalyzer – Technology Profiler	Firefox	Know-Safe	Kept