iGNITE Technologies

FIREFOX ADDONS FOR PENTESTING

www.hackingarticles.in

Contents

Firefox For Pen-testers

In this article, we will learn how to customise the Firefox browser for efficient pen-testing along with extensions you can use for the same purpose.

Introduction

In the ever-evolving landscape of cybersecurity, penetration testing stands as a crucial pillar of defence against the relentless onslaught of cyber threats. Penetration testers, often referred to as ethical hackers, play a pivotal role in identifying vulnerabilities and weaknesses within computer systems and applications. They simulate real-world attacks to uncover security flaws that malicious actors could exploit. One of the essential tools in a penetration tester's arsenal is their web browser, and customizing it for this purpose is of paramount importance. This article delves into why browser customization is vital for penetration testing and outlines the best practices for doing so.

Understanding the Role of the Browser in Penetration Testing

Before diving into the specifics of browser customization, it's essential to grasp the significance of the web browser in the realm of penetration testing. A web browser is more than just a tool for browsing websites; it is a versatile interface through which testers interact with web applications, inspect and manipulate data, and uncover vulnerabilities. Here's why browser customization matters in this context:

- Control and Intercept Traffic: Customizing your browser allows you to exert fine-grained control over the HTTP traffic between your machine and web servers. Penetration testers need to intercept and analyse this traffic to identify vulnerabilities, such as injection attacks (e.g., SQL injection or Cross-Site Scripting), security misconfigurations, or sensitive data exposure. Customization facilitates the interception of requests and responses for in-depth analysis.

- Seamless Integration with Tools: Leading penetration testing tools like Burp Suite and OWASP ZAP act as proxies that intercept, modify, and inspect HTTP traffic. Customizing your browser is essential to ensure that all web traffic flows through these tools, enabling a seamless integration that simplifies the testing process. Without customization, the tools cannot effectively capture and analyse the data.

- Mimic Real-World Scenarios: Web applications often respond differently based on various factors, such as user agents, cookies, and headers. By customizing your browser, you can mimic these real-world scenarios and assess how the application behaves under different conditions. This is critical for understanding how security controls and mechanisms react to various inputs.

- Enhanced Efficiency: Efficiency is a core concern for penetration testers. Customizing your browser with the necessary extensions, configurations, and settings streamlines the testing process. It enables testers to perform tasks more efficiently, saving time and increasing overall productivity.

- Reducing False Positives: False positives can be a significant concern during penetration testing. Customizing your browser to closely resemble real user behaviour reduces the chances of encountering false positives. This ensures that the vulnerabilities identified are more likely to be genuine security issues, allowing organizations to focus on addressing critical weaknesses.

- Session Management: Web applications often rely on session management and authentication mechanisms. Customizing your browser with cookie editors and session management tools allows penetration testers to simulate different user sessions, test for session fixation, and assess the overall security of authentication processes.

- Bypassing Security Controls: Web applications may implement security controls or obfuscation techniques that hinder testing efforts, such as client-side validation or anti-automation mechanisms. Customizing your browser can help you bypass or work around these controls, allowing testers to identify vulnerabilities that may remain hidden otherwise.

- Script and Payload Testing: Penetration testers often need to test custom scripts and payloads for vulnerabilities like Cross-Site Scripting (XSS) or SQL Injection. Customized browser settings aid in injecting and executing these scripts, enabling thorough testing and validation of security issues.

- Automation: Customized browsers can be integrated into automated testing frameworks, enabling the automation of repetitive tasks and vulnerability scanning. Automation is invaluable for large-scale assessments and continuous monitoring of web applications.

- Personalized Testing Environment: Different penetration testers may have different preferences and methodologies. Browser customization allows each tester to tailor their environment to meet their specific needs, ensuring that they can conduct assessments effectively and efficiently.

Extensions for efficient pen-testing

When it comes to penetration testing, having the right browser extensions can significantly enhance your capabilities and efficiency. Here is a list of some of the best browser extensions for penetration testing:

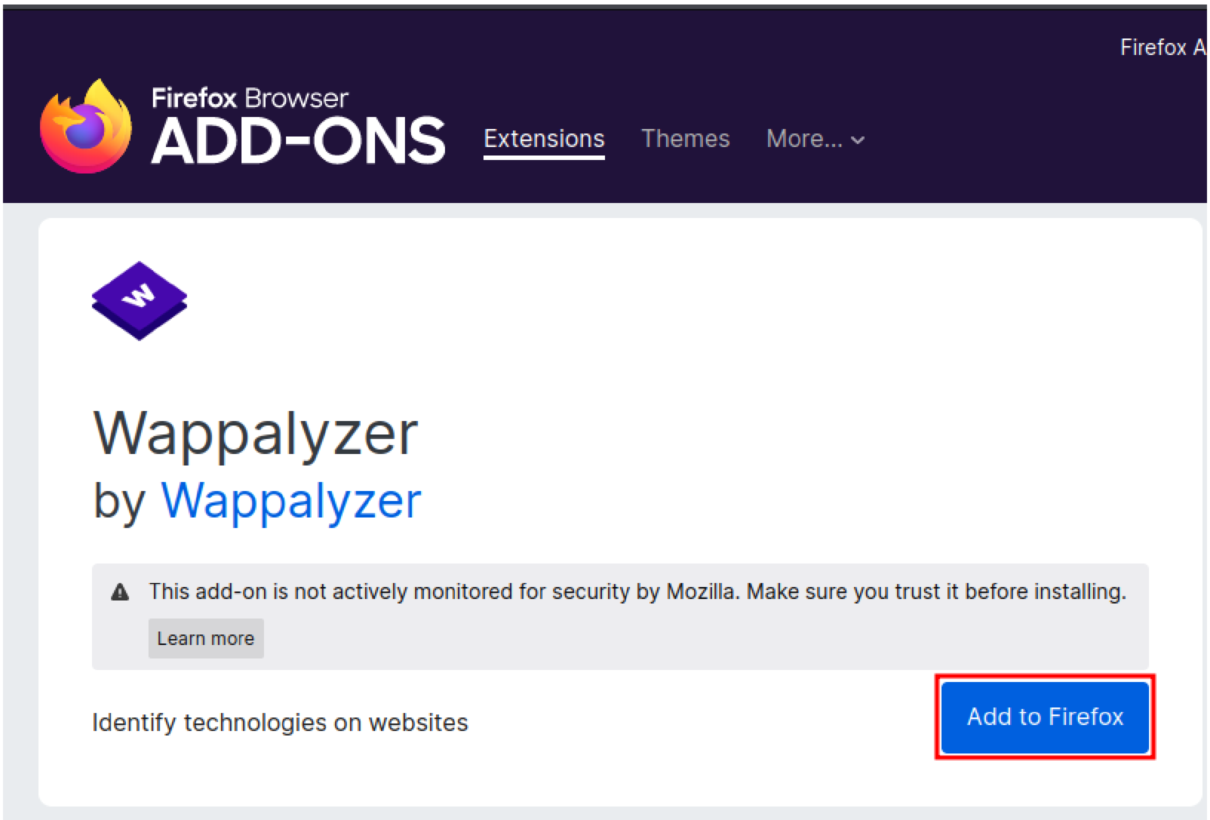
Wappalyzer

While not strictly a penetration testing extension, Wappalyzer helps you identify the technologies and frameworks used by a website. This information can be valuable for understanding the attack surface and potential vulnerabilities. Once installed in Firefox, the Wappalyzer extension works quietly in the background. When you visit a website, it scans the site and then displays a small icon in the browser toolbar. Clicking on this icon reveals a wealth of information about the site's underlying technologies.

Wappalyzer can identify various aspects of a website, including the content management system (CMS), e-commerce platforms, web servers, programming languages, analytics tools, and more. This information can be invaluable for competitive analysis, SEO optimization, or understanding the security implications of the technologies in use. This extension doesn't interfere with a website's functionality; it simply provides you with useful metadata that can inform your decisions. This extension is especially beneficial for web developers who may want to examine the technologies used on websites for inspiration or troubleshooting.

Overall, Wappalyzer is a legitimate and widely used extension that promotes transparency and understanding in the online world, making it a valuable resource for web professionals and enthusiasts alike. You can install it in your browser from the following link:

https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search



Wappalyzer
by Wappalyzer

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Identify technologies on websites

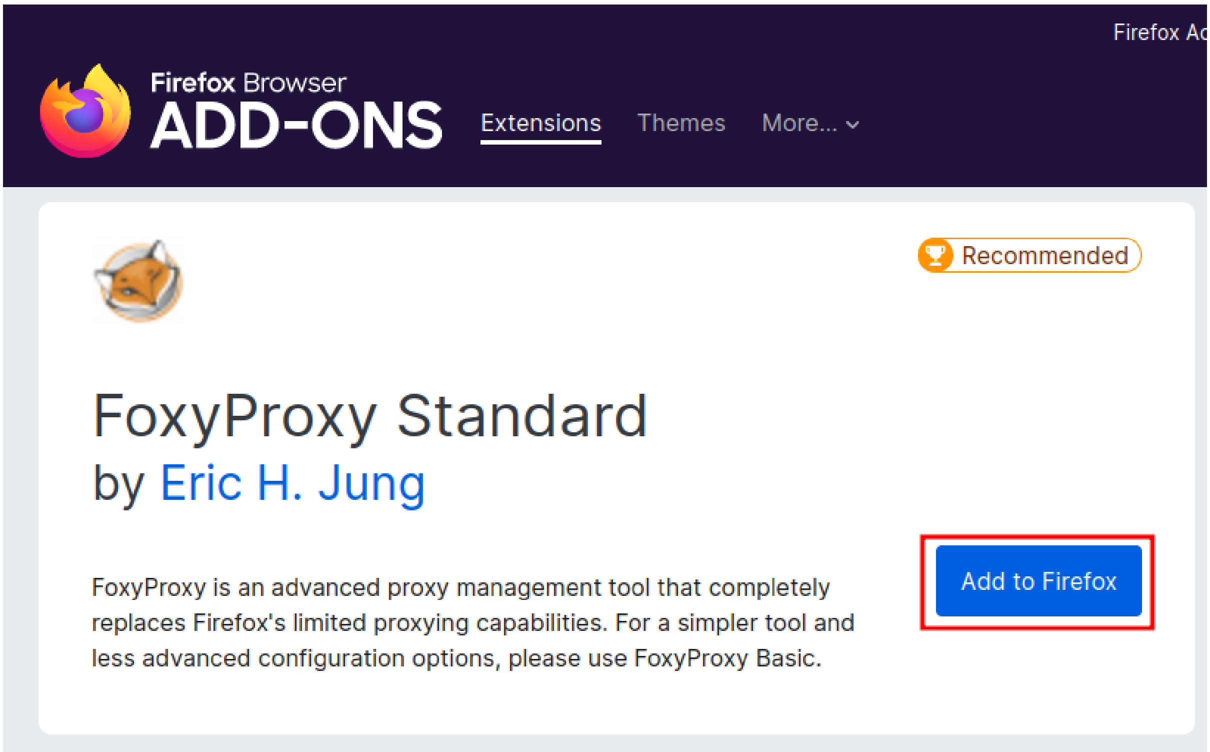
FoxyProxy

FoxyProxy is a Firefox extension that empowers users to manage and optimize their proxy settings effortlessly. It's an invaluable tool for individuals seeking enhanced online privacy, security, and control over their internet browsing experience.

Once installed, FoxyProxy allows users to easily switch between multiple proxy servers, routing their internet traffic through different locations or configurations. This is particularly useful for circumventing geo-restrictions, accessing region-locked content, or maintaining anonymity by masking your IP address. It offers a user-friendly interface that lets you create profiles for various proxy configurations. You can define rules to determine when specific proxies should be used, based on website URLs, IP addresses, and other criteria. This level of granular control ensures that your internet activity remains secure and private.

Additionally, FoxyProxy supports both HTTP and SOCKS proxy protocols, making it compatible with a wide range of proxy servers. Whether you're a privacy-conscious user, a digital marketer conducting geo-targeting research, or a web developer testing different proxy setups, FoxyProxy is a versatile and powerful extension that simplifies proxy management within the Firefox browser. You can download FoxyProxy from the following link:

https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search



FoxyProxy Standard
by Eric H. Jung

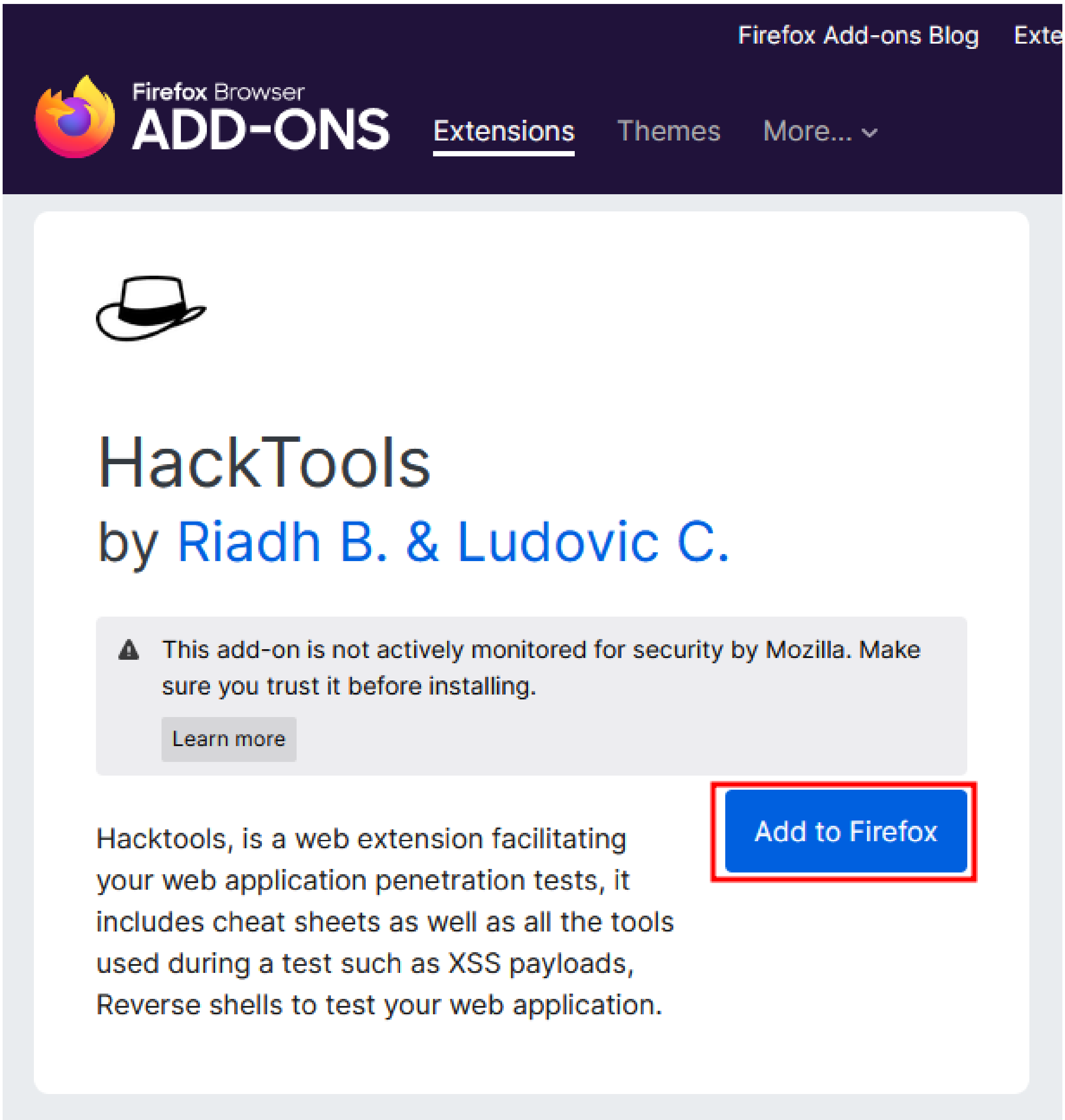
FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

HackTool

HackTools is a web extension designed to assist in conducting web application penetration tests. It offers a comprehensive set of resources, including cheat sheets and various tools commonly used during tests, such as XSS payloads and reverse shells. With this extension, the need to search for payloads on various websites or within your local storage is eliminated. Most of the necessary tools are readily accessible with just a single click. HackTools can be conveniently accessed through the browser's DevTools section, either as a pop-up or within a dedicated tab, accessible with the F12 key.

You can download the extension with the following link:

https://addons.mozilla.org/en-US/firefox/addon/hacktools/



HackTools
by Riadh B. & Ludovic C.

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

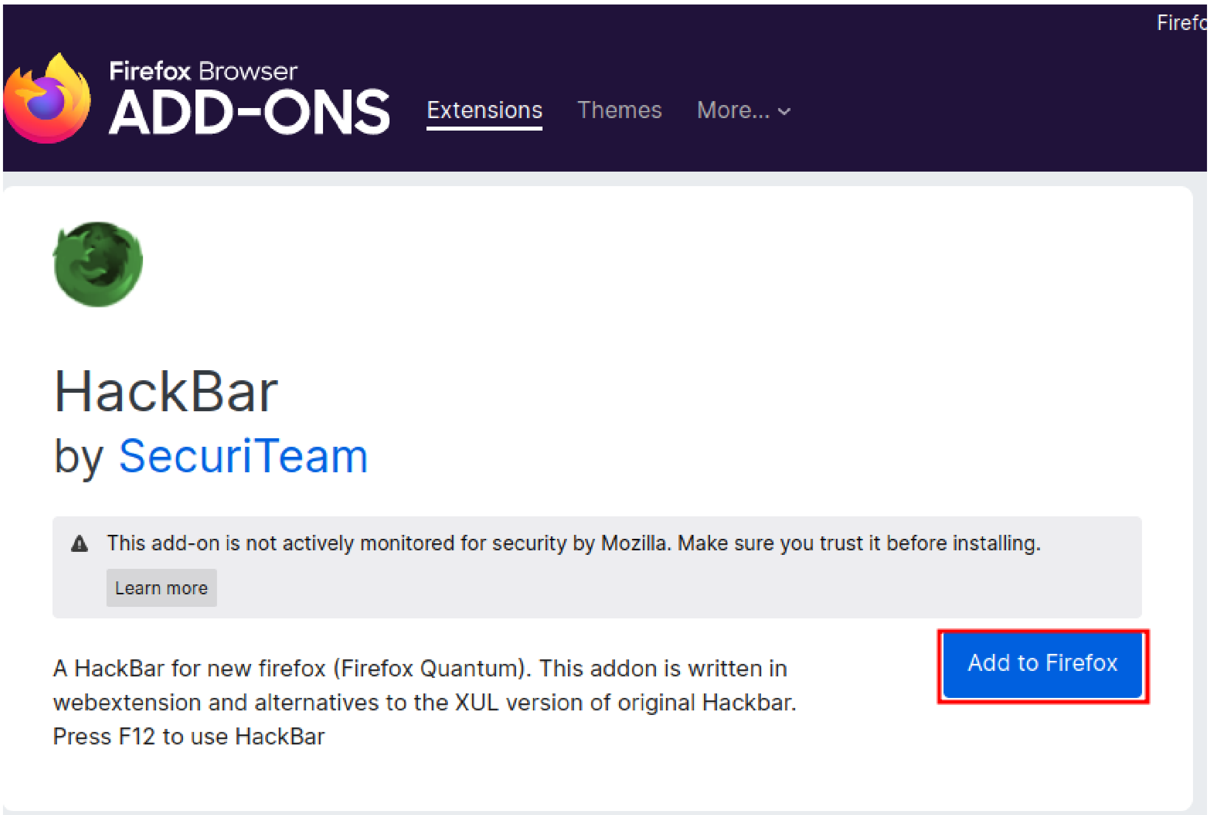
Hacktools, is a web extension facilitating your web application penetration tests, it includes cheat sheets as well as all the tools used during a test such as XSS payloads, Reverse shells to test your web application.

Hack bar

Hackbar is a free Firefox extension that proves invaluable for security researchers during web application and web server testing. It simplifies common tasks such as interacting with domains, subdomains, and URLs of the target, as well as modifying parameters in the browser's address bar and reloading websites. These actions, while essential, can be time-consuming. Hackbar is a freely available open-source tool accessible on GitHub. It serves as a valuable aid for evaluating the security of web applications and web servers. Security researchers often employ Hackbar for tasks such as checking cross-site scripting (XSS) and SQL injection vulnerabilities on websites. It facilitates the discovery of website subdomains. Hackbar is compatible with multiple operating systems, including Windows.

You can download hackbar from the following link:

https://addons.mozilla.org/en-US/firefox/addon/hackbartool/



HackBar
by SecuriTeam

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

A HackBar for new firefox (Firefox Quantum). This addon is written in webextension and alternatives to the XUL version of original Hackbar. Press F12 to use HackBar

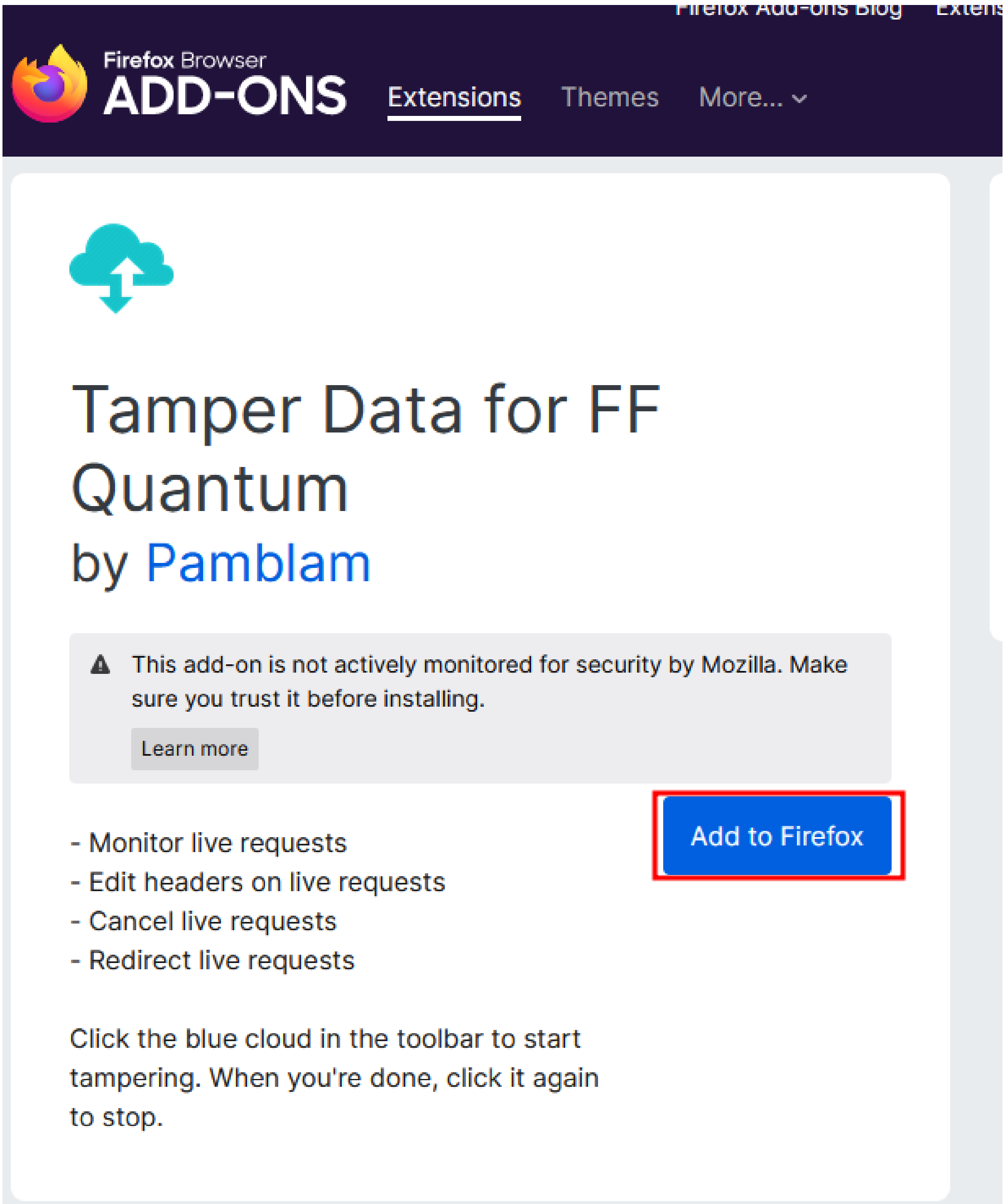
Tamper Data

Tamper Data is a Firefox extension that plays a pivotal role in the realm of web security and development. It empowers users, particularly security professionals, ethical hackers, and developers, to inspect and modify data exchanged between their browser and web servers in real-time. With Tamper Data, users can intercept and view HTTP/HTTPS requests and responses, gaining granular control over the data flow. It acts as a proxy between the browser and the server, allowing you to scrutinize the headers, cookies, and parameters of each request. This level of insight is indispensable for identifying security vulnerabilities, debugging web applications, and optimizing performance.

Tamper Data is instrumental in various security assessments. Security experts use it to test for common web vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL Injection. It enables them to observe how data is transmitted and processed, helping uncover potential weaknesses that could be exploited by malicious actors.

You can download Tamper data from the following link:

https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/



Tamper Data for FF Quantum
by Pamblam

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

- Monitor live requests
- Edit headers on live requests
- Cancel live requests
- Redirect live requests

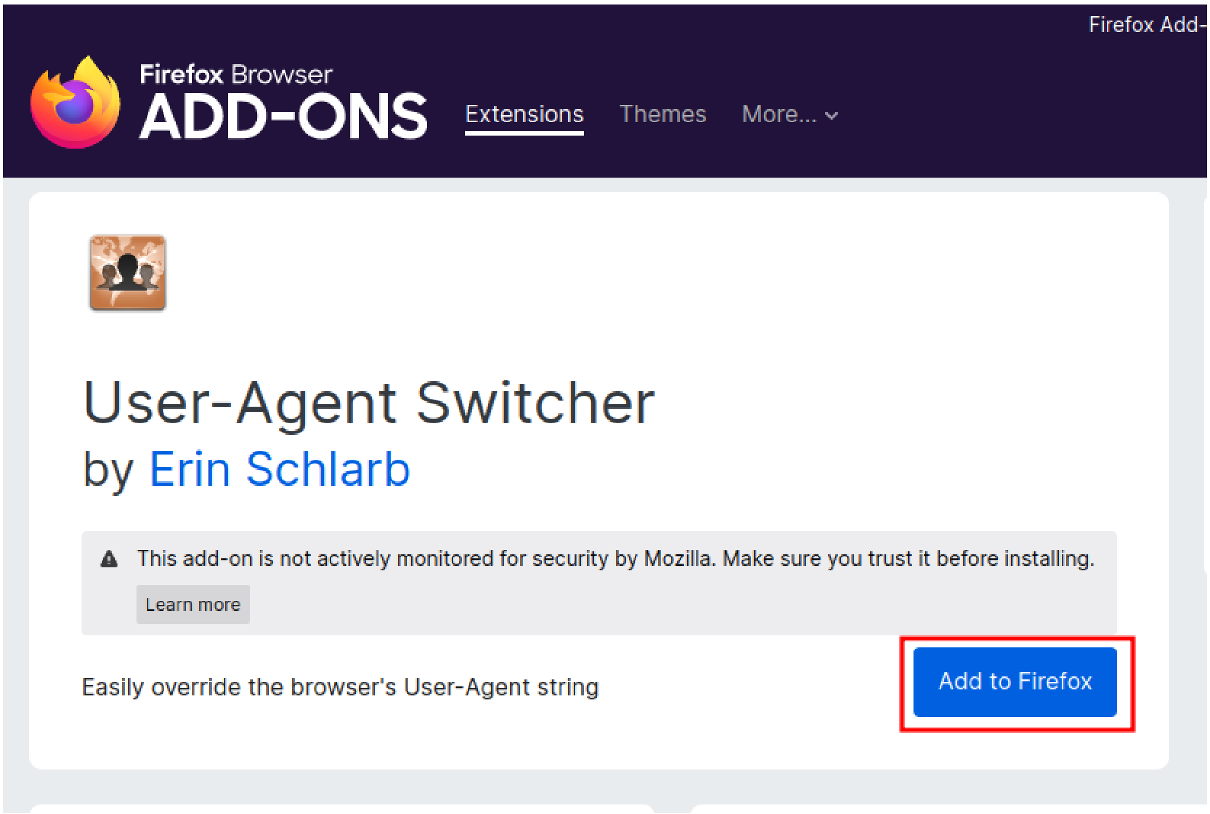
Click the blue cloud in the toolbar to start tampering. When you're done, click it again to stop.

User Agent Switcher

The User-Agent Switcher is a valuable Firefox extension that grants users the ability to change their browser's user agent string, effectively disguising their browser identity when interacting with websites. It's a versatile tool with various practical applications. This extension proves exceptionally useful for web developers and testers. They can simulate different user agents to assess how websites respond to various browsers and devices. This helps ensure that web content is responsive and functions correctly for a diverse user base. By switching user agents, developers can catch and address compatibility issues early in the development process. Additionally, the User-Agent Switcher is handy for privacy-conscious individuals. They can use it to enhance online anonymity by altering their user agent string, making it more challenging for websites to track and profile them based on their browser information.

You can download the extension from the following link:

https://addons.mozilla.org/en-US/firefox/addon/uaswitcher/



User-Agent Switcher
by Erin Schlarb

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Easily override the browser's User-Agent string

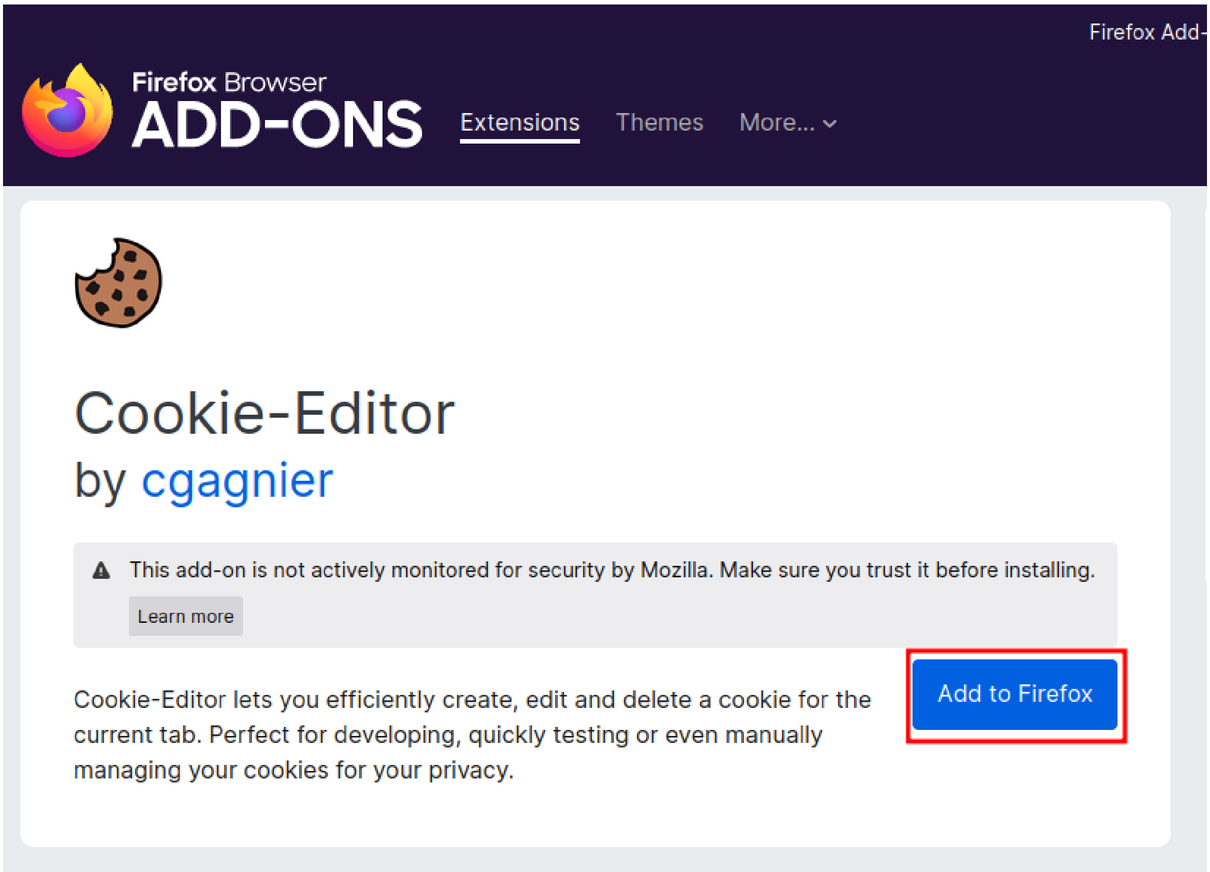
Cookie Editor

Cookie Editor enables users to view, edit, delete, and add cookies for specific websites. This level of control is crucial for enhancing online privacy, as users can choose which cookies to retain and which to discard. It's an effective means of blocking unwanted tracking cookies while allowing essential cookies to function.

Furthermore, web developers and testers find Cookie Editor invaluable for debugging and testing web applications. They can manipulate cookies to simulate different user scenarios and assess how websites respond under various conditions. This helps identify and address potential issues related to cookie handling within web applications.

You can download this extension from the following link:

https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/



Cookie-Editor
by cgagnier

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

Temp Mail

A Temporary Email extension for Firefox is a handy tool for enhancing online privacy and reducing email-related clutter. This type of extension generates disposable email addresses, allowing users to receive emails without revealing their primary email addresses. Here are some key benefits and applications:

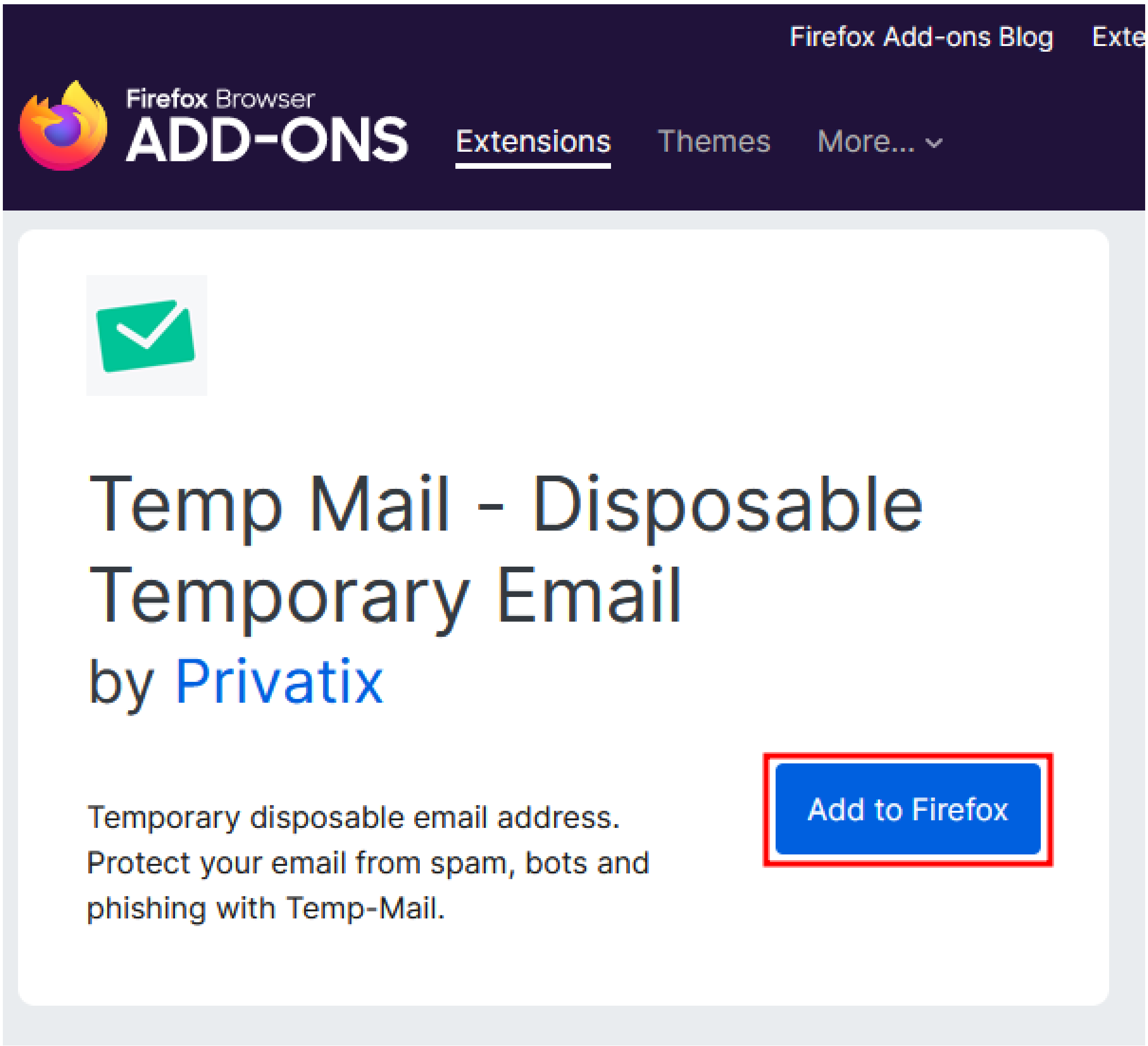
- Privacy Protection: Temporary email addresses shield your primary email account from spam, phishing attempts, and potential data breaches. You can use these disposable addresses for online registrations, subscriptions, or any situation where you want to avoid sharing your personal email.

- Reduced Inbox Clutter: Many online services send promotional emails or newsletters after registration. Using a temporary email address keeps such emails separate from your primary inbox, helping you stay organized.

- Verification and Testing: Web developers and testers often use temporary email addresses for testing user registration and email verification processes in applications without using real email accounts.

- Anonymous Sign-ups: When exploring new websites or platforms, you can sign up using a temporary email address to avoid revealing your identity until you're comfortable with the service.

- Bypass Email Verification: In some cases, you can use a temporary email address to bypass email verification requirements, making it easier to access certain content or services.



Temp Mail - Disposable Temporary Email

by Privatix

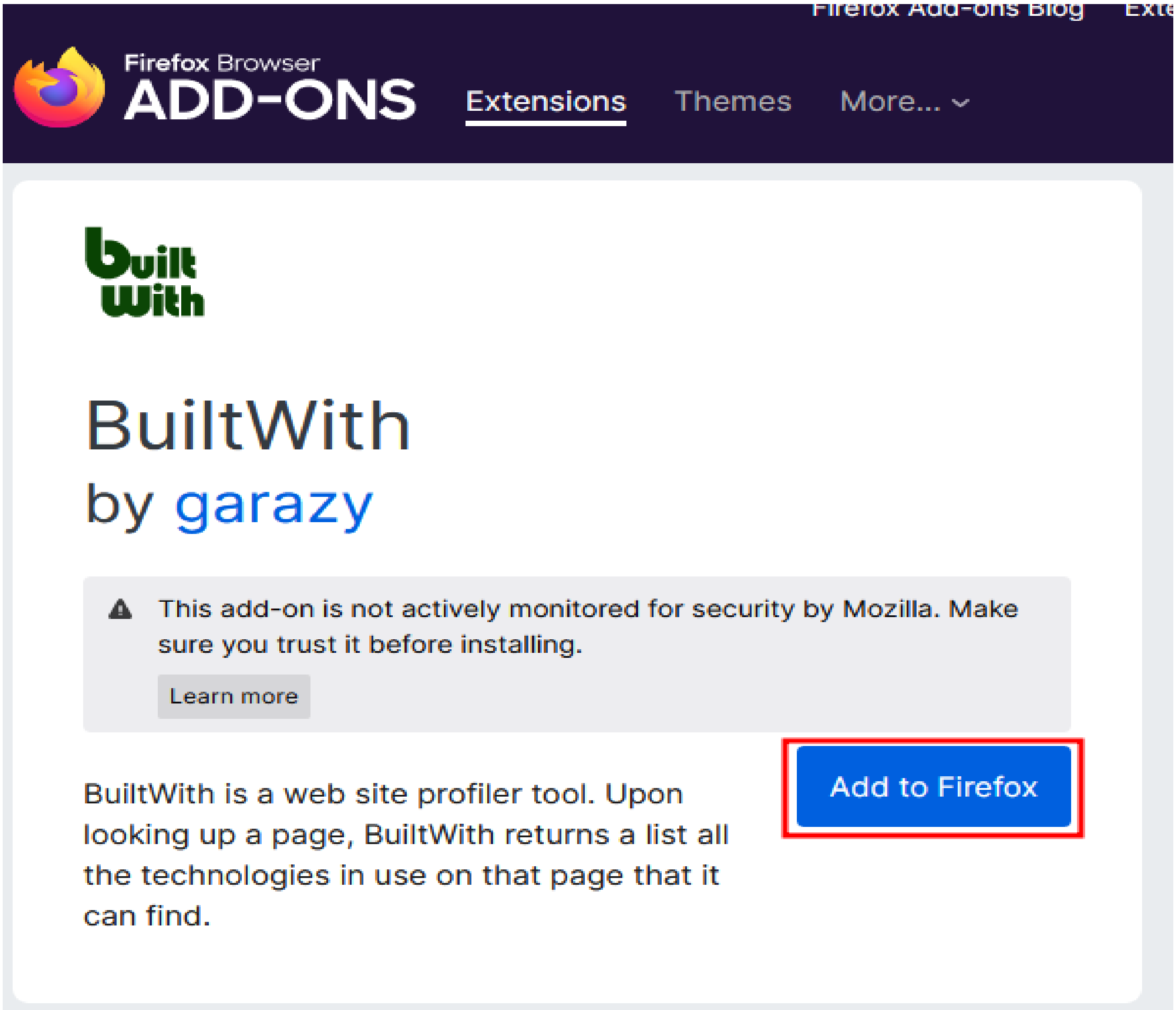
Temporary disposable email address. Protect your email from spam, bots and phishing with Temp-Mail.

Built With

BuiltWith operates seamlessly within Firefox, allowing users to quickly assess websites' underlying technologies with a simple click. It offers a wealth of information, including details about the Content Management System (CMS), web hosting, programming languages, analytics tools, and more. This data can be instrumental for competitive analysis, optimizing digital marketing strategies, or exploring potential business collaborations.

Web developers benefit from BuiltWith by gaining insights into the technologies used by websites, aiding in understanding best practices and industry trends. It can also be used for debugging purposes, helping developers identify compatibility issues or security vulnerabilities related to specific technologies.

You can download the extension from the following link:
https://addons.mozilla.org/en-US/firefox/addon/builtwith/



BuiltWith
by garazy

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

BuiltWith is a web site profiler tool. Upon looking up a page, BuiltWith returns a list all the technologies in use on that page that it can find.

Conclusion

Customizing your web browser for penetration testing is an indispensable practice that empowers ethical hackers to identify and mitigate vulnerabilities in web applications effectively. The browser serves as the primary interface through which testers interact with web resources, analyse HTTP traffic, and manipulate data to uncover security flaws.

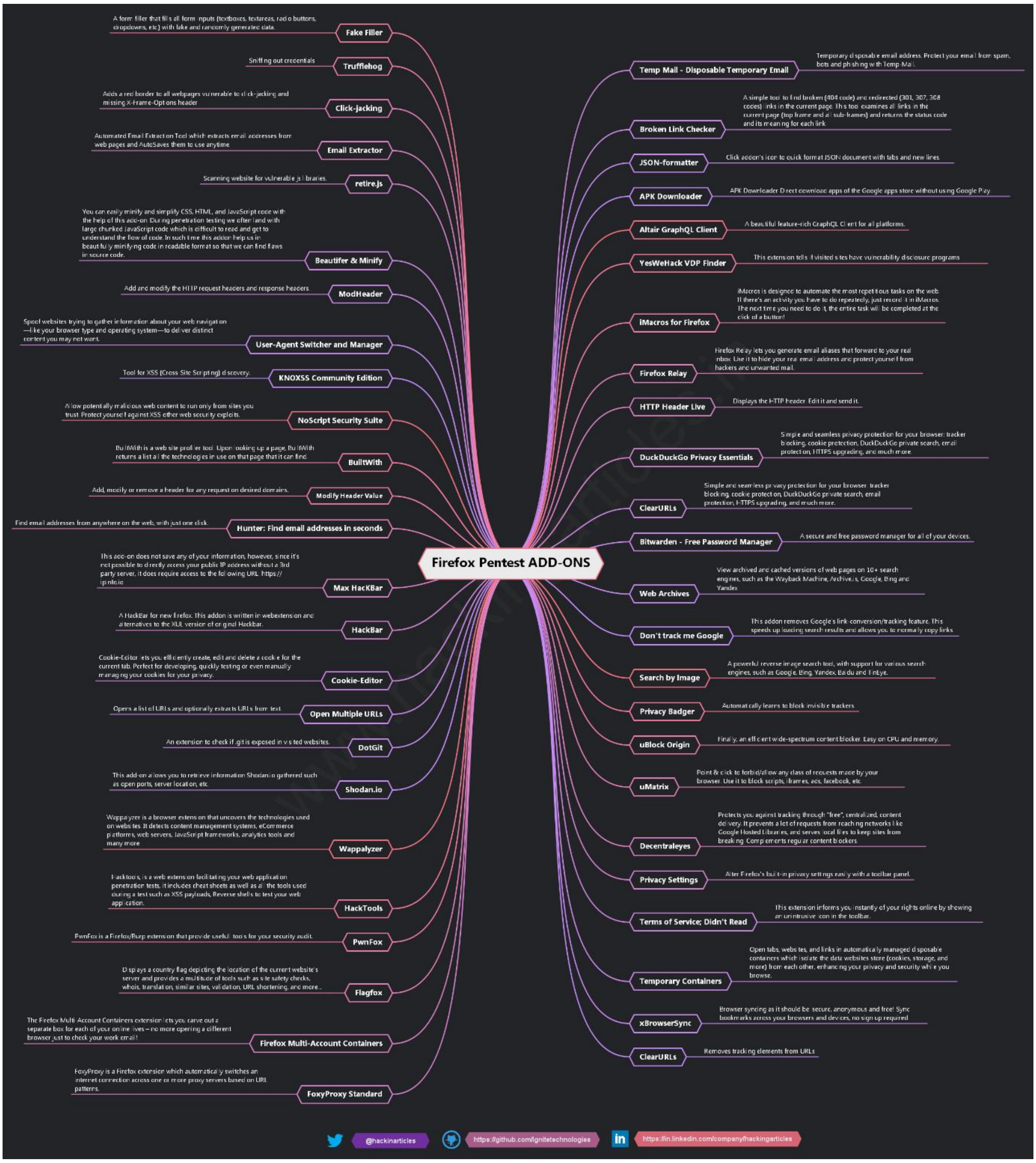
By customizing your browser, you gain control over traffic, seamlessly integrate with security tools, mimic real-world scenarios, enhance efficiency, reduce false positives, manage sessions, bypass security controls, and test scripts and payloads. Moreover, a personalized testing environment tailored to your needs ensures that you can conduct assessments with precision and accuracy.

To customize your browser effectively, select the right browser, install security-oriented extensions, configure proxy settings, manage SSL/TLS certificates, disable unnecessary features, secure your environment, stay informed about the latest vulnerabilities, and document your findings meticulously. Following these best practices enables penetration testers to maximize their impact in safeguarding the digital landscape against cyber threats, ultimately enhancing the security posture of organizations and individuals alike.

Mindmap

There are so many extensions/ addons for Firefox from which you can choose to be efficient in your testing process. All of such extensions are mentioned in the following mind map. To download this Mindmap in HD please follow the link:

https://github.com/Ignitetechnologies/Mindmap/tree/main/Firefox%20Pentest%20Addons



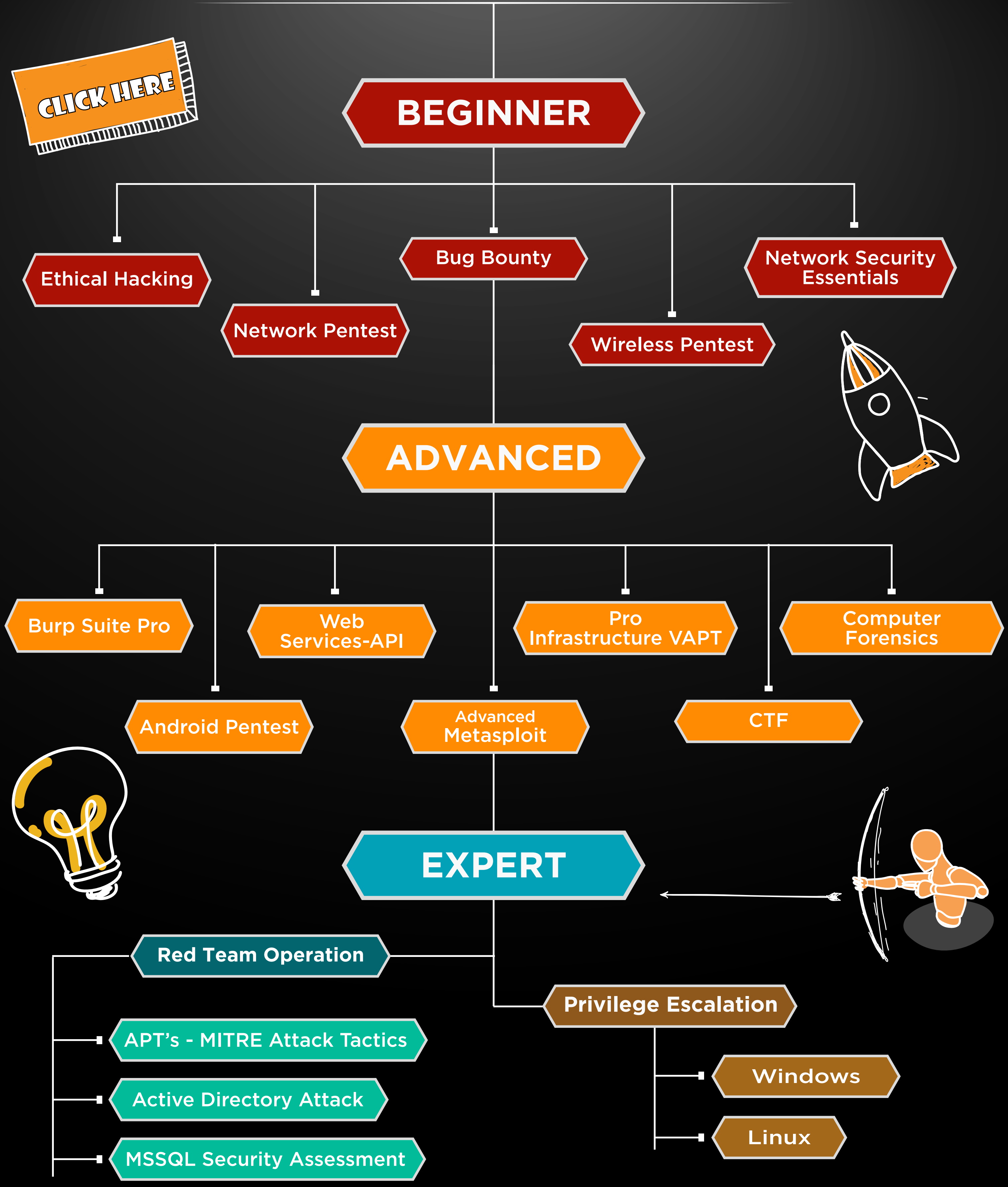
Firefox Pentest ADD-ONS

- **Fake Filler** – A form filler that fills all form inputs (textboxes, textareas, radio buttons, dropdowns, etc) with fake and randomly generated data.
- **Trufflehog** – Sniffing out credentials
- **Click-jacking** – Adds a red border to all webpages vulnerable to click-jacking and missing X-Frame-Options header
- **Email Extractor** – Automated Email Extraction Tool which extracts email addresses from web pages and AutoSaves them to use anytime
- **retire.js** – Scanning website for vulnerable js libraries.
- **Beautifer & Minify** – You can easily minify and simplify CSS, HTML, and JavaScript code with the help of this add-on. During penetration testing we often land with large chunked JavaScript code which is difficult to read and get to understand the flow of code. In such time this addon help us in beautifully minifying code in readable format so that we can find flaws in source code.
- **ModHeader** – Add and modify the HTTP request headers and response headers.
- **User-Agent Switcher and Manager** – Spoof websites trying to gather information about your web navigation —like your browser type and operating system—to deliver distinct content you may not want.
- **KNOXSS Community Edition** – Tool for XSS (Cross-Site Scripting) discovery.
- **NoScript Security Suite** – Allow potentially malicious web content to run only from sites you trust. Protect yourself against XSS other web security exploits.
- **BuiltWith** – BuiltWith is a web site profiler tool. Upon looking up a page, BuiltWith returns a list all the technologies in use on that page that it can find.
- **Modify Header Value** – Add, modify or remove a header for any request on desired domains.
- **Hunter: Find email addresses in seconds** – Find email addresses from anywhere on the web, with just one click.
- **Max HacKBar** – This add-on does not save any of your information, however, since it's not possible to directly access your public IP address without a 3rd party server, it does require access to the following URL https://ipinfo.io
- **HackBar** – A HackBar for new firefox. This addon is written in webextension and alternatives to the XUL version of original Hackbar.
- **Cookie-Editor** – Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.
- **Open Multiple URLs** – Opens a list of URLs and optionally extracts URLs from text.
- **DotGit** – An extension to check if .git is exposed in visited websites.
- **Shodan.io** – This add-on allows you to retrieve information Shodan.io gathered such as open ports, server location, etc.
- **Wappalyzer** – 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
- **HackTools** – Hacktools, is a web extension facilitating your web application penetration tests, it includes cheat sheets as well as all the tools used during a test such as XSS payloads, Reverse shells to test your web application.
- **PwnFox** – PwnFox is a Firefox/Burp extension that provide usefull tools for your security audit.
- **Flagfox** – Displays a country flag depicting the location of the current website's server and provides a multitude of tools such as site safety checks, whois, translation, similar sites, validation, URL shortening, and more..
- **Firefox Multi-Account Containers** – The Firefox Multi-Account Containers extension lets you carve out a separate box for each of your online lives – no more opening a different browser just to check your work email!
- **FoxyProxy Standard** – FoxyProxy is a Firefox extension which automatically switches an internet connection across one or more proxy servers based on URL patterns.
- **Temp Mail - Disposable Temporary Email** – Temporary disposable email address. Protect your email from spam, bots and phishing with Temp-Mail.
- **Broken Link Checker** – A simple tool to find broken (404 code) and redirected (301, 307, 308 codes) links in the current page. This tool examines all links in the current page (top frame and all sub-frames) and returns the status code and its meaning for each link
- **JSON-formatter** – Click addon's icon to quick format JSON document with tabs and new lines.
- **APK Downloader** – APK Downloader Direct download apps of the Google apps store without using Google Play
- **Altair GraphQL Client** – A beautiful feature-rich GraphQL Client for all platforms.
- **YesWeHack VDP Finder** – This extension tells if visited sites have vulnerability disclosure programs
- **iMacros for Firefox** – iMacros is designed to automate the most repetitious tasks on the web. If there's an activity you have to do repeatedly, just record it in iMacros. The next time you need to do it, the entire task will be completed at the click of a button!
- **Firefox Relay** – Firefox Relay lets you generate email aliases that forward to your real inbox. Use it to hide your real email address and protect yourself from hackers and unwanted mail.
- **HTTP Header Live** – Displays the HTTP header. Edit it and send it.
- **DuckDuckGo Privacy Essentials** – Simple and seamless privacy protection for your browser: tracker blocking, cookie protection, DuckDuckGo private search, email protection, HTTPS upgrading, and much more
- **ClearURLs** – Simple and seamless privacy protection for your browser: tracker blocking, cookie protection, DuckDuckGo private search, email protection, HTTPS upgrading, and much more.
- **Bitwarden - Free Password Manager** – A secure and free password manager for all of your devices.
- **Web Archives** – View archived and cached versions of web pages on 10+ search engines, such as the Wayback Machine, Archive.is, Google, Bing and Yandex
- **Don't track me Google** – This addon removes Google's link-conversion/tracking feature. This speeds up loading search results and allows you to normally copy links
- **Search by Image** – A powerful reverse image search tool, with support for various search engines, such as Google, Bing, Yandex, Baidu and TinEye.
- **Privacy Badger** – Automatically learns to block invisible trackers.
- **uBlock Origin** – Finally, an efficient wide-spectrum content blocker. Easy on CPU and memory.
- **uMatrix** – Point & click to forbid/allow any class of requests made by your browser. Use it to block scripts, iframes, ads, facebook, etc.
- **Decentraleyes** – Protects you against tracking through "free", centralized, content delivery. It prevents a lot of requests from reaching networks like Google Hosted Libraries, and serves local files to keep sites from breaking. Complements regular content blockers.
- **Privacy Settings** – Alter Firefox's built-in privacy settings easily with a toolbar panel.
- **Terms of Service; Didn't Read** – This extension informs you instantly of your rights online by showing an unintrusive icon in the toolbar.
- **Temporary Containers** – Open tabs, websites, and links in automatically managed disposable containers which isolate the data websites store (cookies, storage, and more) from each other, enhancing your privacy and security while you browse.
- **xBrowserSync** – Browser syncing as it should be: secure, anonymous and free! Sync bookmarks across your browsers and devices, no sign up required.
- **ClearURLs** – Removes tracking elements from URLs

@hackinarticles https://github.com/ignitetechnologies https://in.linkedin.com/company/hackingarticles iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE



BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in