Firefox Addons for Security Practitioners

Join the Discussion
Connect

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Prerequisites

Firefox browser

I think we can all agree that web browsers themselves are tools for information security practitioners and analysts. I will freely admit that I use all major browsers (Internet Explorer, Firefox, Safari, and Opera) as a function of web application security testing and researching the nuances of web-based malware. But that said, I more often use Firefox for one reason in particular (no, we're not going to have that "Which browser is more secure?" debate): all of the add-ons available with a security-specific focus or applicability. There are add-ons loaded in my instances of Firefox that I quite simply can't live without and I assume that is likely the case for some of you as well. One thing to keep in mind as we discuss a variety of add-ons for Firefox: add-ons themselves can introduce security vulnerabilities. Always install them from trusted resources and keep them updated. Remember, just because you download the add-on from Add-ons for Firefox,[1] there's no guarantee of safety. As I write this, Firefox 3.6 was released. In addition to the new Plugin Check, the Component Directory Lockdown feature prevents silently installed rogue add-ons as an attack vector.

I'll likely miss someone's favorite add-on and hear about it; if there's an add-on you simply can't live without, let me know via email and I'll write a follow up blog post.

Installing add-ons

Add-on installation is very simple. Find the add-on you're looking for in at the Add-ons for Firefox site and click the Add to Firefox button. A great starting point is the Privacy and Security[2] category.

Using add-ons

On the above mentioned Privacy and Security page you'll note Top Downloads. There are few add-ons that are on that list for good reason.

No Script, FoxyProxy Standard, BetterPrivacy, and Torbutton are all loaded on my Firefox instances; most of these you've likely heard of.

NoScript[3] is Giorgio Maone's add-on that blocks JavaScript, Java, Flash, Silverlight, and others from executing until explicitly permitted to do so by the user. You can then choose to whitelist known good sites and content. NoScript provides anti-cross-site scripting (XSS) protections (see Figure 1) and ClearClick to help protect you from Clickjacking.

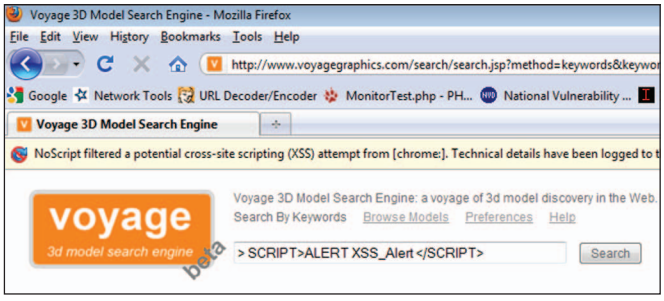

Figure 1 – NoScript prevents an XSS attempt

As I write this, the current version is 1.9.9.39 and offers many enhancements.

Note: NoScript and web application security testing do not play well together as NoScript will prevent you from busting loose on a site until you allow it. It's easier to disable NoScript (Allow Scripts Globally) while you test, then re-enable it.

Eric Jung's FoxyProxy[4] is an excellent proxy switching tool that is essential when you utilize numerous proxies as I do (see Figure 2).

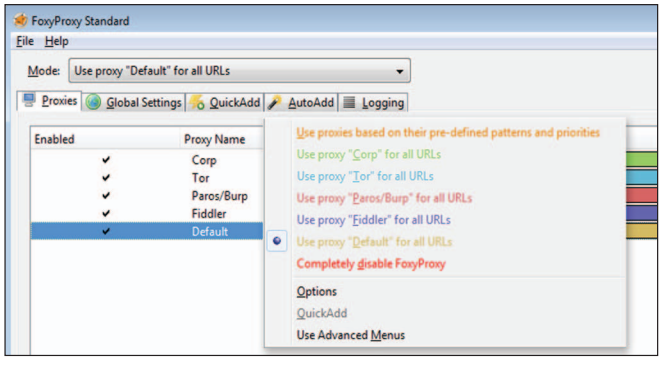

Figure 2 – FoxyProxy selection menu.

Imagine you use Burp Suite on port 8080, Paros on 8081, and you also need a quick Tor connection, and you want to be able

1 https://addons.mozilla.org/en-US/firefox.

2 https://addons.mozilla.org/en-US/firefox/browse/type:1/cat:12.

3 https://addons.mozilla.org/en-US/firefox/addon/722.

4 https://addons.mozilla.org/en-US/firefox/addon/2464.

to bounce services on the fly, or set rules that move certain traffic through one proxy while other traffic heads out through a different proxy. Want to do all that manually? Heck no, FoxyProxy to the rescue. Many a nuance can be finely configured with this add-on; I consider this add-on essential.

BetterPrivacy offers exactly what it says. Do what you will to purge cookies and tracking mechanisms to keep your browsing history private, but forget to wipe out Flash cookies, or Local Shared Objects (LSO), and all your efforts are for naught.

LSO Flash cookies never expire, offer 25 times the amount of storage of regular cookies, browsers aren't aware of them, can access and store highly specific personal and technical information, send said information without your permission, and so on, ad infinitum. Ready to get rid of the LSOs? Go get BetterPrivacy and set it to delete LSOs at a chosen interval or browser exit.

Mike Perry's Torbutton[5] provides a button to securely and easily enable or disable the browser's use of Tor. It is currently the only add-on that will safely manage your Tor browsing to prevent IP address leakage, cookie leakage, and general privacy attacks.[6] If you use Tor (the onion router; think "Layers. Onions have layers." - *Shrek*), the Torbutton is both convenient and ideal for managing Tor security (see Figure 3).

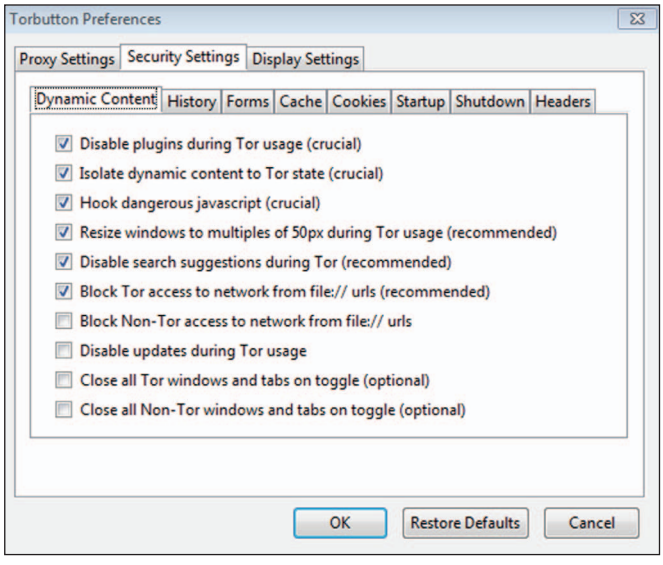

Figure 3 – Torbutton security settings.

Some add-ons you may not have heard of…

PassiveRecon

A new favorite of mine, Justin Morehouse's PassiveRecon,[7] will let you dig up everything you ever wanted to know about a given site you may be browsing or analyzing.

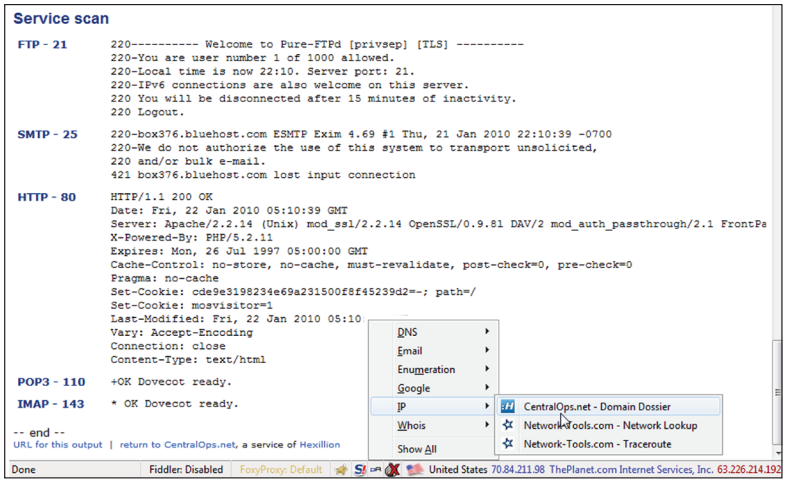

Figure 4 – PassiveRecon pulls the Domain Dossier.

As an example, consider holisticinfosec.org (surprise). Perhaps you're considering spending more time on my website, but you want to learn a bit more and quickly. Left click the PassiveRecon (PR) button tucked quietly away in the lower right-hand corner of your Firefox UI. You'll see a menu containing DNS, Email, Enumeration, Google, IP, and Whois. Each of those menu headings includes submenus chock full of options. Under IP, you'll find CentralOps Domain Dossier (my favorite), best used for address lookup, whois, DNS records, traceroute, and service scans all in one fell swoop.

You can even choose to unleash all options by selecting Show All. Be forewarned: open a new browser window if you want to use this option as it will open 23 tabs of information about the domain you are studying, including various Google filetype queries as well as feedback from Netcraft, Robtex, intoDNS, and the above mentioned CentralOps.

WorldIP

WorldIP[8] from WIPmania.com is very cool and very useful. It provides everything you could every need to know or trace with regard to IP addresses and geolocation. WorldIP will display the IP of any site you visit, its flag and country, while also displaying your external IP. If you want to see the AS number, reverse DNS, or data center, they're all there for you. I like to traceroute via WorldIP from one IP to another (see Figure 5) in some far off land such as Russia or Lithuania (hmm, I wonder why).

Additionally you can retrieve county data, report wrong country data, copy data to the clipboard, and research providers. This add-on excels when conducting recon against foreign targets.

Tamper Data

I wrote an entire column in April 2009[9] on Tamper Data as I consider it a *toolsmith* premier offering. Use Tamper Data to view and modify HTTP/HTTPS headers and post param-

5 https://addons.mozilla.org/en-US/firefox/addon/2275.

6 https://addons.mozilla.org/en-US/firefox/addon/2275.

7 https://addons.mozilla.org/en-US/firefox/addon/6196.

8 https://addons.mozilla.org/en-US/firefox/addon/8661.

9 http://holisticinfosec.org/toolsmith/docs/april2009.pdf.

eters.[10] I can't do my job effectively without it, but it's well documented in that issue so I suggest simply that you read up on it there.

Groundspeed

Last on my list for this month is Felipe Moreno-Strauch's Groundspeed, a newer add-on "that allows security testers to manipulate the application user interface to eliminate annoying limitations and client-side controls that interfere with the web application penetration tests."[11] In short Felipe means to perform input validation testing directly in the user interface with no dependence on proxies. OWASP aficionados rejoice!

Groundspeed allows you to modify the forms and form elements loaded in the page. Some practical uses include:

- Change the types of form fields. For example you can change hidden fields into text fields so you can easily edit their contents.
- Quickly remove size and length limitations on text fields so you have more space to type your attack strings.
- Change form target so the form submits in another tab.
- Remove or edit the JavaScript event handlers to bypass client side validation.[12]

Mmm…yummy, let's take a look. Again referring to holisticinfosec.org (I own it, so we can poke it ;-)), let's explore the search feature with Groundspeed. If I wanted to explore the forms associated with search functionality, I'd simply click Tools from the Firefox menu, choose Groundspeed, then Click to Load Forms. There are lots of options thereafter, including numerous encoding and decoding of Base64, Hex, HTML entities, Unicode, and URLs, as well as MD5 and SHA1 hash values for HIDDEN, TEXT, SUBMIT, RADIO, ELEMENT, and SELECT forms and others. Attributes can then be manipulated as well in order to play with value input options (see Figure 6).

Figure 5 – Traceroute the globe with WorldIP.

Don't forget the ability to remove length limits and modify size of any form parameter. All options are but a right-click away with Groundspeed loaded. Web application testers should make a swift addition of Groundspeed to their arsenals; it's light and packs a lot of punch.

In Conclusion

As I mentioned in the introduction, there are numerous other security-related Firefox add-ons that you may feel strongly about and want to share with a larger audience. Let me know via russ at holisticinfosec.org and I'll build a follow up feature to share the feedback.

Make good use of these and other add-ons while performing your infosec duties; they won't let you down.

Cheers…until next month.

Acknowledgments

— Giorgio Maone for NoScript
— Eric Jung for FoxyProxy
— Mike Perry for Torbutton
— Justin Morehouse for PassiveRecon
— Felipe Moreno-Strauch for Groundspeed

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.

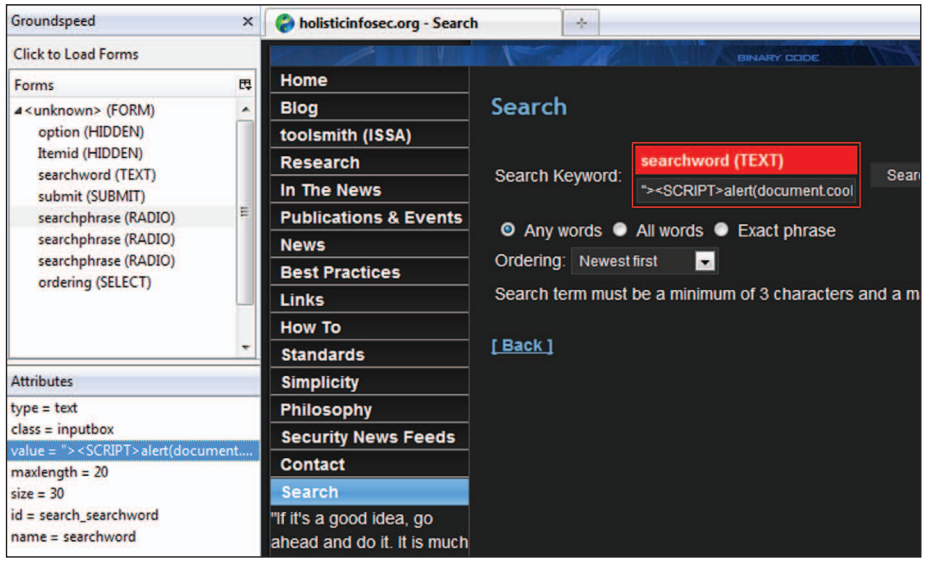

Figure 6 – Play a game of Whack-a-form with Groundspeed.

10 https://addons.mozilla.org/en-US/firefox/addon/966.

11 https://addons.mozilla.org/en-US/firefox/addon/46698.

12 http://groundspeed.wobot.org/about.