Turning Firefox to an Ethical Hacking Platform

February 2007, by Security-Database

Internet is an amazing virtual world where you can "virtually" do anything: gambling, playing, watching movies, shopping, working, "VoIPying", spying other people and for sure auditing remote systems.

The security testers' community has a large panel of security tools, methodologies and much more to perform their pentests and audit assessments. But what happens if you find yourself weaponless.

No more Top 100 security tools, no more LiveCDs and no more exploitation frameworks. A security auditor without toolbox is like a cop without gun.

Nevertheless, there is maybe a way to rescue yourself from this nightmare situation.

The magical solution could be Firefox and its extensions developed by ethical hackers and coders.

This article comes as an update for what we posted previously about how to switch your Firefox to more than an usual simple browser. It was about application auditing

Here is an updated list of useful security auditing extensions:

- **Information gathering**
  - **Whois and geo-location**
    - ShowIP : Show the IP address of the current page in the status bar. It also allows querying custom services by IP (right mouse button) and Hostname (left mouse button), like whois, netcraft.
    - Shazou : The product called Shazou (pronounced Shazoo it is Japanese for mapping) enables the user with one-click to map and geo-locate any website they are currently viewing.
    - HostIP.info Geolocation : Displays Geolocation information for a website using hostip.info data. Works with all versions of Firefox.
    - Active Whois : Starting Active Whois to get details about any Web site owner and its host server.
    - Bibirmer Toolbar : An all-in-one extension. But auditors need to play with the toolbox. It includes (WhoIs, DNS Report, Geolocation, Traceroute, Ping). Very useful for information gathering phase
  - **Enumeration / fingerprinting**
    - Header Spy : Shows HTTP headers on statusbar
    - Header Monitor : This is Firefox extension for display on statusbar panel any HTTP response header of top level document returned by a web server. Example: Server (by default), Content-Encoding, Content-Type, X-Powered-By and others.
  - **Social engineering**
    - People Search and Public Record : This Firefox extension is a handy menu tool for investigators, reporters, legal professionals, real estate agents, online researchers and anyone interested in doing their own basic people searches and public record lookups as well as background research.

- **Googling and spidering**
    - Advanced dork : Gives quick access to Google's Advanced Operators directly from the context menu. This could be used to spider a site or scan for hidden files (this spider technique is used via scroogle.org)
    - SpiderZilla : Spiderzilla is an easy-to-use website mirror utility, based on Httrack from www.httrack.com.
    - View Dependencies : View Dependencies adds a tab to the "page info" window, in which it lists all the files which were loaded to show the current page. (useful for a spidering technique)

- **Security Assessment / Code auditing**
    - **Editors**
        - JSView : The 'view page source' menu item now opens files based on the behaviour you choose in the jsview options. This allows you to open the source code of any web page in a new tab or in an external editor.
        - Cert Viewer Plus : Adds two options to the certificate viewer in Firefox or Thunderbird: an X.509 certificate can either be displayed in PEM format (Base64/RFC 1421, opens in a new window) or saved to a file (in PEM or DER format - and PKCS#7 provided that the respective patch has been applied - cf.
        - Firebug : Firebug integrates with Firefox to put a wealth of development tools at your fingertips while you browse. You can edit, debug, and monitor CSS, HTML, and JavaScript live in any web page
        - XML Developer Toolbar : Allows XML Developer's use of standard tools all from your browser.
    - **Headers manipulation**
        - HeaderMonitor : This is Firefox extension for display on statusbar panel any HTTP response header of top level document returned by a web server. Example: Server (by default), Content-Encoding, Content-Type, X-Powered-By and others.
        - RefControl : Control what gets sent as the HTTP Referrer on a per-site basis.
        - User Agent Switcher : Adds a menu and a toolbar button to switch the user agent of the browser
    - **Cookies manipulation**
        - Add N Edit Cookies : Cookie Editor that allows you add and edit "session" and saved cookies.
        - CookieSwap : CookieSwap is an extension that enables you to maintain numerous sets or "profiles" of cookies that you can quickly swap between while browsing
        - httpOnly : Adds httpOnly cookie support to Firefox by encrypting cookies marked as httpOnly on the browser side
        - Allcookies : Dumps ALL cookies (including session cookies) to Firefox standard cookies.txt file
    - **Security auditing**
        - HackBar : This toolbar will help you in testing SQL injections, XSS holes and site security. It is NOT a tool for executing standard exploits and it will NOT teach you how to hack a site. Its main purpose is to help a developer do security audits on his code.
        - Tamper Data : Use "tamper data" to view and modify HTTP/HTTPS headers and post parameters.
        - Chickenfoot : Chickenfoot is a Firefox extension that puts a programming environment in the browser's sidebar so you can write scripts to manipulate web pages and automate web browsing. In Chickenfoot, scripts are written in a superset of JavaScript that includes special functions specific to web tasks.

- **Proxy/web utilities**
  - FoxyProxy : FoxyProxy is an advanced proxy management tool that completely replaces Firefox's proxy configuration. It offers more features than SwitchProxy, ProxyButton, QuickProxy, xyzproxy, ProxyTex, etc
  - SwitchProxy : SwitchProxy lets you manage and switch between multiple proxy configurations quickly and easily. You can also use it as an anonymizer to protect your computer from prying eyes
  - POW (Plain Old WebServer) : The Plain Old Webserver uses Server-side JavaScript (SJS) to run a server inside your browser. Use it to distribute files from your browser. It supports Server-side JS, GET, POST, uploads, Cookies, SQLite and AJAX. It has security features to password-protect your site. Users have created a wiki, chat room and search engine using SJS.
- **Misc**
  - **Hacks for fun**
    - Greasemonkey : Allows you to customize the way a webpage displays using small bits of JavaScript (scripts could be download here)
  - **Encryption**
    - Fire Encrypter : FireEncrypter is a Firefox extension which gives you encryption/decryption and hashing functionalities right from your Firefox browser, mostly useful for developers or for education & fun.
- **Malware scanner**
  - QArchive.org web files checker : Allowing people to check web files for any malware (viruses, trojans, worms, adware, spyware and other unwanted things) inclusions.
  - Dr.Web anti-virus link checker : This plugin allows you to check any file you are about to download, any page you are about to visit
  - ClamWin Antivirus Glue for Firefox : This extension scans every downloaded file automatically with ClamWin.
- **Anti Spoof**
  - refspoof : Easy to pretend to origin from a site by overriding the URL referrer (in a http request). — It incorporates this feature by using the pseudo-protocol spoof:// .. Thus it's possible to store the information in a "hyperlink" - that can be used in any context... like html pages or bookmarks

Besides, we keep watching new extensions and we are on the way to develop a new extension for Nmap and Nessus. So keep watching us.

Feel free to send us (info@security-database.com) any useful information about security and audit oriented Firefox extensions.