# Assessing and Exploiting Web Applications with the Open-Source Samurai Web Testing Framework

Raul Siles

Taddong, Spain
raul@raulsiles.com

The Samurai Web Testing Framework (WTF) is an open-source LiveCD based on Ubuntu and focused on web application security testing. It includes an extensive collection of pre-installed and pre-configured top penetration testing and security analysis tools, becoming the perfect environment for assessing and exploiting web applications. The tools categorization guides the analyst through the web-app penetration testing methodology, from reconnaissance, to mapping, discovery and exploitation. The project web page is http://sf.net/projects/samurai/.

Samurai WTF pretends to become the weapon of choice for professional web app pen-testers, offering a well established environment that acts as a time saver as it includes all the required web application security tools pre-configured and ready to run.

This talk describes the actively developed Samurai WTF distribution, its tool set, including the recently created Samurai WTF Firefox add-ons collection (to convert the browser in the ultimate pen-testing tool), available at https://addons.mozilla.org/en-US/firefox/ collection/samurai, the advanced features provided by the integration of multiple attack tools, plus the new tool update capabilities. This recently added SVN update functionality provides frequent update capabilities for Samurai WTF, new update feature for the most actively developed security testing tools, and offers an improved collaboration model between the Samurai WTF community members.

The talk ends up with a live demonstration on a target web application of the advanced attack techniques provided by the integration of tools like Sqlninja and Metasploit. The combination of both tools offers the pen-tester the option to take full control of a vulnerable web infrastructure, including the internal database servers.

C. Serrão, V. Aguilera, and F. Cerullo (Eds.): IBWAS 2009, CCIS 72, p. 13, 2010.