

Assessing and Exploiting Web Apps with Samurai-WTF

Raúl Siles

● Taddong

IB '09
WAS



Taddong

www.taddong.com



SAMURAI WEB TESTING FRAMEWORK

[HTTP://SAMURAI.INGUARDIANS.COM](http://samurai.inguardians.com)



Samurai-WTF

- Web Testing Framework (WTF)
 - Very active & cutting-edge security field
- Open-source project
- Live CD ISO (and VMware image)
- Based on Ubuntu (v9.04)
- Current version: v0.7 (+ SVN)
- Latest SVN revision: 3
 - Named "IBWAS'09"

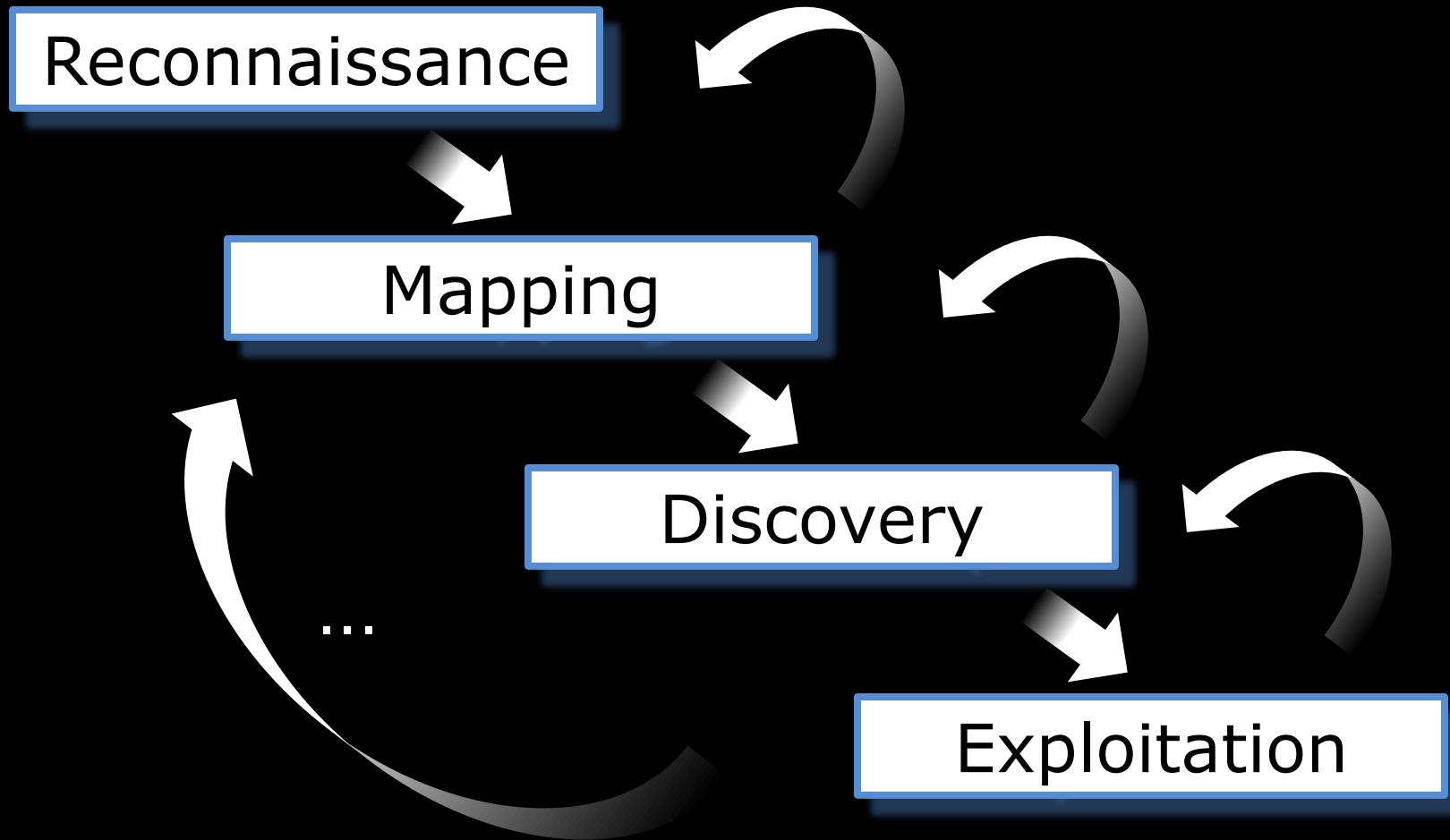


Samurai-WTF Goals

- Become the de facto open-source environment for web app security testing
 - Weapon of choice for professional web app pen-testers
- Web app security tools ready to run
 - Time saver
- Integration of various tools
 - Advanced attacks
- SVN
 - Frequent updates & better collaboration



Web App Assessment Methodology



Automated vs. Manual Testing



Automated vs. Manual Testing



Automated vs. Manual Testing



Which one is the best? 😊

Samurai-WTF Login

Credentials: samurai/samurai

SAMURAI WEB TESTING FRAMEWORK

HTTP://SAMURAI.INGUARDIANS.COM



Please enter your username

USERNAME AND PASSWORD ARE SAMURAI

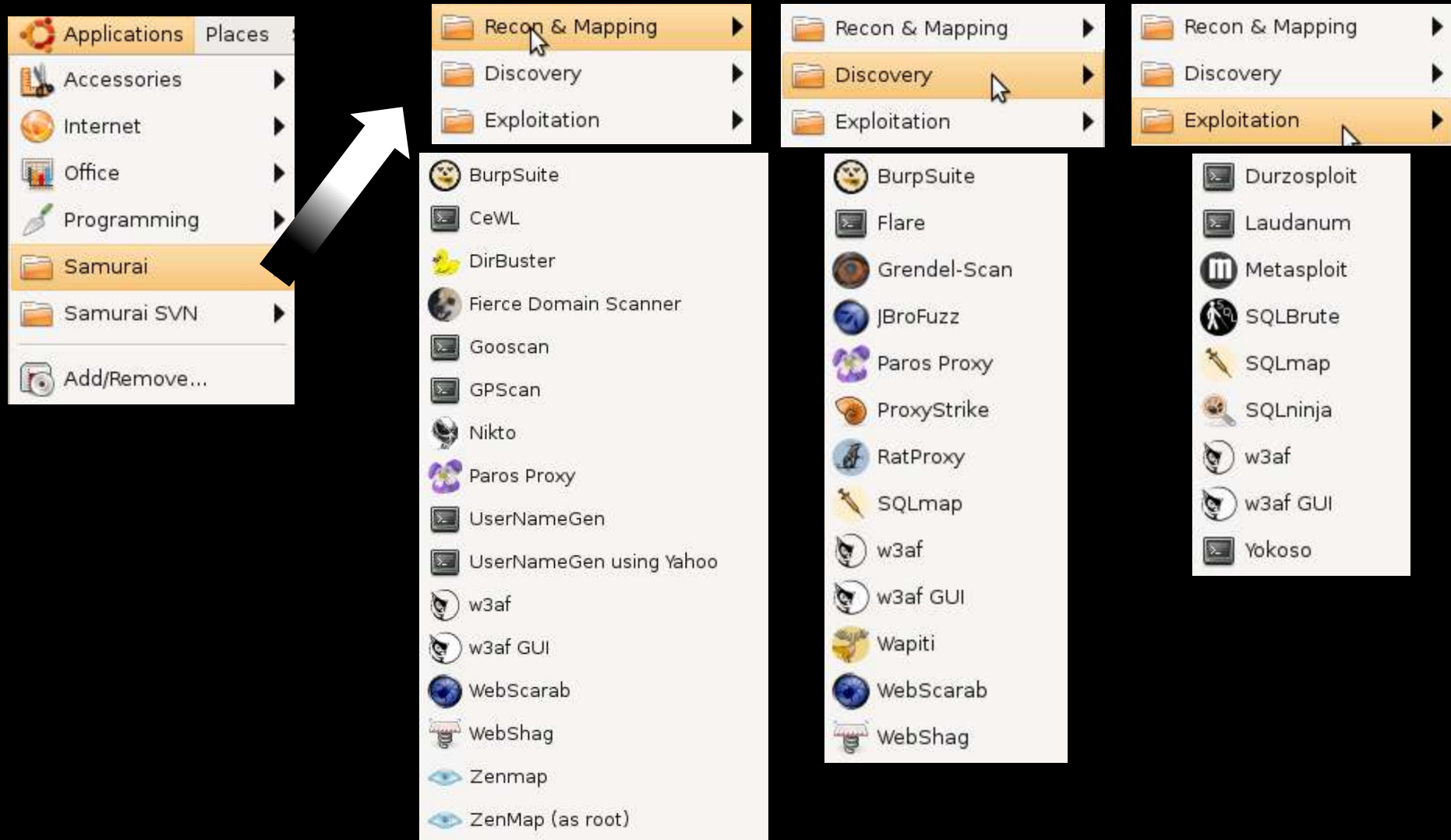
samurai

Tue Dec 08, 3:05 AM

← Sessions →

← Actions →

Samurai-WTF Toolset



“A tool a day keeps the attackers away”

Tools ~ Recon & Mapping

- Whois & DNS
- Fierce Domain Scanner
- Gooscan
- GPscan
- Maltego CE
- CeWL
- Reconnoiter
- Nmap & Zenmap
- Nikto
- DirBuster
- W3C link checker
- wget, curl, httrack, HTTPing, MySQL, Apache, html2text, w3m...
- *Wiki (MoinMoin)*



Tools ~ Discovery

- w3af
- Grendel-Scan
- RatProxy
- JBroFuzz
- WebShag
- Wapiti
- Flare
- Burp Suite
- Paros Proxy
- WebScarab
- ProxyStrike



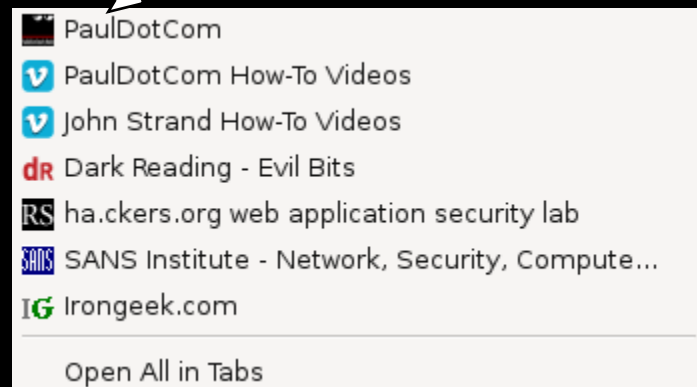
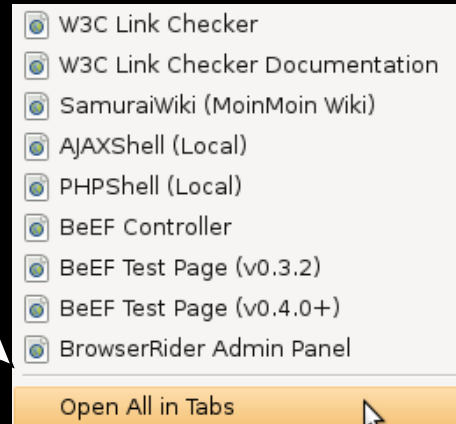
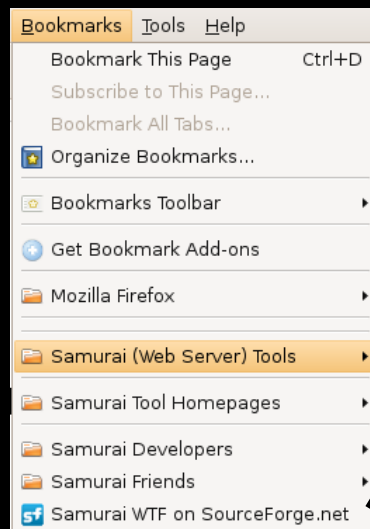
Tools ~ Exploitation

- BeEF
- BrowserRider
- Durzosploit
- PHPShell
- AJAXShell
- SQLBrute
- SQLmap
- SQLninja
- Laudanum
- Yokoso



Tools: Firefox Bookmarks

- AJAX/PHP Command Shell
- BeEF - BindShell.Net
- Browser Rider - A hacking framework for brow...
- Burp Suite - PortSwigger.net
- CeWL - DigiNinja.org
- DirBuster
- Durzosplit Introduction - Engineering For Fun
- Fierce Domain Scan
- Flare- no|wrap.de
- gpscan - DigiNinja.org
- Grendel-Scan
- JBroFuzz - OWASP
- Laudanum: Injectable Functionality for Penetr...
- Maltego » Community Edition
- The Metasploit Project
- Nikto | CIRT.net
- Nmap - Free Security Scanner For Network E...
- MoinMoinWiki - MoinMoin
- Parosproxy.org - Web Application Security
- PHP Shell
- ProxyStrike - Edge-Security
- ratproxy - Project Hosting on Google Code
- Reconnoiter | Get Reconnoiter at SourceForg...
- sqlmap: automatic SQL injection tool
- sqlninja - a SQL Server injection & takeover t...
- SQLBrute - Gotham Digital Science
- w3af - Web Application Attack and Audit Fra...
- Wapiti - Web application security auditor
- WebScarab - OWASP
- Webshag
- Wireshark
- Yokoso! Infrastructure Fingerprinting via XSS



Tools: Firefox Add-on Collection



Access Me 0.2.3
An extension to test for page access vulnerabilities (session tampering).

Add N Edit Cookies 0.2.1.3
Cookie Editor that allows you add and edit session and saved cookies

Advanced Dork: 2.3.3.6
Advanced Dork: gives quick access to Google's Advanced Operators directly from the context menu.
Options Disable Uninstall

DOM Inspector 2.0.4
Inspects the structure and properties of a window and its contents.

Firebug 1.4.5
Web Development Evolved.

FoxyProxy Standard 2.15
FoxyProxy - Premier proxy management for Firefox

Greasemonkey 0.8.20090920.2
A User Script Manager for Firefox

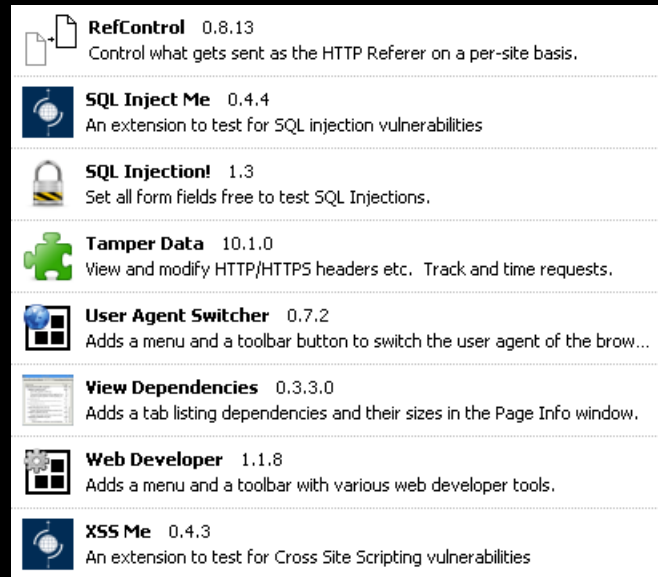
HackBar 1.4.2
A toolbar that helps you find and test SQL injections

Header Spy 1.3.3.3
Shows HTTP headers on statusbar

Java Quick Starter 1.0

JavaScript Deobfuscator 1.5.4
Shows you what JavaScript code gets to run on webpages

JSView 2.0.5
View the source code of external stylesheets and javascripts.



RefControl 0.8.13
Control what gets sent as the HTTP Referer on a per-site basis.

SQL Inject Me 0.4.4
An extension to test for SQL injection vulnerabilities

SQL Injection! 1.3
Set all form fields free to test SQL Injections.

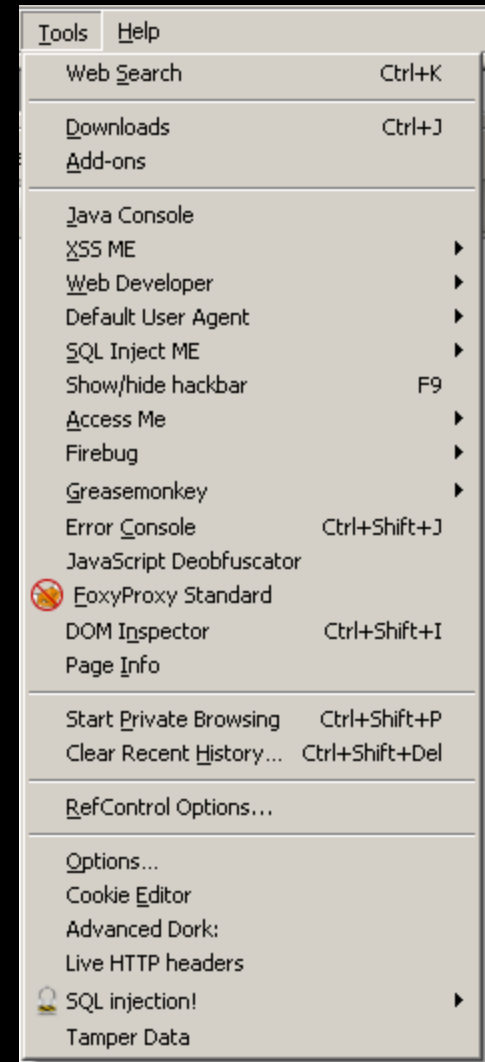
Tamper Data 10.1.0
View and modify HTTP/HTTPS headers etc. Track and time requests.

User Agent Switcher 0.7.2
Adds a menu and a toolbar button to switch the user agent of the browser.

View Dependencies 0.3.3.0
Adds a tab listing dependencies and their sizes in the Page Info window.

Web Developer 1.1.8
Adds a menu and a toolbar with various web developer tools.

XSS Me 0.4.3
An extension to test for Cross Site Scripting vulnerabilities



Tools Help

- Web Search Ctrl+K
- Downloads Ctrl+J
- Add-ons
- Java Console
- XSS ME
- Web Developer
- Default User Agent
- SQL Inject ME
- Show/hide hackbar F9
- Access Me
- Firebug
- Greasemonkey
- Error Console Ctrl+Shift+J
- JavaScript Deobfuscator
- FoxyProxy Standard
- DOM Inspector Ctrl+Shift+I
- Page Info
- Start Private Browsing Ctrl+Shift+P
- Clear Recent History... Ctrl+Shift+Del
- RefControl Options...
- Options...
- Cookie Editor
- Advanced Dork:
- Live HTTP headers
- SQL injection!
- Tamper Data



Integration of various tools

- Examples.-
 - SQLmap & Metasploit
 - SQLninja & Metasploit
 - BeEF & Metasploit
 - Nmap & Yokoso
 - BrowserRider & BeEF & Durzosploit
 - w3af & Burp/WebScarab
 - ...



Samurai-WTF SVN Repository (1)

Log in as the "samurai" user:

```
$ cd /tmp
$ svn co ➤
  https://samurai.svn.sourceforge.net/svnroot/samurai/trunk ➤
  samurai
$ cd samurai
```

Open the README file & follow instructions:

```
# Cleanup script for Samurai v0.7
$ sudo ./cleanup_v0.7.sh

# New Samurai SVN update infrastructure for most of the tools
$ sudo ./install_samurai_svn.sh
...
```

Samurai-WTF SVN Repository (2)

Installation of new tools:

```
...  
# Script to setup new tools or update current tools (!in SVN)  
$ sudo ./install_samurai_setup.sh
```

Set current version and release disk space:

```
# Set current version for Samurai v0.7 + SVN revision  
$ ./set_samurai_version.sh  
  
# Remove the Samurai-WTF SVN copy to release disk space  
$ cd /tmp  
$ rm -rf samurai
```

SVN Update Infrastructure

- Samurai-WTF SVN **!=** SVN update infrastructure for most security tools
- Easy & quick update capabilities for current and new tools
- Sync with actively developed tools
 - SVN is the source for cutting-edge releases
- Overcome the constraints of the official OS repositories
 - Eg. Wireshark 1.0.7 (12/2009) vs. 1.2.4



SVN Update Infrastructure Menus



What is Coming...?

- Automated installation of the Firefox Add-on Collection from SVN scripts
- Kubuntu
- Debian packages
- Optional modules to add vulnerable applications for training purposes
- More, more & more new tools...



How Can You Get Involved?

- Download Samurai-WTF and use it
 - Spread the word (only if you like it 😊)
- Provide feedback
 - Bugs
 - New capabilities and improvements
- Test the new SVN capabilities
- Join the devel mailing-list (sf.net)
- Develop new web app security tools



Similar Projects

- OWASP Live CD



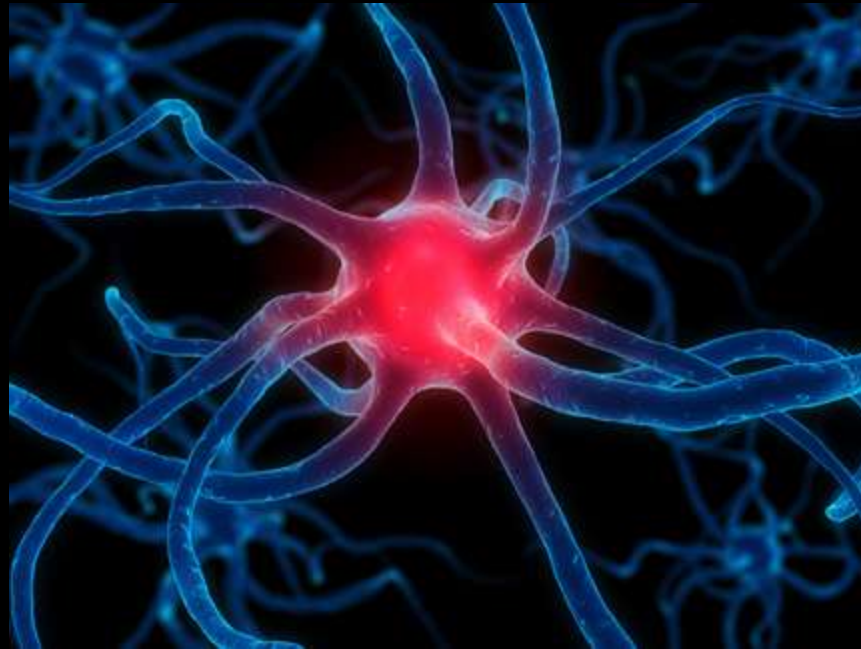
- Matt Tesauro (future collaboration)
- OWASP oriented
- Tools, documentation, and vulnerable web apps (WegGoat)

- Backtrack



- remote-exploit.org crew
- Network pen-testing Live CD (& VM)

DEMOS



Contact Info



Taddong

www.taddong.com

Radajo

www.radajo.com

ℳ Raúl Siles

www.raulsiles.com

raul@raulsiles.com



References

- Samurai-WTF
 - <http://samurai.inguardians.com>
 - <http://sf.net/projects/samurai/>
- Samurai-WTF Firefox Add-on Collection
 - <https://addons.mozilla.org/en-US/firefox/collection/samurai>
- Samurai-WTF training (coming to cons)
- Dev Team:
 - Kevin Johnson & Justin Searle
 - Frank DiMaggio
 - Raul Siles