Assessing and Exploiting Web Apps with Samurai-WTF

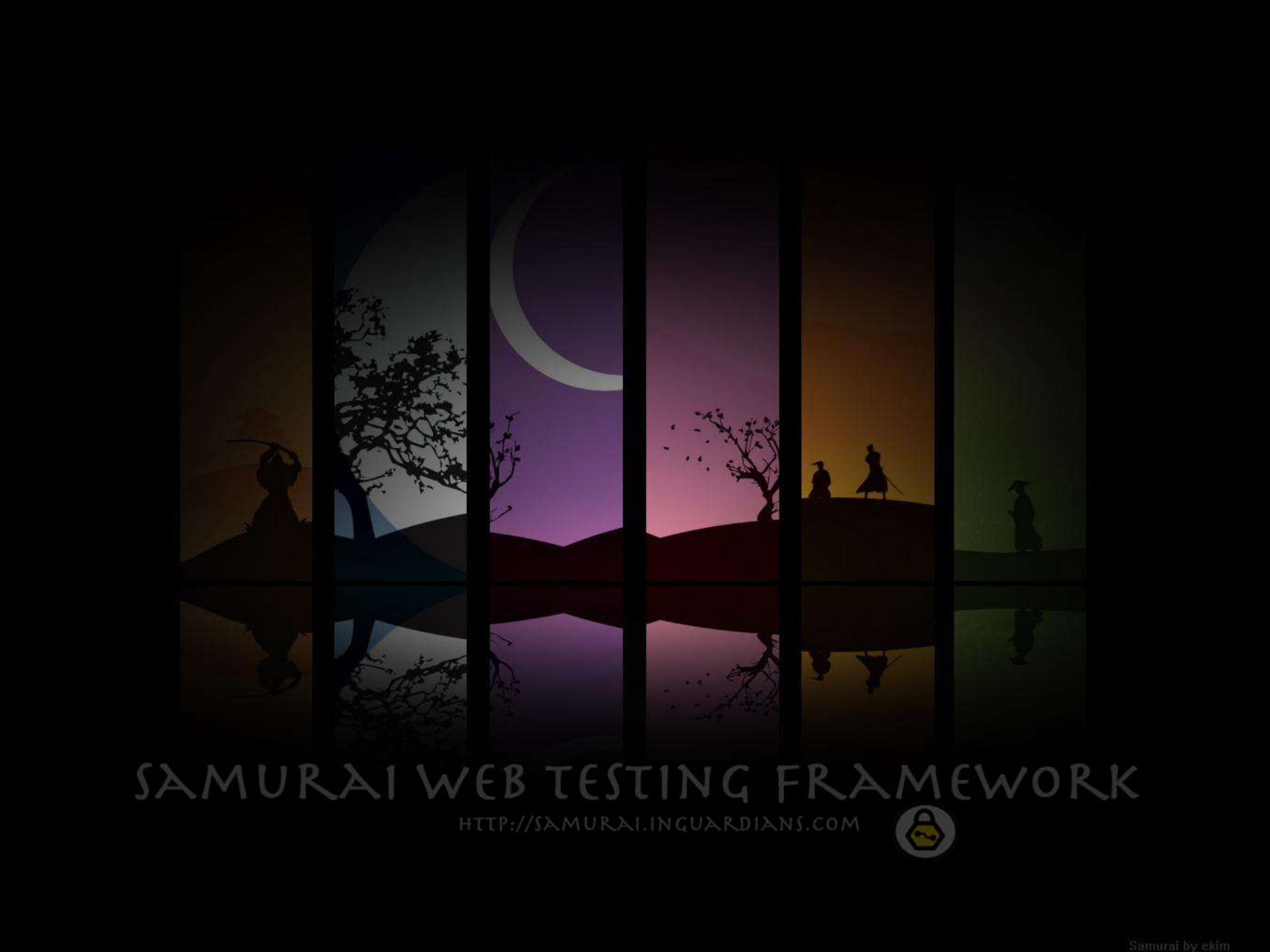
Raúl Siles

Taddong

IBWAS '09

Taddong

www.taddong.com


SAMURAI WEB TESTING FRAMEWORK
HTTP://SAMURAI.INGUARDIANS.COM
Samurai by ekim

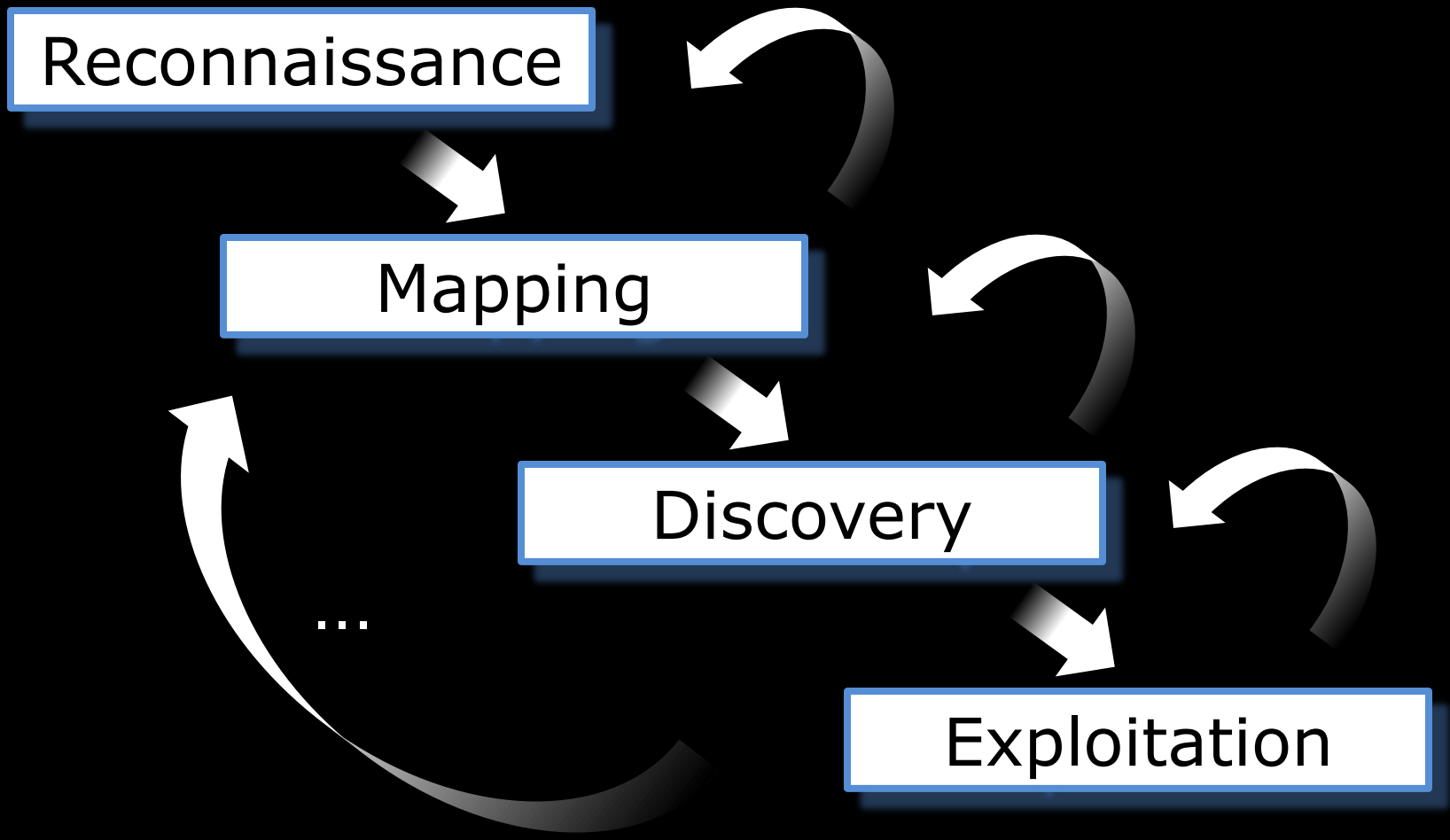
Samurai-WTF

- 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

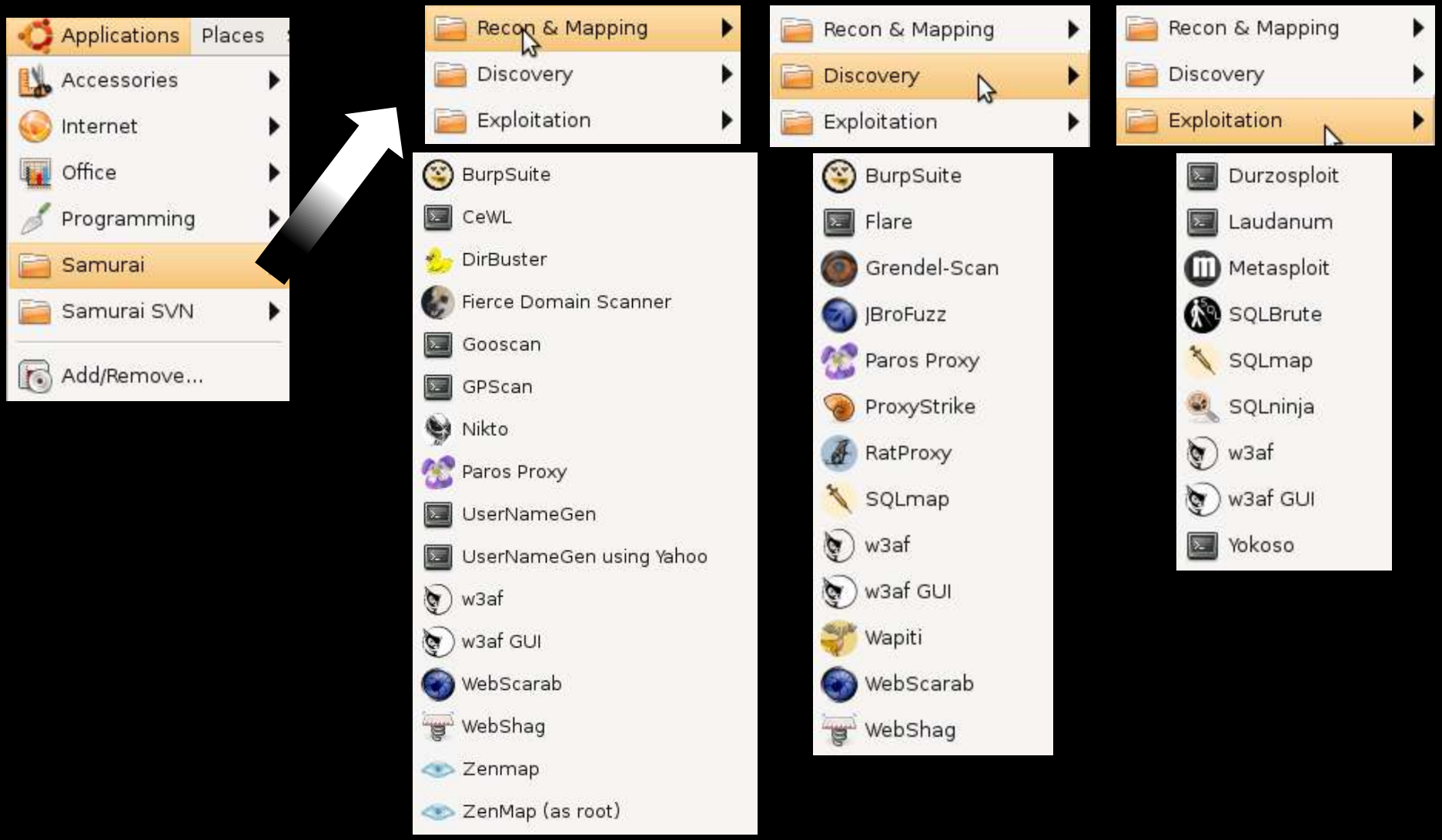
Automated vs. Manual Testing

Which one is the best? ☺

Samurai-WTF Login

Credentials: samurai/samurai

Samurai-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

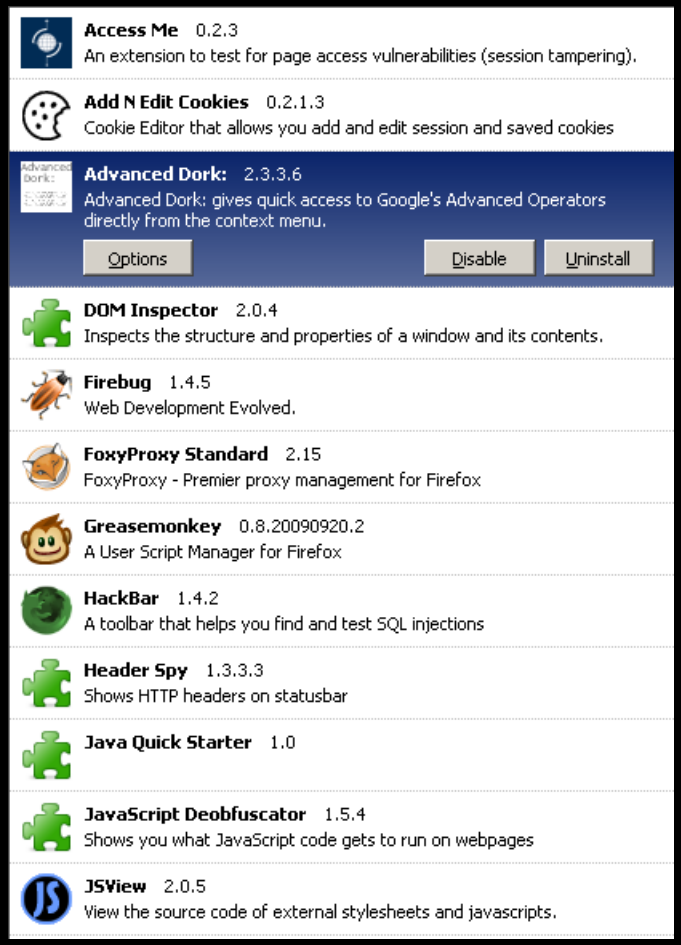
- w3af
- Grendel-Scan
- RatProxy
- JBroFuzz
- WebShag
- Wapiti
- Flare
- Burp Suite
- Paros Proxy
- WebScarab
- ProxyStrike

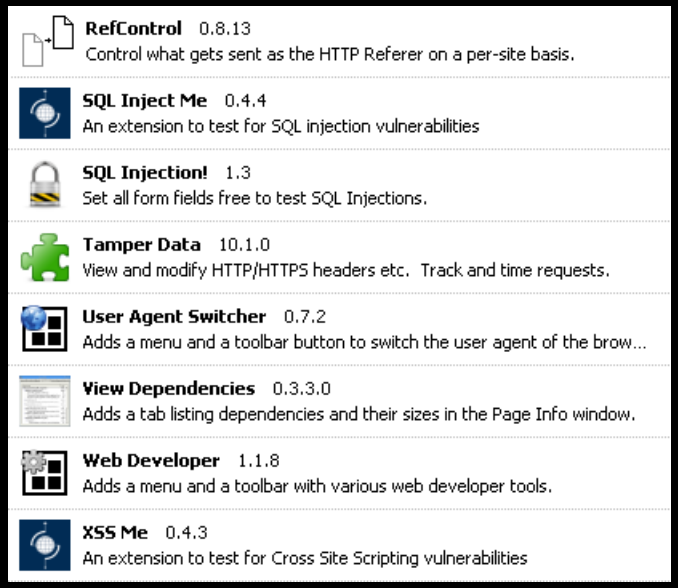
Tools ~ Exploitation

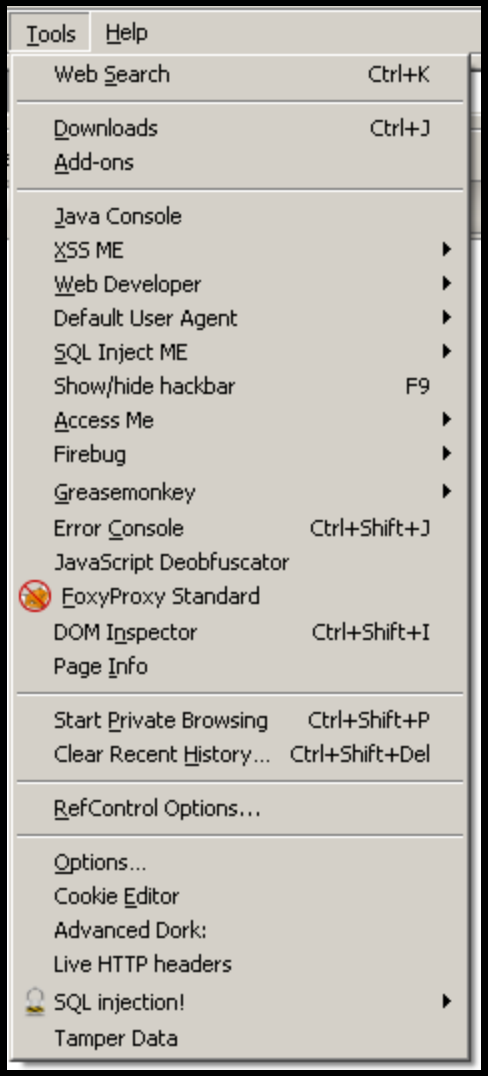
- BeEF
- BrowserRider
- Durzosploit
- PHPShell
- AJAXShell
- SQLBrute
- SQLmap
- SQLninja
- Laudanum
- Yokoso

Tools: Firefox Bookmarks

Tools: Firefox Add-on Collection







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:

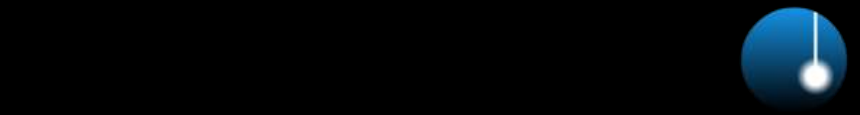
```
...
# Script to setup new tools or update current tools (!in SVN)
$ sudo ./install_samurai_setup.sh
```

Set current version and release disk space:

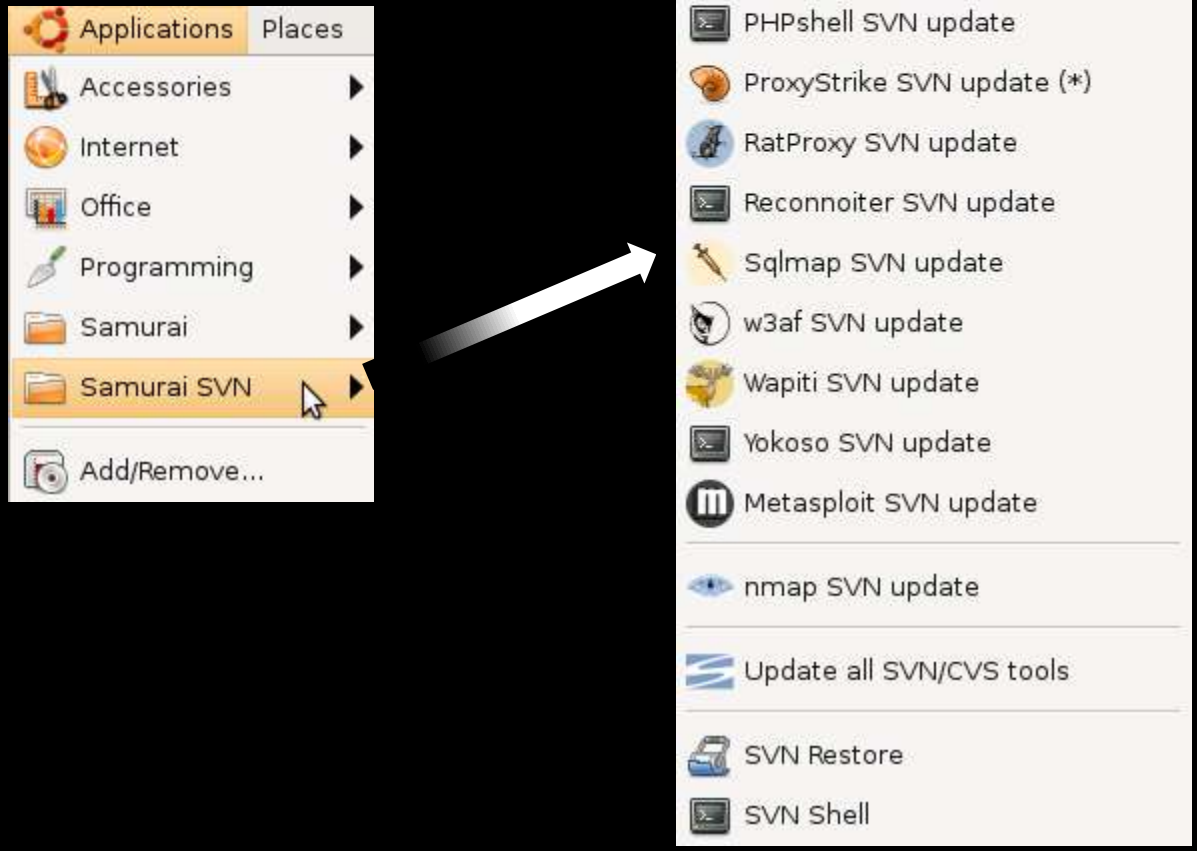
```
# Set current version for Samurai v0.7 + SVN revision
$ ./set_samurai_version.sh

# 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…

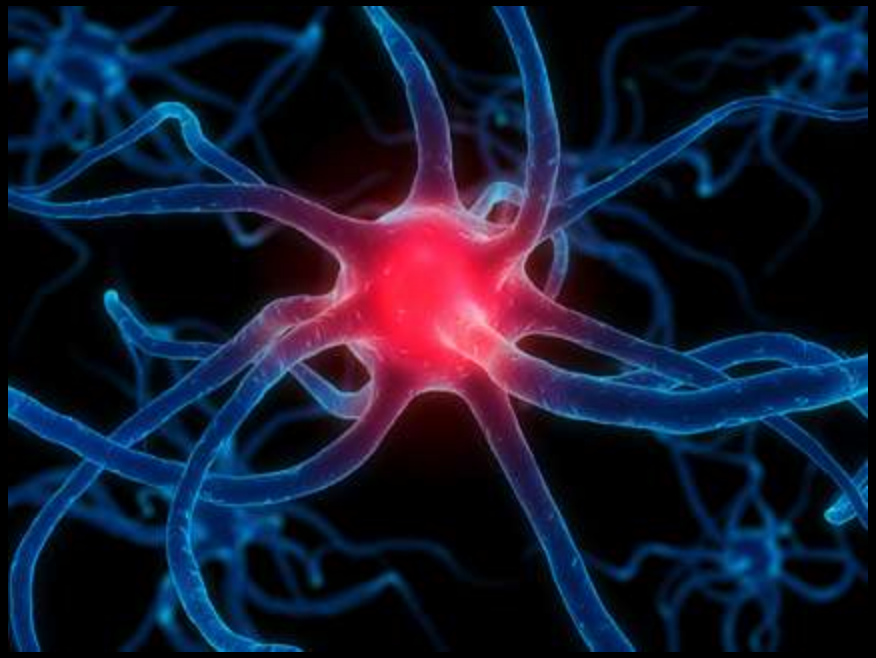
How Can You Get Involved?

- 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

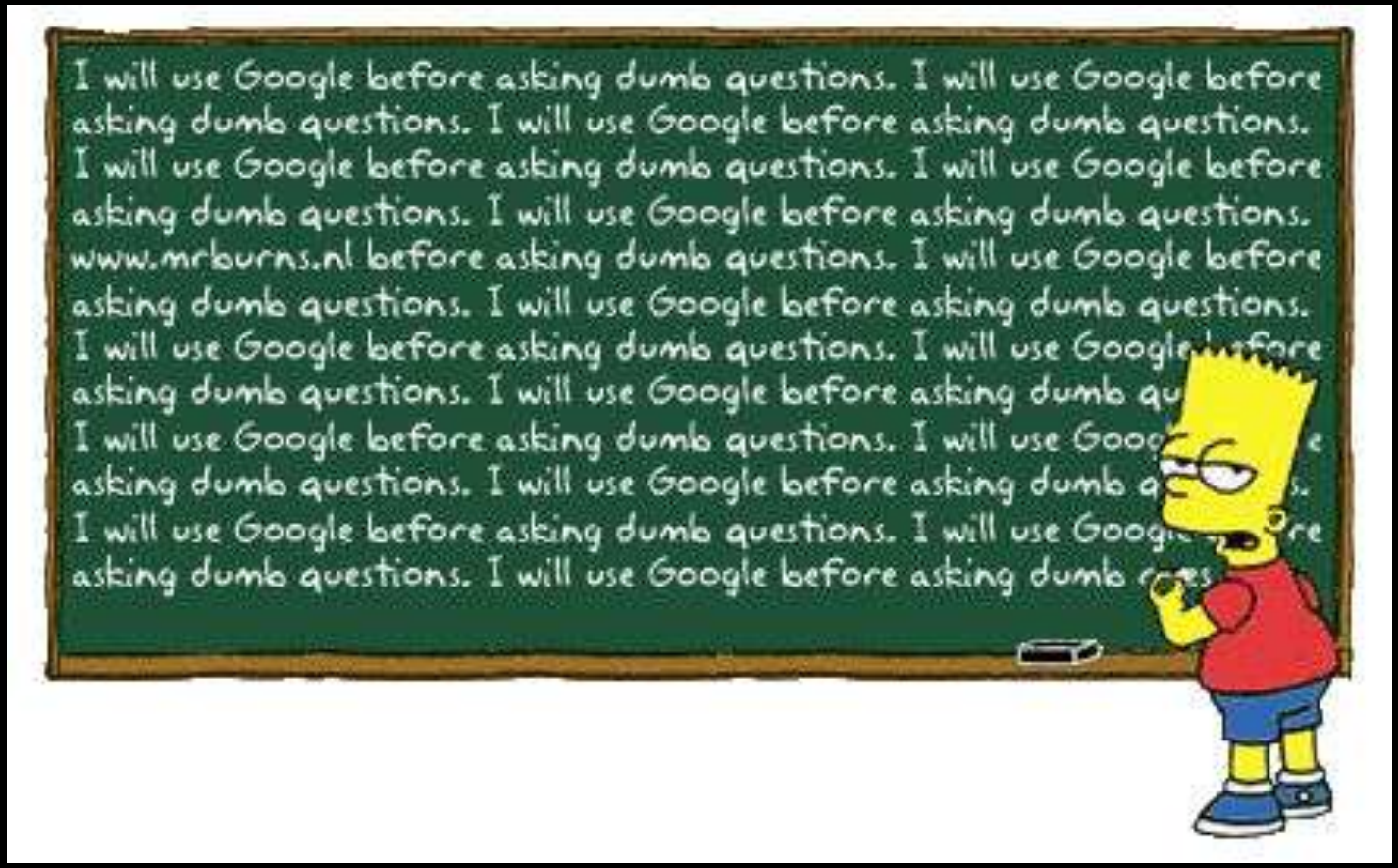
Similar Projects

- 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



Questions ☺


I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. www.mrburns.nl before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions.

Contact Info

Taddong

www.taddong.com

RaDaJo

www.radajo.com

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