Newsletter - January 2015

ToolsWatch Team
NJ OUCHN & MJ SOLER

Tools! Lots of Tools Released!

During January 2015, we published 13 Posts with 7 News Tools.

Organized by Date

- [New Tool] CapTipper v0.1 – Malicious HTTP Traffic Explorer Tool
- [New Tool] Forpix v1.02 – Forensic Images Tool Released
- PEStudio v8.46 Released
- WPScan v2.6 Released
- Wireshark v1.12.3 Released
- SPARTA Beta Network Infrastructure Pen Test Tool Released
- SeeS v4.1 Social Enginnering Email Sender Released
- oclHashcat v1.31 Released
- [New Tool] Babel Scripting Framework (babel-sf) v0.1 Released
- [New Tool] Crowbar v1.0 Brute Forcing Tool Released
- [New Tool] pwntools v2.2.0 CTF Framework and Exploit Dev Library
- [New Tool] AIEngine v0.8 (Artificial Inteligent Engine)
- [New Tool] NexusTaco v1.0 SNMP Scanner Cisco Nexus Switches (CVE-2014-3341)

Black Hat Arsenal ASIA 2015 - Call for Tools

March 25-26, 2015 @ Marina Bay Sands, Singapore

http://www.toolswatch.org/?p=132027

Developer Corner

Articles:

- IDASynergy: Tool for collaborative reversing with IDA Pro. (By ***Cubica Labs***)

Papers

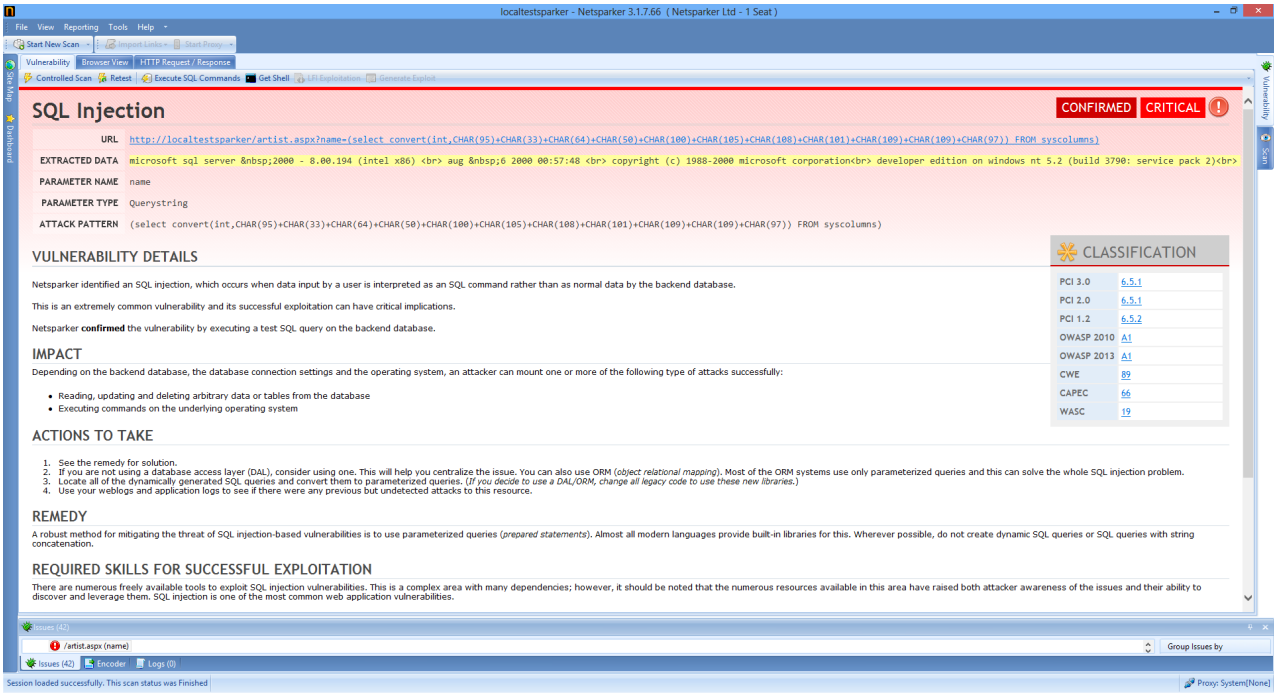
- 2014 Top Security Tools as Voted by ToolsWatch.org Readers

Find Vulnerabilities in your Web Applications with Netsparker

Malicious hackers are constantly looking for vulnerable web applications to hack into and steal sensitive business intelligence data, customer information, credit card numbers and more.

The more your business relies on web applications the more of a target these web applications become because they are available 24/7 and are unprotected. Web application vulnerabilities can be automatically detected and are easily exploited.

You can find web application vulnerabilities such as **SQL Injection** and **Cross-site Scripting** (XSS) with the Netsparker Web Application Security Scanner before hackers do and ensure that your web applications, business operations and reputation are protected. Netsparker is the only fully automated **False Positive Free** web application security scanner that detects vulnerabilities on websites and in web applications and reports extensive details about every detected vulnerability.



Netsparker is the only False-positive-free web application security scanner

www.netsparker.com

Tools! Lots of Tools Released!

[New Tool] CapTipper v0.1 – Malicious HTTP Traffic Explorer Tool

CapTipper is a python tool to analyze, explore and revive HTTP malicious traffic. CapTipper sets up a web server that acts exactly as the server in the PCAP file, and contains internal tools, with a powerful interactive console, for analysis and inspection of the hosts, objects and conversations found.

http://www.toolswatch.org/?p=132058

[New Tool] Forpix v1.02 – Forensic Images Tool Released

Forpix is a forensic program for identifying similar images that are no longer identical due to image manipulation.

http://www.toolswatch.org/?p=132055

PEStudio v8.46 Released

PEStudio is a unique tool that performs the static investigation of 32-bit and 64-bit executable. PEStudio is free for private non-commercial use only.

http://www.toolswatch.org/?p=132052

WPScan v2.6 Released

WPScan is a black box WordPress vulnerability scanner.

http://www.toolswatch.org/?p=132038

Wireshark v1.12.3 Released

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

http://www.toolswatch.org/?p=132011

SPARTA Beta Network Infrastructure Pen Test Tool Released

SPARTA is a python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase.

http://www.toolswatch.org/?p=132007

SeeS v4.1 Social Enginnering Email Sender Released

SeeS is a Social Engineering Attack/Audit Tool for Spear Phishing. Most of the companies nowadays have their firewalls, threat monitoring and prevention security appliances setup. With these mechanisms in place, security precautions are taken and incidents are monitored. Inbound traffic being restricted, SEES on the other hand is developed for sending targeted phishing emails in order to carry sophisticated social engineering attacks/audits.

http://www.toolswatch.org/?p=132002

oclHashcat v1.31 Released

oclHashcat is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.

http://www.toolswatch.org/?p=131996

[New Tool] Babel Scripting Framework (babel-sf) v0.1 Released

The Babel Scripting Framework (babel-sf) is a collection of custom scripts to facilitate useful pentest related functions via scripting languages.

http://www.toolswatch.org/?p=131987

[New Tool] Crowbar v1.0 Brute Forcing Tool Released

Crowbar (crowbar) is brute forcing tool that can be used during penetration tests. It is developed to brute force some protocols in a different manner according to other popular brute forcing tools.

http://www.toolswatch.org/?p=131982

[New Tool] pwntools v2.2.0 CTF Framework and Exploit Dev Library

pwntools is a CTF framework and exploit development library. Written in Python, it is designed for rapid prototyping and development, and intended to make exploit writing as simple as possible. This is the CTF framework used by Gallopsled in every CTF.

http://www.toolswatch.org/?p=131980

[New Tool] AIEngine v0.8 (Artificial Inteligent Engine)

AIEngine is a next generation interactive/programmable packet inspection engine with capabilities of learning without any human intervention, NIDS functionality, DNS domain classification, network collector and many others.

http://www.toolswatch.org/?p=131976

[New Tool] NexusTaco v1.0 SNMP Scanner Cisco Nexus Switches

NexusTaco is a snmp scanner that can be used both for internal testing and external testing to assess Cisco Nexus switches (all models). This tool uses the Cisco NX-OS Software SNMP Information Disclosure Vulnerability (CVE-2014-3341).

http://www.toolswatch.org/?p=131974

Do you have or know tools to be published?
Don't hesitate and contact us, send it!
http://www.toolswatch.org/submit-a-tool/

IDASynergy: Tool for collaborative reversing with IDA Pro

(By Cubica Labs)

Were you ever in the situation of reversing a binary as a team and needed to share information? Then IDASynergy is for you!

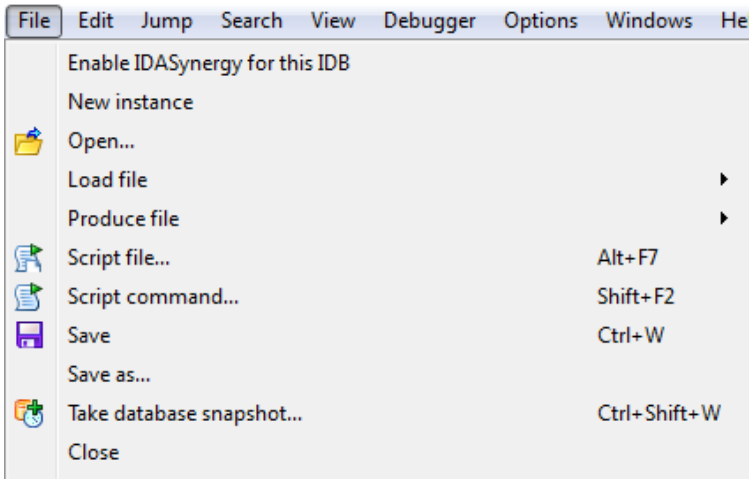
With previous efforts for collaborative reversing, you are required to setup a special centralized server or require all parties to be connected simultaneously. IDASynergy philosophy is to rely on current and well-established software change management tools like svn, git, mercurial, etc. This way you don't need to host a special service and can use tools you are already familiar with, that even allow you to work offline.

How it works?

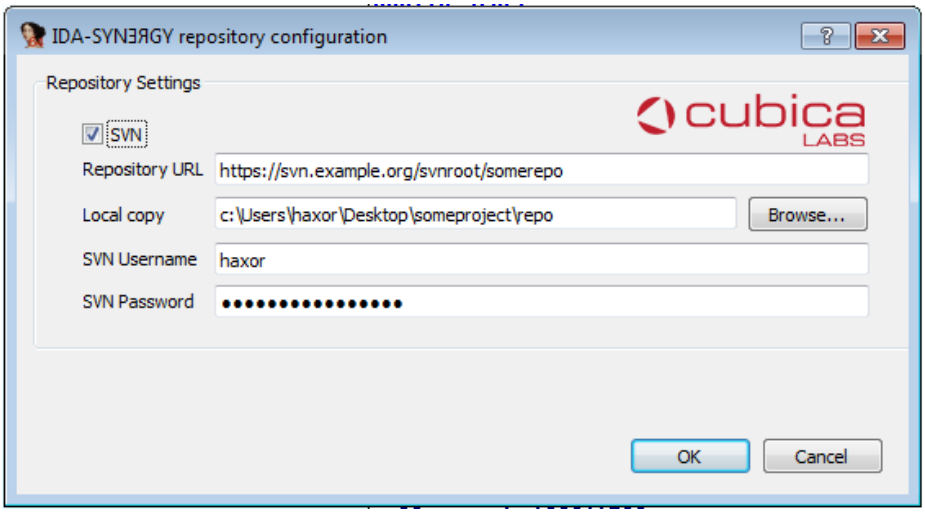
IDASynergy obtains information about the modifications you perform by a series of hooks. While you perform actions like adding comment, renaming functions, changing segments, defining structs or defining marks the changes are collected. When you are ready to share your changes this information enriched by the export of the IDB file to idc, serialized as JSON and stored as local files in what is called your local repository. You can manually commit this files to any revision control system you want, or take advantage of IDASynergy integrated commit, update and merge functions if you are using SVN.

IDASynergy in action:

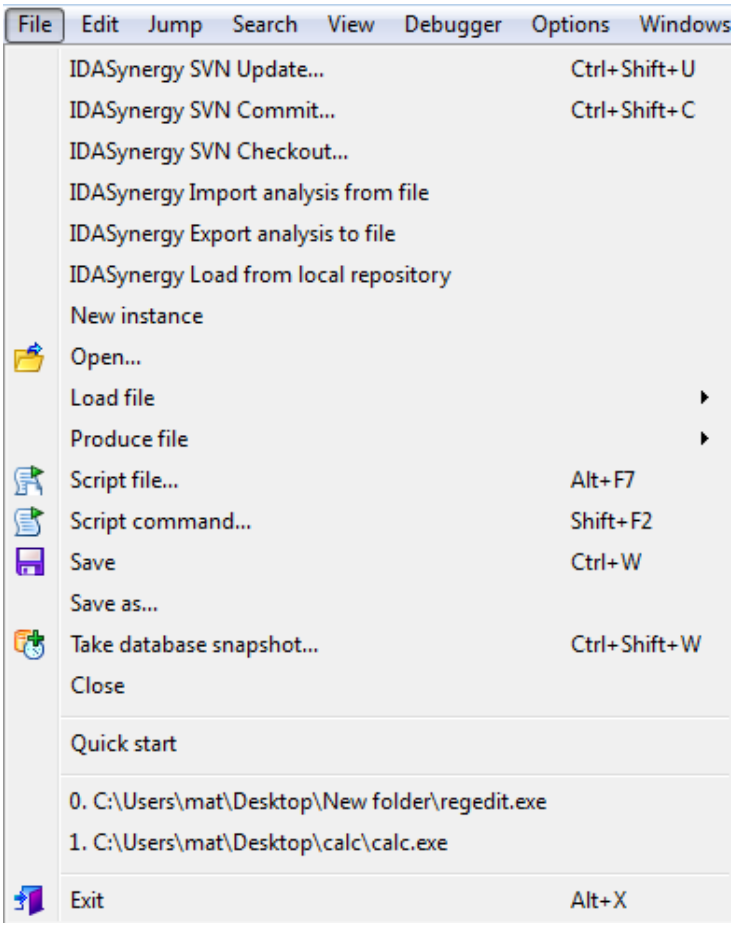
After installing the plugin simply by copying to the IDA application data folder. When you load a binary or an existing IDB to IDA Pro, you will find a new option under the file menu.



Once you enable IDASynergy for this IDB, you will be greeted by the configuration dialog where you can setup an SVN repository or just specify the local repository path if you are not using SVN.

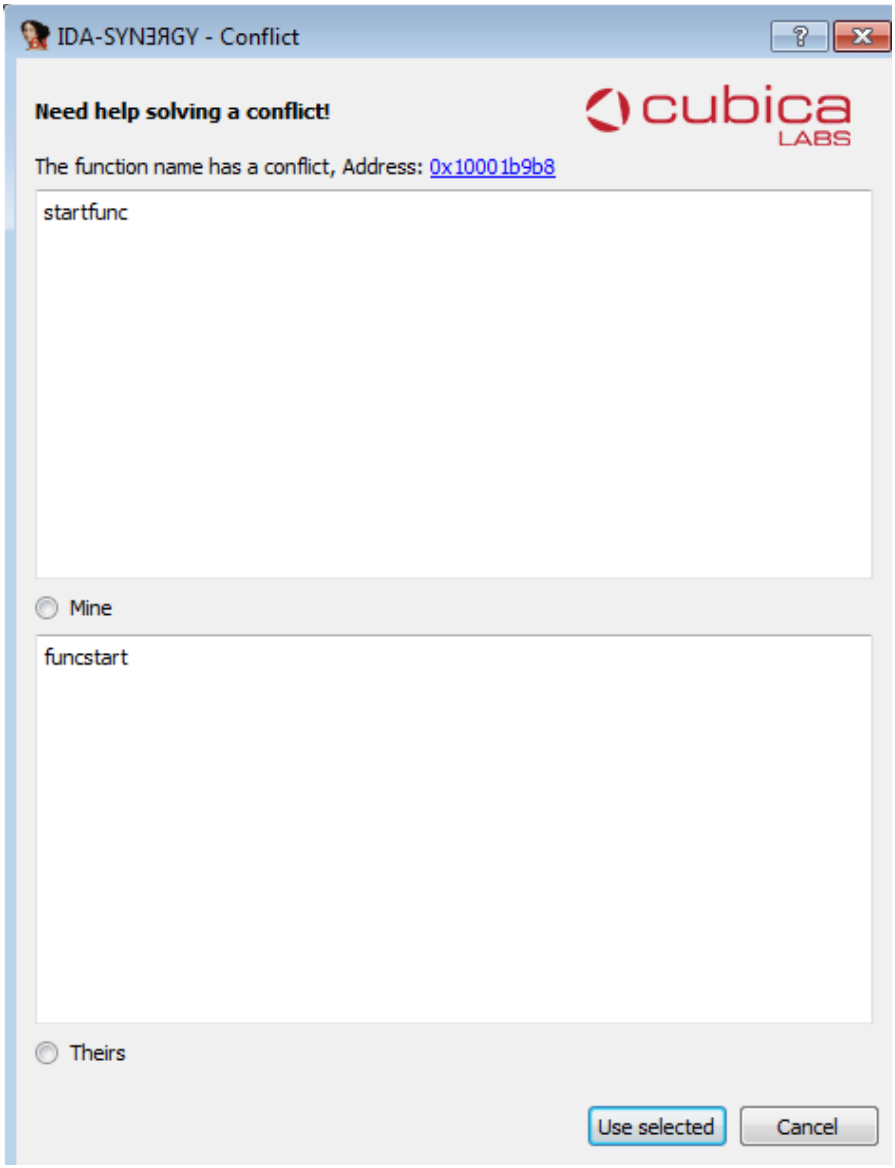


Once you finished configuring IDASynergy. You can start your work as you would normally: Identify code, add comments, rename functions, etc. When you are ready to share your changes you can use the integrated commit functions on the file menu (SVN only) or the convenient associated shortcuts, to commit, update and checkout your projects accordingly.



In the unlikely event of a conflict, which can happen if you and someone else on your team modified the same name, a comment on the same line, etc. IDASynergy will provide the

following dialog allowing you to decide how to resolve the conflict. This what the conflict resolution dialog looks like:



As you can see, in this case the conflict was created when one researcher name a function funcstart and the other startfunc, apparently this two researchers don't have a naming convention.

Installation:
You can get IDASynergy from https://github.com/CubicaLabs/IDASynergy You'll need the dependencies pysvn and pyside for IDA, see the project's github readme file for details. Once that's taken care of, simply copy the contents of the source tree to %APPDATA%\Hex-Rays\IDA Pro\ then launch IDA as usual and you are good to go!

We'd love to hear any comments, ideas, bug reports and even insults please reach out to idasynergy@cubicalabs.com

Papers

2014 Top Security Tools as Voted by ToolsWatch.org Readers

We are honored to announce the **2014 Top Security Tools as Voted by ToolsWatch.org Readers**, this is the second edition of our online voting by users and readers.

Results 2014

01 - Unhide (NEW)
02 - OWASP ZAP - Zed Attack Proxy Project (-1↓)
03 - Lynis (+3↑)
04 - BeEF - The Browser Exploitation Framework (-2↓)
05 - OWASP Xenotix XSS Exploit Framework (0→)
06 - PeStudio (-2↓)
07 - OWASP Offensive (Web) Testing Framework (NEW)
08 - Brakeman (NEW)
09 - WPScan (0→)
10 - Nmap (NEW)

 http://www.toolswatch.org/?p=132031