
Newsletter - August 2014

ToolsWatch Team
NJ OUCHN & MJ SOLER

# Tools! Lots of Tools Released!

**During August 2014, we published 19 Posts with 9 News Tools.**

## Organized by Date

- [New Tool] HoneyDrive v3 Royal Jelly – Honeypot Linux Distro Released
- [New Tool] WPHardening v1.3 Released
- **BHUSA Arsenal 2014:** Viproy – VoIP Penetration Testing Kit v2.0 Released
- Suricata v2.0.3 Released
- Lynis v1.5.9 Released
- Mobius Forensic Toolkit v0.5.20 Released
- [New Tool] OWASP WebSpa Project v0.7 – Java Web Knocking Tool Released
- [New Tool] OWASP RainbowMaker v1.2 Released
- [New Tool] iOS Reverse Engineering Toolkit (iRET) v1.0 Released
- [New Tool] XSSYA (XSS Scanner & Vuln Confirmation) Beta Released
- Backdoor Factory Proxy (BDFProxy) v0.1 Released
- Volatility v2.4 – Art of Memory Forensics Released
- [New Tool] Haka v0.2 Protocols and Policies Analyzer Released
- Netsparker Web Application Security Scanner v3.5.5 Released
- SAMHAIN v3.1.2 Released
- XCat v0.7 Released
- Shellter v1.7 A Dynamic ShellCode Injector – Released
- [New Tool] American Fuzzy Lop v0.26b Released
- [New Tool] BackdoorFactory v2.2.1 Released

# Black Hat Arsenal USA 2014 - Wrap up Day 1


http://www.toolswatch.org/?p=108766

# Developer Corner

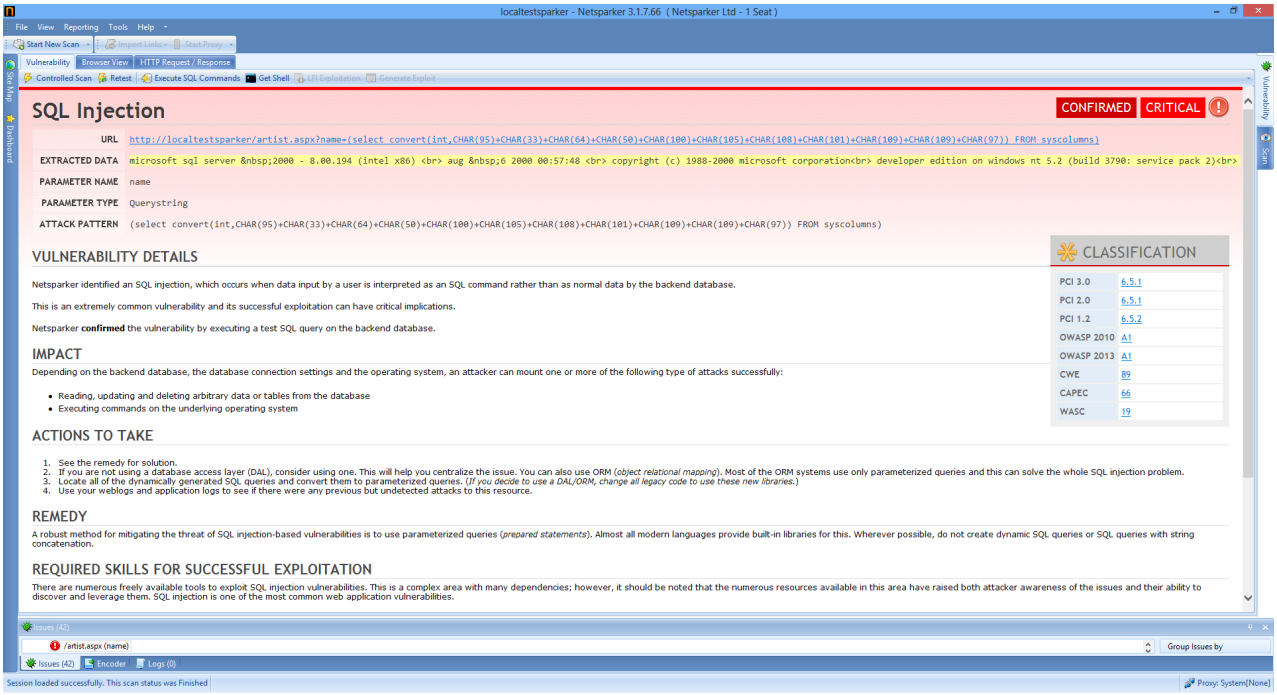
This is a **new section** where some developers have the possibility to tell us about their tools.
Do you want to participate? maxisoler *noSPAM* toolswatch dot org

# 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](http://www.netsparker.com)

# Tools! Lots of Tools Released!

## [New Tool] BackdoorFactory v2.2.1 Released

Patch win86/64 PE and linux86/64 binaries with shellcode. The goal of The Backdoor Factory is to patch executable binaries with user desired shellcode and continue normal execution of the binary  prepatched state. Under a BSD 3 Clause License.

http://www.toolswatch.org/?p=107692

## [New Tool] American Fuzzy Lop v0.26b Released

American Fuzzy Lop uses a novel type of compile-time instrumentation to automatically discover clean, interesting test cases and substantially improve the functional coverage for the tested code.

http://www.toolswatch.org/?p=107936

## Shellter v1.7 A Dynamic ShellCode Injector – Released

Shellter is a dynamic shellcode injection tool aka dynamic PE infector. It can  be used in order to inject shellcode into native Windows applications (currently 32-bit apps only). The shellcode can be something yours or something generated through a framework, such as Metasploit.

http://www.toolswatch.org/?p=107985

## XCat v0.7 Released

XCat is a command line program that aides in the exploitation of blind XPath injection vulnerabilities. It can be used to retrieve the whole XML document being processed by a vulnerable XPath query, read arbitrary files on the hosts filesystem and utilize out of bound HTTP requests to make the server send data directly to xcat.

http://www.toolswatch.org/?p=107987

## SAMHAIN v3.1.2 Released

The Samhain host-based intrusion detection system (HIDS) provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.

http://www.toolswatch.org/?p=1086186

## Netsparker Web Application Security Scanner v3.5.5 Released

Netsparker can crawl, attack and identify vulnerabilities in all custom web applications regardless of the platform and the technology they are built on, just like an actual attacker.

It can identify web application vulnerabilities like SQL Injection, Cross-site Scripting (XSS), Remote Code Execution and many more. It has exploitation built on it, for example you can get a reverse shell out of an identified SQL Injection or extract data via running custom SQL queries.

http://www.toolswatch.org/?p=108626

## [New Tool] Haka v0.2 Protocols and Policies Analyzer Released

Haka is an open source security oriented language which allows to describe protocols and apply security policies on (live) captured traffic. Licensed under Mozilla Public License v2.0

http://www.toolswatch.org/?p=108710

## Volatility v2.4 - Art of Memory Forensics Released

The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples.

http://www.toolswatch.org/?p=108713

## Backdoor Factory Proxy (BDFProxy) v0.1 Released

This script rides on two libraries for usage: The Backdoor Factory (BDF) and the mitmProxy.

http://www.toolswatch.org/?p=108717

## [New Tool] XSSYA (XSS Scanner & Vuln Confirmation) Beta Released

XSSYA Cross Site Scripting Scanner & Vulnerability Confirmation wrote in python work by execute the payload encoded to bypass Web Application Firewall which is the first method request and response if it respond 200 it turn to Method 2 which search that payload decoded in web page HTML code if it confirmed get the last step which is execute document.cookie to get the cookie.

http://www.toolswatch.org/?p=108719

## [New Tool] iOS Reverse Engineering Toolkit (iRET) v1.0 Released

The iOS Reverse Engineering Toolkit is a toolkit designed to automate many of the common tasks associated with iOS penetration testing.

http://www.toolswatch.org/?p=108722

## [New Tool] OWASP RainbowMaker v1.2 Released

OWASP Rainbow Maker is a tool aimed to break hash signatures. It allows testers to insert a hash value and possible keywords and values that might used by the application to create it, then it tried multiple combinations to find the format used to generate the hash value.

http://www.toolswatch.org/?p=108946

## [New Tool] OWASP WebSpa Project v0.7 - Java Web Knocking Tool

The OWASP WebSpa Project is a Java web knocking tool for sending a single HTTP/S request to your web server in order to authorize the execution of a premeditated Operating System (O/S) command. It provides a cryptographically protected "open sesame" mechanism on the web application layer, comparable to well-known port-knocking techniques. It is licensed under the Creative Commons Attribution-ShareAlike 3.0.

http://www.toolswatch.org/?p=108949

## Mobius Forensic Toolkit v0.5.20 Released

Mobius Forensic Toolkit is a forensic framework written in Python/GTK that manages cases and case items, providing an abstract interface for developing extensions. Cases and item categories are defined using XML files for easy integration with other tool.

http://www.toolswatch.org/?p=108951

## Lynis v1.5.9 Released

Lynis is an auditing tool which tests and gathers (security) information from Unix based systems. The audience for this tool are security and system auditors, network specialists and system maintainers.

http://www.toolswatch.org/?p=108954

## Suricata v2.0.3 Released

The Suricata Engine is an Open Source Next Generation Intrusion Detection and Prevention Engine. This engine is not intended to just replace or emulate the existing tools in the industry, but will bring new ideas and technologies to the field. The Suricata Engine and the HTP Library are available to use under the GPLv2.

http://www.toolswatch.org/?p=109066

# BHUSA Arsenal 2014

## Viproy - VoIP Penetration Testing Kit v2.0 Released

Viproy Voip Pen-Test Kit provides penetration testing modules for VoIP networks. It supports signalling analysis for SIP and Skinny protocols, IP phone services and network infrastructure.

Viproy 2.0 is released at Blackhat Arsenal USA 2014 with TCP/TLS support for SIP, vendor extentions support, Cisco CDP spoofer/sniffer, Cisco Skinny protocol analysers, VOSS exploits and network analysis modules. Furthermore, Viproy provides SIP and Skinny development libraries for custom fuzzing and analyse modules.

http://www.toolswatch.org/?p=109070

## [New Tool] WPHardening v1.3 Released

WPHardening is a security tool for WordPress. Different tools to hardening WordPress.

http://www.toolswatch.org/?p=109153

## [New Tool] HoneyDrive v3 Royal Jelly - Honeypot Linux Distro

HoneyDrive is the premier honeypot Linux distro. It is a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It contains over 10 pre-installed and pre-configured honeypot software packages such as Kippo SSH honeypot, Dionaea and Amun malware honeypots, Honeyd low-interaction honeypot, Glastopf web honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients and more.

http://www.toolswatch.org/?p=109161

## The CSO's Myopia (By Jordan M. Bonagura)

Before reading this article imagine what it would be like to be able to manage your own company without your customer's data or, yet, imagine what it would be like if your competitors had these data…

Well, it is more than established for the market how valuable data is for the companies. Your customers' database and the experience they acquire along the years are fundamental and represent a great competitive advance in this new corporative era.

Having it in mind we can realize the importance of implementing specific policies in order to build a base to guarantee these data are safe.

There has been a recent increase in the incidents related to security issues in a way that IT management has become more and more complex and, automatically the need for a new kind of professional has emerged, the CSO.

The CSO has become the responsible for risk areas, data security and, also for the definition and implementation of the security strategies and policies that the company will implement.

Such policies are developed to reduce risks and impacts and limit exposure to liability in all areas.

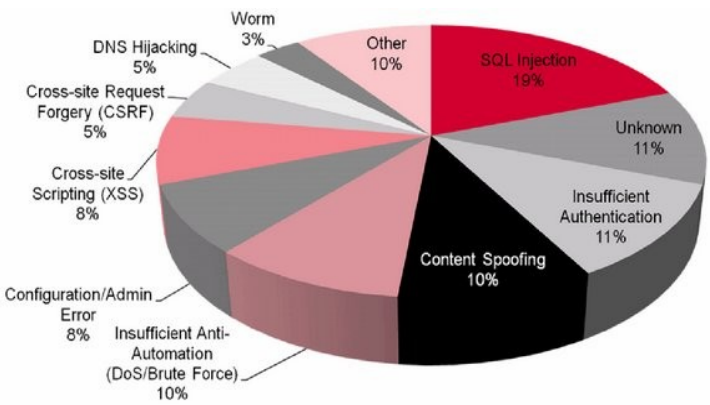
The picture below shows the direct relation between security enhancement and risks reduction, in other words, the higher the security the lower the risks.


However, the major questions it addresses to does not approach the urge for good professionals in security or the development of good policies but, indeed, the constructive process every company must go through when it decides to implement or organize such policies.

The "**in box**" vision, commonly used at the moment of creating these policies, is not, at large, enough to comprise all the company's existing range of vulnerabilities.

When we analyze the graphic published by Breach Security Labs on August, 2009 on "*The Web Hacking Incidents Database 2009*", demonstrating which vulnerabilities were the hackers most favorite during the first semester 2009, we obviously and automatically face a high percentage in a particular breach in the SQL Injection (19%) – an opening for data stealing. I say obviously because, as previously mentioned, data is one of the company's most valuable assets.

### What vulnerabilities do hackers use?




Source: Breach Security Labs

Such analyses are extremely relevant for a CSO, for through them it has become possible to enhance and update the logic control mechanisms (Firewalls, Anti Virus, IDS/IPS and, etc.) and thus, reduce the risks relating to the well-known breaches that are considered by the company's established policies. Furthermore, to be able to take into account new ways to explore these breaches.

One specific risk I would like to quickly approach is that there are people in charge of the administration and that people are subject to flaws. Some might ponder that policies exist for this purpose and, they are to be carried out precisely by their employees, yet, it is worth reinforcing that policies require continuous review as much as physical and logical mechanisms require updating. And, also competent professionals involved in security matters require constant training.

Everything sounds perfect now, doesn't it?

Unfortunately not! Let's refer to the Bible where we find that "the foolish man who built his castle on the sand..."

The major problem is that every security policy is developed under an "**in box**" vision, although, a large range of well-known breaches are available "**out box**". In other words, the ones living the problems are the ones who can't see them.

If the CSO is simply based on his own policy he will not be able to see what it does not comprise, he will be bounded by his pseudo-security. That is what I call **CSO myopia**. To believe with his defined policy he can control the whole thing, when, actually, he is only controlling his whole policy.

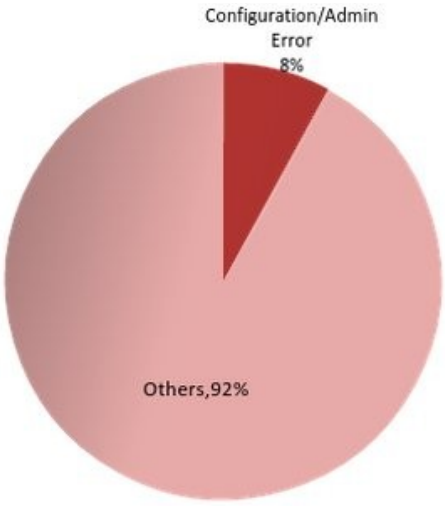
However, once it has been developed on existing breach patterns not privileging new ones, still unknown "in box" ones. Then, it won't completely guarantee his company's security.

But, after all, what do I mean by that?

I mean: "*Sometimes we hide the key under the doormat and forget to lock the door…*"

One of the main problems in this myopia is when we treat, for example, the risks concerning the errors of configuration and administration (Configuration/Admin Error (8%)) as in the graphic below.

**What vulnerabilities do hackers use?**




Source: Adapted from Breach Security Labs

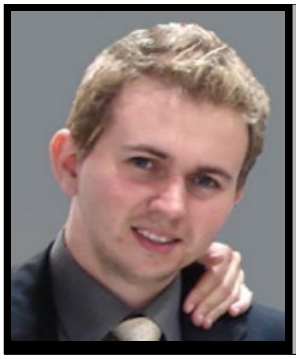
This sort of error besides being considered a breach, may enhance the identification process and consequent exploration of other breaches. A practical example is the directory listing of a web server showing data base configuration files.

Calm down! Not all is lost…

It is often difficult to have the "out box" 100% of the time when you are dedicated

to the “in box” and, mainly on the idea that everything is under control. A very important recommendation, in my opinion, is to resort to specialized consulting professionals (Pentest), who are experts at analyzing breaches which are still not familiar to the company and, the different forms to explore the ones already considered by your present policy.
Attitudes like this might contribute to the decrease in the problems coming from the managerial myopia.

**Keep alert, Keep safe!**



**Jordan M. Bonagura** is a computer scientist, post graduated in Business Strategic Management, Innovation and Teaching (teaching methodology and research). He works as a business consultant and researcher in information security with emphasis on new breaches.

He is lecturer in the area of information technology at various institutions, among them the Brazilian Institute of Advanced Technology (Veris/IBTA).