



Newsletter - July 2014

**ToolsWatch Team**  
NJ OUCHN & MJ SOLER

## Tools! Lots of Tools Released!

During July 2014, we published 13 Posts with 8 News Tools.

### Organized by Date

- [New Tool] SlowHTTPTest v1.6 – DoS Attacks Released
- [New Tool] Spotlight Inspector v1.1.46 – Metadata OSX Released
- Lynis v1.5.8 Released
- Binwalk v2.0.0 Released
- [New Tool] Praeda v0.02.2.103 Beta Released
- Syhunt Sandcat Browser v5.0 Beta 1 Released
- Lynis v1.5.7 Released
- Netsparker Web Application Security Scanner v3.5 Released
- [New Tool] Email Grab v0.3.5 Released
- [New Tool] OSUETA v0.8 OpenSSH User Enumeration Timing Attack Released
- [New Tool] iAppliScan v0.02 Beta Released
- [New Tool] FSDroid v0.02 Beta Released
- [New Tool] El Jefe v2.1 – Windows Process Monitoring Released

## Black Hat USA 2014: Arsenal Tools



Soon we will publish the information about the tools released. :) Stay tuned!



<http://www.toolswatch.org/?p=45832>

## 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.

The screenshot shows the Netsparker interface with a detected SQL Injection vulnerability. The main content area displays the following details:

- URL:** `http://localhostsparker/artist.aspx?name=(select_convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(108)+CHAR(105)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns)`
- EXTRACTED DATA:** `microsoft sql server &nbsp;2000 - 8.00.194 (intel x86) <br> aug &nbsp;6 2000 00:57:48 <br> copyright (c) 1988-2000 microsoft corporation<br> developer edition on windows nt 5.2 (build 3790: service pack 2)<br>`
- PARAMETER NAME:** name
- PARAMETER TYPE:** Querystring
- ATTACK PATTERN:** `(select_convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(108)+CHAR(105)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns)`

**VULNERABILITY DETAILS**

Netsparker identified an SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database. This is an extremely common vulnerability and its successful exploitation can have critical implications. Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database.

**IMPACT**

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

**ACTIONS TO TAKE**

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (object relational mapping). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (If you decide to use a DAL/ORM, change all legacy code to use these new libraries.)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

**REMEDY**

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (prepared statements). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

**REQUIRED SKILLS FOR SUCCESSFUL EXPLOITATION**

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

**CLASSIFICATION**

PCI 3.0	6.5.1
PCI 2.0	6.5.1
PCI 1.2	6.5.2
OWASP 2010	A1
OWASP 2013	A1
CWE	89
CAPEC	66
WASC	19

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] SlowHTTPTest v1.6 – DoS Attacks Released

SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks. It works on majority of Linux platforms, OSX and Cygwin - a Unix-like environment and command-line interface for Microsoft Windows.



<http://www.toolswatch.org/?p=107655>

## [New Tool] Spotlight Inspector v1.1.46 – Metadata OSX Released

Spotlight is name of Apple OSX's desktop search functionality. It indexes all the files on a volume storing (among other things) metadata about filesystem objects (e.g. file, directory) in an effort to provide fast and extensive file searching capabilities.



<http://www.toolswatch.org/?p=107652>

## Lynis v1.5.8 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=107650>

## Binwalk v2.0.0 Released

Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. Binwalk uses the libmagic library, so it is compatible with magic signatures created for the Unix file utility.



<http://www.toolswatch.org/?p=107632>

## **[New Tool] Praeda v0.02.2.103 Beta Released**

Praeda - Latin for "plunder, spoils of war, booty". Praeda is an automated data/information harvesting tool designed to gather critical information from various embedded devices.



<http://www.toolswatch.org/?p=107486>

## **Syhunt Sandcat Browser v5.0 Beta 1 Released**

Sandcat is a lightweight multi-tabbed web browser that combines the speed and power of Chromium and Lua. Sandcat comes with built-in live headers, an extensible user interface and command line console, resource viewer, and many other features that are useful for web developers and pen-testers.



<http://www.toolswatch.org/?p=107483>

## **Lynis v1.5.7 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=107380>

## **Netsparker Web Application Security Scanner v3.5 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.



<http://www.toolswatch.org/?p=107368>

## **[New Tool] Email Grab v0.3.5 Released**

Email Grab is a software project for Intelligence and Information Gathering. The aim is to look for valid email address of a company looking in the websites owned by it, on google, on pgp/gpg servers, whois and other resources.



<http://www.toolswatch.org/?p=102579>

## **[New Tool] OSUETA v0.8 OpenSSH User Enumeration Timing Attack**

OSUETA stands for OpenSSH User Enumeration Timing Attack and is a small script written in Python to exploit a bug present in versions 5.\* and 6.\* of OpenSSH. In these versions during the authentication process, you may obtain a list of users in the system discriminated by the time it takes the system to evaluate an arbitrarily long password.



<http://www.toolswatch.org/?p=102277>

## **[New Tool] iAppliScan v0.02 Beta Released**

iAppliScan lets you automate the review of the iOS application with passing few parameters. It gives pointers to possible vulnerabilities or weakness of the application.



<http://www.toolswatch.org/?p=45894>

## **[New Tool] FSDroid v0.02 Beta Released**

FSDroid is an automated program to penetrate and analyze local storage of the most widely used mobile platform - Android.



<http://www.toolswatch.org/?p=45890>

## **[New Tool] El Jefe v2.1 – Windows Process Monitoring Released**

El Jefe (pronounced 'ell-HEFF-ay') is a Windows based process monitoring solution. El Jefe produces a unique view into how processes are created, what privileges they possess and what child processes they spawn. All of this information is stored, and categorized into a central logging server, which allows a user to quickly see any suspicious behavior that could indicate compromise or malware proliferation.



<http://www.toolswatch.org/?p=45882>



**Do you have or know tools to be published?**

**Don't hesitate and contact us, send it!**

**<http://www.toolswatch.org/submit-a-tool/>**

## **vFeed**

**The Open Source Cross-linked Local Vulnerability Database**

- Security Standards: CVE, CWE, CPE, OVAL, CAPEC, CVSS, and more!
- Vulnerability Assessment & Exploitation IDs.
- Vendors Security Alerts.

**<https://github.com/toolswatch/vFeed>**