Newsletter - September 2014

ToolsWatch Team
NJ OUCHN & MJ SOLER

Tools! Lots of Tools Released!

During September 2014, we published 7 Posts with 2 News Tools.

Organized by Date

- OWASP Xenotix XSS Exploit Framework v6 Released
- Lynis v1.6.2 Released
- [New Tool] Hakabana v0.2.1 – Visualization Tool Released
- Lynis v1.6.0 Released
- Nmap v6.47 Released
- Arachni v1.0 – Web User Interface v0.5 Released
- [New Tool] dirs3arch v0.2.5 – Brute Force Directories and Files

Black Hat Arsenal USA 2014 - Wrap up Day 2

http://www.toolswatch.org/?p=109219

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

Articles:

- OWASP Xenotix XSS Exploit Framework v6 (By ***Ajin Abraham***)
- MKBRUTUS: Password bruteforcer for Mikrotik devices or boxes running RouterOS (By ***Ramiro J. Caire*** & ***Federico Massa***)

Papers

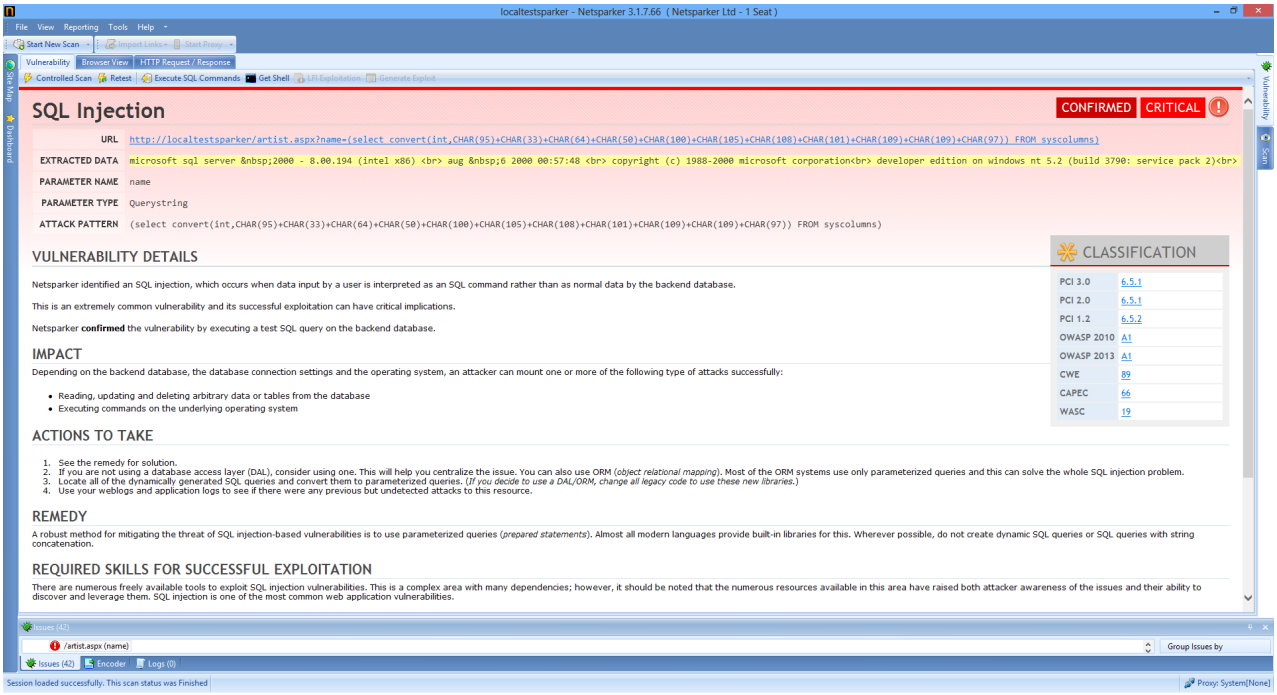
- (IN)Secure Magazine issue 43 (September 2014) available

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!

OWASP Xenotix XSS Exploit Framework v6 Released

OWASP Xenotix XSS Exploit Framework is an advanced Cross Site Scripting (XSS) vulnerability detection and exploitation framework. It provides Zero False Positive scan results with its unique Triple Browser Engine (Trident, WebKit, and Gecko) embedded scanner.

http://www.toolswatch.org/?p=123979

Lynis v1.6.2 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=123976

[New Tool] Hakabana v0.2.1 - Visualization Tool Released

Visualize Haka traffic in real-time using Kibana and Elasticsearch. Haka is an open source security oriented language which allows to describe protocols and apply security policies on (live) captured traffic.

http://www.toolswatch.org/?p=123939

Lynis v1.6.0 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=109438

Nmap v6.47 Released

Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for network

inventory, managing service upgrade schedules, monitoring host or service uptime, and many other tasks.

http://www.toolswatch.org/?p=109433

Arachni v1.0 – Web User Interface v0.5 Released

Arachni is a feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications.

http://www.toolswatch.org/?p=109409

[New Tool] dirs3arch v0.2.5 – Brute Force Directories and Files

dirs3arch is a simple command line tool designed to brute force directories and files in websites. Licensed under GNU General Public License, version 2.

http://www.toolswatch.org/?p=109353

OWASP Xenotix XSS Exploit Framework v6 (By Ajin Abraham)

OWASP Xenotix XSS Exploit Framework is an advanced Cross Site Scripting (XSS) vulnerability detection and exploitation framework.

It provides Zero False Positive scan results with its unique Triple Browser Engine (Trident, WebKit, and Gecko) embedded scanner. It is claimed to have the world's 2nd largest XSS Payloads of about 4700+ distinctive XSS Payloads for effective XSS vulnerability detection and WAF Bypass.

Xenotix provides Zero False Positive XSS Detection by performing the Scan within the browser engines where in real world, payloads get reflected. Xenotix Scanner Module is incorporated with 3 intelligent fuzzers to reduce the scan time and produce better results. If you really don't like the tool logic, then leverage the power of Xenotix API to make the tool work like you wanted it to be.

OWASP Xenotix is built with powerful offensive modules for performing Information Gathering and Exploitation. Say no to alert pop-ups in PoC. Pen testers can now create appealing Proof of Concepts within a few clicks.

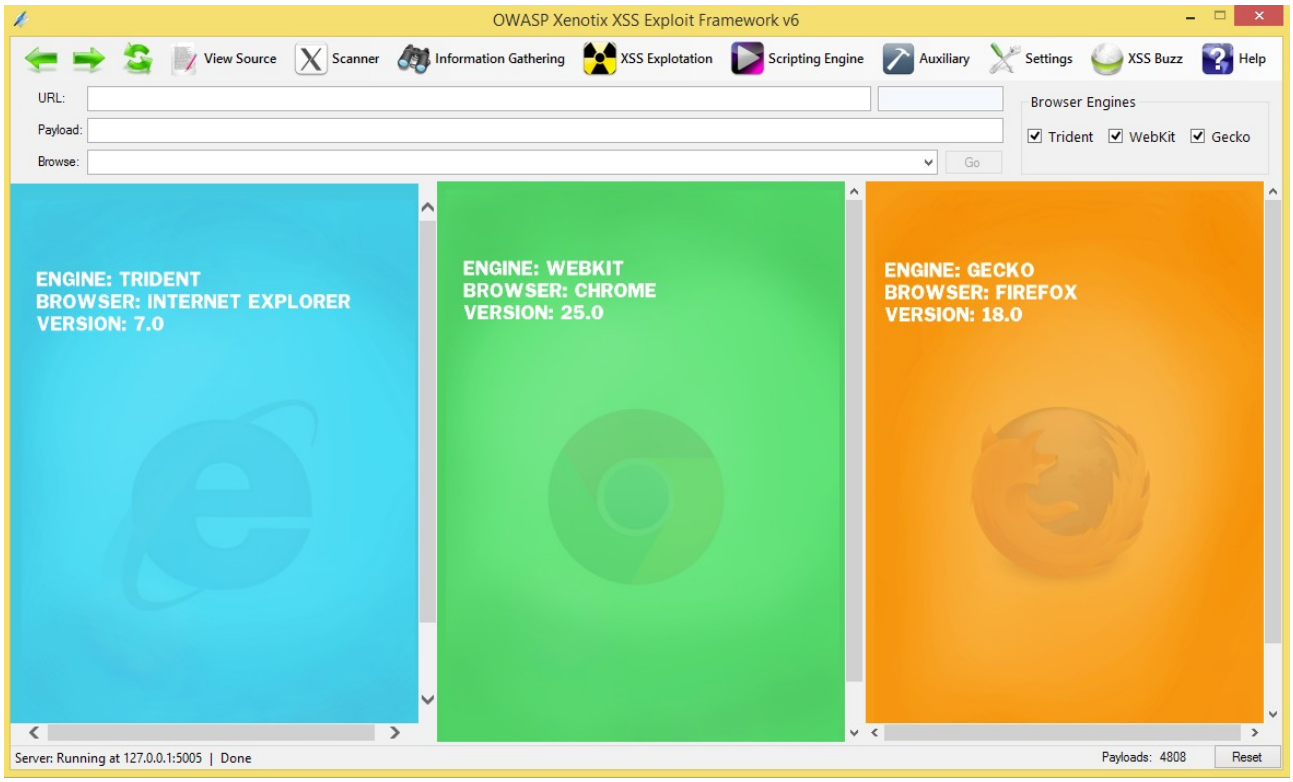
Xenotix offers a couple of XSS Information Gathering & Exploitation Modules that work Cross Platform and with the latest Browsers.

V6 Changes

- Intelli Fuzzer
- Context Based Fuzzer
- Blind Fuzzer
- HTA Network Configuration
- HTA Drive-By
- HTA Drive-By Reverse Shell
- JSFuck 6 Char Encoder
- jjencode Encoder
- aaencode Encoder
- IP to Location
- IP to GeoLocation
- IP Hinting
- Download Spoofer
- HTML5 Geolocation API
- Reverse TCP Shell Addon (Linux)
- OAuth 1.0a Request Scanner
- 4800+ Payloads
- SSL Error Fixed

More Information:

[OWASP Xenotix XSS Exploit Framework]



Ajin Abraham An Information Security Enthusiast interested in learning new things everyday. Areas of interest includes Security Research, Fuzzing and Reversing anything of Interest, Actively Develops Hacker's Arsenal, Graphics & Web Design.

Contributes to Free and Open Information Security Eduction via OpenSecurity.

MKBRUTUS: Password bruteforcer for Mikrotik devices or boxes running RouterOS (By Ramiro J. Caire & Federico Massa)

Motivation & Scenario

Mikrotik brand devices (www.mikrotik.com), which runs the RouterOS operative system, are worldwide known and popular with a high networking market penetration. Many companies choose them as they are a great combination of low-cost and good performance. RouterOS can be also installed on other devices such as PC.

This system can be managed through the following ways: Telnet, SSH, HTTP, Winbox (proprietary GUI of Mikrotik) and Mikrotik API. Both, Winbox and API ports, uses a RouterOS proprietary protocol to "talk" with management clients.

Many network sysadmins choose to close Telnet, SSH and HTTP ports, leaving the Winbox port open for graphical management or to use it with another client (developed by third parties) which use the RouterOS API port, such as applications for Android or web front-ends. At this point, MKBRUTUS comes into play ;)

MKBRUTUS In Action

MKBRUTUS is a Password bruteforcer for MikroTik devices or boxes running RouterOS. MKBRUTUS is a tool developed in Python that performs bruteforce attacks (dictionary-based) against RouterOS systems (ver. 3.x or newer) which have the 8728/TCP port open. Currently has all the basic features of a tool to make **dictionary-based attacks**, but in the future we plan to incorporate other options.

Fig. 1 - MKBRUTUS options.

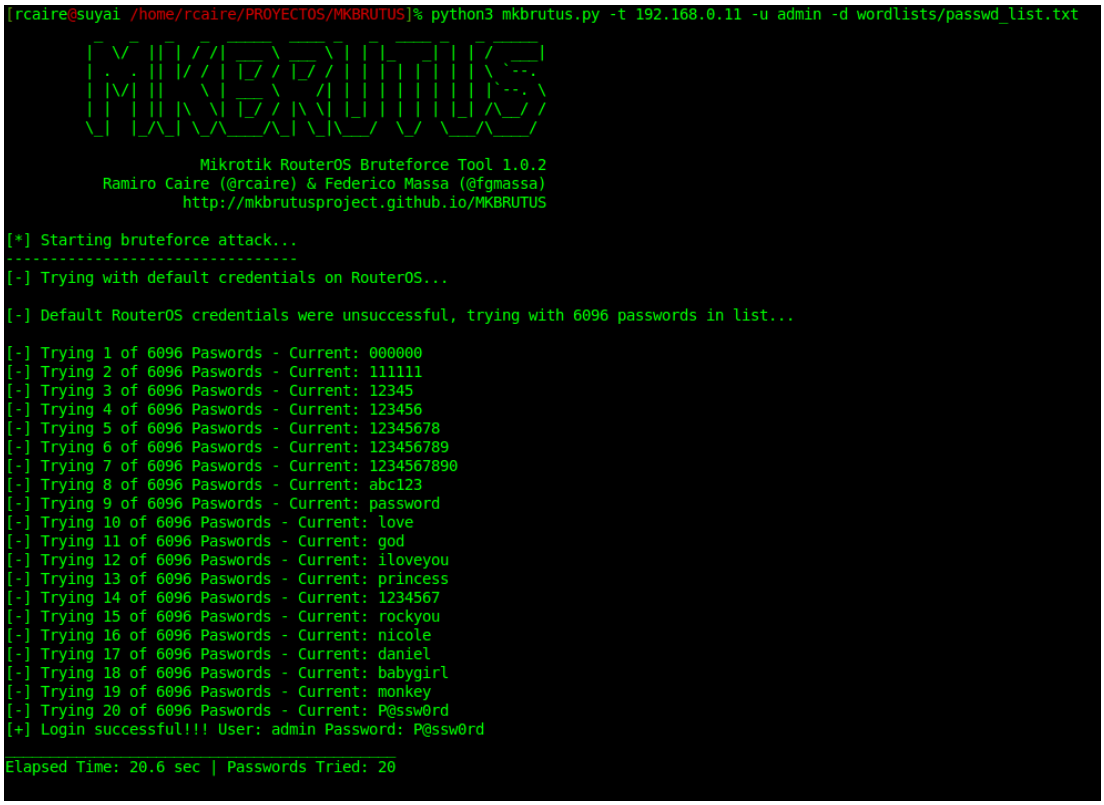


Fig. 2 - MKBRUTUS performing an attack!

Installation

The project is available here in GitHub, and you can install the tool just by typing:

```
# git clone https://github.com/mkbrutusproject/MKBRUTUS.git
```

It is necessary to have Python 3.x installed in order to run this tool. It was successfully tested in KALI LINUX, previous Python3 installation (apt-get install python3).

More Information:

http://mkbrutusproject.github.io/MKBRUTUS/

Ramiro J. Caire is an Pentester and Ethical Hacking consultant. Trainer & speaker. Member of HoneynetAR Project. Author of MKBRUTUS and several infosec papers.

Areas of interest includes Hacking, malware research, OSINT, Cybercrime and new technologies.

Federico Massa is an independent Security consultant specialized in Ethical Hacking. He has been involved in several national and international security projects. He is the developer of the tools VScan (presented at BlackHat 2013) and MKBrutus.

Papers

(IN)Secure Magazine issue 43 (September 2014)

(IN)SECURE Magazine is a freely available digital security magazine discussing some of the hottest information security topics.

http://www.toolswatch.org/?p=110393