

NEW CHECKS

3058 new server checks were added during 2009.

USABILITY ENHANCEMENTS

Ability to generate reports while a scan is in progress.

Ability to remember the last web structure of hosts.

Improved management of target settings. Target settings can now be applied to any port or specific host ports. Now you can also enable or disable target settings with a single click.

PERFORMANCE & STABILITY ENHANCEMENTS

Added a new, intelligent HTML parser. This means that Sandcat is equipped to handle malformed HTML like web browsers.

Refactored code for multithreaded requests. Significantly lower CPU usage when scanning with multi-thread enabled.

Improved memory management. Sandcat has been optimized to use less memory, specially when run over an extended period of time.

More. Faster and more robust report generation. New faster fault injection database format. Faster session data refreshing. Improved packetforming routines.

WHAT'S NEW IN SANDCAT

Recently we implemented a large number of features in [Sandcat Pro](#) and revolutionized the way you conduct web application security assessment. This document briefly covers the most important changes made to Sandcat since version 3.6.

New Features:



Significantly Enhanced User Interface - Monitor closely the progress of your scan. Easily manage sessions using the new Session Manager add-on. Quickly access features using the new toolbars. Receive aid from Sandcat's advanced content analyzers during the manual review of scanned hosts. Insert quick notes everywhere and get them automatically in your report.



Modern Browser Emulation - Simulate web-based attacks while automatically executing JavaScript and interacting with web pages. Customize Sandcat's extensive browser emulation feature set. Review the cached snapshot of the fetched web pages.



Multi-Layer Defense Evasion - Evade common XSS filters. Evade WAFs and IDS systems using techniques that specifically target bugs recently discovered in them.



Multi-Threaded Sessions - Create and manage concurrent sessions using the new Session Launcher tool. Import target lists from files. Schedule scans. Launch Sandcat sessions via command-line.

MODERN BROWSER EMULATION

While spidering a web site and hunting down vulnerabilities, Sandcat emulates a modern, HTML 5-aware web browser. Sandcat's browser emulation feature set includes:

- * Intelligent HTML parsing (handles malformed HTML like a web browser)
- * JavaScript emulation (ability to behave as both Firefox and IE) / AJAX support
- * User interaction simulation (key press, mouse click, etc)
- * HTML 5-aware / CSS 2.1-aware
- * Auto form filling & form login
- * Multi-process (every new web site you scan is a different process on your operating system)
- * Cookies support
- * HTTPS support (SSL 2/SSL 3/TLS 1) / Certificates support
- * Basic & NTLM authentication support
- * HTTP 1.0 and 1.1 support / Keep-Alive support / HTTP redirection support

System Requirements: 1. 128 MB of memory. 2. 100 MB of free disk space. 3. Internet connection (optional for remote scanning or performing automatic updates). 4. Windows XP, 2003, 2008, Vista or 7. It should run on older versions of Windows as well. 5. As a user of a more recent Windows version you may need to be logged in with full administration rights

MULTI-LAYER DEFENSE EVASION

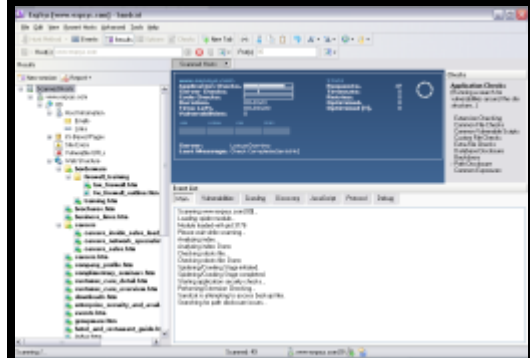
The Multi-Layer Defense Evasion is the ability of Sandcat to combine multiple techniques aimed at a wide array of security mechanisms to perform stealthy tests. Today's Sandcat defense evasion feature set includes:

- * **Anti-XSS Filters evasion** - Bypasses regular expression filters used against XSS.
- * **UTF8-Decode** - Ability to take advantage of UTF8-Decode problems to evade filters when performing injection checks.
- * **Signature-Based Web Honeypot and Application Firewall Detection**
- * **Common IDS evasion techniques (over 10 techniques)**
- * **Multiple WAF and IDS evasion techniques, targeting specifically:**
 - mod_security
 - PHP-IDS

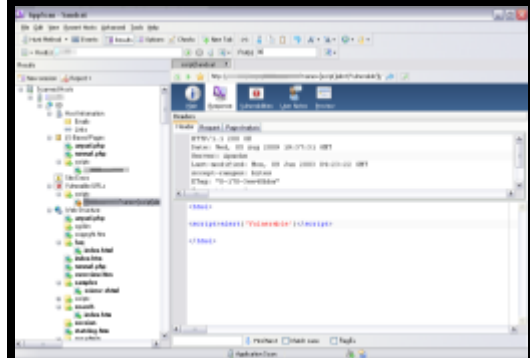
MORE IN WORKS

Thank you to all the kind people and organizations that joined our customer community. We are currently working on new versions of both Sandcat and Sandcat for PHP to make them better than ever for you. We're pleased to have the opportunity to help you automate web application security testing and proactively guard your Web infrastructure against web application security threats.

SANDCAT'S NEW USER INTERFACE



Redesigned Scan Progress screen. Includes a new JavaScript tab to display JS related events



Redesigned URL Info screen.

For more information about Sandcat, visit www.syhunt.com.

