WhiteHat SECURITY

SPOTLIGHT: SENTINEL DYNAMIC

Threat Research Center

An extension of your Application Security Team

WhiteHat Sentinel Dynamic, our dynamic analysis offering, enables your organization to quickly deploy a web application security program. Our unique Software-as-a-Service platform combines automated web application assessment via the Sentinel Scanner with the manual assessment expertise of our Threat Research Center (TRC). Our TRC is an elite team of the industry's top security experts, who are a critical and integral component of the WhiteHat product family.

Sentinel Dynamic performs continuous and concurrent risk assessments, searching for vulnerabilities within web applications, in a production safe environment. The TRC experts verify all vulnerabilities reported by the Sentinel scanner, using customized tests and algorithms, delivering near zero false positives.

Sentinel Scanner

The Sentinel Scanner powers Sentinel Dynamic and is designed for augmentation by the expert configuration, intervention and verification by an expert of the TRC. Sentinel Scanner spiders a web application and performs cutting edge tests. We use benchmarking tools like WAVSEP and Google Firing Range, as well as internal analysis to ensure our scanner can find every possible vulnerability.

Tests

Our testing takes a number of actions and discovers vulnerable behavior rather than specific known issues. These tests are augmented and updated on a daily basis by members of the TRC to detect new attacks when discovered.

Configuration

The Sentinel Scanner is easy to set up with ongoing configuration by a TRC engineer. This configuration includes monitoring, tuning and customization of scans to ensure Sentinel properly tests all forms and provides thorough coverage.

Verification

Our team of experts provides ongoing verification of all vulnerabilities found by the Sentinel Scanner. The TRC engineer confirms the vulnerabilities, adjusts the scores, provides solutions and adds descriptions of the vulnerabilities and remediation advice where applicable.

Business logic assessments

Automated scanners cannot detect business logic flaws in applications as they cannot be programmed to understand the context. To understand the functionality of an application and to find unconventional ways in which a vulnerability can be exploited by a hacker, we need to approach things through the eyes of the hacker to find weaknesses.

WhiteHat Sentinel Dynamic offers special testing to find business logic vulnerabilities through Business Logic Assessments (BLAs). BLAs are focused on finding the kinds of issues that automated scanning is unlikely to find and test sensitive areas of production applications. BLAs involve testing for authentication and authorization issues, process logic flaws, as well as hard to find technical vulnerabilities such and blind XSS and blind SQLi.

The BLAs include an evaluation of user-application interactions such as:

- Account Profile/Account Settings
- Account Transactions/Account History
- Checkout
- Contact Us
- File Upload
- Forgotten username or password
- Authentication/Authorization
- Session Management
- Registration
- Search
- Shopping Cart processes (adding/ removing items, updating the cart)
- Site administration

Business logic vulnerabilities evaluated by TRC include:

- Clickjacking
- Cross-Site Scripting
- Cross-Site Request Forgery
- Embedded Flash and Silverlight modules

Supported Vulnerabilities

Sentinel Dynamic tests for a large number of vulnerabilities* including:

Technical Vulnerabilities - WASC Threat Classification 2.0

- Application Misconfiguration
- Directory Indexing
- HTTP Response Smuggling
- Improper Input Handling
- Insufficient Transport Layer Protection
- OS Commanding
- Remote File Inclusion
- SQL Injection
- XML External Entities
- XQuery Injection
- Content Spoofing
- Fingerprinting
- HTTP Response Splitting
- Improper Output Handling
- Mail Command Injection
- Path Traversal
- Routing Detour
- SSL Injection
- XML Injection
- Cross-Site Scripting
- Format String Attack
- Improper File System Permissions
- Information Leakage
- Null Byte Injection
- Predictable Resource Location
- Server Misconfiguration
- URL Redirector Abuse
- XPath Injection

Technical Vulnerabilities - OWASP Top 10:

- A1 - Injection
- A2 - Broken Authentication and Session Management
- A3 - Cross-Site Scripting
- A4 - Insecure Direct Object References
- A5 - Security Misconfiguration
- A6 - Sensitive Data Exposure
- A7 - Missing Function Level Access Control
- A8 - Cross-Site Request Forgery
- A9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

**A complete list per product line available upon request.*

About WhiteHat Security

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites – including sites in highly regulated industries, such as top e-commerce, financial services, and healthcare companies. For more information on WhiteHat Security, please visit www.whitehatsec.com.

WhiteHat SECURITY

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com