WhiteHat SECURITY

WHITEHAT SCOUT™

WhiteHat Scout™

Fast, Accurate Security in the Developer's Back Pocket

Building 100% defect-free applications is challenging, if not impossible. Developers understand the importance of automated testing. They run unit tests, and they check for functional defects. But even with a top-notch development team, it's possible for some security flaws to sneak by. Development teams have an imperative to develop and release applications quickly, so they need testing solutions that won't slow them down.

WhiteHat Scout, a part of the WhiteHat Application Security Platform, is a fully-automated static application security testing (SAST) product, focused squarely on developers. WhiteHat Scout enables developers to scan their code for security vulnerabilities as a part of their iterative, fast-paced, Agile SDLC processes.

With WhiteHat Scout, developers can:

- **Test applications quickly and easily as they are writing code**
- **Iteratively scan Java apps to support rapid "scan-fix-scan" cycles**
- **Find common, but easily overlooked critical security flaws in the code**
- **Embrace static analysis as a fast and easy process that fits seamlessly in their iterative development cycle**
- **Integrate security into their normal workflows via Maven and APIs**
- **Become better developers by writing secure code, every time**

EASY-TO-USE

Drag and drop code files into the simple web interface to get started or kick off a scan through your IDE

FAST

Grab that cup of coffee while a scan completes in minutes

ACCURATE

Get true positive, highly accurate results backed by WhiteHat's 15 years of experience

SECURE

Data encryption in transit and at rest, and all artifacts deleted upon scan completion

PRIVATE SECURITY FEEDBACK

You run the scans and only you can see the results

GUIDANCE

Get specific remediation guidance for each flaw to easily fix it

Security at the speed of automation, powered by our Attack Vector Intelligence™ Technology

WhiteHat Scout uses Attack Vector Intelligence™ (AVI) technology to deliver the most accurate results required for DevSecOps. AVI is based on Machine Intelligence that combines WhiteHat's patented correlation engine and Threat Research Center's 16 years of data on application vulnerabilities and >100 million verified attack vectors.

CATCH 'EM EARLY

Bring early visibility into the security flaws to the individual developers, as code is being written, leading to a continuous feedback loop

FAST, EASY, ACCURATE

Quickly obtain accurate scan results in minutes to assess common, but easily overlooked, security flaws

SPEED UP TIME-TO-FIX

Fix defects while the developers are still in the middle of the sprint and "in-the-zone" – all the apps, all the time

DESIGNED FOR DEVELOPERS

Improve the quality and security of their code, allowing developers to become "secure coding heroes"

REMEDIATION GUIDANCE IN YOUR SDLC

Bring security advice to the left of the SDLC process – by allowing clear guidance on vulnerabilities while still in binary

SECURITY POWERED BY MACHINE LEARNING

Fully-automated solution based on AVI Technology, a combination of machine intelligence and 16 years of data on verified application vulnerabilities and >100 million attack vectors

SUPPORTED VULNERABILITIES

WhiteHat Scout supports the WhiteHat Top 40 most prevalent vulnerability classes, including the OWASP Top 10. Supported vulnerabilities include:

Cross Site Scripting
Information Leakage: Error Disclosure
Unpatched Library
Application Misconfiguration: Global Error Handling Disabled
SQL Injection
Application Misconfiguration: Debug
Path Traversal
UI Redressing: Clickjacking/Tapjacking
Missing Access Strategy
Cryptography: Insecure Digest
Denial of Service: ReadLine
Injection: HTTP Response Splitting
Insufficient Session Expiration
Insufficient Transport Layer Protection
URL Redirector Abuse
Unvalidated Automatic Library Activation
Information Leakage: Logging
Information Leakage: Session ID
OS Command Injection
Insufficient Authorization: HTTP Verb Tampering
Cryptography: Cipher Transformation Insecure
Information Leakage: SSN
Cryptography: Insecure Cipher
Cryptography: Improper Certificate Validation
Cryptography: Insecure Protocol
Injection: Remote Code Execution
Insufficient Authentication: Basic Authentication Usage
Cryptography: Provider Undefined
Binary Protection: Missing PT_DENY_ATTACH
Insecure Data Storage: Unencrypted SSN
Unsafe Code Usage
Cryptography: Insecure Cipher Mode
LDAP Injection
Directory Indexing
Injection: HTTP Request Splitting
Insufficient Authorization: CORS Policy
Sensitivedata location precision
Denial of Service: ReadFile
Remote File Inclusion
Access Control: File Permissions

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com