Code Sight

Find and fix application security defects as you code

Benefits for Developers

Intuitive workflow

- Fix weak code and vulnerable open source dependencies without having to be a security expert
- Get automatic alerts for issues in every file you open, save, and edit, or manually run rapid scans on demand
- Focus only on your tasks or support full project codebases with local scans and Team View

Better code

- Address issues in source code, open source dependencies, API calls, cryptography, infrastructure-as-code, and more
- Quickly see how to fix issues with clear guidance that helps developers become more risk-aware and security-capable
- Uphold end-to-end security standards with instant access to priority issues from pipeline scans

Increased productivity

- Avoid rework by resolving issues before checking in code
- Keep moving quickly with IDE-optimized rapid scanning
- Reduce the vulnerability backlog for security teams by eliminating issues before downstream tests

Overview

A developer's role may not be strictly tied to security, but through their role they have a direct impact on the security risk posture of their projects and the organization. They need insight into risks as they code, and they need help understanding how to fix an issue that entered the project inadvertently in the first place.

Developers need all this as part of their workflow, without additional steps or tools that may adversely affect productivity.

Code Sight™ IDE Plug-in is an IDE plugin that helps developers uphold higher standards for application security without switching tools or interrupting their day-to-day tasks. Combining static application security testing (SAST) and software composition analysis (SCA), Code Sight delivers real-time alerts and visibility into

- Security weaknesses (CWEs) in your code
- Known vulnerabilities (CVEs) in open source dependencies
- Insecure infrastructure-as-code (IaC) configurations
- Potential secrets/sensitive data leakage risks
- Vulnerable API usage

Designed for rapid DevOps workflows and CI pipelines, Code Sight can analyze large projects and file structures in seconds, with automation controls to scan whole codebases or modified projects. This allows teams to address defects before checking-in code and avoiding the costly rework required when vulnerabilities aren't discovered until downstream testing.

Code Sight complements and improves the effectiveness of other application security testing (AST), alerting development teams to issues detected by other Black Duck® AST tools and associated security policy violations. To help developers quickly fix issues, Code Sight provides detailed remediation guidance directly in the IDE, with recommendations for open source patches, coding best practices, and links to interactive developer security training, powered by Secure Code Warrior.

Benefits for Security

Earlier static analysis

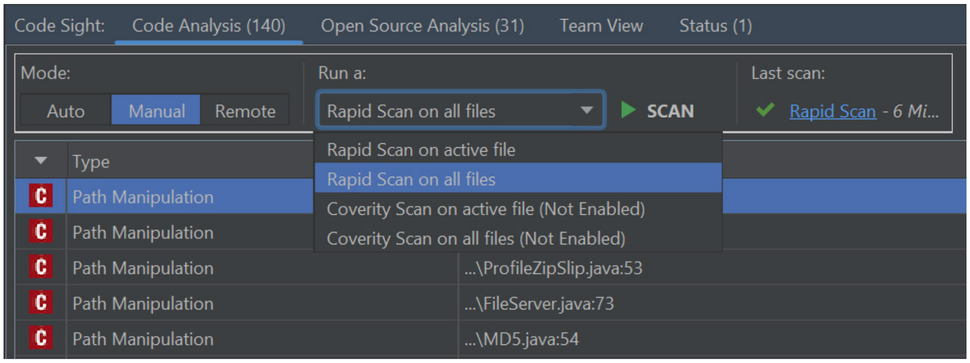
- Analyze source code automatically, as it's written, to detect issues as early as possible
- Give development teams unified insight into project risks across contributors with the Team View tab
- Standardize security skills across developers with clear fix guidance and interactive secure coding training

A smarter supply chain

- Identify known vulnerabilities in direct and transitive open source dependencies as developers introduce them
- Prioritize and assign issues that might be overlooked by developers, detected at later stages, or seen after third-party assets are resolved into the project
- Automatically recommend the next available vulnerability-free or lower-risk version of a component to help developers make smarter, more-secure choices

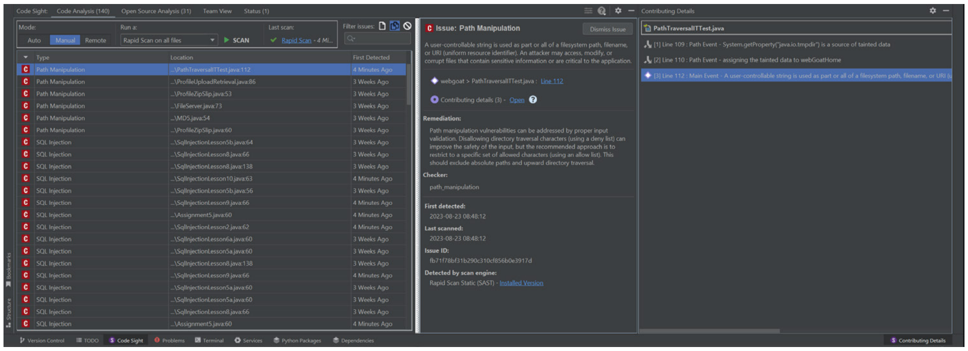
Flexibility for DevSecOps

- Integrate policy violation alerts for connected Coverity® Static Analysis, Black Duck®, Software Risk Manager™, and Black Duck Polaris® Platform servers
- Choose to deploy as a standalone solution for secure development or with connected Black Duck AST solutions



	Type	
C	Path Manipulation	
C	Path Manipulation	
C	Path Manipulation	...\ProfileZipSlip.java:53
C	Path Manipulation	...\FileServer.java:73
C	Path Manipulation	...\MD5.java:54

Flexible source code scanning options to balance speed and depth of analysis



	Type	Location	First Detected
C	Path Manipulation	...\PathTraversalITTest.java:112	4 Minutes Ago
C	Path Manipulation	...\ProfileUploadRetrieval.java:86	3 Weeks Ago
C	Path Manipulation	...\ProfileZipSlip.java:53	3 Weeks Ago
C	Path Manipulation	...\FileServer.java:73	3 Weeks Ago
C	Path Manipulation	...\MD5.java:54	3 Weeks Ago
C	Path Manipulation	...\ProfileZipSlip.java:60	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson5b.java:64	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson8.java:66	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson8.java:138	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson10.java:63	4 Minutes Ago
C	SQL Injection	...\SqlInjectionLesson5b.java:56	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson9.java:66	4 Minutes Ago
C	SQL Injection	...\Assignment5.java:60	4 Minutes Ago
C	SQL Injection	...\SqlInjectionLesson2.java:62	4 Minutes Ago
C	SQL Injection	...\SqlInjectionLesson6a.java:60	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson5a.java:60	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson8.java:138	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson9.java:66	4 Minutes Ago
C	SQL Injection	...\SqlInjectionLesson5a.java:60	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson5a.java:60	3 Weeks Ago
C	SQL Injection	...\SqlInjectionLesson8.java:66	3 Weeks Ago
C	SQL Injection	...\Assignment5.java:60	4 Minutes Ago

Issue: Path Manipulation

A user-controllable string is used as part or all of a filesystem path, filename, or URI (uniform resource identifier). An attacker may access, modify, or corrupt files that contain sensitive information or are critical to the application.

webgoat > PathTraversalITTest.java : Line 112

Contributing details (3) - Open

Remediation:

Path manipulation vulnerabilities can be addressed by proper input validation. Disallowing directory traversal characters (using a deny list) can improve the safety of the input, but the recommended approach is to restrict to a specific set of allowed characters (using an allow list). This should exclude absolute paths and upward directory traversal.

Checker:

path_manipulation

First detected:

2023-08-23 08:48:12

Last scanned:

2023-08-23 08:48:12

Issue ID:

fb71f78bf31b290c310cf856b0e3917d

Detected by scan engine:

Rapid Scan Static (SAST) - Installed Version

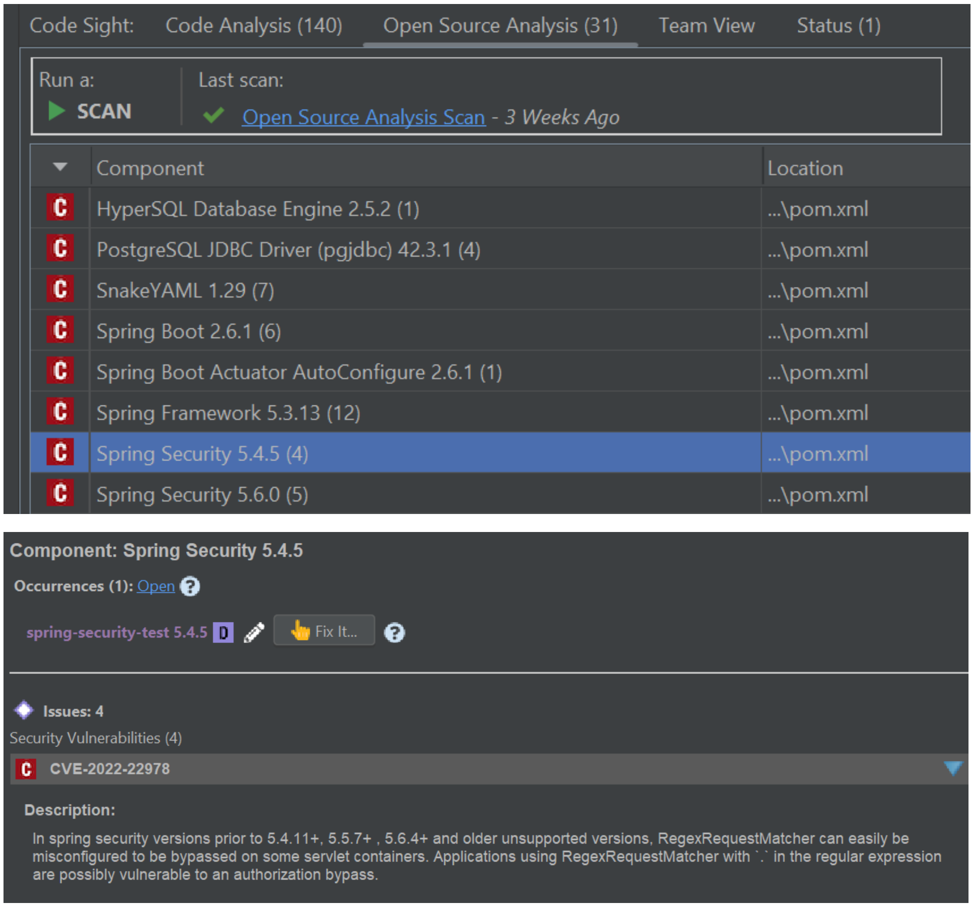
PathTraversalITTest.java

[1] Line 109 : Path Event - System.getProperty("java.io.tmpdir") is a source of tainted data

[2] Line 110 : Path Event - assigning the tainted data to webGoatHome

[3] Line 112 : Main Event - A user-controllable string is used as part or all of a filesystem path, filename, or URI (u

Rapid code analysis (SAST), detailed remediation guidance, and links to Black Duck® Developer Security Training, powered by Secure Code Warrior



	Component	Location
C	HyperSQL Database Engine 2.5.2 (1)	...\pom.xml
C	PostgreSQL JDBC Driver (pgjdbc) 42.3.1 (4)	...\pom.xml
C	SnakeYAML 1.29 (7)	...\pom.xml
C	Spring Boot 2.6.1 (6)	...\pom.xml
C	Spring Boot Actuator AutoConfigure 2.6.1 (1)	...\pom.xml
C	Spring Framework 5.3.13 (12)	...\pom.xml
C	Spring Security 5.4.5 (4)	...\pom.xml
C	Spring Security 5.6.0 (5)	...\pom.xml

Component: Spring Security 5.4.5

Occurrences (1): Open

spring-security-test 5.4.5 D

Issues: 4

Security Vulnerabilities (4)

C **CVE-2022-22978**

Description:

In spring security versions prior to 5.4.11+, 5.5.7+ , 5.6.4+ and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.

Rapid open source analysis (SCA) with vulnerability details and fix recommendations

Code Sight IDE Plugin | Developer-First or End-to-End Security

Code Sight is available as a standalone plugin designed to help development teams produce more-secure software from the start. It is also available as an IDE extension of the Black Duck suite of AST tools, which delivers priority issues and fix guidance directly to developers from later-stage, pipeline-based security tests.

Standalone Code Sight

Best for speed and secure DevOps for development teams.

Provide development teams with quality and security risk information for code, open source, and IaC templates used in their projects, directly within the IDE. Fix issues before pushing downstream and avoid late-stage rework.

Available for $500 per developer. 10 minimum, volume discount available. Free trial includes full standalone capabilities.

Code Analysis

✓ Rapid Scan Static

~~Full Scan (powered by Coverity SAST)~~

Open Source Analysis

✓ Rapid Scan SCA

Risk Insight

✓ Vulnerability severity, prioritization, and reachability metrics (e.g., CVSS)

✓ Unsecure coding practices (e.g., CWE)

✓ Black Duck Security Advisories

✓ Risk severity, location within code

✓ Remediation guidance

Enterprise Readiness

~~View security and quality risks detected across teams and projects~~

~~Custom security and license policy configuration~~

~~Automatic policy notification and enforcement~~

Scan Configurations

✓ Automatic and manual scan options

✓ Single-file scan and full project scan options

Deployment

✓ Available as standalone IDE plugin for popular IDEs

✓ Free trial available in VS Code, Visual Studio, Eclipse, and IntelliJ

Code Sight Plugin for Black Duck AST Tools

Best for full-life cycle application security for the enterprise.

Extend the full application security capabilities of Black Duck, Coverity, Software Risk Manager, and the Polaris Platform, without breaking established workflows. Security teams maintain control over pipeline-based tests while developers cultivate risk awareness directly in the IDE.

Included with Coverity SAST, Black Duck SCA, Software Risk Manager, and Polaris Software Integrity Platform®. Solution terms vary.

Code Analysis

✓ Rapid Scan Static

✓ Full Scan (powered by Coverity SAST)

Open Source Analysis

✓ Rapid Scan SCA

Risk Insight

✓ Vulnerability severity, prioritization, and reachability metrics (e.g., CVSS)

✓ Unsecure coding practices (e.g., CWE)

✓ Black Duck Security Advisories

✓ Risk severity, location within code

✓ Remediation guidance

Enterprise Readiness

✓ View security and quality risks detected across teams and projects

✓ Custom security and license policy configuration

✓ Automatic policy notification and enforcement

Scan Configurations

✓ Automatic and manual scan options

✓ Single-file scan and full project scan options

Deployment

✓ Available as IDE plugin–view documentation for complete list

Explore our documentation for updated Code Sight language and framework support matrices. Additional technical support specifications are available when using the Code Sight extension for Coverity SAST, Black Duck SCA, Polaris Software Integrity Platform, or Software Risk Manager.

This datasheet applies to Code Sight 2024.4.0 and later releases.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.