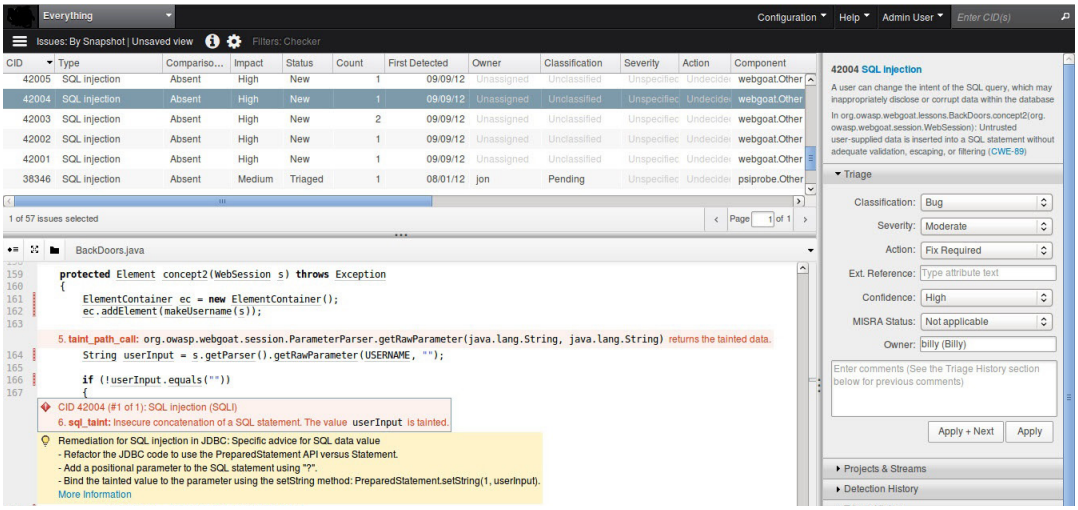
Coverity® is an accurate and comprehensive static analysis and Static Application Security Testing (SAST) platform that finds critical defects and security weaknesses in code as it's written before they become vulnerabilities, crashes, or maintenance headaches.



Actionable remediation guidance enables developers to quickly address potential security vulnerabilities.

ADDRESS SECURITY AT THE SOURCE

- Arm your developers with the information they need to troubleshoot and fix critical defects quickly and efficiently
- Build quality and security into development to reduce the cost of rework and delayed time to market resulting from defects found late in the cycle
- Reduce the risk of costly and brand-damaging software failures and security breaches in the field or in production

Product Overview

Coverity helps reduce risk and lower overall project cost by identifying critical quality defects and potential security vulnerabilities during development, with accurate and actionable remediation guidance, based on patented techniques and a decade of research and development and analysis of over 10 billion lines of proprietary and open source code

Key Features

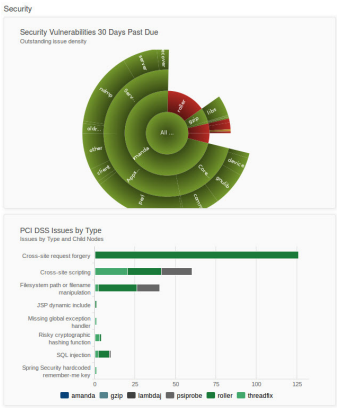
Depth and Accuracy of Analysis

- Coverity integrates seamlessly with any build system and generates a high fidelity representation of the source code to ensure a deep understanding of its behavior.
- Coverity provides full path coverage, ensuring that every line of code and every potential execution path are tested. It utilizes multiple patented techniques to ensure deep, accurate analysis.
- Through a deep understanding of the source code and the underlying frameworks, Coverity platform provides highly accurate analysis results so developers do not waste time managing large volume of false positive results. This enables them to effectively build security into the development lifecycle.

Speed and Scale of Analysis

Coverity was built from the ground up to fit into your existing workflow with the following capabilities:

- Parallel analysis allows Coverity to run on up to sixteen cores simultaneously and delivers up to a 10X performance improvement over serial analysis.
- Fast Desktop Analysis enables analysis acceleration by only re-analyzing the code which has changed or been impacted by a change, instead of the entire codebase each time.



Coverity's Policy Manager enables users to easily monitor and report on status, risks, and trends.

- Coverity scales to accommodate thousands of developers in geographically distributed environments and can analyze projects in excess of 100 million lines of code with ease.

Efficient Issue Management and Remediation

- With Coverity Connect, the platform's collaborative issue management interface, developers gain access to actionable information and precise remediation guidance, showing them the right way to fix the defect and the best place in the code to fix it without requiring deep security domain expertise.
- Coverity Connect provides source code navigation to identify the exact path to the defect and automatically identify every occurrence of the defect across shared code.
- Defects can be automatically assigned to the appropriate developer for resolution, and users can quickly view all outstanding security issues, OWASP Top 10 issues, CWE, and PCI related issues.

Software Development Lifecycle (SDLC) Integration

- Coverity platform allows rapid integration of critical tools and systems used to support the development process such as source control management, build and continuous integration, bug tracking, integrated development environments (IDE) and application lifecycle management (ALM) solutions.
- Coverity is an open platform that allows developers to import third party analysis results into the workflow to view and manage all types of defects in the same way with a single view of software defects and risks.

Drive Adoption and Mitigate Risk

Coverity Policy Manager enables organizations to define and enforce a consistent standard for code security as well as quality and testing across development teams. It provides visibility into which teams, projects or components are compliant with these standards and can create measurable stage gates based on predefined criteria regarding defects and testing. The customizable views in Coverity Policy Manager allows the selection of development metrics and thresholds that align to specific objectives for embedded, enterprise, and mobile applications.

Extend Vulnerability Detection

Coverity Extend is an easy-to-use Software Development Kit (SDK) that allows developers to detect unique defect types. The SDK is a framework for writing program analyzers, or checkers, which allows them to identify custom or domain specific defects. Customized checkers also help enable compliance with corporate security requirements and industry standards or guidelines.

Coverity is also proud to serve the open source community with more than 4000 projects currently using our free Coverity Scan, including Linux, Python, PostgreSQL, Firefox, OpenSSL, Perl, Apache Hadoop, and many more.

Supported Languages and Frameworks

C/C++	C#	Java
JavaScript	PHP	Python
ASP .NET	Objective-C	JSP
Node.js	Ruby	Andriod

Supported Platforms

Windows	Linux	Mac OS X	Solaris
AIX	HP-UX	NetBSD	FreeBSD

Some Supported Compilers

• VisualDSP++	• IBM XLC	• S SUN (Oracle) CC
• ARM C/C++	• Intel C++	• ynopsys Metaware C and C++
• Borland C++	• Keil Compilers	• TI Code Composer
• Clang	• Marvell MSA	• Visual Studio
• Cosmic C	• QNX C/C++	• Wind River C/++
• Freescale Codewarrior	• Renesas C/C++	• JDK for Mac OS X
• GNU GCC/G++	• SNC C/C++	• OpenJDK
• Green Hills C/C++/EC++	• SNC GNU C/C++	• Sun/Oracle JDK
• HI-TECH PICC	• Sony ORBIS SDK	
• HP aCC	• Sony PS4	
• IAR C/C++	• STMicroelectronics GNU C/C++	
	• STMicroelectronics ST Micro C/C++	

SDLC Integration

SCM	IDE/CI	Issue Tracking
• Accurev	• Android Studio	• JIRA
• Clearcase	• Eclipse	• Bugzilla
• CVS	• IBM RTC	
• Git	• IntelliJ	
• Hg (Mercurial)	• QNX Momentics	
• Perforce	• MS Visual Studio	
• SVN	• Wind River Workbench	
	• Jenkins	
	• TFS	

Critical Checks

API usage errors	Integer handling issues
Best practice coding errors	Integer overflows
Build system issues	Memory – corruptions
Buffer overflows	Memory – illegal accesses
Class hierarchy inconsistencies	Null pointer dereferences
Code maintainability issues	Path manipulation
Concurrent data access violations	Performance inefficiencies
Control flow issues	Program hangs
Cross-site scripting (XSS)	Race conditions
Cross-site request forgery (CSRF)	Resource leaks
Deadlocks	Rule violations
Error handling issues	Security best practices violations
Hard-coded credentials	Security misconfigurations
Incorrect expression	SQL Injection
Insecure data handling	Uninitialized members

SYNOPSYS®

www.synopsys.com/software

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com