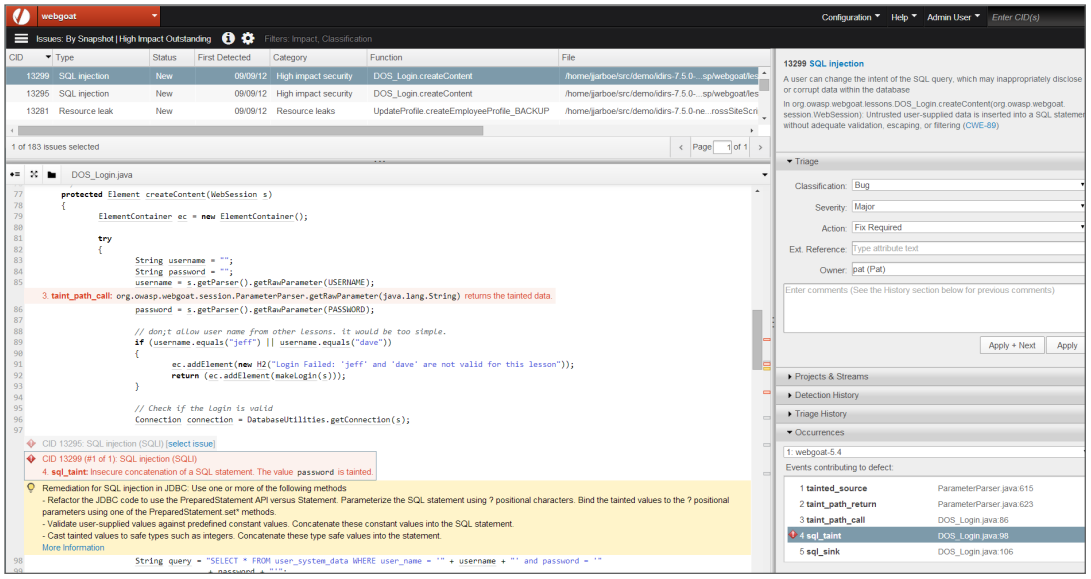
COVERITY
BY SYNOPSYS

Coverity Software Testing for Security

The Coverity® platform helps developers identify, manage and remediate critical security vulnerabilities and reduce the risk of software errors.



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

ADDRESS SECURITY AT THE SOURCE

- Identify and remediate critical OWASP Top 10 issues including Java web application security defects such as SQL injection, XSS and others
- Eliminate resource leaks, web application framework defects, command injection vulnerabilities and other security issues
- Understand what issues to address, where to find them and how to fix them with precise and prescriptive remediation advice

Solution Overview

Security breaches make headline news and have a material impact on the business. According to a recent study, the average cost of a security breach is more than seven million dollars. Software applications and the underlying code are the most vulnerable, with 75% of attacks happening at the application layer.

With the rising complexity of applications and the increasing threat of attacks, security risks can no longer be left to the security auditors to tackle on their own. With development teams outnumbering security audit teams by 1,000 to 1, security is no longer an option, but an imperative for software development organizations. By addressing application security in development with the Coverity Software Testing Platform, organizations can lower their overall risk and reduce the time and cost of security risk mitigation.

Key Capabilities

Deep Code Intelligence through Sophisticated Analysis Techniques

The Coverity Software Testing Platform applies multiple patented analysis techniques to automatically test code as it is written and accurately detect security vulnerabilities. It finds OWASP Top 10 and other CWE security-related issues without requiring developers to become security experts. Through a deep understanding of the source code and the underlying frameworks, the Coverity platform provides

highly accurate analysis results so developers don't waste time managing a large volume of false positive results. This enables them to effectively build security into the development lifecycle, reducing the cost, time and risk of security vulnerabilities.

Manage and Remediate Java Issues

A key reason legacy security tools fail in development is because they require too much security expertise and lack actionable remediation guidance. Within 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.

Defects can be automatically assigned to the appropriate developer for resolution, and users can quickly view all outstanding security issues, OWASP Top 10 issues and PCI related issues. Coverity Connect even provides source code navigation to identify the exact path to the defect and automatically identify every occurrence of the defect across shared code.

The Coverity platform can be extended so third party analysis tools can be integrated for simplified code analysis and management.

Integration into the SDLC

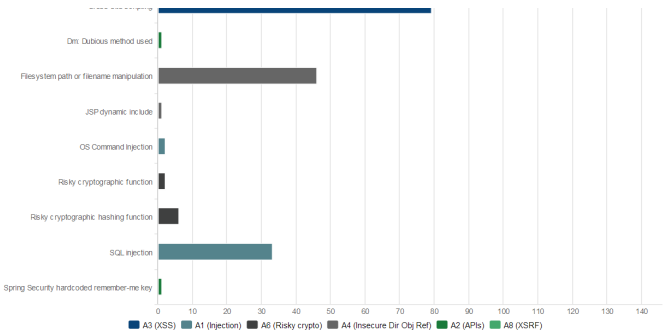
The platform allows rapid integration of critical tools and systems used to support the development process such as source control management, build and continuous integration, bug tracking, integrated development environments and application lifecycle management solutions.

Drive Adoption and Mitigate Risk

Coverity Policy Manager allows 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 pre-defined criteria regarding defects and testing.

The customizable views in Coverity Policy Manager allow the selection of development metrics and thresholds that align to specific objectives.

It enables the creation of heatmaps and other charts that specifically focus in on OWASP Top 10, PCI and other security issues to monitor and pinpoint areas of risk. It can also establish a stage gate to ensure that the product is not promoted to the next phase of the lifecycle unless all identified issues have been inspected, critical security defects addressed, and critical code has been covered by an automated test. This code intelligence enables managers to make better decisions and improves the predictability of releases.



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 such as MISRA or FDA guidelines. Some examples of custom checkers include:

- Check class with managed resources.
- Check unsafe pass structs in call.
- Check for unsafe conversions.
- Check for Floating Point Conditional Expression in Loop.

Interactive Application Security Testing (IAST)

Coverity is the market leader for Static Application Security Testing (SAST). For Dynamic Application Security Testing (DAST), Coverity has partnered with NT OBJECTives (NTO), and the results from NTOSpider can be automatically correlated with the Coverity platform's SAST findings and integrated into the development workflow through Coverity Connect for a complete IAST solution.

COVERITY® BY SYNOPSYS

www.coverity.com

Coverity Inc. Headquarters
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