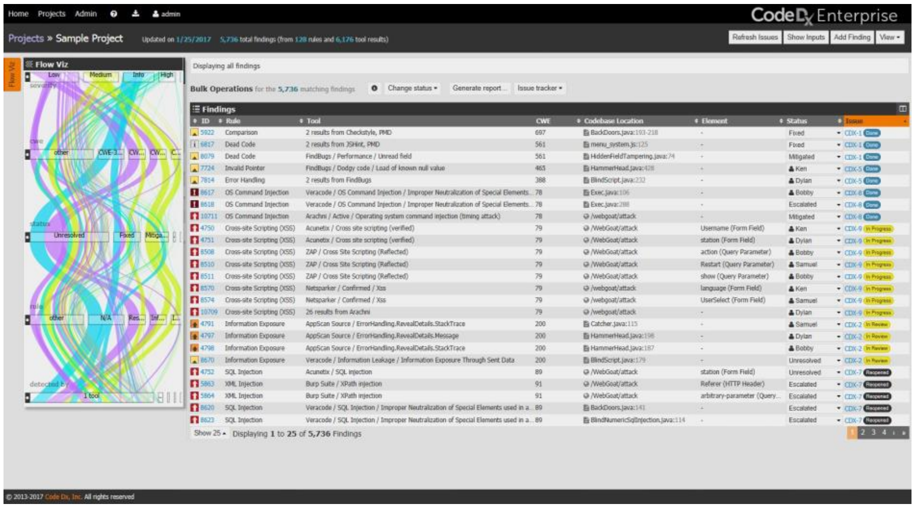
Code Dx Enterprise
Application Vulnerability Manager

FACT SHEET

Find and fix more vulnerabilities, with fewer false positives, automatically and in less time, with less work, and reduced labor costs.

Amplify your SAST, DAST, and IAST tools with automatic consolidation, correlation, and de-duplication of findings, integrated into your AppSec and DevSecOps processes, saving weeks of time.



Projects » Sample Project Updated on 1/25/2017 5,736 total findings (from 128 rules and 6,176 tool results)

Displaying all findings

Bulk Operations for the 5,736 matching findings Change status ▾ Generate report... Issue tracker ▾

Findings

ID	Rule	Tool	CWE	Codebase Location	Element	Status	Issue
5922	Comparison	2 results from Checkstyle, PMD	697	BackDoors.java:193-218	-	Fixed	CDX-1 Done
6817	Dead Code	2 results from JSHint, PMD	561	menu_system.js:125	-	Fixed	CDX-1 Done
8079	Dead Code	FindBugs / Performance / Unread field	561	HiddenFieldTampering.java:74	-	Mitigated	CDX-1 Done
7724	Invalid Pointer	FindBugs / Dodgy code / Load of known null value	465	HammerHead.java:428	-	Ken	CDX-5 Done
7814	Error Handling	2 results from FindBugs	388	BlindScript.java:232	-	Dylan	CDX-5 Done
8617	OS Command Injection	Veracode / OS Command Injection / Improper Neutralization of Special Elements...	78	Exec.java:106	-	Bobby	CDX-8 Done
8618	OS Command Injection	Veracode / OS Command Injection / Improper Neutralization of Special Elements...	78	Exec.java:288	-	Escalated	CDX-8 Done
10711	OS Command Injection	Arachni / Active / Operating system command injection (timing attack)	78	/webgoat/attack	-	Mitigated	CDX-8 Done
4750	Cross-site Scripting (XSS)	Acunetix / Cross site scripting (verified)	79	/WebGoat/attack	Username (Form Field)	Ken	CDX-9 In Progress
4751	Cross-site Scripting (XSS)	Acunetix / Cross site scripting (verified)	79	/WebGoat/attack	station (Form Field)	Dylan	CDX-9 In Progress
8508	Cross-site Scripting (XSS)	ZAP / Cross Site Scripting (Reflected)	79	/WebGoat/attack	action (Query Parameter)	Bobby	CDX-9 In Progress
8510	Cross-site Scripting (XSS)	ZAP / Cross Site Scripting (Reflected)	79	/WebGoat/attack	Restart (Query Parameter)	Samuel	CDX-9 In Progress
8511	Cross-site Scripting (XSS)	ZAP / Cross Site Scripting (Reflected)	79	/WebGoat/attack	show (Query Parameter)	Bobby	CDX-9 In Progress
8570	Cross-site Scripting (XSS)	Netsparker / Confirmed / Xss	79	/webgoat/attack	language (Form Field)	Ken	CDX-9 In Progress
8574	Cross-site Scripting (XSS)	Netsparker / Confirmed / Xss	79	/webgoat/attack	UserSelect (Form Field)	Samuel	CDX-9 In Progress
10709	Cross-site Scripting (XSS)	26 results from Arachni	79	/webgoat/attack	-	Dylan	CDX-9 In Progress
4791	Information Exposure	AppScan Source / ErrorHandling.RevealDetails.StackTrace	200	Catcher.java:115	-	Samuel	CDX-2 In Review
4797	Information Exposure	AppScan Source / ErrorHandling.RevealDetails.Message	200	HammerHead.java:198	-	Dylan	CDX-2 In Review
4798	Information Exposure	AppScan Source / ErrorHandling.RevealDetails.StackTrace	200	HammerHead.java:187	-	Bobby	CDX-2 In Review
8670	Information Exposure	Veracode / Information Leakage / Information Exposure Through Sent Data	200	BlindScript.java:179	-	Unresolved	CDX-2 In Review
4752	SQL Injection	Acunetix / SQL injection	89	/WebGoat/attack	station (Form Field)	Unresolved	CDX-7 Reopened
5863	XML Injection	Burp Suite / XPath injection	91	/WebGoat/attack	Referer (HTTP Header)	Escalated	CDX-7 Reopened
5864	XML Injection	Burp Suite / XPath injection	91	/WebGoat/attack	arbitrary-parameter (Query...	Escalated	CDX-7 Reopened
8620	SQL Injection	Veracode / SQL Injection / Improper Neutralization of Special Elements used in a...	89	BackDoors.java:141	-	Escalated	CDX-7 Reopened
8623	SQL Injection	Veracode / SQL Injection / Improper Neutralization of Special Elements used in a...	89	BlindNumericSqlInjection.java:114	-	Escalated	CDX-7 Reopened

Show 25 ▴ Displaying 1 to 25 of 5,736 Findings 1 2 3 4 › »

© 2013-2017 Code Dx, Inc. All rights reserved

Code Dx Enterprise is a comprehensive Application Vulnerability Manager featuring:

Correlation Create a unified, de-duplicated set of findings from *multiple techniques*: static (SAST), dynamic (DAST), interactive (IAST) application security testing, third-party component analysis, threat modeling, and manual review. Results of *multiple and diverse commercial and open source tools* are normalized to common nomenclature and severity ratings.

Analysis *Triage and prioritize* flaws and vulnerabilities based on industry standards, *regulatory compliance*, and your own rules and best practices.

Management A central console where you assign vulnerabilities for remediation, track progress, collaborate across security and development teams (optionally through Jira), and *report vulnerability trends* within your organization.

PROBLEM To properly secure your application you *must use multiple techniques, and combine the results*. You need to thoroughly analyze your source code, and then attack your running application. Each technique—static, dynamic, interactive, library analysis, manual review—yields different results for different categories of weaknesses. *Consolidating the results from these techniques is tedious and time-consuming*. Then, for each technique, such as static analysis, you must run and correlate results from *multiple tools*, because no one tool—commercial or open source—covers all programming languages or offers enough coverage to find every issue. The work to *consolidate, correlate and de-duplicate the results is labor-intensive and time-consuming*.

SOLUTION **Code Dx Enterprise** automatically consolidates, correlates, and de-duplicates results of multiple tools and multiple techniques, improving vulnerability coverage with fewer false positives. Since more tools mean better results, we even bundle and install for you a collection of open source SAST tools. Code Dx Enterprise identifies those vulnerabilities considered most-critical based on industry standards and *regulatory compliance*. It also helps you manage the consolidated results with easy ways to assign and track vulnerabilities for remediation, and report progress. Enterprise does this while seamlessly integrated into your development environment; it works smoothly with popular build servers and issue trackers, and adds security to your DevOps process.

The result is better *vulnerability coverage, less manual work, better collaboration across the development and security teams, and greater management insight* into the status of vulnerability remediation.

KEY BENEFITS

More effective software testing

- Better vulnerability coverage by combining multiple *tools* and *techniques*
- Fewer false positives
- Removes duplicate findings

Saves time and resources

- Automates the tedious process of combining results from multiple techniques
- Automates laborious work of correlating results of multiple tools within a technique
- Automatically selects and runs a collection of open source SAST tools and third-party library analyzers against your code

Analysis tools help you focus

- Identifies most-critical vulnerabilities based on industry standards, and on *potential for violation of regulatory compliance*
- Rapidly triage thousands of vulnerabilities into a manageable set to fix first

Helps you manage and track remediation

- Takes you directly to specific lines of code where vulnerabilities exist, and identifies neighboring flaws and vulnerabilities
- Centralized console to assign, track and monitor progress of remediation
- Vulnerability status across releases
- Reports on time taken to remediate vulnerabilities

Improves collaboration and communication

- Shared tool for security and dev teams to communicate findings and discuss remediation
- Communicates issues and resolutions *automatically, through Jira*
- Provides application security results in SIEM format for use by network security team

Works within your development process

- Developers can process vulnerabilities directly from their IDEs
- Fits into continuous integration environments, giving you continuous security assessment
- Integrates with version control systems and issue tracking systems

Who uses Code Dx Enterprise?

- Software Developers & Managers
- Security Analysts
- Quality Assurance Professionals
- Compliance Auditors
- Accreditors

How do they use it?

- Secure software development
- Security & Quality Assurance reviews
- Verification & Accreditation support
- Compliance reviews
- Code audits
- Pre-procurement software evaluations
- Process improvement

Comprehensive application vulnerability correlation and management for the enterprise

Code Dx Enterprise gives you the power to quickly and efficiently build security into your application development and DevOps environments. Load your source code and Enterprise automatically selects and runs a pre-configured set of open source SAST tools and third-party vulnerability analyzers to find flaws and vulnerabilities based on the languages in your code. Then add results from commercial and other SAST tools you've run, and of any dynamic and interactive (DAST/IAST) tools. Enterprise automatically combines these results with the static findings to provide a comprehensive application security picture. And if you do manual code reviews, Enterprise can incorporate those findings as well.

The Analysis and Management console helps you triage and prioritize vulnerabilities, assign and track their remediation, and monitor the progress of that remediation. All of this is integrated into the development environment, to work seamlessly with popular build servers and issue trackers.

KEY FEATURES

- Integrates results from more than 40 commercial and open source application security testing tools
- Tool connectors to automatically pull results from specific tools, including meta- data for tool-specific filters, searches, and reports
- Automatically combines and normalizes output of multiple SAST, DAST and IAST tools, third-party vulnerability scanners, and manual findings into a single set of results using a common nomenclature and severity scale
- Automatically installs, configures and runs many open source SAST tools, and tools to check vulnerabilities in third-party libraries
- Maps results to Common Weakness Enumeration (CWE) and industry standards
- including OWASP Top 10, **OWASP Top 10 Mobile**, SANS Top 25
- Identifies vulnerabilities that are potential violations of regulatory compliance including PCI-DSS, HIPAA, **NIST 800-53, DISA STIG 4.3**
- Provides easy way to triage and prioritize findings
- **Manage multiple, nested projects**; group by subproject or by organizational unit
- to manage your in accordance with your business structure
- Manage remediation with tools to assign, track, and report on vulnerability fixes
- Integrates with the popular Jira issue tracker to automatically create tickets, and automatically mark them as resolved when a tool reports an issue has cleared
- Integrates with popular development tools (Eclipse/Visual Studio/**IntelliJ**) to put
- findings into the hands of developers who can fix them
- Integrates with Git version control, for easy access to your code, and its history
- Embeds in continuous integration environments to build security into your pro- cess; enables integration to other build servers with its REST API
- Supports XML input for integration to custom or proprietary analysis tools
- Provides results in SIEM format for use by network security team

Specifications

Code Dx Enterprise is a scalable server application that supports teams of any size. Enterprise runs on Windows, Linux, and MacOS, and supports all modern browsers.

Security & Quality
Software GmbH

Freimanner Str. 14; 85737 Ismaning, Germany

www.sq-software.com/codedx

FEATURE DETAILS

Operating system support

Windows (7, 8, 10 & Server 2012 R2+)
Mac OS X 10.8+
Linux (Ubuntu, Fedora, Debian, RHEL, CentOS)

Language support

C / C++	Java	Javascript
JSP	.NET (C#, VB)	PHP
Python	Ruby	Scala

SAST support *open source*

Android Lint	Brakeman	CAT.NET
CheckStyle	Clang	CppCheck
ErrorProne	FxCop	FindBugs
Gendarme	Jlint	JSHint
PHP_CodeSniffer	PHPMD	PMD
Pylint	ScalaStyle	

SAST support *commercial*

Checkmarx	Coverity	HP Fortify
IBM AppScan	Parasoft	Veracode

Armorize CodeSecure
GrammaTech Code Sonar
WhiteHat Sentinel Source

DAST support *commercial & open source*

Acunetix	**AppSpider**	Arachni
Burp Suite	HP Webinspect	
IBM AppScan	Netsparker	OWASP ZAP
Veracode	WhiteHat Sentinel Dynamic	

IAST support *commercial*

Contrast Security Assess

Mobile support *commercial & open source*

NowSecure
Android Lint OCLint

Software Composition Analysis

Black Duck Hub
OWASP Dependency-Check
Sonatype Nexus Retire.js

IDE support

MS Visual Studio Eclipse **IntelliJ**

Issue tracking support

Jira, Jira Template Expressions

Continuous integration support

Jenkins
REST API for custom integrations

Version control system support

Git

SIEM & scanner support

AlienVault Nessus

Threat modeling.

Microsoft Threat Modeling