



Partner Technical Enablement

JASON KHOO

CISSP, CSSLP, CISA, Technical Account Manager

jason.khoo@checkmarx.com

10-11 October 2019

/ Objective

**To have the capability to demonstrate
CxSAST / CxOSA and the knowledge to
perform the Proof-of-Concept successfully.**

/ Agenda

Day 1

Software Security Platform

CxSAST Introduction and Configuration

CxSAST Feature and Capabilities

Java Project: EasyBuggy, Result Review & Remediation

CxSAST Integration

Day 2

CxAudit Session

CxUniversity

CxSAST Demonstration

/ Agenda

Exercises:

[Partner Technical Enablement Exercise - JasonK.docx](#)

CxTraining Machines:

[Jason khoo-CxTraining-r426 -APJ_Partner-7-13--10-2019.csv](#)

Training Resource on GitHub:

[https://github.com/cx-jason](#)

CxSAST Web Trial Portal:

[https://cxapactrial.checkmarx.net](#)

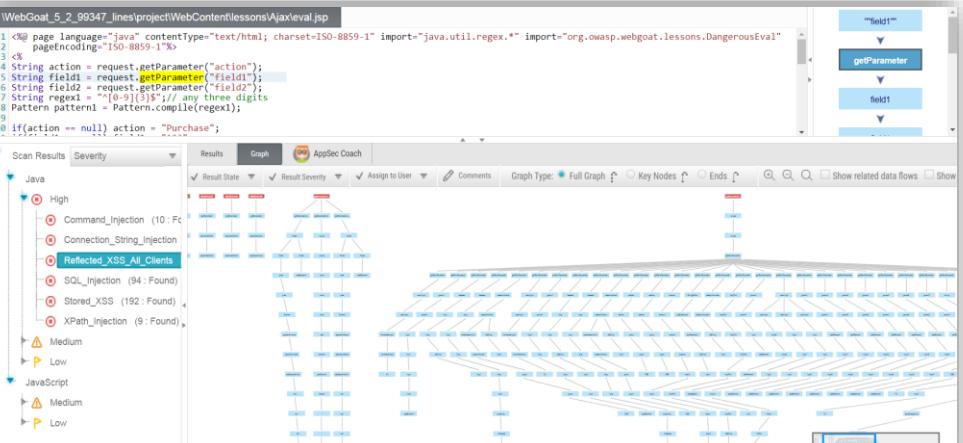
/ Software Security Platform

/ Checkmarx Software Security Platform

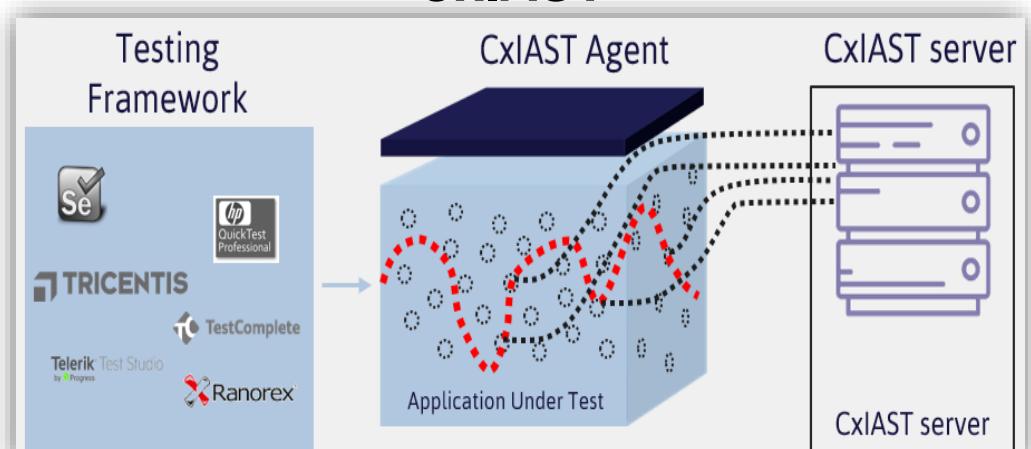


/ Checkmarx Software Security Platform

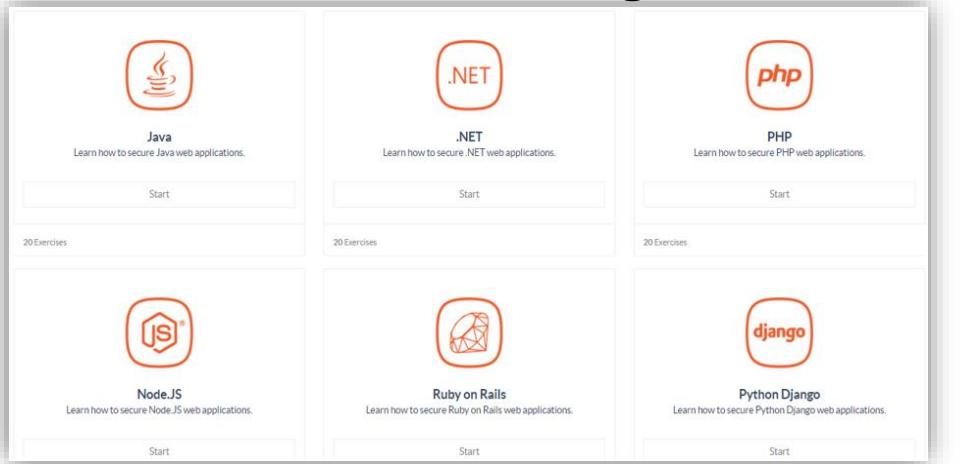
CxSAST



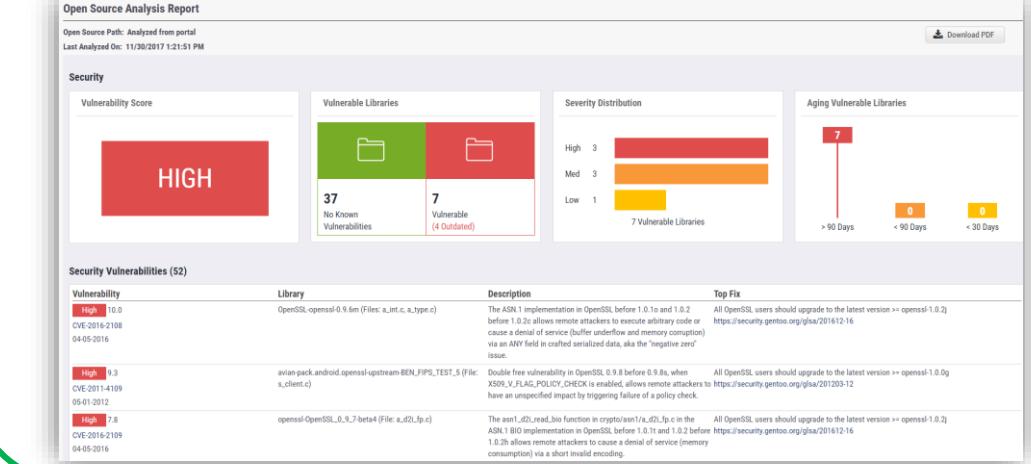
CxIAST



CodeBashing



CxOSA



/ Checkmarx Knowledge Center

<https://checkmarx.atlassian.net/wiki/spaces/KC/overview>

Checkmarx Knowledge Center

Checkmarx Knowledge Center includes our Technical Documentation, such as, Quick Start, Installation, Configurations, Plugin & Integration Solutions, Authentication, New Releases, User's Guides, Troubleshooting, and FAQ.

What can we help you with?

Checkmarx Documentation

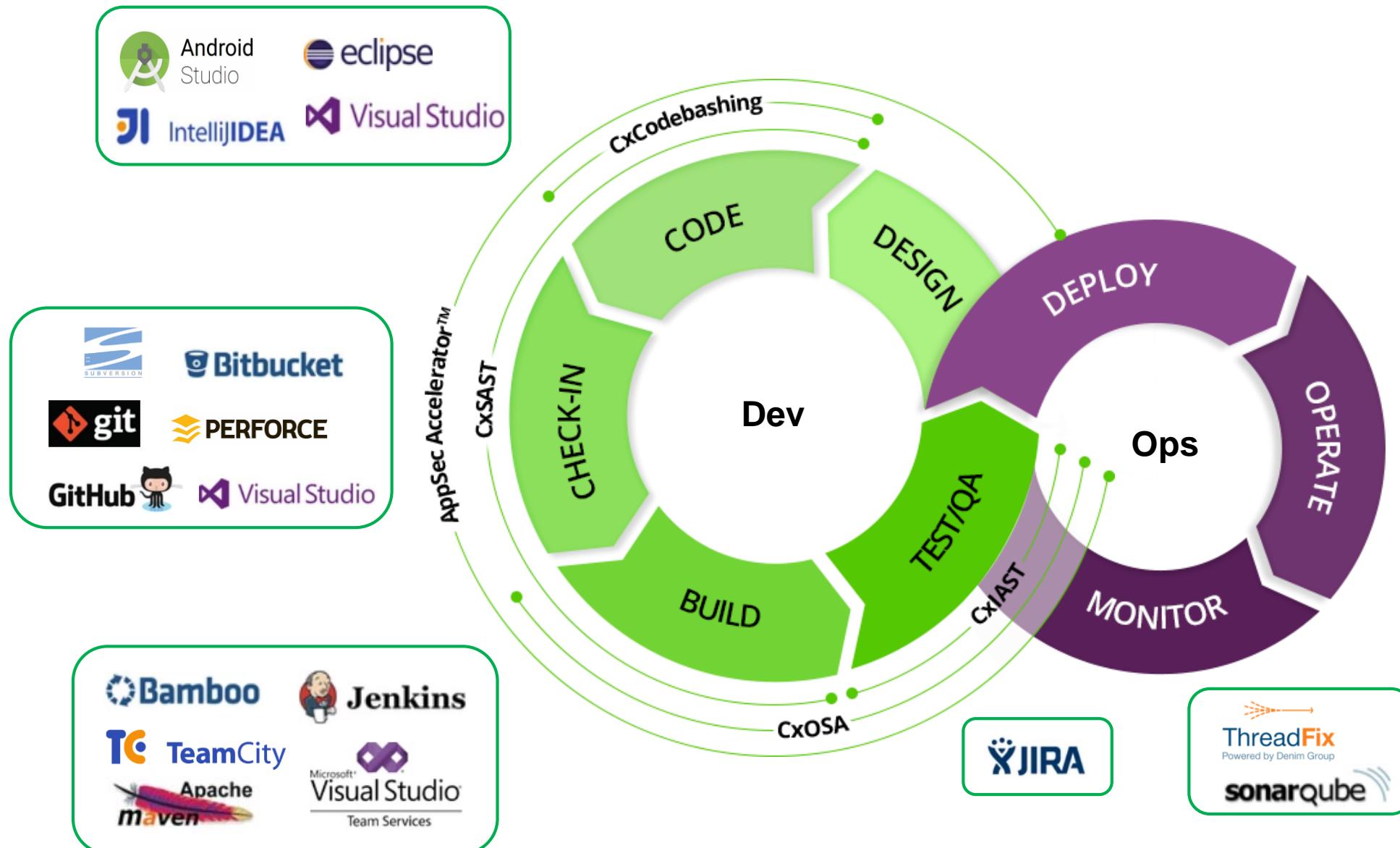
Discover	Get Started	IDE	Plugins	Integration	Authentication	Utilities	Get Help
Recommended Popular WATCH VIDEO	Release Notes Downloads Setup Quick Start User Guide Audit Guide API CLI Archived GET A FREE DEMO!	Eclipse Visual Studio IntelliJ	Jenkins Maven Bamboo TeamCity SonarQube TFS MS-VSTS	Ant Maven (CLI) JIRA GIT GitHub ThreadFix Bitbucket Codebashing Integration	SAML LDAP	Cx ZIP CMD Line Counter Cx File Extension Script Generator	Troubleshooting Frequently Asked Questions Getting Help & Support Contact Us

/ Software Development

				
TypeScript				
				
				
.NET Core				

- Supports 25 coding and scripting languages and their frameworks
- Coverage for the latest development technologies
- Zero configuration to scan any language

/ Secure SDLC & DevOps Environment



/ Common Weakness Enumeration, CWE

<https://cwe.mitre.org>

The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website. At the top left is the "CWE" logo and the text "Common Weakness Enumeration" followed by "A Community-Developed List of Software Weakness Types". To the right is a "CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS" badge. A search bar at the top right includes an "ID Lookup" field and a "Go" button. Below the header is a navigation menu with links for Home, About, CWE List, Scoring, Community, News, and Search. A main text area states: "CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts." Below this is a section titled "View the List of Weaknesses" with three buttons: "by Research Concepts", "by Development Concepts", and "by Architectural Concepts". Further down is a "Search CWE" section with a search input field and a "Google Custom Search" link. A note says "Easily find a specific software weakness by performing a search of the CWE List by keyword(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space." At the bottom, it says "See the full [CWE List](#) page for enhanced information, downloads, and more." and "Total Software Weaknesses: 716". The footer contains a "Page Last Updated: April 03, 2018" note, the MITRE logo, and legal disclaimers about terms of use and trademarks. On the right side of the footer are links for Privacy Policy, Terms of Use, Site Map, and Contact Us.

CWE Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

by Research Concepts | by Development Concepts | by Architectural Concepts

Search CWE

Easily find a specific software weakness by performing a search of the CWE List by keyword(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

Google Custom Search

See the full [CWE List](#) page for enhanced information, downloads, and more.

Total Software Weaknesses: 716

Page Last Updated: April 03, 2018

MITRE

Use of the Common Weakness Enumeration and the associated references from this website are subject to the [Terms of Use](#). For more information, please email cwe@mitre.org.
CWE is sponsored by [US-CERT](#) in the office of [Cybersecurity and Communications](#) at the [U.S. Department of Homeland Security](#). Copyright © 2006-2017, The MITRE Corporation. CWE, CWSS, CWRAF, and the CWE logo are trademarks of [The MITRE Corporation](#).

[Privacy Policy](#)
[Terms of Use](#)
[Site Map](#)
[Contact Us](#)

/ Common Vulnerabilities and Exposures, CVE

<https://cve.mitre.org>

The screenshot shows the official website for Common Vulnerabilities and Exposures (CVE). The top navigation bar includes links for "CVE List", "CNAs", "Board", "About", "News & Blog", and a "NVD" section with links to "CVSS Scores", "CPE Info", and "Advanced Search". Below the navigation is a black header bar with five buttons: "Search CVE List", "Download CVE", "Data Feeds", "Request CVE IDs", and "Update a CVE Entry". A total count of "TOTAL CVE Entries: 105329" is displayed. The main content area features three columns: "CNA Participation Growing Worldwide" (a world map with colored dots indicating participation), "Latest CVE News" (with links to minutes from a teleconference and a report on vulnerability remediation strategies), and "Newest CVE Entries" (a Twitter feed from @CVEnew). The "Newest CVE Entries" section highlights CVE-2016-8621, which is described as being vulnerable to an out-of-bounds read if it receives an input with one digit short.

CVE® is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity [products and services](#) from around the world, including the U.S. National Vulnerability Database ([NVD](#)).

CNA Participation Growing Worldwide



Latest CVE News

- Minutes from CVE Board Teleconference Meeting on July 11 Now Available
- CVE Is Main Source of Vulnerability Data Used in 2018 Vulnerability Remediation Strategies Report

[More >](#)

CVE Blog

CNA Processes Documentation Now on GitHub

We have updated the collection of processes

Newest CVE Entries

Tweets by @CVEnew

CVE @CVEnew

CVE-2016-8621 The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short. bit.ly/2LSWx6n

6h

/ SANS Top 25 Most Dangerous Software Errors

<https://www.sans.org/top25-software-errors>

CWE/SANS TOP 25 Most Dangerous Software Errors

What Errors Are Included in the Top 25 Software Errors?

The Top 25 Software Errors are listed below in three categories:

- Software Error Category: Insecure Interaction Between Components (6 errors)
- Software Error Category: Risky Resource Management (8 errors)
- Software Error Category: Porous Defenses (11 errors)

[The New 25 Most Dangerous Programming Errors](#)
[The Scoring System](#)
[The Risk Management System](#)

Click on the CWE ID in any of the listings and you will be directed to the relevant spot in the MITRE CWE site where you will find the following:

- Ranking of each Top 25 entry,
- Links to the full CWE entry data,
- Data fields for weakness prevalence and consequences,
- Remediation cost,
- Ease of detection,
- Code examples,
- Detection Methods,
- Attack frequency and attacker awareness
- Related CWE entries, and
- Related patterns of attack for this weakness.

Each entry at the Top 25 Software Errors site also includes fairly extensive prevention and remediation steps that developers can take to mitigate or eliminate the weakness.

Subscribe to SANS Newsletters

Join the SANS Community to receive the latest curated cyber security news, vulnerabilities and mitigations, training opportunities, and our webcast schedule.

Enter email address...

Enter country...

Subscribe

[Home](#)

[Archive](#)

/ OWASP Top Ten Project

<https://www.owasp.org/index.php>

The screenshot shows a Wikipedia page for the "Category:OWASP Top Ten Project". The page title is "Category:OWASP Top Ten Project". The top navigation bar includes links for "Category", "Discussion", "Read", "View source", "View history", "Search", and a "Help" link. Below the title, there is a horizontal menu with links: "Main", "Translation Efforts", "OWASP Top 10 for 2013", "OWASP Top 10 for 2010", "Project Details", and "Some Commercial & OWASP Uses of the Top 10". A large green banner at the top of the main content area features the words "FLAGSHIP" in white and "mature projects" in a smaller font. The main content section starts with a heading "OWASP Top 10 2017 Released" and a subtext "The OWASP Top 10 - 2017 is now available." It also includes a heading "OWASP Top 10 Most Critical Web Application Security Risks" and a paragraph about the project's purpose and members. To the right, a sidebar titled "Quick Download" lists links to various versions of the OWASP Top 10 document.

Category:OWASP Top Ten Project

Main Translation Efforts OWASP Top 10 for 2013 OWASP Top 10 for 2010 Project Details Some Commercial & OWASP Uses of the Top 10

FLAGSHIP mature projects

OWASP Top 10 2017 Released

The OWASP Top 10 - 2017 is now available.

OWASP Top 10 Most Critical Web Application Security Risks

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

We urge all companies to adopt this awareness document within their organization and start the process of ensuring that their web applications minimize these risks. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

Quick Download

- OWASP Top 10 - 2017 - PDF
- OWASP Top 10 - 2017 - wiki
- Historic:
 - OWASP Top 10 2013 - PDF
 - OWASP Top 10 2013 - wiki
 - OWASP Top 10 2013 Presentation (PPTX)

CxSAST Download Page

<https://www.checkmarx.com/downloads>

Downloads

Welcome to the Checkmarx Software Download Page

CxSAST Enterprise Edition Version 8.9.0

SHA256: 78E9D04413DAF97F639819120BD4E7095C7069FB68C9926BCE4B5FBBC8D28361

Last updated on April 30, 2019

Request Download Link

Enter your email to receive download link

SUBMIT

Please use your organization email to submit the request

Note the hotfix needs to be installed on the CxManager, CxEngines and CxAudit machines. In a distributed environment, the hotfix should also be installed on the Portal machine

Please download and install [HF5](#)

Click here for the silent [HF5](#) installation instructions

Click here for [HF5](#) for Release Notes

CxPlugins Download Page

<https://www.checkmarx.com/plugins>

Plugins

CxPlugins page

CLI	Command Line Interface can be used from Windows or Linux OS Cx Plugin Version: 8.90.1 CxSast Min Version: 8.9.0 Older Versions	Download
Eclipse	Eclipse IDE Plugin Cx Plugin Version: 8.9.0.0 CxSast Min Version: 8.9.0 Older Versions	Download
IntelliJ	IntelliJ IDE Plugin Cx Plugin Version: 8.90.0 CxSast Min Version: 8.9.0 Older Versions	Download
Visual Studio	VS IDE Plugin Cx Plugin Version: 8.50.2 CxSast Min Version: 8.5.0 Older Versions	Download
Jenkins	Plugin for Jenkins build server Cx Plugin Version: 8.90.4 CxSast Min Version: 8.9.0 Older Versions	Download
SonarQube	Plugin for SonarQube (Sonar 6.3 - 6.7.1 LTS) Cx Plugin Version: 8.90.0 CxSast Min Version: 8.9.0 Older Versions	Download

SonarQube Widget	SonarQube Dashboard Widget (Sonar 4.5.4-6.1) Cx Plugin Version: 8.42.0 CxSast Min Version: 8.4.1
Maven	Maven Plugin Cx Plugin Version: 8.80.2 CxSast Min Version: 8.8.0 Older Versions
Bamboo	Bamboo Plugin Cx Plugin Version: 8.90.0 CxSast Min Version: 8.9.0 Older Versions
TeamCity	TeamCity Plugin Cx Plugin Version: 8.90.0 CxSast Min Version: 8.9.0 Older Versions
TFS	TFS Build server plugin Cx Plugin Version: 1.4.0.2 CxSast Min Version: 7.1.2
CxAPI	CxAPI Examples Cx Plugin Version: 7.2.3 CxSast Min Version: 7.2.3

/CxUtilities Download Page

<https://www.checkmarx.com/cxutilities>

Utilities

Download Cx Utilities - All information and instructions are available at:

<https://checkmarx.atlassian.net/wiki/display/KC/CxSAST+Utilities+Guide>

Cx HID Generator

Download

Cx Zip

Download

Cx Cmd Line Counter

Download

Cx Create Domain User

Download

Cx Zip Longpath Support

Download

Cx Cmd HID Generator

Download

/ Exercise 1: POC Document and Discovery

CxSAST POC Plan Document – Partner
[CxSAST POC Plan Document v1.3.docx](#)

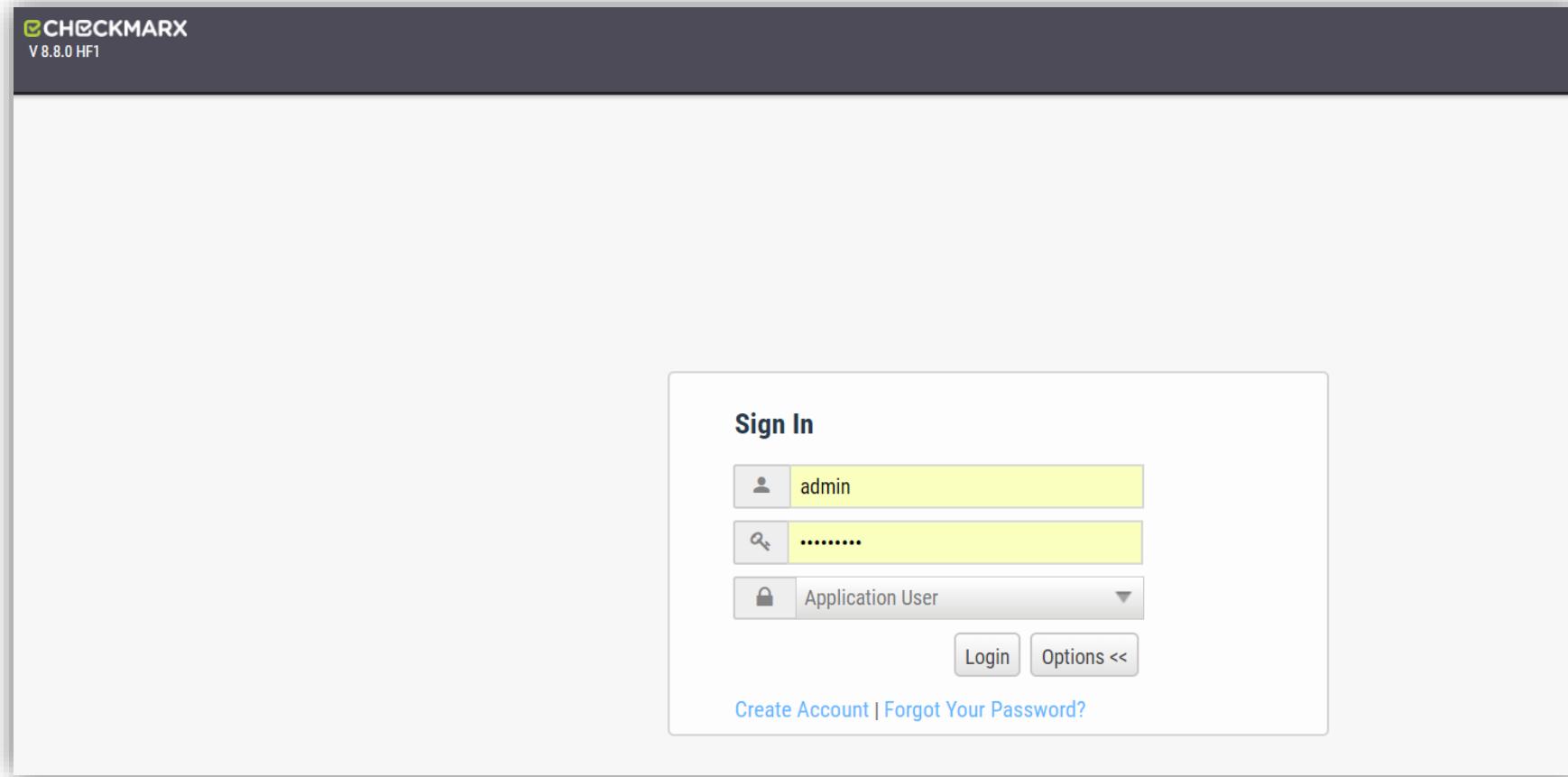
CxSAST POC Plan Document – Checkmarx Internal
[CxSAST POC Template - JasonK.docx](#)

Hardware Sizing – Checkmarx Internal
[Sizing AWS Hardware \(r-2\) For SE.xlsx](#)

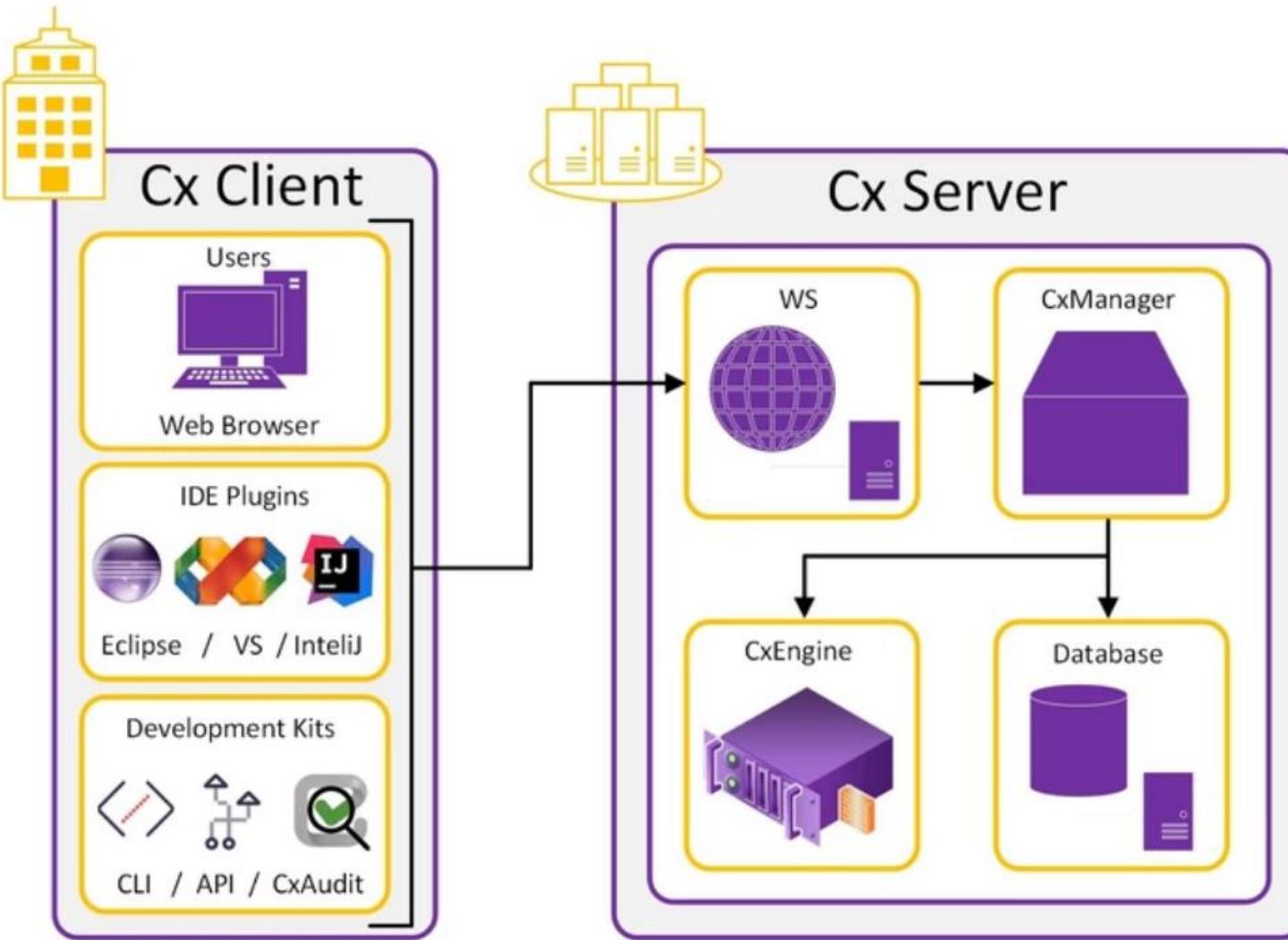
/ CxSAST

Introduction & Configuration

/CxSAST Introduction



/ Checkmarx CxSAST Architecture



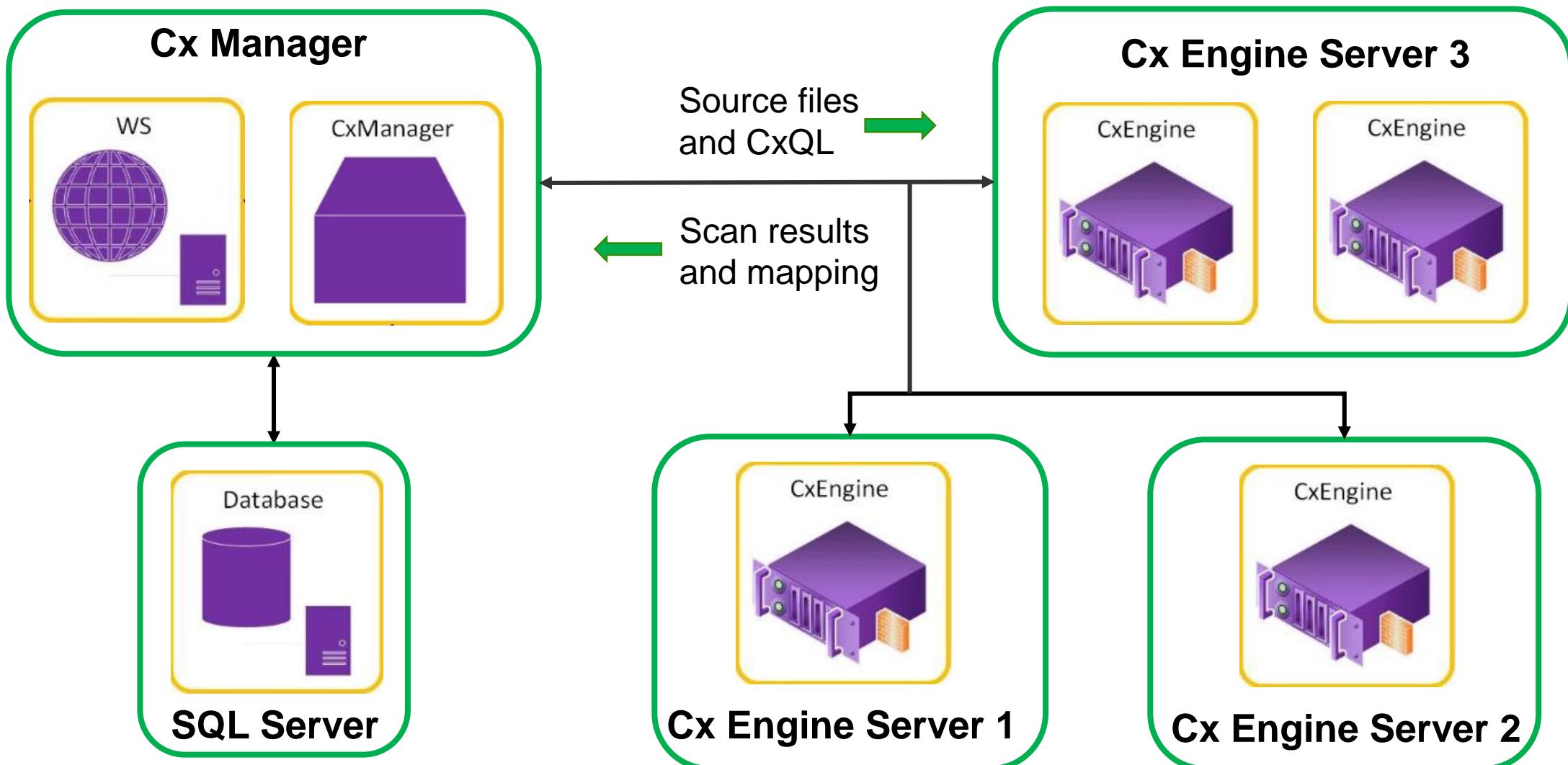
Server

- IIS web portal
- CxManager
- CxEngines
- SQL database

Client

- Web browsers
- Command line
- Third-party systems plugins
- IDE plugins

/ Checkmarx CxSAST Engine Architecture



/ Checkmarx CxSAST Engine Architecture

On the CxSAST web portal, Engine Management, user can register the

1. Engine Server URL
2. Engine Server Name
3. Scan Size

The screenshot shows the Checkmarx CxSAST web portal interface. The top navigation bar includes links for Dashboard, Projects & Scans, Management (with sub-options: Scan Settings, Connection Settings, Application Settings, Maintenance, Manage Custom Fields), Users & Teams, Data Analysis, My Profile, and a user account section for admin/admin. Below the navigation is a breadcrumb trail: Management / Application Settings / Engine Management. The main content area is titled "Engine Management". It displays a table with two rows of engine configurations:

Engine Server Name	Status	Engine URL	Scan Size	Actions
VM CxEngine-1	Offline	http://192.168.239.129/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 1000000	...
CxEngine-1	Scanning (1 of 3)	http://jasonk-laptop/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 999999999	...

A green rectangular box highlights the status "Scanning (1 of 3)" for the second engine entry.

/ Checkmarx CxSAST Engine Architecture

To edit the number of concurrent scans in one CxEngine Server, locate the file:

...\\Checkmarx\\Checkmarx Engine Server\\CxSourceAnalyzerEngine.WinService.exe.config

Key: MAX_SCANS_PER_MACHINE

Value: 3

Result:

This CxEngine Server can perform up to 3 concurrent scans

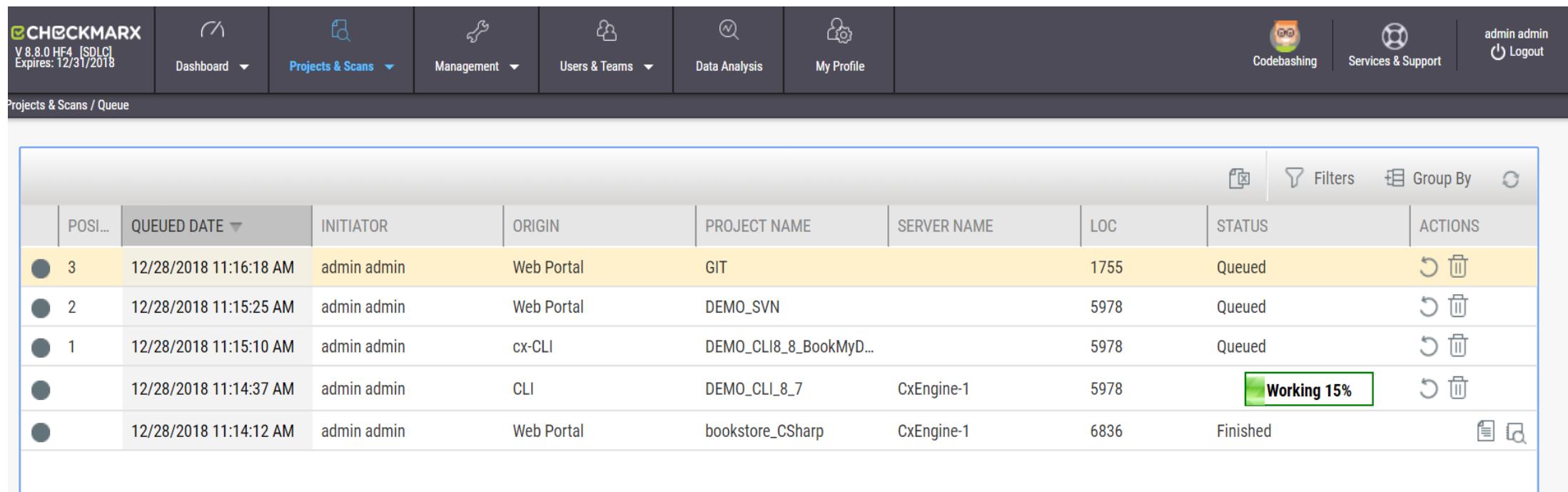
```
<instrumentationConfiguration performanceCountersEnabled="fa  
applicationInstanceName="" />  
<appSettings>  
  <!--<add key="BASE_PATH" value="C:\\Checkmarx\\Enterprise\\SOA-b  
  <add key="SOURCE_PATH" value="C:\\CxSrc" />  
  <!--  
  <add key="CACHE_PATH" value="C:\\Checkmarx\\Enterprise\\SOA-b  
  <add key="CONFIG_PATH" value="C:\\Checkmarx\\Enterprise\\SOA-b  
  <add key="RESULTS_PATH" value="C:\\Checkmarx\\Enterprise\\SOA-b  
  -->  
  <!--<add key="SCAN_AGENT_PATH" value="C:\\Checkmarx\\Enterpr  
  <add key="MAX_SCANS_PER_MACHINE" value="3" />  
  <add key="RESERVED_SCANS_TIME_OUT_MINUTES" value="15" />  
  <add key="PATH_LENGTH_LIMIT" value="80" />  
  <add key="MEMORY_LIMIT" value="350" />  
  <add key="ClientSettingsProvider.ServiceUri" value="" />  
  <add key="produceEngineResultsReport" value="false" />  
</appSettings>  
<startup>
```

/ Checkmarx CxSAST Queue Management

This is Queue Management to show the status for each Scan requests

Status:

New >> Waiting to process >> Source pulling & deployment >> LOC determined
>> Queued >> Working (%) >> Finished / Failed (Comment)



The screenshot shows the Checkmarx CxSAST Queue Management interface. At the top, there is a navigation bar with links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, My Profile, Codebashing, Services & Support, and Logout. Below the navigation bar, the main title is "Projects & Scans / Queue". The main content area displays a table of scan requests with the following columns: POSI..., QUEUED DATE, INITIATOR, ORIGIN, PROJECT NAME, SERVER NAME, LOC, STATUS, and ACTIONS. The table has five rows of data. The first four rows are yellow, indicating they are in the "Queued" state. The fifth row is white, indicating it is "Working 15%". The "Actions" column contains icons for each row.

POSI...	QUEUED DATE	INITIATOR	ORIGIN	PROJECT NAME	SERVER NAME	LOC	STATUS	ACTIONS
3	12/28/2018 11:16:18 AM	admin admin	Web Portal	GIT		1755	Queued	 
2	12/28/2018 11:15:25 AM	admin admin	Web Portal	DEMO SVN		5978	Queued	 
1	12/28/2018 11:15:10 AM	admin admin	cx-CLI	DEMO_CLI8_8_BookMyD...		5978	Queued	 
	12/28/2018 11:14:37 AM	admin admin	CLI	DEMO_CLI_8_7	CxEngine-1	5978	Working 15%	 
	12/28/2018 11:14:12 AM	admin admin	Web Portal	bookstore_CSharp	CxEngine-1	6836	Finished	 

/ Checkmarx CxSAST Configuration

CxSAST Web Portal – Application Settings

The screenshot shows the 'Management / Application Settings / General' page of the Checkmarx CxSAST web portal. The top navigation bar includes links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, My Profile, Codebashing, Services & Support, and Logout. The user 'admin admin' is logged in.

Server Settings

Reports Folder	C:\CxReports
Results Folder	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results
Executables Folder	C:\Program Files\Checkmarx\Executables
Path to GIT client executable	C:\Program Files\Git\bin\git.exe
Path to Perforce command-line client executable	(empty)
Maximum number of concurrent scans	2
Web Server Address	http://localhost
Long Path Support	<input type="checkbox"/>
Default Server Language	English (United States)

SMTP Settings

Host	smtp.gmail.com
Port	587
Encryption Type	TLS
Email From Address	(empty)
Use Default Credentials	<input type="checkbox"/>

/ Checkmarx CxSAST Configuration

CxSAST Web Portal – Installation Information

The screenshot shows the Checkmarx CxSAST Configuration web portal. The top navigation bar includes links for Dashboard, Projects & Scans, Management (selected), Users & Teams, Data Analysis, My Profile, and user account information (admin admin). The main content area is titled "Management / Application Settings / Installation Information". A sub-section titled "System Components" displays a table of installed components:

NAME	INSTALLATION PATH	DNS	IP	VERSION	HOTFIX	STATE
Checkmarx Web Services	C:\Program Files\Checkmarx\Checkmarx Web Services\	JasonK-Laptop	192.168.239.1	8.8.0.72	1	
Checkmarx Audit	C:\Program Files\Checkmarx\Checkmarx Audit\	JasonK-Laptop	192.168.239.1	8.8.0.72	0	
Checkmarx Scans Manager	C:\Program Files\Checkmarx\Checkmarx Scans Manager\	JasonK-Laptop	192.168.239.1	8.8.0.72	1	On
Checkmarx System Manager	C:\Program Files\Checkmarx\Checkmarx System Manager\	JasonK-Laptop	192.168.239.1	8.8.0.72	1	
Checkmarx Engine Server	C:\Program Files\Checkmarx\Checkmarx Engine Server\	JasonK-Laptop	192.168.239.1	8.8.0.72	0	
Checkmarx Jobs Manager	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\	JasonK-Laptop	192.168.239.1	8.8.0.72	1	On
CheckmarxWebPortal	C:\Program Files\Checkmarx\CheckmarxWebPortal\	JasonK-Laptop	192.168.239.1	8.8.0.72	0	

/ Checkmarx CxSAST Configuration

CxSAST Web Portal – License Details



V 8.8.0 HF1 [SDLC]
Expires: 10/1/2018

Dashboard ▾ Projects & Scans ▾ Management ▾ Users & Teams ▾ Data Analysis My Profile

Codebashing Services & Support admin admin Logout

Management / Application Settings / License Details

General

Edition: SDLC
Expiration Date: 1/10/2018
LOC: 500000
HID: #5136697493101869587701
OSA License: Enabled [?](#)

Supported Languages

<input type="checkbox"/> Apex	<input checked="" type="checkbox"/> ASP	<input checked="" type="checkbox"/> CPP	<input checked="" type="checkbox"/> CSharp	<input checked="" type="checkbox"/> Go
<input checked="" type="checkbox"/> Groovy	<input checked="" type="checkbox"/> HTML5	<input checked="" type="checkbox"/> Java	<input checked="" type="checkbox"/> JavaScript	<input checked="" type="checkbox"/> Objc
<input checked="" type="checkbox"/> Perl	<input checked="" type="checkbox"/> PHP	<input checked="" type="checkbox"/> PLSQL	<input checked="" type="checkbox"/> Python	<input checked="" type="checkbox"/> Ruby
<input checked="" type="checkbox"/> Scala	<input checked="" type="checkbox"/> Swift	<input checked="" type="checkbox"/> Typescript	<input checked="" type="checkbox"/> VB6	<input checked="" type="checkbox"/> VbNet
<input checked="" type="checkbox"/> VbScript				

Capacity

	In Use	Available
Users	3	10 
Auditors	1	1 
Projects	7	20 
Number of Concurrent Scans	2	2 

/ Checkmarx CxSAST Configuration

CxSAST Web Portal – Engine Server Management

The screenshot shows the Checkmarx CxSAST Engine Management interface. At the top, there is a navigation bar with the following items:

- Checkmarx logo and version: V 8.8.0 HF1 [SDLC] Expires: 10/1/2018
- Dashboard
- Projects & Scans
- Management
- Users & Teams
- Data Analysis
- My Profile

On the right side of the top bar, there are three user-related icons: Codebashing, Services & Support, and Logout.

The main content area has a breadcrumb navigation: Management / Application Settings / Engine Management.

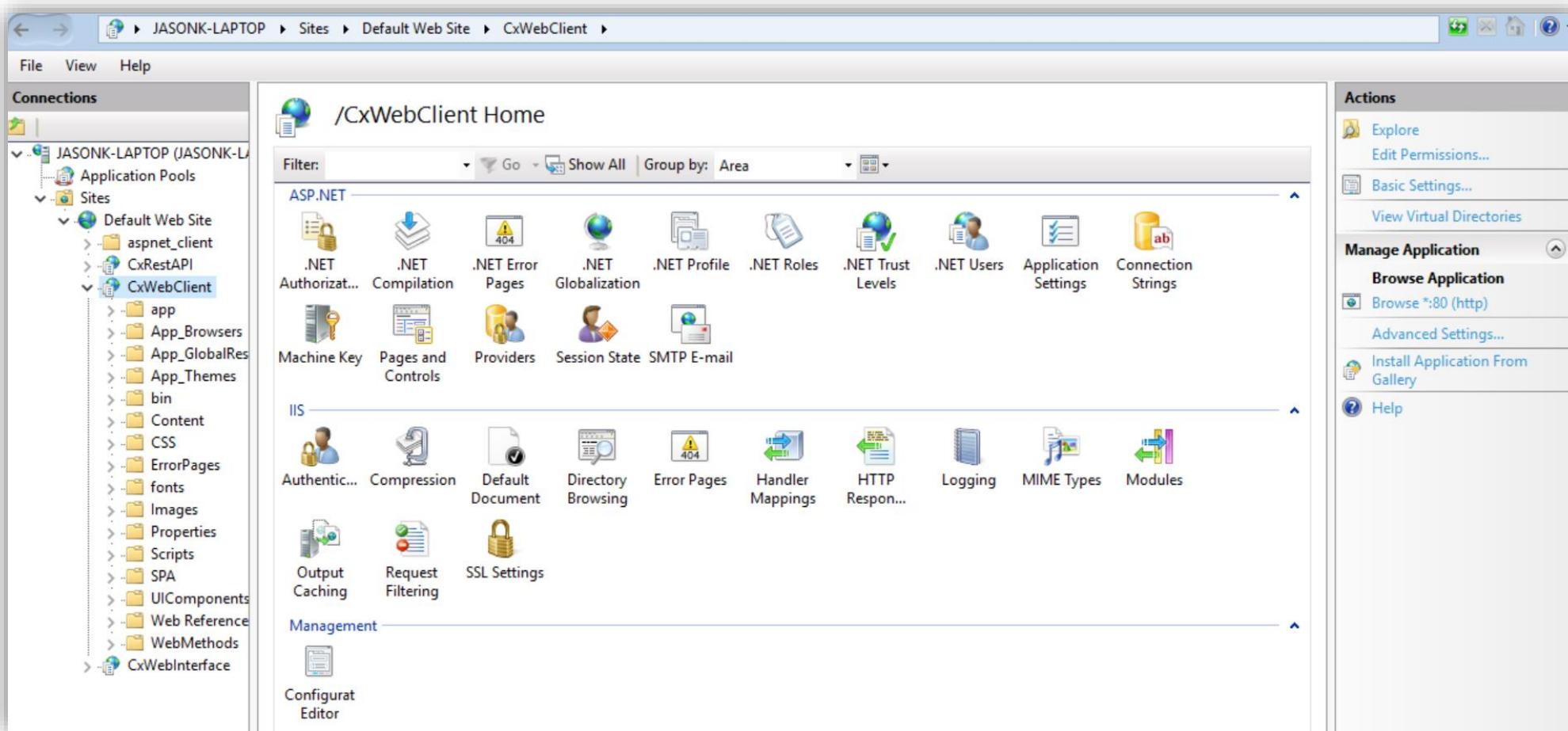
The "Engine Management" section contains a table with the following data:

Engine Server Name	Status	Engine URL	Scan Size	Actions
Localhost	Idle	http://localhost/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 999999999	...
Addon CxEngine	Idle	http://jasonk-laptop/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 999999999	...

A blue "REGISTER ENGINE SERVER" button is located at the top right of the "Engine Management" section.

/Checkmarx CxSAST Configuration

Microsoft Internet Information Services Manager



/ Checkmarx CxSAST Configuration

Microsoft Windows Services

- CxJobsManager
- CxScanEngine
- CxScansManager
- CxSystemManager
- SQL Server

Name	Description	Status	Startup Type
Credential Manager	Provides secure storage and retrieval of creden...	Running	Manual
Cryptographic Services	Provides three management services: Catalog ...	Running	Automatic
CxARM	CxARM Tomcat Server		Manual
CxARMETL	ETL Service	Running	Automatic
CxJobsManager	Service of Checkmarx Jobs Manager	Running	Automatic (Delayed Start)
CxScanEngine	Service of Checkmarx Scan Engine	Running	Automatic (Delayed Start)
CxScansManager	Service of Checkmarx Scans Manager	Running	Automatic (Delayed Start)
CxSystemManager	Service of Checkmarx System Manager	Running	Automatic (Delayed Start)
Data Sharing Service	Provides data brokering between applications.		Manual (Trigger Start)

Name	Description	Status	Startup Type
Spot Verifier	Verifies potential file system corruptions.		Manual (Trigger Start)
SQL Server (SQLEXPRESS2016)	Provides storage, processing and controlled ac...	Running	Automatic
SQL Server (SQLSERVER2016)	Provides storage, processing and controlled ac...	Running	Automatic
SQL Server Agent (SQLEXPRE...	Executes jobs, monitors SQL Server, fires alerts, ...		Disabled
SQL Server Agent (SQLSERVE...	Executes jobs, monitors SQL Server, fires alerts, ...		Disabled
SQL Server Browser	Provides SQL Server connection information to...	Running	Automatic
SQL Server CEIP service (SQL...	CEIP service for Sql server		Manual
SQL Server CEIP service (SQL...	CEIP service for Sql server		Manual

/ Checkmarx CxSAST Configuration

Microsoft SQL Server Database

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface. The left pane displays the Object Explorer with a tree view of the database structure, including the CxDB database. The central pane shows a table of configuration data with columns: Id, Key, Value, and Description. The right pane shows the Properties window for a query named [Qry] Query1.dtq.

Id	Key	Value	Description
171	ActivationURL	https://cxauth....	Authorization s...
216	ActiveMessage...	tcp://JasonK-La...	ActiveMQ servi...
94	AllowAutoSignIn	True	Not In Use
42	APP_TEMP_PATH	C:\Program File...	Defines applica...
173	AppSecCoach...	https://cxauth....	Authorization s...
223	ArmResponseQ...	ArmResponseQ...	Default queue ...
164	AuditKeepAlive...	5400	Defines the exp...
165	AuditKeepAlive...	6000	Defines the ma...
104	AUTHENTICATI...		Defines the Gui...
178	AuthorizationS...	https://cxauth....	Authorization s...
211	BEAUTIFIER_TI...	180	Maximum time...
212	BestFixLocation...	0.61	BFL group size ...
205	CentralizedLog...		Centralized pat...
144	CHECK_RESULT...	False	Enables a check...
7	CleanOrphaned...	600	Defines the del...
3	CleanScanQue...	60	Defines the del...
198	codebashingIsE...	false	Enable/Disable ...
177	COMPLETED_S...	10	NULL
214	ConfidenceLev...	2.8	Confidence lev...
201	CxArmAccessT...	86400	Determines the ...
218	CxARMPolicyURL	http://JasonK-L...	CxARM policy ...
217	CxARMURL	http://JasonK-L...	CxARM CxAnal...
170	CxSignExpirati...	1	Time in minute...

Properties Window:

- (Identity)**
 - Name: Query1.dtq
 - Database Name: CxDB
 - Server Name: jasonk-laptop\sqlserver
- Query Designer**
 - Destination Table: (None)
 - Distinct Values: No
 - GROUP BY Extension: <None>
 - Output All Columns: No
 - Query Parameter: No parameters have been defined.
 - SQL Comment: **** Script for SelectToTable
 - Top Specification: Yes

/ Exercise 2: Installation and Configuration

CxSAST Uninstallation and Installation

License file

Backup DB and restore DB

First Administrator

SMTP and GIT

CxEngines

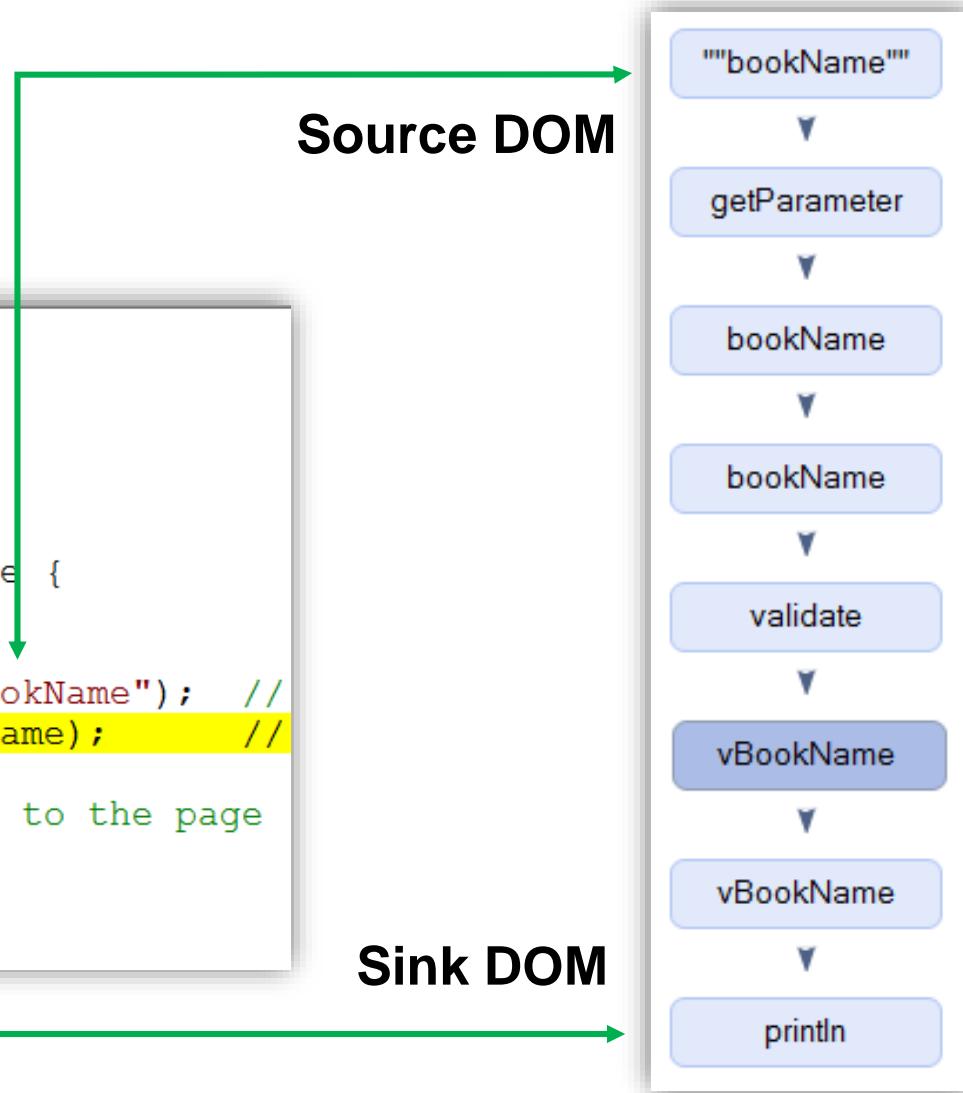
Internet information Services and Windows Services

/ CxSAST and CxOSA Features and Capabilities

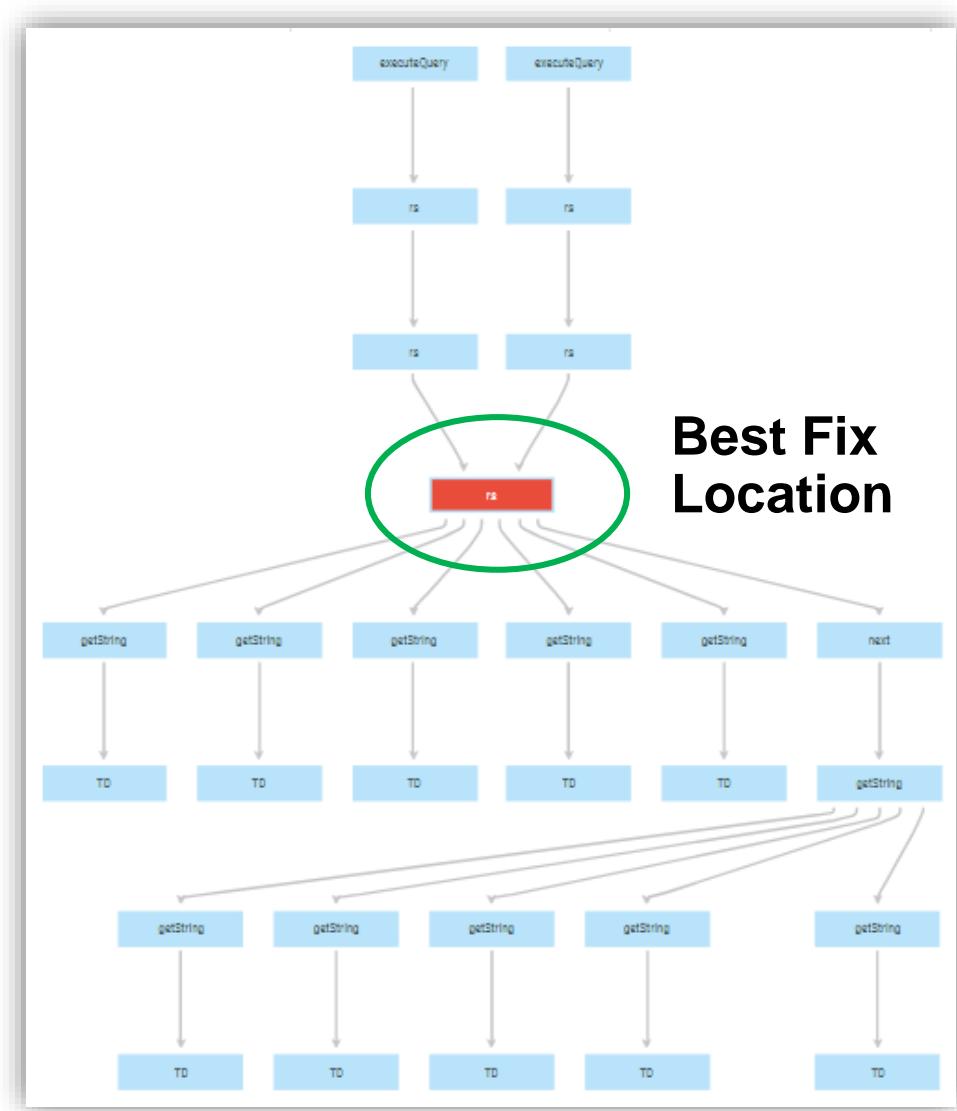
/ Checkmarx CxSAST Technology

- Data Object Model, DOM
- Data Flow Graph, DFG
- Best Fix Location

```
1 import javax.servlet.*;
2 import javax.servlet.http.*;
3 import javax.servlet.jsp.*;
4 import org.apache.jasper.runtime.*;
5 import cnt.Security.*;
6
7 public class BookDetail_jsp extends HttpJspBase {
8
9     public static String loadDriver () {
10         String bookName = request.getParameter("bookName"); //
11         String vBookName = Security.validate(bookName); //
12
13         out.println(vBookName); // print vbookName to the page
14     }
15 }
16 }
```



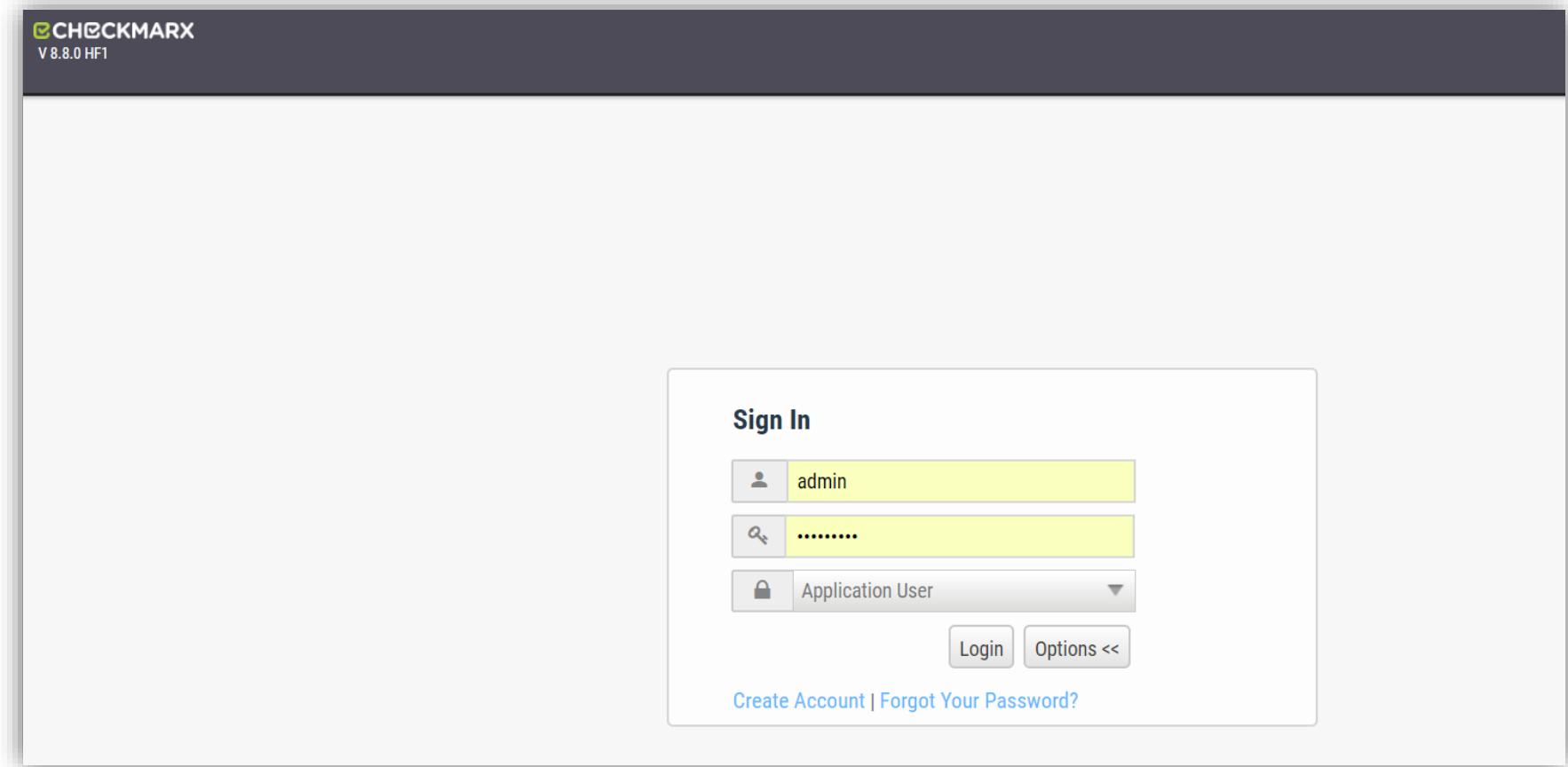
/ Checkmarx CxSAST Technology



/ Checkmarx CxSAST Web Portal

CxSAST Web Portal

- Login
- Create account
- Forget password



/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Projects Overview

Screenshot of the Checkmarx CxSAST Web Portal – Projects Overview page.

The page displays a table of projects with the following columns:

Project Name	Last Scan Date	Team	LOC	Risk Level Score	High Vulnerabilities	Medium Vulnerabilities	Actions
DEMO_EasyBuggy	9/6/2018	CxServer	7286	 (52)	4	91	View Edit Delete
DEMO_Benchmark	9/6/2018	CxServer	410649	 (100)	2892	3423	View Edit Delete
DEMO_CLI_8_7	9/5/2018	CxServer\SP\Company\Te...	5978	 (49)	26	130	View Edit Delete
DEMO_WebGoat_5_2	9/4/2018	CxServer	118873	 (100)	687	932	View Edit Delete
DEMO_GitHub	9/4/2018	CxServer\SP\Company\Te...	1755	 (32)	3	9	View Edit Delete
DEMO SVN	9/4/2018	CxServer\SP\Company\Te...	5978	 (49)	26	130	View Edit Delete
DEMO_BookMyDoc-master	9/4/2018	CxServer\SP\Company\Te...	5978	 (49)	26	130	View Edit Delete

Page navigation and settings:

- Page size: 10
- 7 items in 1 pages

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Project Dashboard

Projects State / DEMO_EasyBuggy

< Back | Projects State: DEMO_EASYBUGGY

Summary Scans History

Current status (Public Scan on 9/6/2018 3:50:44 PM)

SAST Vulnerabilities Status

High Med Low Recurrent

Full Scan Results >

Severity	New	Recurrent	Solved
High	4	0	4
Med	91	21	24
Low	297	54	53

0 New
4 Recurrent
4 Solved

91 Med
21 New
70 Recurrent
24 Solved

297 Low
54 New
243 Recurrent
53 Solved

SAST progress status

Previous Solved Recurrent

Category	Previous	Solved	Recurrent
HIGH	8	0	4
MED	94	91	0
LOW	296	0	297

Open Source Analysis (OSA) (i)

Last Scan on 9/8/2018 5:15:31 AM

61 Libraries were analyzed

61 No Known Vulnerabilities

0 Vulnerable (0 outdated)

[View Analysis Results >](#)

/ Checkmarx CxOSA Web Portal

CxSAST Web Portal – Open Source Analysis, CxOSA

DEMO_EasyBuggy

LIBRARIES VULNERABILITIES OSA Scan : Start: 9/8/2018- 15:45:22 → End: 9/8/2018- 15:46:53

All Libraries 10

Outdated Version Libraries 10 (4 Vulnerable)

Vulnerable Libraries 4

Libraries At Legal Risk 1 (High & Med)

All Libraries (10)							Search Library Name <input type="text"/>		
Library Name	Version	Severity 	License Type	Legal Risk	Match Type				
struts2-core-2.3.20.jar	2.3.20	14 3 1	Apache 2.0	No Risk	Exact Match				
commons-collections-3.1.jar	3.1	3 0 0	Apache 2.0	No Risk	Exact Match				
log4j-core-2.8.1.jar	2.8.1	1 0 0	Apache 2.0	No Risk	Exact Match				
commons-beanutils-1.8.3.jar	1.8.3	1 0 0	Apache 2.0	No Risk	Exact Match				

/ Checkmarx CxOSA Web Portal

CxSAST Web Portal – Open Source Analysis, CxOSA

LIBRARIES VULNERABILITIES

OSA Scan : Start: 9/8/2018- 15:45:22 → End: 9/8/2018- 15:46:53

← Back
struts2-core-2.3.20.jar
Match Type: Exact Match

Security Vulnerabilities **18**

Version **2.3.20**

Your version is outdated

2.3.20 Your version (11/21/2014)
2.5.17 Newest stable version 8/14/2018

30 New versions since your most recent update.
Consider updating to latest version

Instances in other projects **4**

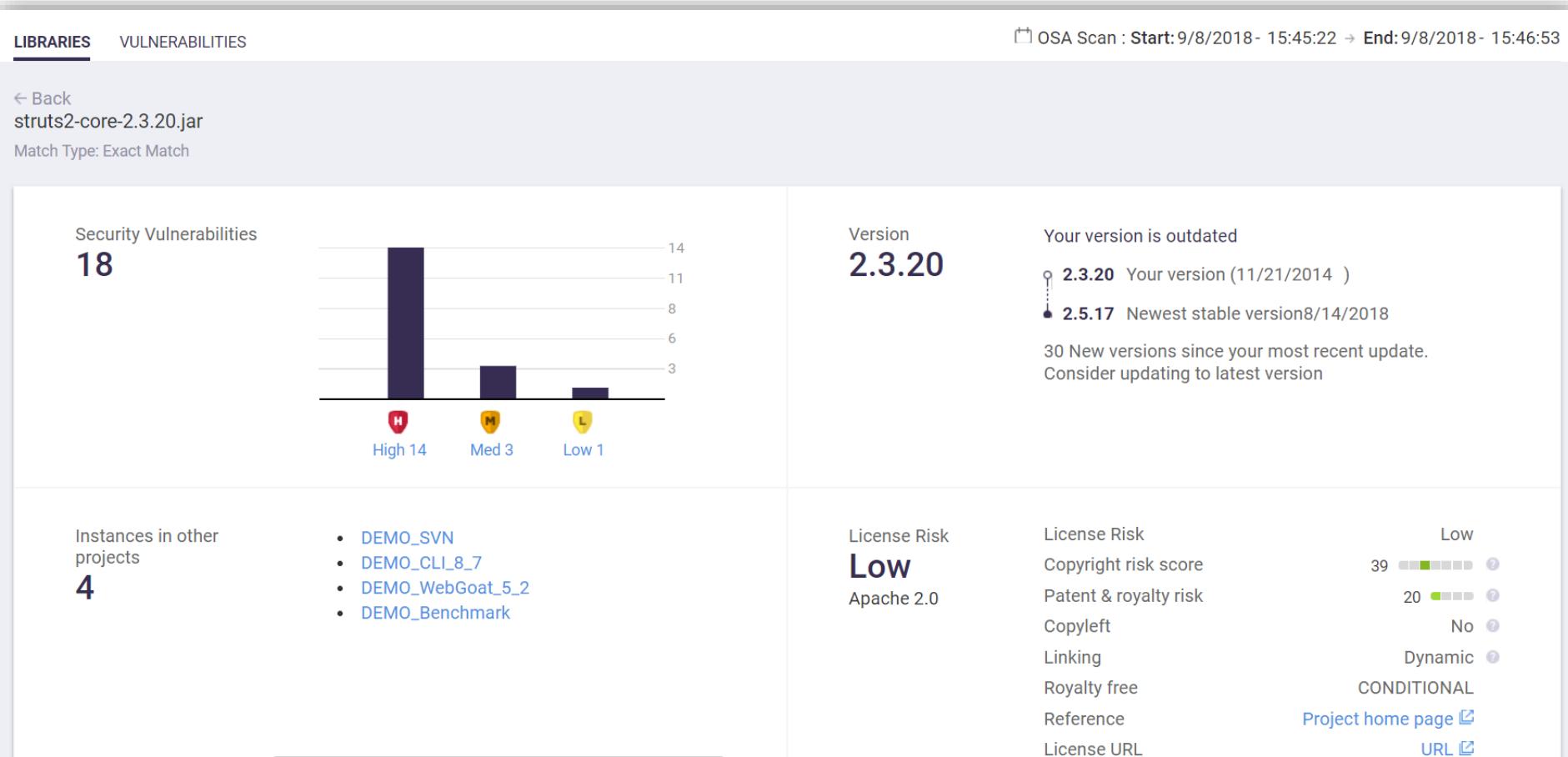
- DEMO_SVN
- DEMO_CLI_8_7
- DEMO_WebGoat_5_2
- DEMO_Benchmark

License Risk **Low**

Apache 2.0

License Risk

Copyright risk score	Low
Patent & royalty risk	39
Copyleft	20
Linking	No
Royalty free	Dynamic
Reference	CONDITIONAL
License URL	Project home page ↗ URL ↗



/ Checkmarx CxOSA Web Portal

CxSAST Web Portal – Open Source Analysis, CxOSA

DEMO_EasyBuggy

LIBRARIES **VULNERABILITIES** OSA Scan : Start: 9/8/2018- 15:45:22 → End: 9/8/2018- 15:46:53

Filter By: Library Name ▾ State ▾ Comment ▾ Detection Date ▾ | [Reset](#)

All 23	High 19	Med 3	Low 1
CVF-2016-4438			9.8
struts2-core-2.3.20.jar (14)			
CVE-2017-12611	9/20/2017 To Verify	9.8	
CVE-2018-11776	8/23/2018 To Verify	9.5	
CVE-2016-3082	4/26/2016 To Verify	9.8	
CVE-2016-3081	4/26/2016 To Verify	8.1	
CVE-2017-9787	7/13/2017 To Verify	7.5	

CVE-2018-11776

9.5 To Verify struts2-core-2.3.20.jar Version 2.3.20 8/23/2018

Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when using results with no namespace and in same time, its upper action(s) have no or wildcard namespace. Same possibility when using url tag which doesn't have value and action set and in same time, its upper action(s) have no or wildcard namespace. [CVE-2018-11776](#)

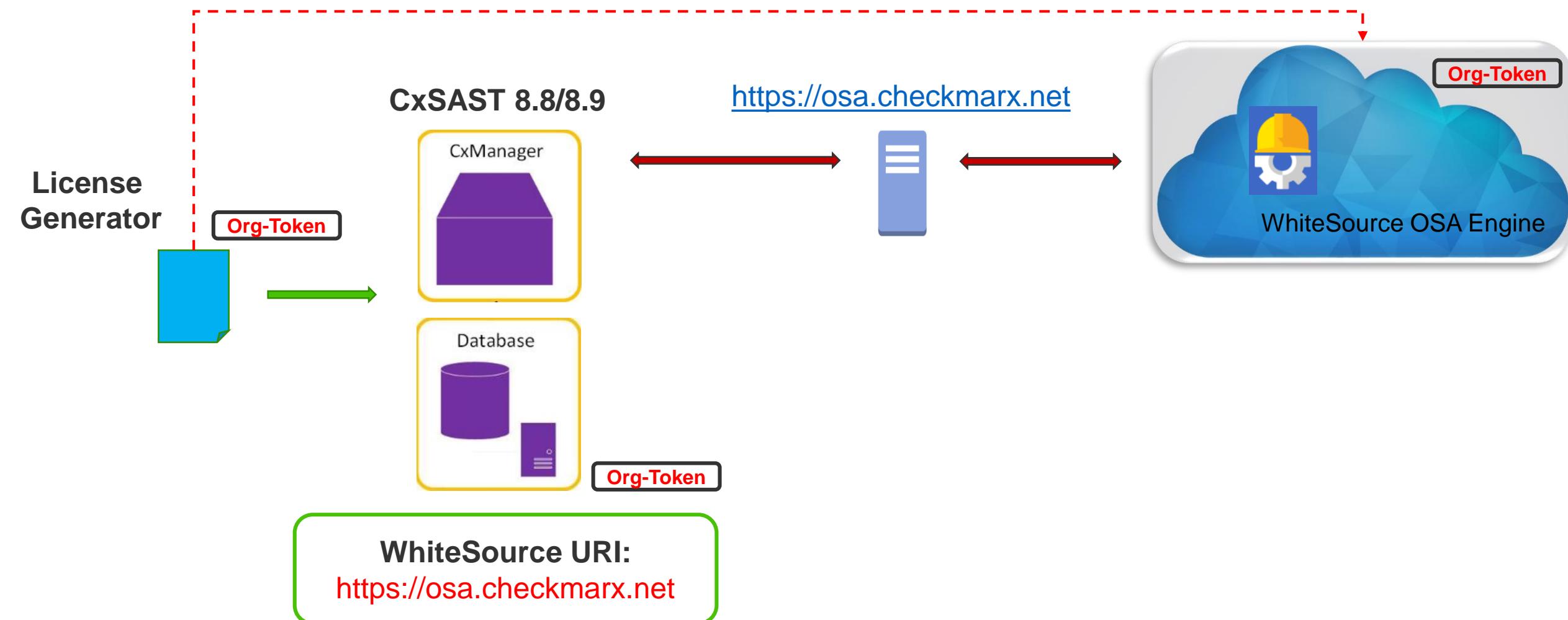
Vulnerability Recommendations:

Upgrade to Struts 2.3.35 or Struts 2.5.17

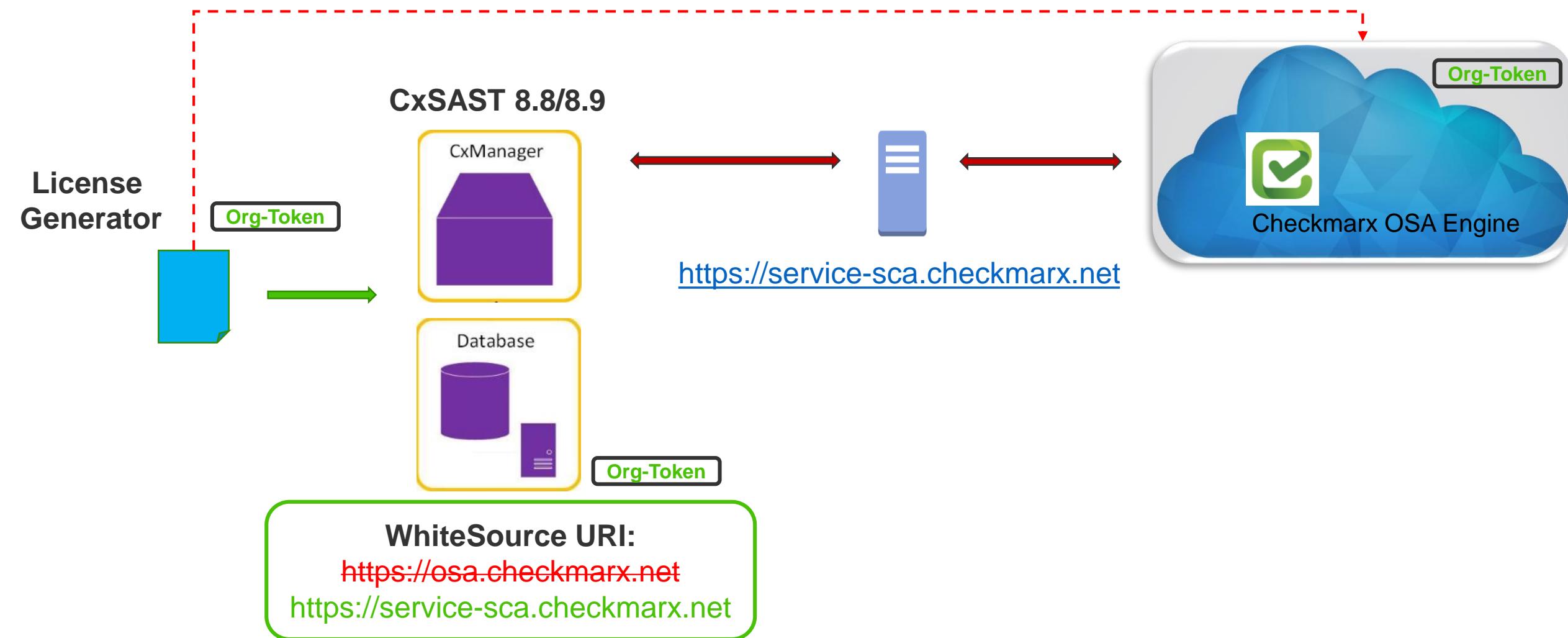
Library Information: struts2-core-2.3.20.jar

Versions: Your version is outdated
2.3.20 Your version (11/21/2014)

/ Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)



/ Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)



/ Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)

Organization Token

87fe54bf-0cef-48d9-b864-961c83064b69

COPY

Scan options

Standard Scan (This option analyses open source identifiers (e.g. file name, accuracy, but less confidentiality.)

Restricted Scan (This option analyses open source fingerprints only (SHA-1) for confidentiality, but less detection accuracy.)

TEST CONNECTION

Organization Token from CxSAST8.9 Web portal

Database Table: CxComponentConfiguration

dbo.CxComponentConfiguration	109	TRUST_ALL_JIRA_SSL_CERTIFICATES	false	Disable SSL cert...
	140	UniqueTeamPerPendingUser	False	Enables unique ...
	228	UnzipLocalPath		NULL
	90	UseEncryptionOnSmtp	False	Defines if SMTP...
	134	UseSSO	True	Enables config...
	97	WaitForEngineTimeoutMinutes	10	Defines the eng...
	93	WebServer		Defines the we...
	187	WhiteSourceOrganizationToken	87fe54bf-0cef-48d9-b864-961c83064b69	White source or...
	189	WhiteSourceRequiredFilesExtensions	6pl;6pm;a;aar;air;al;ar;asp;asp;x;c#;c++;cc;cgi;cp;...	White source re...
	188	WhiteSourceUri	https://service-sca.checkmarx.net	White source uri
	124	ZipFileEncoding	IBM437	Defines the enc...
*	NULL	NULL	NULL	NULL

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Project Scans List

Checkmarx V 8.8.0 HF1 [SDLC]
Expires: 10/1/2018

Dashboard Projects & Scans Management Users & Teams Data Analysis My Profile

Codebashing Services & Support admin admin Logout

Projects & Scans / View Project Scans / DEMO_EasyBuggy

	SCAN DATE	SCAN CO...	RISK LEVEL SCORE	LOC	TEAM	INITIATOR	ORIGIN	SERVER N...	CX VERSI...	COMMEN...	ACCESS	LOCKED	ACTION
<input type="checkbox"/>	● 9/8/2018 ...	9/9/2018 ...	<div style="width: 58%;"><div style="width: 100%;">0 100</div></div> (58)	6931	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/8/2018 ...	9/8/2018 ...	<div style="width: 58%;"><div style="width: 100%;">0 100</div></div> (58)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 H...		Private		
<input type="checkbox"/>	● 9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;"><div style="width: 100%;">0 100</div></div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;"><div style="width: 100%;">0 100</div></div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;"><div style="width: 100%;">0 100</div></div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/6/2018 ...	9/6/2018 ...	<div style="width: 52%;"><div style="width: 100%;">0 100</div></div> (52)	7286	CxServer	admin ad...	Web Portal	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/6/2018 ...	9/6/2018 ...	<div style="width: 64%;"><div style="width: 100%;">0 100</div></div> (64)	7274	CxServer	admin ad...	Web Portal	Localhost	8.8.0.72 H...		Public		
<input type="checkbox"/>	● 9/4/2018 ...	9/4/2018 ...	<div style="width: 70%;"><div style="width: 100%;">0 100</div></div> (70)	7253	CxServer	admin ad...	Web Portal	Localhost	8.8.0.72 H...		Public		

Page size: 10 8 items in 1 pages

/ Create New Project

CxSAST Web Portal – Create New Project – Step 1 – General

The screenshot shows the Checkmarx CxSAST Web Portal interface for creating a new project. The top navigation bar includes links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, and My Profile, along with user account information for 'admin admin'. The main content area is titled 'Projects & Scans / New Project' and displays a step-by-step wizard. The current step is 'General', which is highlighted with a blue arrow. The next steps are 'Location', 'Scheduling', 'Advanced Actions', 'Custom Fields', and 'Data Retention'. A sub-section titled 'Step 1: Enter Project General Settings' contains fields for 'Project Name' (set to 'DEMO123'), 'Preset' (set to 'Checkmarx Default'), 'Configuration' (set to 'Default Configuration'), and 'Team' (set to 'CxServer'). At the bottom of the form are buttons for 'Back', 'Next', 'Cancel', and 'Finish'.

General

Location

Scheduling

Advanced Actions

Custom Fields

Data Retention

Step 1: Enter Project General Settings

Project Name: DEMO123

Preset: Checkmarx Default

Configuration: Default Configuration

Team: CxServer

Back Next Cancel Finish

Create New Project

CxSAST Web Portal – Create New Project – Step 2 – Location

General Location Scheduling Advanced Actions Custom Fields Data Retention

Step 2: Choose Source To Scan

Local Select ? Count Lines

Shared Select ?

Source Control Select ?

Source Pulling Select ?

Exclude Folders ?

Exclude Files ?

/ Create New Project

CxSAST Web Portal – Create New Project – Step 2A – Location

The screenshot displays two side-by-side dialog boxes for connecting to source control systems.

Left Dialog (SVN):

- Choose a Folder from Source Control:** SVN
- Connection Details:**
 - Repository URL: `http://jasonk-laptop:4443/svn/BookMyDoc/BookM`
 - Port Number: 8080
 - Required Authentication
 - User Name: svn
 - Password: ***
 - SSH Authentication
- Buttons:** OK ✓ Cancel ✘

Right Dialog (GIT):

- Choose a Folder from Source Control:** GIT
- Connection Details:**
 - Repository URL: `https://bitbucket.org/cxdemosg/springmvchiberna` Private
 - Authentication:
 - None
 - Credentials
 - Personal Token
 - SSH
 - User Name: cxdemosg@gmail.com
 - Password:
 - Test Connection** Connection Successful
 - GitHub Scan Automation (webhook)
- Buttons:** OK ✓ Cancel ✘

Create New Project

CxSAST Web Portal – Create New Project – Step 3 – Scheduling

The screenshot shows the 'Create New Project' interface in the Checkmarx CxSAST Web Portal. The top navigation bar includes links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, and My Profile. It also features social media integration for Codebashing and Services & Support, and user account information for admin/admin.

The main content area is titled 'Projects & Scans / New Project'. A progress bar at the top indicates the current step: General, Location, **Scheduling**, Advanced Actions, Custom Fields, and Data Retention. A callout box highlights 'Step 3: Choose the scan execution time'.

The scheduling options are as follows:

- None (with a question mark icon)
- Now (with a question mark icon)
- By Schedule (with a question mark icon)

Below these options, there is a section labeled 'Run On Weekdays' with checkboxes for Monday through Sunday. There is also a 'Run Time' field with a clock icon.

At the bottom of the form are buttons for Back, Next, Cancel, and Finish, with the Finish button being highlighted.

/ Create New Project

CxSAST Web Portal – Create New Project – Step 4 – Advanced Actions

General Location Scheduling Advanced Actions Custom Fields Data Retention

Step 4: Define pre and post scan actions

Send pre-scan e-mail to:
jason.khoo@checkmarx.com

Send post-scan e-mail to:
jason.khoo@checkmarx.com

Send scan failure e-mail to:
jason.khoo@checkmarx.com

Run post scan action:
None

Issue Tracking Settings
None Select ✓

/ Create New Project

CxSAST Web Portal – Create New Project – Step 5 – Custom Fields

The screenshot shows the Checkmarx CxSAST Web Portal interface for creating a new project. The top navigation bar includes links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, and My Profile. On the right, there are icons for Codebashing, Services & Support, and user admin information. The main title is "Projects & Scans / New Project". Below the title is a breadcrumb navigation: General > Location > Scheduling > Advanced Actions > Custom Fields > Data Retention. The "Custom Fields" step is currently selected. A sub-step titled "Step 5: Set custom fields" is displayed. The form contains four entries: Scrum Master (Arron), Product Owner (Benson), AppSec (Charlie), and DevOps (Darren).

Scrum Master	Arron
Product Owner	Benson
AppSec	Charlie
DevOps	Darren

/ Create New Project

CxSAST Web Portal – Create New Project – Step 6 – Data Retention

The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a navigation bar with the following items: Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, My Profile, Codebashing, Services & Support, and a user account section for admin. Below the navigation bar, the breadcrumb navigation shows 'Projects & Scans / New Project'. The main content area displays a progress bar with six steps: General, Location, Scheduling, Advanced Actions, Custom Fields, and Data Retention. The 'Data Retention' step is currently selected, indicated by a blue background. A sub-section titled 'Step 6: Set data retention settings' contains a label 'Number of latest scans to keep' followed by an empty input field. The overall interface is clean and modern, using a dark grey header and light grey body sections.

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Queue

The screenshot shows the 'Scan Queue' section of the Checkmarx CxSAST Web Portal. The interface includes a top navigation bar with links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, and My Profile. It also features social media sharing icons for LinkedIn, Facebook, and Twitter, and links for Codebashing, Services & Support, and Logout.

The main content area displays a table of scan jobs. The columns are: POSI..., QUEUED DATE, INITIATOR, ORIGIN, PROJECT NAME, SERVER NAME, LOC, STATUS, and ACTIONS. The table contains six rows of data:

Posi...	Queued Date	Initiator	Origin	Project Name	Server Name	Loc	Status	ACTIONS
2	9/9/2018 4:53:27 AM	admin admin	Web Portal	DEMO_BookMyDoc-master		5978	Queued	↻, 🗑
	9/9/2018 4:53:11 AM	admin admin	Web Portal	DEMO_SVN	Localhost	5978	Working 0%	↻, 🗑
1	9/9/2018 4:53:04 AM	admin admin	Web Portal	DEMO_GitHub		1755	Queued	↻, 🗑
3	9/9/2018 4:52:56 AM	admin admin	Web Portal	DEMO_Benchmark		410649	Queued	↻, 🗑
	9/9/2018 4:52:27 AM	admin admin	Eclipse	DEMO_EasyBuggy	Localhost	6931	Working 71%	↻, 🗑
	9/9/2018 4:51:50 AM	admin admin	CLI	DEMO_CLI_8_7	Localhost	5978	Finished	📄, 🔍

At the bottom left, there are navigation buttons for first, previous, next, and last pages, along with a 'Page size:' dropdown set to 10. At the bottom right, it says '6 items in 1 pages'. Below the table, a summary box provides details for the selected row (Position 2):

Position	2
Queued Date	9/9/2018 4:53:27 AM
Initiator	admin admin

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review

The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a code editor window displaying Java code from `BackDoors.java`. A specific line of code is highlighted in yellow: `ResultSet rs = statement.executeQuery(arrSQL[0]);`. Below the code editor is a sidebar titled "Scan Results" which lists various vulnerabilities categorized by severity: High, Medium, and Low. Under the "High" category, several issues are listed, including "Stored XSS" (164 : F). The main panel below the sidebar contains a table titled "Results" showing a list of findings. The table has columns for Id, Direct, Status, Source Folder, Source File, Source Line, Source Obj, Destination, Destination, Destination, Result State, Result Severity, Assigned User, Ticket ID, and Comments. There are 161 items in total, with 17 pages shown.

Id	Direct	Status	Source Folder	Source File	Source Line	Source Obj	Destination	Destination	Destination	Result State	Result Severity	Assigned User	Ticket ID	Comments
1	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	97	TD	To Verify	High			
2	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	98	TD	To Verify	High			
3	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	99	TD	To Verify	High			
4	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	100	TD	To Verify	High			
5	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	101	TD	To Verify	High			
6	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	106	TD	To Verify	High			
7	Recur...	\WebG...	BackDo...	146	execut...	\WebG...	BackDo...	107	TD	To Verify	High			

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review

The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a code editor window displaying Java code from `BackDoors.java`. The code includes several database operations and a message indicating success in exploiting a query. Below the code editor is a navigation bar with tabs for "Results", "Graph", and "Codebashing". The "Graph" tab is selected, showing a complex dependency graph of nodes representing code components and their interactions. On the left side, a sidebar titled "Scan Results" lists findings categorized by severity: High, Medium, and Low. Under "High", several vulnerabilities are listed, including "Command_Injection", "Connection_String_Injection", "Reflected_XSS_All_Clients", "SQL_Injection", and "Stored_XSS (164 : F)". The "Stored_XSS" entry is highlighted with a blue box. The "Medium" and "Low" categories also contain entries. The main graph view displays multiple interconnected nodes, with one specific node highlighted in red and labeled "org.owasp.webgoat.lessons.BackDoors.addDBEntriesToEC.rs.getString". This node is connected to numerous other nodes, illustrating its role in the application's flow.

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review – OWASP Top 10

The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a code editor window displaying Java code from file \WebGoat_5_2_99347_lines\project\WebContent\lessons\Ajaxlevel.jsp. The code includes imports for java.util.regex.* and org.owasp.webgoat.lessons.Dang, and logic for handling parameters action, field1, and field2.

On the right side of the code editor, a call tree diagram is shown for the variable "field1". It starts with "field1" at the top, which branches down to "getParameter", then "field1", and finally "field1".

The main interface below the code editor has tabs for "Results" (selected), "Graph" (active), and "Codebashing". The "Graph" tab displays a dependency graph for the Java code. The graph shows various nodes representing methods like "getParameters", "searchName", and "value", connected by arrows indicating data flow. A specific node for "Reflected_XSS_All_Clients" is highlighted in red.

The left sidebar contains a navigation menu under "Scan Results OWASP Top 10 2017" for Java, listing categories such as A1-Injection, A2-Broken Authentication, A3-Sensitive Data Exposure, A4-XML External Entities (XXE), A5-Broken Access Control, A6-Security Misconfiguration, and A7-Cross-Site Scripting (XSS). Under A7-XSS, several vulnerabilities are listed, including "Reflected_XSS_All_Clients" (highlighted in red), "Stored_XSS (164 : Found"), "CGI_Reflected_XSS_All_C", and "CGI_Stored_XSS (3 : Fou".

/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review – PCI DSS

\WebGoat_5_2_99347_lines\project\WebContent\lessons\Ajax\eval.jsp

```
1 <%@ page language="java" contentType="text/html; charset=ISO-8859-1" import="java.util.regex.*" import="org.owasp.webgoat.lessons.Dang
2   pageEncoding="ISO-8859-1"%>
3 <%
4 String action = request.getParameter("action");
5 String field1 = request.getParameter("field1");
6 String field2 = request.getParameter("field2");
7 String regex1 = "^[0-9]{3}$"; // any three digits
8 Pattern pattern1 = Pattern.compile(regex1);
9
10 if(action == null) action = "Purchase";
11 <
```

Scan Results **PCI DSS v3.2**

Results Graph Codebashing

Result State Result Severity Assign to User Comments

Graph Type: Full Graph Key Nodes Ends

Java

- PCI DSS (3.2) - 6.5.1 - Injection f...
- PCI DSS (3.2) - 6.5.3 - Insecure d...
- PCI DSS (3.2) - 6.5.4 - Insecure d...
- PCI DSS (3.2) - 6.5.5 - Improper...
- PCI DSS (3.2) - 6.5.7 - Cross-site...
- Reflected_XSS_All_Clients**
- Stored_XSS (164 : Found)
- CGI_Reflected_XSS_All_C...
- CGI_Stored_XSS (3 : Fou...
- HTTP_Response_Splitting
- HttpOnlyCookies (23 : Fou...

The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a code editor window displaying a Java JSP file named eval.jsp. The code contains several security issues, particularly related to XSS and stored XSS. Below the code editor is a navigation bar with tabs for 'Results', 'Graph', and 'Codebashing'. The 'Results' tab is selected, showing a list of findings categorized by PCI DSS requirements. A significant portion of the screen is occupied by a complex graph visualization. This graph maps the flow of data through various methods like 'getParameter', 'searchName', and 'addElement'. Nodes are color-coded to represent different types of data or states, such as red for errors or specific XSS instances. The graph provides a visual representation of how user input flows through the application, highlighting potential attack vectors and the scope of identified vulnerabilities.

/ Software Vulnerability Result

Is XYZ a Vulnerability ?	Vulnerability : Yes (@)	Vulnerability : No (#)
Test Result : Positive (+)	(@) (+) True Positive	(#) (+) False Positive
Test Result : Negative (-)	(@) (-) False Negative	(#) (-) True Negative

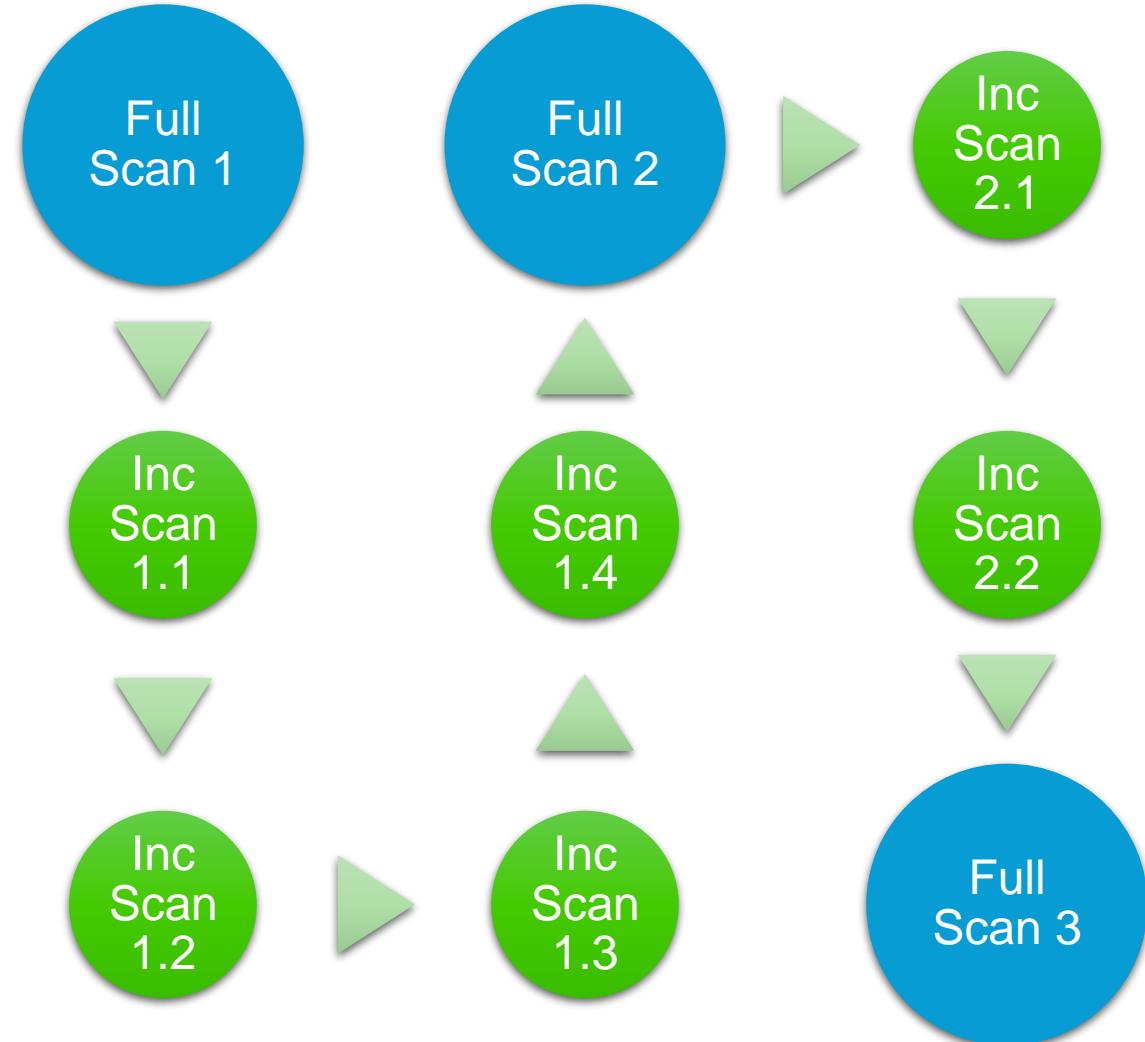
/ Full and Incremental Scans

Full scan

- Comprehensive scanning
- All source files mapping
- Scan result completeness
- Speed 150K ~ 250K LOC

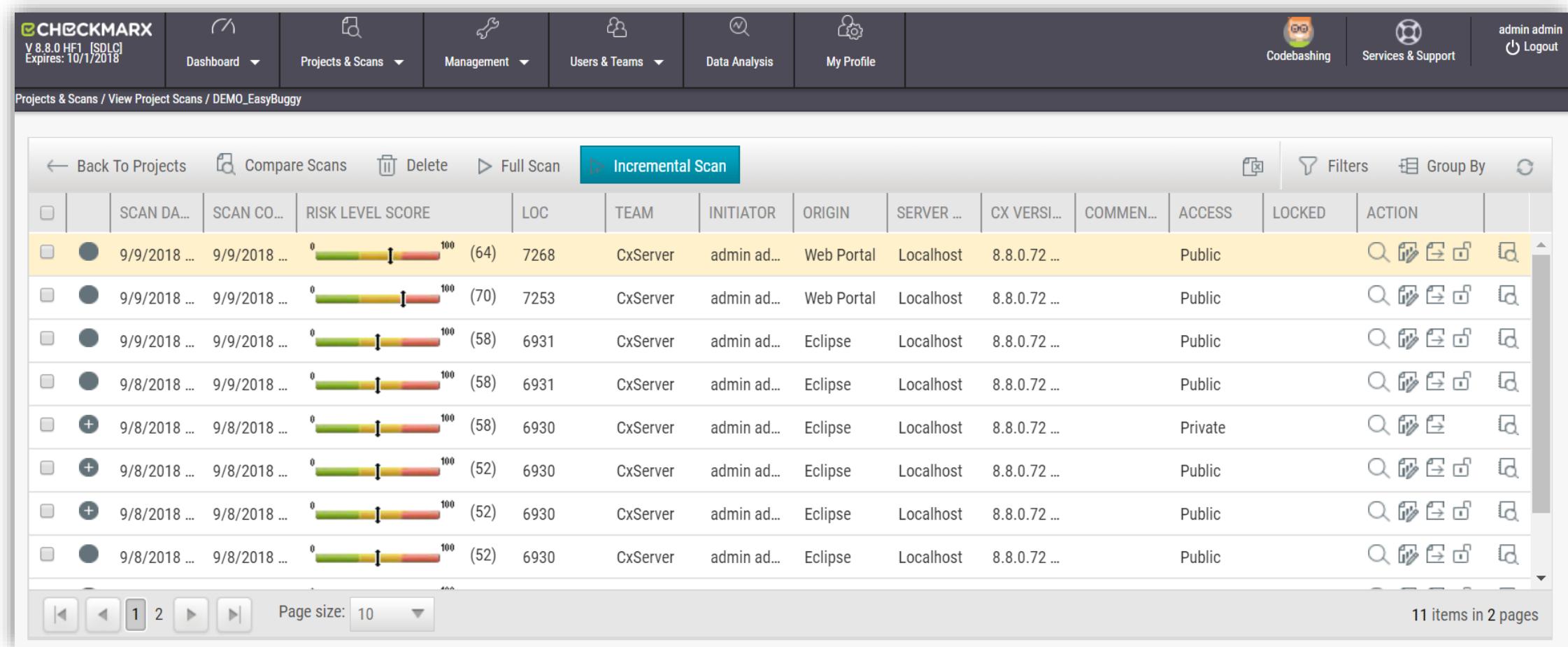
Incremental scan

- Faster scan time
- Up to 7% files modification
- Scan results focus on modified files
- Merge with previous full scan result
- 3~6 Incremental scans between full scan



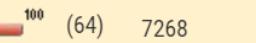
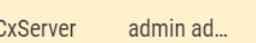
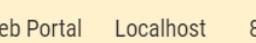
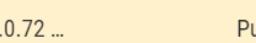
/ Checkmarx CxSAST Web Portal

Full and Incremental Scan Option



The screenshot shows the Checkmarx CxSAST Web Portal interface. At the top, there is a navigation bar with links for Dashboard, Projects & Scans, Management, Users & Teams, Data Analysis, My Profile, Codebashing, Services & Support, and Logout. Below the navigation bar, the URL is displayed as Projects & Scans / View Project Scans / DEMO_EasyBuggy.

In the center, there is a table titled "INCREMENTAL SCAN" with the following columns: SCAN DA..., SCAN CO..., RISK LEVEL SCORE, LOC, TEAM, INITIATOR, ORIGIN, SERVER ..., CX VERSI..., COMMEN..., ACCESS, LOCKED, and ACTION. The table lists eight scan entries, each with a yellow background and a progress bar indicating the risk level. The first two scans are marked as "Public", while the others are marked as "Private". The last two scans have a plus sign icon next to them. The table includes standard data grid controls like sorting and filtering icons.

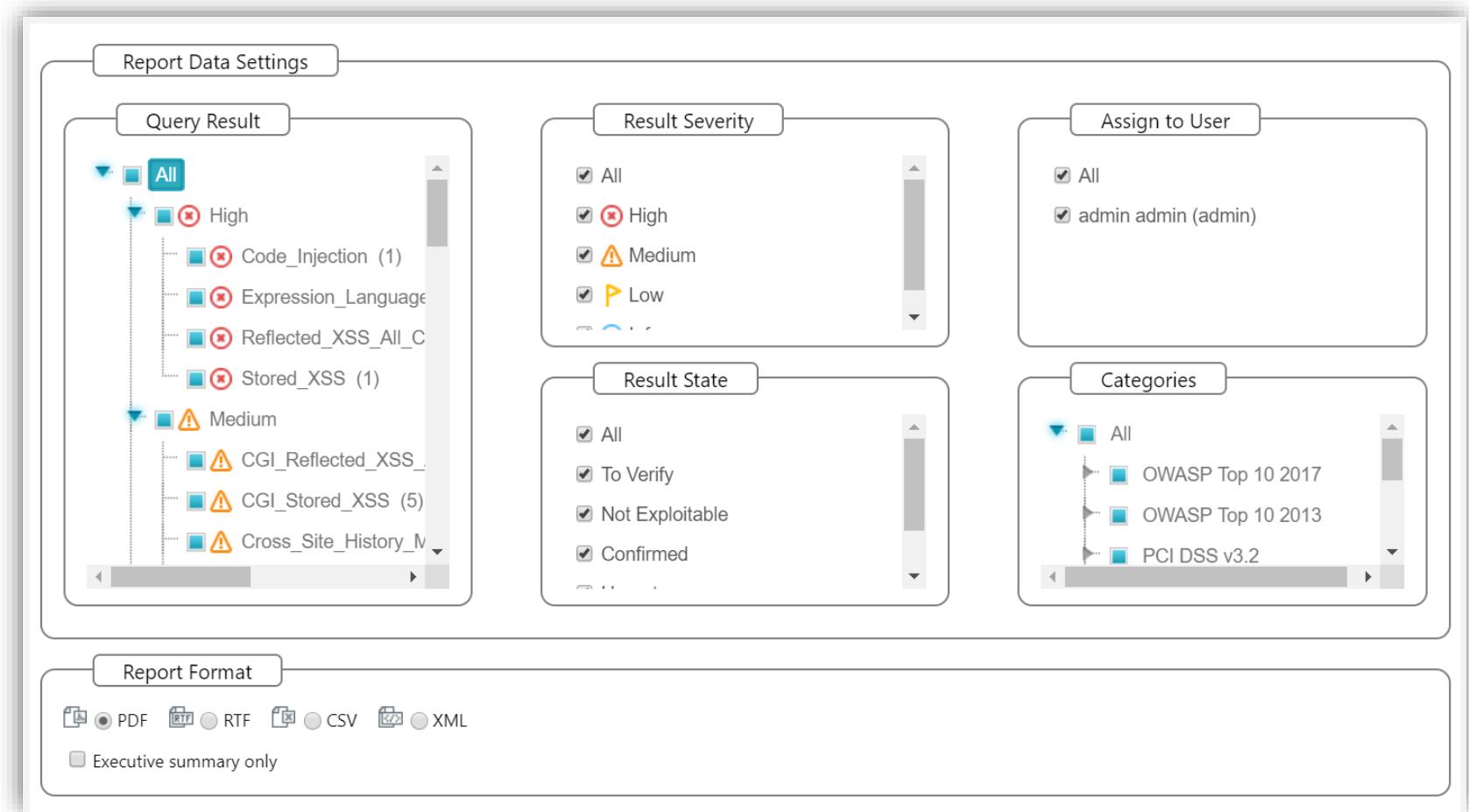
SCAN DA...	SCAN CO...	RISK LEVEL SCORE	LOC	TEAM	INITIATOR	ORIGIN	SERVER ...	CX VERSI...	COMMEN...	ACCESS	LOCKED	ACTION
9/9/2018 ...	9/9/2018 ...	<div style="width: 64%;">0  100</div> (64)	7268	CxServer	admin ad...	Web Portal	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/9/2018 ...	9/9/2018 ...	<div style="width: 70%;">0  100</div> (70)	7253	CxServer	admin ad...	Web Portal	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/9/2018 ...	9/9/2018 ...	<div style="width: 58%;">0  100</div> (58)	6931	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/8/2018 ...	9/9/2018 ...	<div style="width: 58%;">0  100</div> (58)	6931	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/8/2018 ...	9/8/2018 ...	<div style="width: 58%;">0  100</div> (58)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Private		View Edit Delete Details
9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;">0  100</div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;">0  100</div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Public		View Edit Delete Details
9/8/2018 ...	9/8/2018 ...	<div style="width: 52%;">0  100</div> (52)	6930	CxServer	admin ad...	Eclipse	Localhost	8.8.0.72 ...		Public		View Edit Delete Details

At the bottom, there are navigation buttons for page 1 of 2, a page size dropdown set to 10, and a message indicating "11 items in 2 pages".

/ Checkmarx CxSAST Web Portal

Scan Report

- Configurable template
- PDF, RTF, CSV, XML
- Compliance chart
- Executive summary



/ Scan Notification

CxSAST Project Scan – Email Notification

The screenshot shows an email inbox interface with a list of unread emails on the left and a detailed view of a specific email on the right.

Email List (Left):

- Today:**
 - Checkmarx Analyzer - Scan of project DEMO_GitHub ... (4:58 AM)
 - Checkmarx Analyzer - Scan of project DEMO_GitHub i... (4:56 AM)
- Last Week:**
 - Checkmarx Analyzer - Scan of project DEMO_GitHub ... (Tue 4/9)
 - Checkmarx Analyzer - Scan of project DEMO_GitHub i... (Tue 4/9)
- Two Weeks Ago:**
 - Checkmarx Analyzer - Scan of project DEMO_GitHub ... (29/8/2018)
 - Checkmarx Analyzer - Scan of project DEMO_GitHub i... (29/8/2018)

Email View (Right):

From: Checkmarx Analyzer <cxdemo123456@gmail.com>
Date: Sun 9/9/2018 4:58 AM
To: Jason Khoo
Subject: Scan of project DEMO_GitHub completed successfully

Attachment: Report.pdf (132 KB)

Scan details:

Project Name: DEMO_GitHub
Owner: admin
Source location: <https://github.com/payatu/diva-android.git> (/refs/heads/master)
Preset: Checkmarx Default
Configuration: Default Configuration
Start time: 9/9/2018 4:56:05 AM
End time: 9/9/2018 4:57:50 AM

/ Users Management

CxSAST Web Portal – Organizational – Tree Branch View

The screenshot displays the CxSAST Web Portal interface, specifically the 'Organizational – Tree Branch View' section. The top navigation bar includes links for Dashboard, Projects & Scans, Management, Users & Teams (selected), Data Analysis, My Profile, and user account information (Codebashing, Services & Support, Logout). The main content area shows the organizational tree on the left and user details on the right.

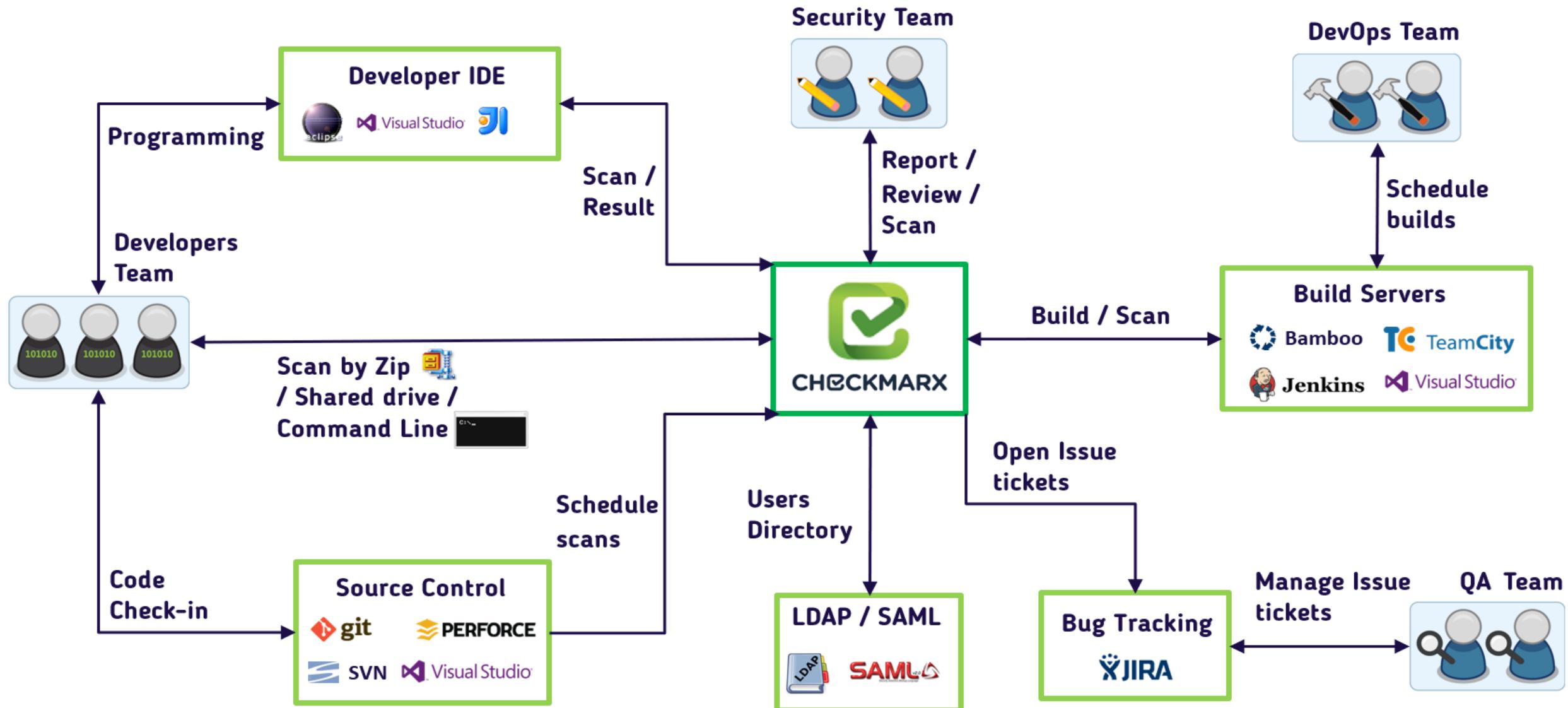
Organizational Tree:

- + Create New Service Provider
- Delete
- CxServer
 - SP
 - Company
 - Team_A
 - Team_B
 - Team_C

Users:

E-MAIL	FULL NAME	ROLE
admin@cx.com	admin admin	ServerManager

/ Checkmarx CxSAST User Group



/ Exercise 3: New Project & Scan

Create 5 Projects and perform Scans with Email notification:

CxSAST projects : Zip

GIT : <https://github.com/cx-jason>

BitBucket : ssh://bitbucket.org/cxdemosg/EasyBuggy.git

CxOSA : Zip

/ Java Project: EasyBuggy Result Review & Remediation

Project EasyBuggy

<https://github.com/cx-jason/easybuggy-1.3.9>



EasyBuggy Don't catch any bugs!

⚠ Warning: Several links cause severe memory leaks increase a CPU usage rate. They can make your computer unstable.
The result may change depending on JRE type / version, Java option, OS, hardware (memory, CPU) or etc.

Vulnerabilities

XSS, SQL Injection, LDAP injection, and so on:

- XSS (Cross Site Scripting): There is a cross site scripting vulnerability in this page.
- SQL Injection: There is an SQL injection vulnerability in this page.
- LDAP Injection: There is an LDAP injection vulnerability in this page.
- Code Injection: There is a code injection vulnerability in this page.
- OS Command Injection: There is an OS command injection vulnerability in this page.
- Mail Header Injection: There is a mail header injection vulnerability in this page.
- Null Byte Injection: There is a null byte injection vulnerability in this page.
- Size Unrestricted File Upload: This page is vulnerable for attacks such as DoS because there are no limits.
- Extension Unrestricted File Upload: This page is vulnerable for attacks such as code injection because there are no limits.
- Login page that allows Open Redirect: There is an open redirect vulnerability in this login page.
- Login page that allows brute-force attacks: This login page is vulnerable for brute-force attack because there are no limits.
- Login page that allows session fixation attacks: This login page is vulnerable for session fixation attack because there are no limits.
- Verbose Authentication Error Messages: It is easy to guess an account who can log in because auth messages are verbose.

cx-jason / easybuggy-1.3.9

Code Issues Pull requests Projects Wiki Security Insights Settings

No description, website, or topics provided. Edit

Manage topics

4 commits 1 branch 0 releases 1 contributor Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

cx-jason Add files via upload Latest commit 8515485 13 hours ago

java/org/t246osslab/easybuggy	Add files via upload	2 days ago
osa	Add files via upload	13 hours ago
resources	Add files via upload	2 days ago
webapp	Add files via upload	2 days ago
LICENSE	Add files via upload	2 days ago
README.jp.md	Add files via upload	2 days ago
README.md	Add files via upload	2 days ago
catalina.policy	Add files via upload	2 days ago
pom.xml	Add files via upload	2 days ago

README.md

build passing License Apache 2.0 release v1.4.0

EasyBuggy



EasyBuggy is a broken web application in order to understand behavior of bugs and vulnerabilities, for example, memory leak, deadlock, JVM crash, SQL injection and so on.

/ Exercise 4: Scan Result Review & Remediation

Remediation for the SQL Injection vulnerabilities

The screenshot shows the Checkmarx application interface. On the left, the Java code for `SQLInjectionServlet.java` is displayed, highlighting the SQL query construction logic. On the right, a vertical stack of boxes indicates the flow of untrusted input from user input "name" through various methods like `getParameter`, `trim`, and `name` to the final `executeQuery` call.

`\easybuggy-1.3.9\src\main\java\org\t246osslab\easybuggy\vulnerabilities\SQLInjectionServlet.java`

```
55     } catch (Exception e) {
56         log.error("Exception occurs: ", e);
57     }
58 }
59
60 private String selectUsers(String name, String password, HttpServletRequest req) {
61     Connection conn = null;
62     Statement stmt = null;
63     ResultSet rs = null;
64     String result = getErrMsg("msg.error.user.not.exist", req.getLocale());
65     try {
66         conn = DBClient.getConnection();
67         stmt = conn.createStatement();
68         rs = stmt.executeQuery("SELECT name, secret FROM users WHERE ispublic = 'true' AND name='"
69             + name + "' AND password='" + password + "'");
70         StringBuilder sb = new StringBuilder();
71         while (rs.next()) {
72             sb.append("<tr><td>" + rs.getString("name") + "</td><td>" + rs.getString("secret") + "</td></tr>");
73         }
74         if (sb.length() > 0) {
75             result = "<table class=\"table table-striped table-bordered table-hover\" style=\"font-size:small;\"><thead>"
76                 + getMsg("label.name", req.getLocale()) + "</thead><tbody>"
77                 + getMsg("label.secret", req.getLocale()) + "</tbody>" + sb.toString() + "</table>";
78         }
79     } catch (Exception e) {
80         log.error("Exception occurs: ", e);
81     } finally {
```

Scan Results Severity

Java

High

- Code_Injection (1 : Found) (?)
- Expression_Language_Injection_
- Reflected_XSS_All_Clients (25)
- SQL_Injection (2 : Found) (?)**
- Stored_XSS (5 : Found) (?)

The application's `selectUsers` method executes an SQL query with `executeQuery`, at line 60 of `easybuggy-1.3.9\src\main\java\org\t246osslab\easybuggy\vulnerabilities\SQLInjectionServlet.java`. The application constructs this SQL query by embedding an untrusted string into the query without proper sanitization. The concatenated string is submitted to the database, where it is parsed and executed accordingly. The attacker would be able to inject arbitrary data into the SQL query, by simply altering the user input "`"name"`", which is read by the `service` method at line 24 of `easybuggy-1.3.9\src\main\java\org\t246osslab\easybuggy\vulnerabilities\SQLInjectionServlet.java`. This input then flows through the code to the database server, without sanitization. This may enable an SQL Injection attack.

Result State	Result Severity	Assign To User	Comments	Save Scan Subset	Open Ticket	Filters	Group By	
New	New	\easybuggy...	SQLInj... 27	"name"	\easybuggy...	SQLInj... 69	executeQue... To Verify	High
New	New	\easybuggy...	SQLInj... 28	"password"	\easybuggy...	SQLInj... 69	executeQue... To Verify	High

CxSAST Integration

/CxSAST REST API

/CxSAST CxConsole, Command Line Interface

```
[2019-10-10 00:53:38,927 INFO ] Verbose mode is activated. All messages and events will be sent to the console or log file.
[2019-10-10 00:53:38,927 INFO ] CxConsole version 8.80.2
[2019-10-10 00:53:38,927 INFO ] CxConsole scan session started
[2019-10-10 00:53:38,927 INFO ]
[2019-10-10 00:53:38,942 INFO ] Default configuration file location: C:\CxWorkSpace\TS\03 CxConsolePlugin\CxConsolePlugin-8.80.2\config\cx_console.properties
[2019-10-10 00:53:40,286 INFO ] Command line parameters were checked successfully
[2019-10-10 00:53:40,286 INFO ] Default log file location: C:\CxWorkSpace\TS\03 CxConsolePlugin\CxConsolePlugin-8.80.2\logs\cx_console.log
[2019-10-10 00:53:44,561 INFO ] Server connectivity test succeeded to: http://localhost
[2019-10-10 00:53:44,572 INFO ] Project name is DEMO_CLI_BookMyDoc2
[2019-10-10 00:53:44,573 INFO ] Logging into Checkmarx server.
[2019-10-10 00:53:44,830 INFO ] Login was completed successfully
[2019-10-10 00:53:44,849 INFO ] Team: "CxServer" was validated in server
[2019-10-10 00:53:44,849 INFO ] Preset: "Checkmarx Default" was validated in server
[2019-10-10 00:53:44,871 INFO ] Engine configuration: "Default Configuration" was validated in server
[2019-10-10 00:53:44,882 INFO ] Project id for project: "DEMO_CLI_BookMyDoc2" was not found in server
[2019-10-10 00:53:44,883 INFO ] SAST scan prerequisites were validated successfully
[2019-10-10 00:53:44,956 INFO ] New project was created successfully
[2019-10-10 00:53:44,987 INFO ] Zipping files from: C:\CxSharedSrc\BookMyDoc-master Please wait
[2019-10-10 00:53:45,242 INFO ] Zipping complete with 90 files.
[2019-10-10 00:53:45,242 INFO ] Compressed file size is: 2 MB
[2019-10-10 00:53:45,266 INFO ] Uploading zipped source files to server, please wait.
[2019-10-10 00:53:45,319 INFO ] Zipped source files were uploaded successfully
[2019-10-10 00:53:45,319 INFO ] Request SAST scan
[2019-10-10 00:53:45,333 INFO ] SAST scan created successfully: Scan ID is 1000093
[2019-10-10 00:53:45,333 INFO ] Full scan initiated, Waiting for SAST scan to finish.
[2019-10-10 00:53:45,640 INFO ] Total scan worked: 0%
[2019-10-10 00:53:45,640 INFO ] Current Stage: New
[2019-10-10 00:54:00,640 INFO ] Total scan worked: 0%
[2019-10-10 00:54:00,641 INFO ] Current Stage: Queued
[2019-10-10 00:54:15,642 INFO ] Total scan worked: 0%
[2019-10-10 00:54:15,642 INFO ] Current Stage: Scanning - Engine starts scan
[2019-10-10 00:54:30,643 INFO ] Total scan worked: 0%
[2019-10-10 00:54:30,643 INFO ] Current Stage: Scanning - Engine starts scan
[2019-10-10 00:54:45,641 INFO ] Total scan worked: 30%
[2019-10-10 00:54:45,641 INFO ] Current Stage: Scanning - Stage # 21 of 33
```

CxSAST Integration with Jenkins Portal

Jenkins

Jenkins > Jenkins_App1 >

Project Jenkins_App1

Jenkins_App1

Back to Dashboard Status Changes Workspace Build Now Delete Project Configure Rename

Build History trend →

find #10 Sep 7, 2018 12:55 PM
#9 Sep 7, 2018 12:44 PM
#8 Sep 7, 2018 11:53 AM
#7 Sep 7, 2018 11:43 AM
#6 Sep 7, 2018 11:38 AM
#5 Sep 7, 2018 11:30 AM
#4 Sep 7, 2018 11:10 AM
#3 Sep 7, 2018 10:45 AM
#2 Aug 20, 2018 4:03 PM
#1 Aug 20, 2018 4:01 PM

RSS for all RSS for failures

Checkmarx Report

CxSAST Vulnerabilities Status

Results PDF Report

High - 0 Medium - 29 Low - 14

0 NEW 0 NEW 1 NEW

CxOSA Vulnerabilities & Libraries

Results

Libraries: 4 Vulnerable and Outdated Libraries

High - 19 Medium - 3 Low - 2

No Known Vulnerability Libraries

CxSAST Full Report

Start: 07/09/18 12:55 End: 07/09/18 12:58 Files: 70 Code Lines: 8,339

Medium 29 Vulnerability Use_of_Cryptographically_Weak_PRNG

Analyze Results PDF Report

General Source Code Management Build Triggers Build Environment Build Post-build Actions

CxSAST Scan

Use default server credentials (Server URL: http://localhost)

Checkmarx project name: DEMO_Jenkins_App1

Project Name Validated Successfully

Existing projects appear in a completion list when server url is provided (up to 20)

Team: CxServer

Preset: Checkmarx Default

Use Global Include/Exclude Settings

Exclude Folders:

Include/Exclude Wildcard Patterns:

```
!**/_cvs/**/, !**/.svn/**/, !**/.hg/**/, !**/.git/**/, !**/.bzr/**/, !**/.bin/**/, !**/obj/**/, !**/backup/**/, !**/.idea/**/, !**/.DS_Store, !**/.ipr, !**/.iws, !**/.bak, !**/.tmp, !**/.aac, !**/.aif, !**/.iff, !**/.m3u, !**/.mid, !**/.mp3, !**/.mpa, !**/.ra, !**/.wav, !**/.wma, !**/.3g2, !**/.3gp, !**/.asf, !**/.asx, !**/.avi, !**/.flv, !**/.mov, !**/.mp4, !**/.mpg, !**/.rm, !**/.swf, !**/.vob, !**/.wmv, !**/.bmp, !**/.gif, !**/.jpg, !**/.png, !**/.psd, !**/.tif, !**/.swf, !**/.jar, !**/.zip, !**/.rar, !**/.exe, !**/.dll, !**/.pdb, !**/.7z,
```

Specific Include/Exclude Settings

CxSAST Integration with Eclipse Plugin

The screenshot illustrates the integration of the CxSAST plugin into the Eclipse IDE. The interface includes:

- Project Explorer:** Shows a Java project named "Web1".
- Code Editor:** Displays Java code for XSSServlet.java, which includes logic for generating an HTML form with user input.
- Context Menu:** Opened over the code editor, showing options for "CxViewer" such as "Scan" and "Incremental Scan".
- CxViewer Results:** A pane showing a dependency graph of code snippets. Nodes include "userid", "getParam", "trim", "userId", and various string manipulation methods like "append", "reverse", and "append".
- CxViewer Path:** A tree view showing the path of analyzed code segments.
- Graph Navigation:** A pane showing the analysis results for the code.
- Bottom Right Panel:** Displays a summary of findings from the analysis, categorized by severity (High, Medium) and type (e.g., Code_Injection, SQL_Injection).

/ Exercise 5: CxSAST Integration

Create new Projects / Scans from :

- Jenkins – Freestyle project and Pipeline
- CxConsole
 - <https://checkmarx.atlassian.net/wiki/spaces/KC/pages/52560015/CxConsole+cxSAST+CLI>
- REST API – start scan on existing Project
- Eclipse

/ Question and Discussion





Partner Technical Enablement

Day 2

CxAudit Session

CxAudit

CxAudit

- Standalone module
- Query language
- CxQL customization
- Manage FP and FN
- Identify data flow
- Independent CxEngine

The screenshot shows the CxAudit IDE interface. The top menu bar includes File, Edit, View, Query, Results, Window, and Help. The toolbar contains icons for Disable Code Slicing, Enable Path Indentation, and other tools. The main window has tabs for demo.xml, sample.xml, xss_sample1.java, xss_sample3.java, and xss_sample2.java. The xss_sample2.java tab is active, displaying Java code:

```
import javax.servlet.*;
import javax.servlet.http.*;
import javax.servlet.jsp.*;
import org.apache.jasper.runtime.*;
import cmt.Security.*;

public class BookDetail_jsp extends HttpJspBase {

    public static String loadDriver () {
        String bookName = request.getParameter("bookName"); // bookName stores user input
        String vBookName = Security.validate(bookName); // vBookName is supposed to be the "cle

        out.println(vBookName); // print vbookName to the page
    }
}
```

The code editor highlights the line `String bookName = request.getParameter("bookName");` in yellow, indicating it is a potential security concern. To the right, a 'Path' pane shows the data flow from the parameter to its validation and finally its output:

- ""bookName""
- getParameter
- bookName
- bookName
- validate
- vBookName
- vBookName
- println

Below the code editor, there are tabs for Query, Results, Comments, and Debug Messages. The Queries tab lists various injection vulnerabilities:

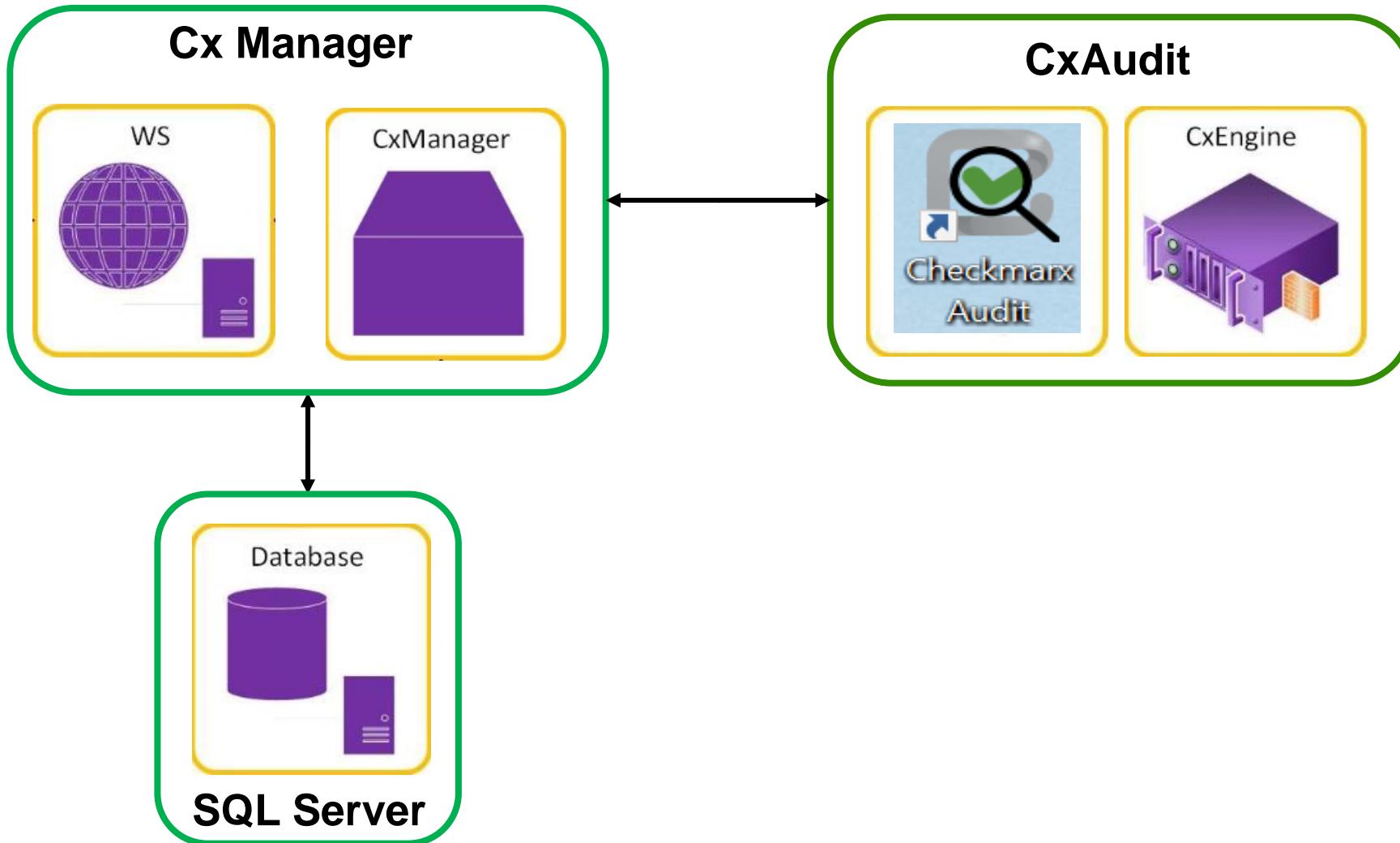
- Connection_String_Injection
- Deserialization_of_Utrust
- Deserialization_of_Utrust
- Expression_Language_Inje
- LDAP_Injection
- Reflected_XSS_All_Clients
- Resource_Injection
- Second_Order_SQL_Injec
- SQL_Injection
- Stored_XSS
- XPath_Injection
- Java_Low_Visibility

The Query Source tab displays the CxList logic:

```
CxList inputs = Find_Interactive_Inputs();
CxList outputs = Find_XSS_Outputs();

CxList sanitized = Find_XSS_Sanitize() + Find_DB_In() + Find_Files_Open() - Find_De
result = inputs.InfluencingOnAndNotSanitized(outputs, sanitized, CxList.InfluenceAll);
result = result.ReduceFlow(CxList.ReduceFlowType.ReduceSmallFlow);
```

CxAudit Architecture



/ Checkmarx CxSAST Web Portal

CxSAST Web Portal – Query Language Viewer

The screenshot shows the Checkmarx CxSAST Web Portal interface, specifically the Query Language Viewer. The top navigation bar includes links for Dashboard, Projects & Scans, Management (selected), Users & Teams, Data Analysis, My Profile, and user account information (admin admin). The left sidebar shows the current path: Management / Scan Settings / Query Viewer. The main content area has two main sections: 'Queries' on the left and 'Cx Description' on the right.

Queries: A list of detection queries, each with a red circular icon and a delete button. The 'SQL_Injection' query is highlighted with a blue background and a white border.

Cx Description:

- SQL_Injection**: The selected query description.
- Risk**: A section describing the risk of SQL injection.
- What might happen**: A detailed description of the potential impact of an attacker gaining access to system data.

Source: The underlying code for the SQL_Injection query:

```
1 CxList db = Find_DB_In() - Find DAL_DB();
2 CxList inputs = Find_Interactive_Inputs();
3 CxList sanitized = Find_SQL_Sanitize();
4
5 result = inputs.InfluencingOnAndNotSanitized(db, sanitized, CxList.InfluenceAlgorithmCalculation.NewAlgorithm);
```

Language Hash: 0129784306302162 Change Date: 8/23/2018

/ Exercise 6: CxAudit Session

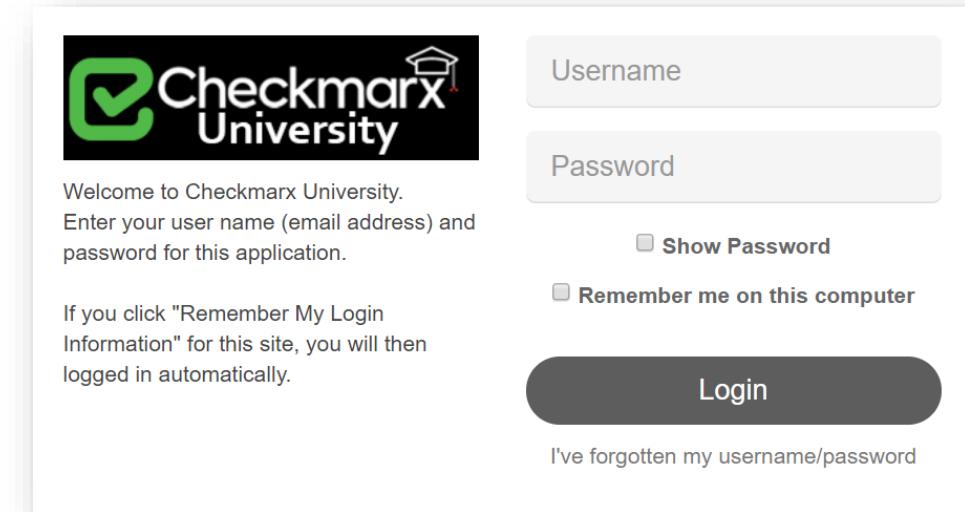
CxAudit demonstration and practice:

- Add customize sanitization function
- False-negative result

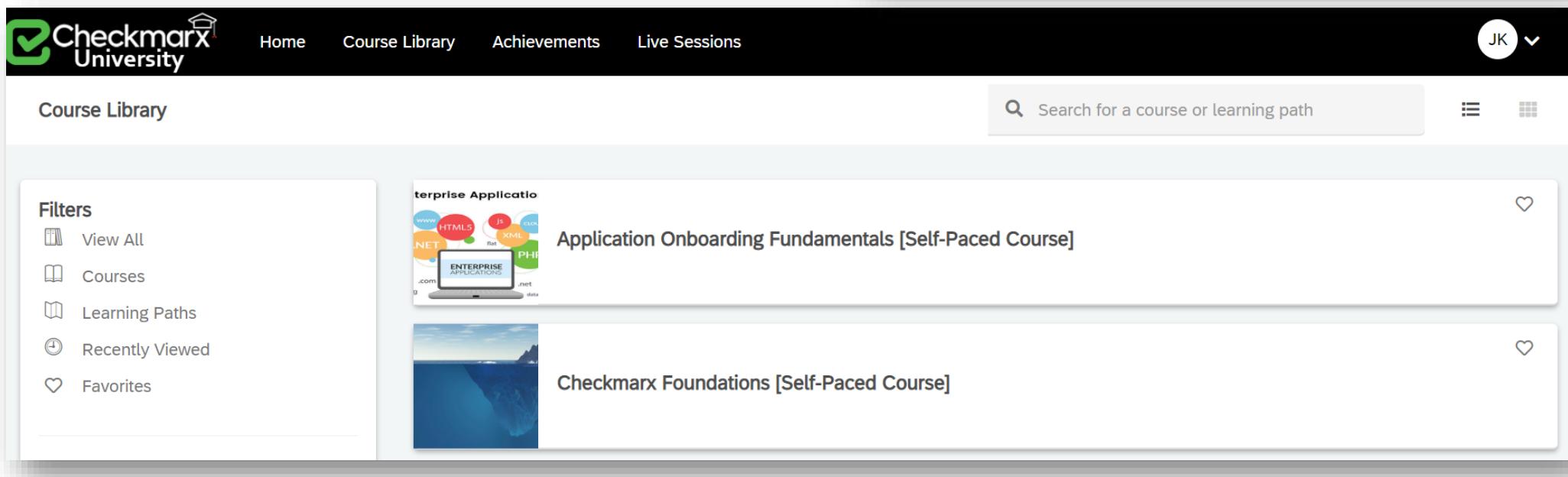
CxUniversity

/ Exercise 7: CxUniversity

<https://checkmarxuniversity.litmos.com>



The image shows the login page for Checkmarx University. It features a logo with a green checkmark icon and the text "Checkmarx University". Below the logo, there is a welcome message: "Welcome to Checkmarx University. Enter your user name (email address) and password for this application." There are two input fields for "Username" and "Password", each with a "Show Password" link. A "Remember me on this computer" checkbox is also present. A large "Login" button is at the bottom, and a "I've forgotten my username/password" link is below it.



The image shows the "Course Library" section of the Checkmarx University website. At the top, there is a navigation bar with links for "Home", "Course Library", "Achievements", and "Live Sessions". On the right, there is a user profile icon labeled "JK" and a search bar with the placeholder "Search for a course or learning path". The main area displays two course cards. The first card is titled "Application Onboarding Fundamentals [Self-Paced Course]" and features a thumbnail image of a computer monitor displaying various programming technologies like HTML5, JS, XML, and PHP. The second card is titled "Checkmarx Foundations [Self-Paced Course]" and has a thumbnail image of a blue landscape. To the left of the cards, there is a sidebar titled "Filters" with options: "View All", "Courses", "Learning Paths", "Recently Viewed", and "Favorites".

CxSAST / CxOSA Demonstration

/ Exercise 8: CxSAST / CxOSA Demonstration



Computer



Recycle Bin



Google
Chrome



Notepad++



Checkmark
Portal



Checkmark
Audit



Cx_Demo_C...
- Shortcut



eclipse.exe -
Shortcut

Think

/ Question and Discussion



Thank you

Email: jason.khoo@checkmarx.com

www.checkmarx.com