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-CxTrainning-r426 -APJ_Partner-7-13--10-2019.csv

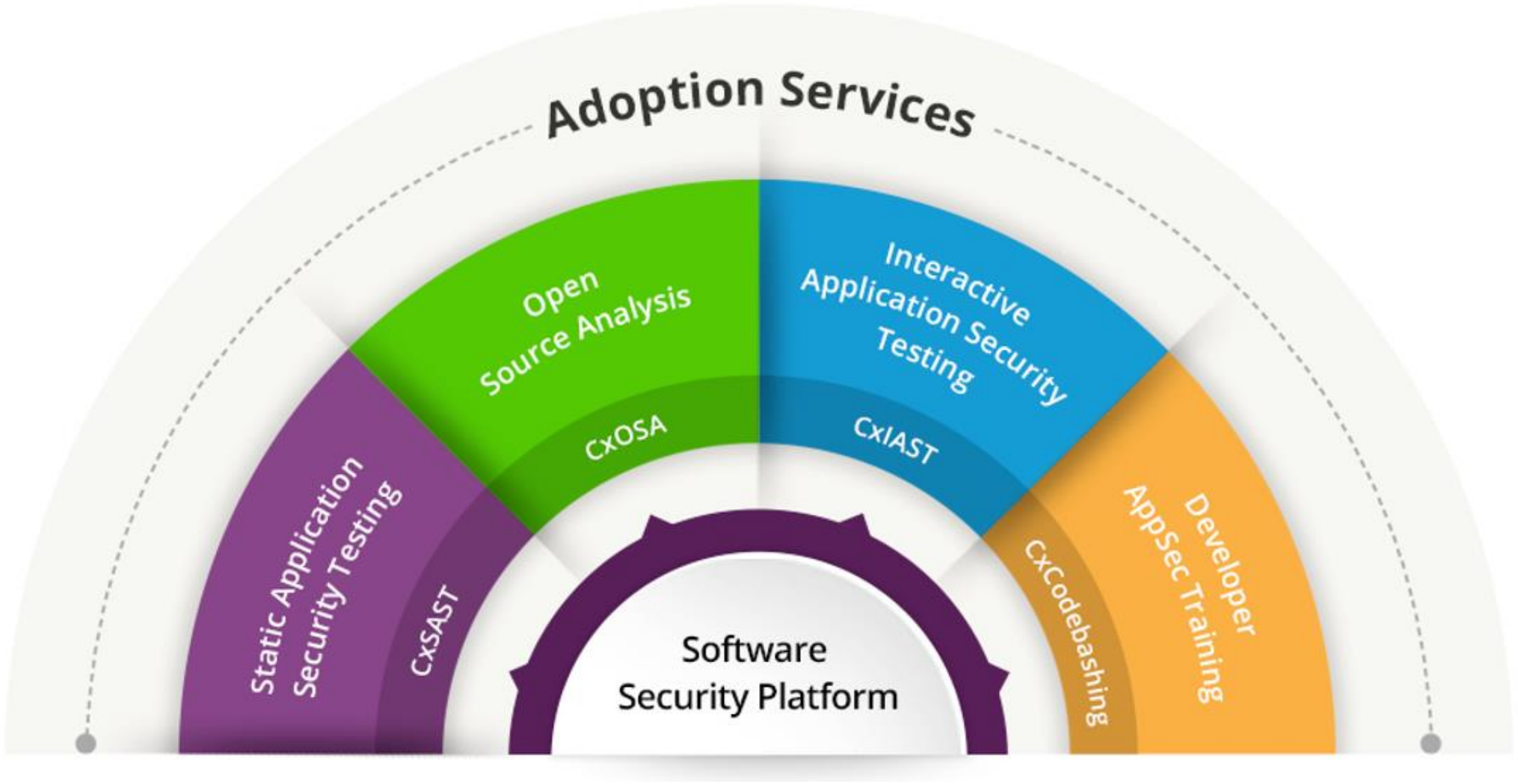
Training Resource on GitHub:
https://github.com/cx-jason

CxSAST Web Trial Portal:
https://cxapactrial.checkmarx.net

/ Software Security Platform

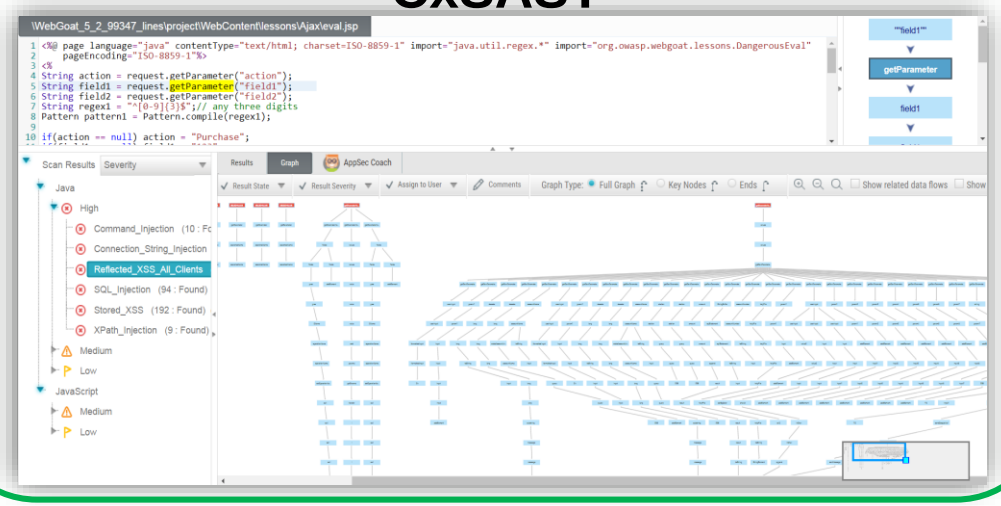
Checkmarx

Checkmarx Software Security Platform

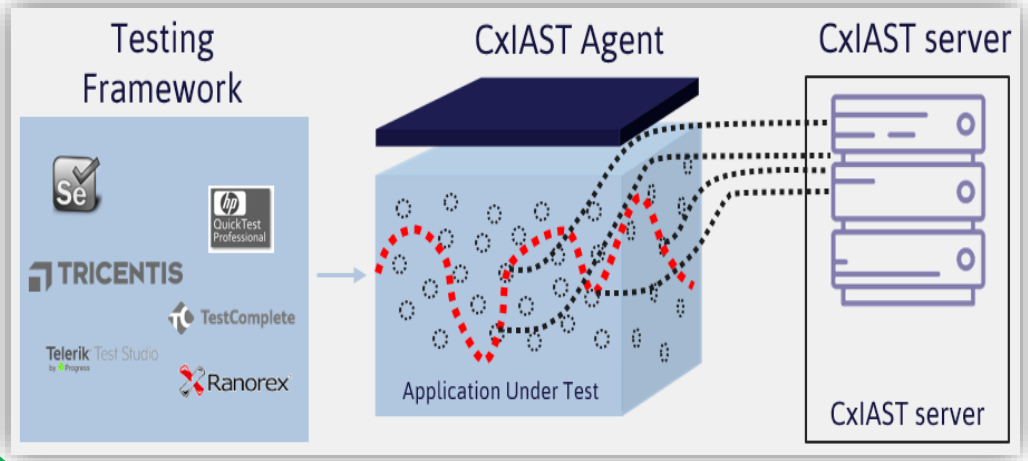


Checkmarx Software Security Platform

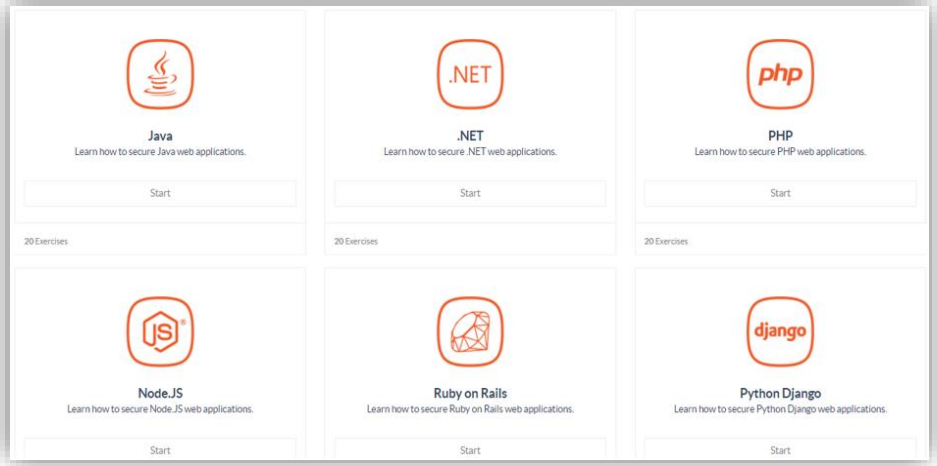
CxSAST



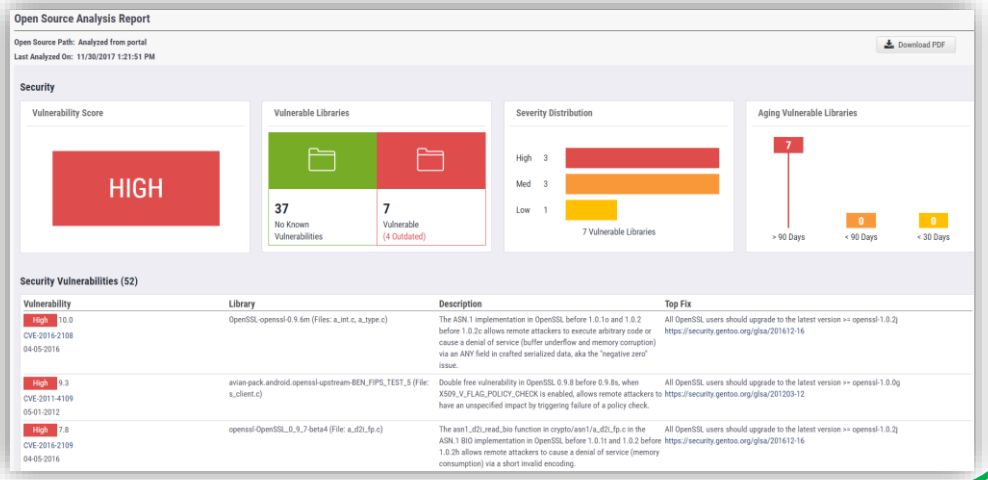
CxIAST



CodeBashing

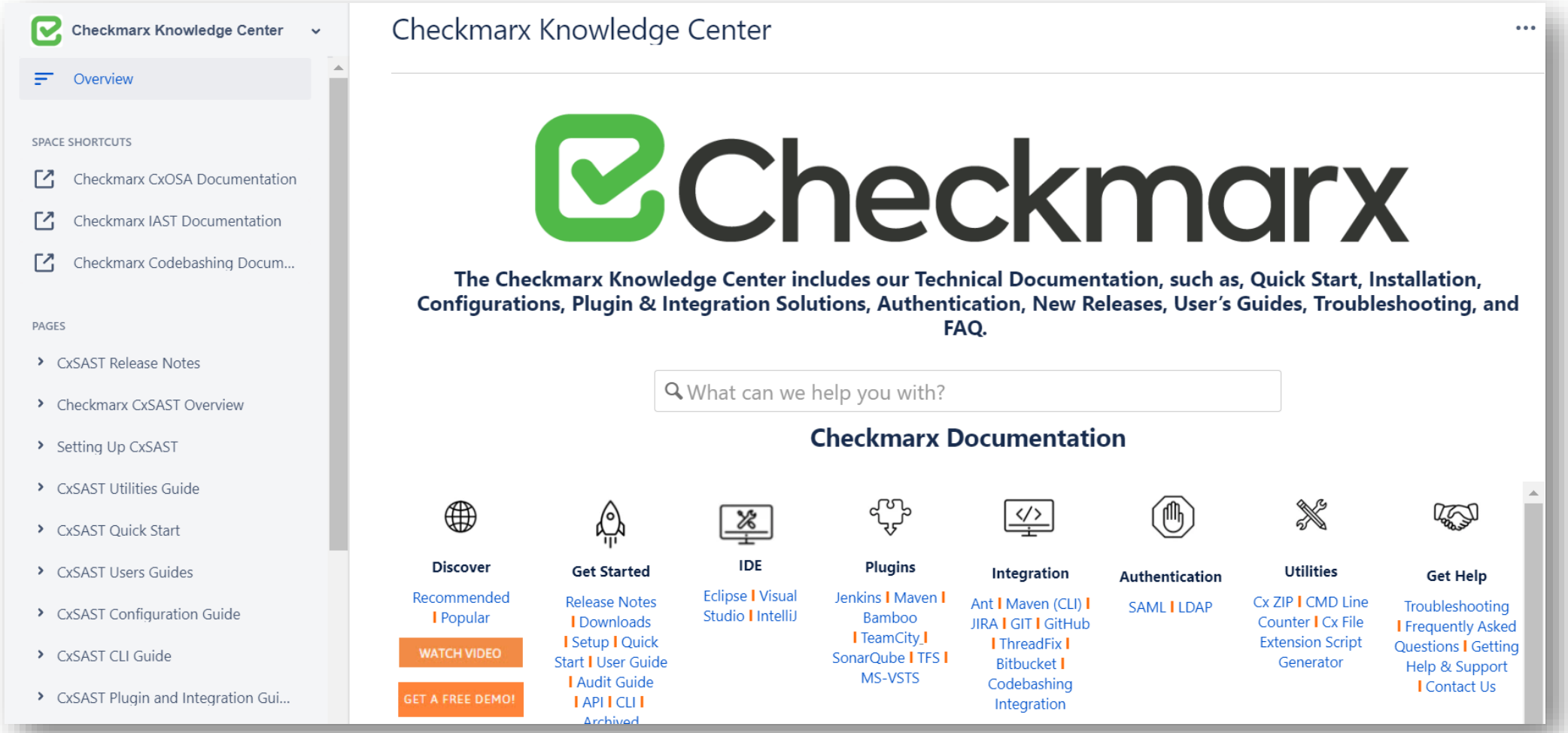


CxOSA

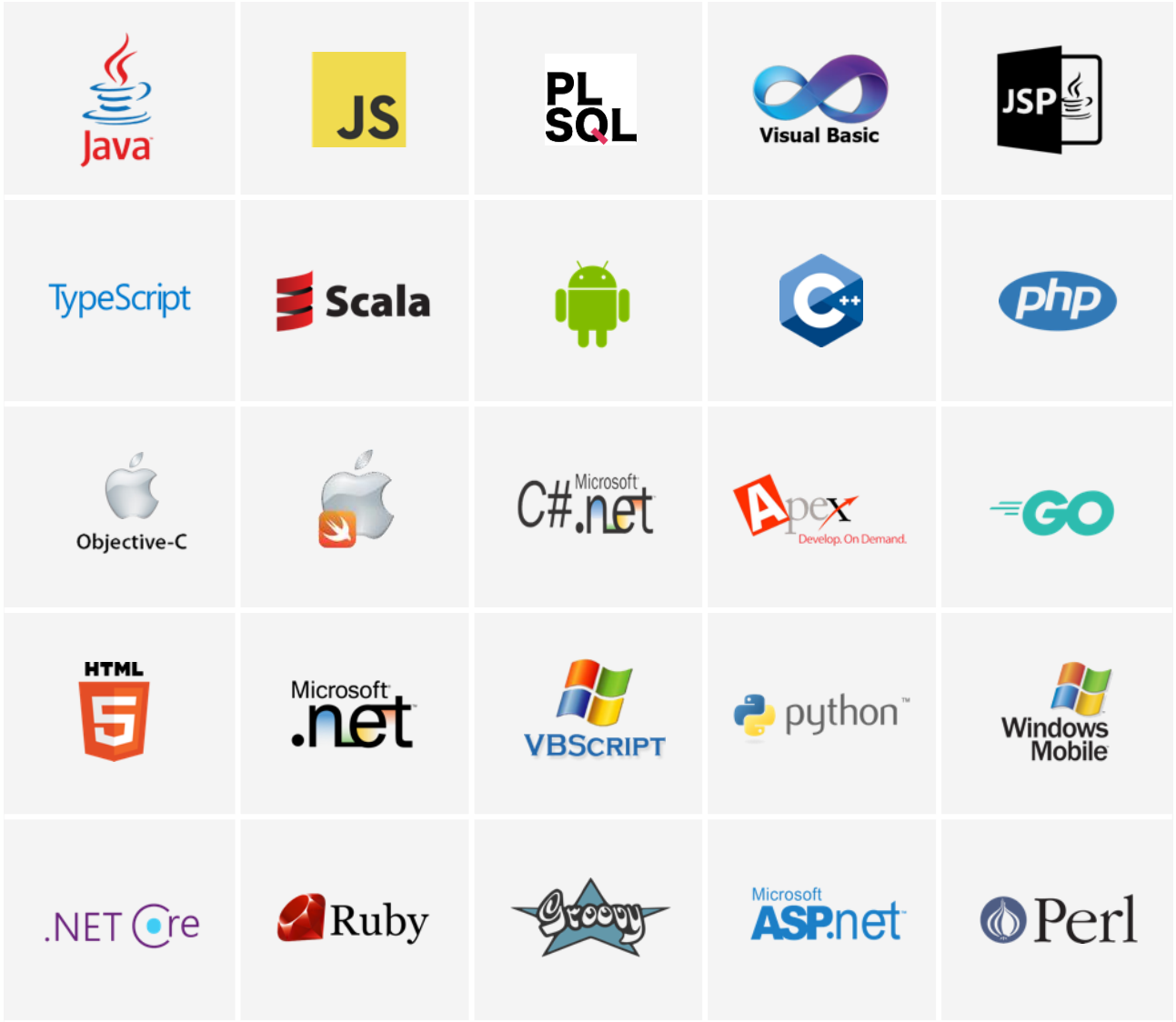


Checkmarx Knowledge Center

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

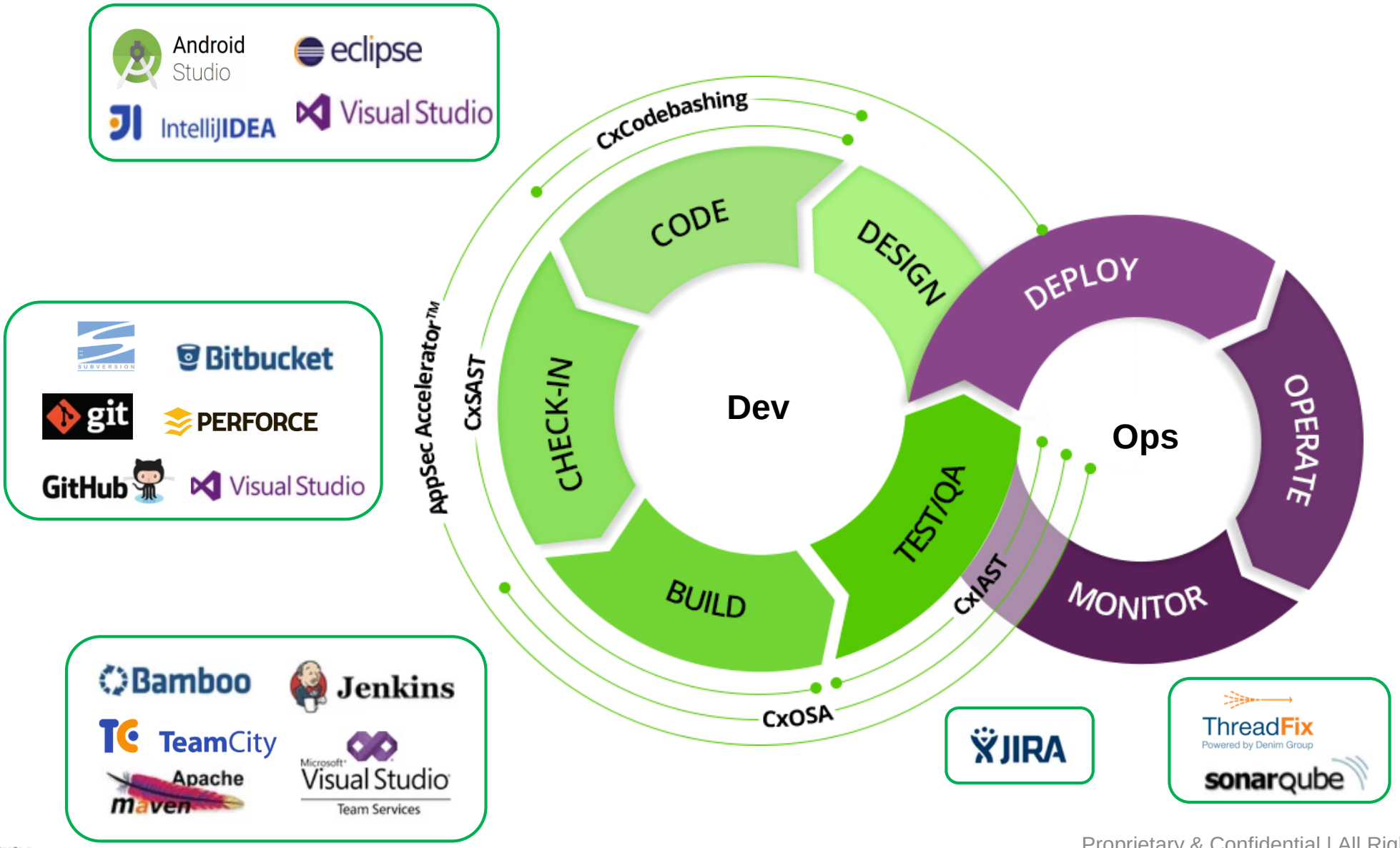


Software Development



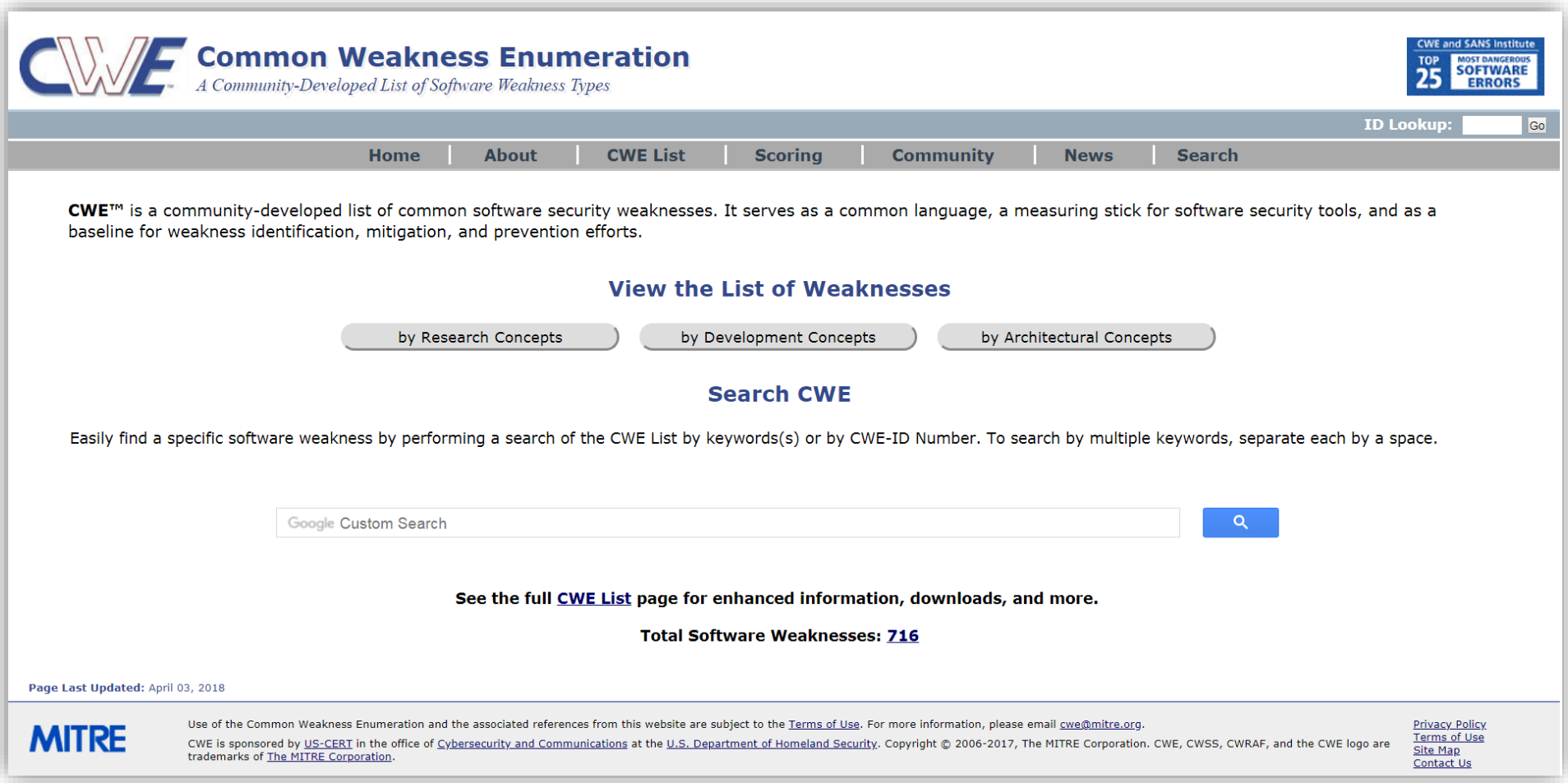
- **Supports 25 coding and scripting languages and their frameworks**
- **Coverage for the latest development technologies**
- **Zero configuration to scan any language**

Secure SDLC & DevOps Environment



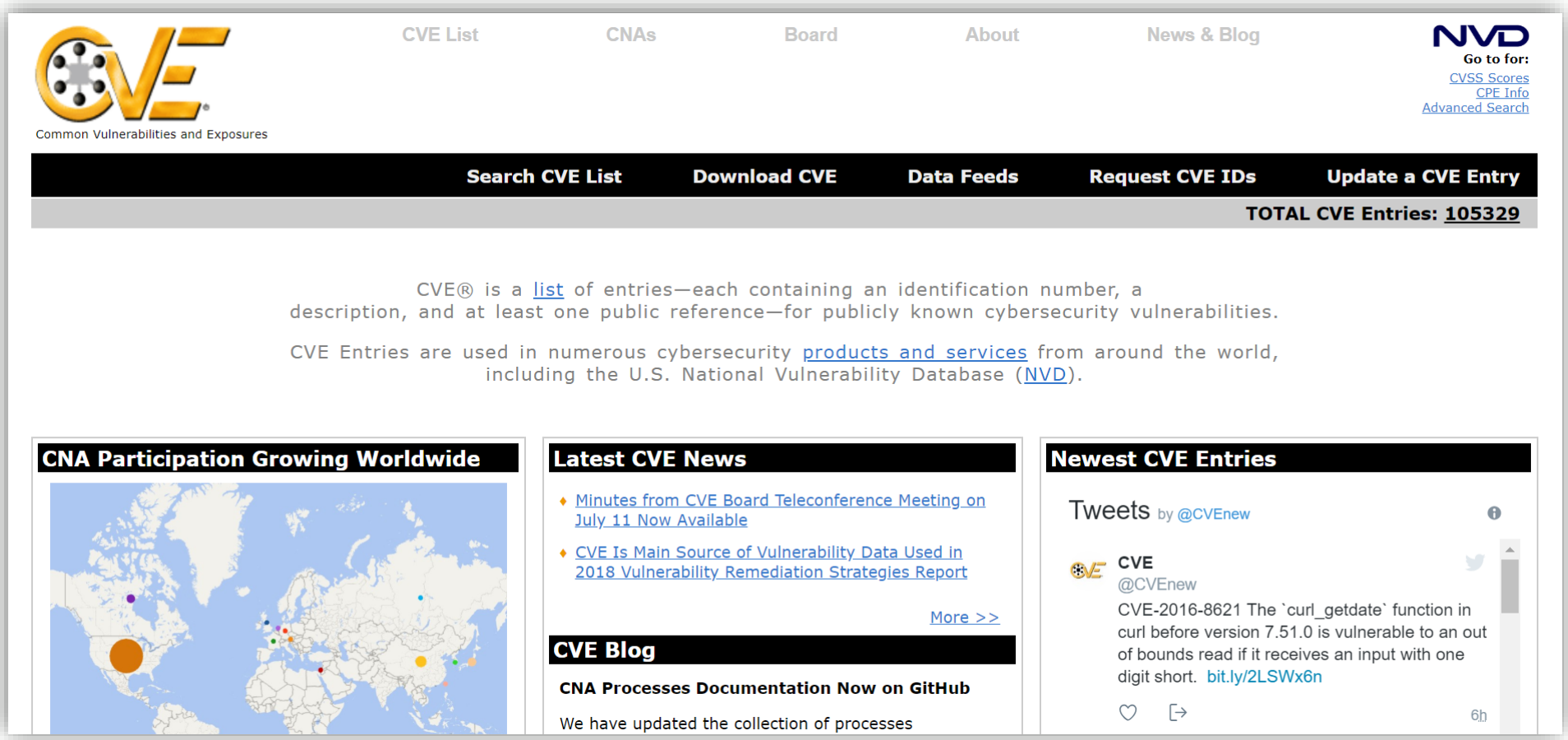
Common Weakness Enumeration, CWE

https://cwe.mitre.org



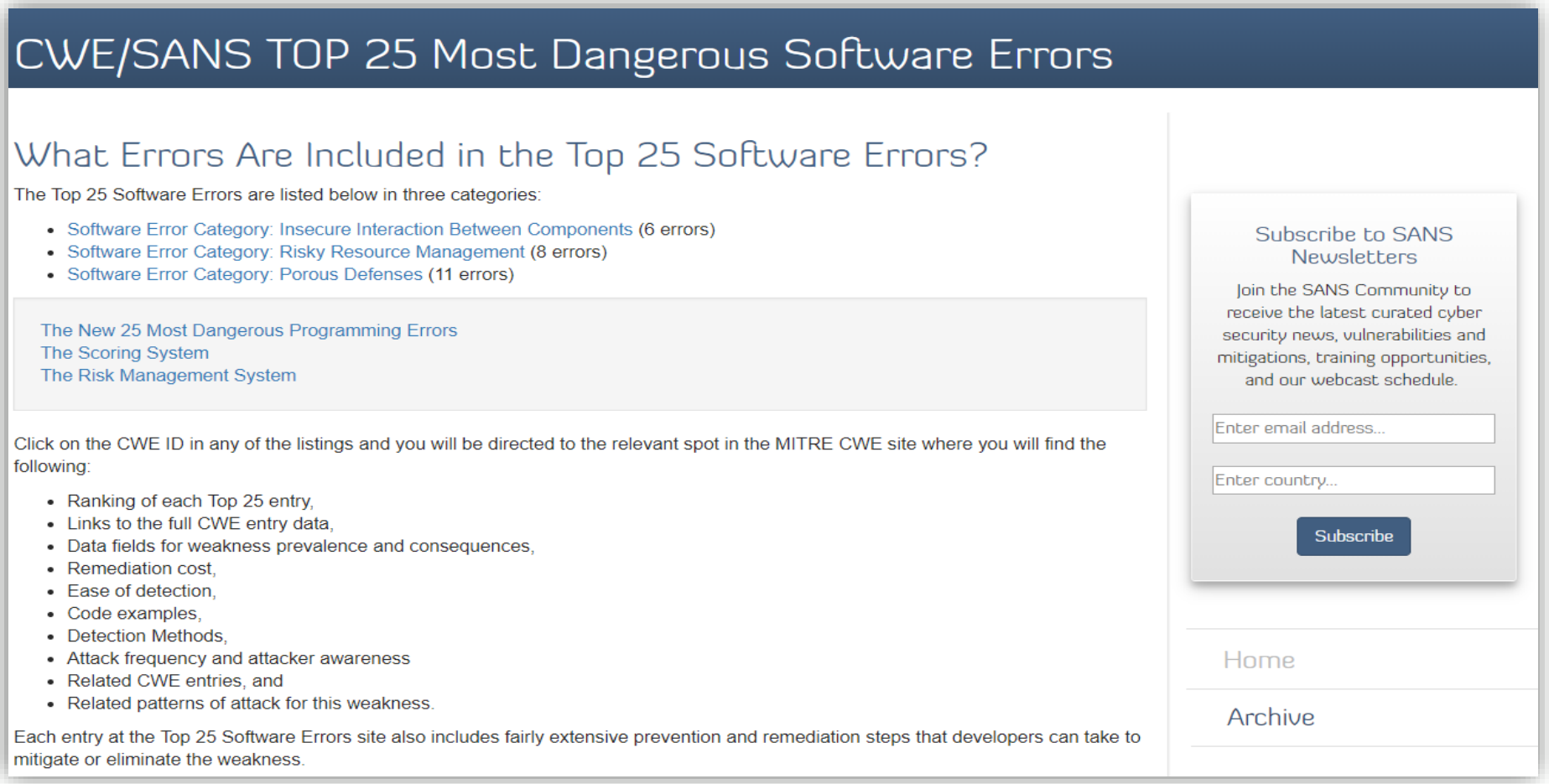
Common Vulnerabilities and Exposures, CVE

https://cve.mitre.org



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

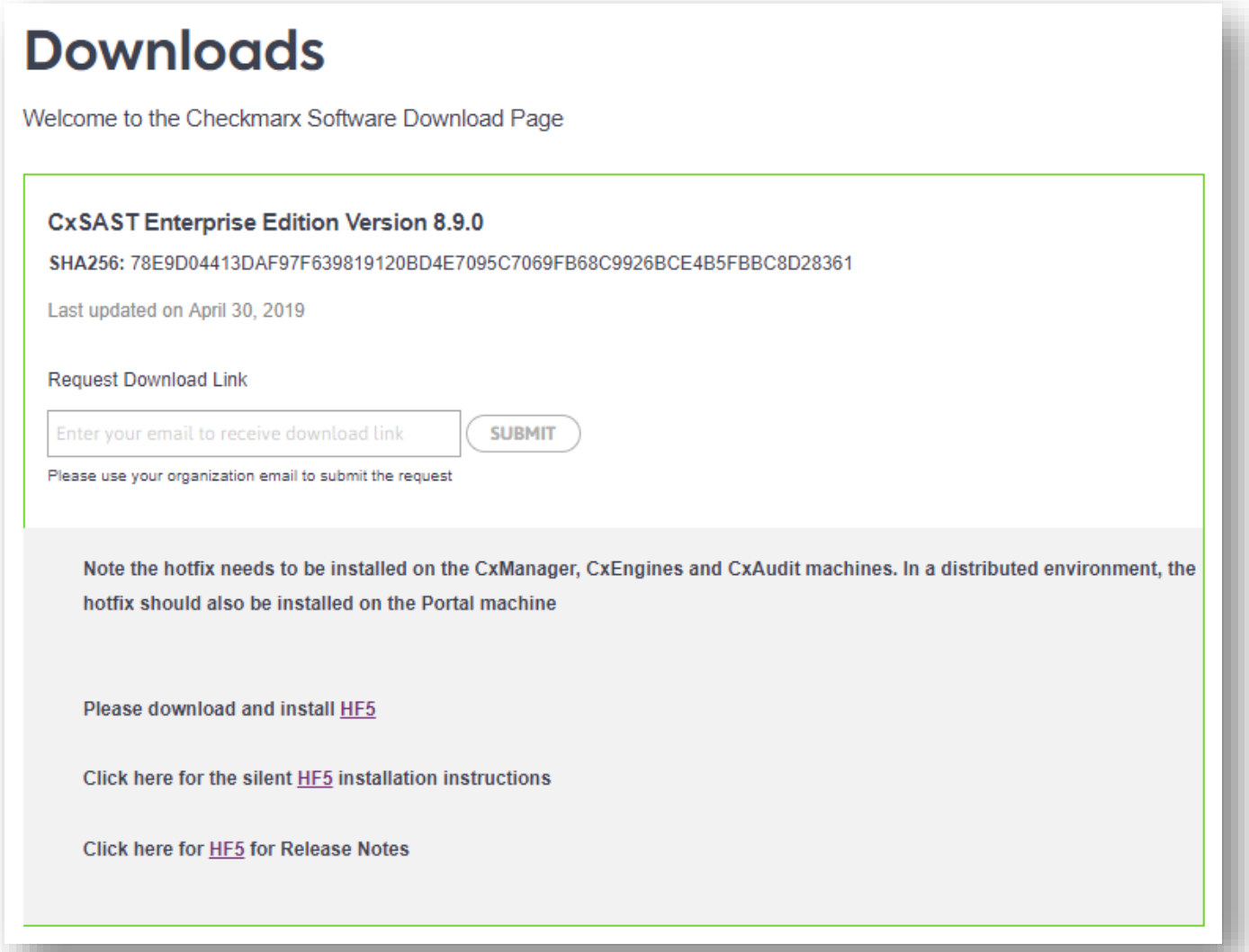
Archive

OWASP Top Ten Project

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

CxSAST Download Page

https://www.checkmarx.com/downloads



CxPlugins Download Page

https://www.checkmarx.com/plugins

Plugins

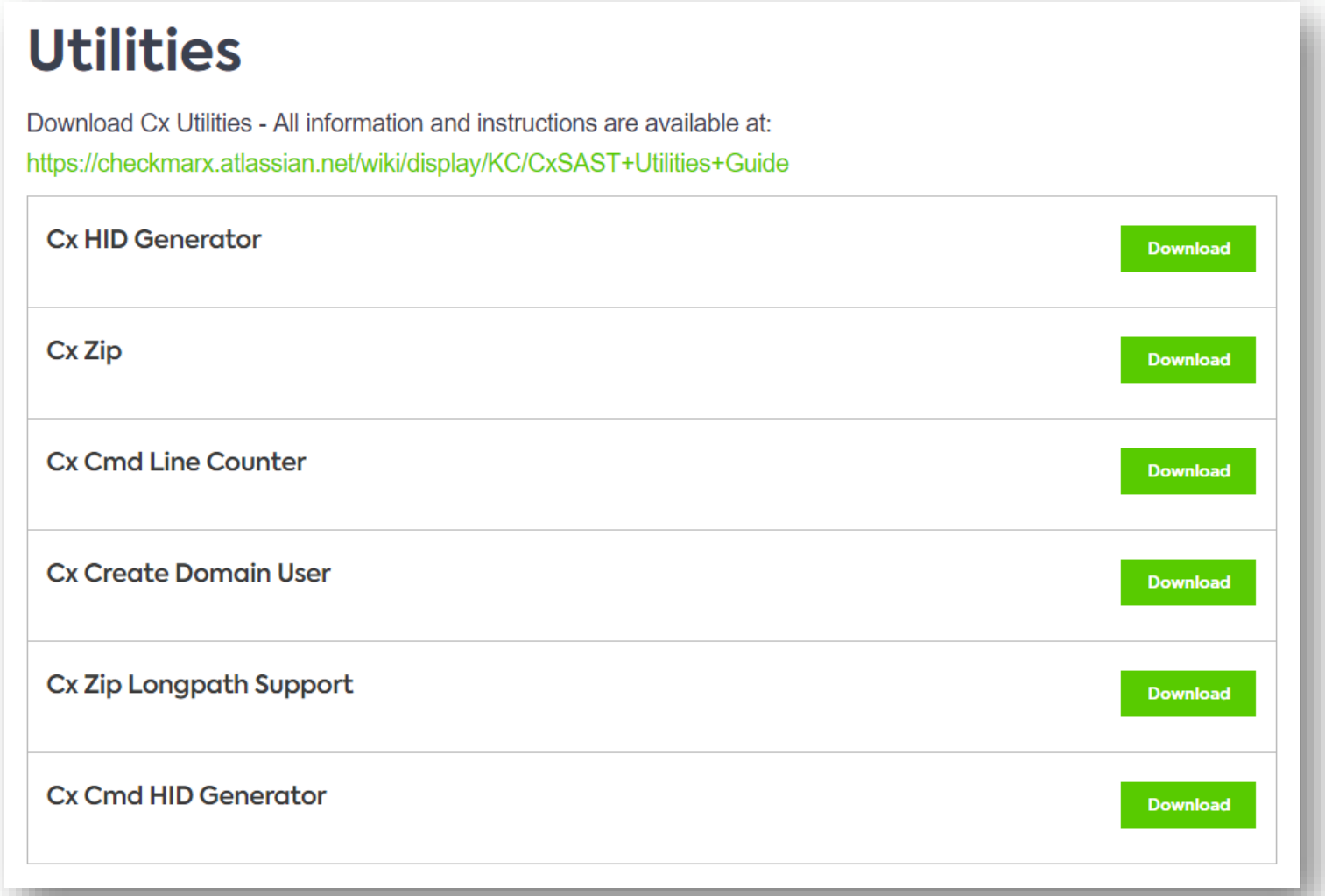
CxPlugins page

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: 89.0.0* | *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



Exercise 1: POC Document and Discovery

CxSAST POC Plan Document – Partner
CxSAST POC Plan Document v1.3.docx

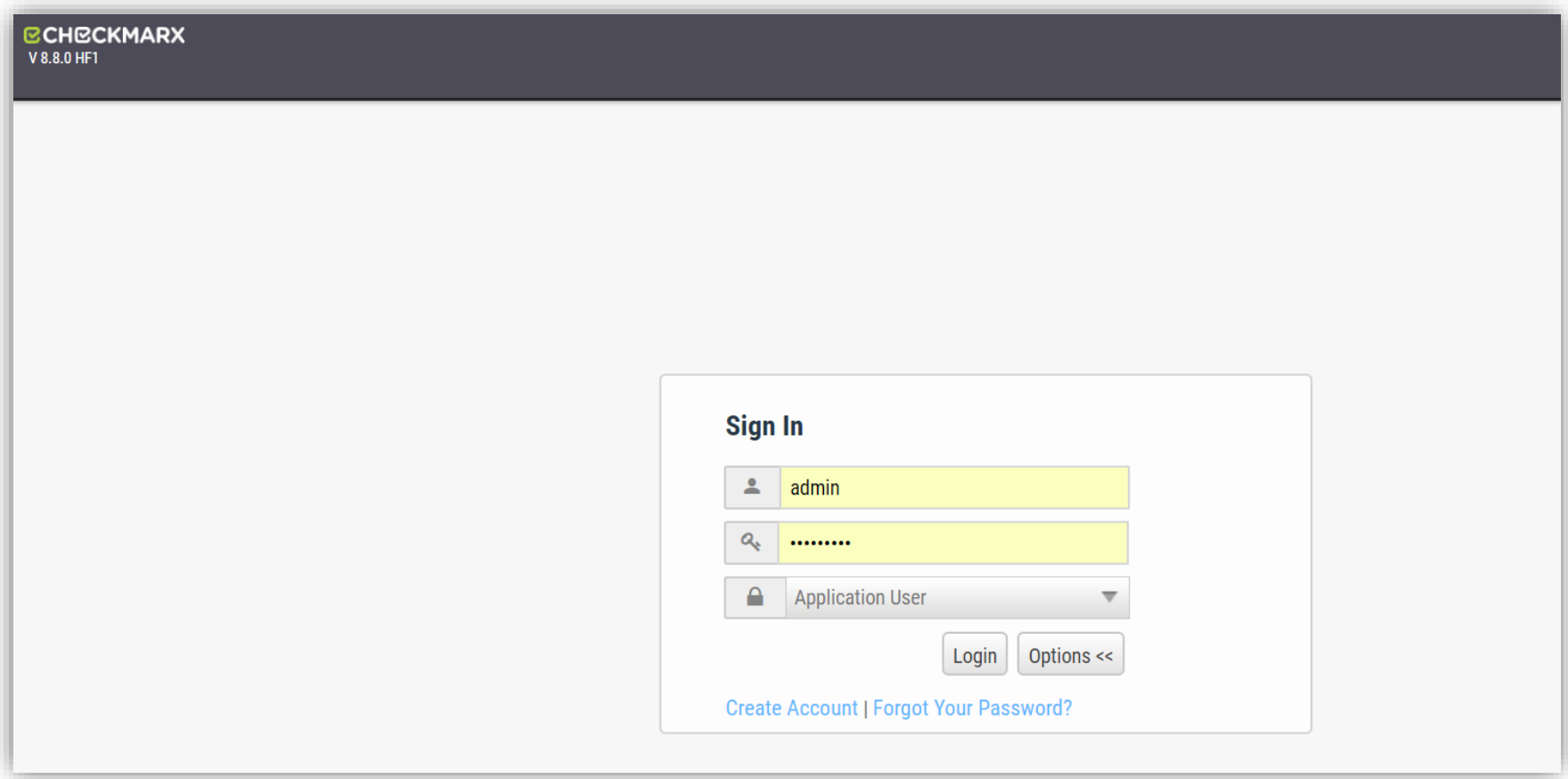
CxSAST POC Plan Document – Checkmarx Internal
CxSAST POC Template - JasonK.docx

Hardware Sizing – Checkmarx Internal
Sizing AWS Hardware (r-2) For SE.xlsx

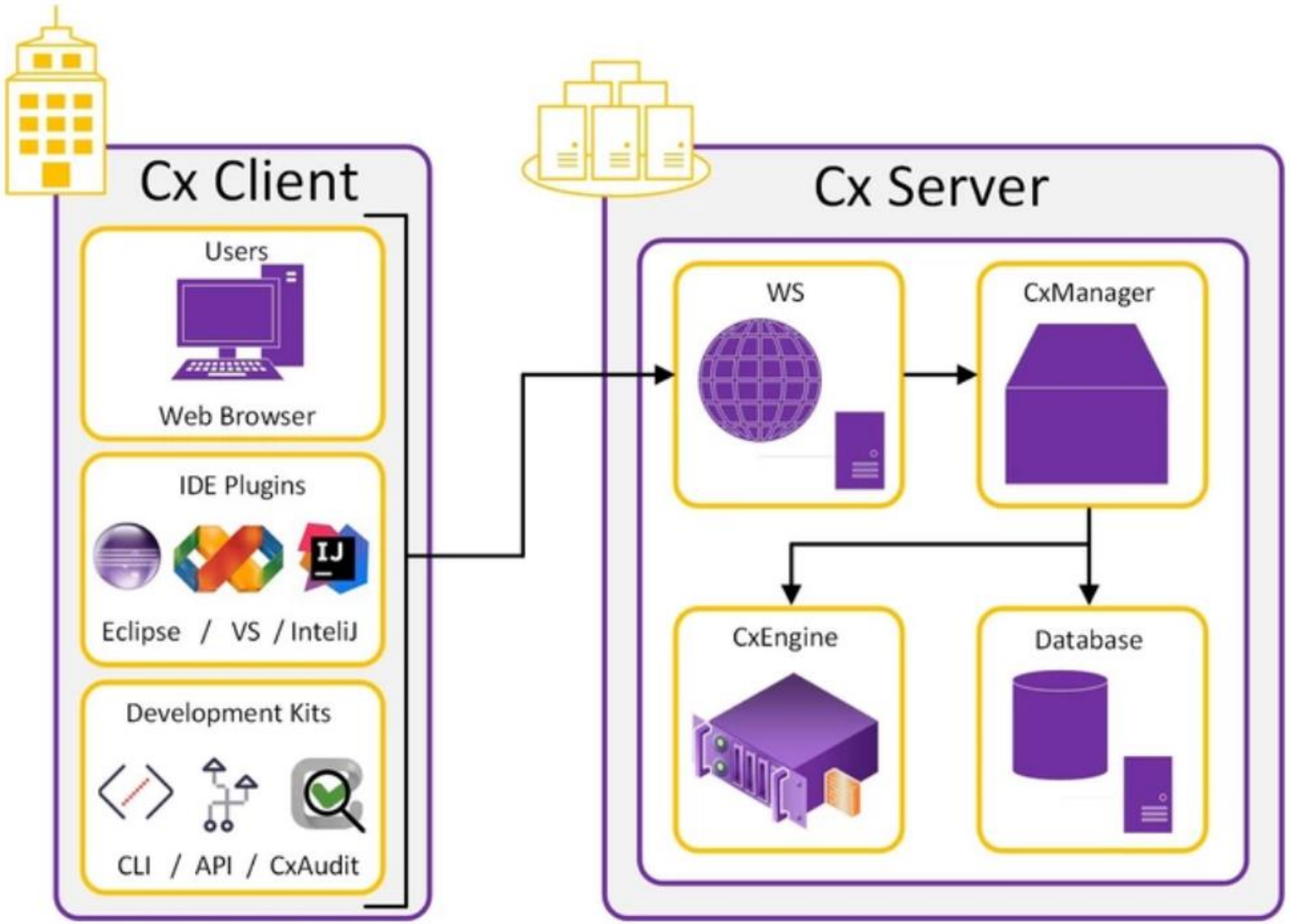
/ CxSAST
Introduction & Configuration

Checkmarx

CxSAST Introduction



Checkmarx CxSAST Architecture



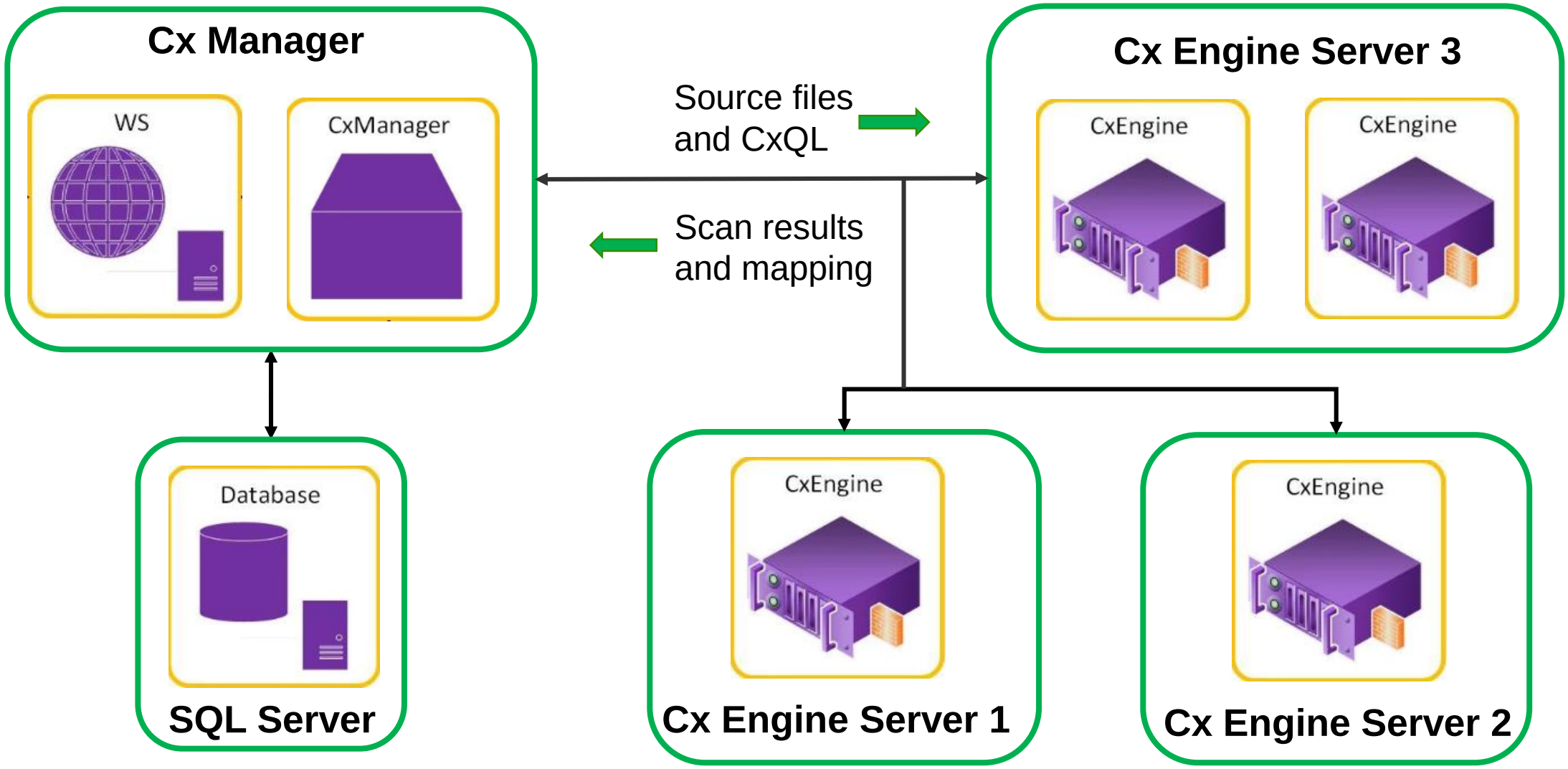
Server

- IIS web portal
- CxManager
- CxEngines
- SQL database

Client

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

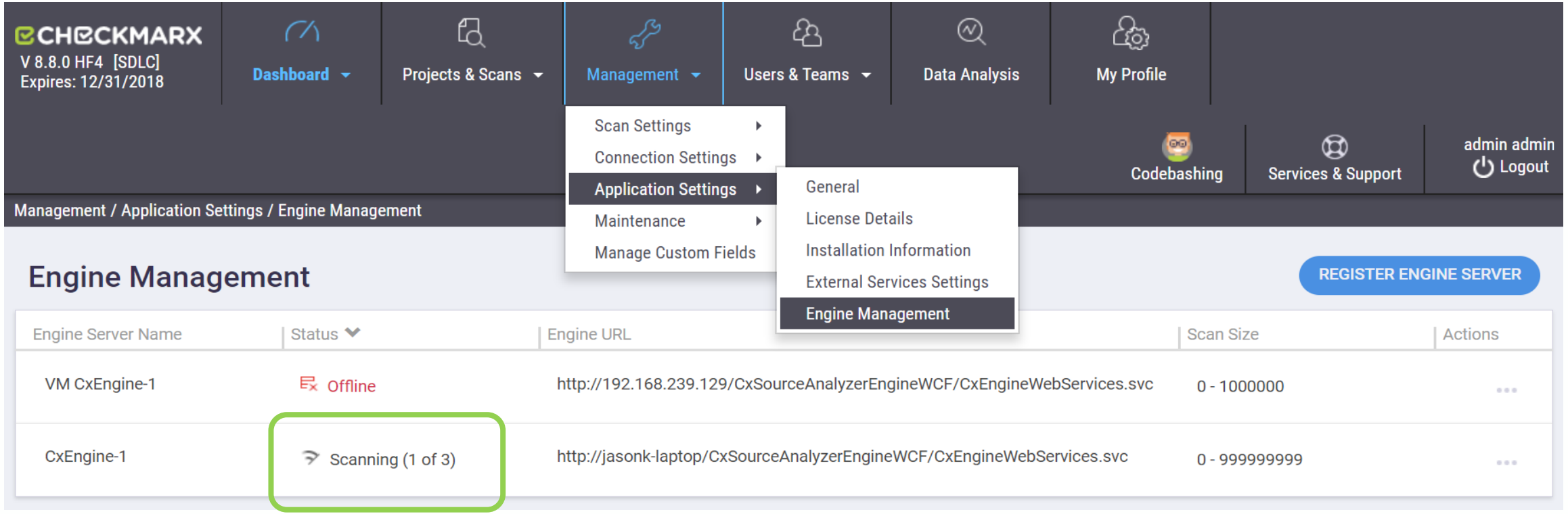
Checkmarx CxSAST Engine Architecture



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



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

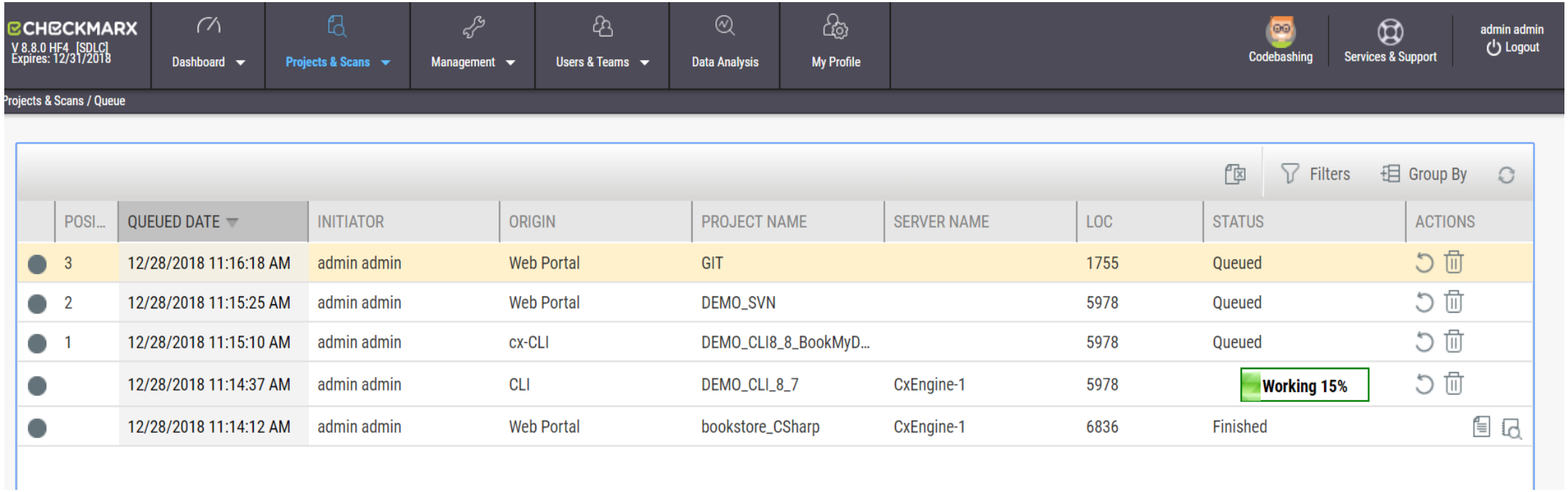
```
<instrumentationConfiguration performanceCountersEnabled="fa
applicationInstanceName="" />
<appSettings>
  <!--<add key="BASE_PATH" value="C:\Checkmarx\Enterprise\SC
  <add key="SOURCE_PATH" value="C:\CxSrc" />
  <!--
  <add key="CACHE_PATH" value="C:\Checkmarx\Enterprise\SOA-b
  <add key="CONFIG_PATH" value="C:\Checkmarx\Enterprise\SOA-
  <add key="RESULTS_PATH" value="C:\Checkmarx\Enterprise\SOA
  -->
  <!--<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

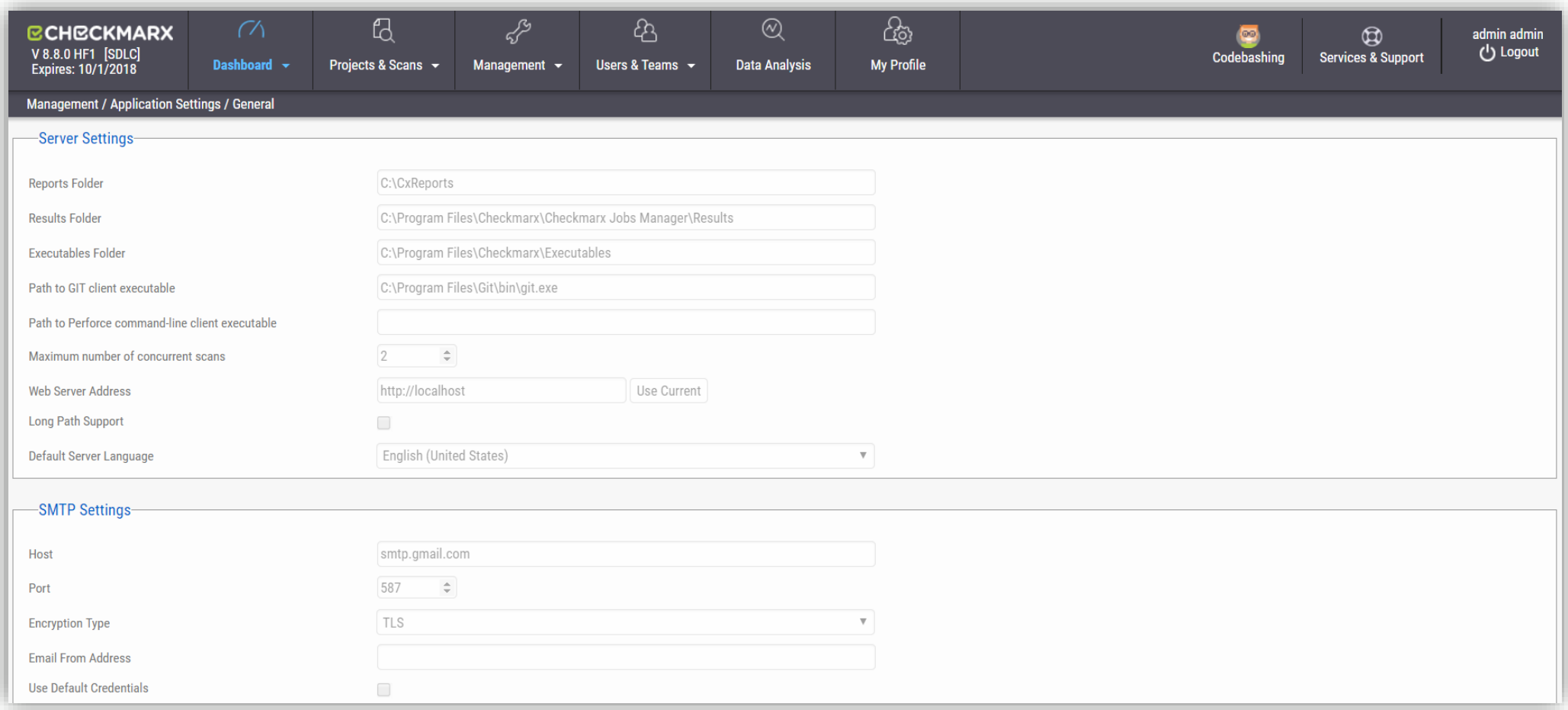
Status:

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



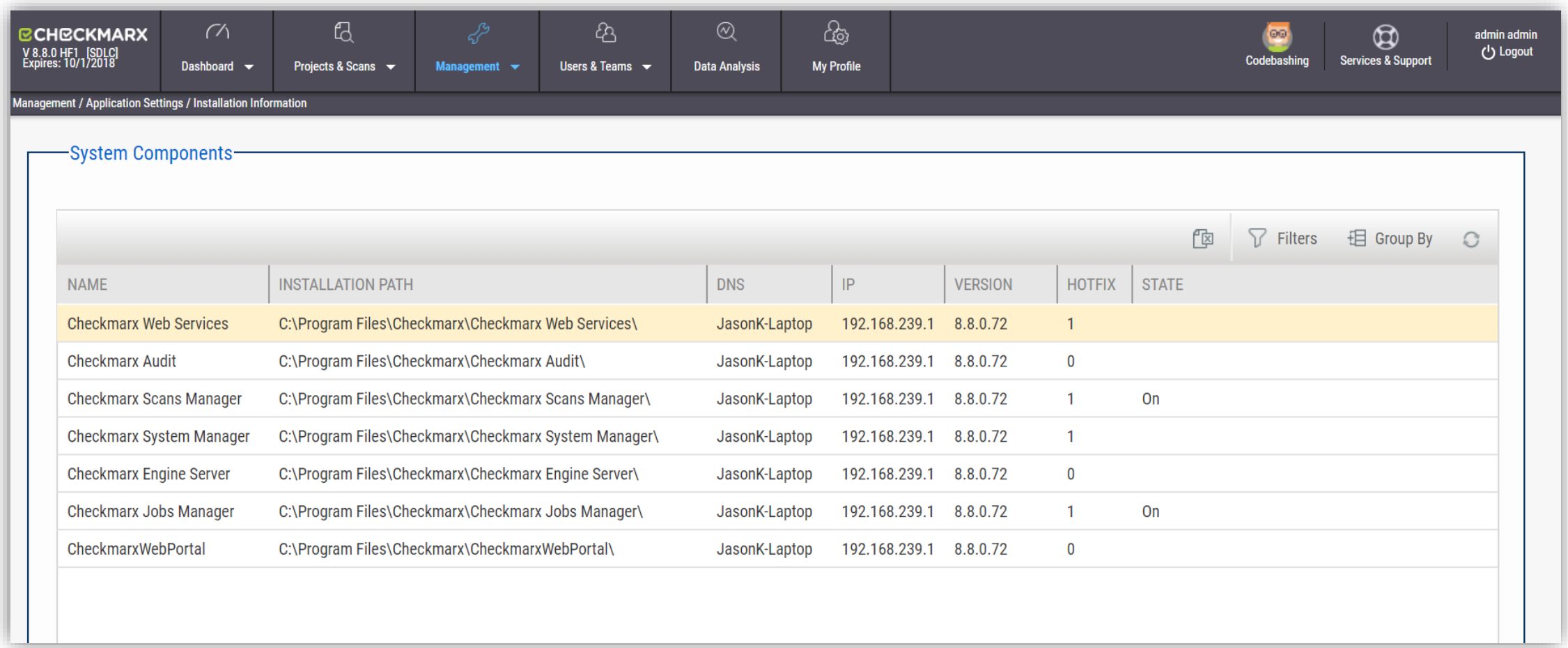
Checkmarx CxSAST Configuration

CxSAST Web Portal – Application Settings



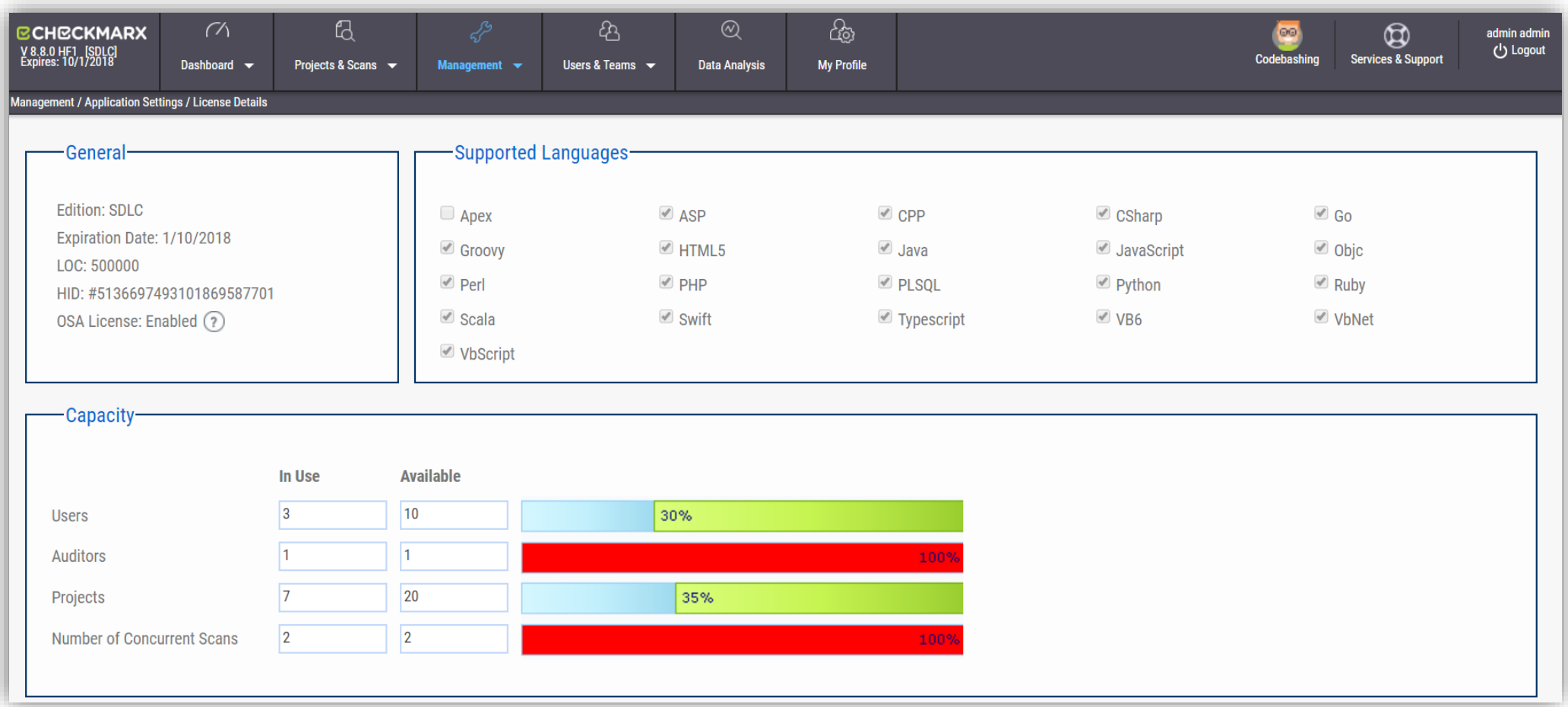
Checkmarx CxSAST Configuration

CxSAST Web Portal – Installation Information



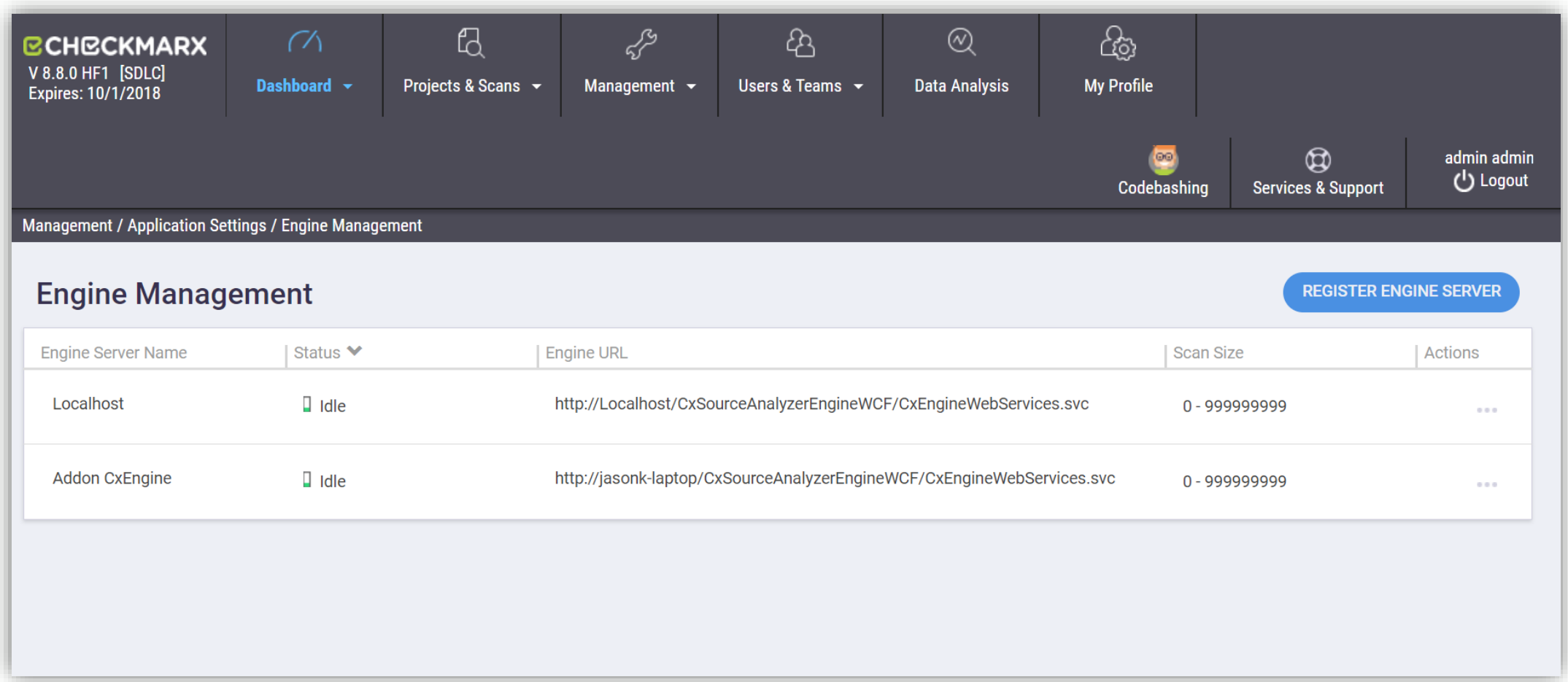
Checkmarx CxSAST Configuration

CxSAST Web Portal – License Details



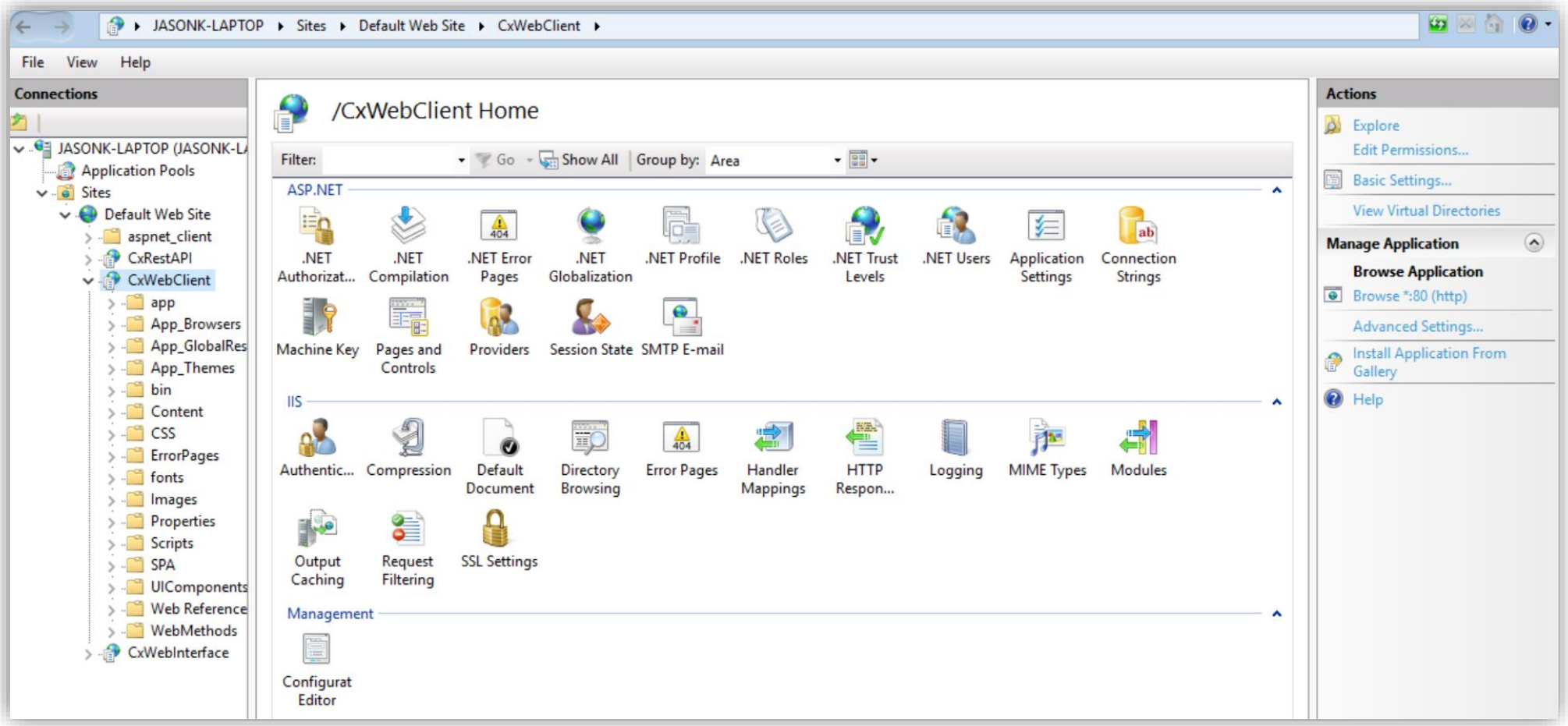
Checkmarx CxSAST Configuration

CxSAST Web Portal – Engine Server Management



Checkmarx CxSAST Configuration

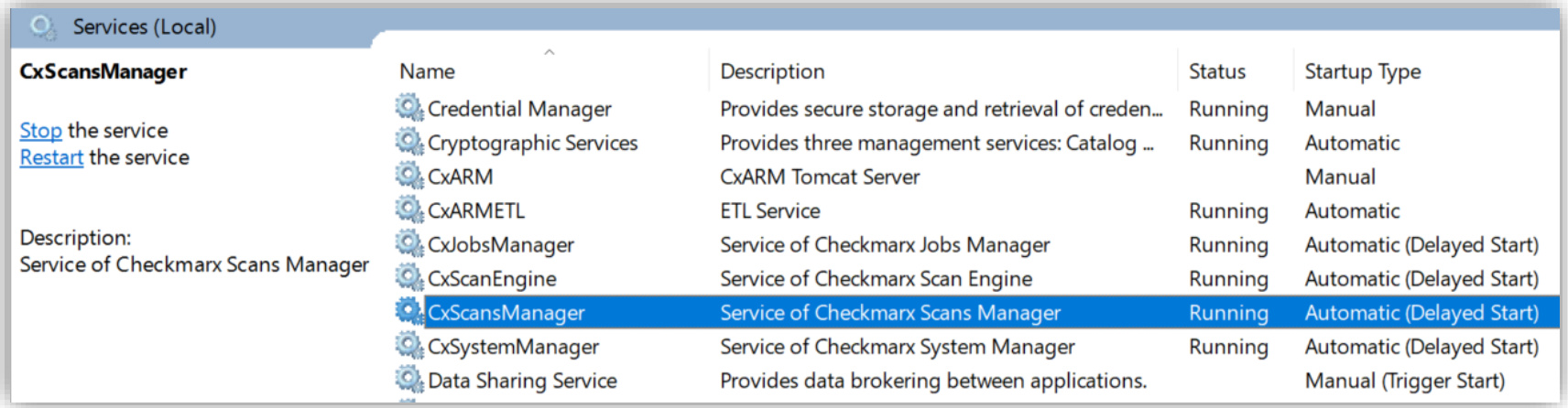
Microsoft Internet Information Services Manager

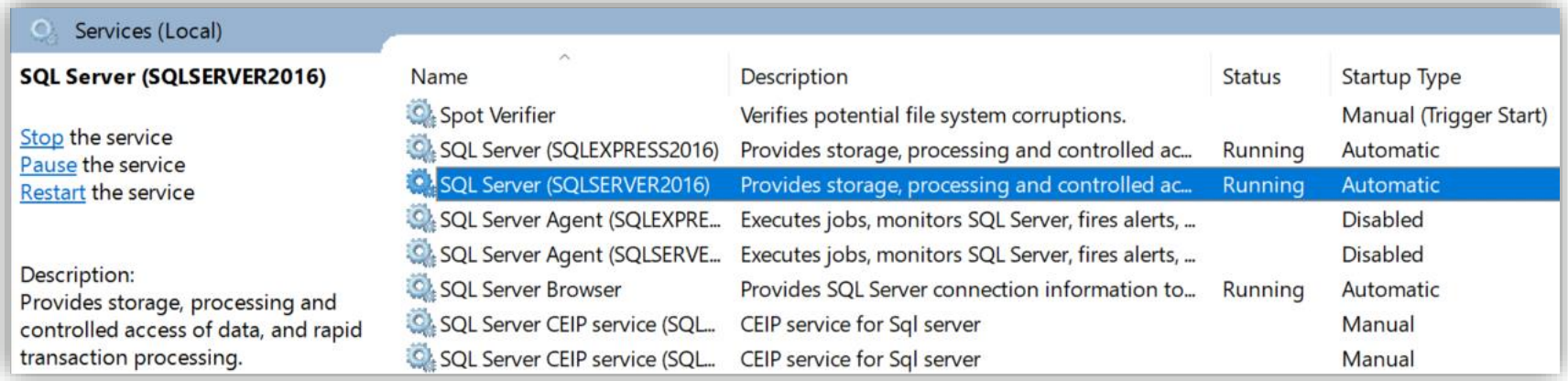


Checkmarx CxSAST Configuration

Microsoft Windows Services

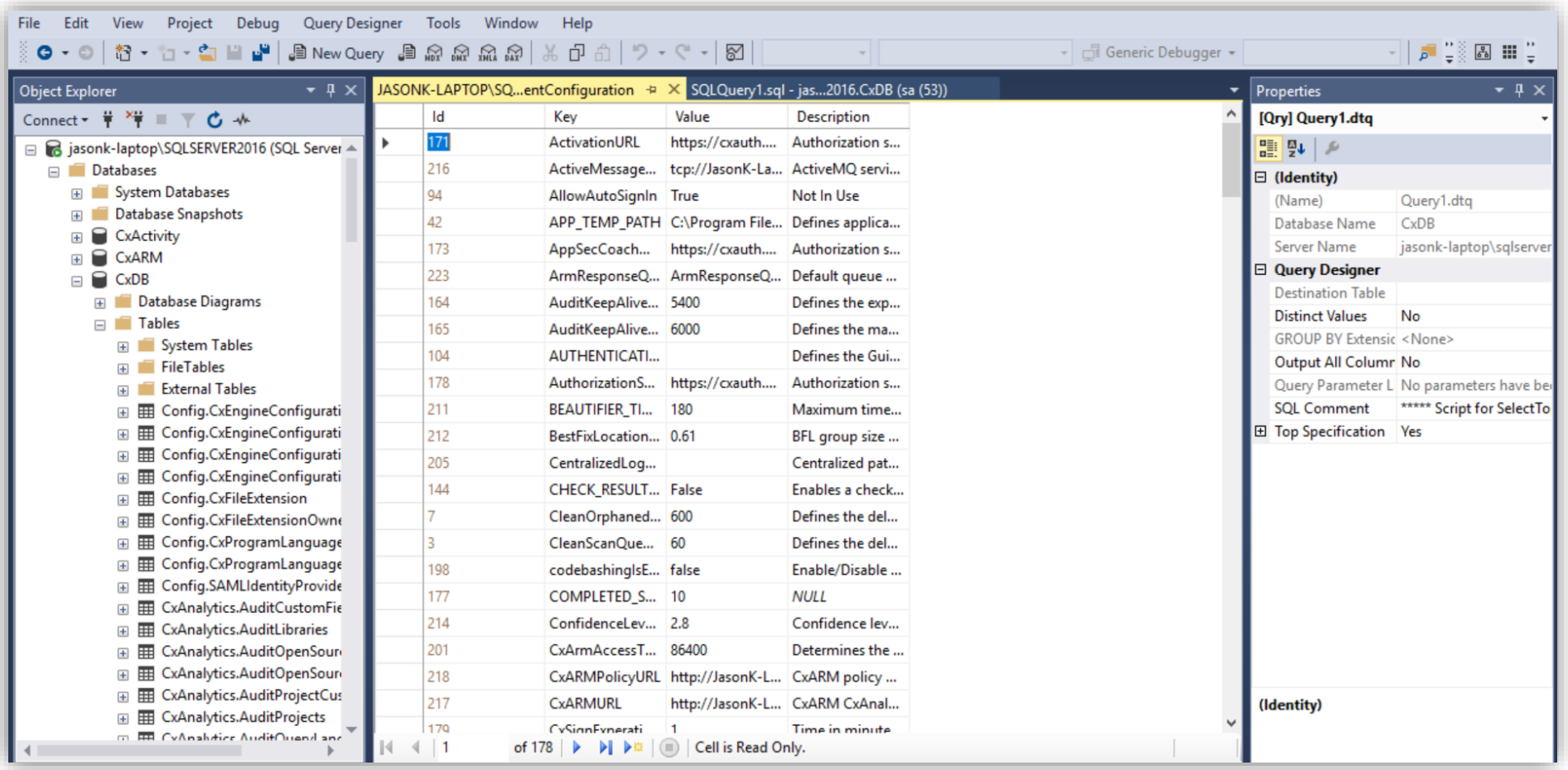
- CxJobsManager
- CxScanEngine
- CxScansManager
- CxSystemManager
- SQL Server





Checkmarx CxSAST Configuration

Microsoft SQL Server Database



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

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 }
```

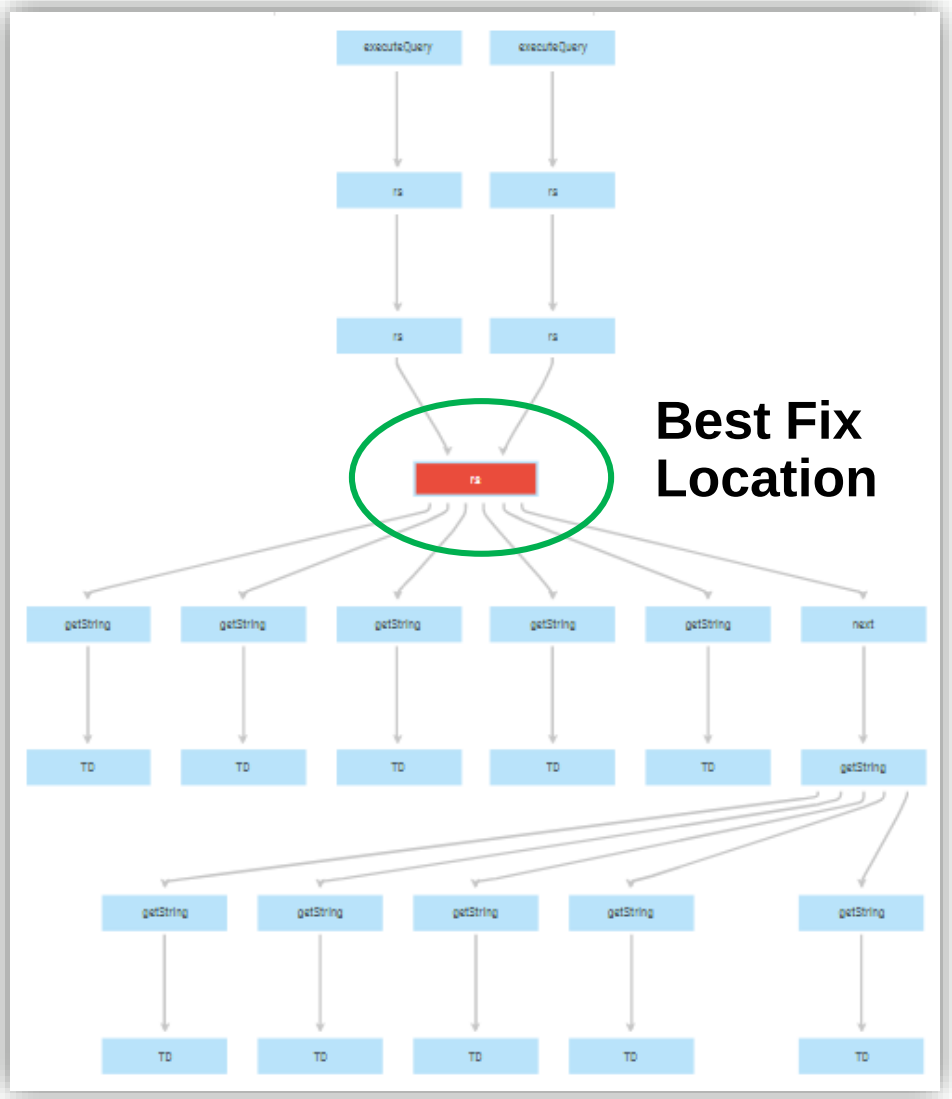
Source DOM

Sink DOM

DFG

Checkmarx CxSAST Technology

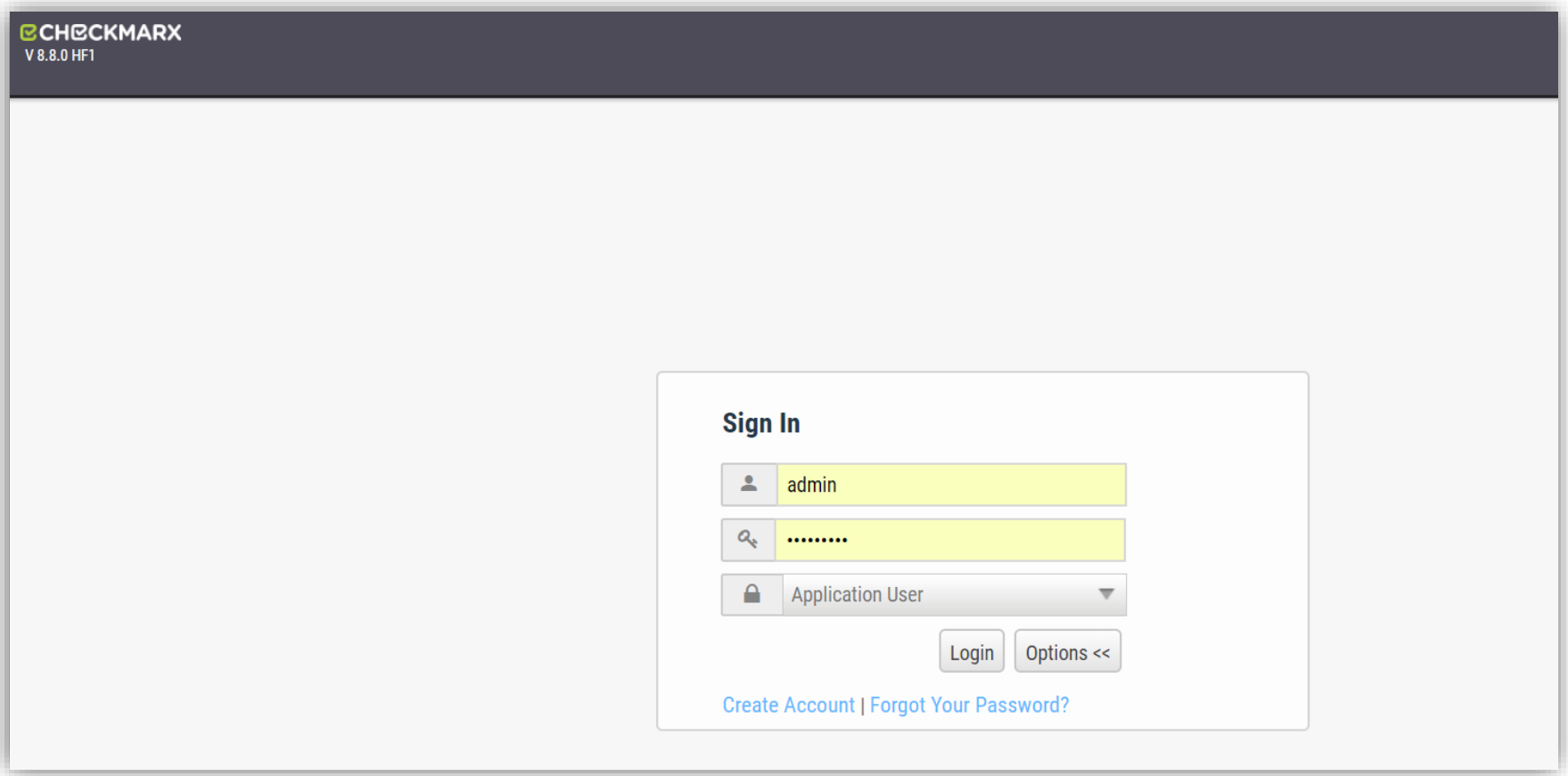
Common Weakness Enumeration



Checkmarx CxSAST Web Portal

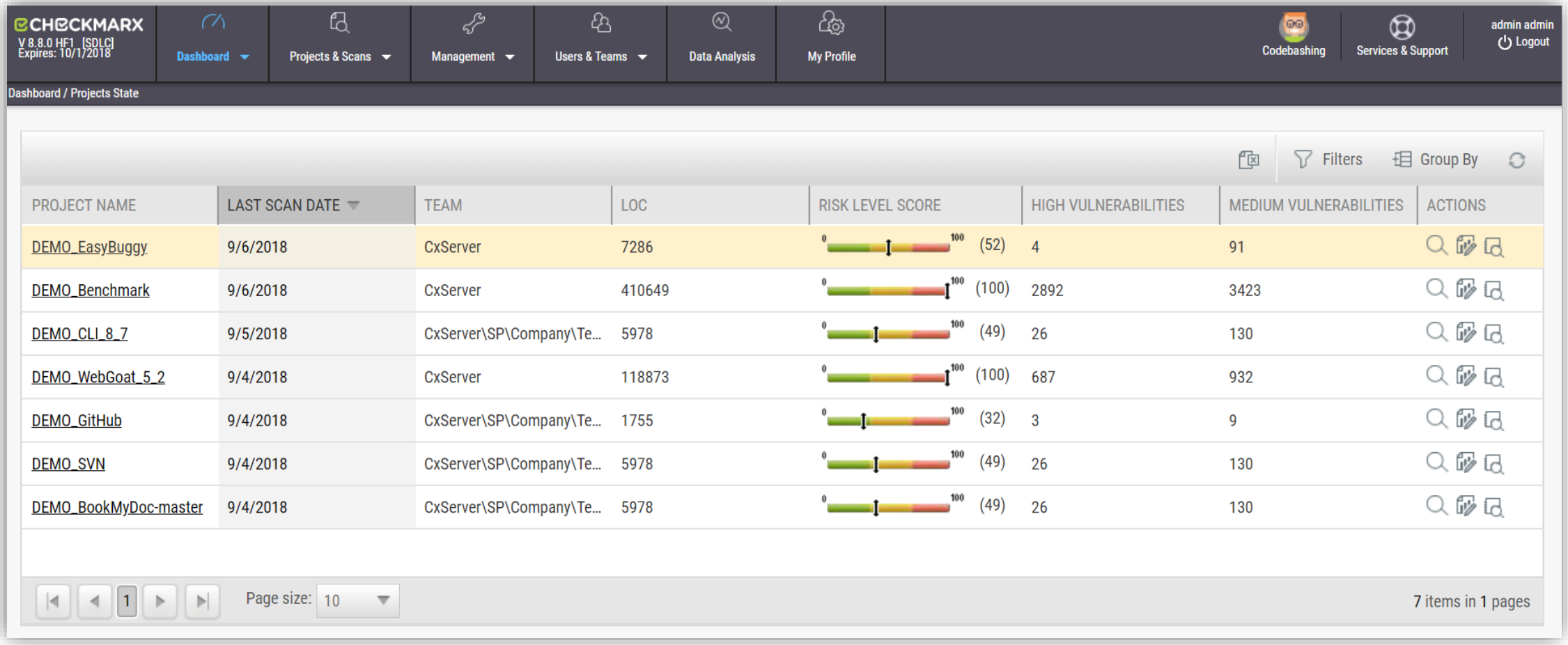
CxSAST Web Portal

- Login
- Create account
- Forget password



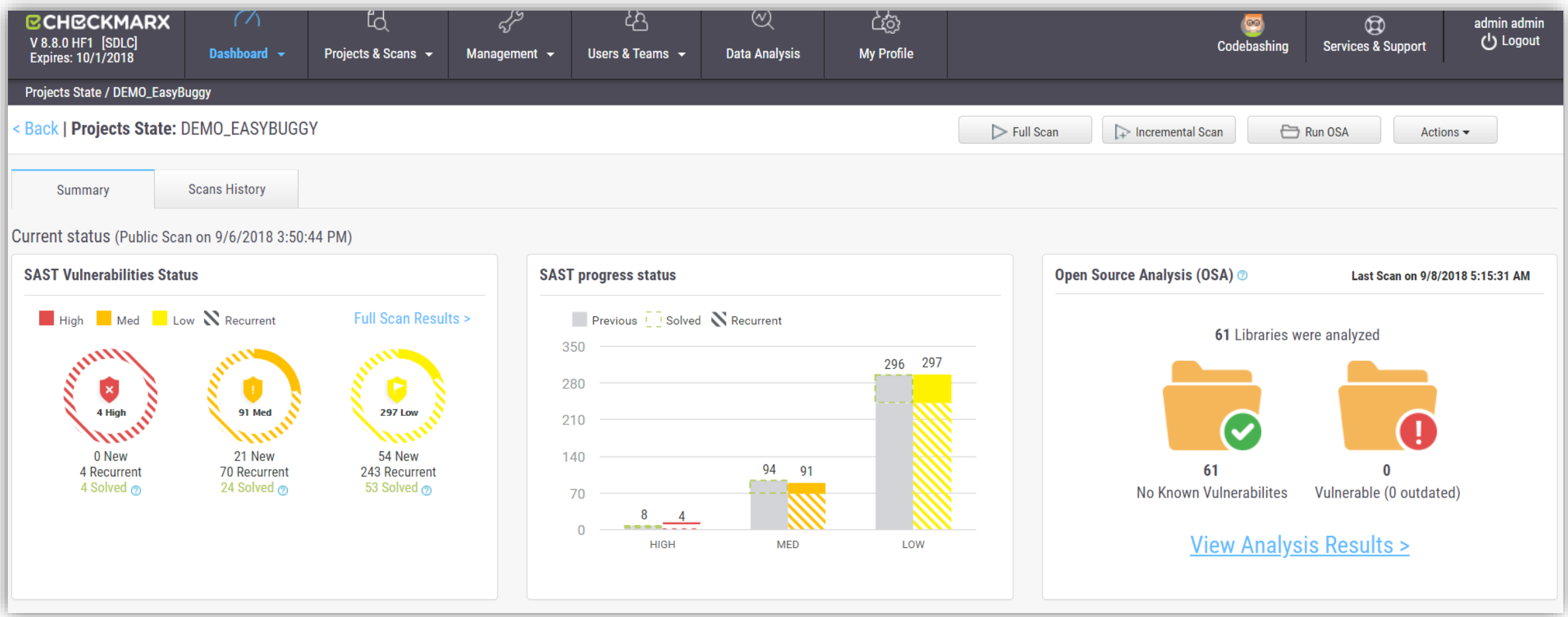
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Projects Overview



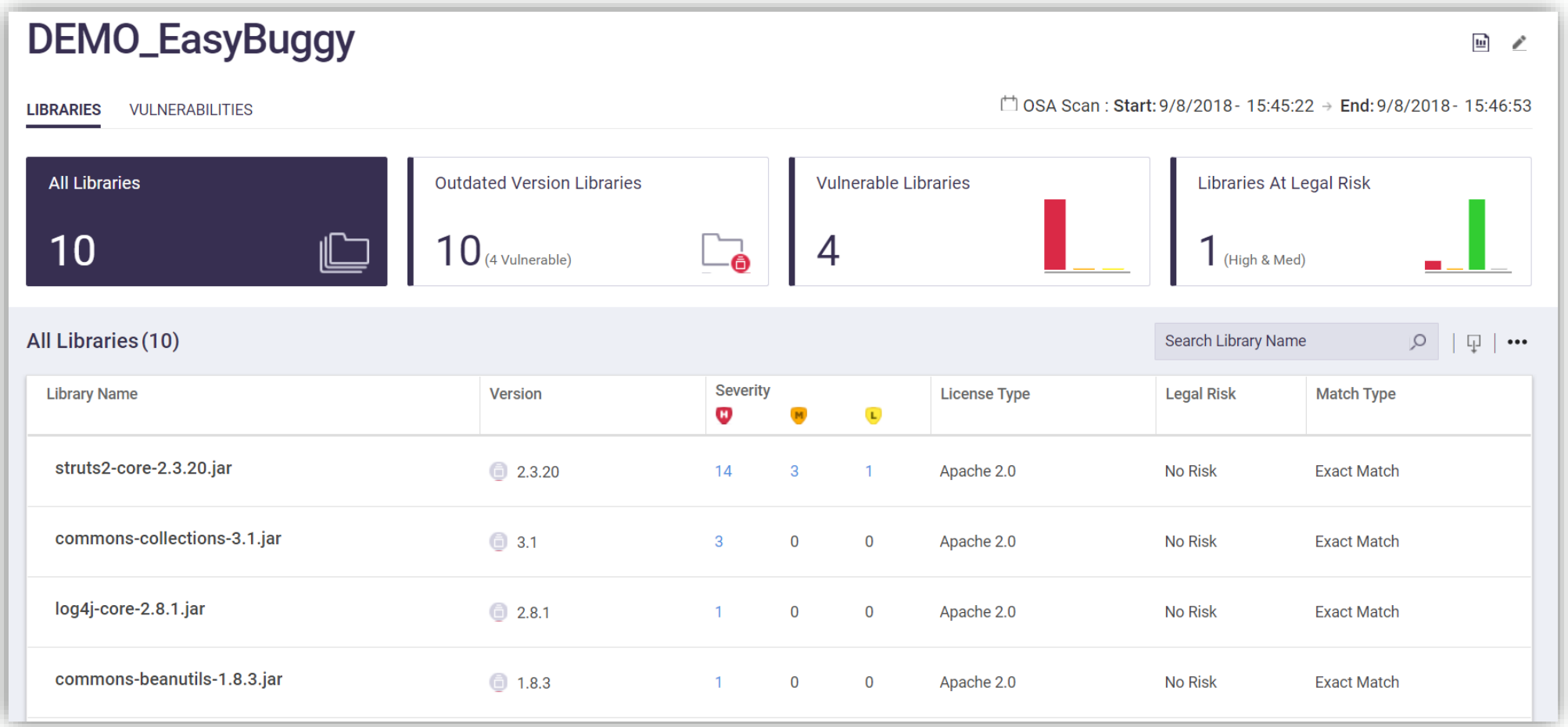
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Project Dashboard



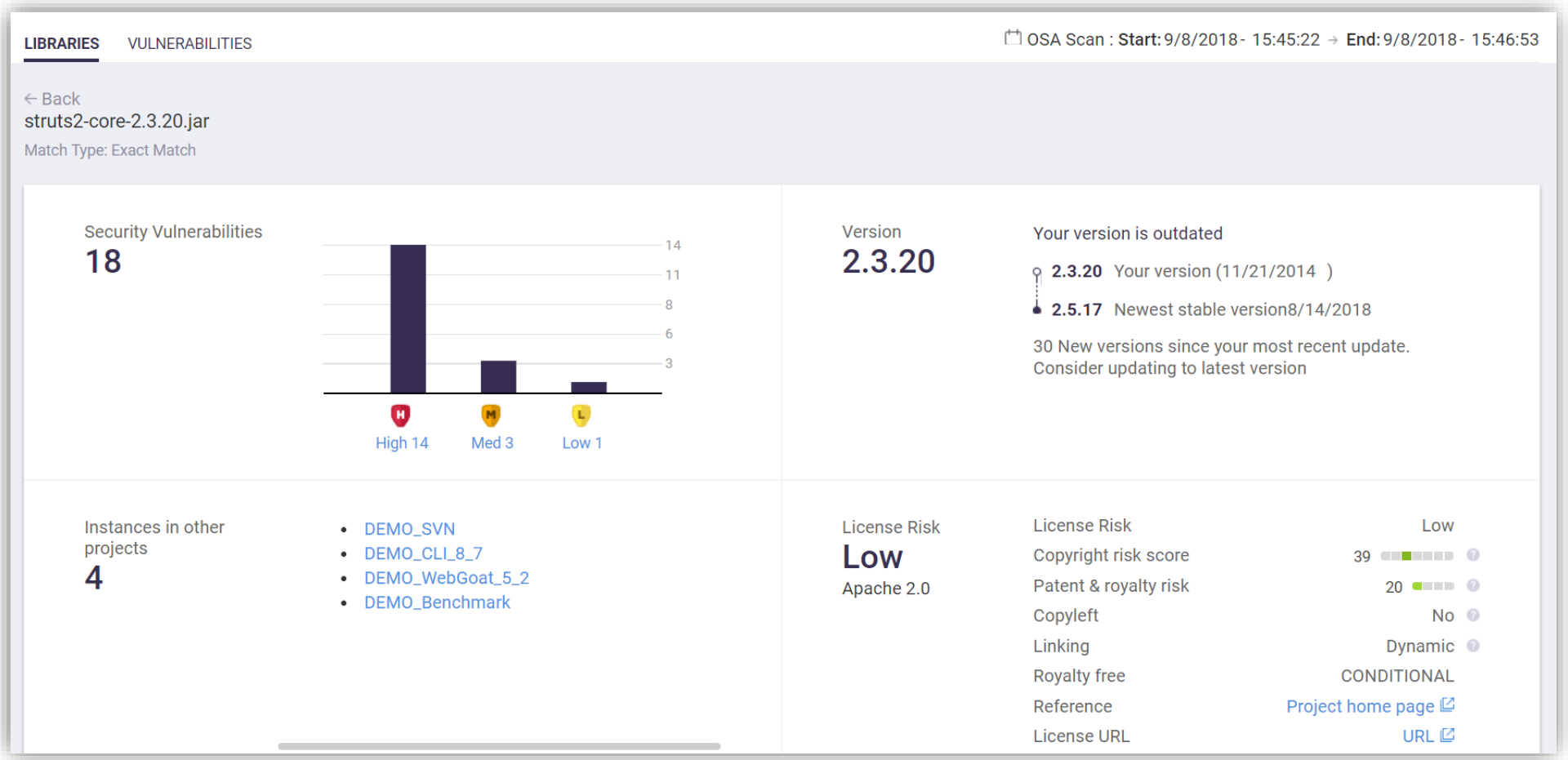
Checkmarx CxOSA Web Portal

CxSAST Web Portal – Open Source Analysis, CxOSA



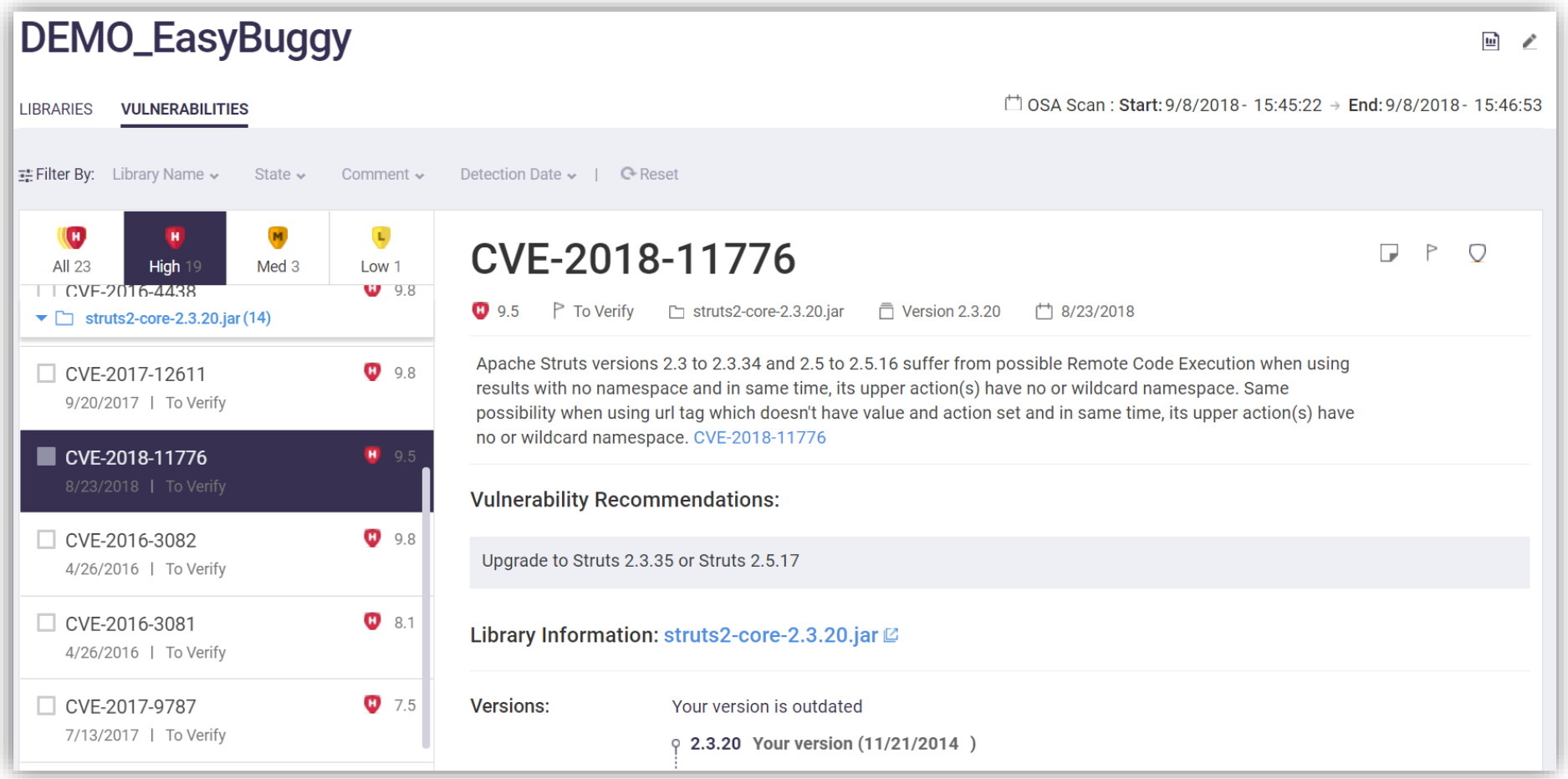
Checkmarx CxOSA Web Portal

CxSAST Web Portal – Open Source Analysis, CxOSA

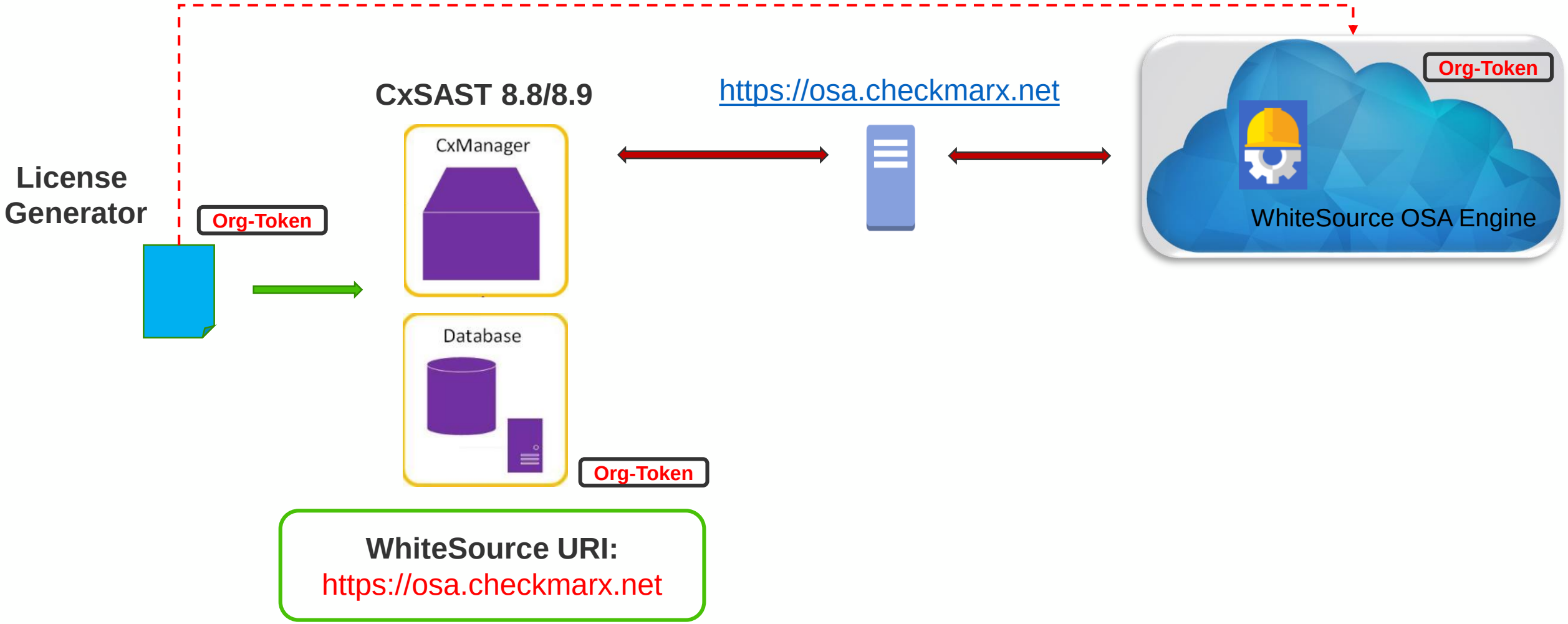


Checkmarx CxOSA Web Portal

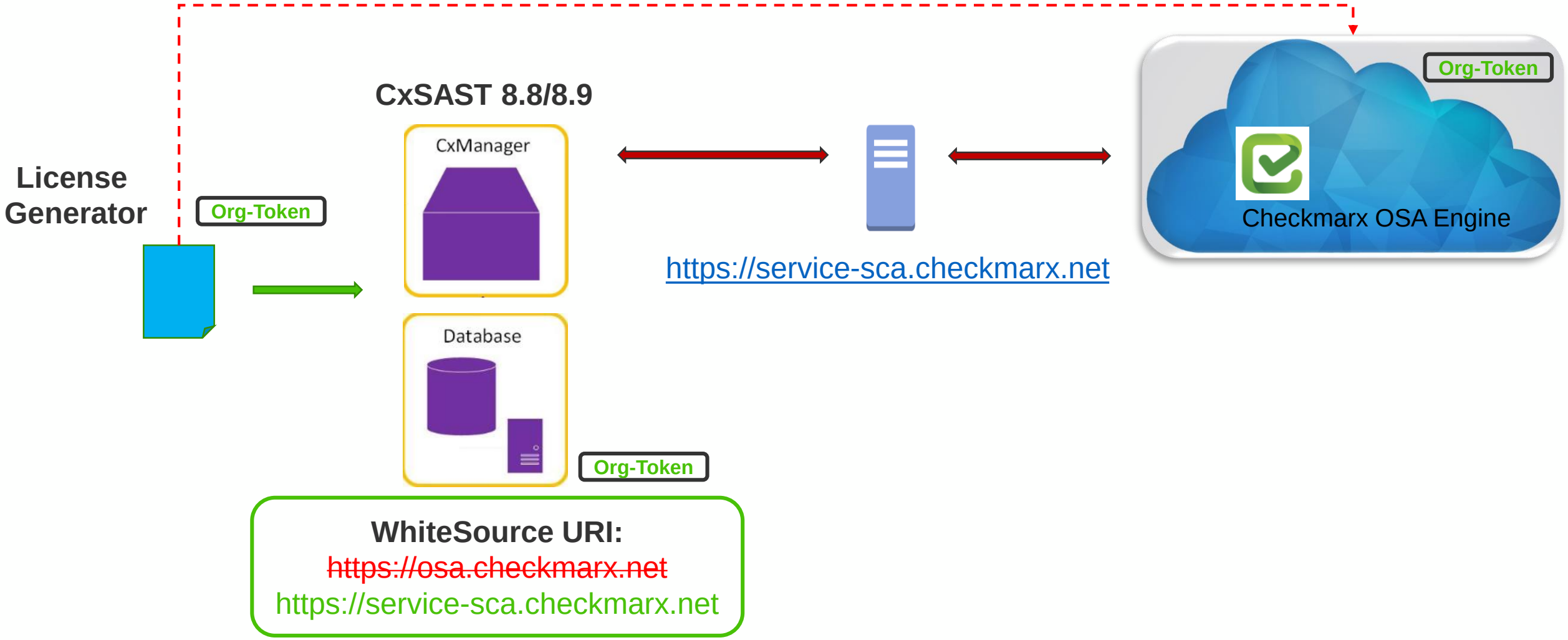
CxSAST Web Portal – Open Source Analysis, CxOSA



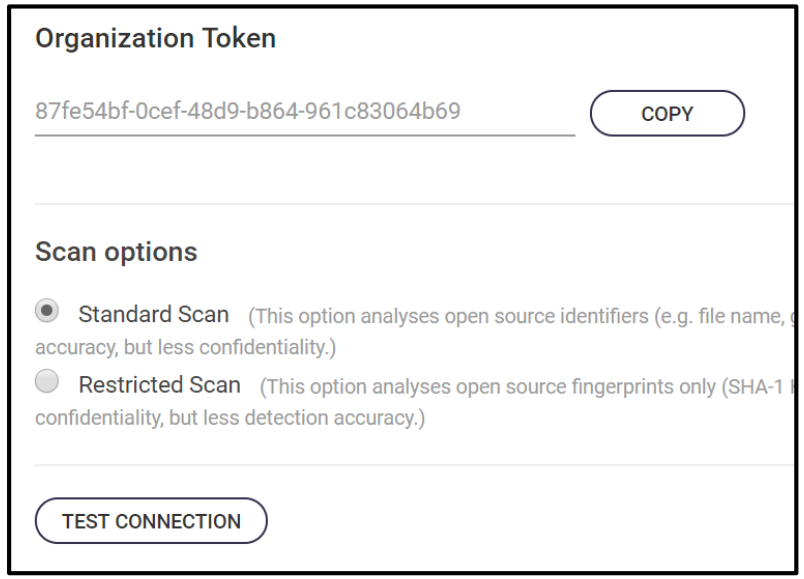
Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)



Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)

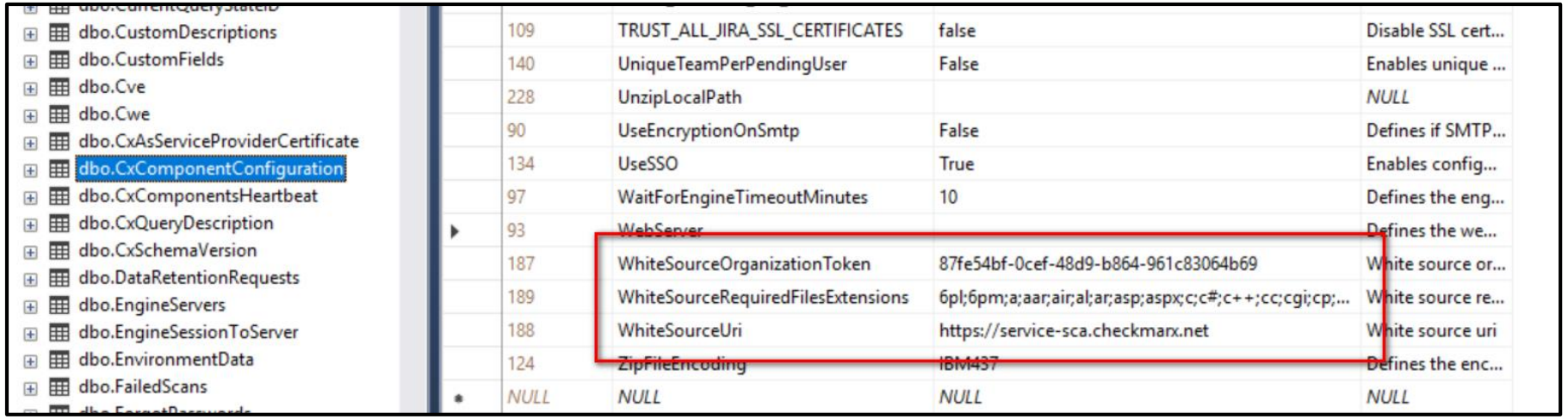


Checkmarx CxOSA Migration (CxSAST 8.8 and 8.9)



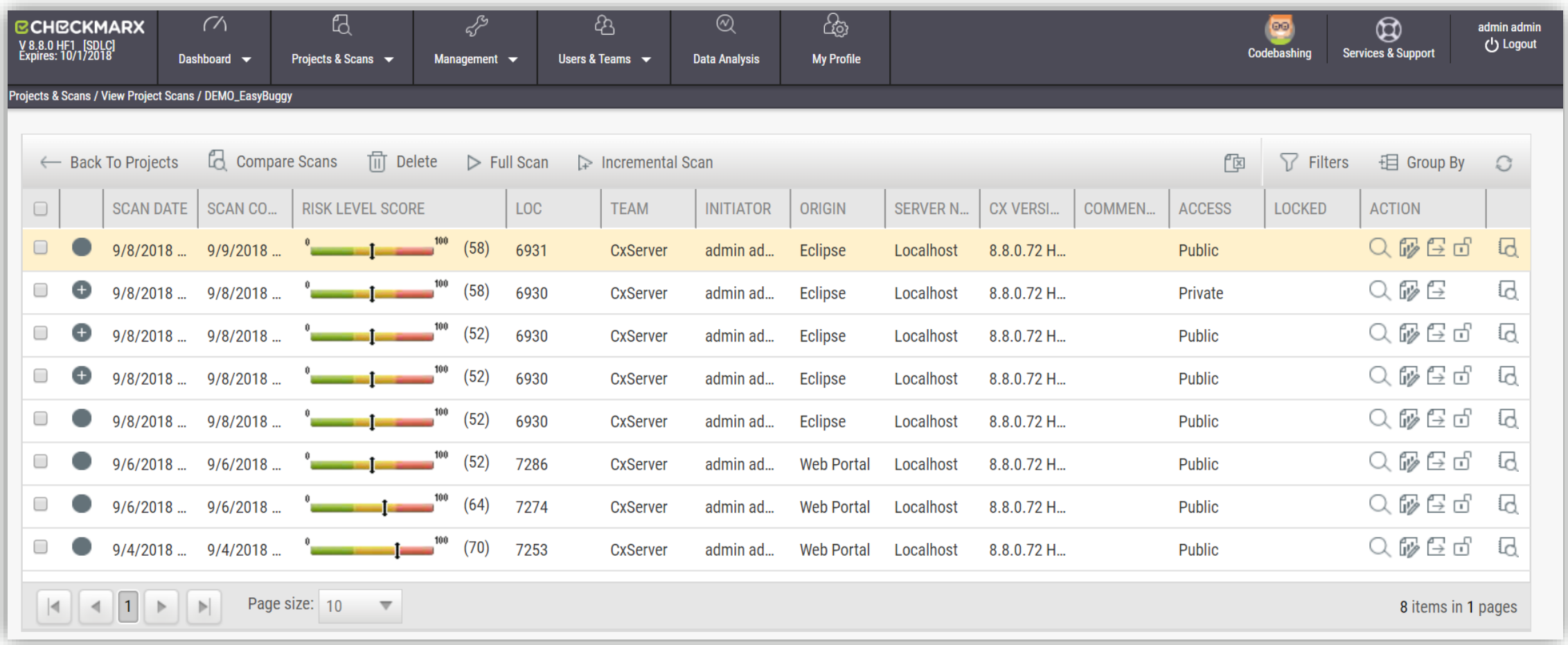
Organization Token from CxSAST8.9 Web portal

Database Table: CxComponentConfiguration



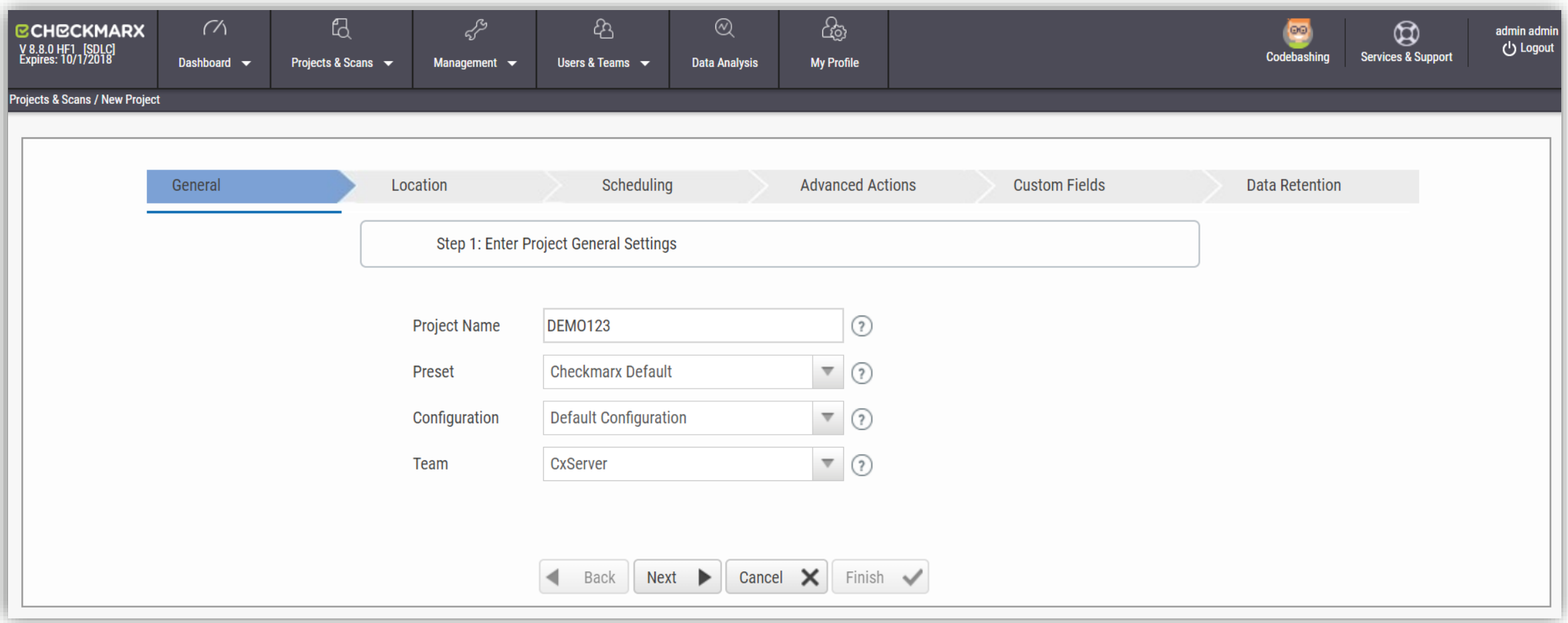
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Project Scans List



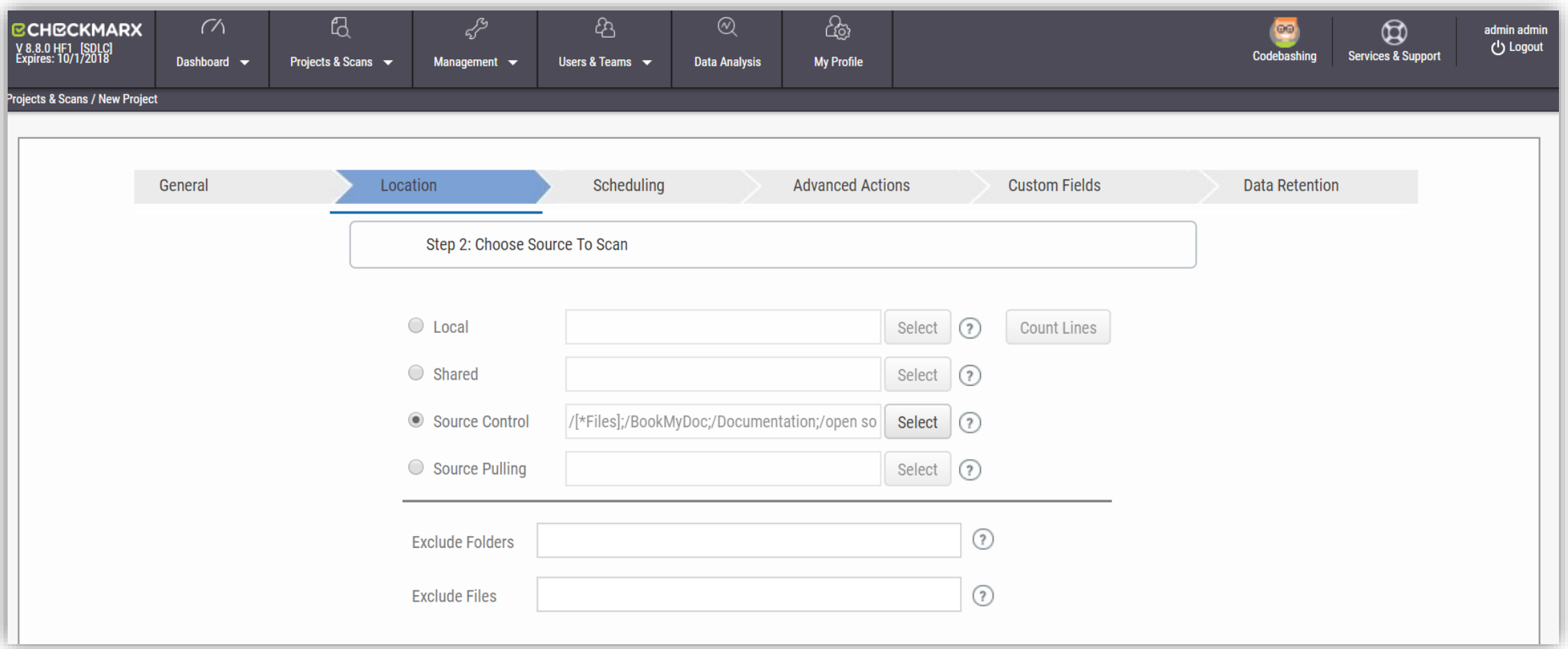
Create New Project

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



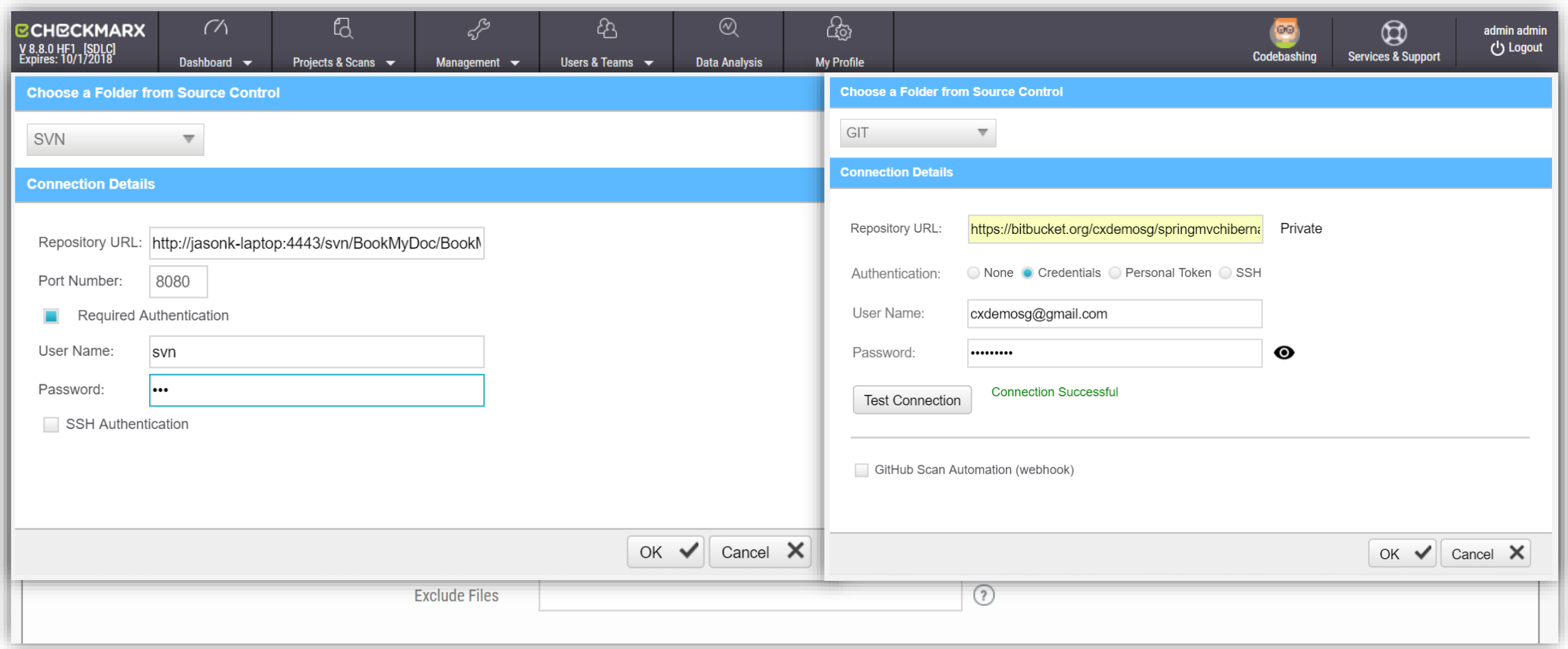
Create New Project

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



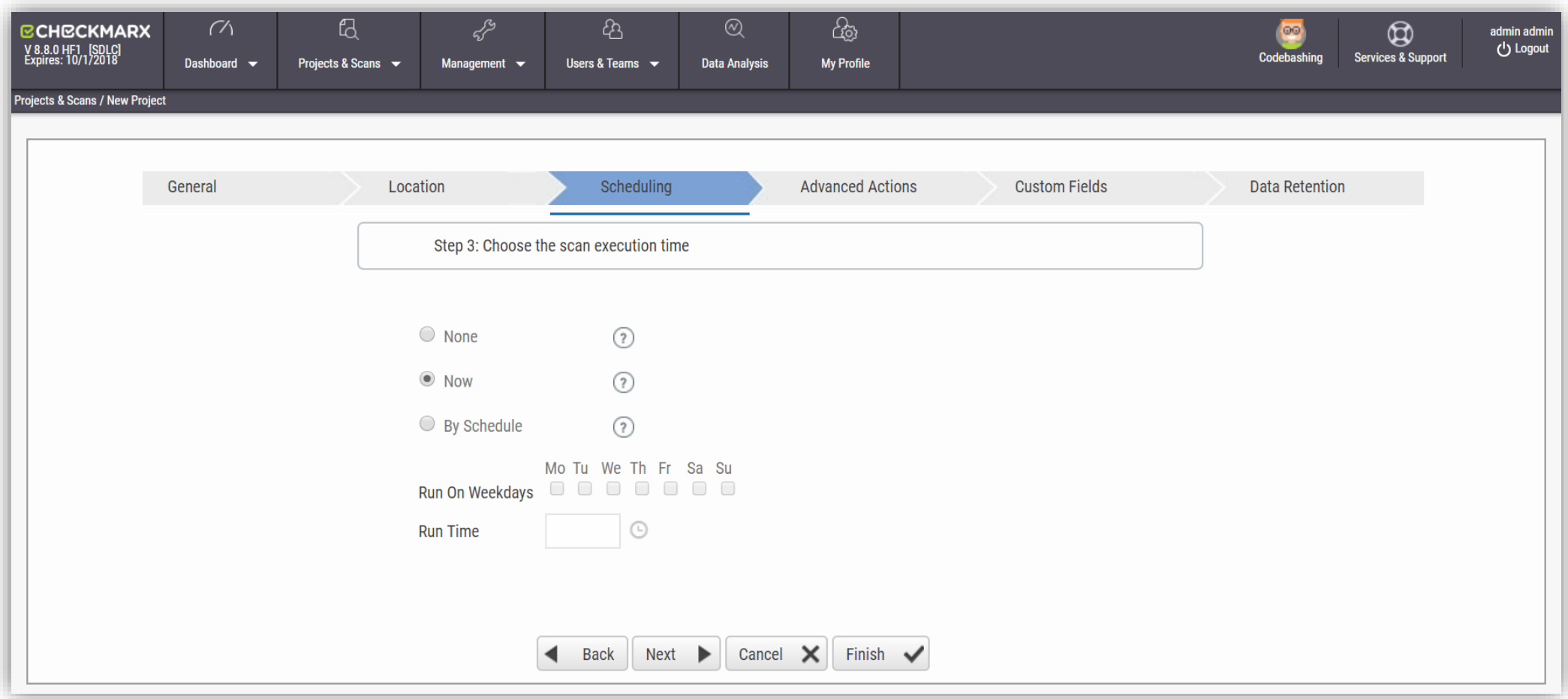
Create New Project

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



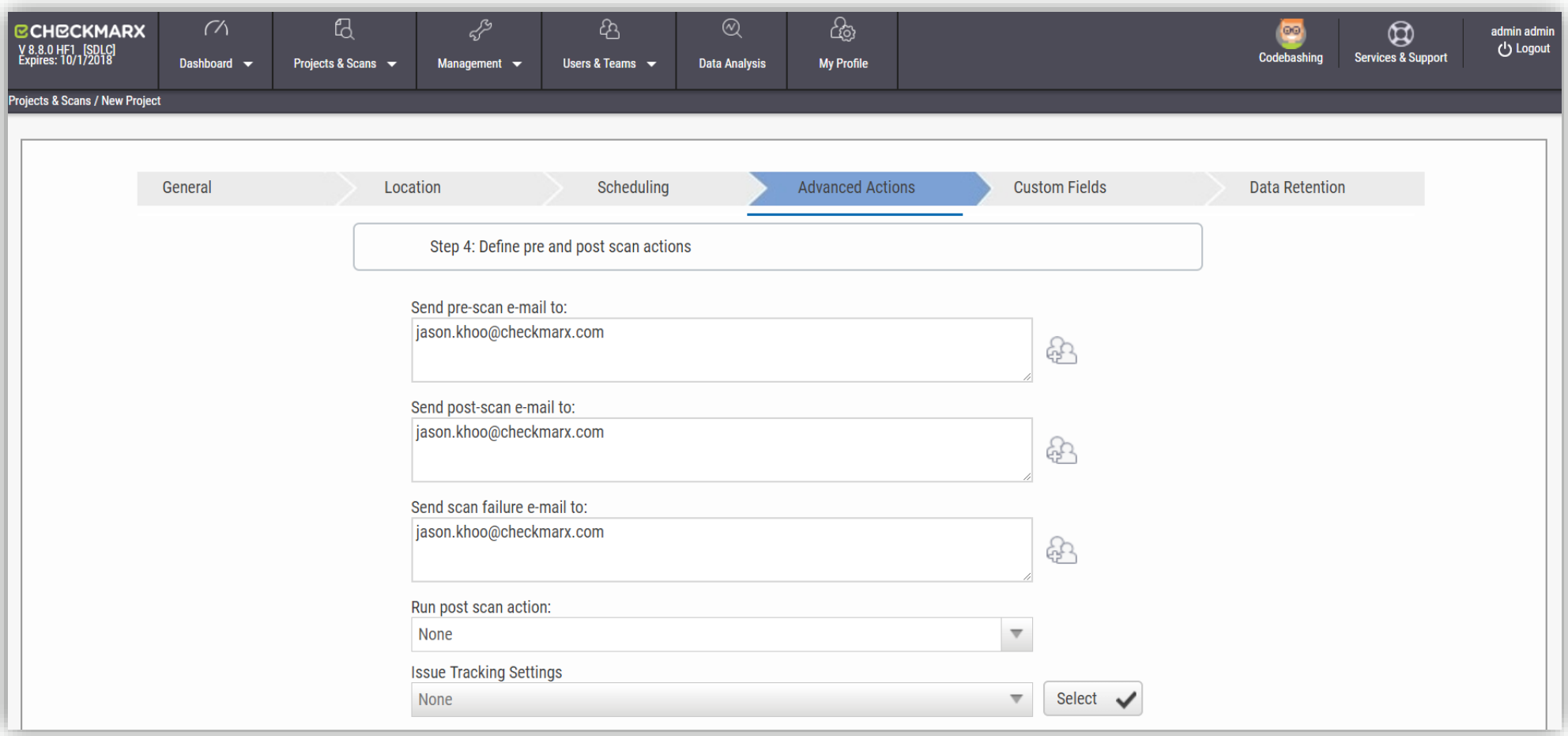
Create New Project

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



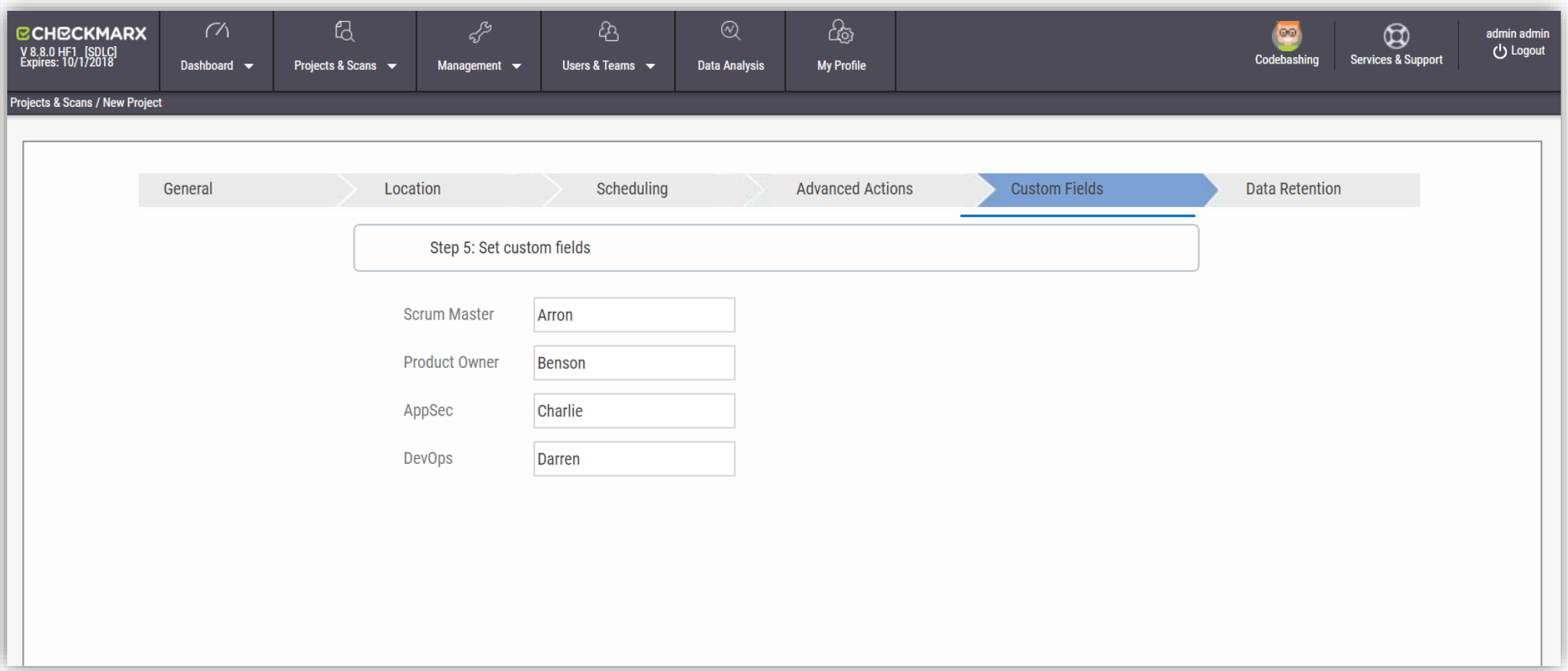
Create New Project

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



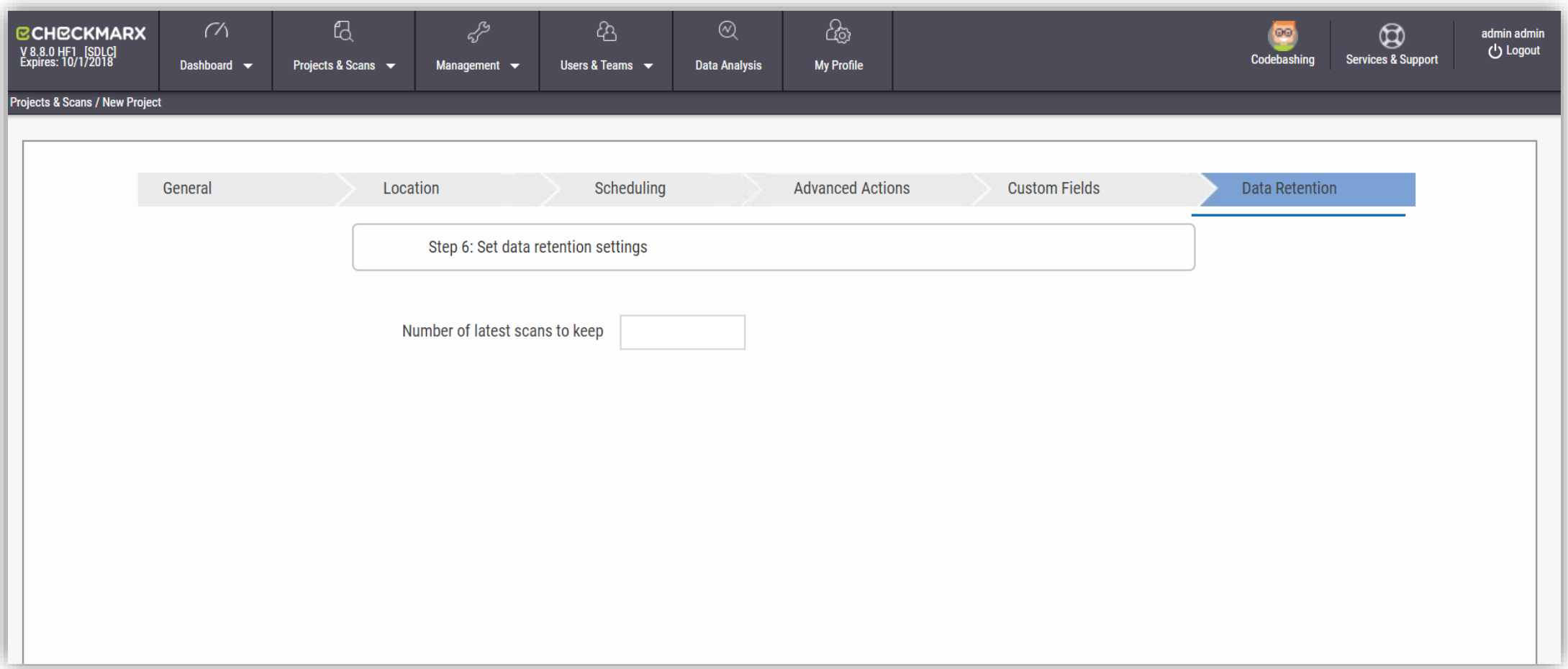
Create New Project

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



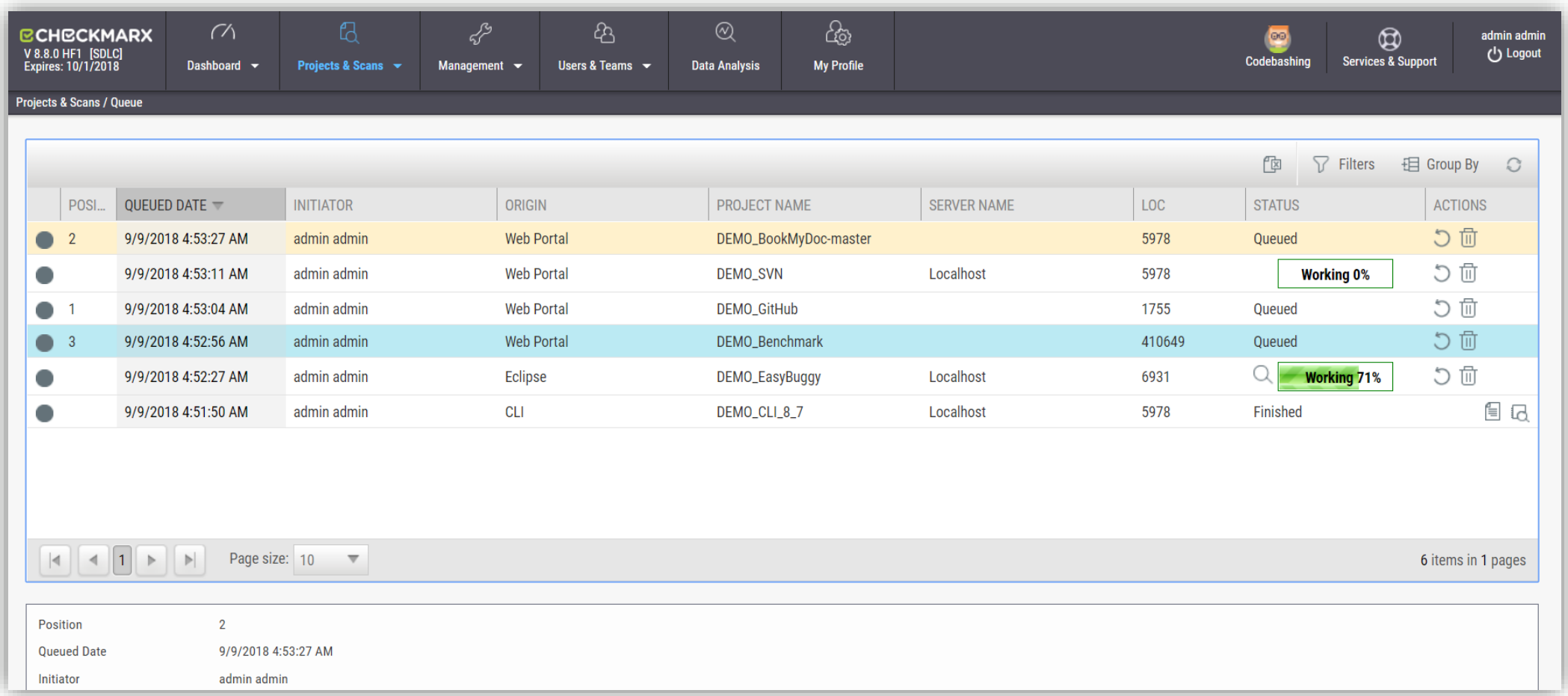
Create New Project

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



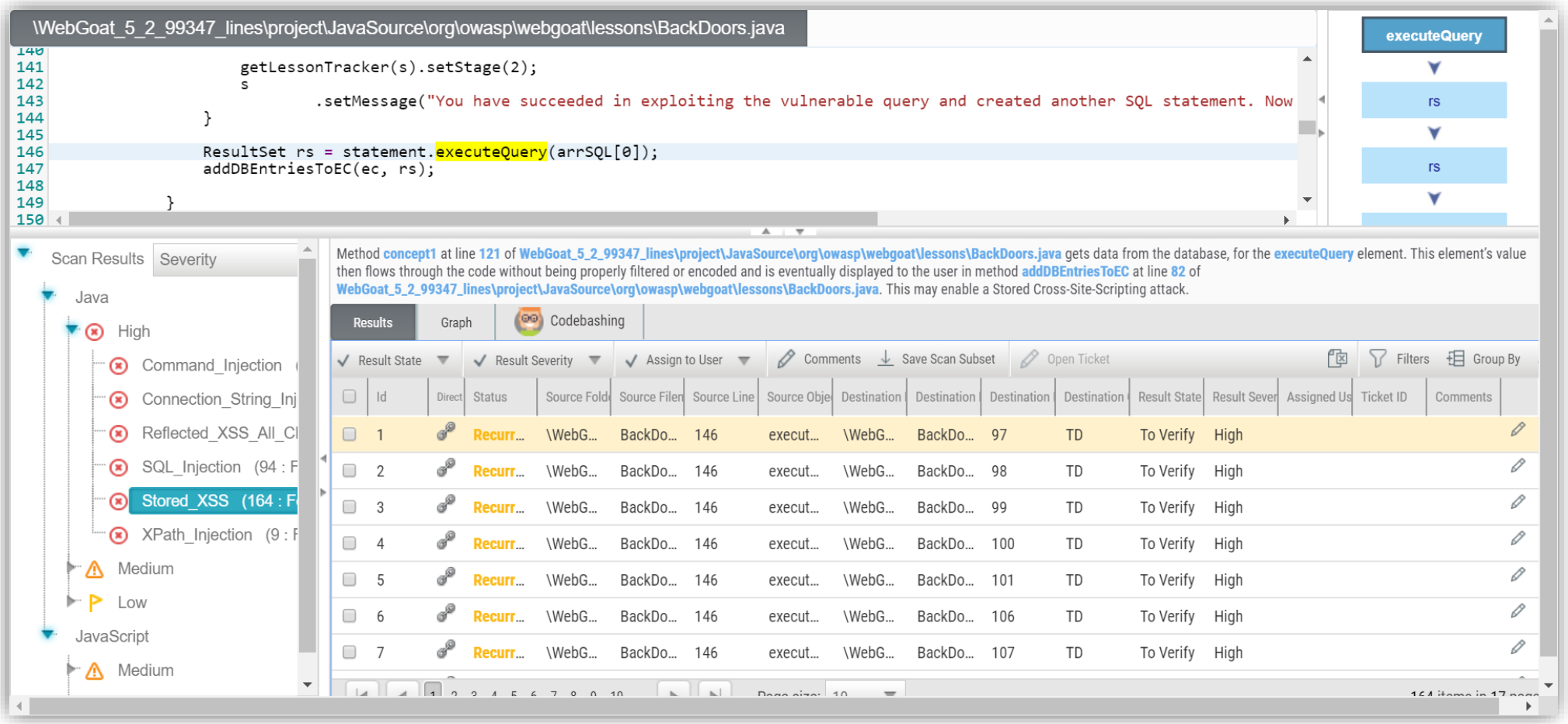
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Queue



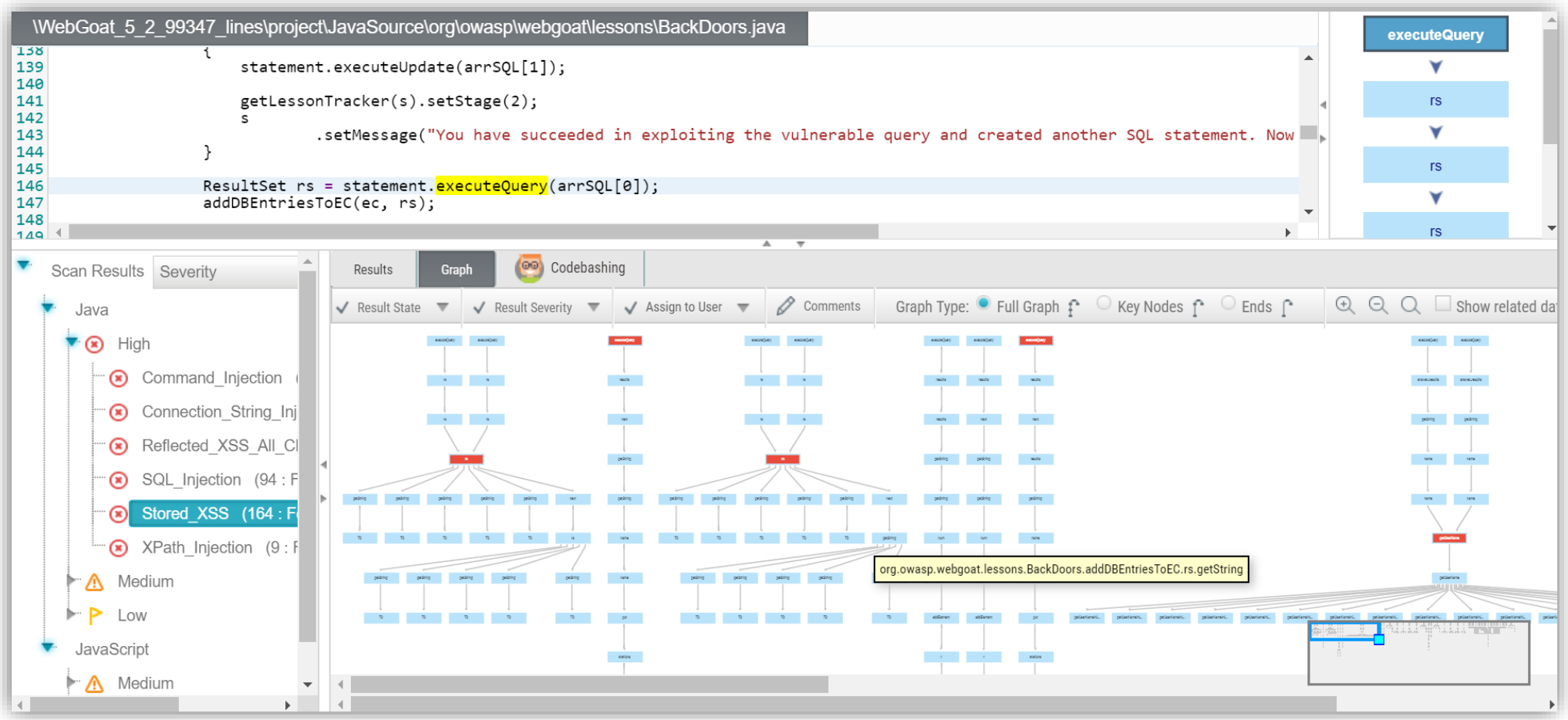
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review



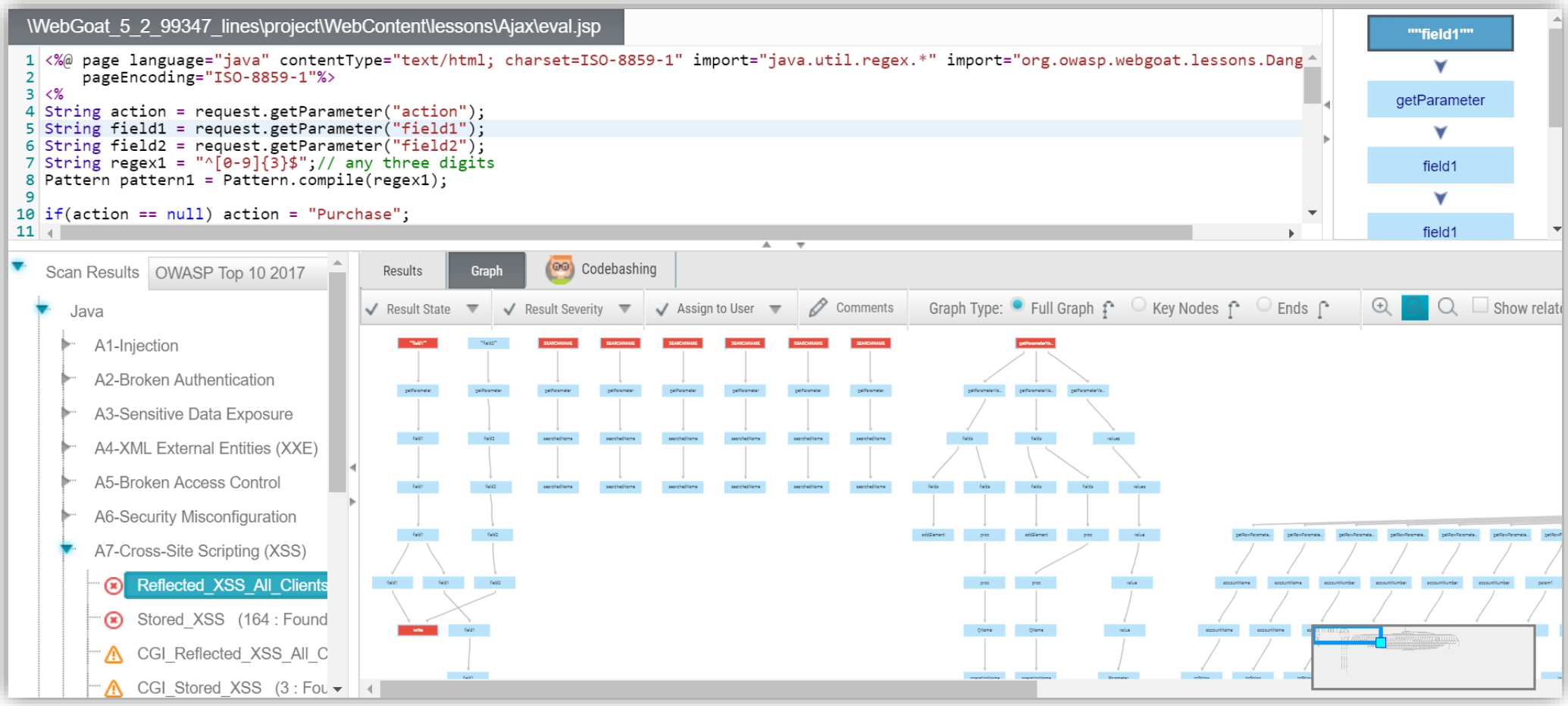
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review



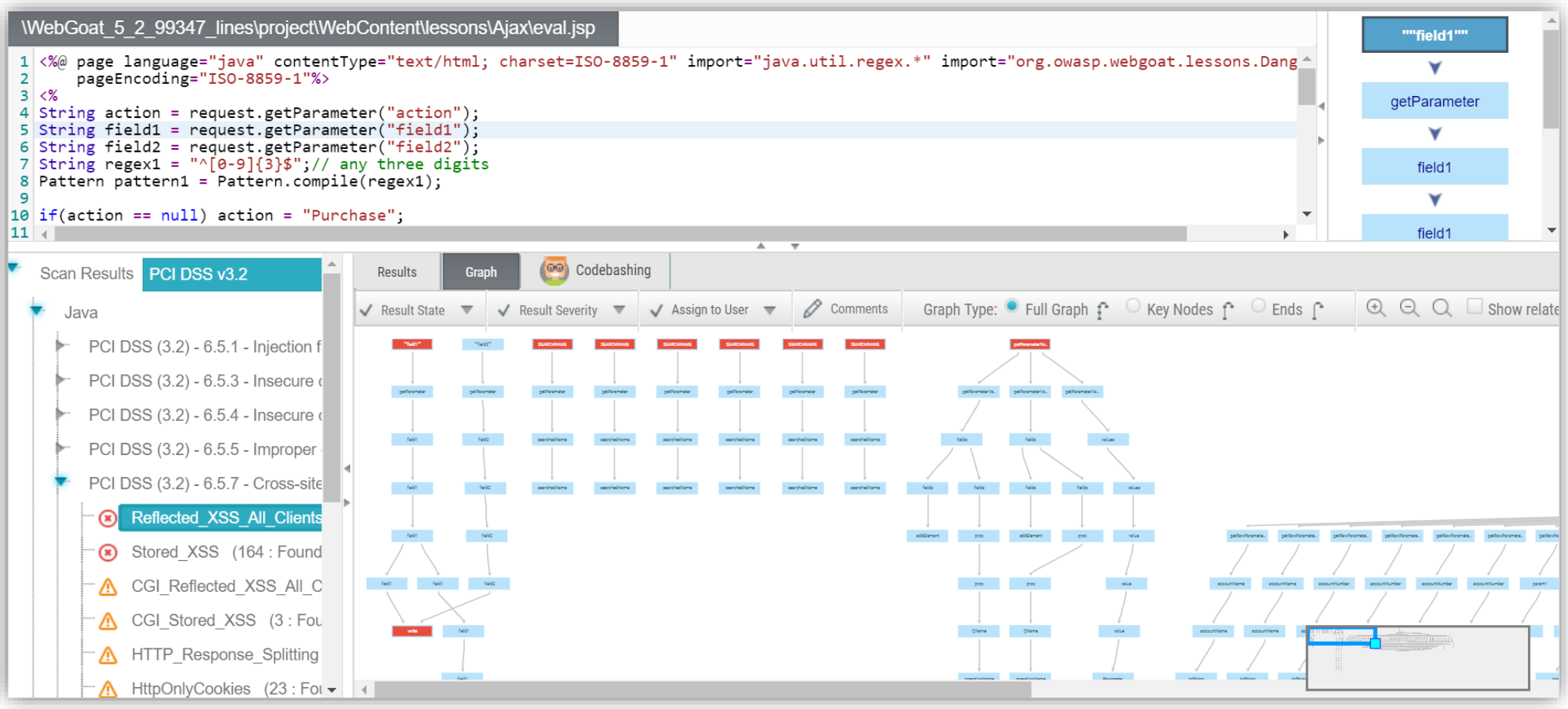
Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review – OWASP Top 10



Checkmarx CxSAST Web Portal

CxSAST Web Portal – Scan Result Review – PCI DSS



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

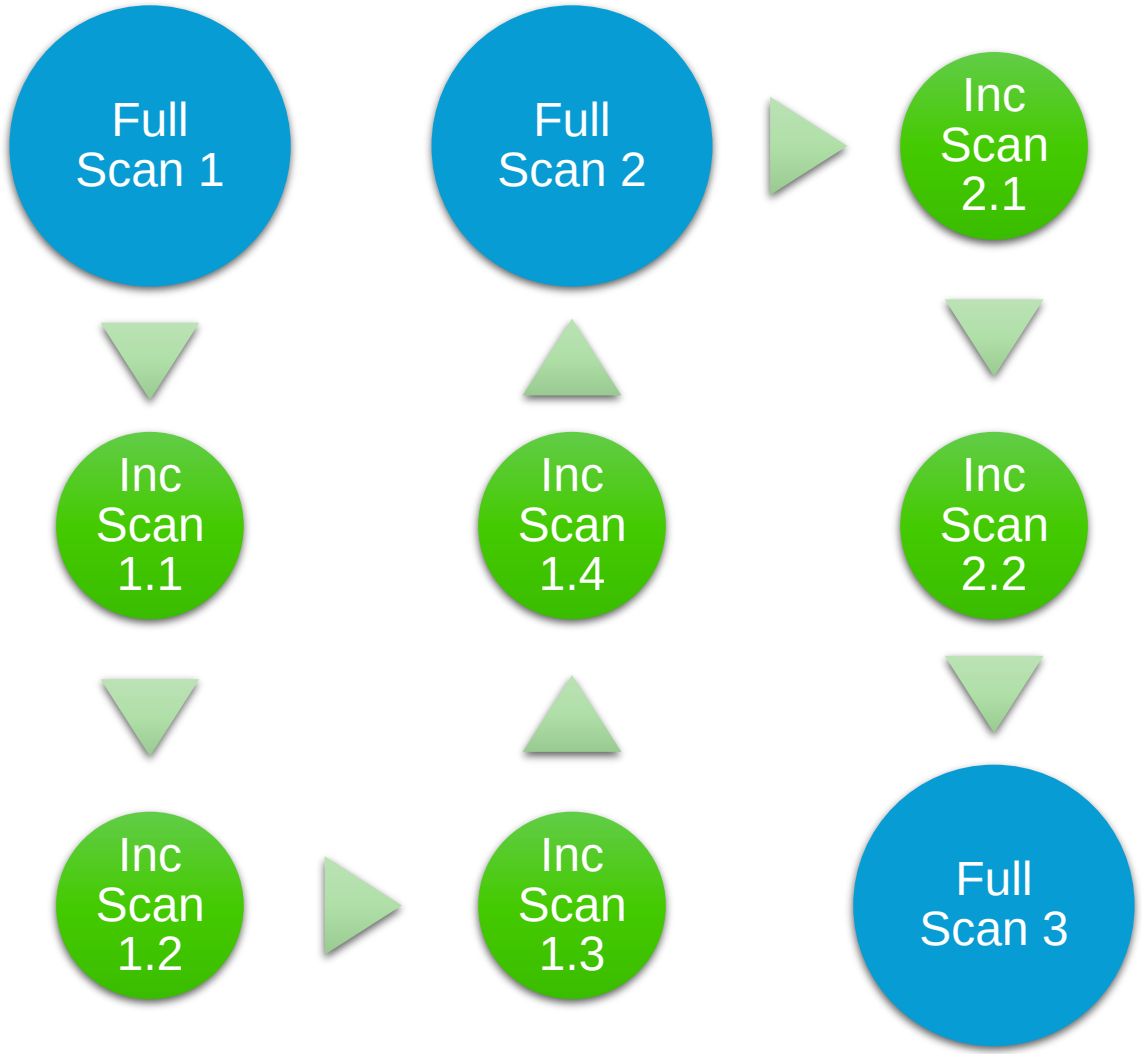
Full and Incremental Scans

Full scan

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

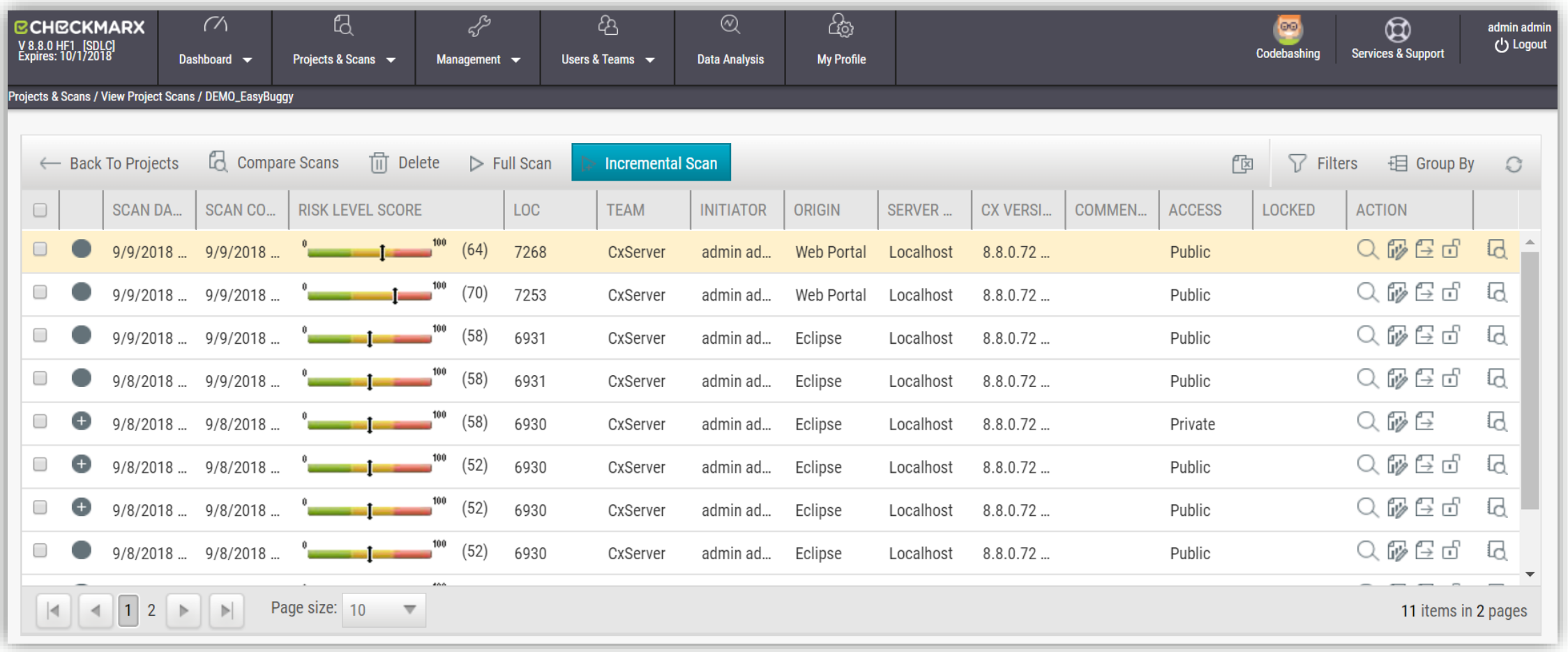
Incremental scan

- 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

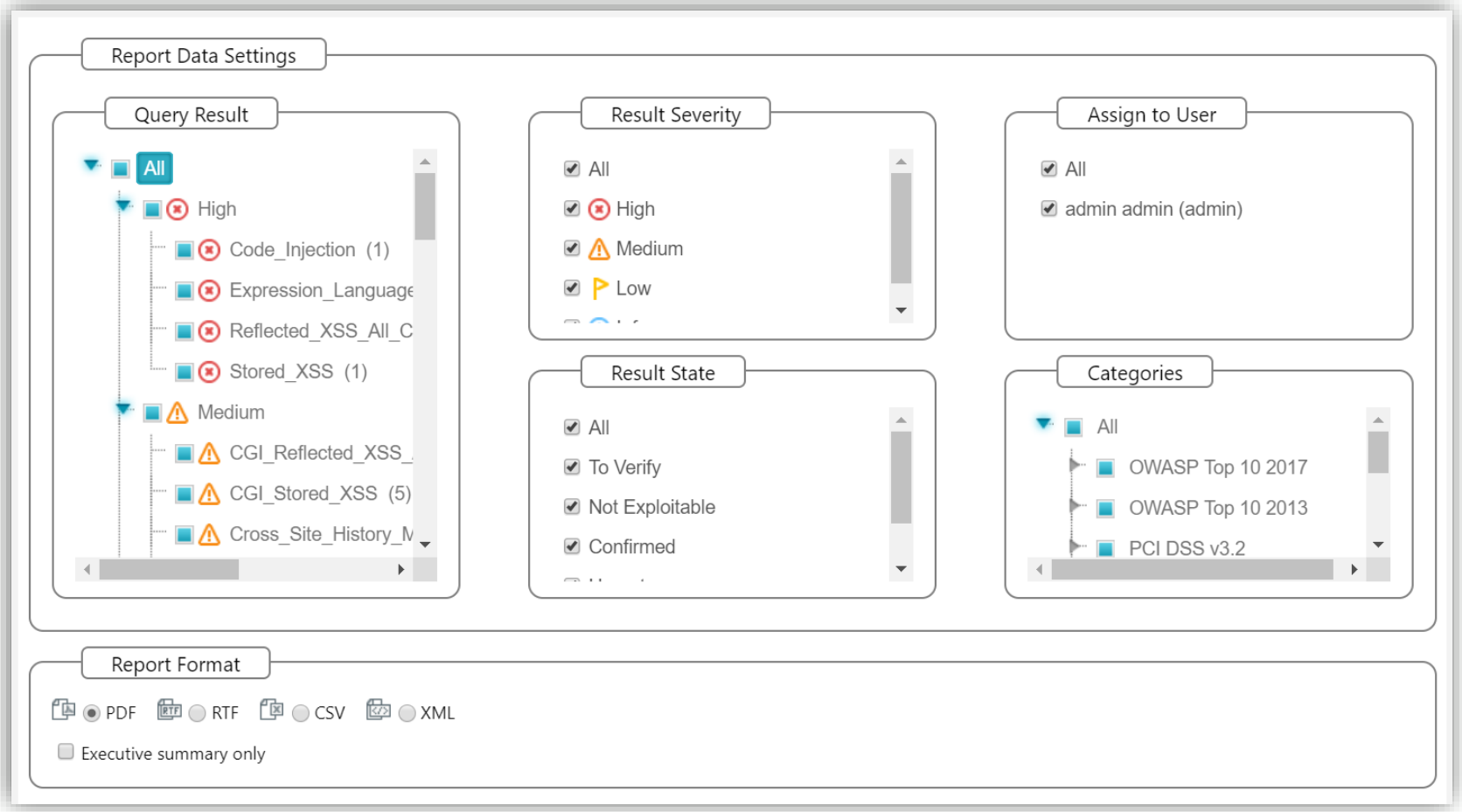
Full and Incremental Scan Option



Checkmarx CxSAST Web Portal

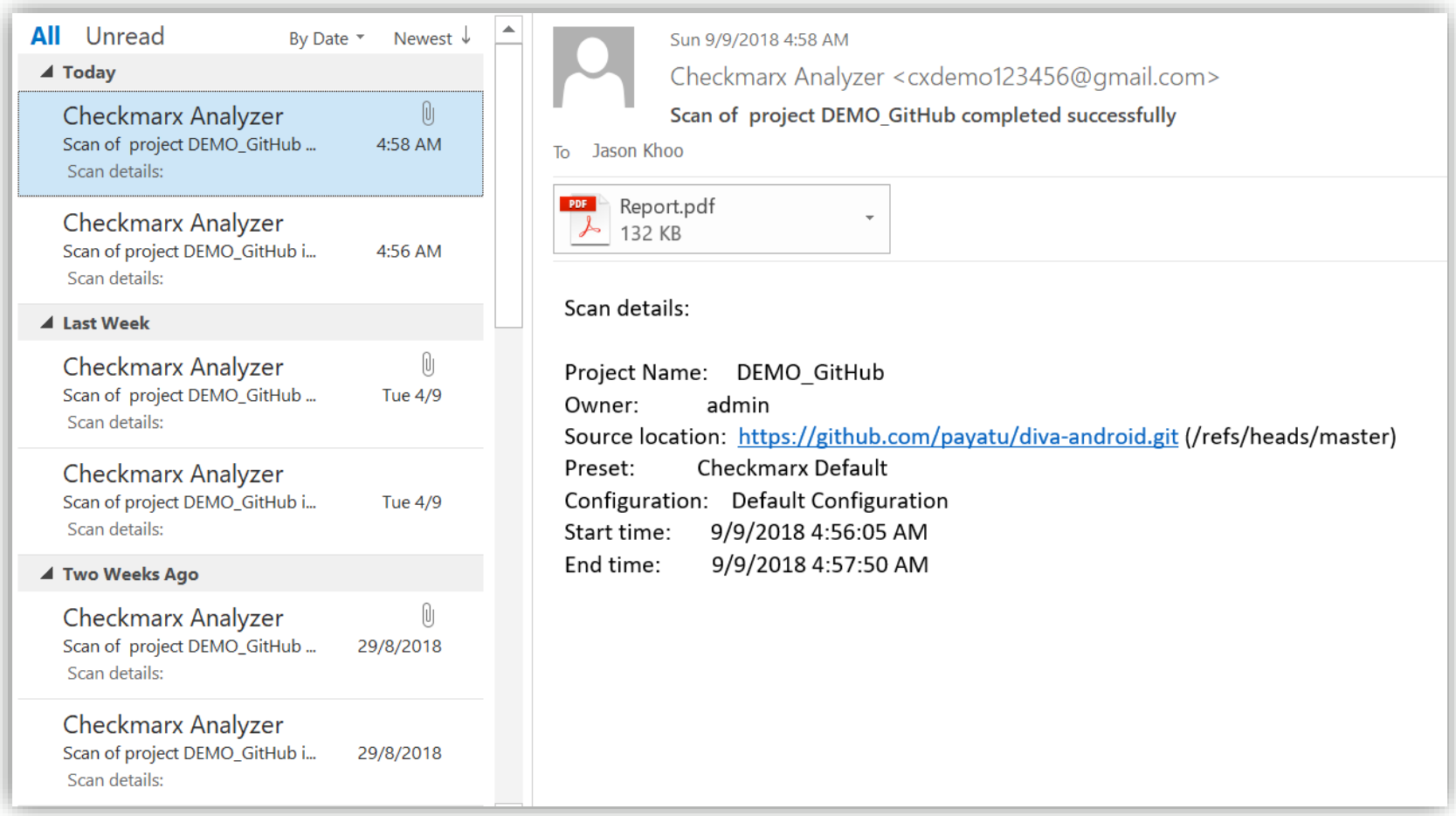
Scan Report

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



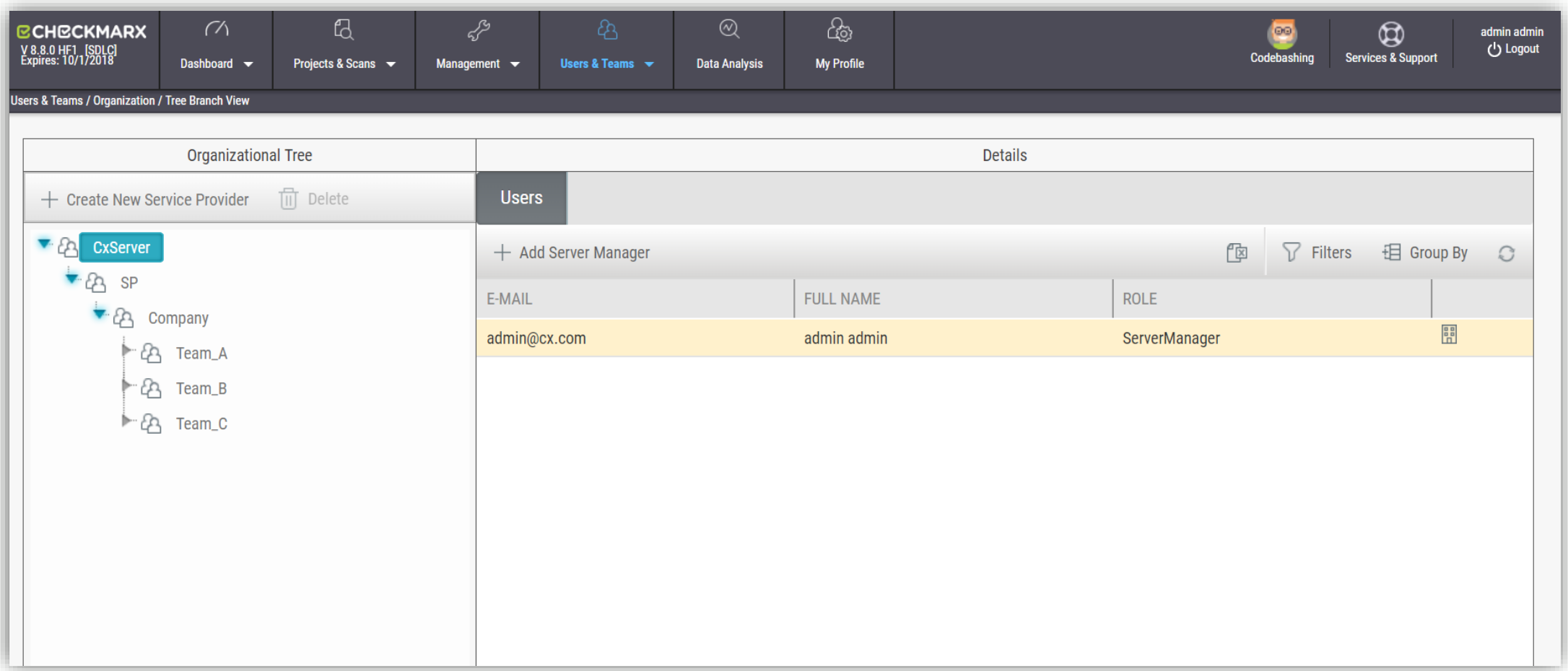
Scan Notification

CxSAST Project Scan – Email Notification

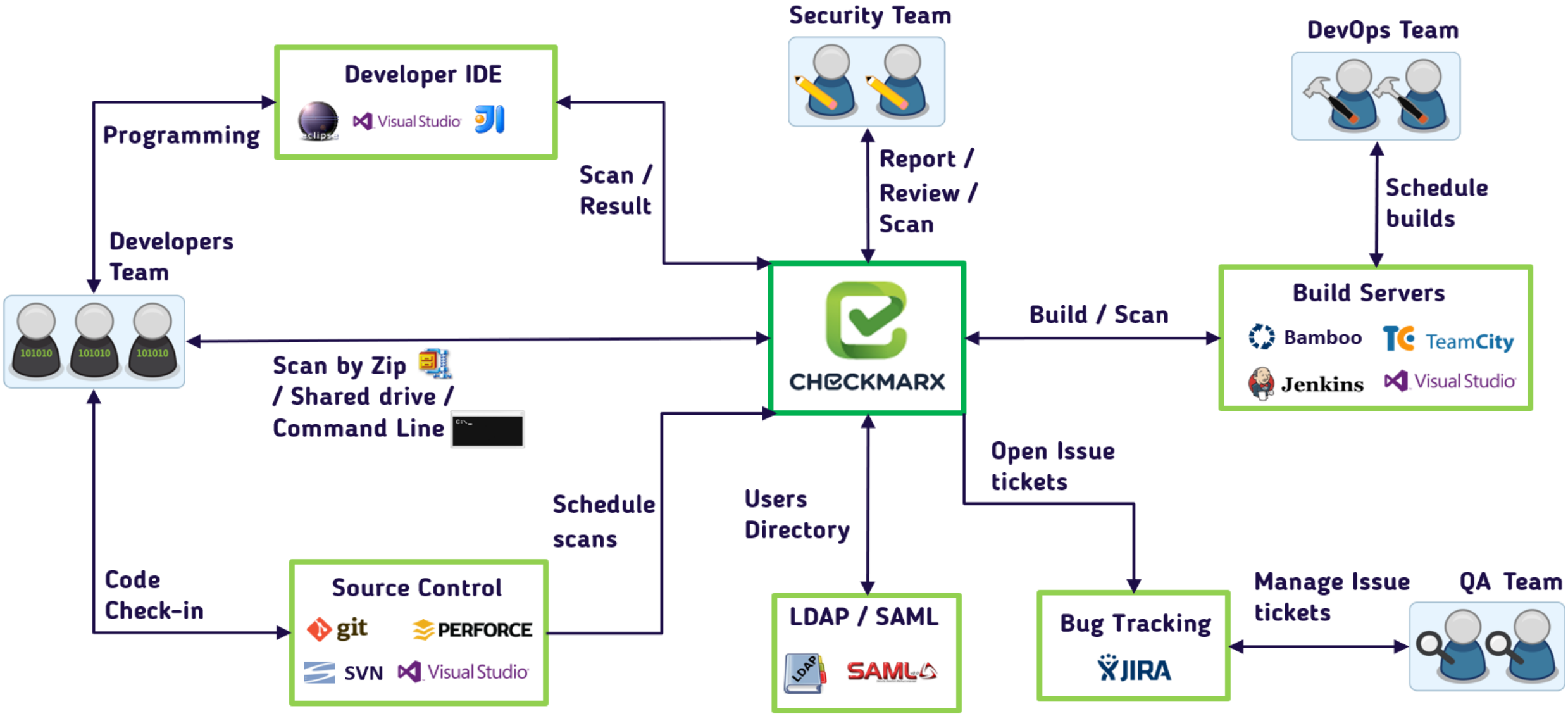


Users Management

CxSAST Web Portal – Organizational – Tree Branch View



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

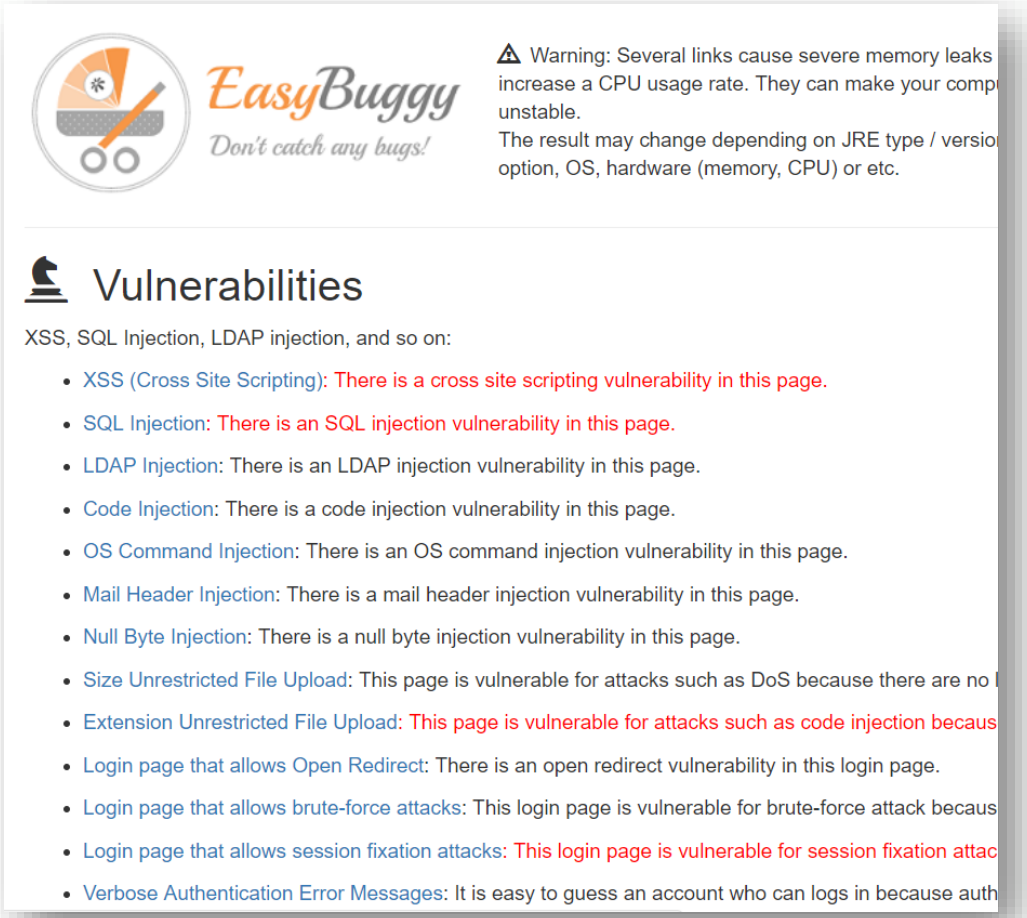
CxOSA : Zip

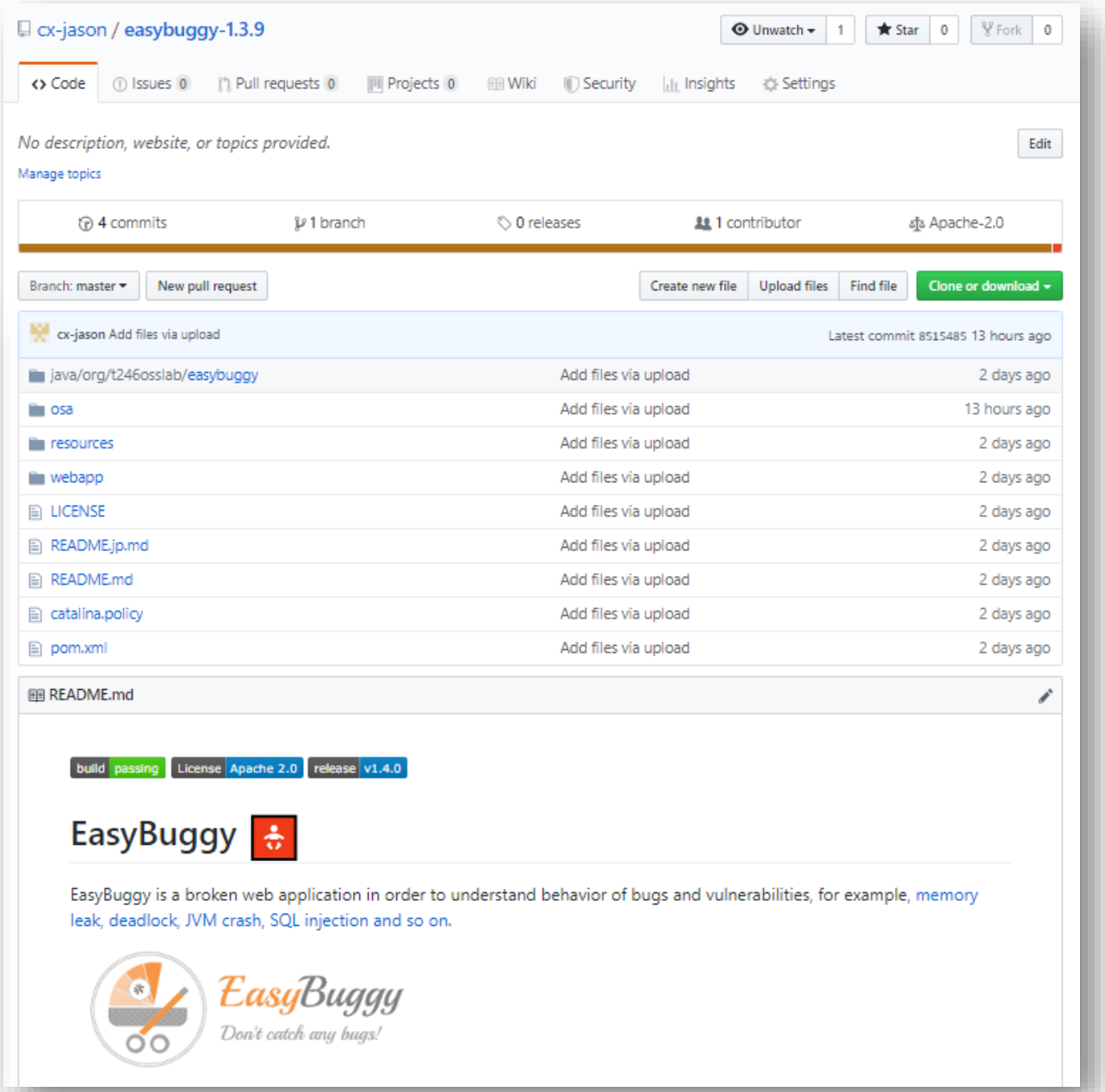
Java Project: EasyBuggy
Result Review & Remediation

Checkmarx

Project EasyBuggy

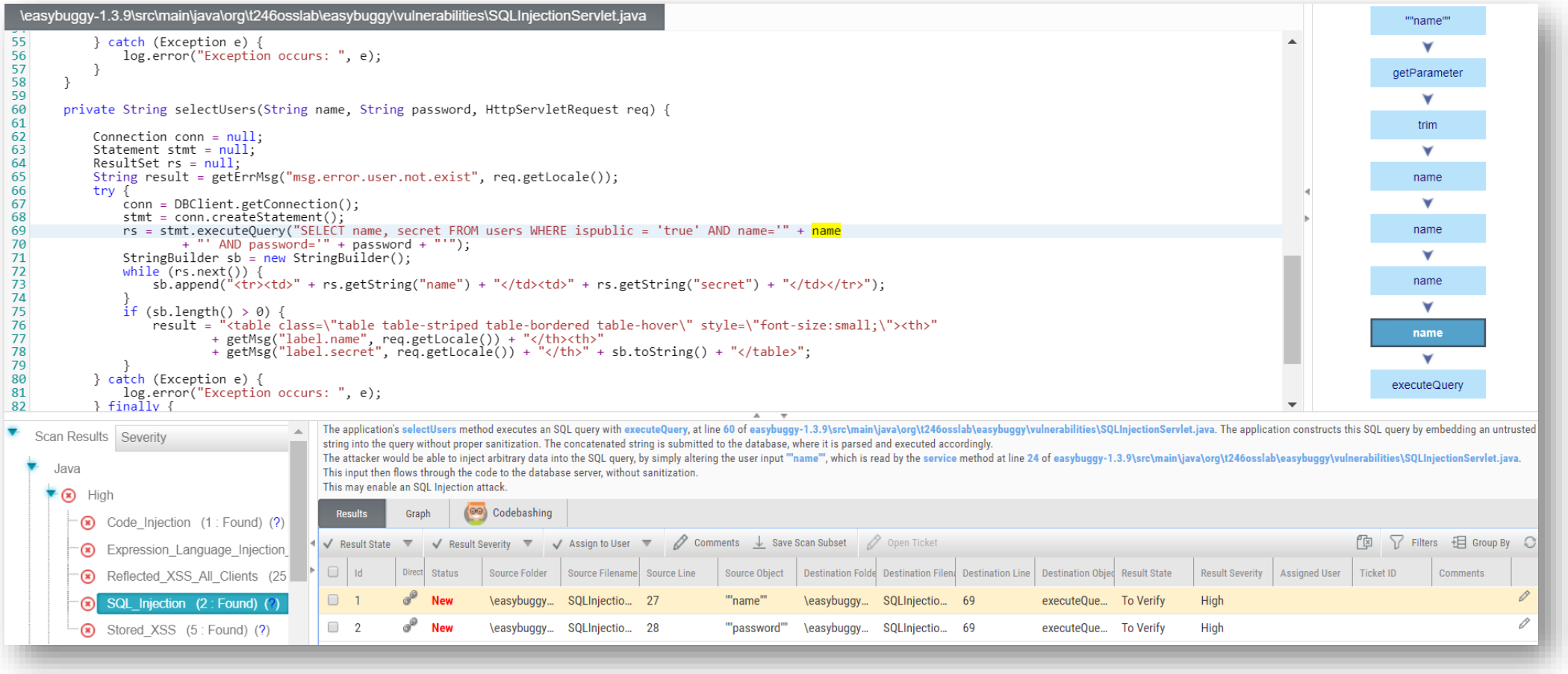
https://github.com/cx-jason/easybuggy-1.3.9





Exercise 4: Scan Result Review & Remediation

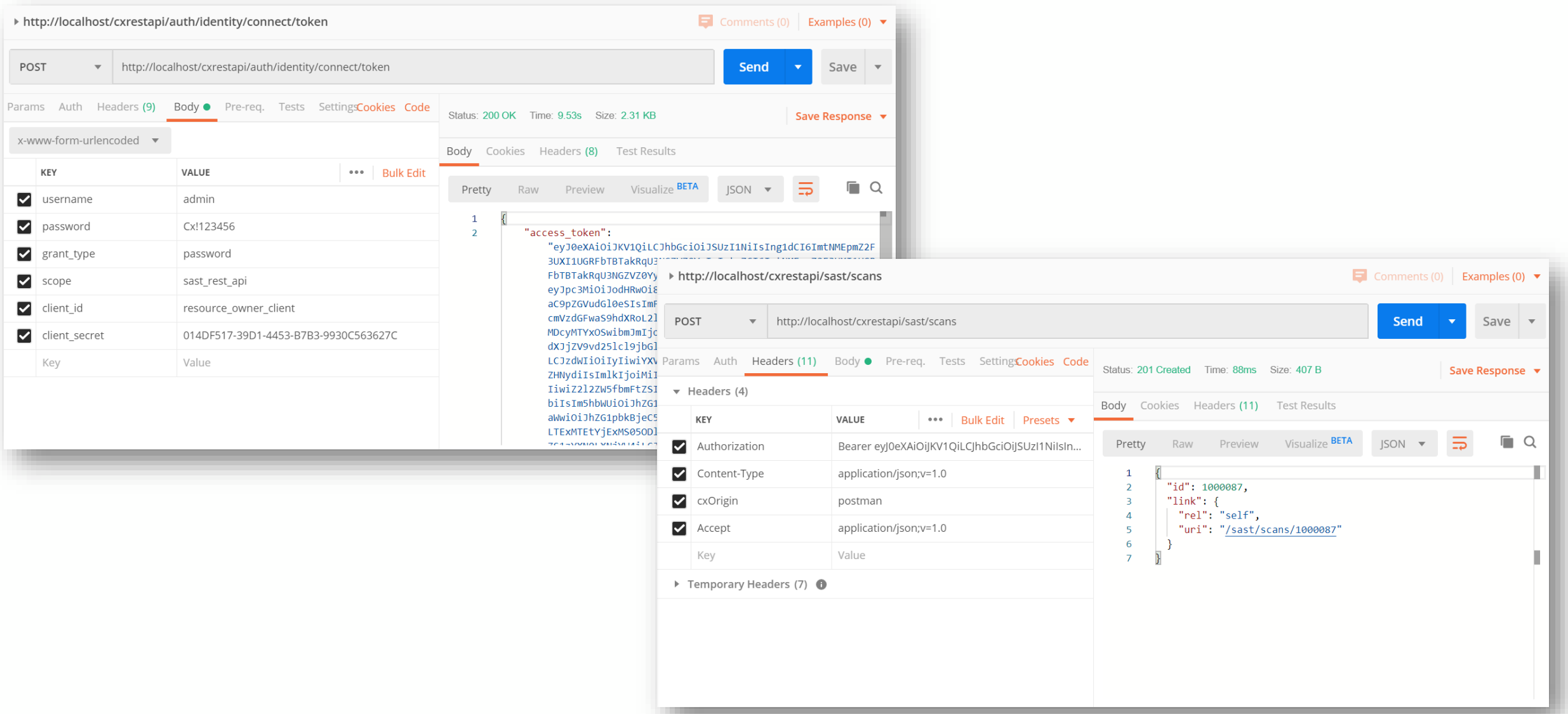
Remediation for the SQL Injection vulnerabilities



/ CxSAST Integration

Checkmarx

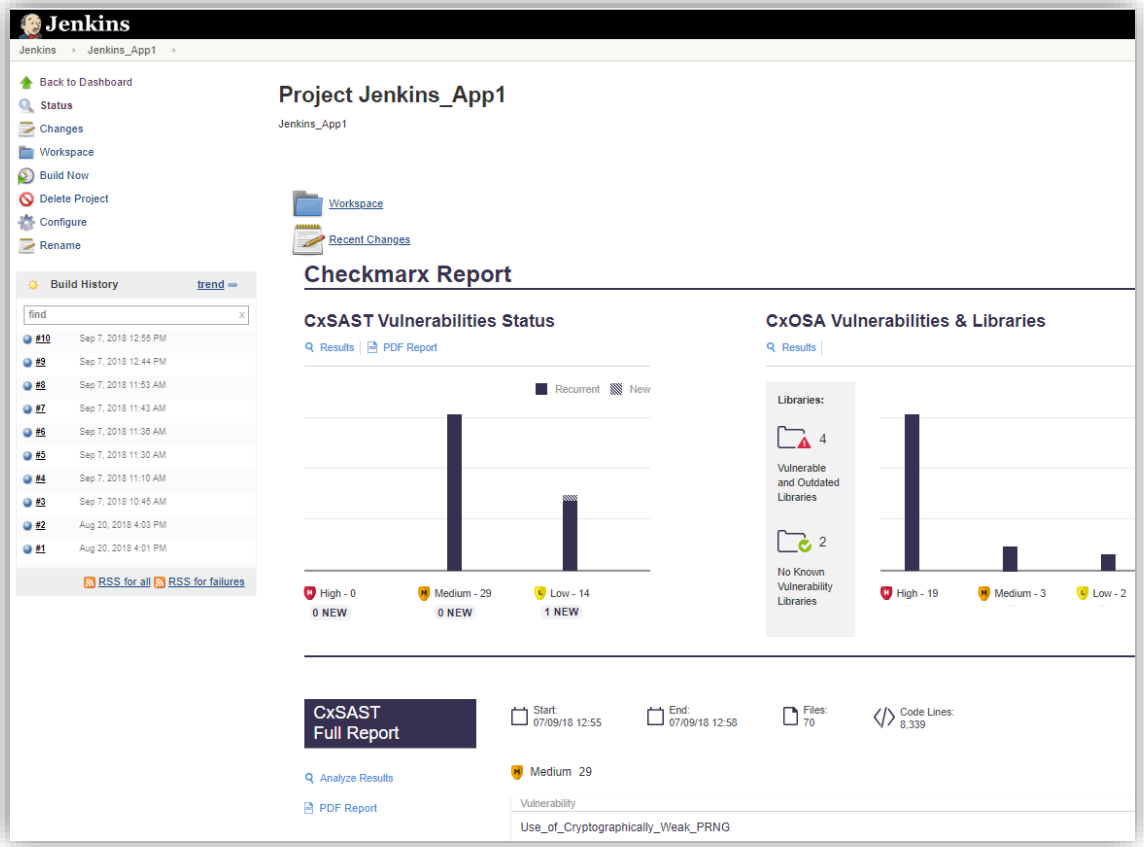
CxSAST REST API

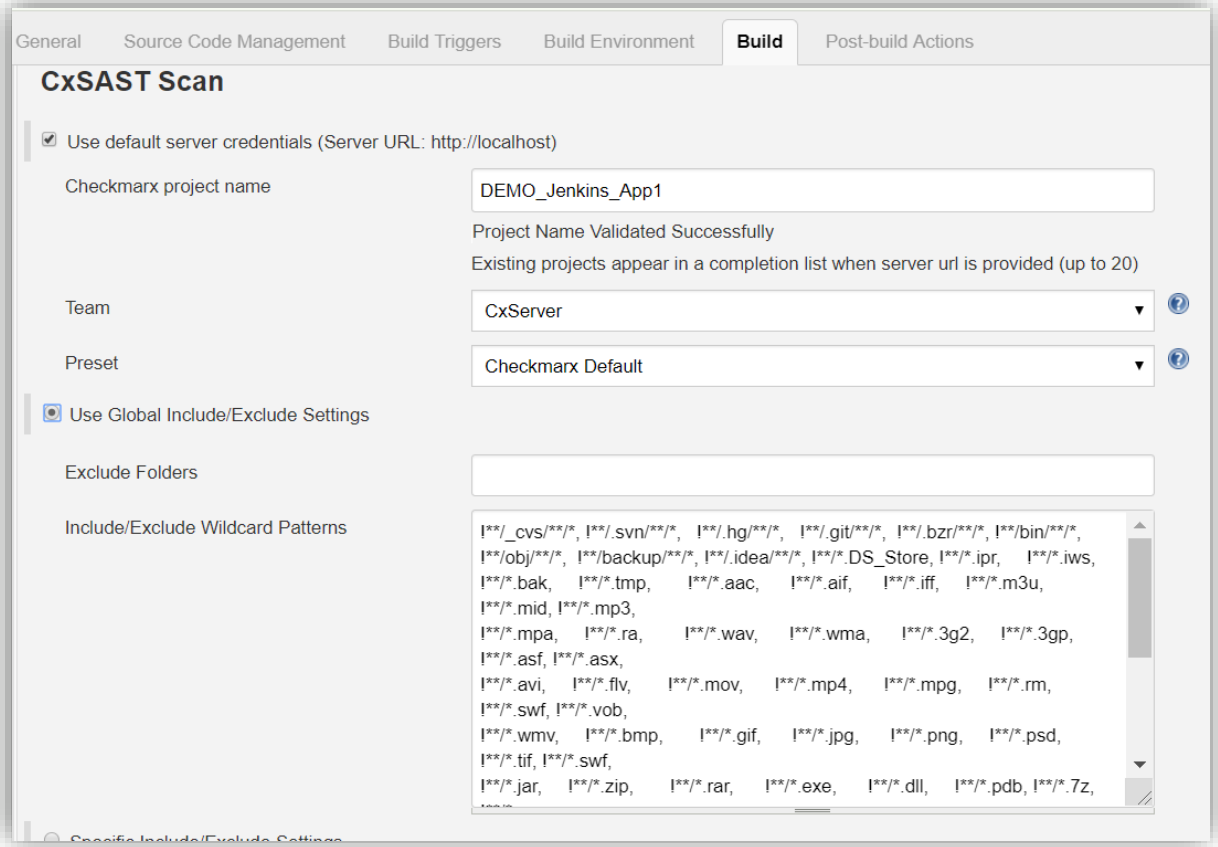


CxSAST CxConsole, Command Line Interface

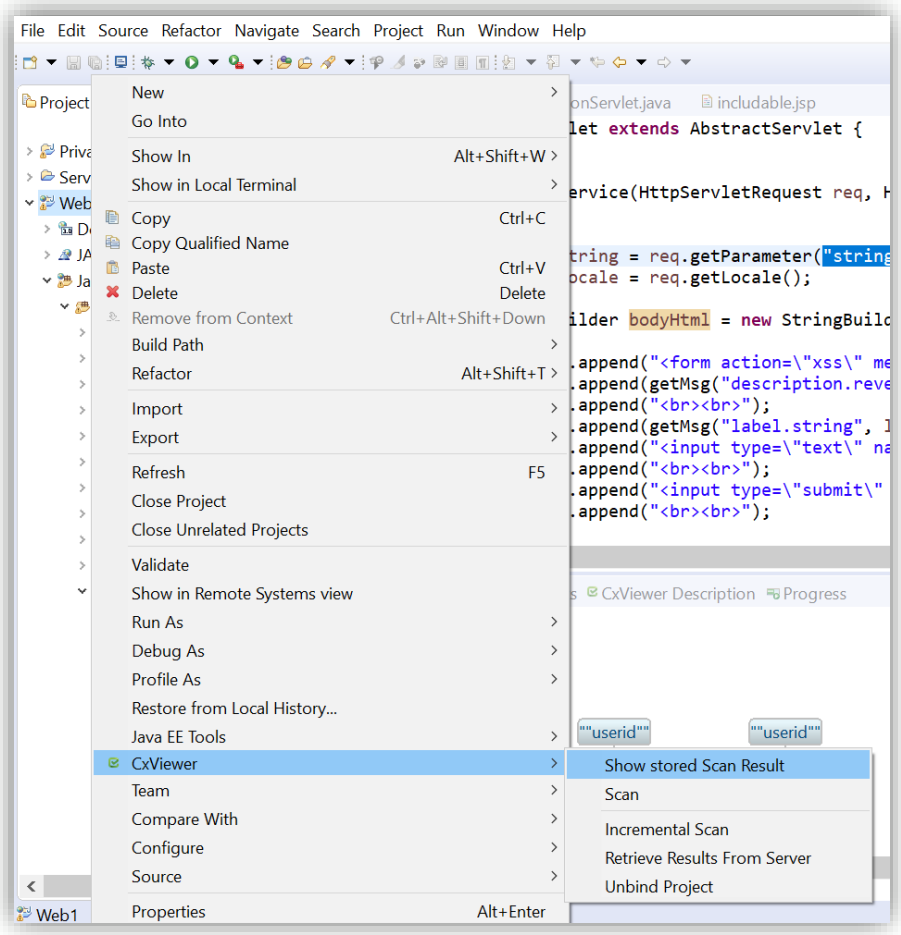
```
[2019-10-10 00:53:38,927 INFO ] Verbose mode is activated. All messages and events will be sent to the console or log file.
[2019-10-10 00:53:38,927 INFO ] CxConsole version 8.80.2
[2019-10-10 00:53:38,927 INFO ] CxConsole scan session started
[2019-10-10 00:53:38,927 INFO ]
[2019-10-10 00:53:38,942 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
```

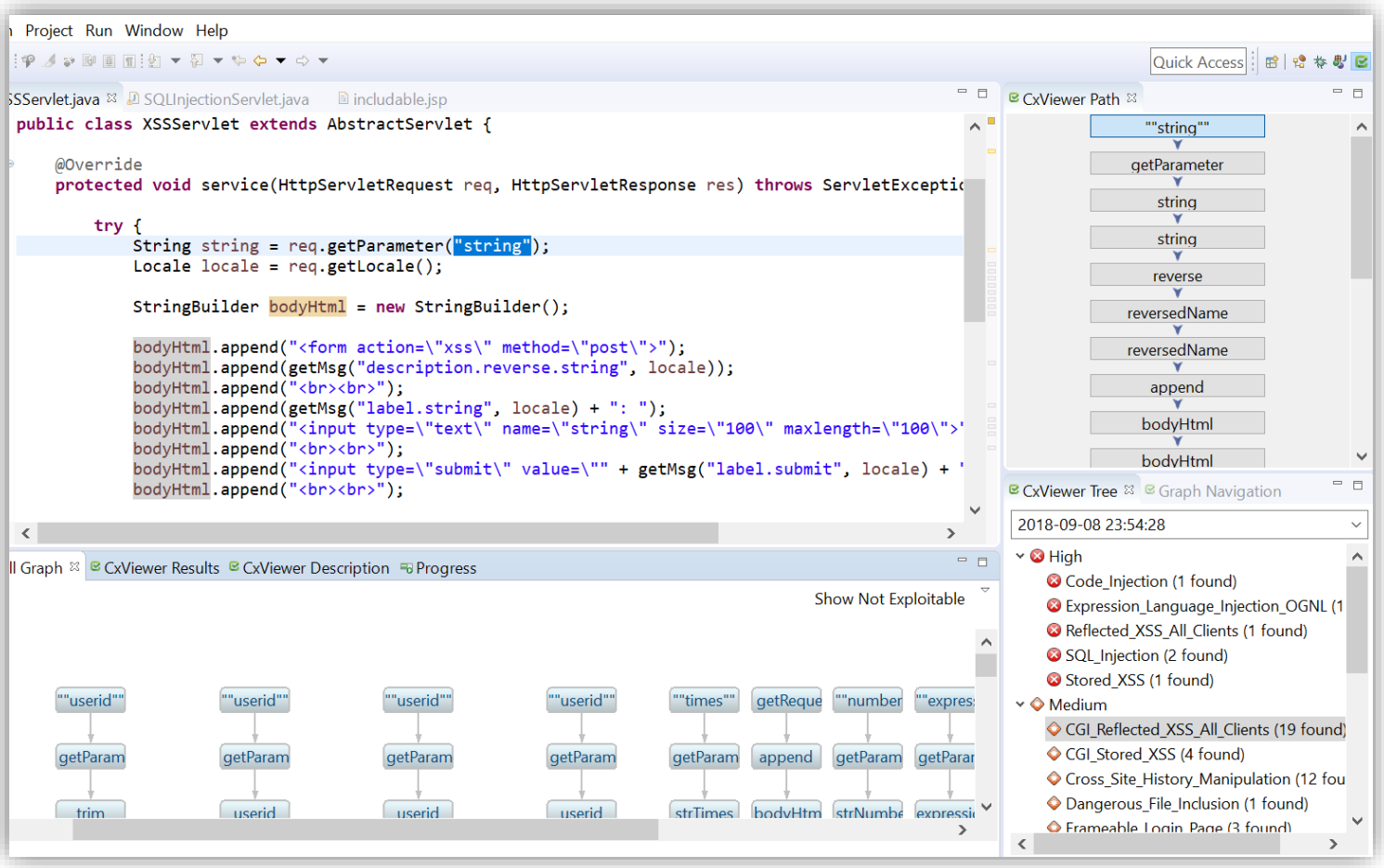
CxSAST Integration with Jenkins Portal





CxSAST Integration with Eclipse Plugin





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

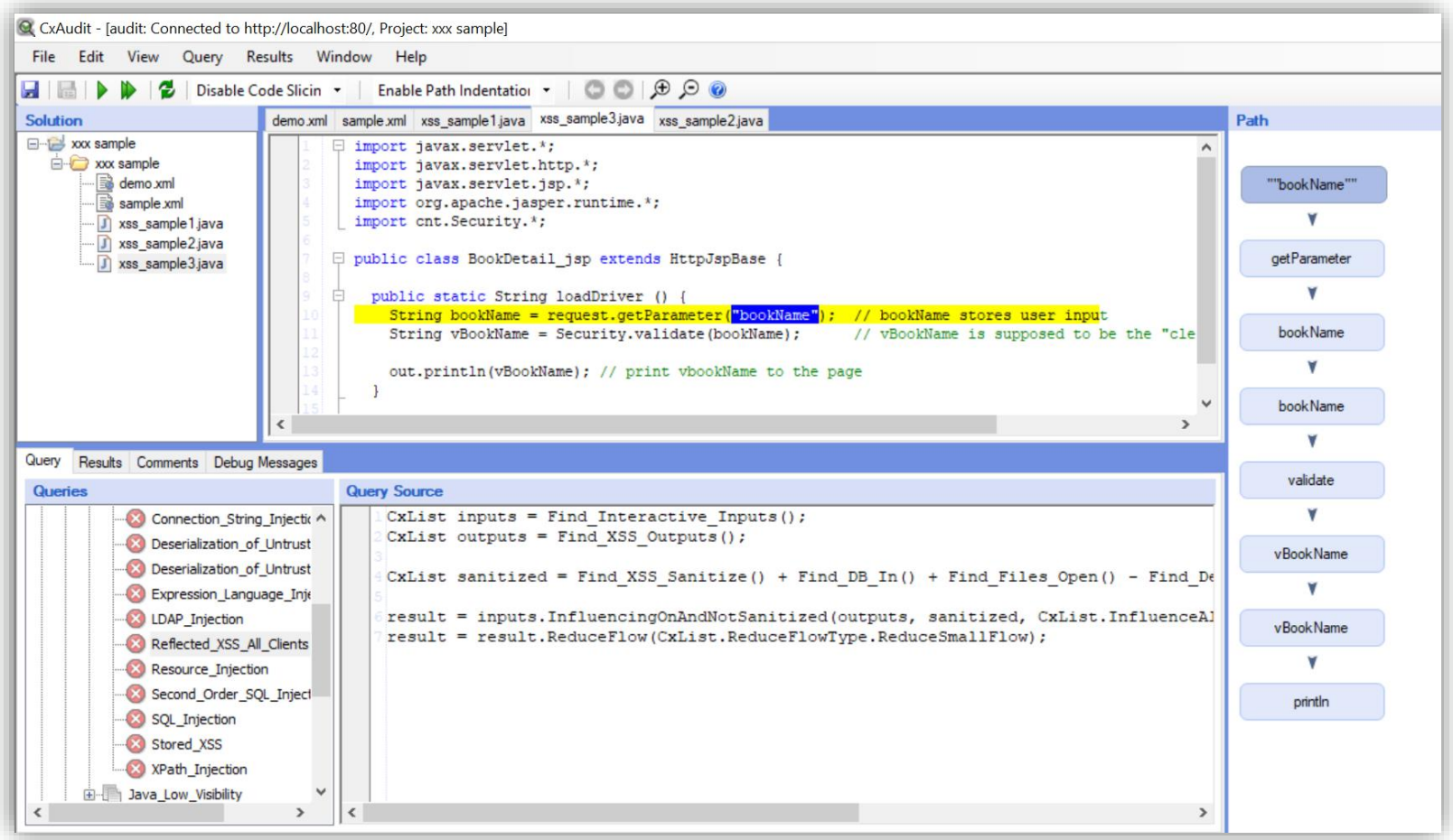
/ CxAudit Session

Checkmarx

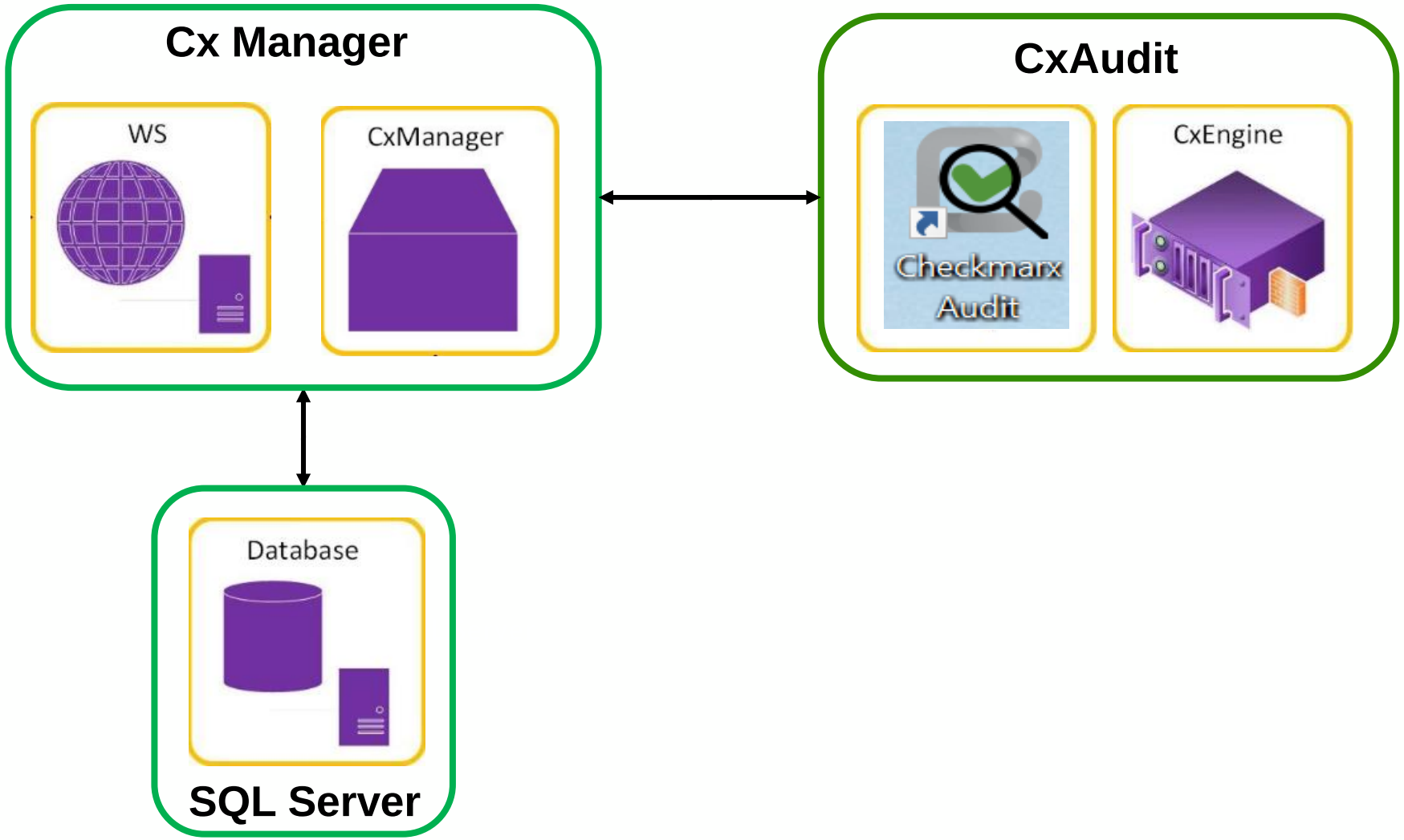
CxAudit

CxAudit

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

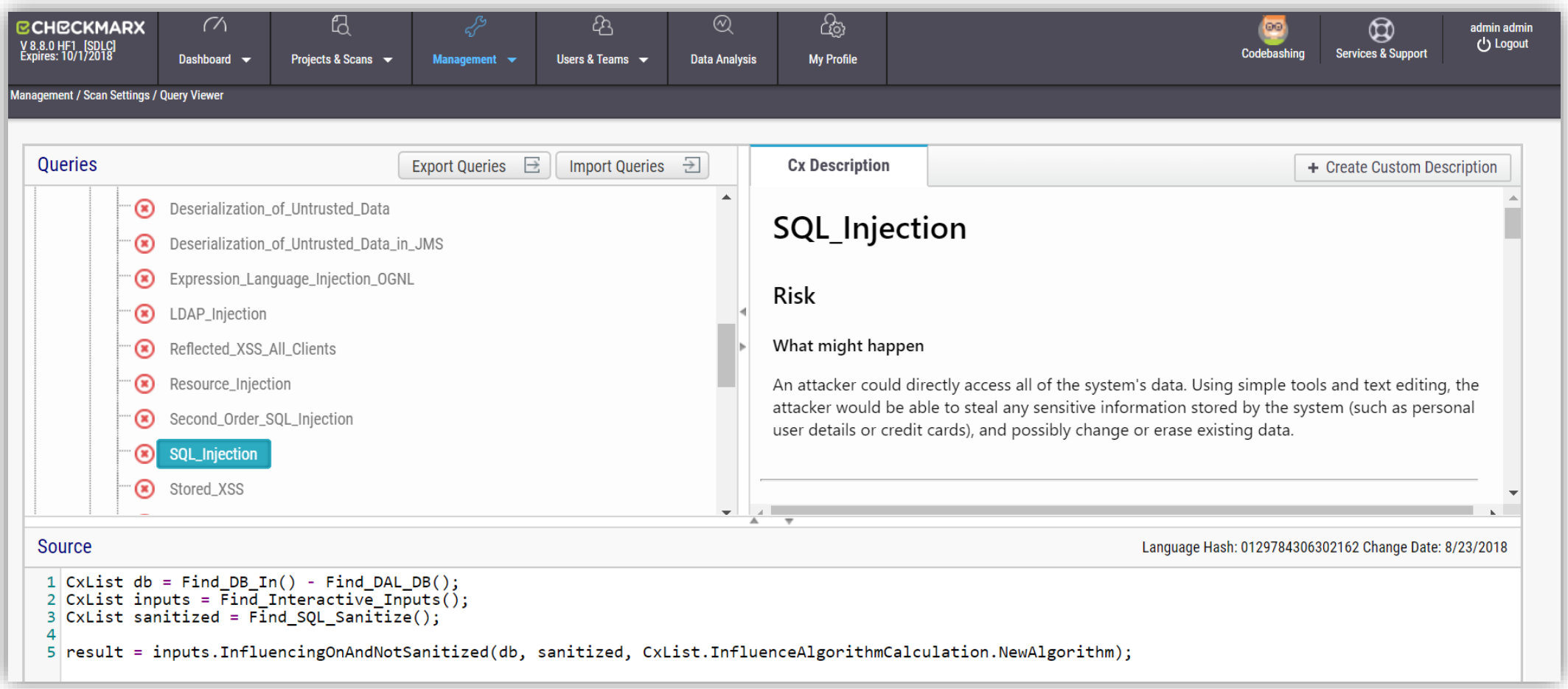


CxAudit Architecture



Checkmarx CxSAST Web Portal

CxSAST Web Portal – Query Language Viewer



Exercise 6: CxAudit Session

CxAudit demonstration and practice:

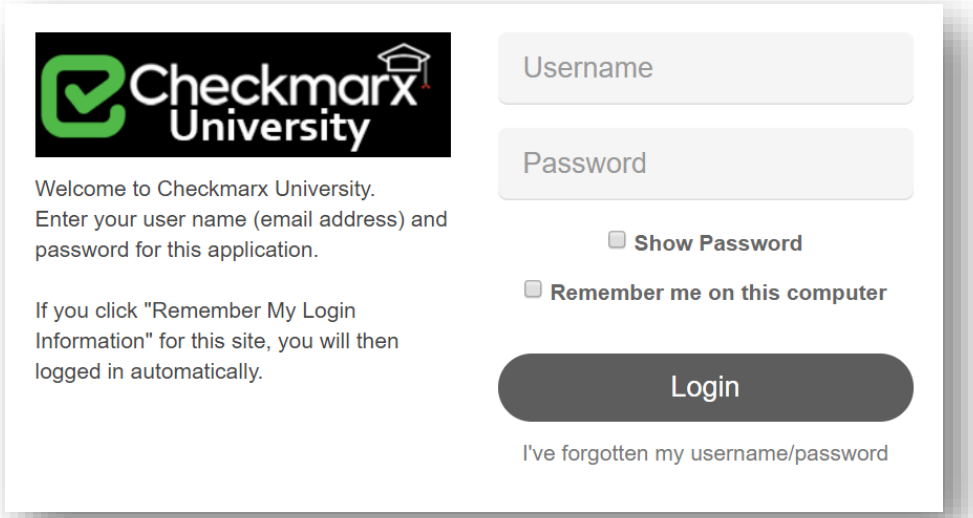
- Add customize sanitization function
- False-negative result

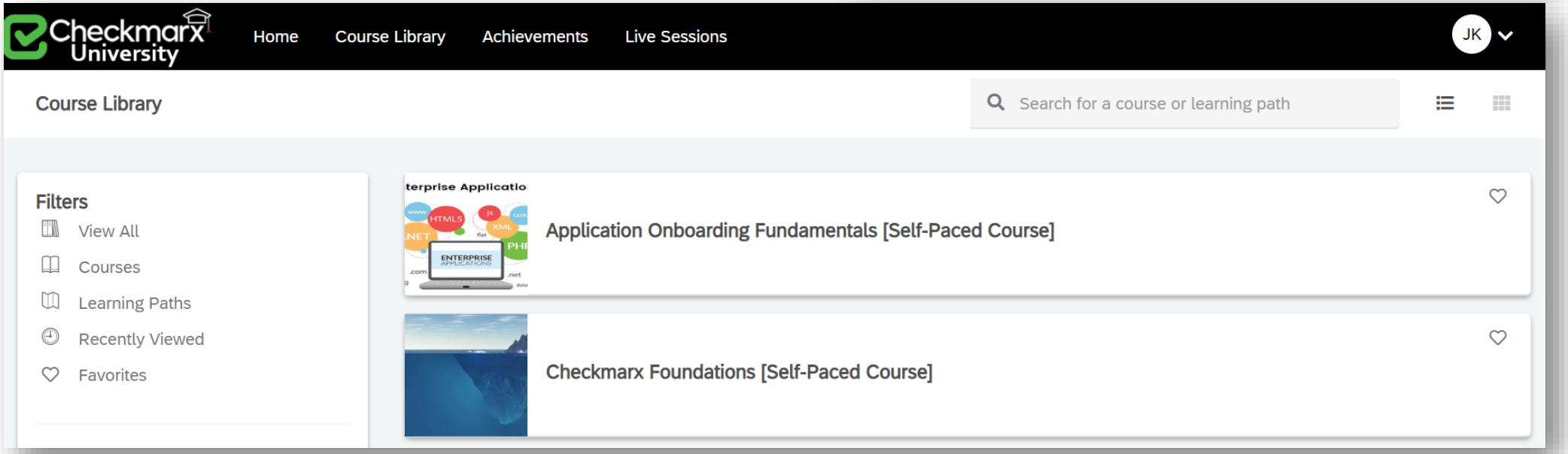
/ CxUniversity

Checkmarx

Exercise 7: CxUniversity

https://checkmarxuniversity.litmos.com

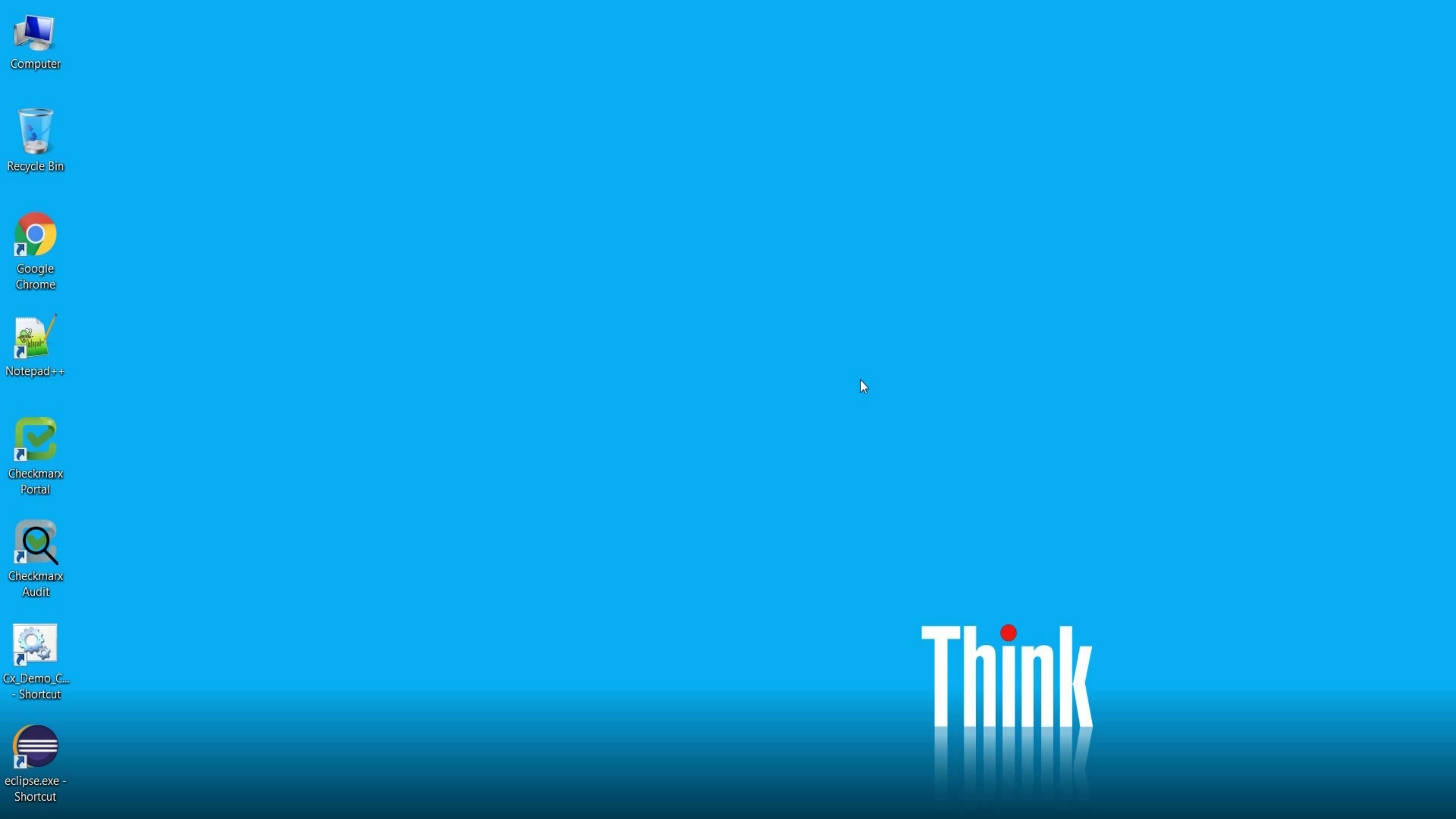




CxSAST / CxOSA Demonstration

Checkmarx

Exercise 8: CxSAST / CxOSA Demonstration


Computer
Recycle Bin
Google Chrome
Notepad++
Checkmarx Portal
Checkmarx Audit
Cx_Demo_C... - Shortcut
eclipse.exe - Shortcut
Think

Question and Discussion

/ Thank you

Email: jason.khoo@checkmarx.com

www.checkmarx.com