CxSAST v9.0.0

User Guide

This document is non-binding and for information purposes only

Contents

CxSAST User Guide

This guide provides information about CxSAST usage, once it has already been set up in your environment.

The CxSAST Web Interface

CxSAST provides an intuitive web interface for managing and analyzing code scan projects and the CxSAST system.

Accessing the CxSAST Web Interface

Upon a successful, first-time installation, first you will be required to create an Administrator user account. The Admin user, who will be a member of the CxServer Team (the top level in the hierarchy) will have complete permissions for managing all applicable users, roles, teams, server settings, and projects.

➢ **To access the administrator user login:**

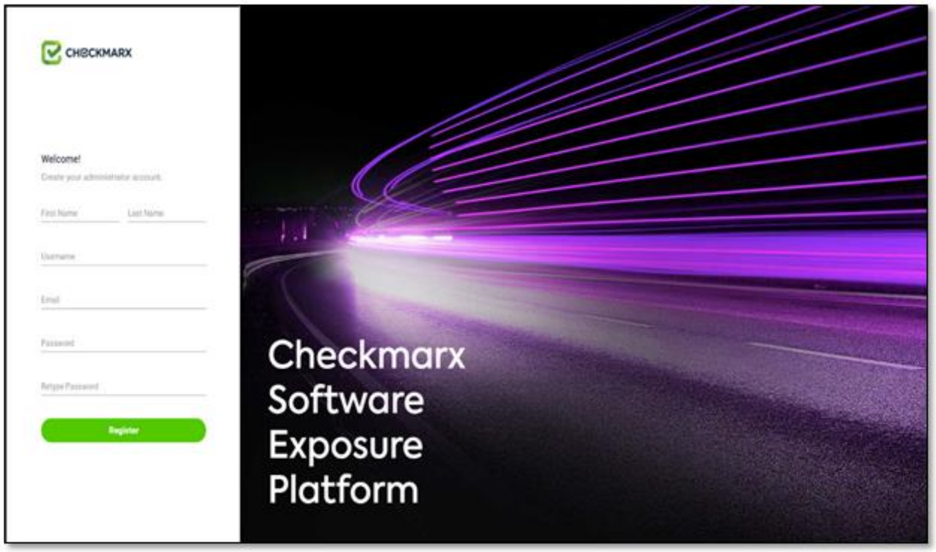
- For local access (server host) - Use the Checkmarx Portal shortcut on the desktop or navigate to the Checkmarx folder (Start > All Programs > Checkmarx > Checkmarx Portal).
- For access from any other computer - Point your browser to: http://<server>/cxwebclient/login.aspx where <server> is the IP address or resolvable hostname of the CxSAST server.

> ⓘ If '3rd party cookies' are disabled in your browser, you will not be able to log into the CxSAST Web Interface via 'http://localhost'. If this is the case you will need to use 'http://<FQDN>', where <FQDN> is the Fully Qualified Domain Name and consists of both the hostname and domain name (e.g. http://mqserver.company.com:5555).

- **To log in:**

1. Enter the required Administrator user account information and then click Register.

   The Checkmarx login prompt appears.

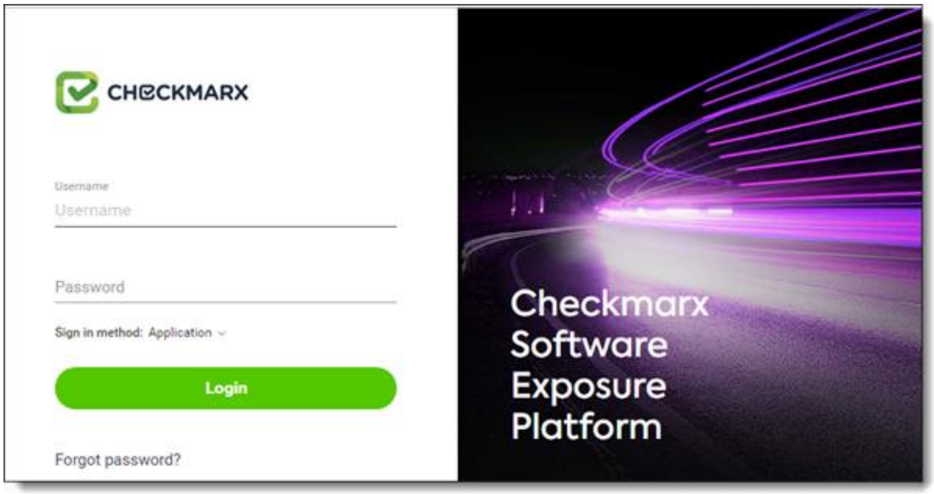


Welcome!

Create your administrator account.

2. The required password complexity is as follows: 9 to 400 characters, at least 1 uppercase letter, at least 1 lower case letter, at least 1 special character, at least 1 digit.
3. Also note the 'Login' and 'Change Password' areas are always displayed in English, regardless of the locale selected.
4. Click **Register.**

   You are redirected to the Checkmarx Login.



Sign in method: Application

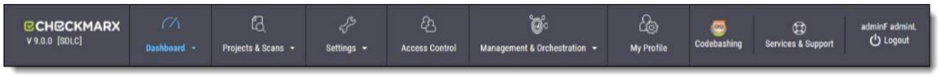
You can subsequently change the Administrator password and add CxSAST users.

A session timeout message is displayed when two thirds of the default idle time (default = 5 mins) has passed. By clicking the OK button, the original session can be continued. If the entire default idle time passes, and once the OK button is clicked, you will be directed back to the login screen. A new login will then be required.

Getting to Know the System Dashboard

The CxSAST web interface includes drop-down navigation menus for each relevant module, as follows:

Dashboard | Projects & Scans | Settings | Access Control | Management & Orchestration | My Profile | Codebashing | Service & Support



ⓘ Visual indicators are displayed just underneath the Checkmarx logo/version and may include:

- Type of product edition currently installed - SDLC or Security Gate
- Expiry date of the current CxSAST license. The indicator appears 90 days (defined in the DB) before the actual license expiry date and, if defined, an email notification is automatically sent to the CxSAST System Administrator.

The Services & Support button allows CxSAST users to navigate to available support resources on our new Checkmarx Customer Center portal. This portal enables the option to open tickets and also provides access to useful Checkmarx links.

CxSAST web interface menu items are described below.

Dashboard Menu

View the state of your engines, scans and queues:

- **Project State:** The current project state, including project information such as Risk level score, High/Medium vulnerabilities, LOC, and Last scan date.
- **Failed Scans:** Log of failed scans, including reason or partial explanation such as "failed to start scanning due to one of the following reasons: source folder is empty, all source files are of an unsupported language or file format".
- **Utilization:** A graphic interface divided into the following four quadrants:
  - **Engine State:** Provides information about the number of scans to engine ratio.
  - **Queue State:** Provides information about the number of scans in the queue and their LOC size/ Average waiting time.

    - **Projects with Longest Scans**: Provides information about the Top 3 scans in the Longest Waiting Time category.
    - **Queue Load**: Provides perspective about the queue load over a 7 day period. The darker the blue the more in the queue; whereas the empty cell with the black outline is the queue running now.

- **Risk:** The Risk graph at the upper half of the window displays the High Risk projects over the last 7 day period, while the lower half displays the Risk Trend of selected projects and Time periods.
- **Data Analysis:** Displays a summary analysis of multiple projects. The data can be presented in several predefined configurations and you can also create your own tables.

Projects and Scans

View projects scans and queues:

- **Create New Project**: Starts the New Project wizard.
- **Queue**: View statuses of currently running scans.
- **Projects**: All projects configured for groups in which the logged-on user is a member.
- **All Scans**: Existing scan results of projects configured for groups in which the logged-on user is a member.

Settings

Manage Scan and Application settings as outlined below.

Scan Settings

- **Query Viewer:** View and manage queries used in the system.
- **Preset Manager:** Create and manage sets of queries according to your needs.
- **Pre & Post Scan Actions:** Allows defining actions, based on preloaded scripts that will run prior or post scan.
- **Source Control Users:** View and modify details of user accounts for accessing source control repositories.

Application Settings

- **General:** Folder locations, SMTP, and other settings.
- **OSA Settings:** Organization token, OSA scan options and test connection settings.
- **License Details:** The installed license details, including supported languages, roles, and number of companies and service providers.
- **Installation Information:** Locations of server components.
- **External Services**: Define settings for external services (e.g. Codebashing enablement).
- **Engine Management**: Manage single/multiple engines.
- **Data Retention**: Set the requested policy for deleting scans from all projects in the system.
- **Issue Tracking Settings**: Configure issue tracking.

Manage Custom Fields

- **Manage Custom Fields**: Define project attributes (metadata) by using custom fields

Access Control

Manage teams, users, roles and access control settings.

Management & Orchestration

- **Policy Manager**: Manage policies
- **Policy Violations**: View policy violations
- **Remediation Intelligence**: Manage remediation intelligence weight and rank settings
- **Analytics**: View analytics results

My Profile

Change personal details (for all user types) and password (only for Application local users, not Windows domain users) of logged-on user.

Codebashing

Codebashing in-context eLearning platform. Codebashing is fully integrated into CxSAST so when developers encounter a security vulnerability, they can activate the appropriate learning module with a single click. Once they have run through the hands-on training, they get straight back to work equipped with the new knowledge to resolve the problem.

Services and Support

Checkmarx customer center with ticketing capabilities, access to the Checkmarx knowledge center and useful links to plugins, utilities and version updates..

Dashboard Menu

As a manager (Server, Company or Service Provider manager), you can view high-level information such as the state of your projects, scan status, utilization and risk and data analysis in the Dashboard menu.

To enter the Dashboard menu, click **Dashboard** and select the relevant sub-menu.

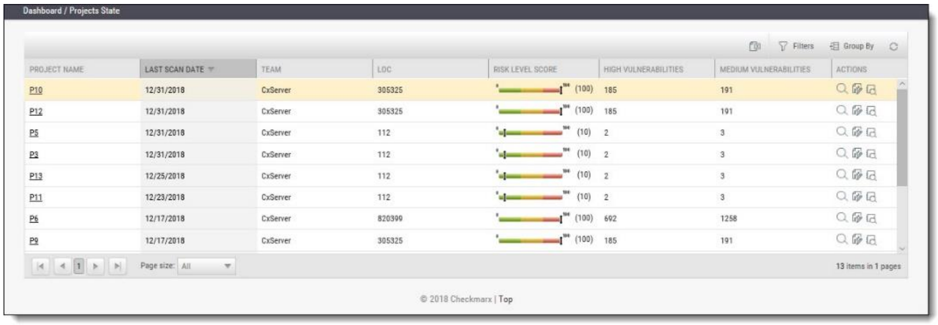
Project State

The Project State window displays the status of all current projects.

➢ **To open the Project State window:**

- Go to **Dashboard > Project State**.

  The Project State window is displayed.



Dashboard / Projects State

PROJECT NAME	LAST SCAN DATE	TEAM	LOC	RISK LEVEL SCORE	HIGH VULNERABILITIES	MEDIUM VULNERABILITIES	ACTIONS
P10	12/31/2018	CxServer	305325	(100)	185	191	
P12	12/31/2018	CxServer	305325	(100)	185	191	
P5	12/31/2018	CxServer	112	(10)	2	3	
P3	12/31/2018	CxServer	112	(10)	2	3	
P13	12/25/2018	CxServer	112	(10)	2	3	
P11	12/23/2018	CxServer	112	(10)	2	3	
P6	12/17/2018	CxServer	820399	(100)	692	1258	
P9	12/17/2018	CxServer	305325	(100)	185	191	

Page size: All

13 items in 1 pages

© 2018 Checkmarx | Top

The Project State window includes the following information:

- Project Name - click on the Project Name link to view the Consolidated Project State
- Last Scan Date
- Team
- LOC
- Risk Level Score
- Vulnerabilities (High, Medium, Low, Info and Total)
- Last Update
- Queue Time
- Scan Time
- Actions (View results, Create report, Download scan logs)

You can Export as CSV File , use the Filter and Group By tools as well as Refresh the current view.

Projects that have not yet had scans performed on them are displayed in the Project State window the the "No SAST Scans performed" message.

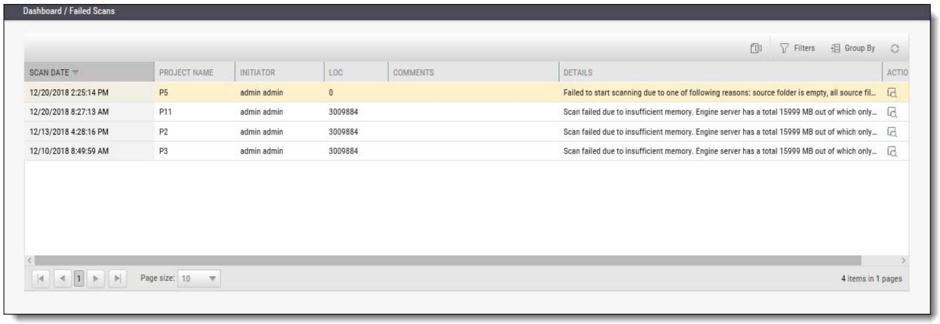
Failed Scans

The failed scans window displays the status of all failed scans.

➢ **To open the Failed Scans window:**

- Go to **Dashboard > Failed Scans**.

  The Failed Scans window is displayed.



Dashboard / Failed Scans

SCAN DATE	PROJECT NAME	INITIATOR	LOC	COMMENTS	DETAILS	ACTIO
12/20/2018 2:25:14 PM	P5	admin admin	0		Failed to start scanning due to one of following reasons: source folder is empty, all source fil...	
12/20/2018 8:27:13 AM	P11	admin admin	3009884		Scan failed due to insufficient memory. Engine server has a total 15999 MB out of which only...	
12/13/2018 4:28:16 PM	P2	admin admin	3009884		Scan failed due to insufficient memory. Engine server has a total 15999 MB out of which only...	
12/10/2018 8:49:59 AM	P3	admin admin	3009884		Scan failed due to insufficient memory. Engine server has a total 15999 MB out of which only...	

Page size: 10

4 items in 1 pages

The Failed Scans window includes the following information:

- Scan Date
- Project Name
- Initiator
- LOC
- Comments (as in The Queue)
- Details
- Actions (Download scan logs)

You can Export as CSV File, use the Filter and Group By tools as well as Refresh the current view.

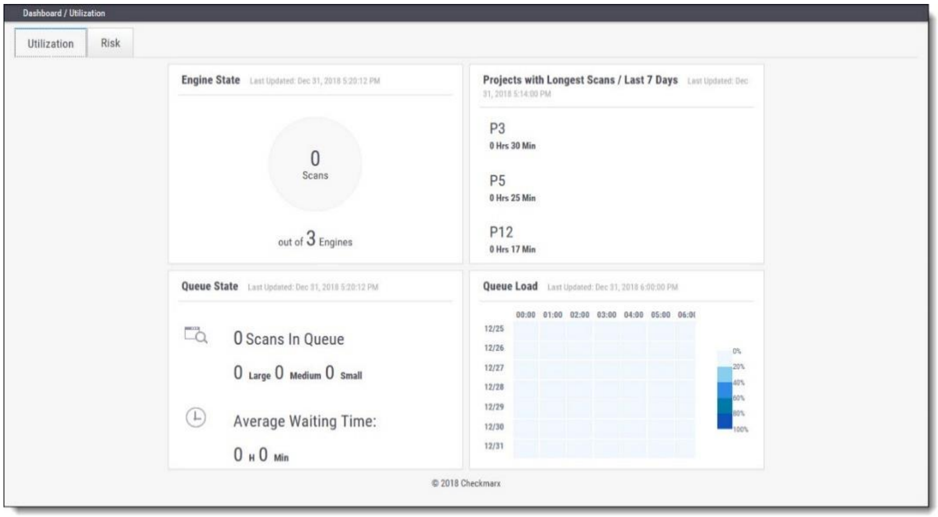
Utilization

The Utilization window displays the status of all completed and running scans.

➢ **To open the Utilization window:**

- Go to **Dashboard > Utilization.**

  The Utilization window is displayed.



Engine State Last Updated: Dec 31, 2018 5:20:12 PM

0 Scans

out of 3 Engines

Projects with Longest Scans / Last 7 Days Last Updated: Dec 31, 2018 5:14:00 PM

P3
0 Hrs 30 Min

P5
0 Hrs 25 Min

P12
0 Hrs 17 Min

Queue State Last Updated: Dec 31, 2018 5:20:12 PM

0 Scans In Queue

0 Large 0 Medium 0 Small

Average Waiting Time:

0 H 0 Min

Queue Load Last Updated: Dec 31, 2018 6:00:00 PM

© 2018 Checkmarx

The Utilization window includes the following information:

- **Engine State** - number of scans to engine ratio
- **Queue State** - number of scans in the queue and their LOC size / average waiting time
- **Projects with Longest Scans** - top 3 scans in the longest waiting time category
- **Queue Load** - queue load over a 7 day period:
  - The darker the blue the more in the queue
  - Empty cell with the black outline indicates currently running queue

Each widget in the Utilization window includes a time stamp indicating the last date and time the data was last updated.

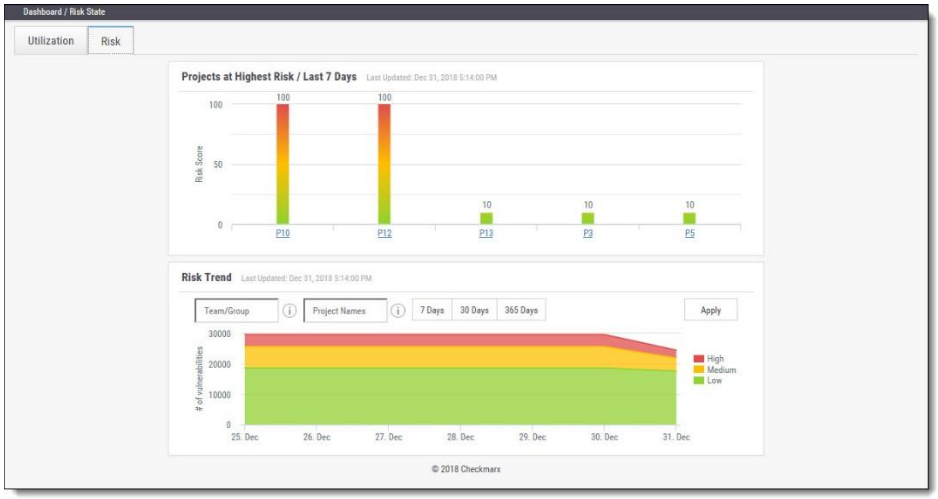
Risk State

The Risk State window displays the number of vulnerabilities and the risk score for each project.

➢ **To open the Risk State window:**

- Go to **Dashboard > Risk State.**

  The Risk State window is displayed.



The Risk State window includes the following information:

- **Projects at Highest Risk / Last 7 Days** - risk score for each project by filtering option
- **Risk Trend** - number of vulnerabilities by filtering option

➢ **To navigate the Risk State window:**

- Filter by **Team/Group**, **Project Name** and **Number of Days**. Click **Apply** to confirm your selection.
- Roll-over the graph to get the project risk and vulnerabilities scores according to the date.
- Click the Project Name link to view the Project State Summary.
- Click the legend to display or hide respective vulnerabilities (High, Medium, Low).

Each widget in the Risk State window includes a time stamp indicating the last date and time the data was last updated.

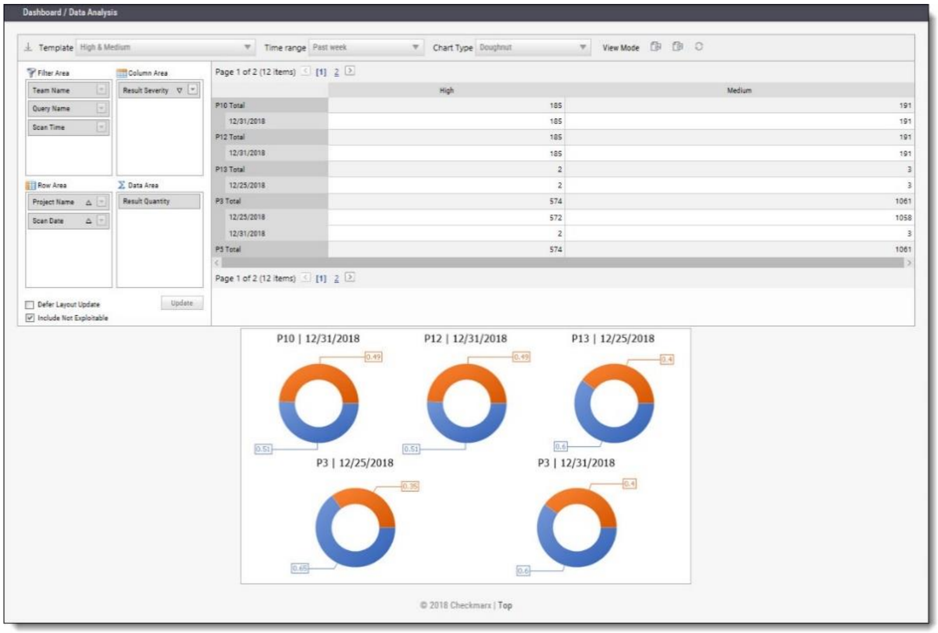
Data Analysis

The Data Analysis window displays a summary analysis of multiple projects. The data can be presented in several predefined configurations and you can also create your own tables.

➢ **To open the Data Analysis window:**

- Go to **Dashboard > Data Analysis**.

The Data Analysis window is displayed.



Dashboard / Data Analysis

Template: High & Medium | Time range: Past week | Chart Type: Doughnut | View Mode

Filter Area: Team Name, Query Name, Scan Time

Column Area: Result Severity

Row Area: Project Name, Scan Date

Data Area: Result Quantity

□ Defer Layout Update

☑ Include Not Exploitable

Update

Page 1 of 2 (12 items) [1] 2

	High	Medium
P10 Total	185	191
12/31/2018	185	191
P12 Total	185	191
12/31/2018	185	191
P13 Total	2	3
12/25/2018	2	3
P3 Total	574	1061
12/25/2018	572	1058
12/31/2018	2	3
P5 Total	574	1061

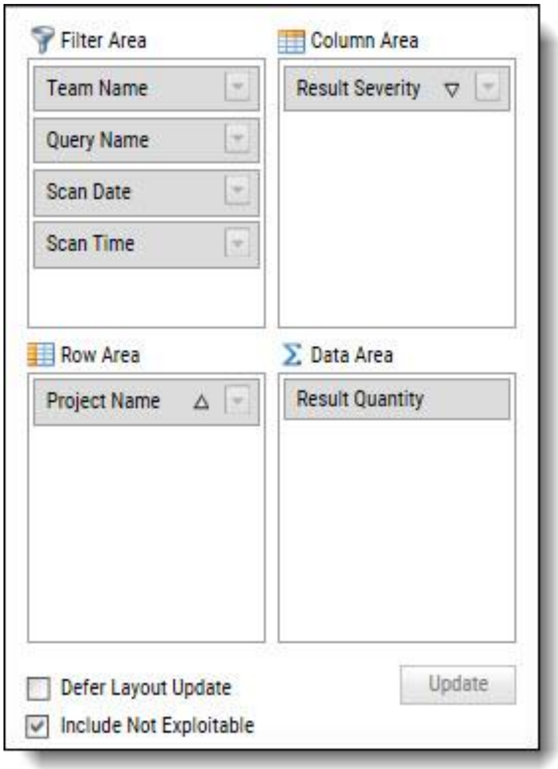
Page 1 of 2 (12 items) [1] 2

© 2018 Checkmarx | Top

The data can be presented in several predefined configurations and you can also create your own tables.

In **Template**, select one of the following table configurations:

- **Project Status:** Displays data for most recent projects
- **High & Medium:** Displays data for projects with High or Medium severity
- **Last week OWASP Top 10:** Displays all projects last week results for OWASP Top 10 queries
- **Basic:** Create a pivot table from scratch. Drag and drop the relevant tab from the Filter area to the Column, Row or Data area.



Filter Area: Team Name, Query Name, Scan Date, Scan Time

Column Area: Result Severity ▽

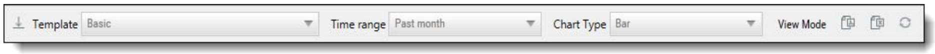
Row Area: Project Name △

Data Area: Result Quantity

□ Defer Layout Update

☑ Include Not Exploitable

- Filter parameters by selecting **Defer Layout Update** to disable filtering.
- Decide whether to **Include** result instances that have been marked as **Not Exploitable**.
- Use the top bar to alter the **Chart Type**, **View Mode** or to **Export** the chart and the table to PDF or Excel file.



Template: Basic | Time range: Past month | Chart Type: Bar | View Mode

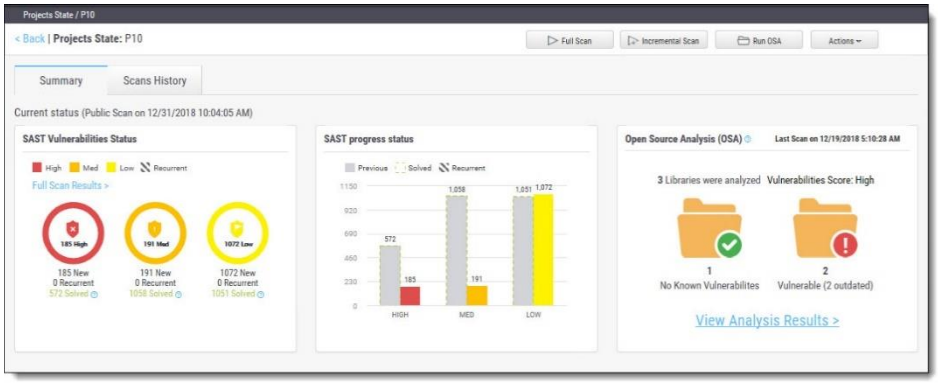
To save a custom table as a template, click **Save**.

Consolidated Project State

The Consolidated Project State window provides a high level summary of the status of each project.

➢ **To display the Consolidated Project State window:**

- Go to **Dashboard > Project State** and click the link on the **Project Name**. The Consolidated Project State window is displayed.



Current status (Public Scan on 12/31/2018 10:04:05 AM)

3 Libraries were analyzed Vulnerabilities Score: High

Summary

You can perform the following actions from the Consolidated Project State window:

- **Full Scan -** perform a SAST scan for the whole project
- **Incremental Scan** - perform a SAST scan for only new and modified files since the last scan
- **Run OSA** - perform Open Source Analysis on predefined open source libraries associated with this project.

> ⓘ A purchased or a trial CxOSA license is required in order to run CxOSA projects. Please contact your Checkmarx Administrator.
>
> ⓘ CI/Build plugins now use new core library with better compatibility and increased result accuracy. The new capability extracts dependencies resolving manifest files on the customer side.

➢ **Additional Actions:**

- **Edit Project** - displays the projects details
- **Open Scan Summary** - displays the scan summary
- **Open Viewer** - displays the scan results viewer
- **CxOSA Viewer** - displays the CxOSA scan results viewer (see Getting to Know the CxOSA Viewer in the Checkmarx OSA Documentation).

> ⓘ Action options on the Consolidated Project State window are available according to the user's permissions

- **Current Status -** Includes the time/date stamp indicating the date and time of the last SAST scan

SAST Vulnerability Status

This status provides a graph with the status of each vulnerability severity.

🟥, 🟧, 🟨 - All new vulnerability instances discovered according to severity (high, medium and low)

▨ - Recurring vulnerability instances from previous scan

Solved - Vulnerabilities fixed/solved since last scan

> ⓘ If no scans have yet been performed a "No Scans Performed" message is displayed. For more details about projects and scans, refer to Creating and Configuring Projects.
>
> ⓘ If a new scan is currently in progress a "New Scan in Progress "message is displayed. For more details about the status of the scan, refer to the Queue.

➢ **To display the scan list for this project:**

- Click the **Full Scan Results** link.

SAST Progress Status

This status provides a graph with the progress status of each vulnerability severity.

🟥, 🟧, 🟨 - All new vulnerability instances discovered according to severity (high, medium and low)

⬜ - Vulnerability instances from previous scan

⬚ - Fixed/solved vulnerability instances from previous scan

▨ - Recurring vulnerability instances from previous scan

Open Source Analysis (CxOSA)

Open Source Analysis (OSA) helps you manage the security risk involved in using open source libraries in your applications. This provides open source analysis results for predefined open source libraries associated with this project. Includes a stamp indicating the date and time of the last analysis.

> ⓘ In order to start working with CxOSA, you need to accept the End User License Agreement (EULA). Click the View EULA button, read and accept the agreement

The following summary results are displayed:

- **No Known Vulnerable Libraries** - Number of libraries without any known security vulnerabilities.
- **Vulnerable Libraries -** Distribution of the vulnerable libraries:
- **Vulnerable** - number of libraries that have at least one security vulnerability
- **Outdated** - number of vulnerable libraries for which a newer version is available (major vs minor release).

If the Open Source Analysis license has not yet been enabled for this project, a warning message is displayed. Please contact your Checkmarx Administrator.

Click the **Run Analysis Now** link to perform an Open Source Analysis. A "New Open Source Analysis is in progress" indicator is displayed.

> ⓘ If the Open Source Library directory location has not yet been configured and you try to run CxOSA, a warning message is displayed. Follow the link and define the Open Source Libraries location before continuing with the analysis.

For more information about Running Open Source Analysis and Open Source Analysis (CxOSA) in general, see Initiating a CxOSA Scan in the Checkmarx CxOSA Documentation.

Scan History

Click the Scans History tab to display the scan results for the project.

CxOSA Viewer

Getting to Know the CxOSA Viewer

For more information about Getting to Know the CxOSA Viewer and Open Source Analysis (CxOSA) in general, see Getting to Know the CxOSA Viewer in the Checkmarx CxOSA Documentation.

Open Source Analysis Report

For more information about Open Source Analysis Report and Open Source Analysis (CxOSA) in general, refer to **Generating a CxOSA Scan Results Report** in the **Checkmarx CxOSA** Documentation.

Creating and Managing Projects

A CxSAST project defines the source to be scanned, scan scheduling, and notification settings. Normally, a CxSAST project should correspond to a software development project, or to part of one. Any time a scan is run (manually or scheduled), the scan results remain associated with the CxSAST project.

For Continuous Integration development methodology, if a new branch is created for each iteration, update the code location within the existing project (rather than creating a new project) so that all the results will reside within a single project. Scanning of projects that include multiple code languages is supported. To enable this feature, please contact Checkmarx professional services.

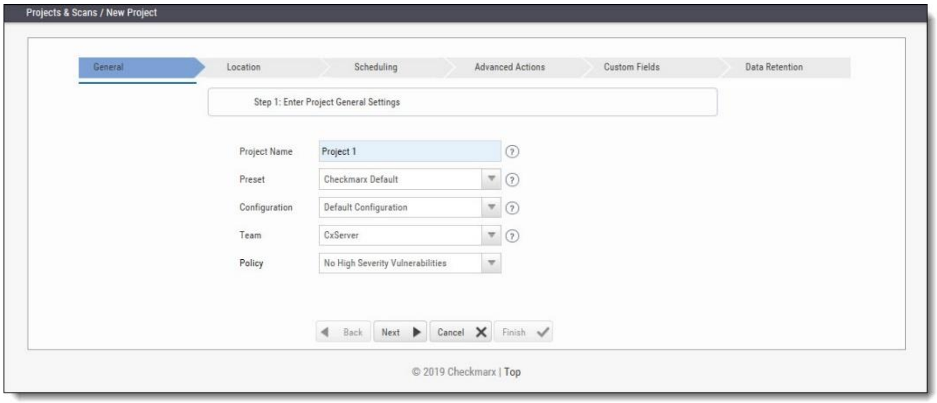
Open Source Analysis (CxOSA) can be added to an existing CxSAST project in cases where open source components are used as part of the development effort. When CxOSA is activated, CxSAST sends the open source fingerprint (SHA-1 hash plus file extension) to the CxOSA service. Using this fingerprint, the CxOSA service maps the open source libraries, identifies any vulnerabilities, analyses license risk and compliance, builds inventory and detects outdated libraries. A comprehensive report can be generated from the Consolidated Project State.

Creating and Configuring Projects

This section explains how to create, configure and manage CxSAST projects.

➢ **To create a CxSAST project:**

1. Select **Project & Scans > Create New Project**.



Step 1: Enter Project General Settings

Project Name: Project 1

Preset: Checkmarx Default

Configuration: Default Configuration

Team: CxServer

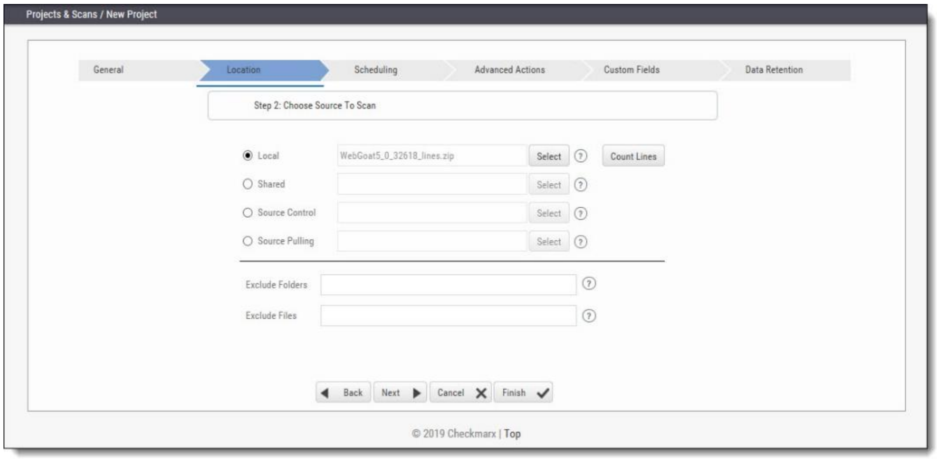
Policy: No High Severity Vulnerabilities

2. Configure the following **General** project properties:
   - **Project Name -** should indicate the source code to be scanned and tracked.
   - **Preset -** set of queries to be run on the code scan. **Default** includes a set of queries recommended by Checkmarx for most projects. Select the preset that best matches your application, for example, for an Android project select **Android**. For a full list of executed queries, see the Vulnerability Queries section in the release notes.
   - **Configuration -** Apart from the default configuration setting, additional configuration selection traditionally for advanced users, can be used for scanning double-byte encoded source code. There is also the possibility to select a multi-language configuration. This means that all files will be scanned, regardless of language type. If there is a need, a threshold parameter can be adjusted in the database.
     - **Default configuration** will scan the primary language (e.g., java, C#, python, etc.) with the most files and all secondary languages (e.g., JavaScript, PL-SQL, vb-script, etc.). For example, a project with 100 java files, 50 python files, and 60 JavaScript files, will have only the java and JavaScript scanned with the Default configuration.
     - The **Multi-language configuration** will scan all languages including multiple primary languages. If the same project with 100 java files, 50 python files, and 60 JavaScript files is scanned, all languages – java, python, and JavaScript will be scanned.
   - **Team** - determines who will be able to view your project and its scan results. Available options depend on the permissions of the logged-on user.

Selecting CxServer allows access only to the server Administrator. If you're working as a single user, leave the default option.

- **Policy** - select a predefined violation policy from the Policy drop-down (e.g. No High Severity Vulnerabilities). Refer to Policy Management for more information about defining violation policies and rules.

3. Click **Next**.



Projects & Scans / New Project

Step 2: Choose Source To Scan

● Local: WebGoat5_0_32618_lines.zip

○ Shared

○ Source Control

○ Source Pulling

Exclude Folders:

Exclude Files:

4. Configure the following source code **Location** properties:

- **Local -** Click **Select** to browse to a local zip file containing the code. Future scans to the project are also via local upload (see Managing Projects and Running Scans).

> ⓘ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.
>
> ⓘ If the zip file is larger than 200 MB, you will not be able to upload it. To create a smaller zip file of only files with specified extensions, use the CxZip utility.
>
> ⓘ Zip files generated in a Linux environment may not function properly.
>
> ⓘ If a zip file is uploaded that contains file path greater than 255 characters, the file will not be sent for scanning. Shorten the file path and try again.
>
> ⓘ If the zip file contains another zip file inside, the internal zip file will not be sent for scanning. Unzip the contents to the main zip file before scanning.

- **Shared -** project code that is maintained on a network server accessible from the CxSAST Server. Click **Select,** provide your Windows domain credentials in order for CxSAST to access the network (username format: domain_name\user name), and select one or more network folders containing the project code.

> ⓘ Zipped source code is not supported for shared location scans. Unzip the contents of the zip file before scanning.

> ⓘ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

- ○ **Source Control -** project code that is maintained in either TFS , SVN , GIT or PerForce source control systems. Click **Select** (see [Configuring the Connection to a Source Control System](#)).

> ⓘ In cases where the project's source control location is defined as Git, the Git branch name will be included under the Source Control field.
>
> ⓘ Files inside a zip file that are located inside a repository will not be sent for scanning. Unzip the contents of the zip file to the repository before scanning.
>
> ⓘ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

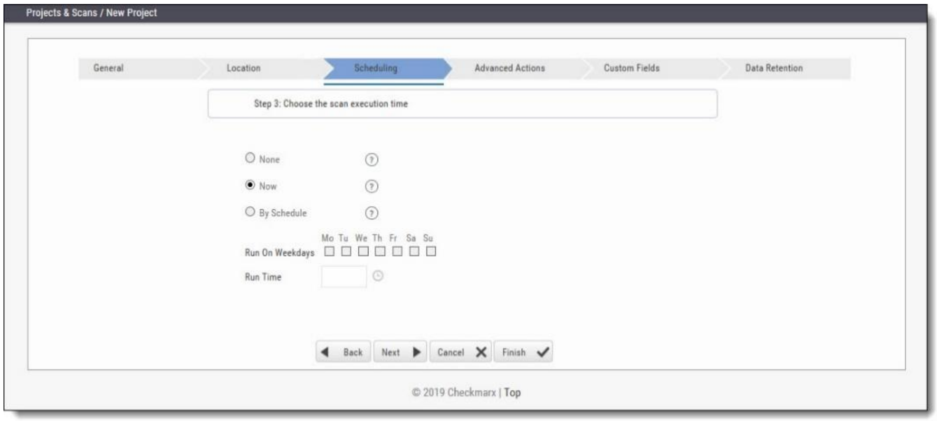
- ○ **Source Pulling -** an extension to "Shared" option above, "Source Pulling" activates a configurable script to pull source code from a source control system into the Shared location specified. Note: this script must be set previously configured in the CxSAST Windows client application.
  - ▪ For any issues, please review: Network and Shared dialogs may not work on "Localhost"
- ○ Optionally, you can exclude certain folders or files from the scan process.

> ⓘ Type a comma-separated list of the folders or files that you would like excluded from the scan; wildcards can also be used. In the below archive, the folder name ‘lib’ and the file name ‘readme.txt’ have been added to the Exclude fields and will not be included for the upcoming project scan
>
> ```
> |+ add-ons
> | |+ connectors
> | | |+ cvc3.js
> | | |+ spass.js
> | | + z3.js
> | | - lib
> | | | - readme.txt
> | | | - smt_solver.js
> | + src
> | +doc
> | - readme.txt
> + src
> - lib
> |- find_sql_injections.js
> |- jquery.js
> + logic.js
> ```
>
> ⓘ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

- Click **Count Lines** to display the number of lines in the current project.

> ⓘ The Java Script is being enhanced in the scan process, the real count of lines might be larger than the result displayed in the Count Lines option or the Cx CMD Line Counter.

- Click **Next**. The following steps of the wizard are optional. You can click **Finish** to skip them.



Step 3: Choose the scan execution time

○ None

● Now

○ By Schedule

Run On Weekdays Mo □ Tu □ We □ Th □ Fr □ Sa □ Su □

Run Time

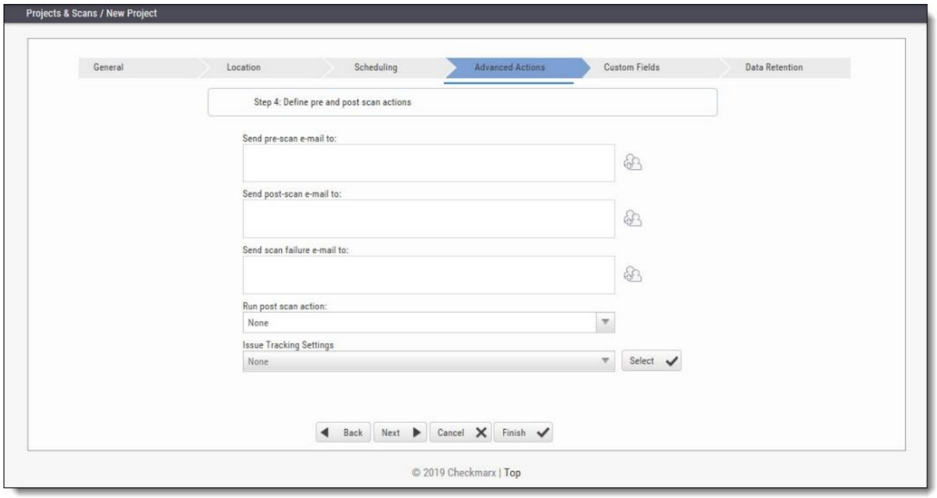
> ⓘ Scheduling is not applicable to a Local source code location, since the CxSAST Server cannot automatically access the local source. You will need to periodically manually upload a new zip file

5. Configure the following scan execution **Scheduling** properties:
   - **None** - defines no scheduling
   - **Now** - defines an immediate scan
   - **By Schedule** - define an automatic weekly scan according to the specified time
     - **Run on Weekdays** - define which day to run the periodic scan
     - **Run Time** - define what time to run the periodic scan.

> ⓘ To support continuous integration development methodology, it is recommended to schedule periodic scanning of source files, so they can be checked after modifications. This can be automated via the CLI in the Build file, but it does not have to be done this way because CxSAST scans source code and does not require building or compiling the source code.

6. Click **Next**.

   The next steps of the wizard are optional. You can click **Finish** to skip them.



Step 4: Define pre and post scan actions

Send pre-scan e-mail to:

Send post-scan e-mail to:

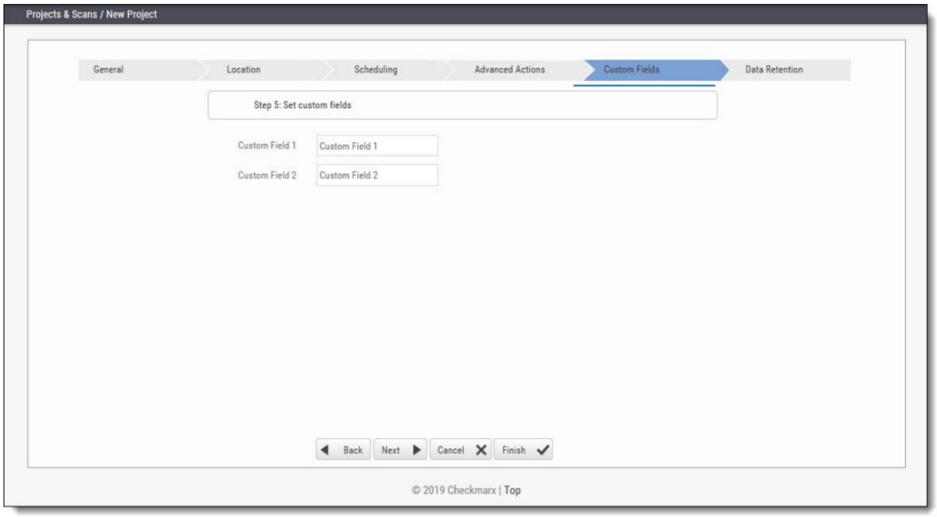
Send scan failure e-mail to:

Run post scan action: None

Issue Tracking Settings: None

7. Configure the following **Advanced Action** properties:
   - **Send pre-scan email to** - define to which e-mail to send a pre-scan notification
   - **Send post-scan e-mail to** - define to which e-mail to send a post-scan notification
   - **Send scan failure e-mail to** - define to which e-mail to send a scan failure notification
   - **Run post scan action** - define which post scan action to run (see Configuring an Executable Action)
   - **Issue Tracking Settings** - define to which issue tracking system to integrate (see Configuring JIRA Integration Settings).
8. Click **Next**.

   The following steps of the wizard are optional. You can click **Finish** to skip them.



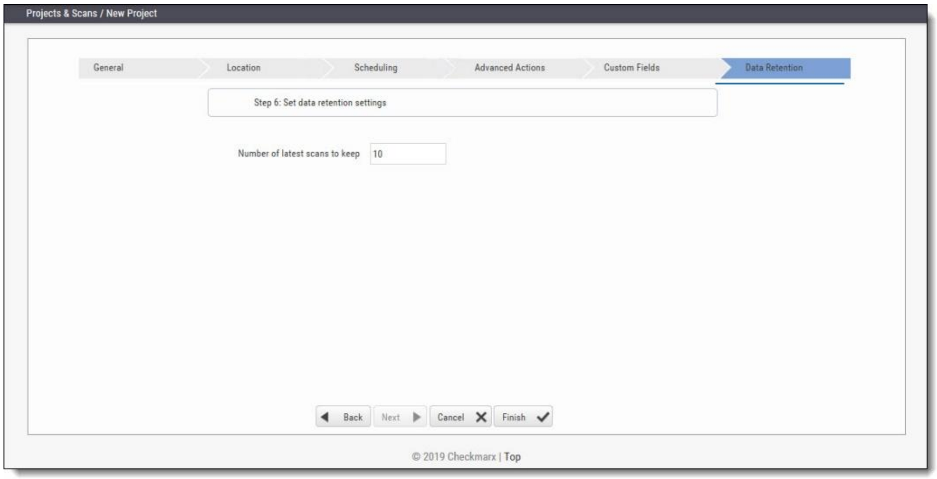
Step 5: Set custom fields

Custom Field 1: Custom Field 1

Custom Field 2: Custom Field 2

9. Configure the **Custom Field** properties according to the available custom fields (see Custom Field Management).
10. Click **Next**.

    The following steps of the wizard are optional. You can click **Finish** to skip them.



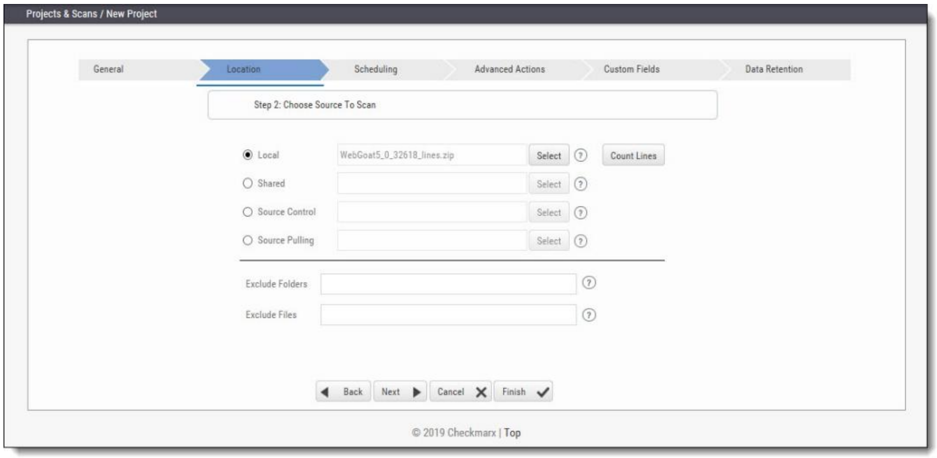
Step 6: Set data retention settings

Number of latest scans to keep: 10

11. Configure the **Data Retention** properties:
    - Number of latest scans to keep - Define the number of latest scans to be kept (see Data Retention Management).
12. Click **Finish** and check the scan status (see The Queue).

Configuring the Connection to a Source Control System

When creating a project and the source code **Location** is set to **Source Control**, you can define to which source control system to connect by selecting a source control type (TFS, SVN, GIT or Perforce).



Step 2: Choose Source To Scan

● Local: WebGoat5_0_32618_lines.zip
○ Shared
○ Source Control
○ Source Pulling

Exclude Folders

Exclude Files

➢ **To configure the connection:**

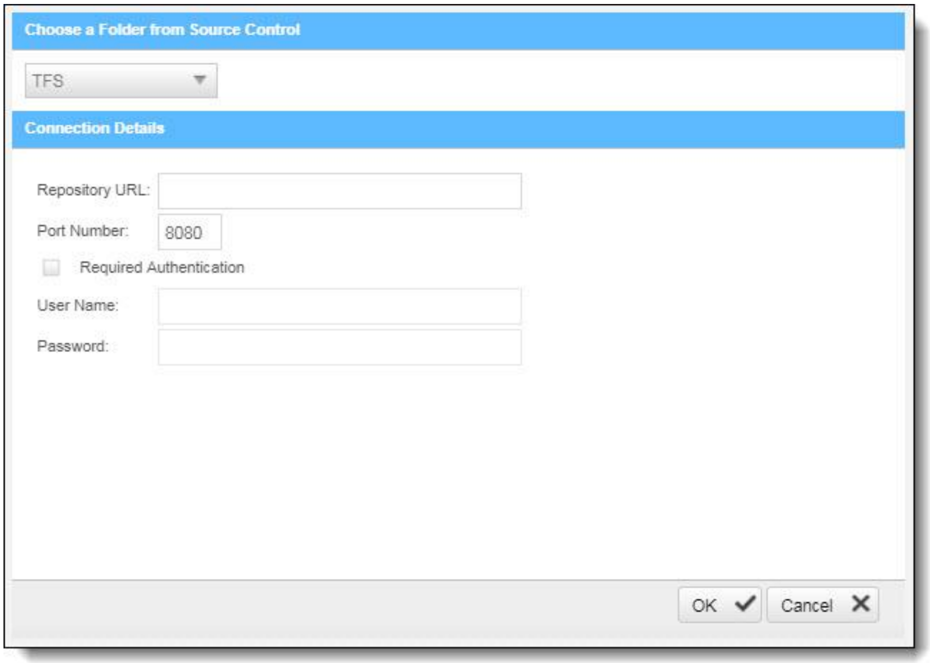
- With Source Control option checked, click **Select**. The Source Control window is displayed (see below for connection options).

> ⓘ Files inside a zip file that are located inside a repository will not be sent for scanning. Unzip the contents of the zip file to the repository before scanning.

Defining Source Control for TFS

1. Select **TFS** from the drop-down.

   The TFS Connection Details panel is displayed.



Choose a Folder from Source Control

TFS

Connection Details

Repository URL:

Port Number: 8080

□ Required Authentication

User Name:

Password:

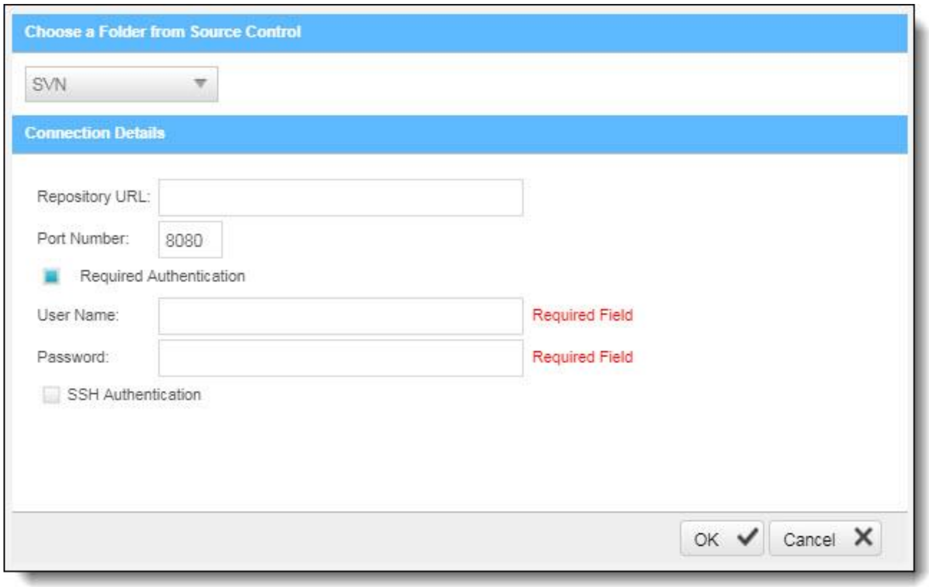
The TFS Connection Details panel includes the following parameters:

- **Repository URL** - the repository URL address (Supports HTTP and HTTPS, i.e. <protocol>://<site name>:<port>/tfs/<Collection> (must point to the repository named <Collection>)).
- **Port Number** - the port number
- **Required Authentication** - select to enforce authentication
- **User Name** - the user name (required with enforced authentication)
- **Password** - the password (required with enforced authentication)

2. Click **OK**.

Defining Source Control for SVN

1. Select **SVN** from the drop-down. The SVN Connection Details panel is displayed.



SVN

Repository URL:

Port Number: 8080

☑ Required Authentication

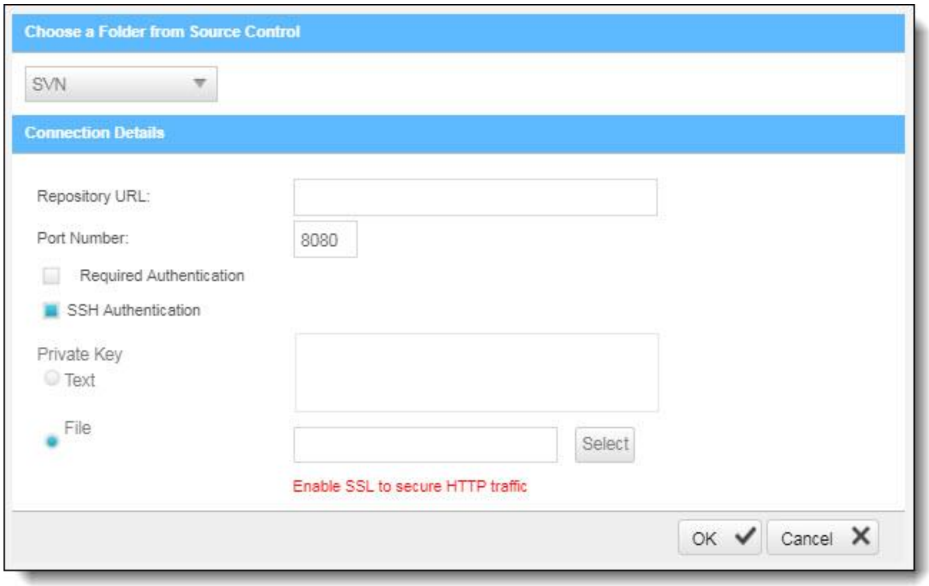
User Name:

Password:

☐ SSH Authentication

The SVN Connection Details panel includes the following parameters:

- **Repository URL** - the repository URL address (Supports HTTP, HTTPS and SSH private/public key infrastructure,
  i.e. <protocol>://<server_ip>/<repository_name>)
- **Port Number** - the port number
- **Required Authentication** - select to enforce authentication
- **User Name** - the user name (required with enforced authentication)
- **Password** - the password (required with enforced authentication)
- **SHH Authentication** - select to use secure authentication with SSH



Choose a Folder from Source Control

SVN

Connection Details

Repository URL:

Port Number: 8080

□ Required Authentication

☑ SSH Authentication

Private Key

○ Text

● File

Enable SSL to secure HTTP traffic

Selecting SHH Authentication displays the following additional parameters:

- **Private Key Text** - add private key text
- **Private Key File** - select and upload a private key file

> ⓘ Checkmarx does not support SSH keys with a passphrase
>
> ⓘ For best results, use ssh-keygen, per these instructions, and not PuTTYgen

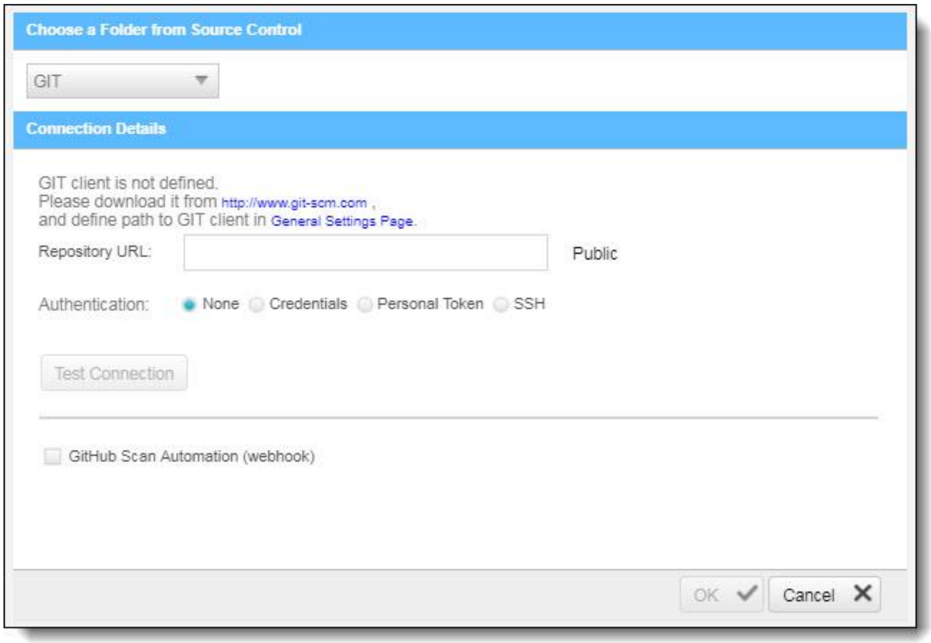
2. Click **OK**.

Defining Source Control for GIT

To meet the requirements for using GIT repository, do the following:

1. Download GIT Installation Package and perform the installation on CxSAST Manager Server (use installation defaults)
2. Define Path+ exe file in CxSAST **Management** > **Application Settings** > **General** > **Path to GIT Client Executable** (i.e. C:\Program Files\Git\bin\git.exe).
3. Select **GIT** from the drop-down.

   The GIT Connection Details panel is displayed.



Choose a Folder from Source Control

GIT

Connection Details

GIT client is not defined.
Please download it from http://www.git-scm.com ,
and define path to GIT client in General Settings Page.

Repository URL: Public

Authentication: ● None ○ Credentials ○ Personal Token ○ SSH

□ GitHub Scan Automation (webhook)

The GIT Connection Details panel includes the following parameters:

- **Repository URL** - The repository URL address (Supports HTTP, HTTPS, i.e. <protocol>://<user>:<password>@<server_ip>/<repository_name>.git or SSH private/public key infrastructure, i.e. git@<git_site>:<user_name>/<repository_name>.git).
- **Authentication** - Select an authentication method.
- **GitHub Scan Automation** - Select to include GitHub Integration.

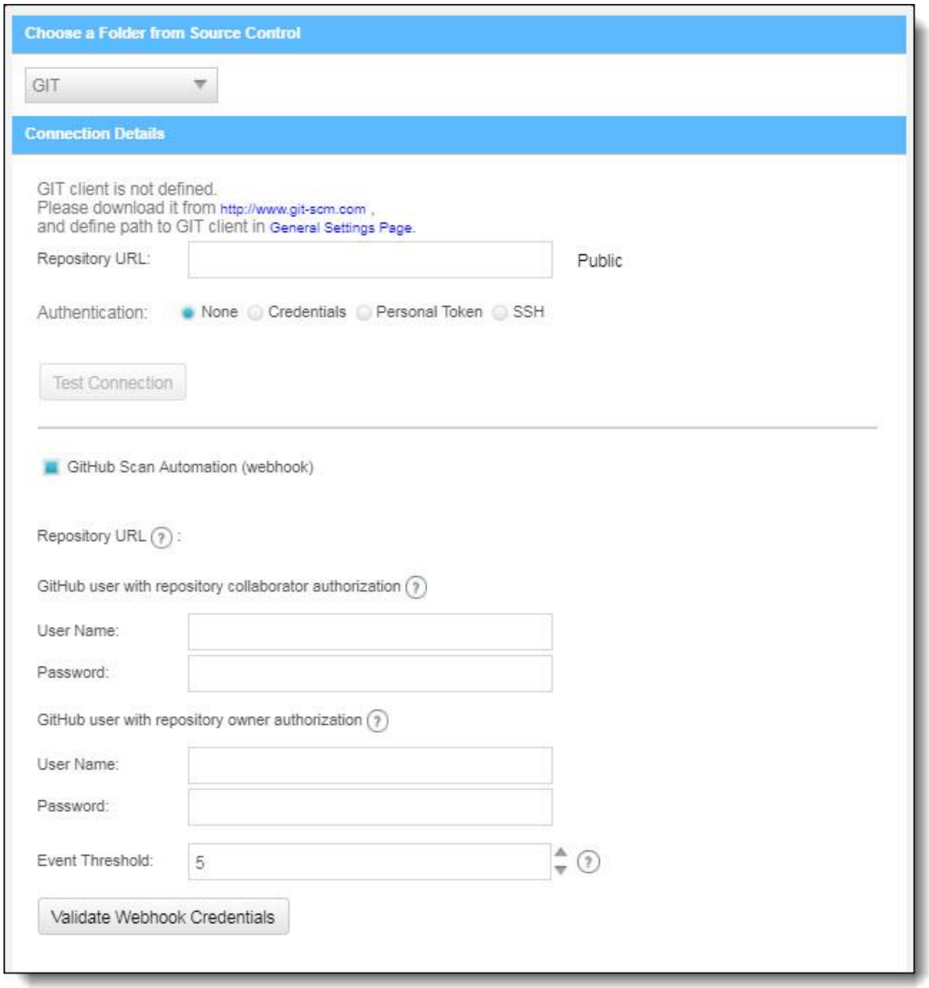
ⓘ If your repository URL contains the character "@", replace it with "%40" (html encoding) before inserting the URL.

ⓘ For tip to find your GIT Repository URL refer to GitHub - Tips on Finding Git / GitHub Repository URLs.

ⓘ For more information about the various athentication methods, please refer to Configuring a Project with Git Integration.

4. Click **Test Connection**.

   Once the 'Connection Successful' message is displayed you can continue.



Choose a Folder from Source Control

GIT ▾

Connection Details

GIT client is not defined.
Please download it from http://www.git-scm.com ,
and define path to GIT client in General Settings Page.

Repository URL: Public

Authentication: ● None ○ Credentials ○ Personal Token ○ SSH

☑ GitHub Scan Automation (webhook)

Repository URL ? :

GitHub user with repository collaborator authorization ?

User Name:

Password:

GitHub user with repository owner authorization ?

User Name:

Password:

Event Threshold: 5 ?

5. Enter the GitHub repository owner and collaborator credentials into the relevant User Name and Password fields.

> ⓘ The GitHub user with repository owner authorization is used for creating and using a GitHub WebHook (see GitHub Webhooks).
>
> ⓘ The GitHub user with repository collaborator authorization is used to create commit comments.

6. Configure the Event threshold. A scan in Checkmarx CxSAST will be initiated only after this number of events has occurred, since the last triggered scan.

> ⓘ By default, the event threshold value is set to 5, because triggering a scan after fewer events may overload the system. If the user specifies a lower number, a warning message is displayed.

7. Click **Validate Webhook Credentials** to confirm authentication to the GitHub webhooks works correctly.

   A 'Server Connection Verified Successfully' message is displayed.

8. Click **OK** to complete the procedure.

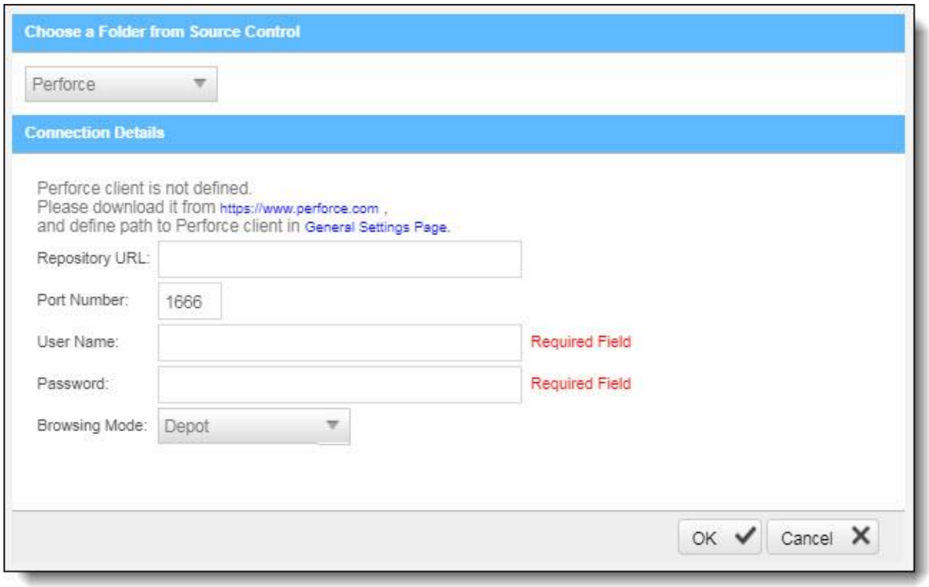
> ⓘ For more information about the various options for GitHub integration, please refer to Github Integration

Defining Source Control for Perforce

> ⓘ Currently CxSAST is unable to scan code from any system that contains symbolic links.

1. Select **Perforce** from the drop-down.

   The Perforce Connection Details panel is displayed.



Choose a Folder from Source Control

Perforce

Connection Details

Perforce client is not defined.
Please download it from https://www.perforce.com ,
and define path to Perforce client in General Settings Page.

Repository URL:

Port Number: 1666

User Name: Required Field

Password: Required Field

Browsing Mode: Depot

The Perforce Connection Details panel includes the following parameters:

- **Repository URL** - the repository URL address (i.e. SSL:<server_ip> or <server_ip>)
- **Port Number** - the port number
- **User Name** - the user name
- **Password** - the unique password
- **Browsing Mode** - select **Depot** (for shared file repositories) or **Workspace** (for grouped file repositories).

2. Click **OK**.

   You can now continue to configure the project.

- ⓘ To set the Perforce client executable path, refer to the Path to P4 command line client executable parameter in the Server Settings.
- ⓘ For All connections - Connection between CxManager Server and 3rd party repo server is done with the credentials that are configured to the CxPool IIS Application Pool.

Configuring Open Source Analysis

For more information about Configuring Open Source Analysis and Open Source Analysis (CxOSA) in general, see **Creating and Configuring CxOSA Projects** in the Checkmarx CxOSA Documentation.

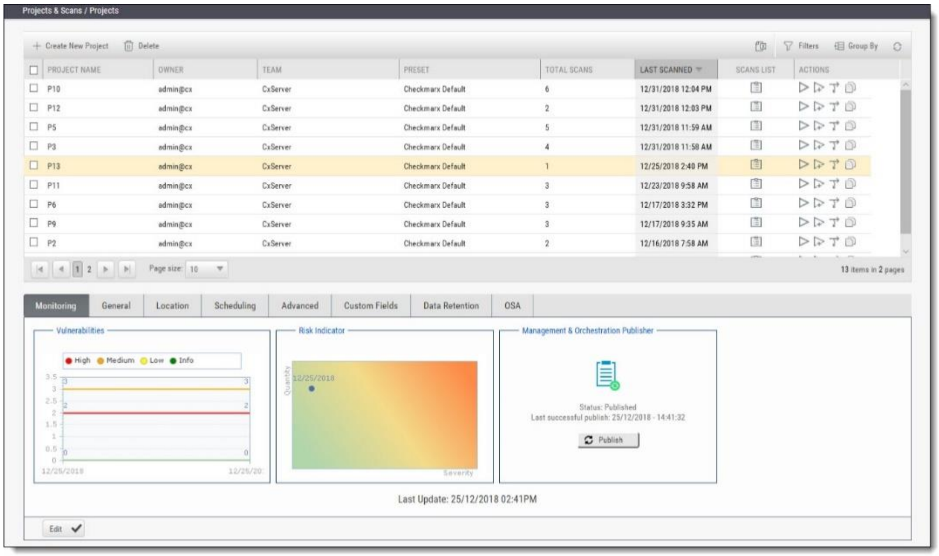
Branching / Duplicating Existing Projects

CxSAST gives you the capability to branch / duplicate an existing project and have the new project inherit all of the issues, comments and dispositions from the source project. Once the project has been branched / duplicated you can treat it as a separate project with separate issues to manage.

- ⓘ **Branch Project** - similar to copy project, except it copies the following set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
- ⓘ When branching a project, the branch should be started from the last successful scan. Successful scan meaning the ‘last real scan’ that was performed, instead of the attempted scan which changed the date of scan start date, but was actually never performed due to there being no change in the code.
- ⓘ **Duplicate Project** - creates a new project based on the settings of the existing one and also copies the following set of properties: Preset, Team, Exclusions, Scheduling, Pre-scan, Post-scan and Scan failure emails.

➢ **To branch or duplicate an existing project:**

1. Go to **Projects & Scans and** select **Projects**.



Projects & Scans / Projects

□	PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS
□	P10	admin@cx	CxServer	Checkmarx Default	6	12/31/2018 12:04 PM		
□	P12	admin@cx	CxServer	Checkmarx Default	2	12/31/2018 12:03 PM		
□	P5	admin@cx	CxServer	Checkmarx Default	5	12/31/2018 11:59 AM		
□	P3	admin@cx	CxServer	Checkmarx Default	4	12/31/2018 11:58 AM		
□	P13	admin@cx	CxServer	Checkmarx Default	1	12/25/2018 2:40 PM		
□	P11	admin@cx	CxServer	Checkmarx Default	3	12/23/2018 9:58 AM		
□	P6	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 3:32 PM		
□	P9	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 9:35 AM		
□	P2	admin@cx	CxServer	Checkmarx Default	2	12/16/2018 7:58 AM		

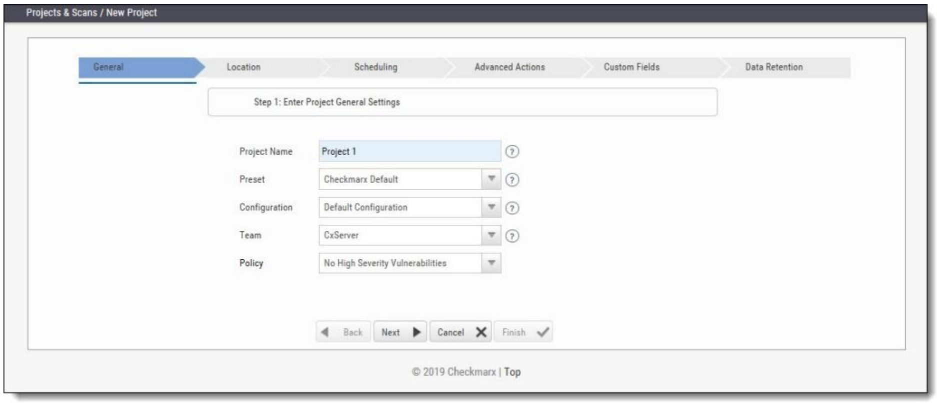
Page size: 10

13 items in 2 pages

Status: Published
Last successful publish: 25/12/2018 - 14:41:32

Last Update: 25/12/2018 02:41PM

2. Click **Branch Project** or **Duplicate Project** .



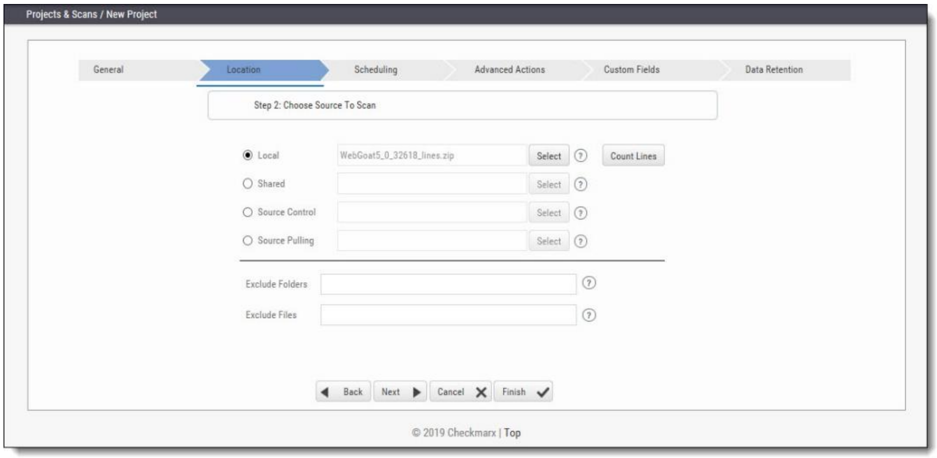
Projects & Scans / New Project

Step 1: Enter Project General Settings

Project Name	Project 1
Preset	Checkmarx Default
Configuration	Default Configuration
Team	CxServer
Policy	No High Severity Vulnerabilities

© 2019 Checkmarx | Top

3. Define **General** settings and click **Next**.



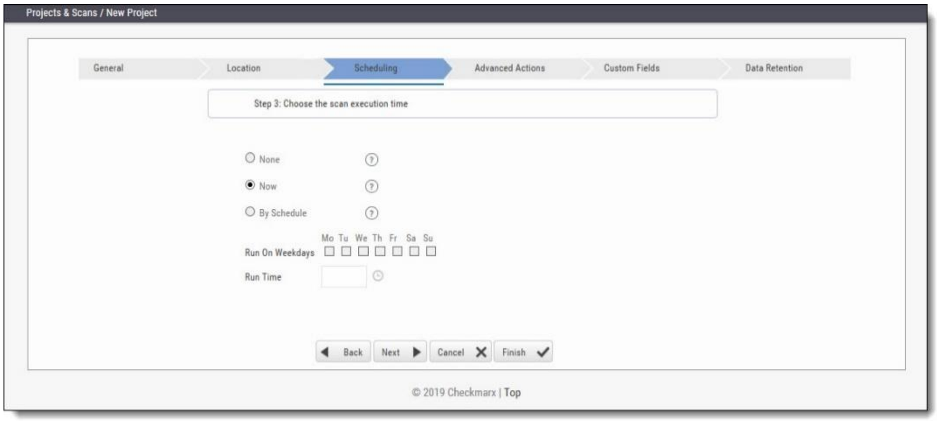
Step 2: Choose Source To Scan

● Local WebGoat5_0_32618_lines.zip Select Count Lines
○ Shared Select
○ Source Control Select
○ Source Pulling Select

Exclude Folders

Exclude Files

4. Define the **Location** of the source code and click **Next**.



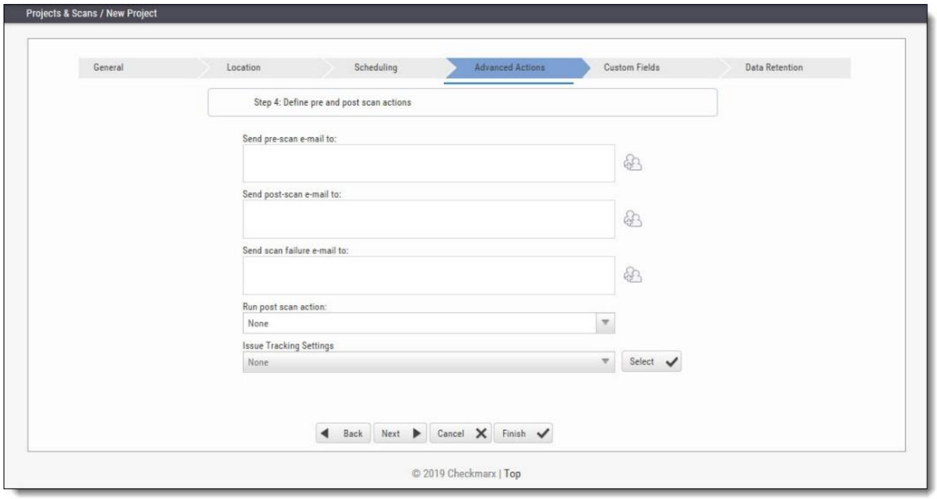
Step 3: Choose the scan execution time

○ None
● Now
○ By Schedule

Run On Weekdays Mo □ Tu □ We □ Th □ Fr □ Sa □ Su □

Run Time

5. Define scan **Scheduling** options and click **Next**.



Step 4: Define pre and post scan actions

Send pre-scan e-mail to:

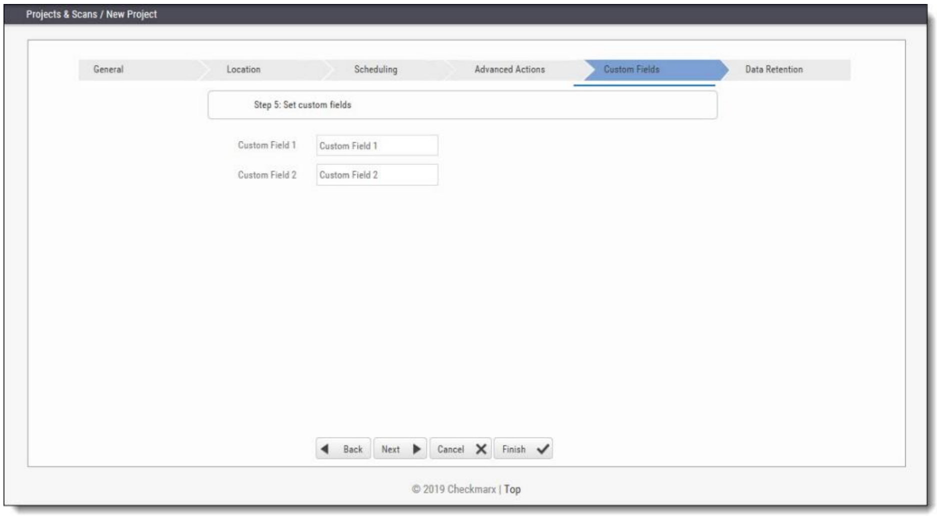
Send post-scan e-mail to:

Send scan failure e-mail to:

Run post scan action: None

Issue Tracking Settings: None

6. Define **Advanced Action** settings and click **Next**.

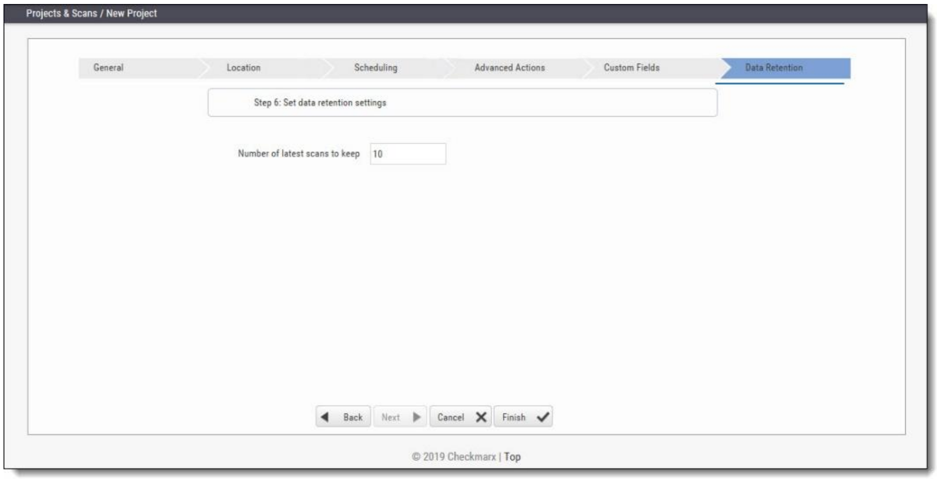


Step 5: Set custom fields

Custom Field 1: Custom Field 1

Custom Field 2: Custom Field 2

7. Define **Custom Field** settings and click **Next**.



Step 6: Set data retention settings

Number of latest scans to keep: 10

8. Define Data Retention settings and click **Next**.
9. Once complete, click **Save**.

   The following message is displayed: "Branching may take a few minutes, would you like to proceed?"

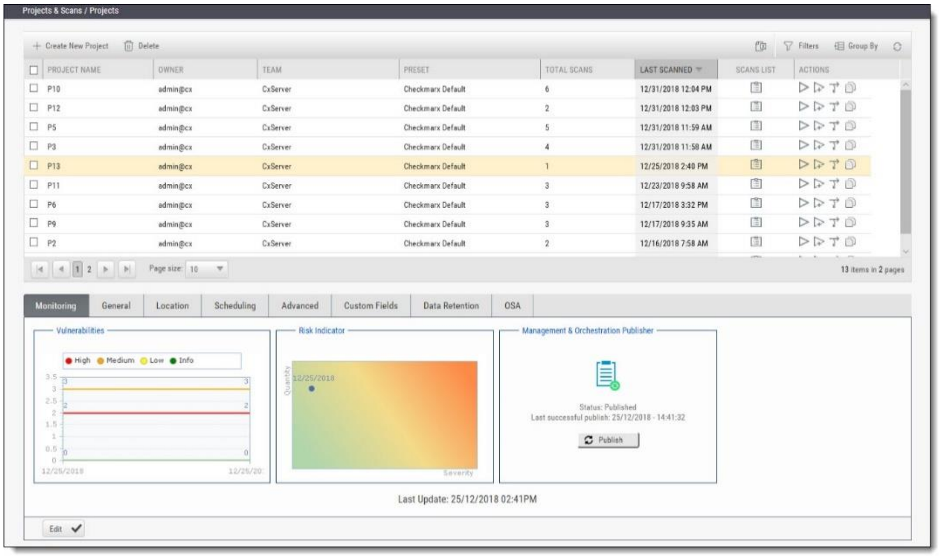
10. Click **OK**.

    The "Branching successfully ended" message is displayed. The branched/duplicated project is displayed in the Projects window.

> ⓘ Branched projects are not counted as additional projects according to the Checkmarx licensing structure. This means that you are not allowed to create new projects once you have reached the maximum project threshold, however, you will be able to open branches of existing projects without forfeiting additional licenses.

Managing Projects and Running Scans

In **Projects & Scans > Projects**, various scans and action lists are available (see also **Creating and Configuring Projects**).



Projects & Scans / Projects

☐	PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS
☐	P10	admin@cx	CxServer	Checkmarx Default	6	12/31/2018 12:04 PM	▤	▷ ▷
☐	P12	admin@cx	CxServer	Checkmarx Default	2	12/31/2018 12:03 PM	▤	▷ ▷
☐	P5	admin@cx	CxServer	Checkmarx Default	5	12/31/2018 11:59 AM	▤	▷ ▷
☐	P3	admin@cx	CxServer	Checkmarx Default	4	12/31/2018 11:58 AM	▤	▷ ▷
☐	P13	admin@cx	CxServer	Checkmarx Default	1	12/25/2018 2:40 PM	▤	▷ ▷
☐	P11	admin@cx	CxServer	Checkmarx Default	3	12/23/2018 9:58 AM	▤	▷ ▷
☐	P6	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 3:32 PM	▤	▷ ▷
☐	P9	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 9:35 AM	▤	▷ ▷
☐	P2	admin@cx	CxServer	Checkmarx Default	2	12/16/2018 7:58 AM	▤	▷ ▷

Page size: 10

13 items in 2 pages

Status: Published
Last successful publish: 25/12/2018 - 14:41:32

Last Update: 25/12/2018 02:41PM

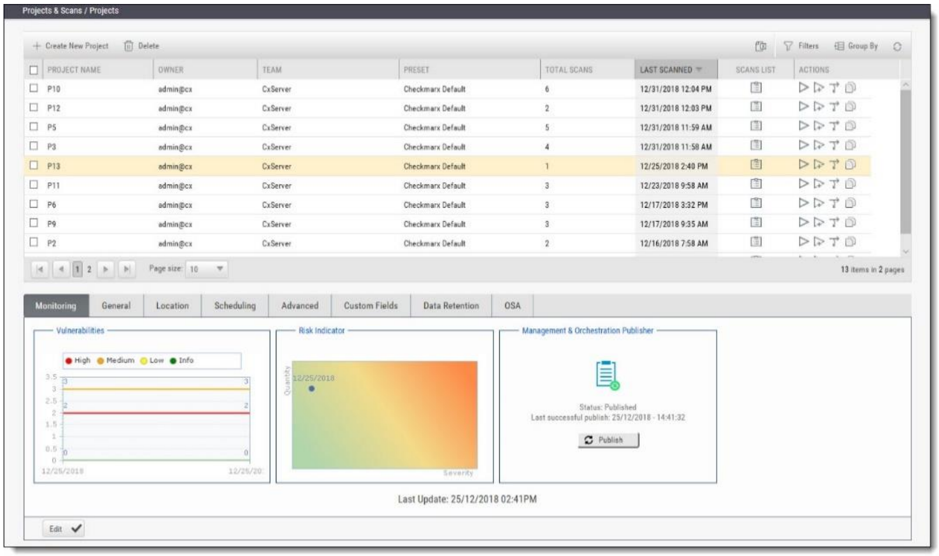
Scan List/Actions

	Action	Description
▤	Scan List	Displays the project in the individual project path, e.g. Projects & Scans/View Project Scans/My Java Projects.
▷	Full Scan	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.
▷	Incremental Scan	Incremental scan is used to increase the scanning speed of the project. It works by scanning only the code that has changed since the last full scan was performed. During the incremental scan, the system takes each file that was sent to be incrementally scanned and creates a hash of it's code. It then compares the value of the hash with the value of the hash of the files with the same name that was scanned on the last full scan. Incremental scan needs to be performed on all of the code, not only on the changed code. Incremental scan is recommended only if the regular scan takes more than 45 minutes. When using incremental scan as part of CI/CD (for example as part of a build process) you need to make sure that a full scan is performed every X amount of incremental scans. Otherwise the changes will aggregate and when more than 7% of the code has changed CxSAST will either run a full scan or fail the scan, depending on the configuration. The following configuration keys are available: INCREMENTAL_SCAN_THRESHOLD Defines the maximum percentage of files changed to allow the incremental scan. Valid values: 1-19, Default value: 7 INCREMENTAL_SCAN_THRESHOLD_ACTION Defines the action to be taken when the threshold exceed in incremental scan. FAIL – fail the scan, FULL – switch to full scan. Valid values: FAIL or FULL. Default value: FAIL

	Action	Description
If a zip file is uploaded that contains file path greater than 255 characters, the file will not be sent for scanning. Shorten the file path and try again.		
	Branch Project	The Branch Project operation is similar to copy project, but it copies a different set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
	Duplicate Project	Duplicate Project creates a new project based on the setting of an existing one. From the existing project it will copy the following: Preset, Team, Exclusions, Scheduling, Pre-scan emails, Post-scan emails and Scan failure emails.

Managing Tables

The various tables in the web interface provide navigation and pagination controls:



PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS
P10	admin@cx	CxServer	Checkmarx Default	6	12/31/2018 12:04 PM		
P12	admin@cx	CxServer	Checkmarx Default	2	12/31/2018 12:03 PM		
P5	admin@cx	CxServer	Checkmarx Default	5	12/31/2018 11:59 AM		
P3	admin@cx	CxServer	Checkmarx Default	4	12/31/2018 11:58 AM		
P13	admin@cx	CxServer	Checkmarx Default	1	12/25/2018 2:40 PM		
P11	admin@cx	CxServer	Checkmarx Default	3	12/23/2018 9:58 AM		
P6	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 3:32 PM		
P9	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 9:35 AM		
P2	admin@cx	CxServer	Checkmarx Default	2	12/16/2018 7:58 AM		

13 items in 2 pages

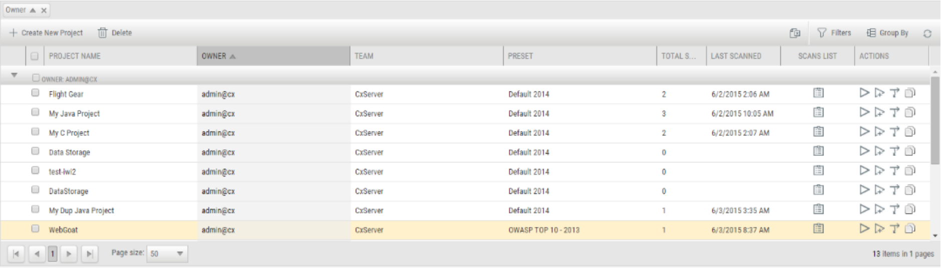
Status: Published
Last successful publish: 25/12/2018 - 14:41:32

Last Update: 25/12/2018 02:41PM

The following actions are available from the table's header bar:

- **Delete** - Delete Delete rows
- A project can contain one or more scans that are locked, or whose deletion requires authorization that the current user does not have. In such cases, all objects that can be deleted are removed, and a message is displayed to notify the user about the objects that could not be deleted.
- When the user deletes a project, the project is not deleted from the database. Instead, the project is marked as "deprecated". All scans under the deleted project are also marked as "deprecated". This deprecated data can be ultimately be removed as part of the Data Retention Management process.

- **Export** - Export to CSV
- **Filters -** Display a filtering field for each column heading. After typing a filter text (not case-sensitive), press **Enter** to filter.
- **Group By** - Group values by dragging the column header to the top bar. For example, a manager could group projects by user.



	PROJECT NAME	OWNER ▲	TEAM	PRESET	TOTAL S...	LAST SCANNED	SCANS LIST	ACTIONS
□	OWNER: ADMIN@CX							
□	Flight Gear	admin@cx	CxServer	Default 2014	2	6/2/2015 2:06 AM		
□	My Java Project	admin@cx	CxServer	Default 2014	3	6/2/2015 10:05 AM		
□	My C Project	admin@cx	CxServer	Default 2014	2	6/2/2015 2:07 AM		
□	Data Storage	admin@cx	CxServer	Default 2014	0			
□	test-iwi2	admin@cx	CxServer	Default 2014	0			
□	DataStorage	admin@cx	CxServer	Default 2014	0			
□	My Dup Java Project	admin@cx	CxServer	Default 2014	1	6/3/2015 3:35 AM		
□	WebGoat	admin@cx	CxServer	OWASP TOP 10 - 2013	1	6/3/2015 8:37 AM		

- To re-order the rows by the values of a column, without grouping, just click the column heading (toggle between ascending and descending order).
- **Refresh** - Refresh the table.

Advanced Actions

CxSAST can automatically perform configurable actions with each scan. The available types of **Advanced Actions** are:

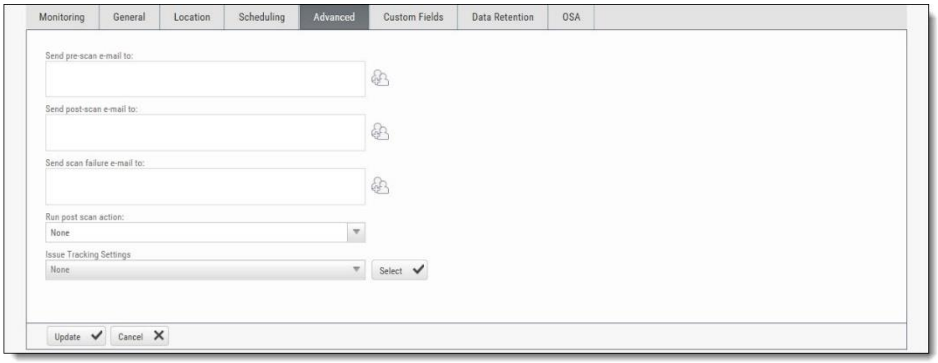
- Send an email message
- Run an executable

Configuring an Email Action

You can configure CxSAST to automatically send an email before or after a scan.

➢ **To configure an automatic email:**

1. In a project's Advanced Actions tab, enter the requested email address under the relevant event:



Send pre-scan e-mail to:

Send post-scan e-mail to:

Send scan failure e-mail to:

Run post scan action: None

Issue Tracking Settings: None

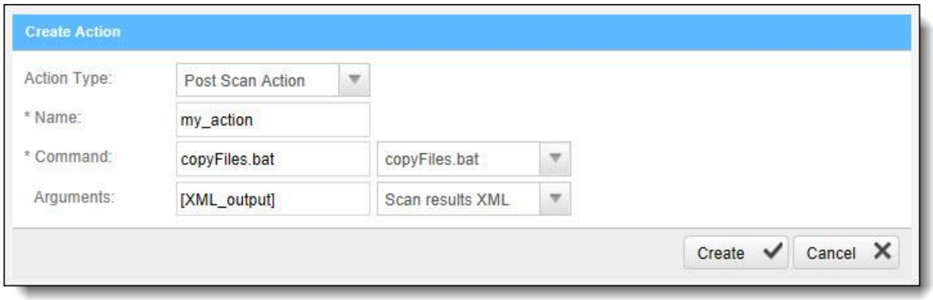
2. Click 👥 and add recipients. Separate email addresses with semicolons (;).
3. Click **Finish**.

ⓘ Email actions require SMTP settings.

Configuring an Executable Action

➢ **To configure CxSAST to run an executable before or after a scan:**

1. Upload an executable: To ensure the integrity of the system and to restrict access, executable files must be uploaded manually by approved personnel.
2. The location used by CxSAST for executable files appears in **Settings > Application Settings > General > Executables Folder**.
3. Define an Action for the executable: Go to **Settings > Scan Settings > Pre & Post Scan Actions > Create New Action**, and configure the following:
   - **Action Type**: Pre-scan or Post-scan.
   - **Name**: This appears in a drop-down list when assigning the actions to a project.
   - **Command**: Use the syntax as required by the executable or select from the list.
   - **Arguments**: Enter arguments required by the command.



Action Type: Post Scan Action

* Name: my_action

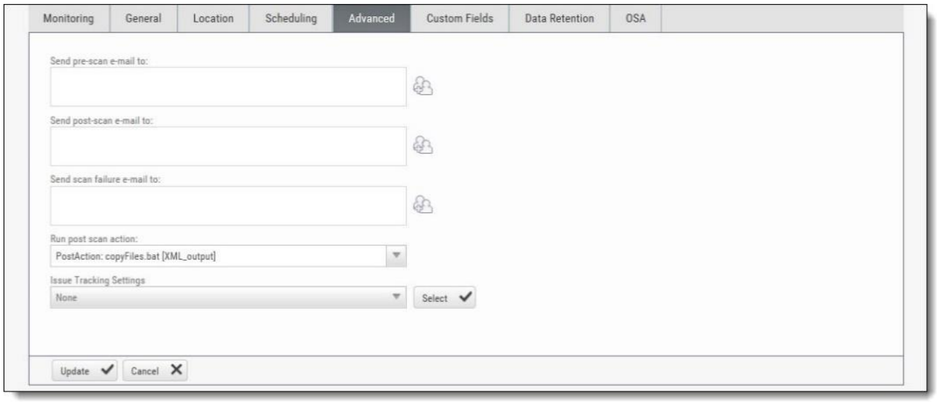
* Command: copyFiles.bat | copyFiles.bat

Arguments: [XML_output] | Scan results XML

ⓘ The command should use the same name that is used for the file located in the ‘Executables’ folder (files present in that folder will show up in the drop-down list), as defined in Settings > Application Settings > General > Executables Folder.

ⓘ For post-scan actions, you can also select whether the scan results is XML or CSV.

4. Assign the action to a project: In a project's Advanced Actions tab, select an action from the list:



Send pre-scan e-mail to:

Send post-scan e-mail to:

Send scan failure e-mail to:

Run post scan action: PostAction: copyFiles.bat [XML_output]

Issue Tracking Settings: None

5. Click **Finish**.

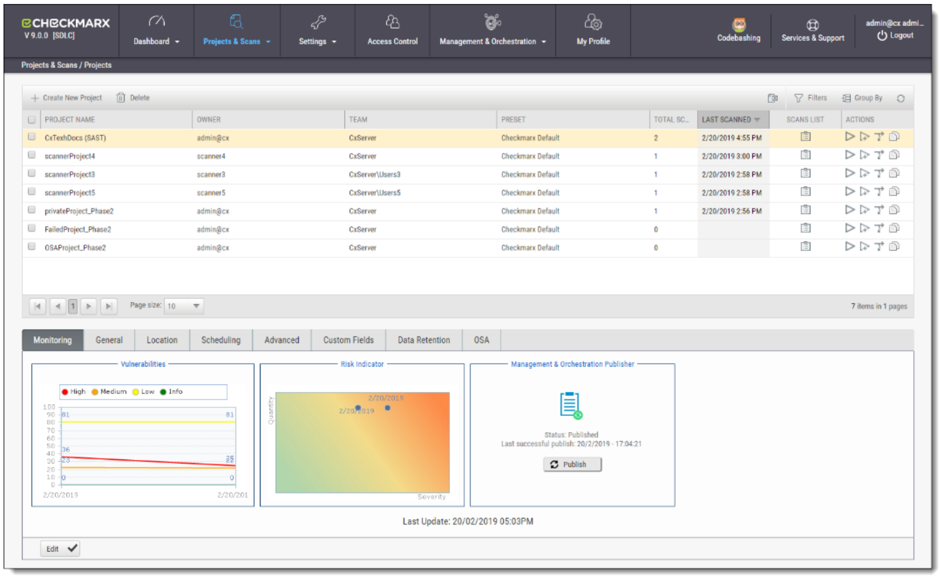
Viewing Project Details

You can view detailed information about a particular project from the Projects window.

➢ **To open the Projects window:**

- Go to **Projects & Scans > Projects.**

  The Projects window is displayed.



PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SC...	LAST SCANNED	SCANS LIST	ACTIONS
CxTexhDocs (SAST)	admin@cx	CxServer	Checkmarx Default	2	2/20/2019 4:55 PM		
scannerProject4	scanner4	CxServer	Checkmarx Default	1	2/20/2019 3:00 PM		
scannerProject3	scanner3	CxServer\Users3	Checkmarx Default	1	2/20/2019 2:58 PM		
scannerProject5	scanner5	CxServer\Users5	Checkmarx Default	1	2/20/2019 2:58 PM		
privateProject_Phase2	admin@cx	CxServer	Checkmarx Default	1	2/20/2019 2:56 PM		
FailedProject_Phase2	admin@cx	CxServer	Checkmarx Default	0			
OSAProject_Phase2	admin@cx	CxServer	Checkmarx Default	0			

Status: Published
Last successful publish: 20/2/2019 - 17:04:21

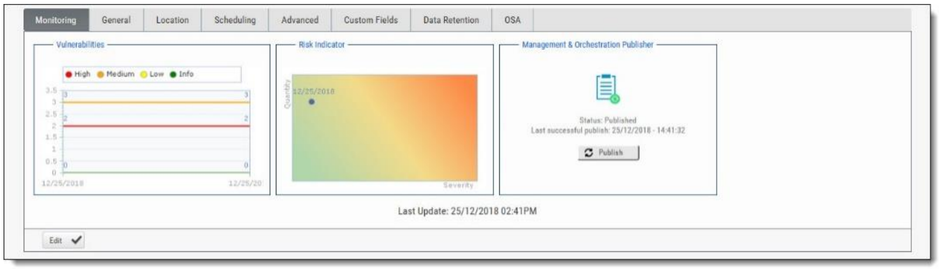
Last Update: 20/02/2019 05:03PM

The Projects window lists all the projects that are configured for groups where the logged-on user is a member. You can also manage the table.

For a non-local project, or for an Incremental scan of a local project, Total Scans counts only scans when the code had changes relative to the previous scan.

For each project, you can view its scans or perform other actions.

Selecting a project displays its details in the tabbed panel below.



Status: Published
Last successful publish: 25/12/2018 - 14:41:32

Last Update: 25/12/2018 02:41PM

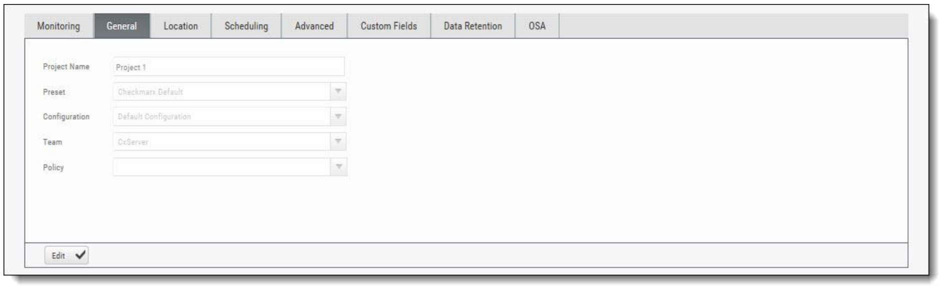
The Monitoring tab represents the evolution of the project last 10 scans focusing on the numbers of found vulnerabilities and overall risk.

- The **Vulnerabilities** chart includes a graph for vulnerabilities of each severity level (High, Medium, Low, and Info). Each graph presents numbers of found vulnerability instances (y axis) for progressive scans by date (x axis).
- The **Risk Indicator** chart represents each scan result combining quantity and severity of found vulnerability instances.
- The **Management & Orchestration Publisher** indicator provides the capability to manually synchronize the latest scan for a specific project to the latest policy definition. This provides you with the most updated policy status for your project. The 'Publish' status indicates that synchronization has not yet been processed. 'In Progress' status means that its currently in-process. Once synchronization is complete, the status changes to 'Published' with the last successful publish date and time displayed.

To change settings, click **Edit** and then click **Update** to save the changes.

General Properties

1. Click the **General** tab to display its properties.



Project Name: Project 1
Preset: Checkmarx Default
Configuration: Default Configuration
Team: CxServer
Policy:

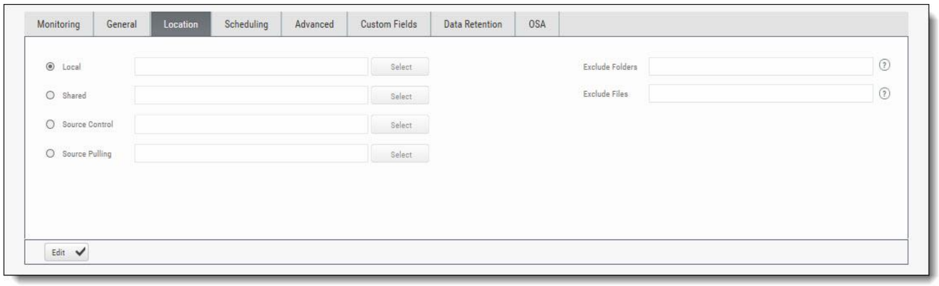
The General tab represents the project name, defined preset, configuration, associated team and policy assigned to the project.

2. Click **Edit** to change settings and then click **Update** to save the changes.

For more information about defining these properties refer to section about General properties in Creating and Configuring Projects.

Location Properties

1. Click the **Location** tab to display its properties.



The Location tab represents the various options for locating and pulling the source code for scanning.

For more information about defining these properties refer to section about Location properties in Creating and Configuring Projects.

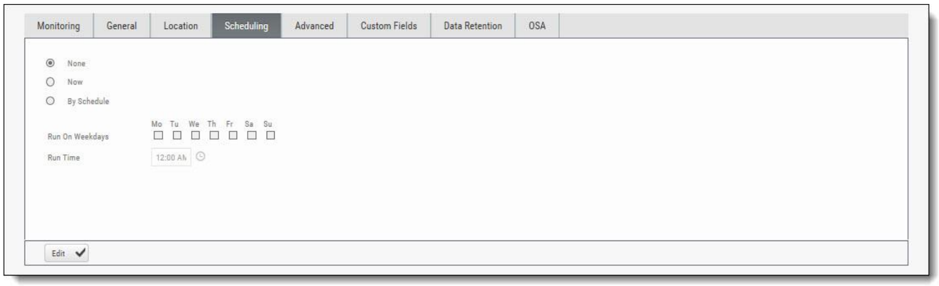
2. Click **Edit** to change settings and then click **Update** to save the changes.

Scheduling Properties

1. Click the **Scheduling** tab to display its properties.

   The Scheduling tab represents the various options for scheduling the automatic scans.

2. Click **Edit** to change settings and then click Update to save the changes.



> ⓘ Scheduling is not available for Local source code location, since the CxSAST Server cannot automatically access the local source. You will need to periodically manually upload a new zip file.

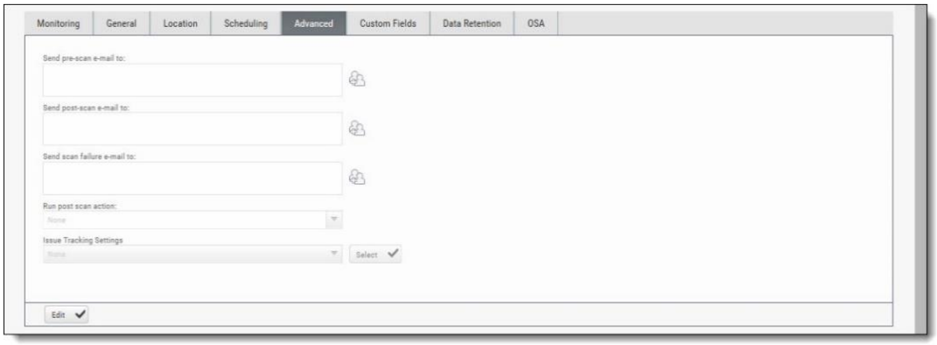
For more information about defining these properties refer to section about Scheduling properties in Creating and Configuring Projects.

Advanced Properties

1. Click the **Advanced** tab to display its properties.

   The Advanced tab represents the various options for pre/post scan actions and issue tracking settings.

2. Click **Edit** to change settings and then click **Update** to save the changes.



Send pre-scan e-mail to:

Send post-scan e-mail to:

Send scan failure e-mail to:

Run post scan action: None

Issue Tracking Settings: None

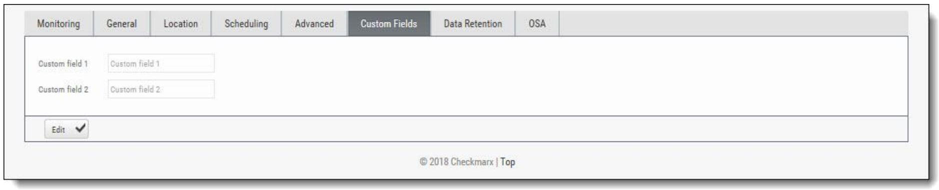
For more information about defining these properties refer to section about Advanced properties in Creating and Configuring Projects.

Custom Fields Properties

1. Click the **Custom Fields** tab to display its properties.

   The Custom Fields tab represents the option to define additional project properties using the predefined custom fields.

2. Click **Edit** to change settings and then click **Update** to save the changes.



Custom field 1: Custom field 1

Custom field 2: Custom field 2

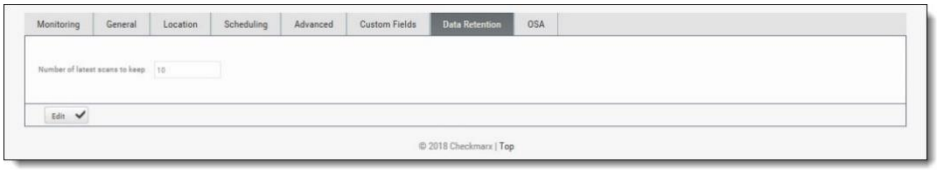
For more information about defining these properties refer to section about Custom Field properties in Creating and Configuring Projects.

Data Retention Properties

1. Click the **Data Retention** tab to display its properties.

   The Data Retention tab represents the option to define the number of last scans to be kept for the project. This helps to manage data storage consumption.

2. Click **Edit** to change settings and then click **Update** to save the changes.



Number of latest scans to keep: 10

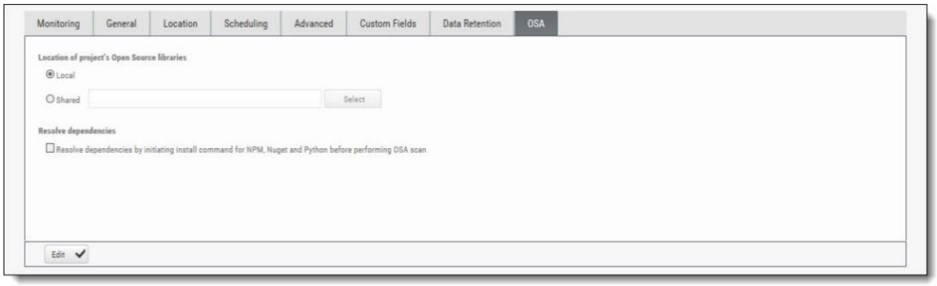
For more information about defining these properties refer to section about Data Retention properties in Creating and Configuring Projects.

CxOSA Properties

1. Click the **OSA** tab to display its properties.

   The OSA tab represents the option to define the location of the open source code libraries for analysis and resolving dependencies.

2. Click **Edit** to change settings and then click **Update** to save the changes.



Location of project's Open Source libraries

● Local

○ Shared

Resolve dependencies

□ Resolve dependencies by initiating install command for NPM, Nuget and Python before performing OSA scan

For more information about defining these properties refer to section about Open Source Analysis properties in Creating and Configuring Projects.

Managing Queries

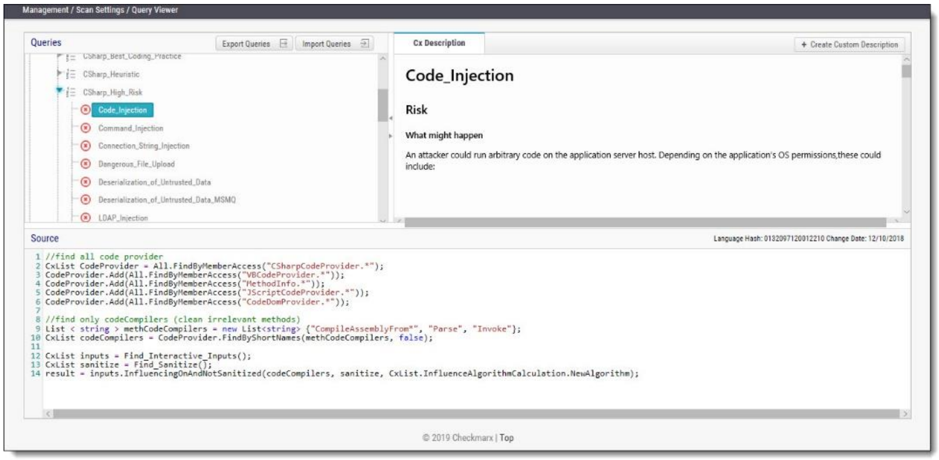
You can import and export CxSAST code queries as XML files. You can manage sets of queries known as **Presets** to be selected per-project to be used.

Viewing, Importing, and Exporting Queries

The Query Viewer displays all Checkmarx default queries and custom queries, with their descriptions and source code. You can import and export custom queries as XML files.

➢ **To export queries:**

1. Go to **Settings** > **Scan Settings** > **Query Viewer**:


Management / Scan Settings / Query Viewer
Queries
Export Queries
Import Queries
CSharp_Best_Coding_Practice
CSharp_Heuristic
CSharp_High_Risk
Code_Injection
Command_Injection
Connection_String_Injection
Dangerous_File_Upload
Deserialization_of_Untrusted_Data
Deserialization_of_Untrusted_Data_MSMQ
LDAP_Injection
Cx Description
+ Create Custom Description
Source
© 2019 Checkmarx | Top

Code_Injection

Risk

What might happen

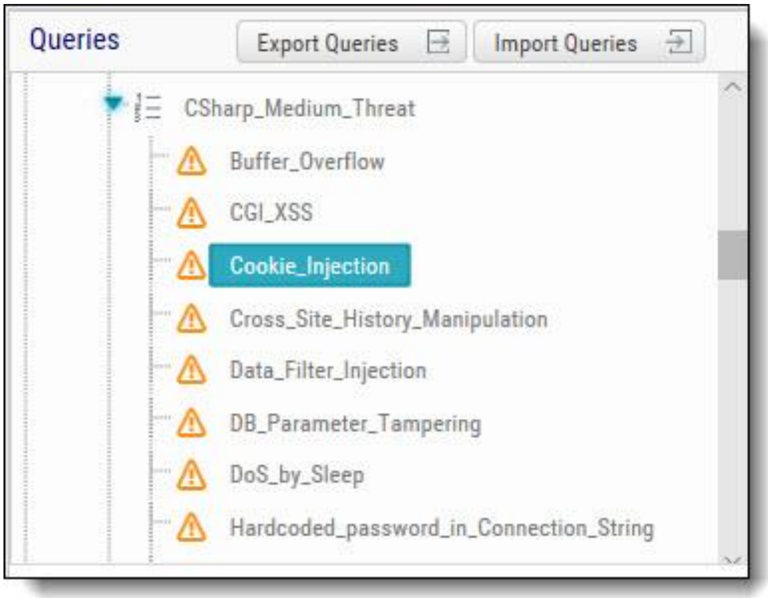
An attacker could run arbitrary code on the application server host. Depending on the application's OS permissions,these could include:

Language Hash: 0132097120012210 Change Date: 12/10/2018

```
//find all code provider
CxList CodeProvider = All.FindByMemberAccess("CSharpCodeProvider.*");
CodeProvider.Add(All.FindByMemberAccess("VBCodeProvider.*"));
CodeProvider.Add(All.FindByMemberAccess("MethodInfo.*"));
CodeProvider.Add(All.FindByMemberAccess("JScriptCodeProvider.*"));
CodeProvider.Add(All.FindByMemberAccess("CodeDomProvider.*"));

//find only codeCompilers (clean irrelevant methods)
List < string > methCodeCompilers = new List<string> {"CompileAssemblyFrom*", "Parse", "Invoke"};
CxList codeCompilers = CodeProvider.FindByShortNames(methCodeCompilers, false);

CxList inputs = Find_Interactive_Inputs();
CxList sanitize = Find_Sanitize();
result = inputs.InfluencingOnAndNotSanitized(codeCompilers, sanitize, CxList.InfluenceAlgorithmCalculation.NewAlgorithm);
```

To keep track of changes to query sets, you can select a language (or one of its child items) and view the **Hash** and **Change Date** of the last changes to the language's query set. To view a query's **Description** and **Source** code, select the query.

2. Select organizational custom queries to be exported



3. Click **Export Queries**.
4. Save the exported XML file.

➢ **To import queries:**

1. Click I**mport Queries**.
2. Select the XML file to be imported.

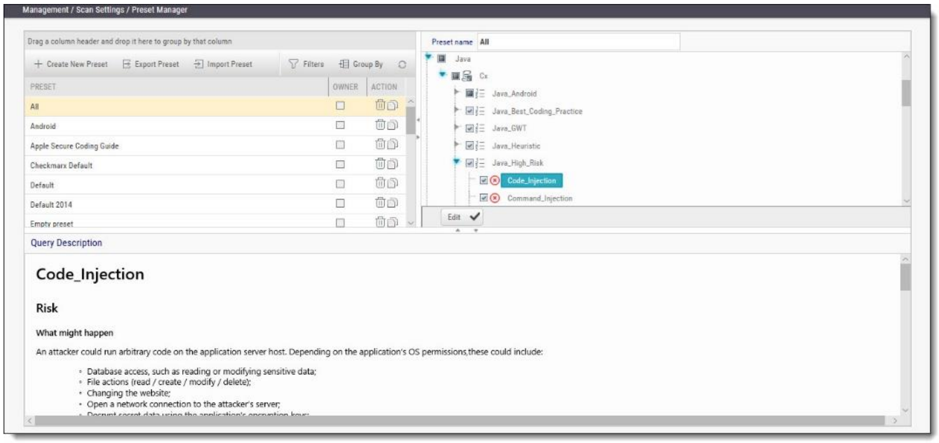
ⓘ If the imported query has the same name as an existing one, the existing query will be overridden

Managing Query Presets

Presets are sets of queries that you can select when Creating and Configuring a CxSAST Project to be used when scanning. Predefined presets are provided, and you can configure your own. You can also import and export presets.

➢ **To create a new preset:**

1. Go to **Settings** > **Scan Settings** > **Preset Manager**, and click **Create New Preset**:



PRESET	OWNER	ACTION
All	☐	
Android	☐	
Apple Secure Coding Guide	☐	
Checkmarx Default	☐	
Default	☐	
Default 2014	☐	
Empty preset	☐	

Code_Injection

Risk

What might happen

An attacker could run arbitrary code on the application server host. Depending on the application's OS permissions,these could include:

- Database access, such as reading or modifying sensitive data;
- File actions (read / create / modify / delete);
- Changing the website;
- Open a network connection to the attacker's server;
- Decrypt secret data using the application's encryption keys;

2. Type a preset **Name** and click **OK**.
3. Select a code language.
4. Select queries to be included in the preset.
5. Click **Save**.

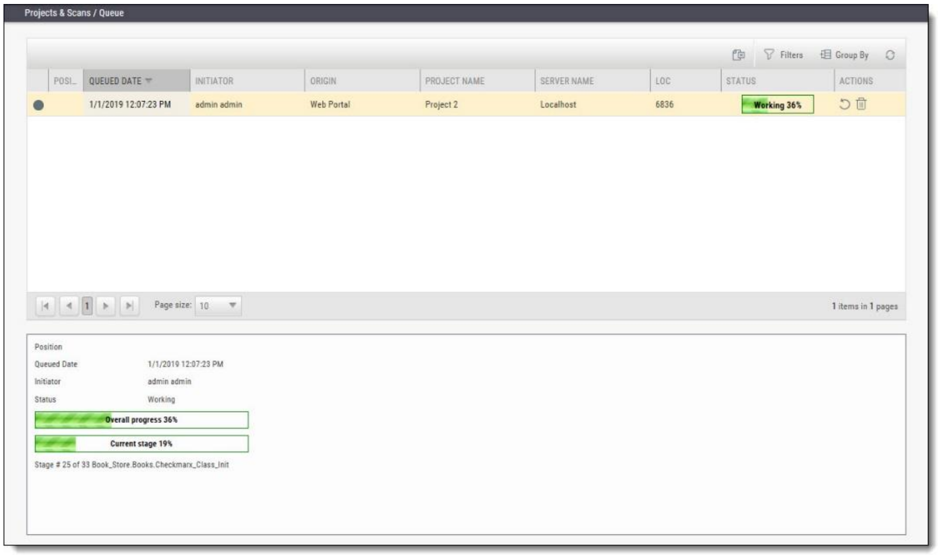
➢ **To export a preset:**

1. Go to **Settings** > **Scan Settings**, and select the preset to be exported.
2. Click **Export Preset**.
3. Save the exported XML file.
4. To import a preset:
5. Go to **Settings** > **Scan Settings**, and click **Import Preset**.
6. Choose the preset XML file to be imported.

> ⓘ If the imported preset includes a query that has the same name as an existing one, the existing query will be overridden.

The Queue

The Queue is accessed via **Projects & Scans > Queue**. It lists the scan that is currently running and the order in which the following scans will be executed. You can manage the table.



	POSI...	QUEUED DATE	INITIATOR	ORIGIN	PROJECT NAME	SERVER NAME	LOC	STATUS	ACTIONS
●		1/1/2019 12:07:23 PM	admin admin	Web Portal	Project 2	Localhost	6836	Working 36%	↺ 🗑

Position	
Queued Date	1/1/2019 12:07:23 PM
Initiator	admin admin
Status	Working

Overall progress 36%

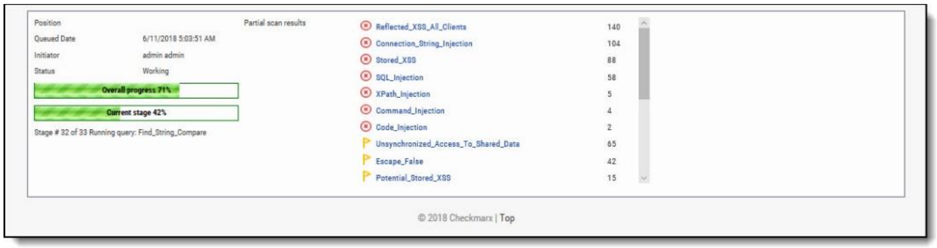
Current stage 19%

Stage # 25 of 33 Book_Store.Books.Checkmarx_Class_Init

For each scan, the Queue table displays details including Date and time, the initiating user, the originating system, the Server name (the CxEngine server performing the scan), the Project name, the number of Lines Of Code (LOC), scan status (see below), and available actions (see below).

1. Click ↺ to postpone a scan. Postpone will stop the current scan and move it to the end of the scan queue. Once the scan gets to the top of the queue, it will start scanning again.
2. Click 🗑 to delete a scan. Delete will remove the current scan from the queue.

Selecting a scan displays its details, and a progress bar indicating the percentage of scan completion, below the table. Once the first query is completed (usually at about 50% of the scan), a summary of partial results appears, with links to the actual results:



Position	
Queued Date	6/11/2018 5:03:51 AM
Initiator	admin admin
Status	Working

Overall progress 71%

Current stage 42%

Stage # 32 of 33 Running query: Find_String_Compare

Partial scan results

⊗ Reflected_XSS_All_Clients	140
⊗ Connection_String_Injection	104
⊗ Stored_XSS	88
⊗ SQL_Injection	58
⊗ XPath_Injection	5
⊗ Command_Injection	4
⊗ Code_Injection	2
⚑ Unsynchronized_Access_To_Shared_Data	65
⚑ Escape_False	42
⚑ Potential_Stored_XSS	15

In the table, each scan shows one of the following in the **Status** column:

- **Progress bar**: Shows the percentage of scan completion
- **Pending**: Scan request submitted, but still performing preparatory tasks, such as uploading or extracting
- **Queued**: Ready to scan but waiting for system resources

- **Finished**: Completed scans remain in the Queue window for a configurable time period (by default, 10 minutes)
- **Failed**: When the scan fails it disappears from the queue and reappears in the failed scans page in the Dashboard

The Queue window refreshes every minute. If an active scan (showing a progress bar) is selected, the window refreshes every 10 seconds.

Multiple projects may be run in parallel, assuming the proper license is installed and system resources availability. Each scan requires its own processing core, and 1GB RAM for every 150,000 lines of code. If system resources are in use but will be available, the project is queued; if total system resources are not sufficient for the scan, an error message is displayed.

Scan Results

Viewing Results from All Scans

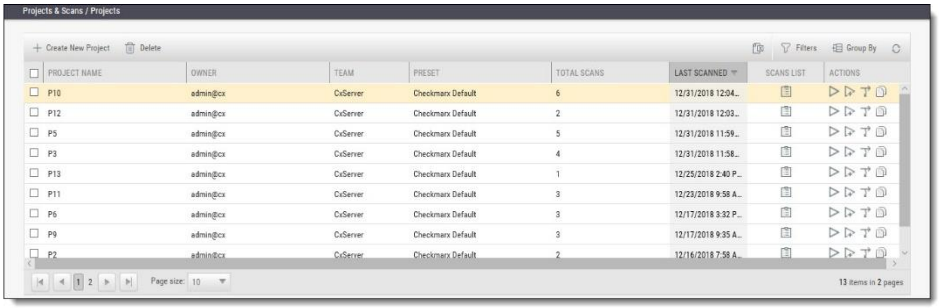
To view scan results, you can view either of the following tables:

- In Projects & Scans > Projects, view an individual project scan results.
- In Projects & Scans > All Scans, view the results from all scans.

To see one project scan results using the All Scans table, in the project's row, click Open Viewer .

Projects Scan List and Actions

In Projects & Scans > Projects, various scans and action lists are available (see Creating and Configuring Projects).



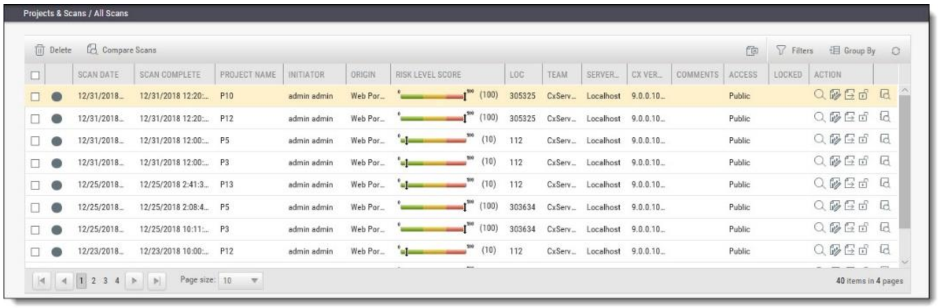
□	PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS
□	P10	admin@cx	CxServer	Checkmarx Default	6	12/31/2018 12:04...		
□	P12	admin@cx	CxServer	Checkmarx Default	2	12/31/2018 12:03...		
□	P5	admin@cx	CxServer	Checkmarx Default	5	12/31/2018 11:59...		
□	P3	admin@cx	CxServer	Checkmarx Default	4	12/31/2018 11:58...		
□	P13	admin@cx	CxServer	Checkmarx Default	1	12/25/2018 2:40 P...		
□	P11	admin@cx	CxServer	Checkmarx Default	3	12/23/2018 9:58 A...		
□	P6	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 3:32 P...		
□	P9	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 9:35 A...		
□	P2	admin@cx	CxServer	Checkmarx Default	2	12/16/2018 7:58 A...		

13 items in 2 pages

Column	Action	Description
Scan List	View Project Scans	Displays the project in the individual project path, for example, Projects & Scans/View Project Scans/My Java Projects.
Actions	Full Scan	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.
	Incremental Scan	A scan of only new and modified files since the last previous scan. Incremental scan significantly shortens the scan time, but it is not recommended for projects with significant amounts of changes.
	Branch Project	The Branch Project operation is similar to copy project, but it copies a different set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
	Duplicate Project	Duplicate Project creates a new project based on the setting of an existing one. From the existing project it will copy the following: Preset, Team, Exclusions, Scheduling, Pre-scan emails, Post-scan emails and Scan failure emails.

All Scans

All Scan results appear in a table with each row representing an individual scan result set. You can manage the table, including sorting by **Scan Date**, **Scan Complete Date**, **Project Name**, or **Risk Level Score**.



Projects & Scans / All Scans

☐		SCAN DATE	SCAN COMPLETE	PROJECT NAME	INITIATOR	ORIGIN	RISK LEVEL SCORE	LOC	TEAM	SERVER...	CX VER...	COMMENTS	ACCESS	LOCKED	ACTION
☐	●	12/31/2018...	12/31/2018 12:20:...	P10	admin admin	Web Por...	(100)	305325	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:20:...	P12	admin admin	Web Por...	(100)	305325	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:00:...	P5	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:00:...	P3	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 2:41:3...	P13	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 2:08:4...	P5	admin admin	Web Por...	(100)	303634	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 10:11:...	P3	admin admin	Web Por...	(100)	303634	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/23/2018...	12/23/2018 10:00:...	P12	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		

1 2 3 4 Page size: 10

40 items in 4 pages

- Indicates scan in process

● - Indicates a full scan

⊕ - Indicates an incremental scan

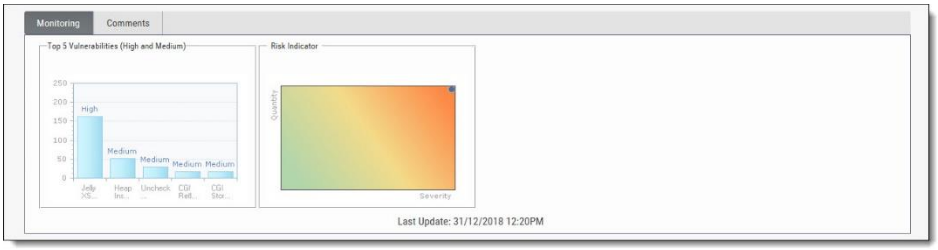
ⓘ Aditionally ❗ indicates a partial scan. Information about why only a partial scan was performed is provided in Scan Summary. For more information about partial scans, refer to the FAQ section.

Each row of the scan results table includes a Risk Level Score and a risk indicator bar, showing the overall risk calculation of all vulnerabilities found in this scan. Some of the other columns are:

- **Initiator**: The user who activated the scan
- **Origin**: The system from which the scan was activated
- **LOC**: The number of Lines of Code in the project
- **Team**: Team that the scan is assigned to
- **Server Name**: The CxEngine server that performed the scan
- **Cx Version**: The CxSAST version number at scan time.
- **Comments**: Indicates any comments maintained for the project, for future scans and for instances that continue to be found.
- **Access**: Defines whether the scan is a private scan (not visible to others, but can be viewed by immediate managers) or a public scan.
- **Locked**: Specific scans may be marked as “Locked” to avoid automated purging of important scan data. Locked scans cannot be deleted.
- There are also additional available Actions.

If a scan was initiated for a non-local project (or, for an Incremental scan for a local project) with no code changes since the previous scan, the **Comments** indicate that the scan was not actually performed.

Selecting a scan in the table displays its details at the bottom of the window:

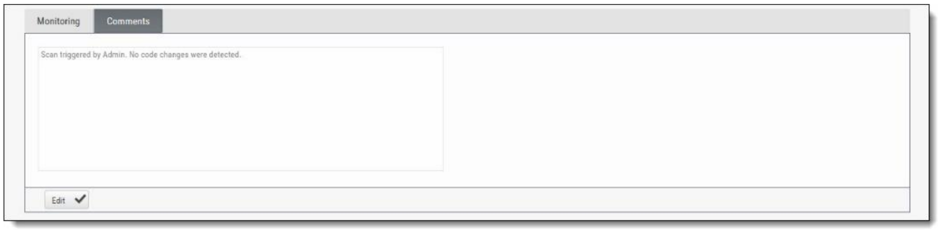


Last Update: 31/12/2018 12:20PM

The Monitoring tab provides two graphical summaries of found vulnerabilities:

- The Top 5 High and Medium Vulnerabilities chart shows the five most common High and Medium vulnerabilities found in this scan.
- The Risk Indicator chart represents the correlation between the severity and the quantity of the results.
    - Severity - Axis X (value between 0 and 100) is calculated according to the number of High, Medium and Low severity results
    - Quantity - Axis Y (value between 0 and 100) is calculated according to the number of High, Medium and Low severity results

The Comments tab allows you to write comments on the scan results.



Scan triggered by Admin. No code changes were detected.

Deleting Scans

➢ **To delete one or more scans:**

1. Select the rows of the requested scans.
2. Click the Delete button. A prompt appears, requesting you to confirm the deletion operation.
3. Click **OK**.

If the user does not have the authorization required for deleting scans, no scan is deleted.

If one or more scans are locked, a message appears indicating, for example, that only 2 of the 3 scans were deleted successfully.

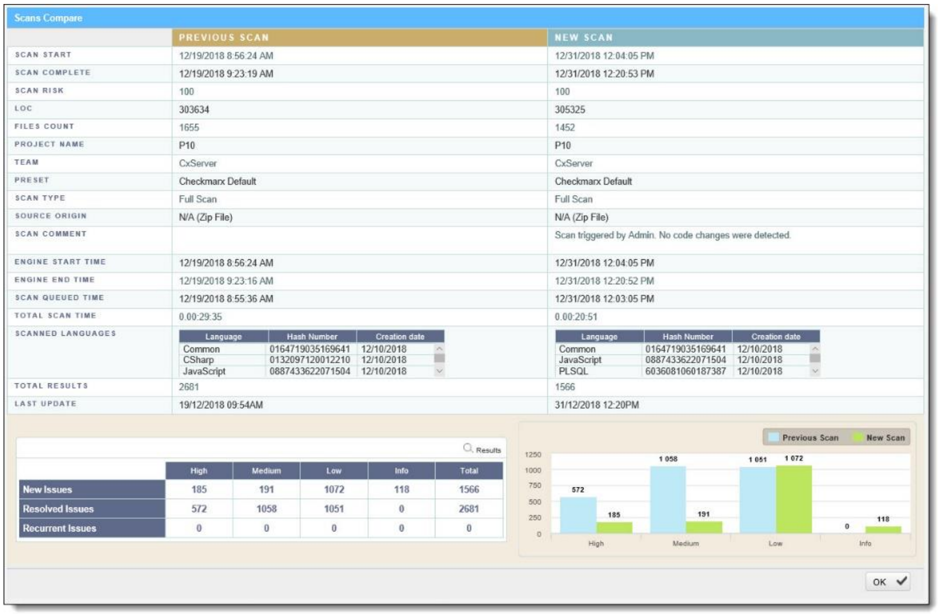
Clicking the Export as CSV File options downloads the DeleteErrors.csv file, which displays the details of the locked scans.

Unlocking all scans indicated in the report enables full deletion of the project.

Comparing Scans

➢ **To compare scans:**

1. In Projects & Scans > All Scans, select two scans to compare.
2. Click the Compare Scans option. The Scans Compare screen is displayed.



Scans Compare

	PREVIOUS SCAN	NEW SCAN
SCAN START	12/19/2018 8:56:24 AM	12/31/2018 12:04:05 PM
SCAN COMPLETE	12/19/2018 9:23:19 AM	12/31/2018 12:20:53 PM
SCAN RISK	100	100
LOC	303634	305325
FILES COUNT	1655	1452
PROJECT NAME	P10	P10
TEAM	CxServer	CxServer
PRESET	Checkmarx Default	Checkmarx Default
SCAN TYPE	Full Scan	Full Scan
SOURCE ORIGIN	N/A (Zip File)	N/A (Zip File)
SCAN COMMENT		Scan triggered by Admin. No code changes were detected.
ENGINE START TIME	12/19/2018 8:56:24 AM	12/31/2018 12:04:05 PM
ENGINE END TIME	12/19/2018 9:23:16 AM	12/31/2018 12:20:52 PM
SCAN QUEUED TIME	12/19/2018 8:55:36 AM	12/31/2018 12:03:05 PM
TOTAL SCAN TIME	0.00:29:35	0.00:20:51
SCANNED LANGUAGES	Language / Hash Number / Creation date Common 0164719035169641 12/10/2018 CSharp 0132097120012210 12/10/2018 JavaScript 0887433622071504 12/10/2018	Language / Hash Number / Creation date Common 0164719035169641 12/10/2018 JavaScript 0887433622071504 12/10/2018 PLSQL 6036081060187387 12/10/2018
TOTAL RESULTS	2681	1566
LAST UPDATE	19/12/2018 09:54AM	31/12/2018 12:20PM

Results

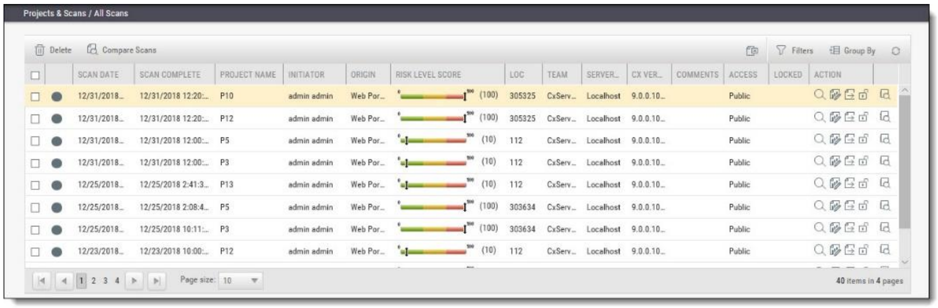
	High	Medium	Low	Info	Total
New Issues	185	191	1072	118	1566
Resolved Issues	572	1058	1051	0	2681
Recurrent Issues	0	0	0	0	0

3. Click on the Results button in order to see a 'file compare' showing the code differences in each file, grouped by vulnerability/scan result.

Scan Result Actions

Navigating All Scans

In the All Scans screen, you can implement the following scan result actions.



Projects & Scans / All Scans

☐		SCAN DATE	SCAN COMPLETE	PROJECT NAME	INITIATOR	ORIGIN	RISK LEVEL SCORE	LOC	TEAM	SERVER...	CX VER...	COMMENTS	ACCESS	LOCKED	ACTION
☐	●	12/31/2018...	12/31/2018 12:20:...	P10	admin admin	Web Por...	(100)	305325	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:20:...	P12	admin admin	Web Por...	(100)	305325	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:00:...	P5	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/31/2018...	12/31/2018 12:00:...	P3	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 2:41:3...	P13	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 2:08:4...	P5	admin admin	Web Por...	(100)	303634	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/25/2018...	12/25/2018 10:11:...	P3	admin admin	Web Por...	(100)	303634	CxServ...	Localhost	9.0.0.10...		Public		
☐	●	12/23/2018...	12/23/2018 10:00:...	P12	admin admin	Web Por...	(10)	112	CxServ...	Localhost	9.0.0.10...		Public		

1 2 3 4 Page size: 10

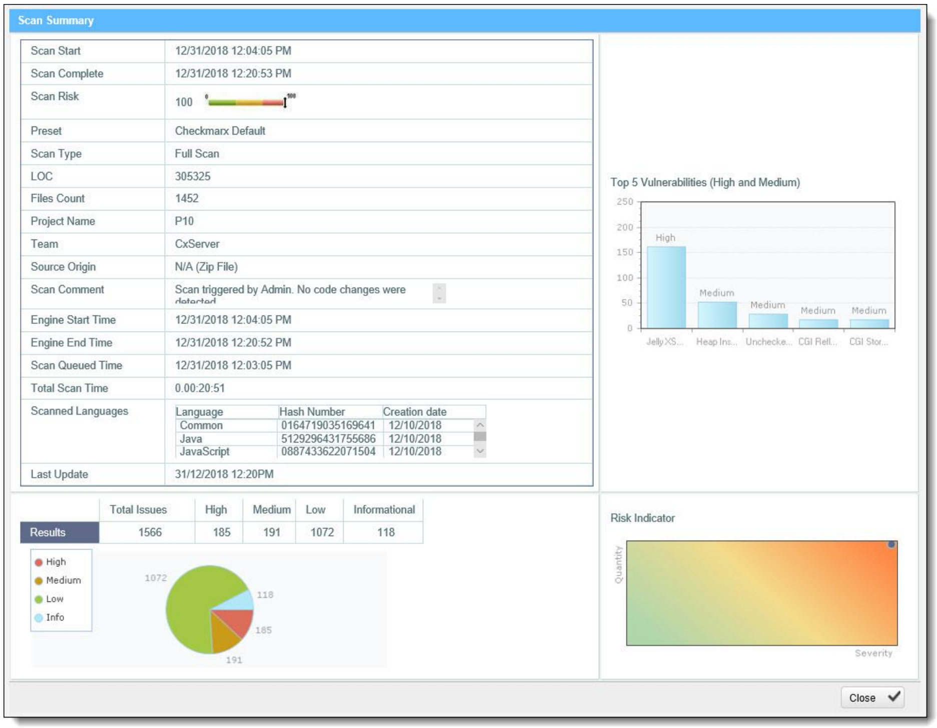
40 items in 4 pages

Column	Action	Description
Action	🔍	View Scan Results
		Create Report
		Open Scan Summary
		Download Scan Logs (requires the 'download_scan_log' permission)

Viewing the Scan Summary

➢ **To view the Scan Summary:**

1. In Projects & Scans > All Scan, click the Open Scan Summary option. The Scan Summary window is displayed.



Scan Summary

Scan Start	12/31/2018 12:04:05 PM
Scan Complete	12/31/2018 12:20:53 PM
Scan Risk	100
Preset	Checkmarx Default
Scan Type	Full Scan
LOC	305325
Files Count	1452
Project Name	P10
Team	CxServer
Source Origin	N/A (Zip File)
Scan Comment	Scan triggered by Admin. No code changes were detected
Engine Start Time	12/31/2018 12:04:05 PM
Engine End Time	12/31/2018 12:20:52 PM
Scan Queued Time	12/31/2018 12:03:05 PM
Total Scan Time	0.00:20:51
Scanned Languages	
Last Update	31/12/2018 12:20PM

Language	Hash Number	Creation date
Common	0164719035169641	12/10/2018
Java	5129296431755686	12/10/2018
JavaScript	0887433622071504	12/10/2018

	Total Issues	High	Medium	Low	Informational
Results	1566	185	191	1072	118

The Scan Summary window includes the following scan information:

- Scan details table: Shows the scan start and finish dates, risk level, LOC (Lines of Code in project), number of files, preset (query set), scan type, source origin, and comment.

> ⓘ For Scan Type ! indicates a partial scan. For more information about partial scans, refer to the FAQ section.

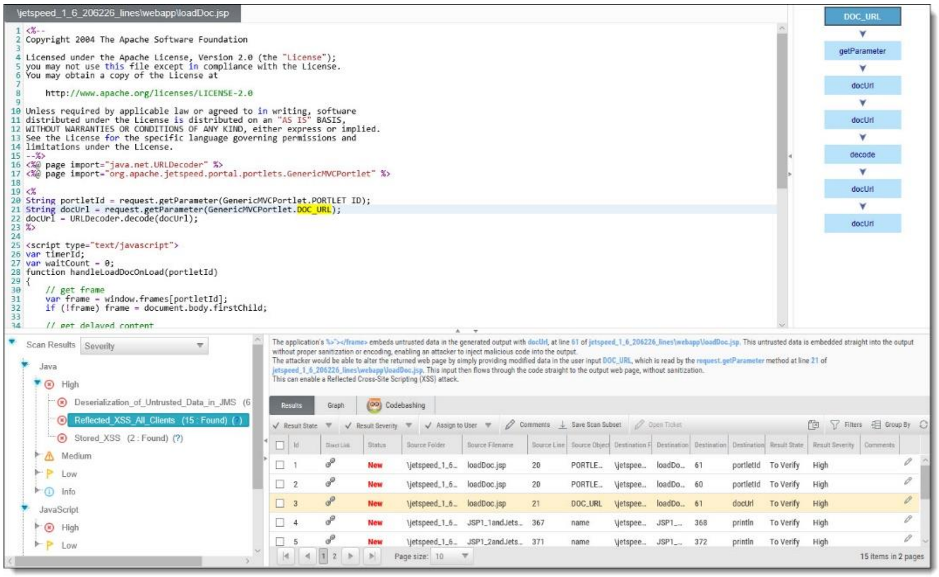
- The Top 5 High and Medium Vulnerabilities chart shows the five most common high and medium vulnerabilities found in this scan.
- The Pie chart shows the number of found vulnerabilities of each severity level as a percentage of all found vulnerabilities.
- The Risk Indicator chart presents the scan status as combination of quantity and severity of found vulnerabilities.

2. Click the Download Scan Logs option to download all server logs related to this scan.

Scan summaries are available to users with 'download_scan_log' permissions only.

Navigating Scan Results

When viewing full Scan Results in the web interface, you can interactively navigate through the results.



\jetspeed_1_6_206226_lines\webapp\loadDoc.jsp

```
<%--
Copyright 2004 The Apache Software Foundation

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
--%>
<%@ page import="java.net.URLDecoder" %>
<%@ page import="org.apache.jetspeed.portal.portlets.GenericMVCPortlet" %>

<%
String portletId = request.getParameter(GenericMVCPortlet.PORTLET ID);
String docUrl = request.getParameter(GenericMVCPortlet.DOC_URL);
docUrl = URLDecoder.decode(docUrl);
%>

<script type="text/javascript">
var timerId;
var waitCount = 0;
function handleLoadDocOnLoad(portletId)
{
    // get frame
    var frame = window.frames[portletId];
    if (!frame) frame = document.body.firstChild;

    // get delayed content
```

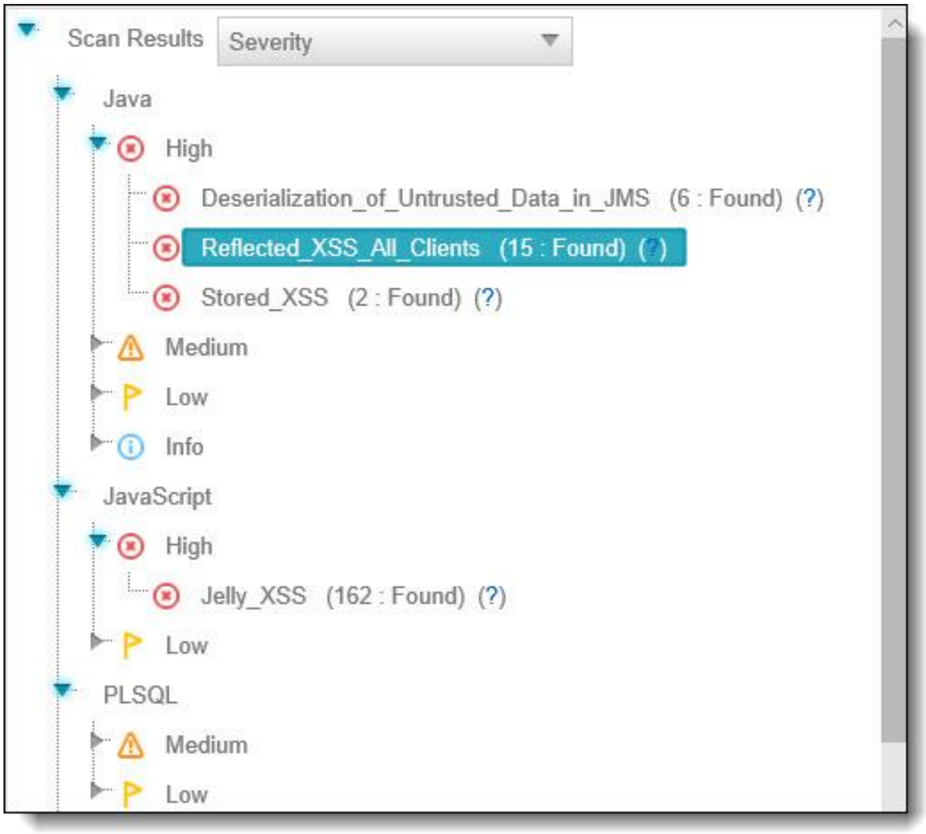
The application's %>"></frame> embeds untrusted data in the generated output with docUrl, at line 61 of jetspeed_1_6_206226_lines\webapp\loadDoc.jsp. This untrusted data is embedded straight into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the output.
The attacker would be able to alter the returned web page by simply providing modified data in the user input DOC_URL, which is read by the request.getParameter method at line 21 of jetspeed_1_6_206226_lines\webapp\loadDoc.jsp. This input then flows through the code straight to the output web page, without sanitization.
This can enable a Reflected Cross-Site Scripting (XSS) attack.

☐	Id	Direct Link	Status	Source Folder	Source Filename	Source Line	Source Object	Destination F	Destination	Destination	Destination	Result State	Result Severity	Comments
☐	1		New	\jetspeed_1_6...	loadDoc.jsp	20	PORTLE...	\jetspee...	loadDo...	61	portletId	To Verify	High	
☐	2		New	\jetspeed_1_6...	loadDoc.jsp	20	PORTLE...	\jetspee...	loadDo...	60	portletId	To Verify	High	
☐	3		New	\jetspeed_1_6...	loadDoc.jsp	21	DOC_URL	\jetspee...	loadDo...	61	docUrl	To Verify	High	
☐	4		New	\jetspeed_1_6...	JSP1_1andJets...	367	name	\jetspee...	JSP1_...	368	println	To Verify	High	
☐	5		New	\jetspeed_1_6...	JSP1_2andJets...	371	name	\jetspee...	JSP1_...	372	println	To Verify	High	

1 2 Page size: 10 15 items in 2 pages

The interface includes four panes with different levels of information. You can drill down from a comprehensive list all the way down to the actual code elements, by moving through the panes in the following order:

Queries (lower-left pane) - Each item in the list is a specific type of vulnerability for which CxSAST queries the scanned code, with the number of found instances of that vulnerability. The queries are sorted by code language, category, and severity.



Scan Results Severity

- Java
  - High
    - Deserialization_of_Untrusted_Data_in_JMS (6 : Found) (?)
    - Reflected_XSS_All_Clients (15 : Found) (?)
    - Stored_XSS (2 : Found) (?)
  - Medium
  - Low
  - Info
- JavaScript
  - High
    - Jelly_XSS (162 : Found) (?)
  - Low
- PLSQL
  - Medium
  - Low

Clicking () takes you to the **Codebashing™**, our interactive learning platform, where you can learn about code vulnerabilities, why they happen, and how to eliminate them. Once there, select a tutorial and start sharpening your skills.

Codebashing provides developers with a new in-context learning platform that sharpens the skills they need to fix vulnerabilities and write secure code. This new approach makes AppSec learning an engaging experience, more effective, with a fast learning curve.

Codebashing is currently available as a free limited edition to all users. This version includes a free edition of Codebashing covering:

- **Lessons**: SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE)
- **Languages**: Java, .Net, PHP, Node.JS, Ruby, Python

The full and paid version will include over 20+ lessons and additional languages:

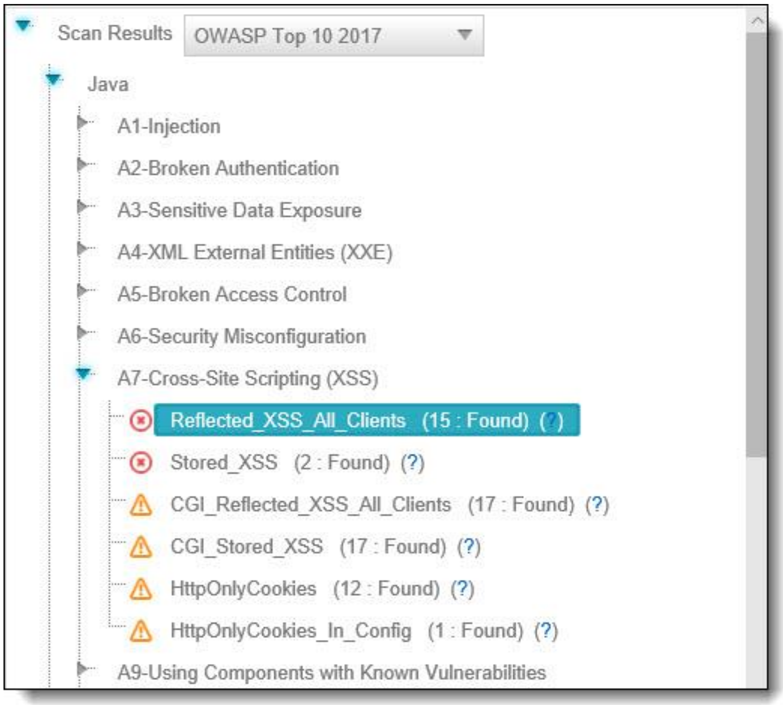
- **Lessons**: Session fixation, Use of insufficiently random values, Reflected XSS, Command Injection, DOM XSS, Directory (Path) Traversal, Privileged Interface Exposure, Leftover Debug Code, Session Exposure in URL, User Enumeration, Horizontal Privilege Escalation, Vertical Privilege Escalation, Authentication Credentials in URL, Cross Site Request Forgery (POST), Cross Site Request Forgery (GET), Click Jacking, Insecure URL Direct.
- **Languages**: Scala, C/C++.

Clicking **(?)** displays comprehensive information about this vulnerability type, including risk details, a description of the cause and mechanism, recommendations for avoiding the vulnerability and source code examples.

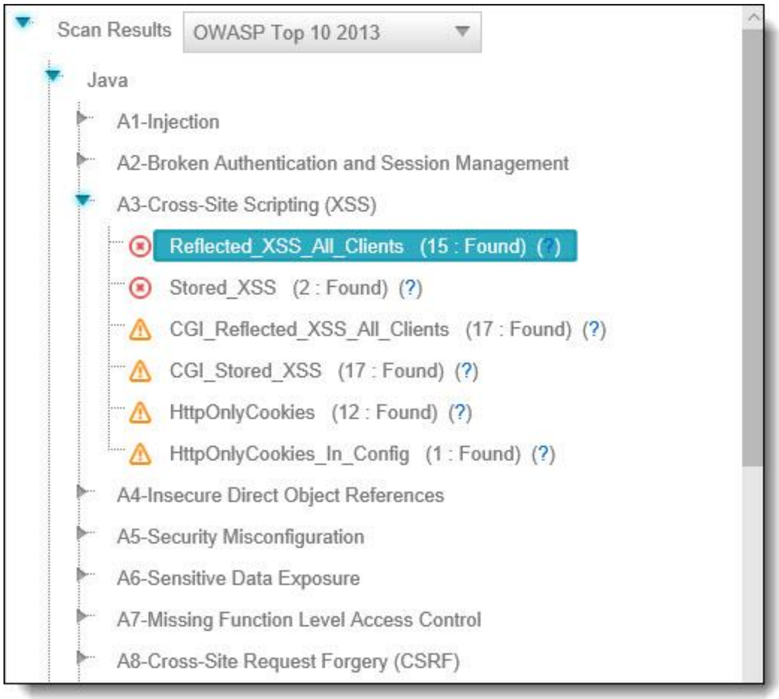
The Severity drop-down list provides the following methods for displaying the detected vulnerabilities:

- **Severity** - displays application security risks (vulnerabilities) by severity (High, Medium and Low)
- **OWASP Top 10 2017 -** displays the vulnerabilities associated with categories (A1 to A10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Top 10 2017 categories are grouped under un-categorized.
- **OWASP Top 10 2013** - displays the vulnerabilities associated with categories (A1 to A10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Top 10 2013 categories are grouped under un-categorized.
- **PCI** - displays the vulnerabilities associated with categories (DSS v3.2), as defined by PCI (Payment Card Industry). All vulnerabilities that do not fall into any of the PCI categories are grouped under un-categorized.
- **FISMA** - displays the vulnerabilities associated with categories (2014), as defined by FISMA (Federal Information Security Modernization Act). All vulnerabilities that do not fall into any of the FISMA categories are grouped under un-categorized.
- **NIST** - displays the vulnerabilities associated with categories (SP 800-53), as defined by NIST (National Institute of Standards and Technology). All vulnerabilities that do not fall into any of the NIST categories are grouped under un-categorized.
- **OWASP Mobile Top 10 2016 -** displays the vulnerabilities associated with categories (M1 to M10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Mobile Top 10 2017 categories are grouped under un-categorized.
- **Custom** - a user-defined method for rating the security levels. Using the Custom method requires integrating the user's severity rating method with CxSAST. For more details, please contact Checkmarx support.

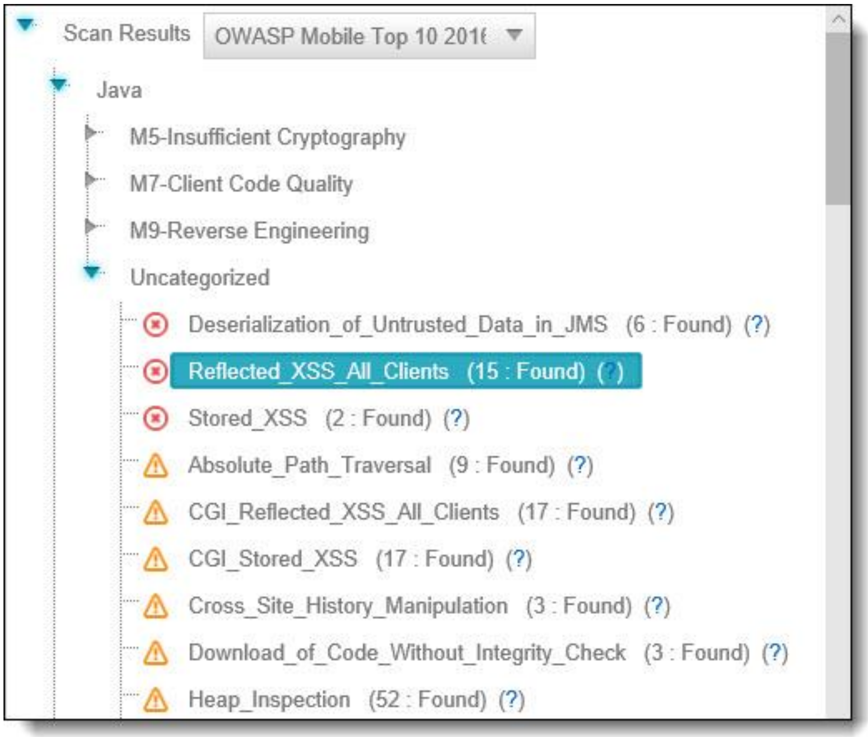
The following images show the Severity drop-down list opened after selecting OWASP Top 10 (2013 or 2017), OWASP Mobile Top 10 (2016) and PCI for the first, second, third and fourth image, respectively.



- Scan Results: OWASP Top 10 2017 ▼
  - Java
    - A1-Injection
    - A2-Broken Authentication
    - A3-Sensitive Data Exposure
    - A4-XML External Entities (XXE)
    - A5-Broken Access Control
    - A6-Security Misconfiguration
    - A7-Cross-Site Scripting (XSS)
      - ⊗ Reflected_XSS_All_Clients (15 : Found) (?)
      - ⊗ Stored_XSS (2 : Found) (?)
      - ⚠ CGI_Reflected_XSS_All_Clients (17 : Found) (?)
      - ⚠ CGI_Stored_XSS (17 : Found) (?)
      - ⚠ HttpOnlyCookies (12 : Found) (?)
      - ⚠ HttpOnlyCookies_In_Config (1 : Found) (?)
    - A9-Using Components with Known Vulnerabilities

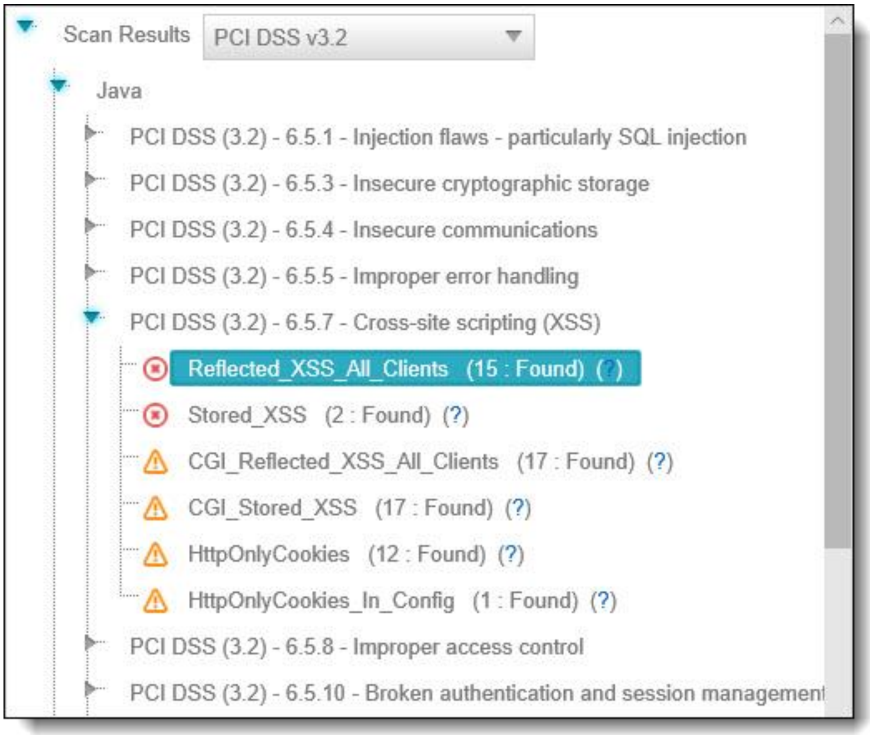


- Scan Results: OWASP Top 10 2013 ▼
  - Java
    - A1-Injection
    - A2-Broken Authentication and Session Management
    - A3-Cross-Site Scripting (XSS)
      - ⊗ Reflected_XSS_All_Clients (15 : Found) (?)
      - ⊗ Stored_XSS (2 : Found) (?)
      - ⚠ CGI_Reflected_XSS_All_Clients (17 : Found) (?)
      - ⚠ CGI_Stored_XSS (17 : Found) (?)
      - ⚠ HttpOnlyCookies (12 : Found) (?)
      - ⚠ HttpOnlyCookies_In_Config (1 : Found) (?)
    - A4-Insecure Direct Object References
    - A5-Security Misconfiguration
    - A6-Sensitive Data Exposure
    - A7-Missing Function Level Access Control
    - A8-Cross-Site Request Forgery (CSRF)



Scan Results OWASP Mobile Top 10 201(

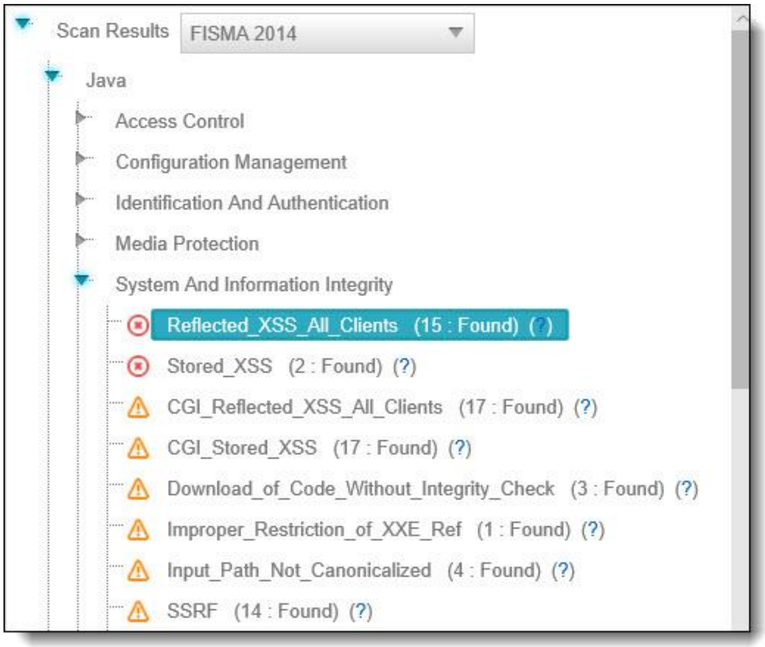
- Java
  - M5-Insufficient Cryptography
  - M7-Client Code Quality
  - M9-Reverse Engineering
  - Uncategorized
    - ⊗ Deserialization_of_Untrusted_Data_in_JMS (6 : Found) (?)
    - ⊗ Reflected_XSS_All_Clients (15 : Found) (?)
    - ⊗ Stored_XSS (2 : Found) (?)
    - ⚠ Absolute_Path_Traversal (9 : Found) (?)
    - ⚠ CGI_Reflected_XSS_All_Clients (17 : Found) (?)
    - ⚠ CGI_Stored_XSS (17 : Found) (?)
    - ⚠ Cross_Site_History_Manipulation (3 : Found) (?)
    - ⚠ Download_of_Code_Without_Integrity_Check (3 : Found) (?)
    - ⚠ Heap_Inspection (52 : Found) (?)



Scan Results PCI DSS v3.2

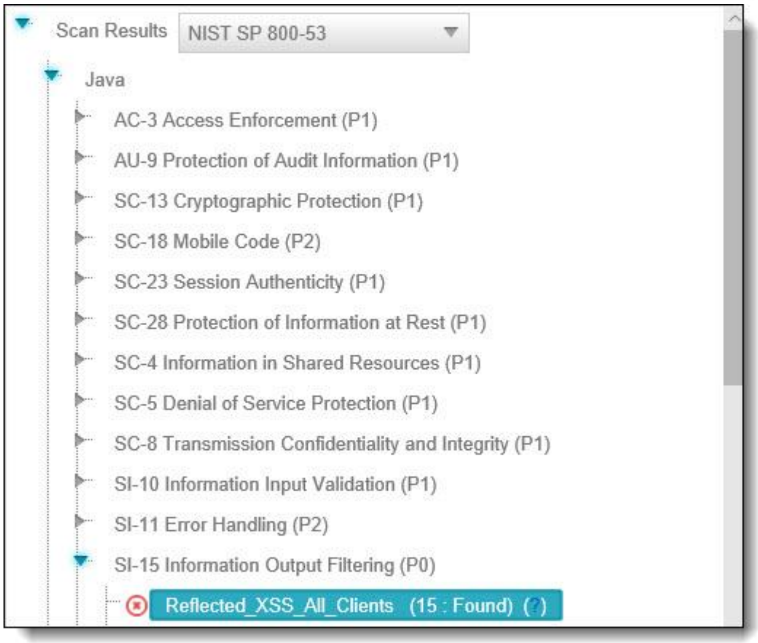
- Java
  - PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
  - PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage
  - PCI DSS (3.2) - 6.5.4 - Insecure communications
  - PCI DSS (3.2) - 6.5.5 - Improper error handling
  - PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
    - ⊗ Reflected_XSS_All_Clients (15 : Found) (?)
    - ⊗ Stored_XSS (2 : Found) (?)
    - ⚠ CGI_Reflected_XSS_All_Clients (17 : Found) (?)
    - ⚠ CGI_Stored_XSS (17 : Found) (?)
    - ⚠ HttpOnlyCookies (12 : Found) (?)
    - ⚠ HttpOnlyCookies_In_Config (1 : Found) (?)
  - PCI DSS (3.2) - 6.5.8 - Improper access control
  - PCI DSS (3.2) - 6.5.10 - Broken authentication and session managemen

The following images show the Severity drop-down list opened after selecting FISMA and NIST for the first and second image, respectively.



Scan Results FISMA 2014

- Java
  - Access Control
  - Configuration Management
  - Identification And Authentication
  - Media Protection
  - System And Information Integrity
    - Reflected_XSS_All_Clients (15 : Found) (?)
    - Stored_XSS (2 : Found) (?)
    - CGI_Reflected_XSS_All_Clients (17 : Found) (?)
    - CGI_Stored_XSS (17 : Found) (?)
    - Download_of_Code_Without_Integrity_Check (3 : Found) (?)
    - Improper_Restriction_of_XXE_Ref (1 : Found) (?)
    - Input_Path_Not_Canonicalized (4 : Found) (?)
    - SSRF (14 : Found) (?)

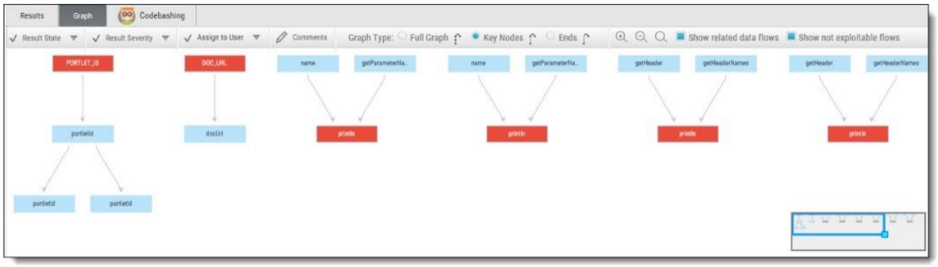


Scan Results NIST SP 800-53

- Java
  - AC-3 Access Enforcement (P1)
  - AU-9 Protection of Audit Information (P1)
  - SC-13 Cryptographic Protection (P1)
  - SC-18 Mobile Code (P2)
  - SC-23 Session Authenticity (P1)
  - SC-28 Protection of Information at Rest (P1)
  - SC-4 Information in Shared Resources (P1)
  - SC-5 Denial of Service Protection (P1)
  - SC-8 Transmission Confidentiality and Integrity (P1)
  - SI-10 Information Input Validation (P1)
  - SI-11 Error Handling (P2)
  - SI-15 Information Output Filtering (P0)
    - Reflected_XSS_All_Clients (15 : Found) (?)

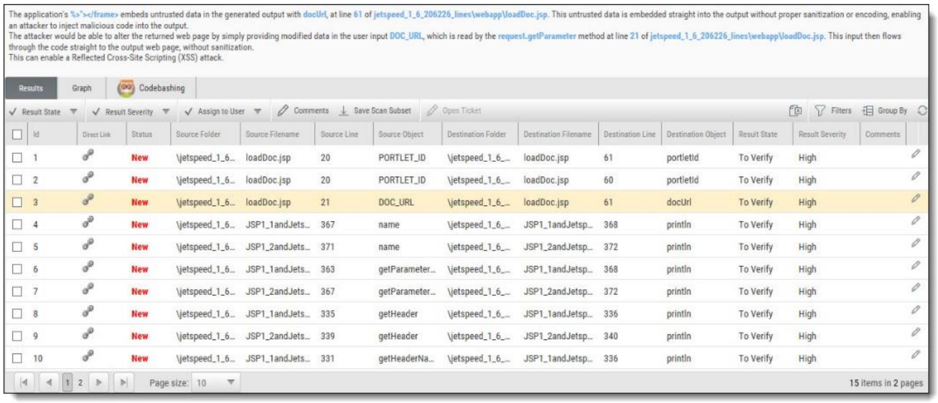
Select a query to view found instances in the **Results** pane:

- **Results** (lower-right pane) - Displays the found instances of the query that is selected in the **Queries** pane in the following two formats:
- **Graph** (right tab in **Results** pane) - Graphical display of first and last code elements of each found instance, with the relationships between them.



In the CxSAST IDE plugins, the Graph pane displays full paths of the code elements that constitute the found instances together with the relationships between them.

- **Results** (left tab in Results pane) - Tabular list of found instances and details. The highlighted instance's code element details appear at the top. You can navigate the results using pagination controls.



The application's %>"></frame> embeds untrusted data in the generated output with docUrl, at line 61 of jetspeed_1_6_206226_lines\webapp\loadDoc.jsp. This untrusted data is embedded straight into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the output.
The attacker would be able to alter the returned web page by simply providing modified data in the user input DOC_URL, which is read by the request.getParameter method at line 21 of jetspeed_1_6_206226_lines\webapp\loadDoc.jsp. This input then flows through the code straight to the output web page, without sanitization.
This can enable a Reflected Cross-Site Scripting (XSS) attack.

□	Id	Direct Link	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination Line	Destination Object	Result State	Result Severity	Comments
□	1		New	\jetspeed_1_6...	loadDoc.jsp	20	PORTLET_ID	\jetspeed_1_6_...	loadDoc.jsp	61	portletId	To Verify	High	
□	2		New	\jetspeed_1_6...	loadDoc.jsp	20	PORTLET_ID	\jetspeed_1_6_...	loadDoc.jsp	60	portletId	To Verify	High	
□	3		New	\jetspeed_1_6...	loadDoc.jsp	21	DOC_URL	\jetspeed_1_6_...	loadDoc.jsp	61	docUrl	To Verify	High	
□	4		New	\jetspeed_1_6...	JSP1_1andJets...	367	name	\jetspeed_1_6_...	JSP1_1andJetsp...	368	println	To Verify	High	
□	5		New	\jetspeed_1_6...	JSP1_2andJets...	371	name	\jetspeed_1_6_...	JSP1_2andJetsp...	372	println	To Verify	High	
□	6		New	\jetspeed_1_6...	JSP1_1andJets...	363	getParameter...	\jetspeed_1_6_...	JSP1_1andJetsp...	368	println	To Verify	High	
□	7		New	\jetspeed_1_6...	JSP1_2andJets...	367	getParameter...	\jetspeed_1_6_...	JSP1_2andJetsp...	372	println	To Verify	High	
□	8		New	\jetspeed_1_6...	JSP1_1andJets...	335	getHeader	\jetspeed_1_6_...	JSP1_1andJetsp...	336	println	To Verify	High	
□	9		New	\jetspeed_1_6...	JSP1_2andJets...	339	getHeader	\jetspeed_1_6_...	JSP1_2andJetsp...	340	println	To Verify	High	
□	10		New	\jetspeed_1_6...	JSP1_1andJets...	331	getHeaderNa...	\jetspeed_1_6_...	JSP1_1andJetsp...	336	println	To Verify	High	

1 2 Page size: 10 ▼

15 items in 2 pages

Select an instance node (Graph tab) or an instance check-box (Results tab) enabling you to change the following states (user permission dependent):

- **Results State** – Useful for disregarding false positives or just for planning what issues to handle
- **To Verify** (default) – instancl requires verification (i.e. authorized user)
- **Not Exploitable** – Instance has been confirmed as not exploitable (i.e. false positive). Instances defined with this state are not represented in the scan summary, graph, reports or dashboard, etc.

> ⓘ Depending on your user permissions you may not be able to select the "Not Exploitable" state. If this is the case, select the “Proposed Not Exploitable” state and then escalate the instance to an authorized user for confirmation.

- **Proposed Not Exploitable** – instance has been proposed as not exploitable (i.e. potential false positive). Instances defined with this state are represented in the scan summary, graph, reports or dashboard, etc. until such a time that the state is changed to “Not Exploitable"

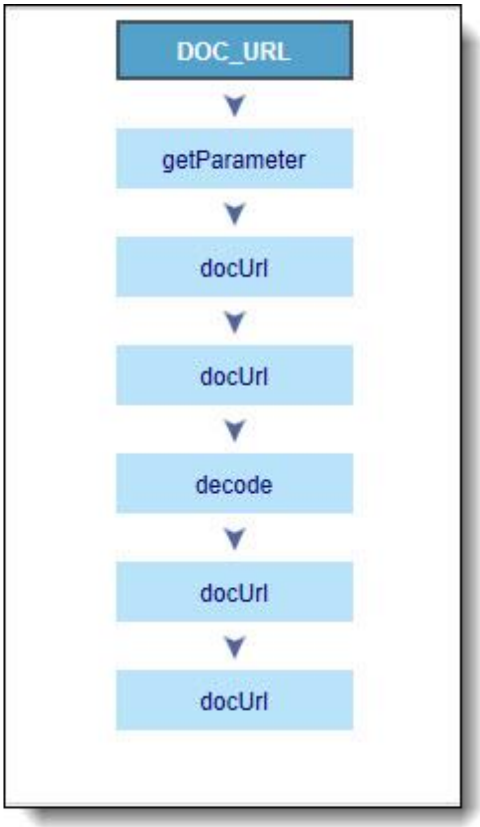
- **Confirmed** – instance has been confirmed as exploitable and requires handling
- **Urgent** – instance has been confirmed as exploitable and requires urgent handling

> ⓘ It is also possible to customize result states to your own preferences. Contact Checkmarx customer support for more information.

- **Result Severity** (High, Medium, Low and Info) - useful for defining the priority level of the selected issue.
- When the state of an instance has changed (i.e. to Not Exploitable), all other instances with same similarity ID are automatically marked with the newly changed state. A popup window is displayed (if enabled) listing all the affected instances including the project name, scan date and a direct link to the affected instance.
- **Assign to User** - useful for planning who should handle the selected issue.

  - To add a comment to an instance, click **Comments** . This metadata is maintained for the project when performing future scans and for instances that continue to be found.
  - For selected instances to appear in the results list as an independent result set, click **Save Scan Subset**.
  - If configured, tickets can be opened in a bug tracking system (e.g. Jira) by clicking **Open Ticket**.
  - Click the link icon to obtain a URL to this results interface with the instance immediately selected.

- **Path** (upper-right pane) - Displays the full path of code elements that constitute the vulnerability instance that is selected in the **Results** pane. This path represents the full attack vector for the vulnerability instance.
- **Priority** (column) - This value is used to prioritize the Findings by rank, signifying, the higher the rank, the higher the priority. Priority is calculated using a weight based formula set when defining Ranking Weights (see Setting Ranking Weights).
- **Confidence Level** (column) - This value is used to indicate the validity of the Finding. The probability (from 1%-100%) of the Finding being a True Positive.
- Select an instance in the **Results** pane (**Results** or **Graph** tab) and view its attack vector in the **Path** pane.

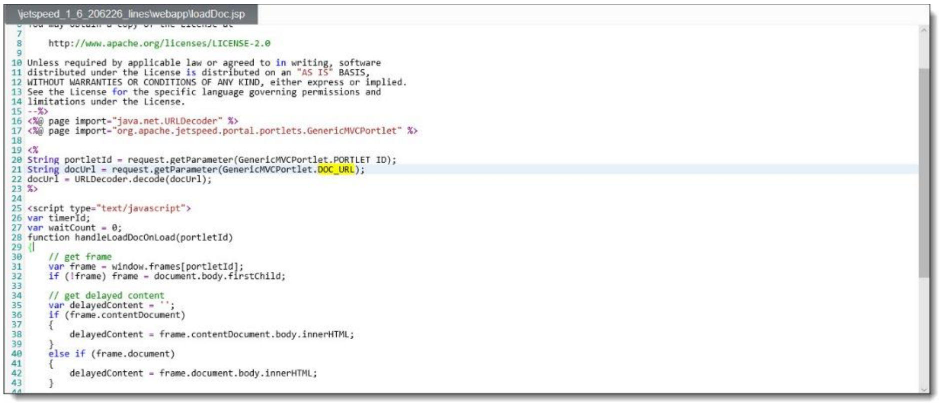


Number of Nodes

The Number of Nodes column in the Results panel provides the number of nodes in the attack vector provided by each result. Sorting, filtering and grouping options are available. This column is disabled by default and can be made available from the Columns selection tool.

Select a code element in the **Path** pane to view it in its code context, in the **Source Code** pane (see below).

Source Code (upper-left pane): Displays the source code files.


\jetspeed_1_6_206226_lines\webapp\loadDoc.jsp

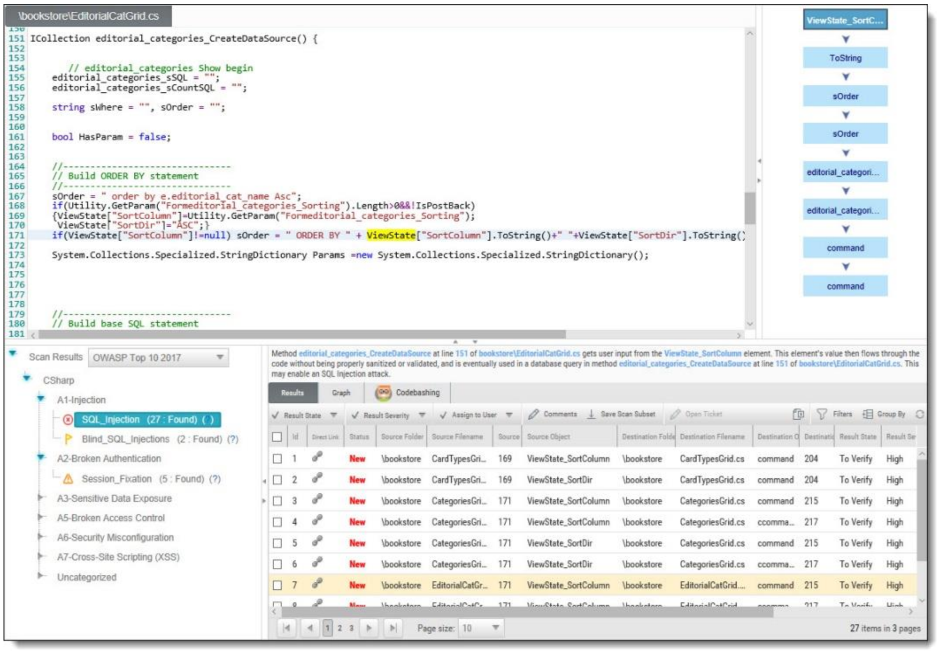
```

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
--%>
<%@ page import="java.net.URLDecoder" %>
<%@ page import="org.apache.jetspeed.portal.portlets.GenericMVCPortlet" %>

<%
String portletId = request.getParameter(GenericMVCPortlet.PORTLET ID);
String docUrl = request.getParameter(GenericMVCPortlet.DOC_URL);
docUrl = URLDecoder.decode(docUrl);
%>

<script type="text/javascript">
var timerId;
var waitCount = 0;
function handleLoadDocOnLoad(portletId)
{
    // get frame
    var frame = window.frames[portletId];
    if (!frame) frame = document.body.firstChild;

    // get delayed content
    var delayedContent = '';
    if (frame.contentDocument)
    {
        delayedContent = frame.contentDocument.body.innerHTML;
    }
    else if (frame.document)
    {
        delayedContent = frame.document.body.innerHTML;
    }
```

Highlights the code line containing the element that is selected in the **Path** pane.

> ⓘ When using the CxSAST IDE plugins, you can immediately fix the code in place!

Scan Results Example

The following is an example of the scan results showing an SQL Injection vulnerability.



```
ICollection editorial_categories_CreateDataSource() {


        // editorial_categories Show begin
    editorial_categories_sSQL = "";
    editorial_categories_sCountSQL = "";

    string sWhere = "", sOrder = "";


    bool HasParam = false;


    //-------------------------------
    // Build ORDER BY statement
    //-------------------------------
    sOrder = " order by e.editorial_cat_name Asc";
    if(Utility.GetParam("Formeditorial_categories_Sorting").Length>0&&!IsPostBack)
    {ViewState["SortColumn"]=Utility.GetParam("Formeditorial_categories_Sorting");
     ViewState["SortDir"]="ASC";}
    if(ViewState["SortColumn"]!=null) sOrder = " ORDER BY " + ViewState["SortColumn"].ToString()+" "+ViewState["SortDir"].ToString(

    System.Collections.Specialized.StringDictionary Params =new System.Collections.Specialized.StringDictionary();





    //-------------------------------
    // Build base SQL statement
```

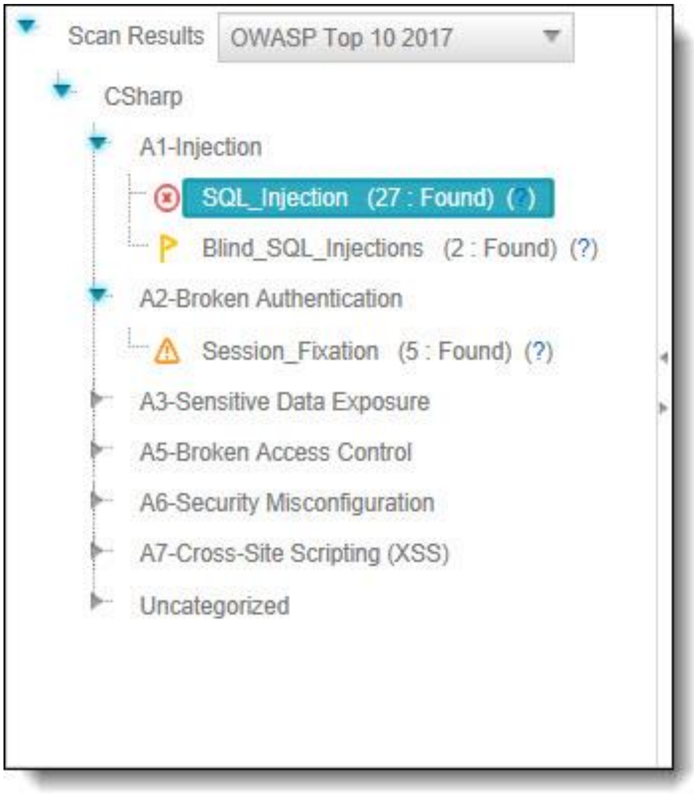
Method editorial_categories_CreateDataSource at line 151 of bookstore\EditorialCatGrid.cs gets user input from the ViewState_SortColumn element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method editorial_categories_CreateDataSource at line 151 of bookstore\EditorialCatGrid.cs. This may enable an SQL Injection attack.

□	Id	Direct Link	Status	Source Folder	Source Filename	Source	Source Object	Destination Folde	Destination Filename	Destination O	Destinatic	Result State	Result Se
□	1	🔗	New	\bookstore	CardTypesGri...	169	ViewState_SortColumn	\bookstore	CardTypesGrid.cs	command	204	To Verify	High
□	2	🔗	New	\bookstore	CardTypesGri...	169	ViewState_SortDir	\bookstore	CardTypesGrid.cs	command	204	To Verify	High
□	3	🔗	New	\bookstore	CategoriesGri...	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	command	215	To Verify	High
□	4	🔗	New	\bookstore	CategoriesGri...	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	ccomma...	217	To Verify	High
□	5	🔗	New	\bookstore	CategoriesGri...	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	command	215	To Verify	High
□	6	🔗	New	\bookstore	CategoriesGri...	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	ccomma...	217	To Verify	High
□	7	🔗	New	\bookstore	EditorialCatGr...	171	ViewState_SortColumn	\bookstore	EditorialCatGrid....	command	215	To Verify	High
□	8	🔗	New	\bookstore	EditorialCatGr...	171	ViewState_SortColumn	\bookstore	EditorialCatGrid	ccomma...	217	To Verify	High

1 2 3 Page size: 10 27 items in 3 pages

Briefly, an SQL_Injection vulnerability exists when user input is used in the syntax of an SQL query. Since those inputs could be interpreted as SQL syntax rather than user input, a user could manipulate the input in such a way as to alter query logic, potentially bypassing security checks and modifying the database, including execution of system commands.

The **Queries** pane (bottom-left) shows that 27 instances of the SQL_Injection vulnerability were found.



Scan Results OWASP Top 10 2017

- CSharp
  - A1-Injection
    - SQL_Injection (27 : Found) (?)
    - Blind_SQL_Injections (2 : Found) (?)
  - A2-Broken Authentication
    - Session_Fixation (5 : Found) (?)
  - A3-Sensitive Data Exposure
  - A5-Broken Access Control
  - A6-Security Misconfiguration
  - A7-Cross-Site Scripting (XSS)
  - Uncategorized

Clicking () takes you to the **Codebashing**, where you can learn more about the selected vulnerability, why it happens, and how to eliminate it.

Codebashing™

Codebashing provides developers with a new in-context learning platform that sharpens the skills they need to fix vulnerabilities and write secure code. This new approach makes AppSec learning an engaging experience, more effective, with a fast learning curve.

Codebashing is currently available as a free limited edition to all users. This version includes a free edition of Codebashing, covering the following:

- **Lessons**: SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE)
- **Languages**: Java, .Net, PHP, Node.JS, Ruby, Python

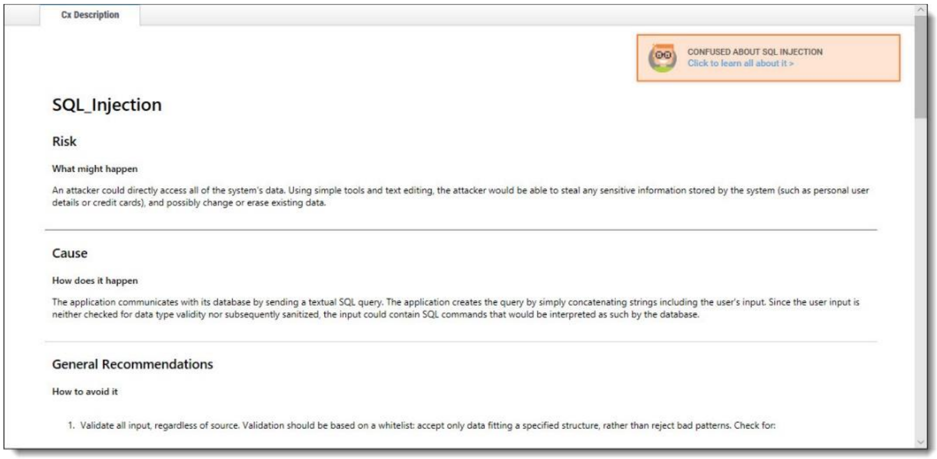
The full and paid version will include over 20+ lessons and additional languages:

- **Lessons**: Session fixation, Use of insufficiently random values, Reflected XSS, Command Injection, DOM XSS, Directory (Path) Traversal, Privileged Interface Exposure, Leftover Debug Code, Session Exposure in URL, User Enumeration, Horizontal Privilege Escalation, Vertical Privilege Escalation, Authentication Credentials in URL, Cross Site

Request Forgery (POST), Cross Site Request Forgery (GET), Click Jacking, Insecure URL Direct.

- **Languages**: Scala, C/C++.

Clicking **(?)** displays full general information for the SQL_Injection, including risk, cause and recommendations with code examples.



SQL_Injection

Risk

What might happen

An attacker could directly access all of the system's data. Using simple tools and text editing, the attacker would be able to steal any sensitive information stored by the system (such as personal user details or credit cards), and possibly change or erase existing data.

Cause

How does it happen

The application communicates with its database by sending a textual SQL query. The application creates the query by simply concatenating strings including the user's input. Since the user input is neither checked for data type validity nor subsequently sanitized, the input could contain SQL commands that would be interpreted as such by the database.

General Recommendations

How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:

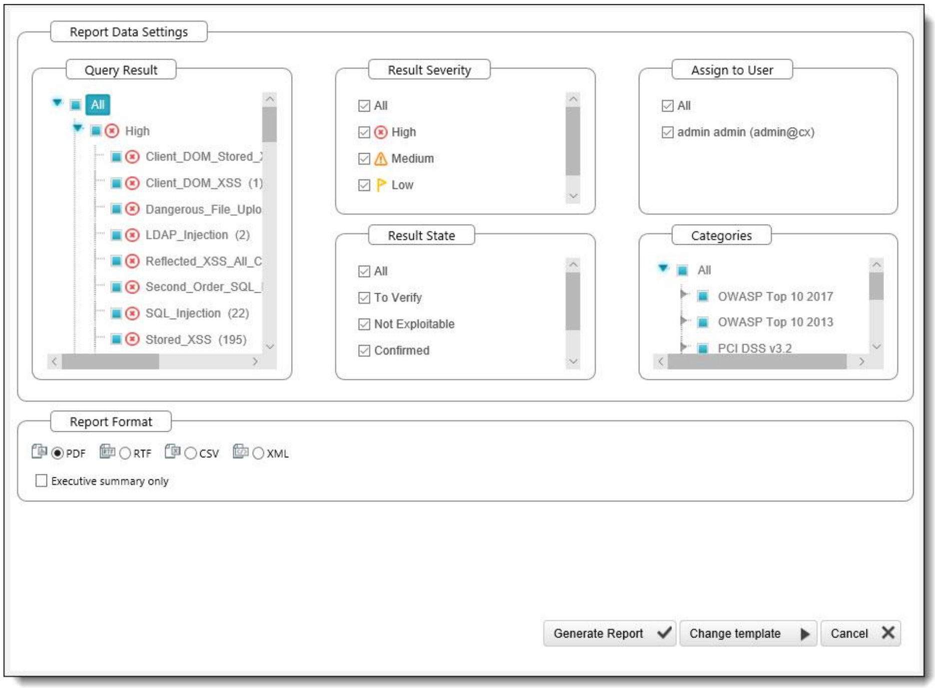
Selecting a specific instance of the vulnerability in the **Results** pane (bottom, center and right) displays the instance's code details at the top of the pane, and displays the path of component code elements in the **Path** pane (top-right). The Path pane shows all the code elements leading from the user input to the SQL query. Selecting each element in turn displays and highlights the element in the code context in the **Source Code** pane (top, left and center). The vulnerability needs to be eliminated somewhere along that path.

Generating Scan Results Report

You can generate a report containing detailed scan results, in any of the following formats: PDF (default), RTF, CSV or XML.

➢ **To generate a scan results report:**

1. In the All Scans table (for all projects or for an individual project), click **Create Report** . The report settings are displayed.



Report Data Settings

Query Result
- ■ All
  - ■ ⊗ High
    - ■ ⊗ Client_DOM_Stored_
    - ■ ⊗ Client_DOM_XSS (1)
    - ■ ⊗ Dangerous_File_Uplo
    - ■ ⊗ LDAP_Injection (2)
    - ■ ⊗ Reflected_XSS_All_C
    - ■ ⊗ Second_Order_SQL_
    - ■ ⊗ SQL_Injection (22)
    - ■ ⊗ Stored_XSS (195)

Result Severity
- ☑ All
- ☑ High
- ☑ Medium
- ☑ Low

Assign to User
- ☑ All
- ☑ admin admin (admin@cx)

Result State
- ☑ All
- ☑ To Verify
- ☑ Not Exploitable
- ☑ Confirmed

Categories
- ■ All
  - ■ OWASP Top 10 2017
  - ■ OWASP Top 10 2013
  - ■ PCI DSS v3.2

Report Format

● PDF ○ RTF ○ CSV ○ XML

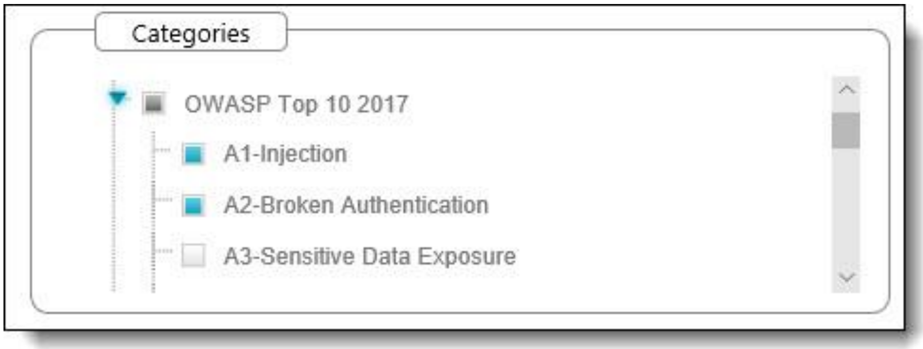
□ Executive summary only

2. Filter results for the generated report and select the report file format.

   By default, all categories are selected to be included in the report.

➢ **To customize categories:**

1. Go to the relevant group under the Categories section, click the group to expand it and clear the vulnerabilities that you do not want to display in the report, as shown below.



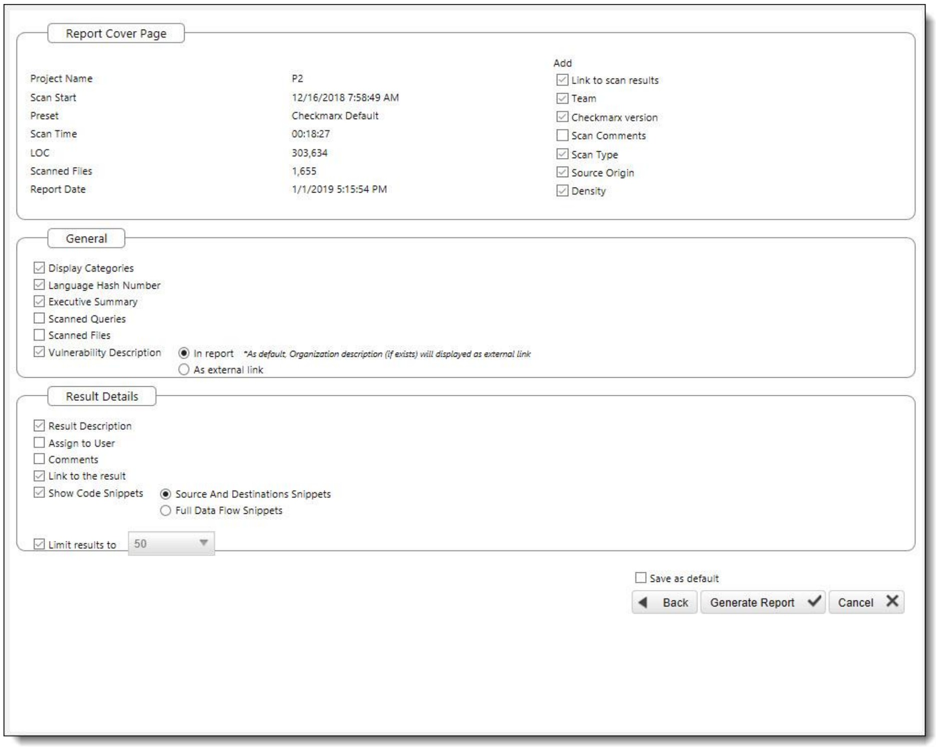
Categories
- ■ OWASP Top 10 2017
  - ■ A1-Injection
  - ■ A2-Broken Authentication
  - □ A3-Sensitive Data Exposure

2. If these changes are only relevant for a specific need and do not need to be saved as a different template, click Generate to generate the report. Otherwise, follow the procedure below to save the modifications you make as an updated report template.

➢ **To change the report template:**

1. Select **Change template**.

   The template settings are displayed.



Report Cover Page

		Add
Project Name	P2	☑ Link to scan results
Scan Start	12/16/2018 7:58:49 AM	☑ Team
Preset	Checkmarx Default	☑ Checkmarx version
Scan Time	00:18:27	□ Scan Comments
LOC	303,634	☑ Scan Type
Scanned Files	1,655	☑ Source Origin
Report Date	1/1/2019 5:15:54 PM	☑ Density

General

☑ Display Categories
☑ Language Hash Number
☑ Executive Summary
□ Scanned Queries
□ Scanned Files
☑ Vulnerability Description ● In report *As default, Organization description (if exists) will displayed as external link
○ As external link

Result Details

☑ Result Description
□ Assign to User
□ Comments
☑ Link to the result
☑ Show Code Snippets ● Source And Destinations Snippets
○ Full Data Flow Snippets

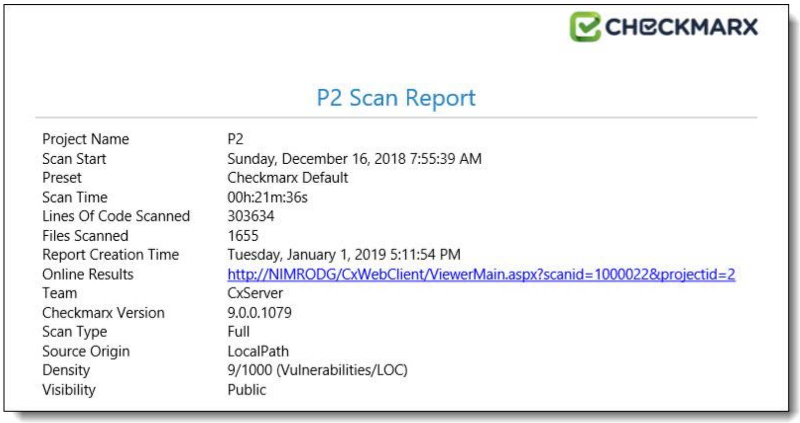
☑ Limit results to 50

□ Save as default

2. Select which details should be presented on the report cover page, in the report itself and what details to show for each result.
3. Select the **Save as default** check-box to save the modified template as the default report template.
4. Click **Back** and review all settings you defined.
5. Click **Generate Report**.

   The report starts generating.

The details about the scan are displayed on the Scan Report section at the beginning of the PDF file, as shown below.

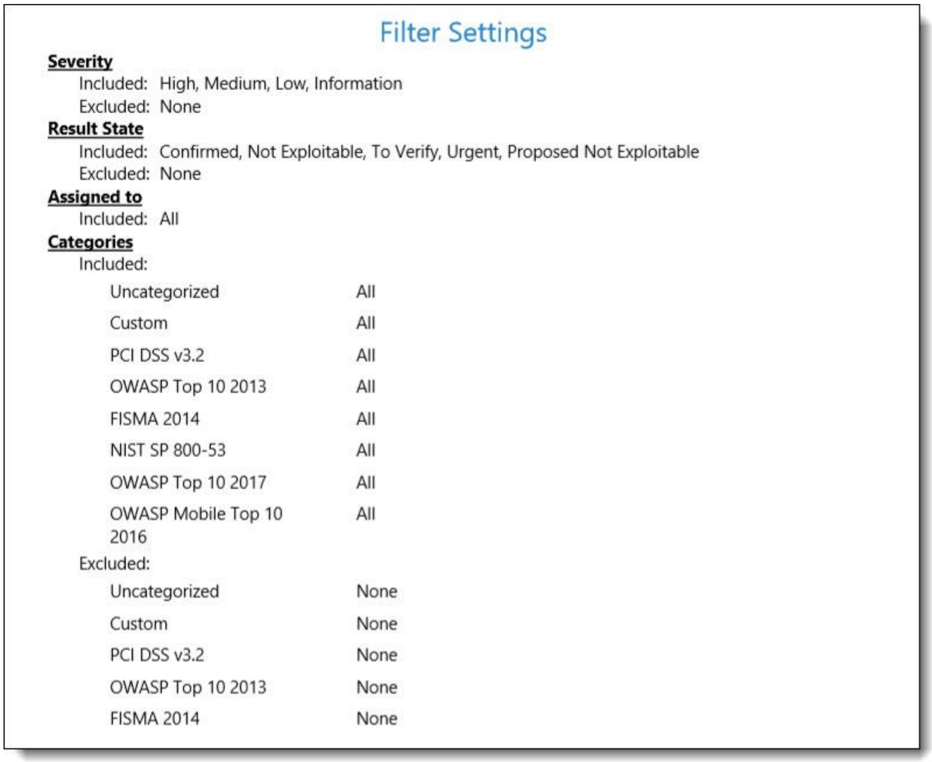


P2 Scan Report

Project Name	P2
Scan Start	Sunday, December 16, 2018 7:55:39 AM
Preset	Checkmarx Default
Scan Time	00h:21m:36s
Lines Of Code Scanned	303634
Files Scanned	1655
Report Creation Time	Tuesday, January 1, 2019 5:11:54 PM
Online Results	http://NIMRODG/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=2
Team	CxServer
Checkmarx Version	9.0.0.1079
Scan Type	Full
Source Origin	LocalPath
Density	9/1000 (Vulnerabilities/LOC)
Visibility	Public

> ⓘ In cases where the project's source location is defined as Git, the Git branch information will also be included in the PDF report underneath the Source Origin field

The exclusions that were made are displayed on the Filter Setting section, as shown below.



Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

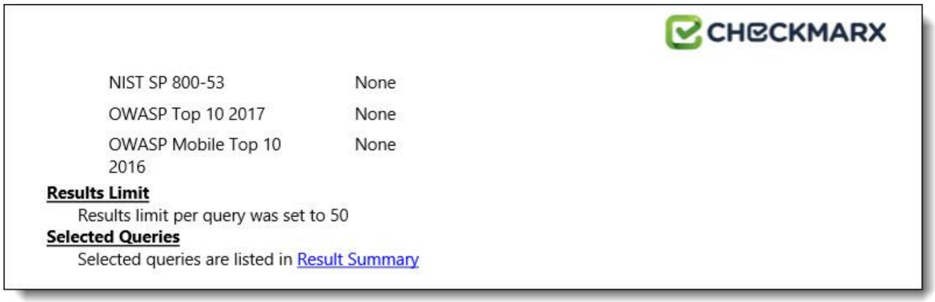
Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None



NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

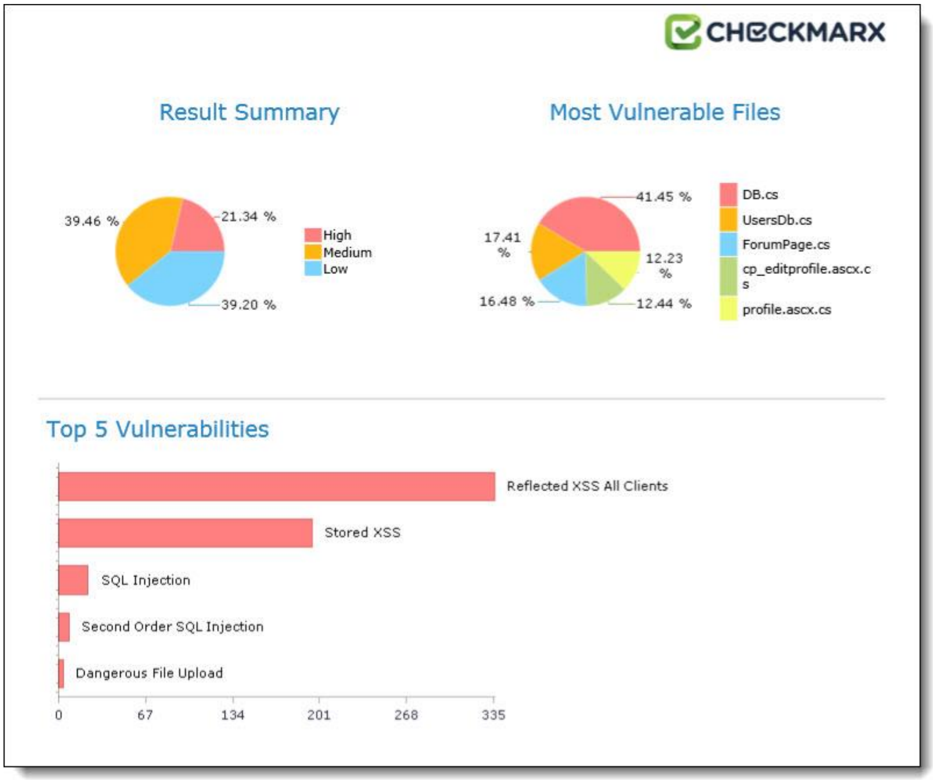
Results Limit

Results limit per query was set to 50

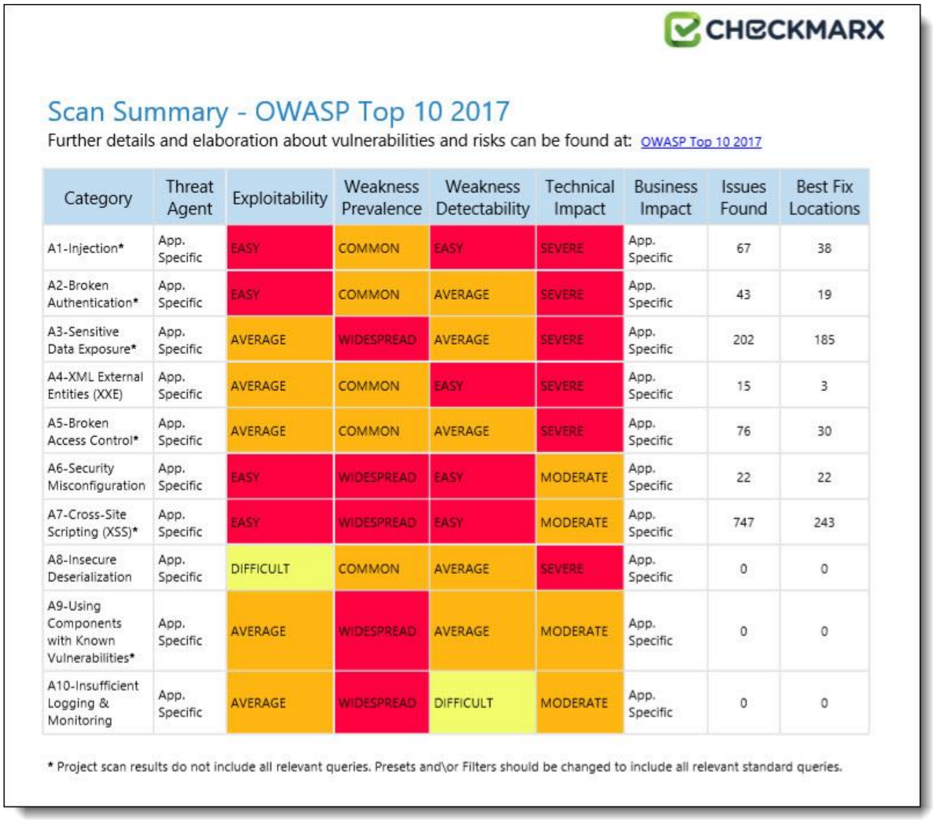
Selected Queries

Selected queries are listed in Result Summary

Parameters that were selected to be displayed will appear in the report even if none of these parameters (for example, OWASP A-6 category) were detected in the scan, in which case they will appear with the count "0".



The OWASP (2017, 2013 & Mobile 2016), PCI, FISMA and NIST summary sections in the scan report include a column named Best Fix Locations, which indicates the number of locations in the flow map that have been found as the best locations to fix the issues that belong to the selected category (for example, A1-Injection).



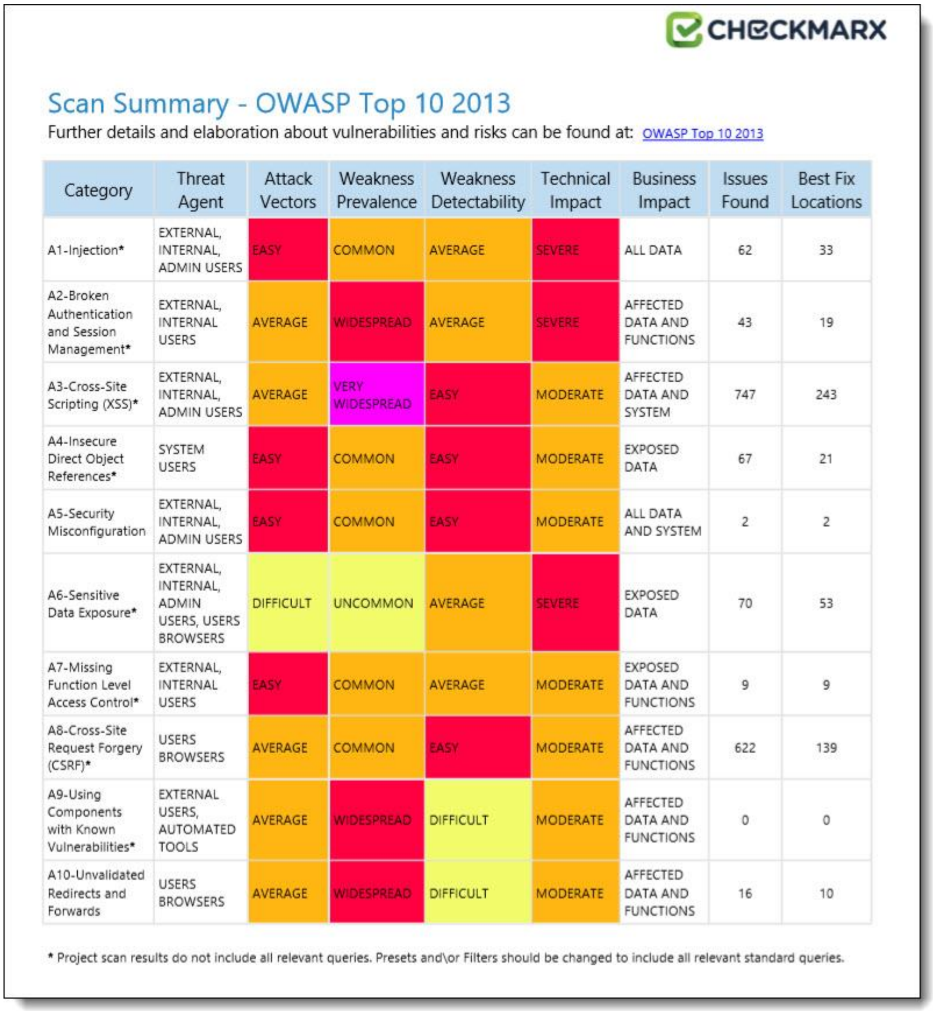
CHECKMARX

Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection*	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	67	38
A2-Broken Authentication*	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	43	19
A3-Sensitive Data Exposure*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	202	185
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	15	3
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	76	30
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	22	22
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	747	243
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

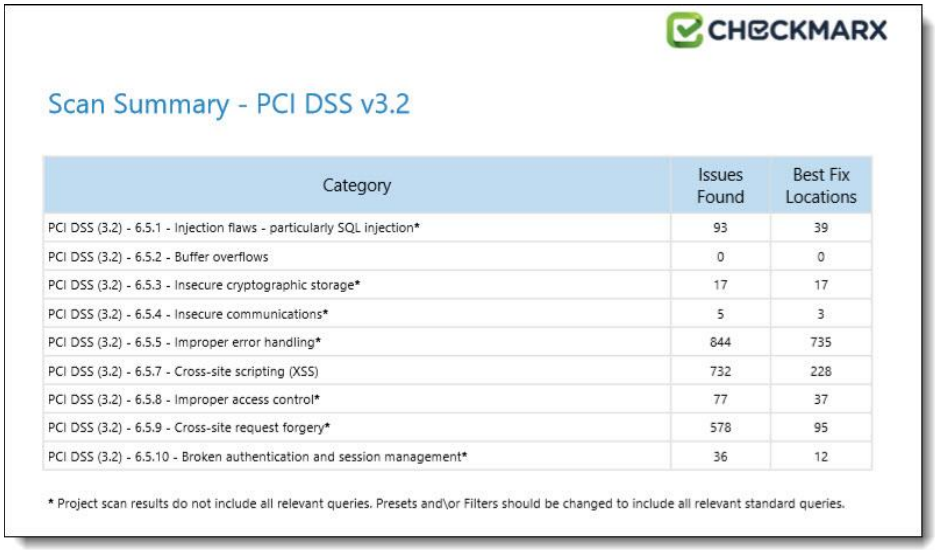


Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection*	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	62	33
A2-Broken Authentication and Session Management*	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	43	19
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	747	243
A4-Insecure Direct Object References*	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	67	21
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	2	2
A6-Sensitive Data Exposure*	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	70	53
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	9	9
A8-Cross-Site Request Forgery (CSRF)*	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	622	139
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	16	10

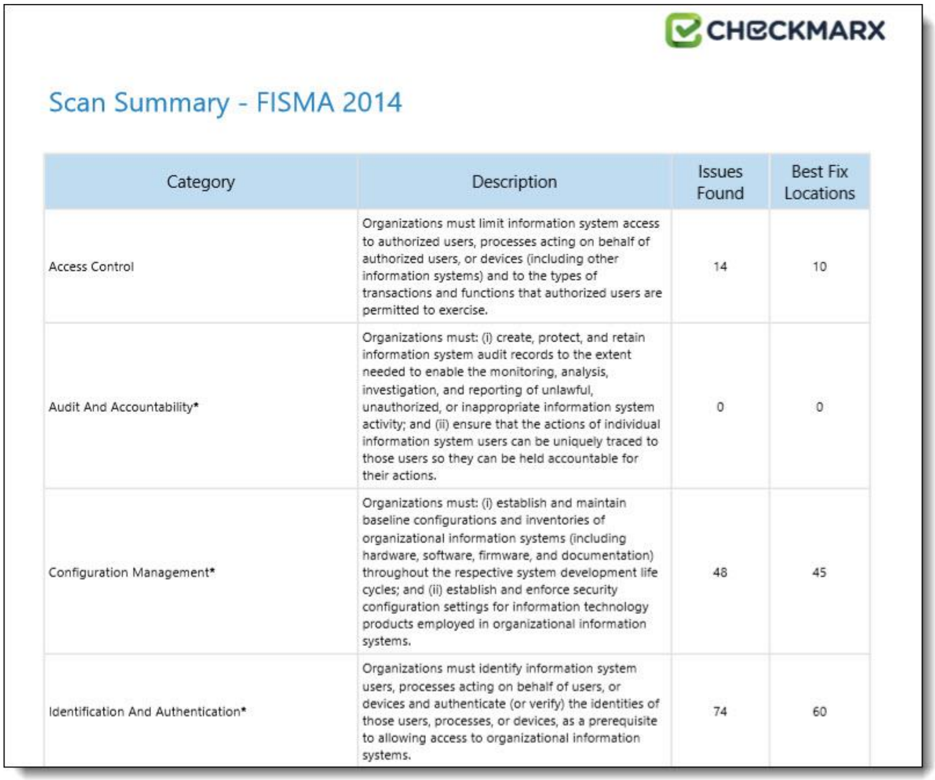
* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.



Scan Summary - PCI DSS v3.2

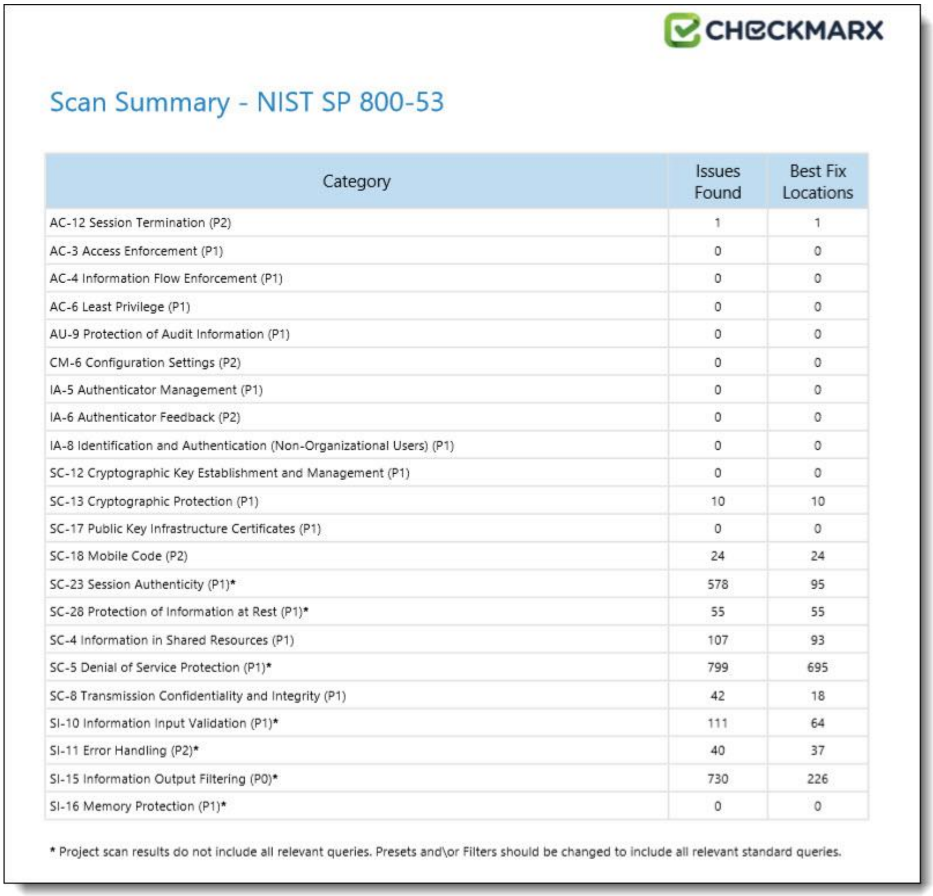
Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection*	93	39
PCI DSS (3.2) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage*	17	17
PCI DSS (3.2) - 6.5.4 - Insecure communications*	5	3
PCI DSS (3.2) - 6.5.5 - Improper error handling*	844	735
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	732	228
PCI DSS (3.2) - 6.5.8 - Improper access control*	77	37
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery*	578	95
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management*	36	12

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.



Scan Summary - FISMA 2014

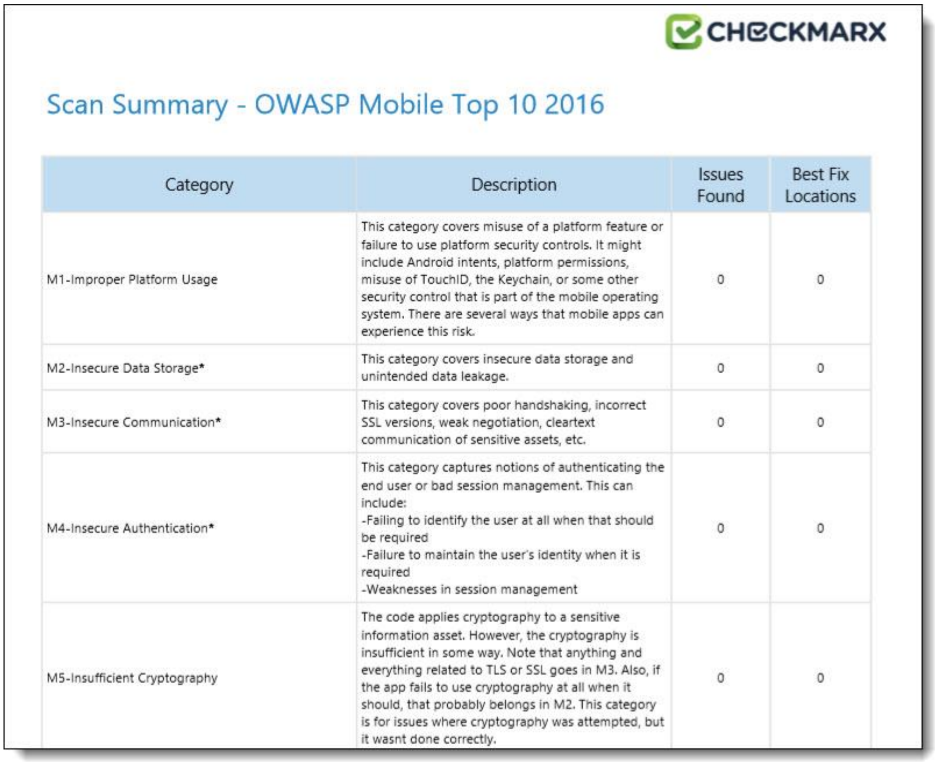
Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	14	10
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management*	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	48	45
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	74	60



Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	1	1
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	10	10
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	24	24
SC-23 Session Authenticity (P1)*	578	95
SC-28 Protection of Information at Rest (P1)*	55	55
SC-4 Information in Shared Resources (P1)	107	93
SC-5 Denial of Service Protection (P1)*	799	695
SC-8 Transmission Confidentiality and Integrity (P1)	42	18
SI-10 Information Input Validation (P1)*	111	64
SI-11 Error Handling (P2)*	40	37
SI-15 Information Output Filtering (P0)*	730	226
SI-16 Memory Protection (P1)*	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.



Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication*	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication*	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0

The Best Fixed Location is an absolute number that cannot be filtered and always displays all of the values. As a result, it is quite probable that while in effect the number of vulnerabilities far exceeds the number of best fix locations for a specified category (for example, 8000 and 600 respectively), the filtered report may display 350 issues and 300 best fix locations.

.CSV Report Results

The following is a basic description of the fields provided in the .csv report result, which is generated by the create report feature if the selected format is .csv:

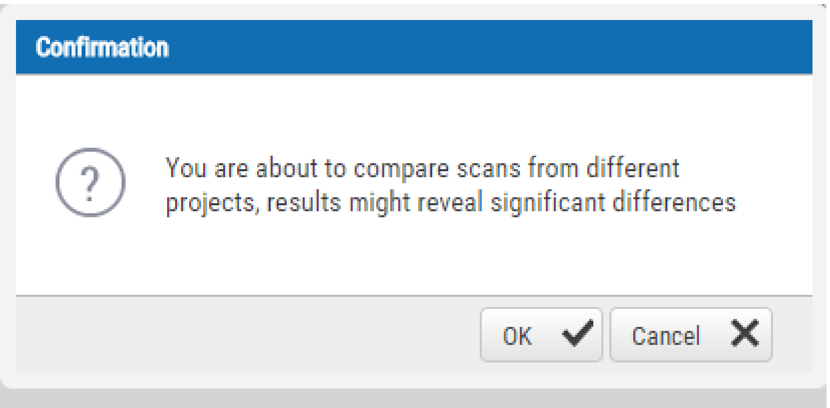
- **SrcFileName** – file name of the first node of the result
- **Line** – line of the first node of the result
- **Column** – column of the first node of the result
- **NodeId** – internal id to be able to identify the query in the first node
- **Name** – text of the first node of the result
- **DestFileName** – file name of the last node of the result
- **DestLine** – line of the last node of the result
- **DestColumn** – column of the last node of the result
- **DestNodeId** – internal id to be able to identify the query in the last node
- **DestName** – text of the last node of the result

Comparing Scan Result Sets

You can now compare the results of two scans in separate projects. CxSAST provides a summary of differences, and an interactive interface similar to the interface for results of single scan.

To view a comparison, select two rows in the table and click **Compare Scans**.

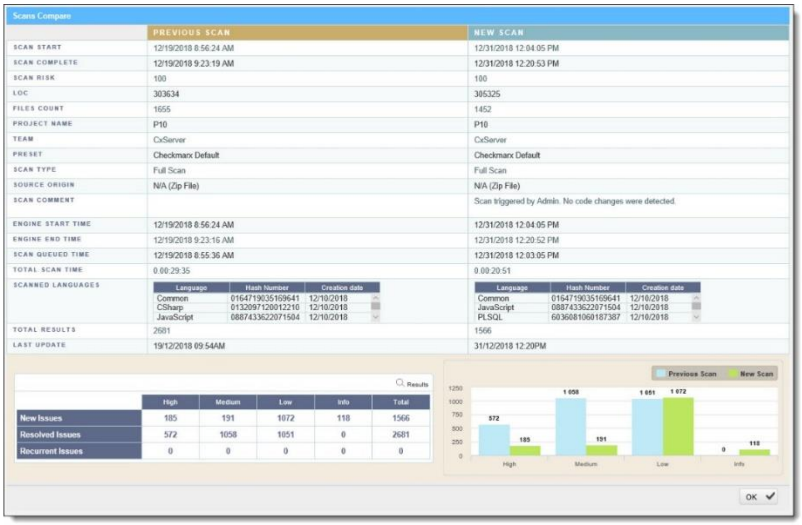
The following message is displayed when comparing scans from different projects: "You are about to compare scans from different projects, results might reveal significant differences"



Confirmation

You are about to compare scans from different projects, results might reveal significant differences

A comparison summary is displayed:



Scans Compare

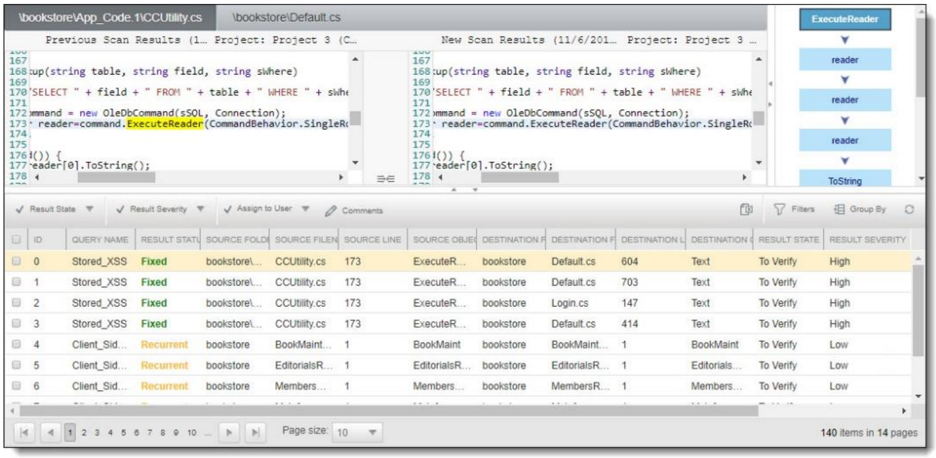
	PREVIOUS SCAN	NEW SCAN
SCAN START	12/19/2018 8:56:24 AM	12/31/2018 12:04:05 PM
SCAN COMPLETE	12/19/2018 9:23:19 AM	12/31/2018 12:20:53 PM
SCAN RISK	100	100
LOC	303634	305325
FILES COUNT	1655	1452
PROJECT NAME	P10	P10
TEAM	CxServer	CxServer
PRESET	Checkmarx Default	Checkmarx Default
SCAN TYPE	Full Scan	Full Scan
SOURCE ORIGIN	N/A (Zip File)	N/A (Zip File)
SCAN COMMENT		Scan triggered by Admin. No code changes were detected.
ENGINE START TIME	12/19/2018 8:56:24 AM	12/31/2018 12:04:05 PM
ENGINE END TIME	12/19/2018 9:23:16 AM	12/31/2018 12:20:52 PM
SCAN QUEUED TIME	12/19/2018 8:55:36 AM	12/31/2018 12:03:05 PM
TOTAL SCAN TIME	0.00:29:35	0.00:20:51
SCANNED LANGUAGES	Language / Hash Number / Creation date Common 0164719035169641 12/10/2018 CSharp 0132097120012210 12/10/2018 JavaScript 0887433622071504 12/10/2018	Language / Hash Number / Creation date Common 0164719035169641 12/10/2018 JavaScript 0887433622071504 12/10/2018 PLSQL 6036081060187387 12/10/2018
TOTAL RESULTS	2681	1566
LAST UPDATE	19/12/2018 09:54AM	31/12/2018 12:20PM

	High	Medium	Low	Info	Total
New Issues	185	191	1072	118	1566
Resolved Issues	572	1058	1051	0	2681
Recurrent Issues	0	0	0	0	0

The comparison summary includes:

- The scan details table, showing the scan start and finish dates, risk levels, LOC (Lines of Code scanned), number of files, query set, source code origin, comments, code language details (including unique identifier and date of last change to the language queries), and total vulnerabilities found.
- The bottom-left table displays changes from the earlier scan to the newer one, in number of issues of each severity level:
  - **New Issues**: Issues that were found only in the newer scan
  - **Resolved Issues**: Issues that were found only in the older scan
  - **Recurring Issues**: Issues that were found in both scans
- The bottom-right chart graphically compares the number of found vulnerabilities in both scans, for each severity level.

To view a code comparison, click **Results**. A code comparison is displayed:



```
Previous Scan Results (1… Project: Project 3 (C…

tup(string table, string field, string sWhere)

'SELECT " + field + " FROM " + table + " WHERE " + sWhe

ommand = new OleDbCommand(sSQL, Connection);
· reader=command.ExecuteReader(CommandBehavior.SingleRo


l()) {
reader[0].ToString();
```

```
New Scan Results (11/6/201… Project: Project 3 …

tup(string table, string field, string sWhere)

'SELECT " + field + " FROM " + table + " WHERE " + sWhe

ommand = new OleDbCommand(sSQL, Connection);
· reader=command.ExecuteReader(CommandBehavior.SingleRo


l()) {
reader[0].ToString();
```

☐	ID	QUERY NAME	RESULT STATU	SOURCE FOLDI	SOURCE FILEN	SOURCE LINE	SOURCE OBJEC	DESTINATION F	DESTINATION F	DESTINATION L	DESTINATION (	RESULT STATE	RESULT SEVERITY
☐	0	Stored_XSS	Fixed	bookstore\...	CCUtility.cs	173	ExecuteR...	bookstore	Default.cs	604	Text	To Verify	High
☐	1	Stored_XSS	Fixed	bookstore\...	CCUtility.cs	173	ExecuteR...	bookstore	Default.cs	703	Text	To Verify	High
☐	2	Stored_XSS	Fixed	bookstore\...	CCUtility.cs	173	ExecuteR...	bookstore	Login.cs	147	Text	To Verify	High
☐	3	Stored_XSS	Fixed	bookstore\...	CCUtility.cs	173	ExecuteR...	bookstore	Default.cs	414	Text	To Verify	High
☐	4	Client_Sid...	Recurrent	bookstore	BookMaint...	1	BookMaint	bookstore	BookMaint...	1	BookMaint	To Verify	Low
☐	5	Client_Sid...	Recurrent	bookstore	EditorialsR...	1	EditorialsR...	bookstore	EditorialsR...	1	Editorials...	To Verify	Low
☐	6	Client_Sid...	Recurrent	bookstore	Members...	1	Members...	bookstore	MembersR...	1	Members...	To Verify	Low

1 2 3 4 5 6 7 8 9 10 ... Page size: 10

140 items in 14 pages

Dashboard Analysis

For Dashboard Data analysis, refer to **Getting to Know the System Dashboard** at the beginning of this user guide.

System Management

Authentication Settings

From v9.0.0 and up, for LDAP and SAML management, refer to Access Control - Settings Tab (v2.0 and up).

LDAP Management

LDAP (Lightweight Directory Access Protocol) is an Internet protocol that web applications can use to look up information about those users and groups from the LDAP server. You can connect the CxSAST application to an LDAP directory for authentication, user and group management. CxSAST provides built-in connectors for the most popular LDAP directory servers; Active Directory, OpenLDAP and Custom LDAP Server. Connecting to an LDAP directory server is useful if user groups are stored in a corporate directory. Synchronization with LDAP allows the automatic creation, update and deletion of users and groups in CxSAST according to any changes being made in the LDAP directory.

For more information about configuring LDAP server settings for this version, refer to **Configuring LDAP Server Settings**.

SAML Management

Security Assertion Markup Language (SAML) is an XML-based format for exchanging authentication and authorization data between an identity provider and a service provider. Checkmarx's Static Analysis Security Solution (CxSAST) has just become SAML 2.0 aware and can now be configured to act as a SAML 2.0 Service Provider. SAML supports the user lifecycle by retrieving users from the Identity Provider (IdP) and defining them in CxSAST. This allows for more centralized and enhanced user management.

For more information about configuring SAML management settings for this version, please refer to **Configuring SAML Settings** and **Single sign-on with OKTA** and **SAML 2.0**.

Application Settings

From v9.0.0 and up, for SMTP and Domain Management settings, refer to **Access Control Settings**.

General Settings

The General screen enables you to set the paths, folders, web server address, and language as well as other application specific settings and SMTP.

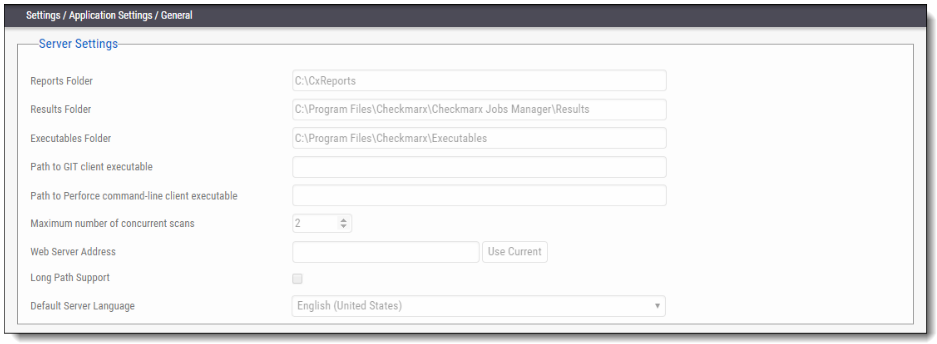
➢ **To open general settings:**

- Select **Settings** > **Application Settings** > **General**.

  The **General Settings** window is displayed.

Server Settings

In the Server settings panel, you can set folder locations, maximum number of scans, default settings and automatic sign in.



Settings / Application Settings / General

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	
Path to Perforce command-line client executable	
Maximum number of concurrent scans	2
Web Server Address	Use Current
Long Path Support	□
Default Server Language	English (United States)

- Click **Edit**.

  The setting fields are enabled.

The panel includes the following settings:

  - **Reports Folder** - Set the reports folder to save reports in (e.g. C:\CxReports)
  - **Results Folder** - Set the results folder to save results in (e.g. C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results)
  - **Executables Folder** - Set the executables folder to save executables in (e.g. C:\Program Files\Checkmarx\Executables)
  - **Path to GIT client executable** - Set the GIT client executable path (e.g. C:\Program Files\git\bin\git.exe).

The validation of 'git.exe' and 'p4.exe' is no longer mandatory in CxSAST when defining the 'Path to GIT client executable' and the 'Path to Perforce command-line client executable' parameters.

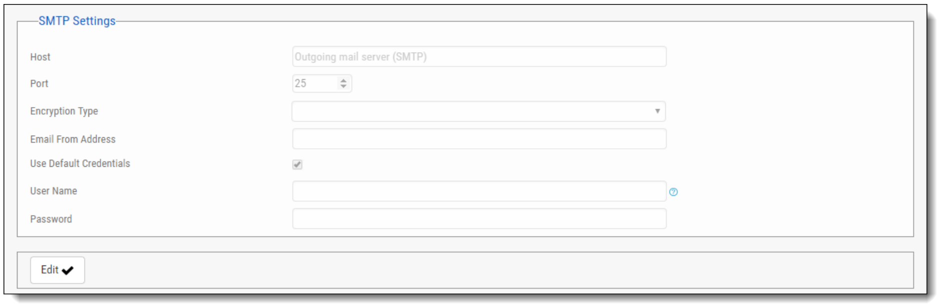
- **Path to P4 command line client executable** - Set the Perforce client executable path (e.g. C:\Program Files\Perforce\p4.exe)

If you haven't already done so, download the P4 command line executable (HELIX P4: COMMAND-LINE) from: https://www.perforce.com/downloads/helix, run the .exe file making sure the installed files are placed into a directory that CxSAST can access (i.e. C:\Program Files\Perforce)". Use this same directory to fill the Path to P4 command line client executable parameter field.

- **Maximum number of concurrent scans** - Set the maximum number of concurrent scans a CxManager can run. This cannot exceed the licensed number of concurrent scans. Reducing the number of concurrent scans below the licensed amount can help to prevent the CxManager out of resources. The default is 2. CxScansManager service must be restarted before any changes to this setting will go into effect.
- **Time remaining until task completion (min)** - Set the time remaining until task completion (timer).
- **Web Server Address** - Set the web server address in order to access links in generated report from outside the organization.
- **Long Path Support** - Enables long path support for the CxSAST application. Enabling long path support is required on all CxEngines and all CxManagers. Without long path support the path of source file to be scanned is limited to 260 characters.
- **Default Server Language** - Set the default server language.
- **Allow Auto Sign In** - Enable/Disable auto sign in.

SMTP Settings

The SMTP settings panel enables you to set the host settings and default credentials of your SMTP.



SMTP Settings

Host: Outgoing mail server (SMTP)

Port: 25

Encryption Type:

Email From Address:

Use Default Credentials: ☑

User Name:

Password:

- Click **Edit**.

  The setting fields are enabled.

  This panel includes the following settings:

  - **Host** - Type in the host domain
  - **Port** - Select a port number
  - **Encryption Type** - Select the encryption type
  - **Email from Address** - Notification by E-mail address
  - **Use Default Credentials** - Enable/disable default credentials. If enabled the default credentials of the host machine are used
  - **User Name** - Type in the user name
  - **Password** - Type in the password

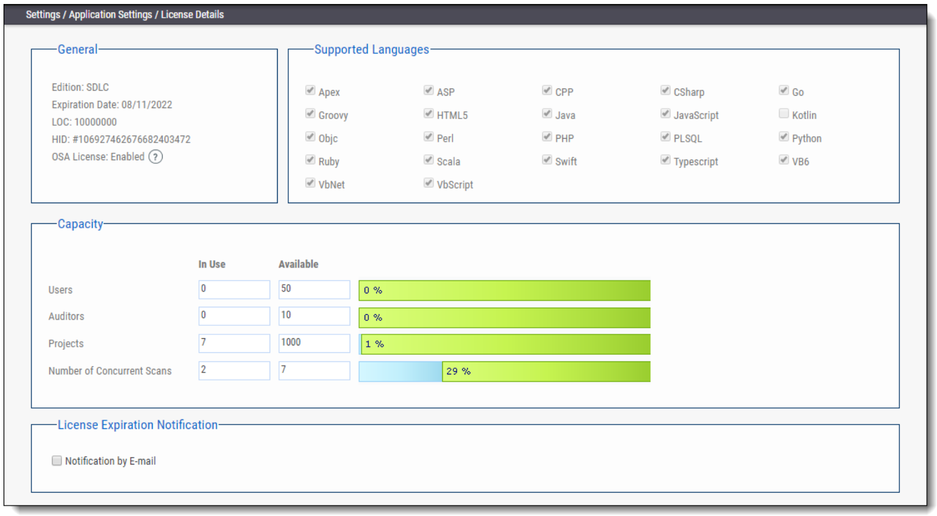
CxOSA Settings

For more information about CxOSA Settings and Open Source Analysis (CxOSA) in general, refer to **CxOSA Settings** in the **Checkmarx CxOSA Documentation**.

License Details

➢ **To open license details:**

- Select **Settings** > **Application Settings** > **License Details**. The **License Details** window is displayed.



Settings / Application Settings / License Details

General

Edition: SDLC
Expiration Date: 08/11/2022
LOC: 10000000
HID: #1069274626766824O3472
OSA License: Enabled ?

Supported Languages

☑ Apex	☑ ASP	☑ CPP	☑ CSharp	☑ Go
☑ Groovy	☑ HTML5	☑ Java	☑ JavaScript	□ Kotlin
☑ Objc	☑ Perl	☑ PHP	☑ PLSQL	☑ Python
☑ Ruby	☑ Scala	☑ Swift	☑ Typescript	☑ VB6
☑ VbNet	☑ VbScript			

Capacity

	In Use	Available	
Users	0	50	0 %
Auditors	0	10	0 %
Projects	7	1000	1 %
Number of Concurrent Scans	2	7	29 %

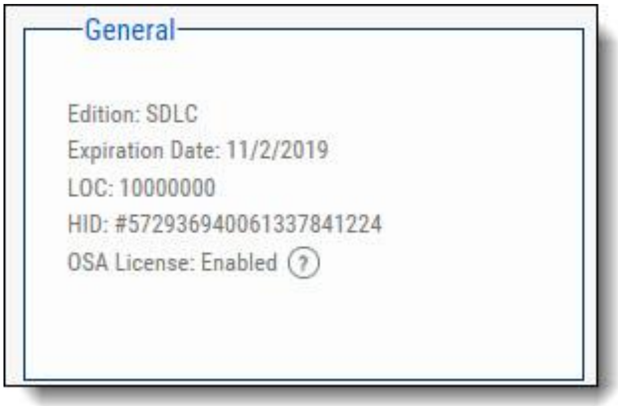
License Expiration Notification

□ Notification by E-mail

The License Details screen is divided into the following windows:

General

The **General** panel provides general license information.



General

Edition: SDLC
Expiration Date: 11/2/2019
LOC: 10000000
HID: #572936940061337841224
OSA License: Enabled ?

It includes the following information:

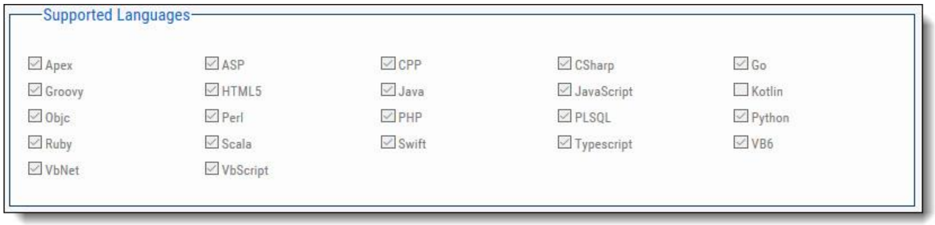
- **Edition -** CxSAST license edition (SDLC or Security Gate). To learn more about the different editions please refer to License Editions Overview.
- **Expiration Date** - Lcense expiry date
- **LOC** - The number of lines of code the license was bought for
- **HID** - Hardware identification number

- **CxOSA License -** Open Source Analysis license status (Enabled, Disabled or Conditional with expiration date for Conditional version). For more information about CxOSA License and Open Source Analysis (CxOSA) in general, see CxOSA License Details in the Checkmarx CxOSA Documentation.

To request a new license, if you have not yet obtained a permanent license, copy your Hardware ID, which you will need in order to obtain a license from Checkmarx. Or, you can later obtain your hardware ID by using the shortcut in the Windows / Start menu Checkmarx folder.

Supported Languages

The Supported Languages panel includes the supported languages used in default queries.

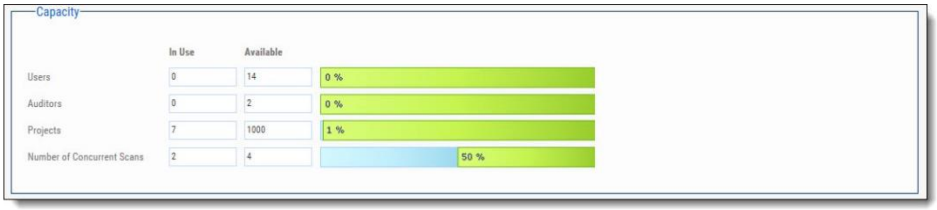


Supported Languages

☑ Apex	☑ ASP	☑ CPP	☑ CSharp	☑ Go
☑ Groovy	☑ HTML5	☑ Java	☑ JavaScript	□ Kotlin
☑ Objc	☑ Perl	☑ PHP	☑ PLSQL	☑ Python
☑ Ruby	☑ Scala	☑ Swift	☑ Typescript	☑ VB6
☑ VbNet	☑ VbScript			

Capacity

The Capacity panel provides information about the number of users (combined roles), projects and engines available and in use in the system according to the current license.



Capacity

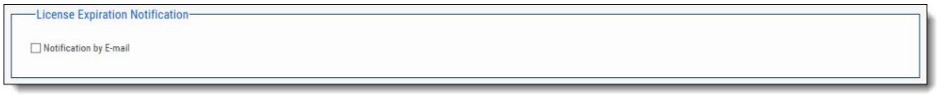
	In Use	Available	
Users	0	14	0 %
Auditors	0	2	0 %
Projects	7	1000	1 %
Number of Concurrent Scans	2	4	50 %

The Capacity panel includes the following information:

- **Users** - Number of users available in the system (i.e. Server Managers, Service Provider Managers, Company Managers, Scanners and Reviewers)
- **Auditors** - Number of users available in the system that have auditing permissions and can run CxAudit (i.e Auditors Users)
- **Projects** - Number of projects available in the system
- **Number of Concurrent Scans** - Number of concurrent scans available in the system.

License Expiration Notification

The License Expiration Notification panel provides notification behavior settings for when your CxSAST license is about to expire.


License Expiration Notification

☐ Notification by E-mail

The License Expiration panel includes the Notification by Email option:

- If checked, a notification email is automatically sent to the CxSAST Administrator User on a weekly basis, starting 90 days (defined in the database) before the actual license is set to expire.

> ⓘ The Notification by E-mail address is defined under the E-mail Notifications parameter in **Server SMTP Setting.**

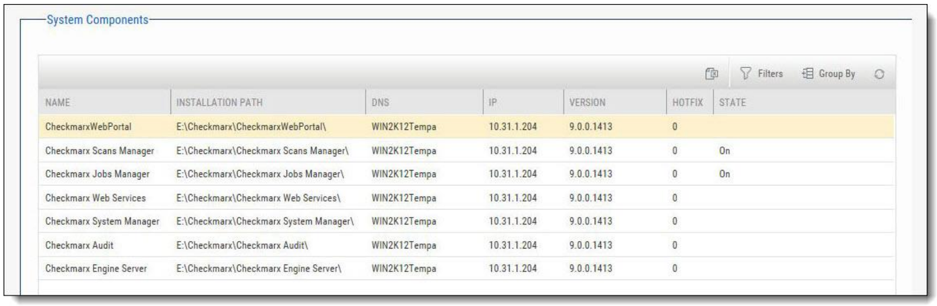
Installation Information

The Installation Information screen provides a list of all the Cx components installed, the Installation Path, Version (with build), DNS, IP, Hotfix, and State.

➢ **To open installation information:**

- Select **Settings** > **Application Settings** > **Installation Information**.

  The **Installation Information** window is displayed.


System Components

NAME	INSTALLATION PATH	DNS	IP	VERSION	HOTFIX	STATE
CheckmarxWebPortal	E:\Checkmarx\CheckmarxWebPortal\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	
Checkmarx Scans Manager	E:\Checkmarx\Checkmarx Scans Manager\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	On
Checkmarx Jobs Manager	E:\Checkmarx\Checkmarx Jobs Manager\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	On
Checkmarx Web Services	E:\Checkmarx\Checkmarx Web Services\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	
Checkmarx System Manager	E:\Checkmarx\Checkmarx System Manager\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	
Checkmarx Audit	E:\Checkmarx\Checkmarx Audit\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	
Checkmarx Engine Server	E:\Checkmarx\Checkmarx Engine Server\	WIN2K12Tempa	10.31.1.204	9.0.0.1413	0	

Content Pack version

The latest queries pack version is also listed in cases where a Content Pack is installed. For more information about the Content Pack for your version, see the relevant version release notes section.

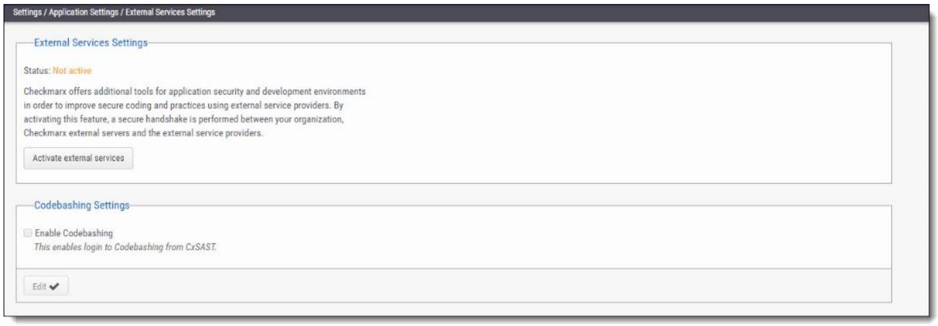
External Services Settings

CxSAST offers additional tools for application security and development environments in order to improve secure coding and practices using external service providers. By activating this feature, a secure handshake is performed between your organization, Checkmarx external servers and the external service providers.

➢ **To open external services settings:**

1. Select **Settings** > **Application Settings** > **External Services Settings**.

   The **External Services Settings** window is displayed.



Settings / Application Settings / External Services Settings

External Services Settings

Status: Not active

Checkmarx offers additional tools for application security and development environments in order to improve secure coding and practices using external service providers. By activating this feature, a secure handshake is performed between your organization, Checkmarx external servers and the external service providers.

Codebashing Settings

□ Enable Codebashing

This enables login to Codebashing from CxSAST.

2. Click the **Activate/Reactivate External Services** button to activate or reactivate (if deactivated) a secure communication path between your organization, CxSAST and the service provider.

> ⓘ In cases where the automatic activation process doesn't perform as expected, you may need to request a manual activation. Please contact Checkmarx support.

3. Click **Edit**. The **Codebashing Settings** fields are enabled.
4. **Enable Codebashing** - If selected, enables **anonymous data collection** in order to provide user analytics. The second checkbox, enables **non-anonymous data collection** in order to provide user analytics. This option, if selected, sends user details (email) to Codebashing for Analytics View.

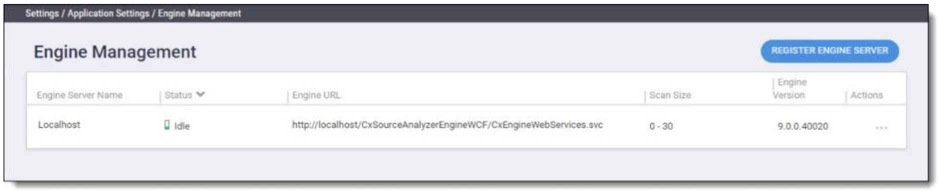
Engine Management

Engine Server Management enables an interface for viewing real-time engine server status information that includes the number of engine servers in the system (active and offline), status of each engine server (scanning, idle, blocked, etc.) and location (URL) and scan size of each engine server. Direct action options (single) include register, edit, unregister and block/unblock engine servers.

➢ **To open engine management:**

- Select **Settings** > **Application Settings** > **Engine Management.**

  The **Engine Management** window is displayed.



Engine Server Name	Status	Engine URL	Scan Size	Engine Version	Actions
Localhost	Idle	http://localhost/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 30	9.0.0.40020	...

The Engine Server Management screen automatically refreshes itself every 20 seconds.

Engine Sever Management provides real-time information about the status of each engine server in the system. Each engine server is listed according to its status. The engine server list includes the following information:

Field	Description
Engine Sever Name	Name of the engine server
Status	Status of the engine server: Scanning Idle (engine server waiting to receive scan requests Blocked (engine server unable to receive scan requests) Offline (engine server unable to communicate to system, e.g. machine down, service stopped, connectivity issues, etc.) Scanning and Blocked (engine server running scans already requested from the system, before the engine server was blocked)
Engine URL	URL of the engine server
Scan Size	Engine server scan size
Engine Version	Engine version number
Actions	Single actions: edit, unregister and block/unblock engine server

Performing Engine Sever Management Actions

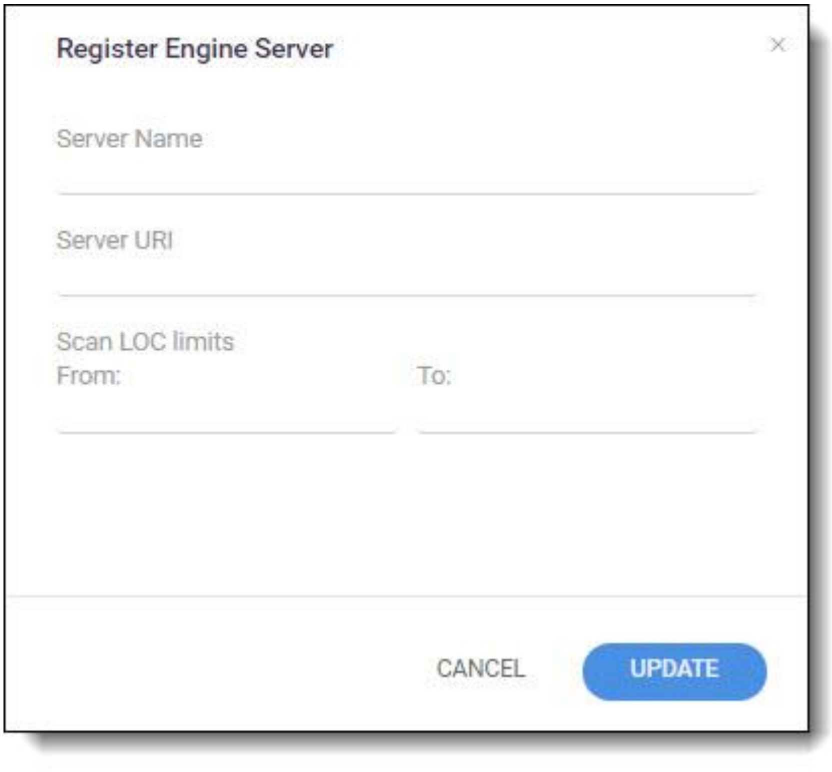
Once the Engine Management screen is displayed you can perform single actions.

Register a New Engine Server

➢ **To register a new engine server:**

1. Click the Register Engine Server button.

   The Register Engine Server dialog is displayed.



2. Define the following attributes:

Parameter	Description
Server Name	Enter the name of the engine server. Each engine server should have a unique name.
Server URI	Enter the URI address of the engine server. URI address must start with the http(s):// prefix.
Scan LOC Limit	Enter the scan LOC (lines of code) limit. The 'From' and 'To' definition must be a whole number between 0 - 999,999,999.

3. Click **Update** to save the changes.

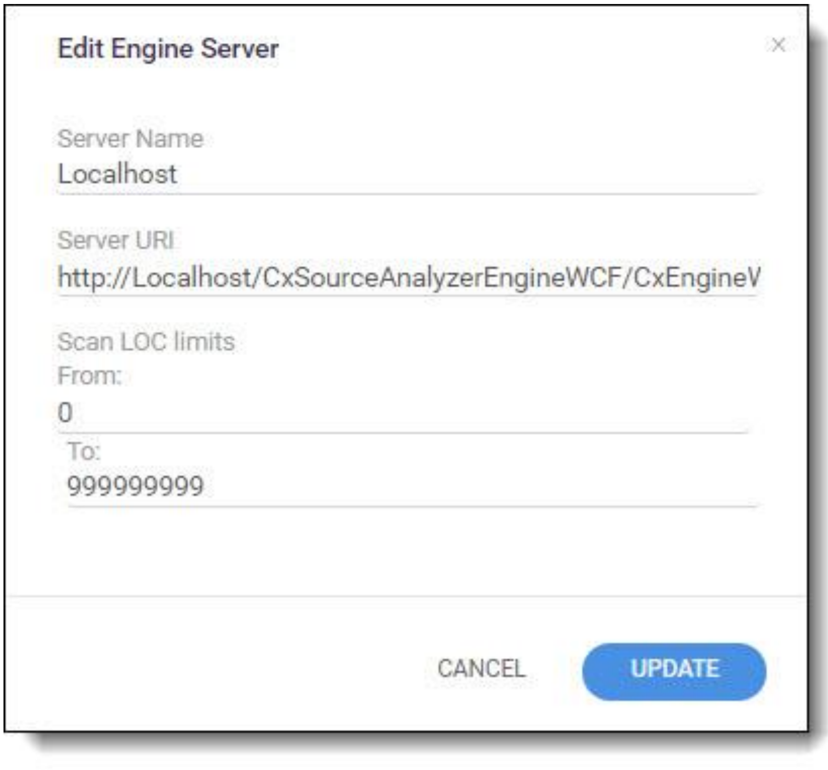
   The new engine server is added to the engine List.

Edit an Existing Engine Servers Attributes

➢ **To edit an existing engine servers attributes:**

1. Click the Actions ⋯ icon in line with the engine server that you would like to edit and select **Edit**.

   The Edit Engine Server dialog is displayed.



Edit Engine Server

Server Name
Localhost

Server URI
http://Localhost/CxSourceAnalyzerEngineWCF/CxEngineV

Scan LOC limits
From:
0
To:
999999999

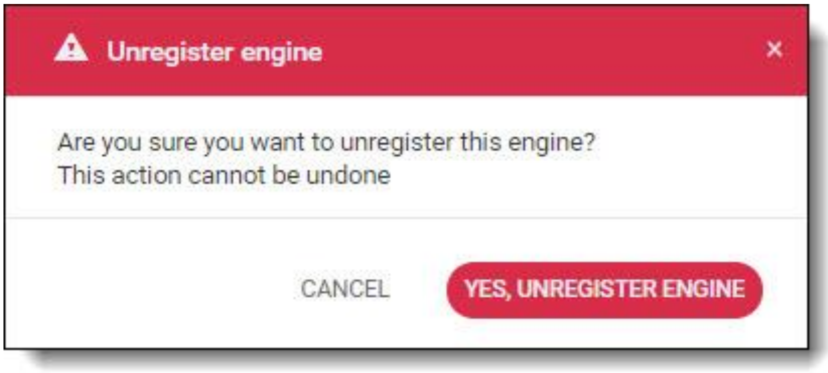
2. Change the engine server's attributes accordingly (see **Register a New Engine Server** for more information about the available attributes).
3. Click **Update** to save the changes.

Unregister an Engine Server

➢ **To unregister an existing engine server:**

1. Click the Actions ⋯ icon in line with the engine server that you would like to unregister and select Unregister.

   The Unregister Engine Server dialog is displayed.



Unregister engine

Are you sure you want to unregister this engine?
This action cannot be undone

2. Click **Unregister Engine** to continue or click **Cancel**.

   The engine server is removed from the engine list.

> ⓘ You cannot unregister an engine server that is currently running a scan.

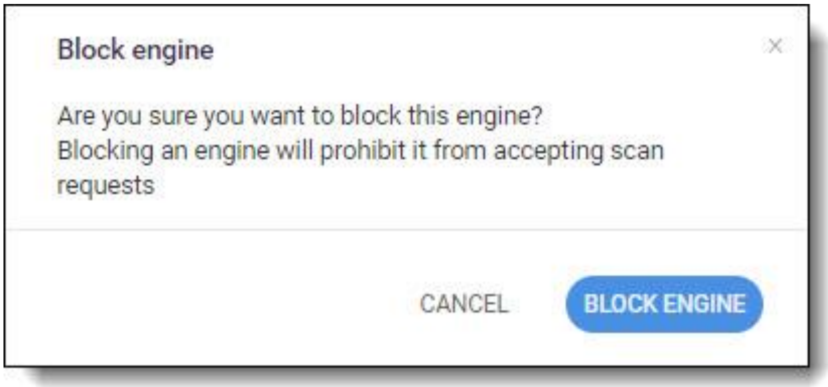
Block/Unblock an Engine Server

You can block an engine server in the system. Blocking prevents the engine server from accepting any new scan requests from the system. Scans already requested from the system, before the engine server was blocked, will continue uninterrupted until completion.

➢ **To block an engine server in the system:**

1. Click the Actions ⋯ icon in line with the engine server that you would like to block and select Block.

   The Block Engine Server dialog is displayed.



Block engine

Are you sure you want to block this engine?
Blocking an engine will prohibit it from accepting scan requests

2. Click **Block Engine** to continue or click **Cancel**. The status of the engine server is changed to **Blocked** in the engine list.

To unblock an engine server in the system, perform the same procedures, as above, and select Unblock until completed. Once the engine server is unblocked it can start to accept new scan

Data Retention Management

In order to properly manage data storage consumption, CxSAST allows for the manual purging of old scan data. An administrator can define the desired storage policy by date range or by defining a minimal number of scans to retain overriding the date range.

> ⓘ Scanned data is purged from the file system as well as the database. Therefore, once deleted, it cannot be reversed. See **Data Retention Purged Data**, below

This process can be automated by using the CxSAST (REST) API for Data Retention.

Data retention settings apply globally to all projects within the system. This global configuration can be overridden for a specific project, either during the project creation or by editing the project's setting through the Data Retention tab (see Creating and Configuring a CxSAST Project and Viewing Project Details.

Specific scans may be marked as “Locked” to avoid automated purging of important scan data.

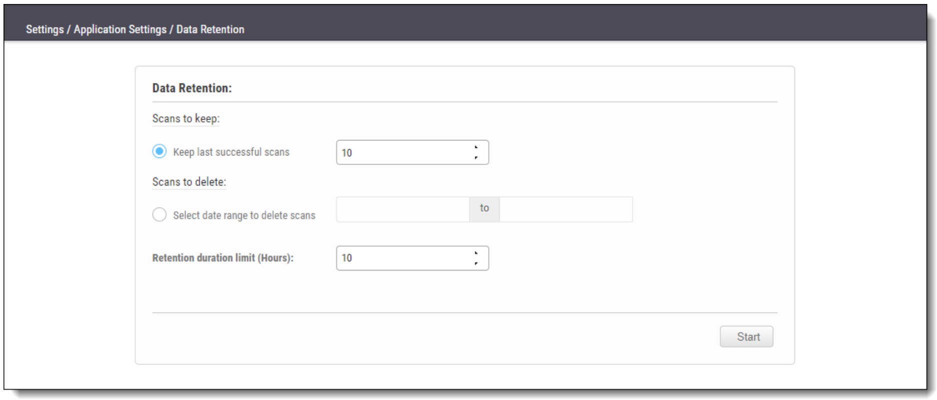
Locked scans cannot be deleted and will be skipped in the data retention process. If you would like to delete all scans within the range defined for deletion, it is highly important to ensure that no locked scans are included within this range. If the range does include locked scans, unlock the scans before executing the Data Retention command (see **Unlocking Scans**).

Defining Data Retention Settings

➢ **To define the data retention settings:**

- Select **Settings** > **Application Settings** > **Data Retention**.

  The Data Retention window is displayed.



Data Retention:

Scans to keep:

● Keep last successful scans: 10

Scans to delete:

○ Select date range to delete scans: to

Retention duration limit (Hours): 10

The Data Retention window includes the following settings:

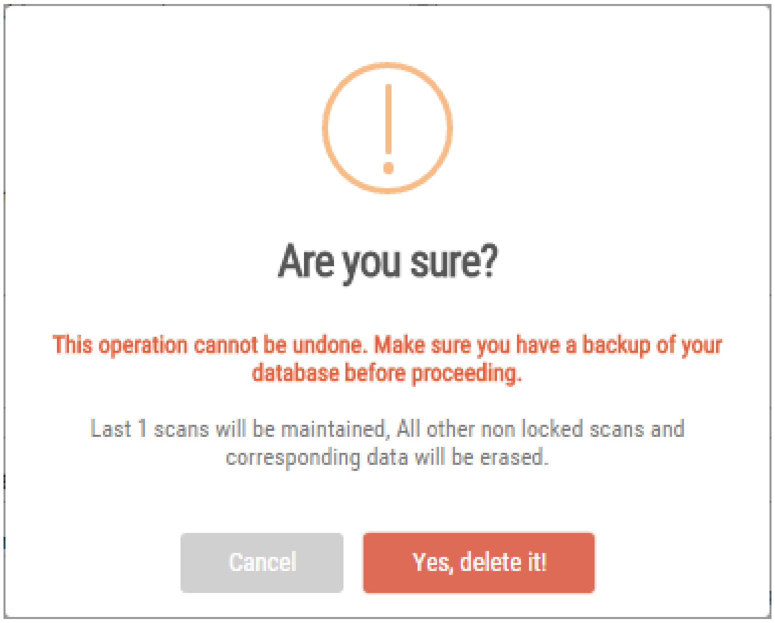
Scans to keep:

- **Keep last successful scans** - Set the requested number of scans to be kept. This setting leaves only the specified number of recent successful last scans and deletes all other scans. For example, if the value is set to 10, it will keep the last 10 successful scans for each project.

Scans to delete:

- **Select date range to delete scans** - Enter a start and an end date. This setting deletes all scans within a predefined time range.

- **Retention duration limit (hours)** - Set a limit to the amount of time the operation should take. If set to 10, then after 10 hours the operation automatically stops, regardless of whether the operation is complete.
- Click **Start**.The following message appears:

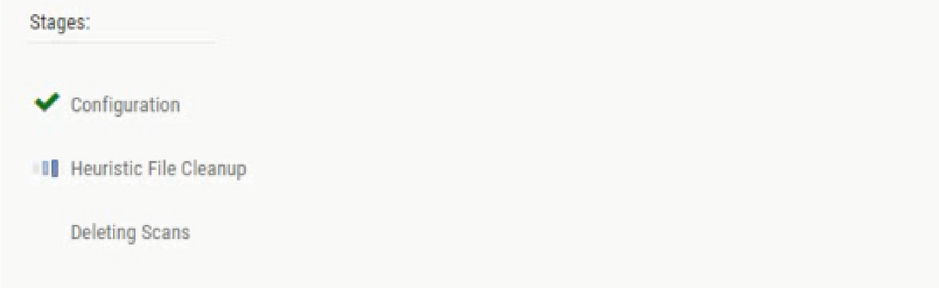


Are you sure?

This operation cannot be undone. Make sure you have a backup of your database before proceeding.

Last 1 scans will be maintained, All other non locked scans and corresponding data will be erased.

- If you are unsure whether you have backed up your database, or if the range you defined for deletion includes locked scans, click **Cancel** to postpone the deletion.
- If you want to continue, click **Yes, delete it.** The following message is displayed "**Data retention is now in progress**" and the progress of the data retention process is represented in the Stages panel.



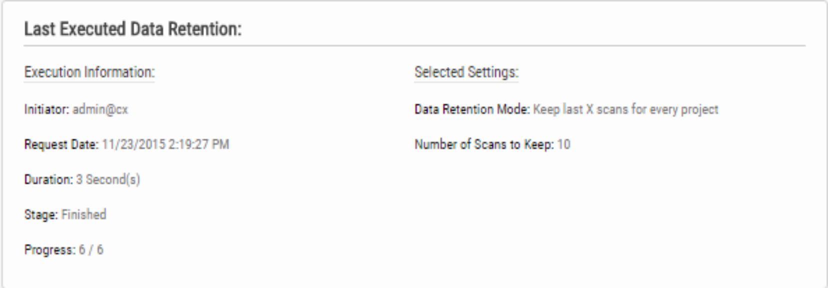
Stages:

✓ Configuration

Heuristic File Cleanup

Deleting Scans

Once the data retention process is complete, status information about last deletion is displayed in the **Last Executed Data Retention** panel.


Last Executed Data Retention:

Execution Information:

Initiator: admin@cx

Request Date: 11/23/2015 2:19:27 PM

Duration: 3 Second(s)

Stage: Finished

Progress: 6 / 6

Selected Settings:

Data Retention Mode: Keep last X scans for every project

Number of Scans to Keep: 10

Data Retention Purged Data

Scanned data is purged from the file system as well as the database, therefore, once deleted cannot be reversed. The following data is purged as part of the data retention:

Database Tables

Selected data from the following tables is purged as part of the data retention:

- All Scans
- TaskScans
- CancelledScans
- TaskScanEnvironment
- ScanReports
- FailedScans
- PathResults
- NodeResults

File System

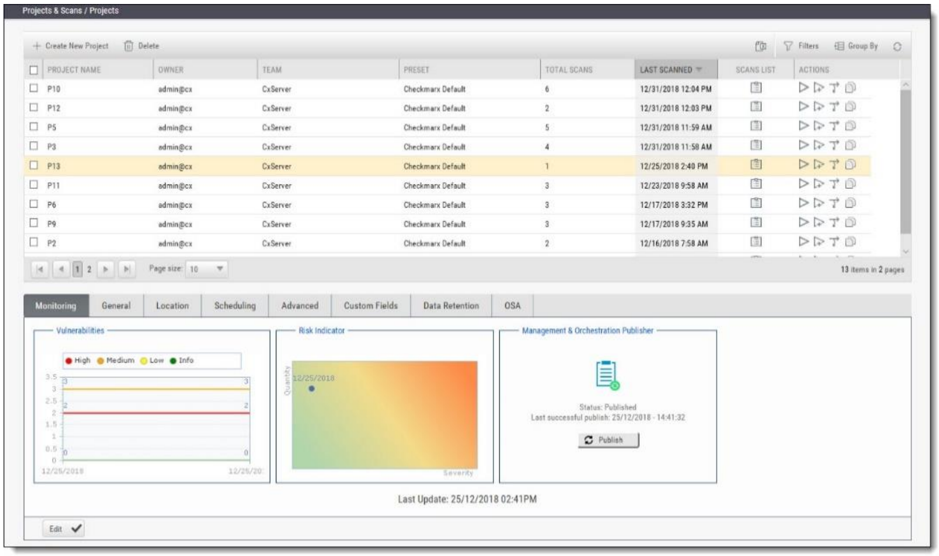
- CxSRC folder – This folder holds the extracted source files which are being scanned. Files and folders inside the CxSrc folder are deleted as part of data retention except for the following scenario:
  In case the exact same sources (ZIP, remote location..) are uploaded to the same existing scan, the extracted folder will be excluded from further data retention cleaning tasks.
- CxReports folder - This folder holds the following:
  - Reports requested by the customer and created in the CxSAST reports page. These reports are deleted as part of the data retention
  - Eclipse IDE reports created after each developer scan request. These reports are not deleted as part of the data retention.

Unlocking Scans (v9.0.0 and up)

One of the most common reasons for having no scans deleted is that one or more of the scans are locked. This can be modified by unlocking the scans.

➢ **To unlock the scans:**

1. Go to **Projects & Scans** > **Projects**.



☐	PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS
☐	P10	admin@cx	CxServer	Checkmarx Default	6	12/31/2018 12:04 PM		
☐	P12	admin@cx	CxServer	Checkmarx Default	2	12/31/2018 12:03 PM		
☐	P5	admin@cx	CxServer	Checkmarx Default	5	12/31/2018 11:59 AM		
☐	P3	admin@cx	CxServer	Checkmarx Default	4	12/31/2018 11:58 AM		
☐	P13	admin@cx	CxServer	Checkmarx Default	1	12/25/2018 2:40 PM		
☐	P11	admin@cx	CxServer	Checkmarx Default	3	12/23/2018 9:58 AM		
☐	P6	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 3:32 PM		
☐	P9	admin@cx	CxServer	Checkmarx Default	3	12/17/2018 9:35 AM		
☐	P2	admin@cx	CxServer	Checkmarx Default	2	12/16/2018 7:58 AM		

Status: Published
Last successful publish: 25/12/2018 - 14:41:32

Last Update: 25/12/2018 02:41PM

2. Select the requested project. If many projects exist, find the project by using the following steps:
3. Click **Filters** on the right.
4. Type one or more identifying criteria for the project, such as the project name, owner, and team.
5. Click **Enter**.
6. Go to the column **Scans List**.
7. Click the button **View project scans**.

   A list of all scans belonging to the selected project appears. If the list contains more than one page, use the directional arrows on the left to move to the next or previous page.

8. Go to the **Locked** column.
9. See if one or more of the scans is locked.
10. Use the **Unlock scan** button (🔓) to remove the lock.

Issue Tracking Settings

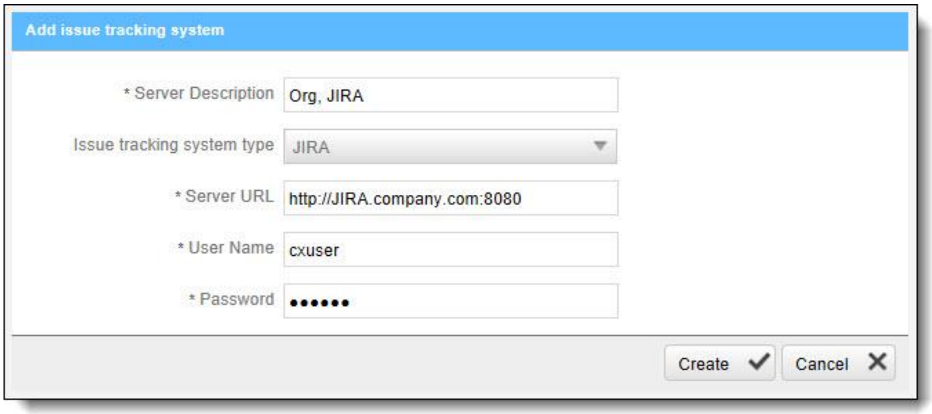
Issue tracking for CxSAST can be performed using JIRA integration. JIRA is a proprietary issue tracking product that allows bug tracking and agile project management.

To configure JIRA integration, CxSAST Manager permissions are required. To enable CxSAST scanners to configure JIRA integration, please contact Checkmarx support.

➢ **To configure JIRA integration:**

1. On the CxSAST server (on CxManager in a distributed deployment), open the following file for editing:

   C:\Program Files\Checkmarx\CheckmarxWebPortal\Web\web.config
2. Under the appSettings element, add:
   `<add key="EnableIssueTracking" value="true"></add>`
3. Log off the CxSAST Web Portal, if currently logged in.
4. Log in to the CxSAST web interface, go to **Settings** > **Application Settings** > **Issue Tracking Settings**, and click **Add Issue Tracking System**:
5. Provide the top-level URL of your JIRA server, including the protocol (**http** or **https**) and port number, and a user account with permissions for creating issues and for reading issue metadata, and click **Create**



* Server Description: Org, JIRA

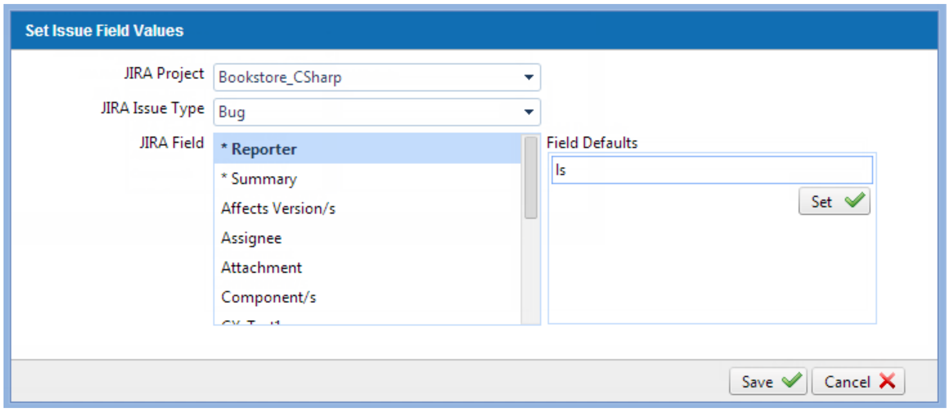
Issue tracking system type: JIRA

* Server URL: http://JIRA.company.com:8080

* User Name: cxuser

* Password: ●●●●●●

6. Create a CxSAST project, and in the Advanced Actions stage, under **Issue Tracking Settings**, select the JIRA server.
7. Click **Select**, and configure JIRA issue submissions:



8. Set the **JIRA Project** and **Issue Type**.
9. Configure default values for issue fields: Select each **JIRA Field**, select a **Field Default** and click **Set**. Make sure to configure values for all mandatory fields (marked with *).
10. Click **Save**.
11. In the CxSAST project, click **Finish**.

License Editions Overview

This document outlines the highlight of difference between the CxSAST license editions. For a detailed comparison please contact Checkmarx support.

	SDLC Edition	Security Gate Edition
CxPortal	:heavy_check_mark:	:heavy_check_mark:
Access Control	:heavy_check_mark:	:heavy_check_mark:
IDE Plugins	:heavy_check_mark:	:heavy_check_mark:
Source Code Repository (git, svn, TFS)	:heavy_check_mark:	:heavy_check_mark:
M&O	:heavy_check_mark:	:heavy_multiplication_x:
Build Servers	:heavy_check_mark:	:heavy_multiplication_x:
REST API / CLI	:heavy_check_mark:	:heavy_multiplication_x:
Management & Collaboration tools (Sonar, Github, etc.)	:heavy_check_mark:	:heavy_multiplication_x:
Ticketing systems (e.g Jira)	:heavy_check_mark:	:heavy_multiplication_x:

Custom Field Management

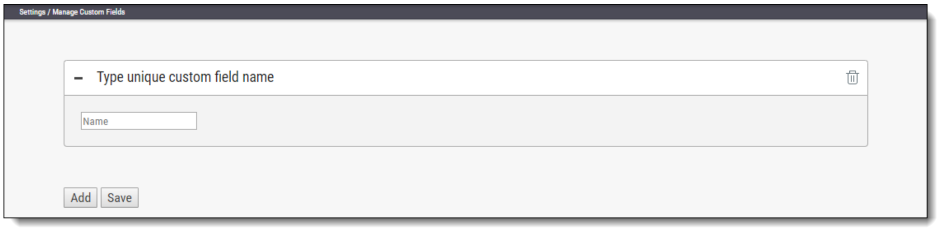
It is now possible to define project attributes (metadata) by using custom fields.

Implementing and consuming project attributes - using the new Custom Fields capability - is a 3 steps process:

1. Creating new custom fields
2. Filling up the custom fields per project
3. Consuming custom fields using the OData REST APIs.

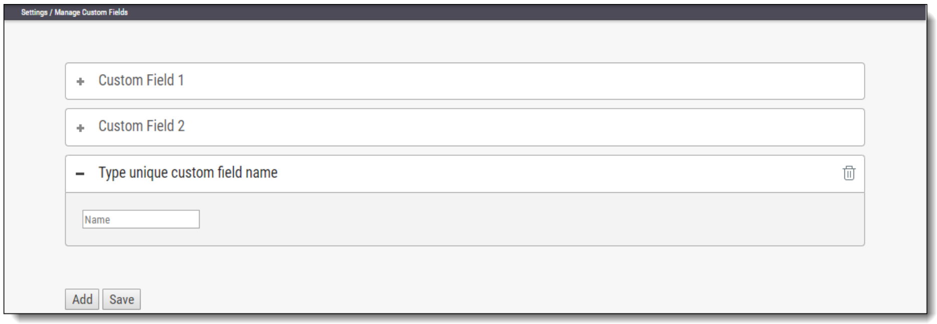
➢ **To define custom fields:**

1. Go to **Settings > Manage Custom Fields.**


Settings / Manage Custom Fields
–
Type unique custom field name
Name
Add
Save

2. Click **Add**.
3. Enter a unique custom field name in the designated field.
4. Click **Save**.

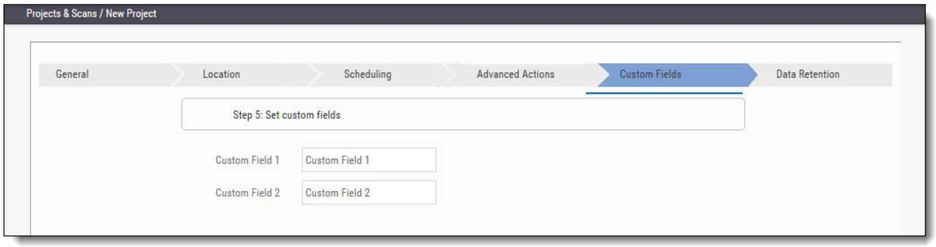
   Each newly added custom field (up to 10) is displayed on the list and can be edited or deleted.


Settings / Manage Custom Fields
+
Custom Field 1
+
Custom Field 2
–
Type unique custom field name
Name
Add
Save

5. To edit the custom field's name:
6. Click the "+" sign to the left of the field name.
7. Perform the requested change in the editable row that appears.
8. Click **Save.**

To delete a custom field row, click the respective delete icon 🗑 and then click "**Yes, delete it**" on the confirmation message.

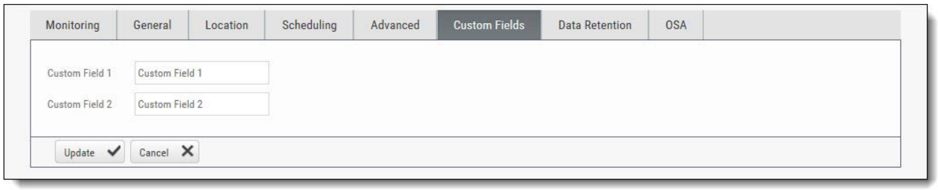
Custom field are available for fill-out in the project attributes screen, both when you create new project and later when you edit an existing project.



Step 5: Set custom fields

Custom Field 1: Custom Field 1

Custom Field 2: Custom Field 2



Custom Field 1: Custom Field 1

Custom Field 2: Custom Field 2

My Profile Settings

From v9.0.0 and up, My Profile settings are handled from the Access Control portal, and clicking the **My Profile** button on the CxSAST dashboard navigates you to that portal – from where all users can define personal user details on the General page, and Application users can change the login password on the Password page.

Scan Settings

This section outlines various available scan setting options.

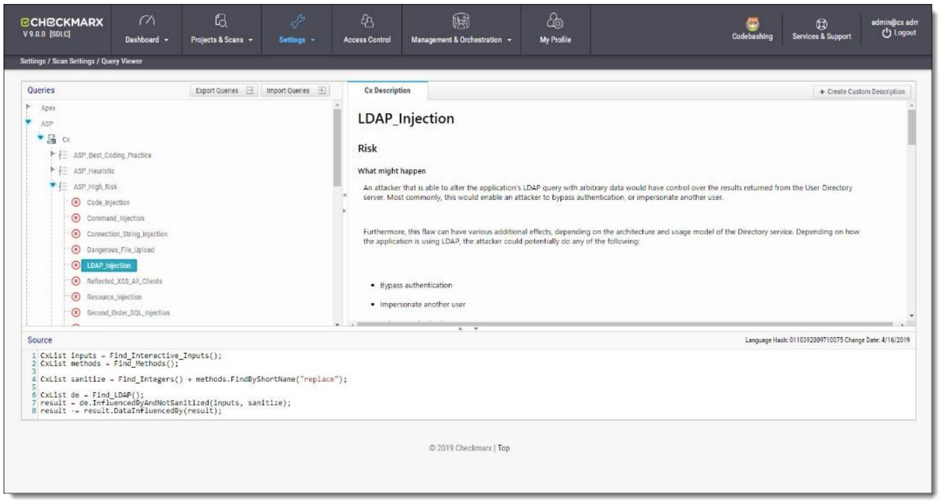
Query Viewer

The **Query Viewer** displays all default queries in CxSAST. A Query is a set of predefined source code used when scanning for vulnerabilities.

➢ **To open the Query Viewer:**

1. Go to **Settings** > **Scan Settings** > **Query Viewer.**

   The **Query Viewer** window is displayed.



LDAP_Injection

Risk

What might happen

An attacker that is able to alter the application's LDAP query with arbitrary data would have control over the results returned from the User Directory server. Most commonly, this would enable an attacker to bypass authentication, or impersonate another user.

Furthermore, this flaw can have various additional effects, depending on the architecture and usage model of the Directory service. Depending on how the application is using LDAP, the attacker could potentially do any of the following:

- Bypass authentication
- Impersonate another user

```
CxList inputs = Find_Interactive_Inputs();
CxList methods = Find_Methods();

CxList sanitize = Find_Integers() + methods.FindByShortName("replace");

CxList de = Find_LDAP();
result = de.InfluencedByAndNotSanitized(inputs, sanitize);
result -= result.DataInfluencedBy(result);
```

2. Select a **Query** in the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk.

   The source code for the query is displayed in the **Source** pane at the bottom of the window.

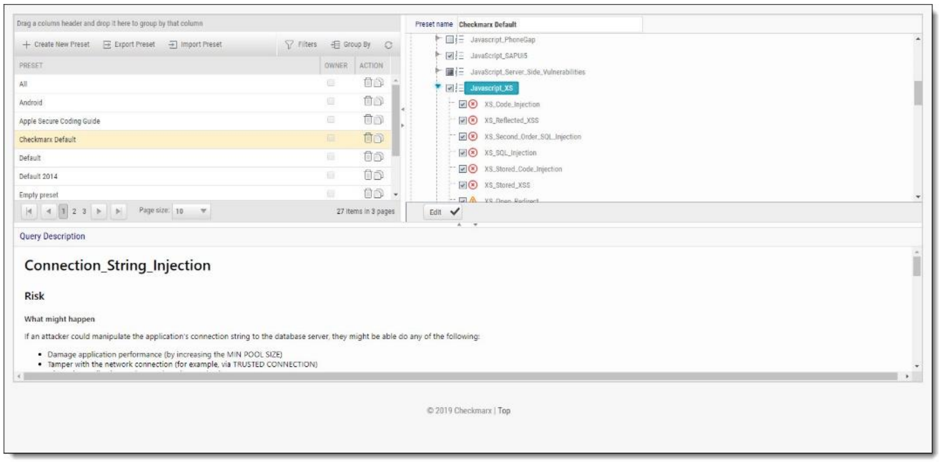
Preset Manager

Presets in CxSAST are predefined sets of queries that can be selected when creating and managing projects. CxSAST provides predefined presets and you can create and configure your own.

➢ **To open the** Presets Manager**:**

1. Go to **Settings** > **Scan Settings** > **Preset Manager**.

   The **Preset Manager** window is displayed.



PRESET	OWNER	ACTION
All	□	
Android	□	
Apple Secure Coding Guide	□	
Checkmarx Default	□	
Default	□	
Default 2014	□	
Empty preset	□	

Preset name: Checkmarx Default

- □ Javascript_PhoneGap
- ☑ JavaScript_SAPUI5
- ■ JavaScript_Server_Side_Vulnerabilities
- ☑ Javascript_XS
  - ☑ XS_Code_Injection
  - ☑ XS_Reflected_XSS
  - ☑ XS_Second_Order_SQL_Injection
  - ☑ XS_SQL_Injection
  - ☑ XS_Stored_Code_Injection
  - ☑ XS_Stored_XSS
  - ☑ XS_Open_Redirect

Connection_String_Injection

Risk

What might happen

If an attacker could manipulate the application's connection string to the database server, they might be able do any of the following:

- Damage application performance (by increasing the MIN POOL SIZE)
- Tamper with the network connection (for example, via TRUSTED CONNECTION)

2. Select a **Preset** in the **Presets** pane. Select a **Query** from the **Queries** pane.

   A description is provided in the **Description** pane with a full explanation of the risk.

3. Click **Create New Preset** to create a new preset.

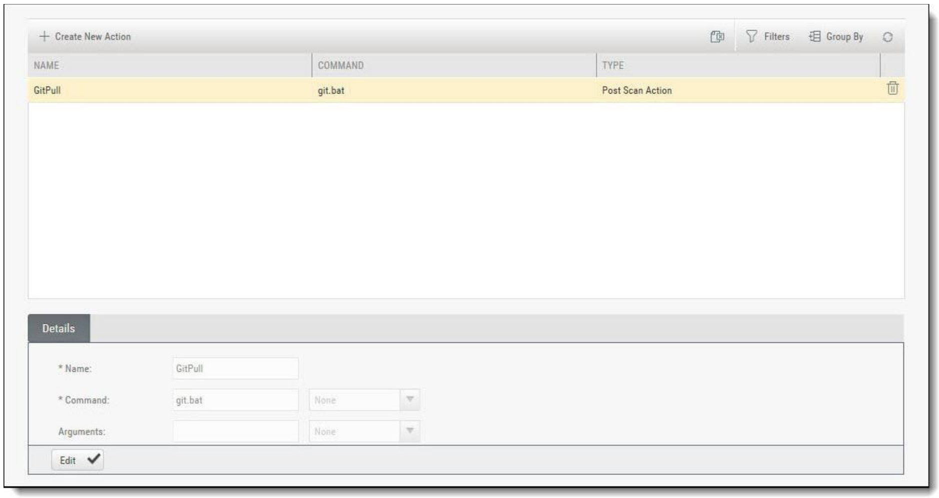
Pre & Post Scan Actions

CxSAST can be configured to perform automatic predefined actions before and after a scan, for example, sending a confirmation email or performing an executable action.

➢ **To open Pre & Post Scan Actions:**

1. Go to **Settings** > **Scan Settings** > **Pre & Post Scan Actions**.

   The **Pre & Post Scan Actions** window is displayed.



NAME	COMMAND	TYPE
GitPull	git.bat	Post Scan Action

* Name:	GitPull	
* Command:	git.bat	None
Arguments:		None

2. Select an **Action** from the **Actions** pane.

   The definitions of the selected action are displayed in the **Details** pane at the bottom of the window.

3. Click **Edit** to update the selected action details.

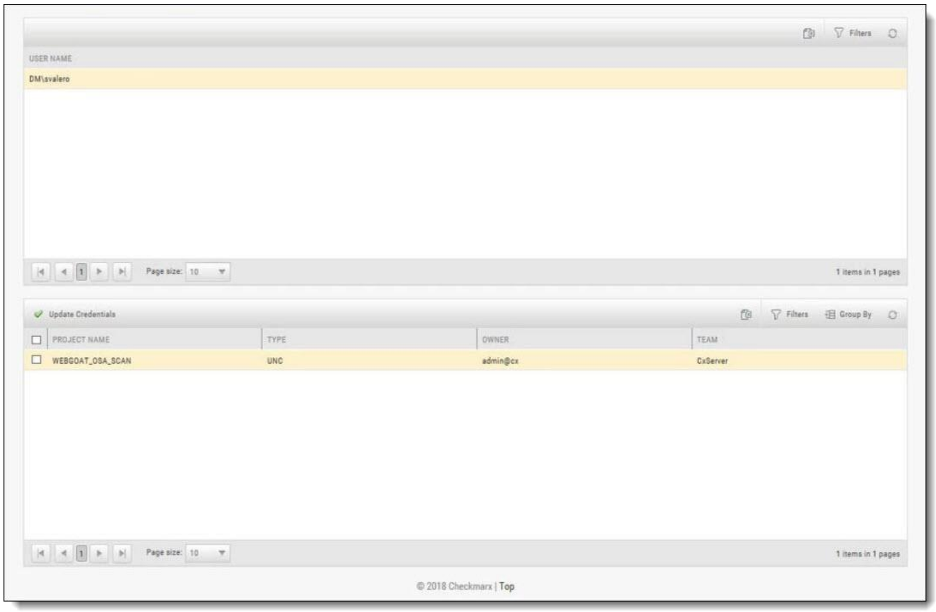
Source Control Users

CxSAST can be configured to connect to a source code control repository (i.e. TFS, SVN, GIT or Perforce) for creating projects. The **Source Control User** window can be used to view and modify the details of the authorized users that have access to these source code control repositories.

➢ **To open** Source Control Users**:**

4. Go to **Settings** > **Scan Settings** > **Source Control Users**.

   The **Source Control User** window is displayed.



USER NAME
DM\svalero

□	PROJECT NAME	TYPE	OWNER	TEAM
□	WEBGOAT_OSA_SCAN	UNC	admin@cx	CxServer

5. Select the **User** from the **Users** pane.

   The credentials of the selected user are displayed in the **Credentials** pane at the bottom of the window.

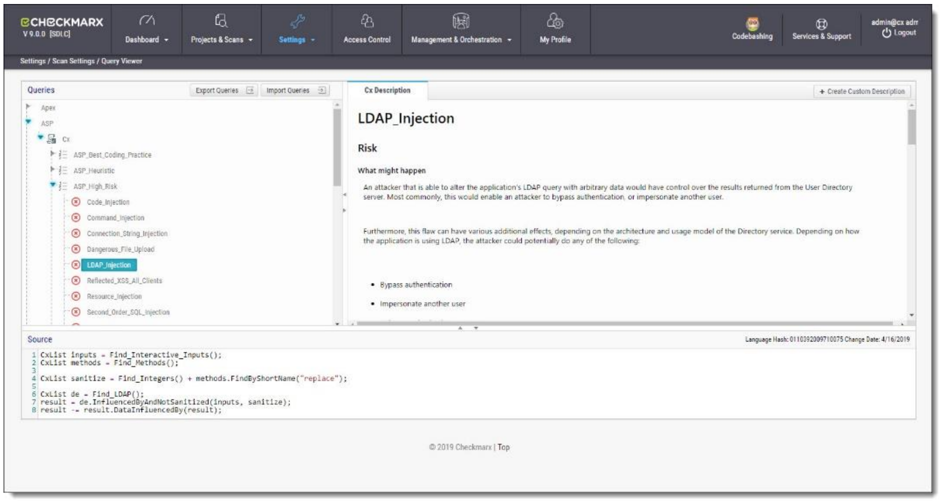
6. Click **Update Credentials** to update the selected user credentials.

Query Viewer

The **Query Viewer** displays all default queries in CxSAST. A Query is a set of predefined source code used when scanning for vulnerabilities. Conventionally descriptions are provided for each query with an explanation of the associated risk, a description of the cause and mechanism, recommendations for avoiding the vulnerability, and source code examples. Custom descriptions can be created to best suit your organizations procedures and best practices, therefore shortening the remediation time for your developers and improving the quality of your code. You can also import and export queries.

➢ **To open the Query Viewer:**

1. Go to **Settings > Scan Settings > Query Viewer**. The **Query Viewer** window is displayed.



LDAP_Injection

Risk

What might happen

An attacker that is able to alter the application's LDAP query with arbitrary data would have control over the results returned from the User Directory server. Most commonly, this would enable an attacker to bypass authentication, or impersonate another user.

Furthermore, this flaw can have various additional effects, depending on the architecture and usage model of the Directory service. Depending on how the application is using LDAP, the attacker could potentially do any of the following:

- Bypass authentication
- Impersonate another user

Language Hash: 0110392009710075 Change Date: 4/16/2019

```
CxList inputs = Find_Interactive_Inputs();
CxList methods = Find_Methods();

CxList sanitize = Find_Integers() + methods.FindByShortName("replace");

CxList de = Find_LDAP();
result = de.InfluencedByAndNotSanitized(inputs, sanitize);
result -= result.DataInfluencedBy(result);
```

2. Select a **Query** in the **Queries** pane.

   A description is provided in the **Description** pane with a full explanation of the risk. The source code is displayed in the **Source** pane at the bottom of the window.

Creating a Custom Description

You can create a Custom Description to best suit your own organizations procedures and best practices.

The custom description creation option is enabled by default for Auditor and Admin users only.

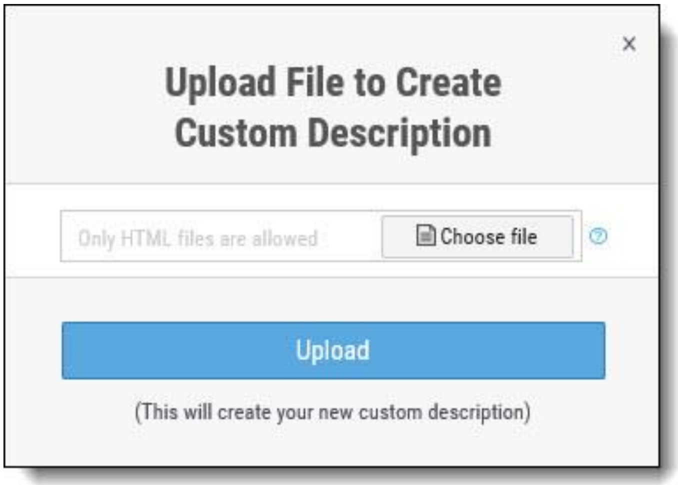
➢ **To create a custom description:**

1. From the **Query Viewer**, select a **Query** in the **Queries** pane.

   A description is provided in the **Description** pane.

2. Click **Create Custom Description**.

   The **Upload File to Create Custom Description** window is displayed.



Upload File to Create Custom Description

(This will create your new custom description)

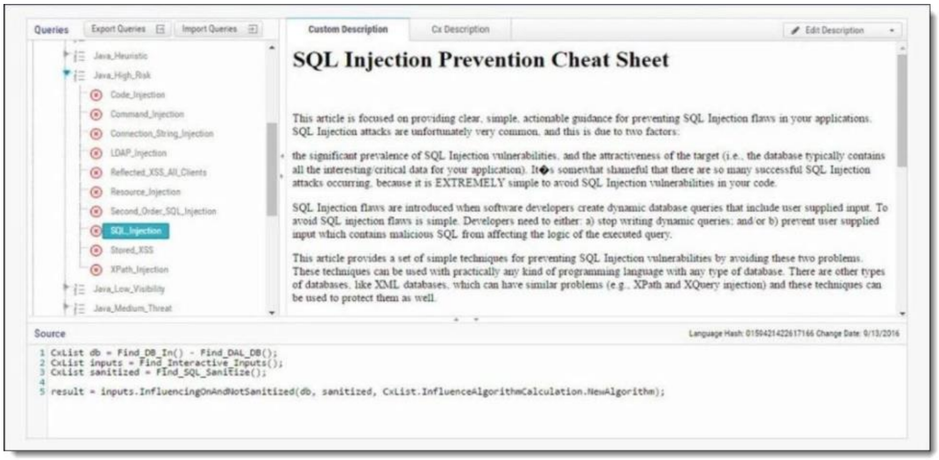
3. Click **Choose File,** navigate to the custom description file (.HTML) and click **Open**.
4. Click **Upload**.

   The **Custom Description** tab is displayed in the **Description** pane.

For security reasons, CxSAST only supports the following HTML tags, attributes and inline styles:

- **Tags** - b, br, caption, center, col, colgroup, dir, div, dl, dt, em, fieldset, font, footer, h1, h2, h3, h4, h5, h6, header, hr, i, li, ol, p, pre, span, strike, strong, table, tbody, td, tfoot, th, thead, tr, u, ul,
- **Attributes** - align, alt, bgcolor, border, cellpadding, cellspacing, charset, color, cols, colspan, dir, height, lang, list, nowrap, radiogroup, rows, rowspan, selected, size, span, style, title, valign, value, vspace, width, wrap
- **Styles (CSS values)** - background, background-color, background-position, background-repeat, border, border-bottom, border-bottom-color, border-bottom-style, border-bottom-width, border-collapse, border-color, border-left, border-left-color, border-left-style, border-left-width, border-right, border-right-color, border-right-style, border-right-width, border-spacing, border-style, border-top, border-top-color, border-top-style, border-top-width, border-width, bottom, caption-side, clear, clip, color, content, counter-increment, counter-reset, cursor, direction, display, empty-cells, float, font, font-family, font-size, font-style, font-variant, font-weight, height, left, letter-spacing, line-height, list-style, list-style-image, list-style-position, list-style-type, margin, margin-bottom, margin-left, margin-right, margin-top, max-height, max-width, min-height, min-width, orphans, outline, outline-color, outline-style, outline-width, overflow, padding, padding-bottom, padding-left, padding-right, padding-top, page-break-after, page-break-before, page-break-inside, quotes, right, table-layout, text-align, text-decoration, text-indent, text-transform, top, unicode-bidi, vertical-align, white-space, widows, width, word-spacing, z-index.

If you try to upload a file with anything else other than what is listed above, the description is not saved.



SQL Injection Prevention Cheat Sheet

This article is focused on providing clear, simple, actionable guidance for preventing SQL Injection flaws in your applications. SQL Injection attacks are unfortunately very common, and this is due to two factors:

- the significant prevalence of SQL Injection vulnerabilities, and the attractiveness of the target (i.e., the database typically contains all the interesting/critical data for your application). It�s somewhat shameful that there are so many successful SQL Injection attacks occurring, because it is EXTREMELY simple to avoid SQL Injection vulnerabilities in your code.

SQL Injection flaws are introduced when software developers create dynamic database queries that include user supplied input. To avoid SQL injection flaws is simple. Developers need to either: a) stop writing dynamic queries; and/or b) prevent user supplied input which contains malicious SQL from affecting the logic of the executed query.

This article provides a set of simple techniques for preventing SQL Injection vulnerabilities by avoiding these two problems. These techniques can be used with practically any kind of programming language with any type of database. There are other types of databases, like XML databases, which can have similar problems (e.g., XPath and XQuery injection) and these techniques can be used to protect them as well.

Language Hash: 0159421422617166 Change Date: 9/13/2016

```
CxList db = Find_DB_In() - Find_DAL_DB();
CxList inputs = Find_Interactive_Inputs();
CxList sanitized = Find_SQL_Sanitize();

result = inputs.InfluencingOnAndNotSanitized(db, sanitized, CxList.InfluenceAlgorithmCalculation.NewAlgorithm);
```

You can replace or delete the custom description by clicking **Edit Description** and selecting **Update Description** or **Delete Description** accordingly.

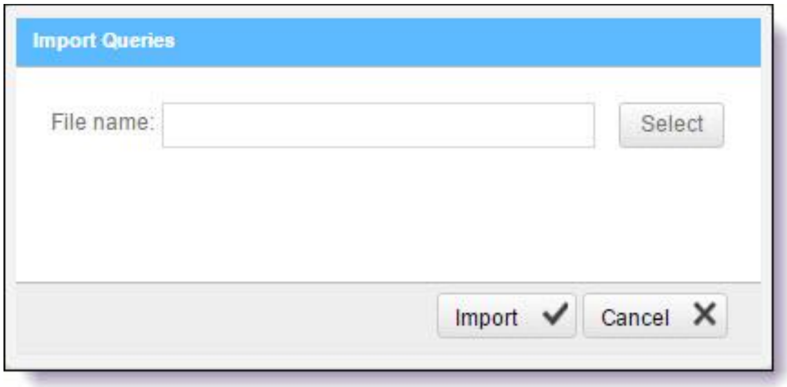
Importing Queries

You can import queries into CxSAST to best suit your own organizations procedures and best practices.

➢ **To import queries:**

1. From the **Query Viewer**, click **Import Queries**.

   The **Import Queries** window is displayed.



2. Click **Import,** navigate to the query file (.XML) and click **Open**.

   The query is displayed in the **Queries** pane.

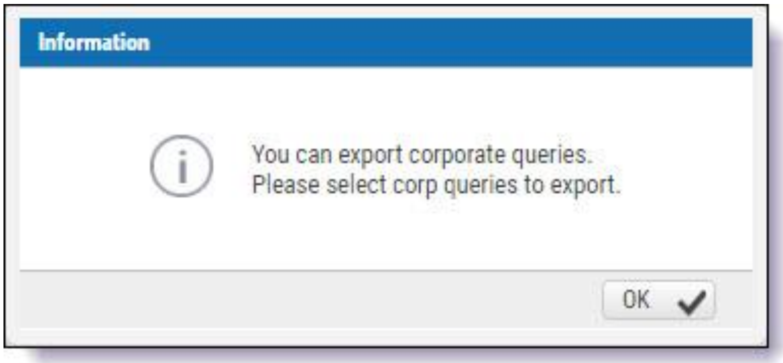
Exporting Queries

You can export queries from CxSAST to use in other departments.

➢ **To export queries:**

1. From the **Query Viewer**, click **Export Queries**.

   The **Export Queries** window is displayed.



Information

You can export corporate queries.
Please select corp queries to export.

2. Click **OK**.

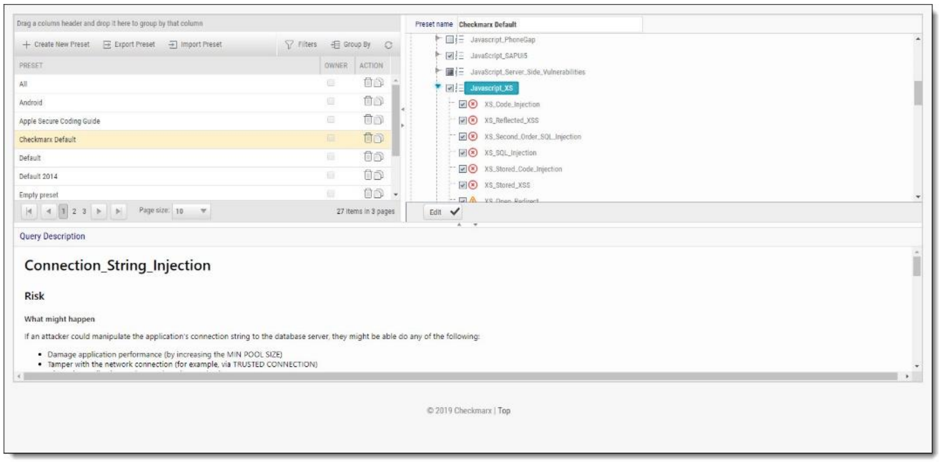
Preset Manager

Presets are predefined sets of queries that you can select when Creating, Configuring and Branching Projects. Predefined presets are provided by Checkmarx and you can configure your own. You can also import and export presets.

➢ **To open the Preset Manager:**

- Go to **Settings > Scan Settings > Preset Manager.**

  The Presets Manager window is displayed.



PRESET	OWNER	ACTION
All		
Android		
Apple Secure Coding Guide		
Checkmarx Default		
Default		
Default 2014		
Empty preset		

Preset name: Checkmarx Default

- ☐ Javascript_PhoneGap
- ☑ JavaScript_SAPUI5
- ▣ JavaScript_Server_Side_Vulnerabilities
- ☑ Javascript_XS
  - ☑ XS_Code_Injection
  - ☑ XS_Reflected_XSS
  - ☑ XS_Second_Order_SQL_Injection
  - ☑ XS_SQL_Injection
  - ☑ XS_Stored_Code_Injection
  - ☑ XS_Stored_XSS
  - ☑ XS_Open_Redirect

Query Description

Connection_String_Injection

Risk

What might happen

If an attacker could manipulate the application's connection string to the database server, they might be able do any of the following:

- Damage application performance (by increasing the MIN POOL SIZE)
- Tamper with the network connection (for example, via TRUSTED CONNECTION)

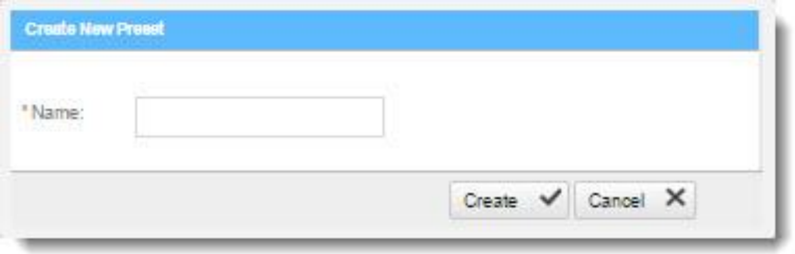
You can quickly create a new preset based on an existing one (duplicate) by selecting a Preset from the Preset pane and clicking ⧉.

Creating a New Preset

➢ **To create a new preset:**

1. From the **Preset Manager**, click **Create New Preset**.

   The Create New Presets window is displayed.



2. Enter a preset **Name** and click **Create**.
3. Select a **Coding Language**.
4. Select the **Queries** to be included in the preset.
5. Click **Save**.

Modifying an Existing Preset

➢ **To modify an existing preset:**

1. From the **Preset Manager**, select a **Preset** from the Preset pane and click **Edit**.
2. Select a **Coding Language**.
3. Select the **Queries** to be included in the preset.

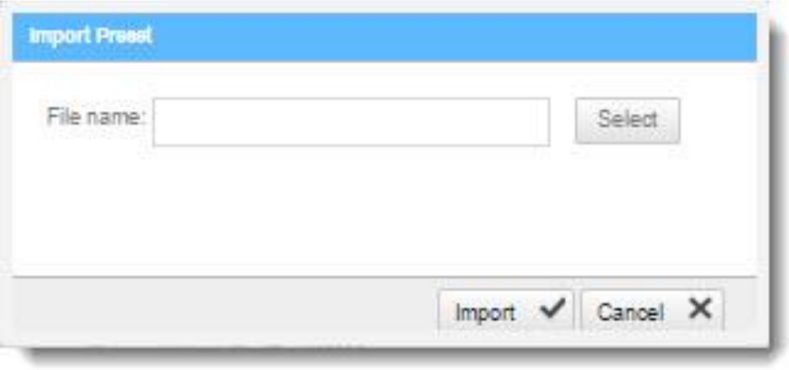
   You can edit a single language, such as Java, selecting and deselecting the queries as needed, and then press Synchronize in order for all related queries in all languages to be selected.
4. Click **Save**.

Importing a Preset

➢ **To import a preset:**

1. From the **Preset Manager**, click **Import Preset**.

   The Import Preset window is displayed.



2. Click **Select**, navigate to the preset (.XML file) and click **Open**.
3. If the imported preset has the same name as an existing one, the existing preset will be overridden.
4. Click **Import**.

   The Preset is displayed in the Preset pane.

Exporting a Preset

➢ **To export a preset:**

- From the **Preset Manager**, click **Export Preset** and save the exported preset (.XML file).

Deleting a Preset

➢ **To delete a preset:**

- From the **Preset Manager**, select a **Preset** from the Preset pane and click 🗑 .

Predefined Presets

The following is a list of all the predefined presets provided by Checkmarx with the recommended usage and which vulnerability queries are included:

Preset	Usage	Includes vulnerability queries for....
All	For all application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
Android	For Android related application security risks	Groovy, Java and Kotlin coding languages
Apple Secure Coding Guide	For IOS related application security risks	ObjectiveC coding language

Preset	Usage	Includes vulnerability queries for....
Checkmarx Default	The Checkmarx Default preset essentially contains all the vulnerabilities that Checkmarx recommends to scan in cases when you are unsure about which preset to use.	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
Default	Default preset (soon to be discontinued)	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Default 2014	Default preset for 2014 (soon to be discontinued)	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Empty Preset	Empty preset with no vulnerability queries. This can be used to create a new preset from scratch	Empty
Error Handling	For error handling related application security risks	Apex, ASP, CPP, CSharp, Java, Perl, PHP, Ruby and VbNet coding languages
FISMA	For homeland security application risks according to the 'Federal Information Security Modernization Act' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High and Medium	For high and medium related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High, Medium and Low	For high, medium and low related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
HIPAA	For sensitive patient data related security risks according to the HIPAA (Health Insurance Portability and Accountability Act) compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, VB6, VbNet and VbScript coding languages
JSSEC	For Android related application security risks according to the JSSEC (Japan's Smartphone Security Association) compliance guidelines	Groovy and Java coding languages
MISRA_C	For C related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language
MISRA_CPP	For C++ related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language

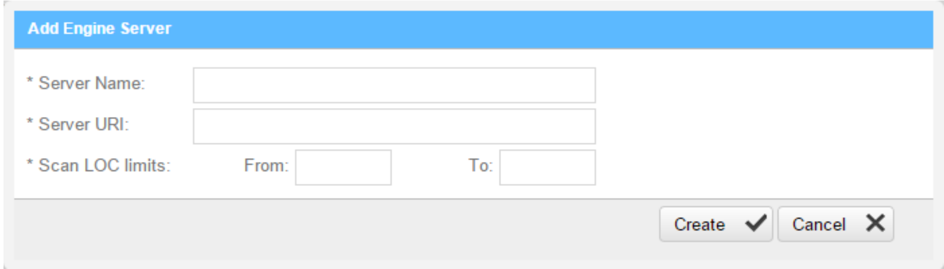
Preset	Usage	Includes vulnerability queries for....
Mobile	For mobile related application security risks	CSharp, Groovy, Java, JavaScript, Kotlin and ObjectiveC coding languages
NIST	For the application security risks according to the 'National Institute of Standards and Technology' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
OWASP Mobile TOP 10-2016	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2016	CSharp, Groovy, Java, JavaScript, Kotlin and ObjectiveC coding languages
OWASP TOP 10-2010	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2010	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2013	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2013	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2017	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2017	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
PCI	For credit card payment application security risks according to the PCI (Payment Card Industry) compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet, and VbScript coding languages
SANS Top 25	For the top 25 web application security risks according the SANS Technology Institute’s compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
STIG	For the application security risks according to the 'Security Technical Implementation Guide' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
WordPress	For WordPress related web application security risks	PHP coding language
XS	For XS SAP related application security risks	JavaScript coding language
XSS and SQLi only	Recommended best practice when starting to scan a new project in order to focus on the most important vulnerabilities first.	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala VB6, VbNet and VbScript coding languages

Limiting Engine Scans

➢ **To Limit Engine Scans:**

- In **Settings > Server Setting > Installation Information**, click + Add Engine Server.

  The Add Engine Server window is displayed.

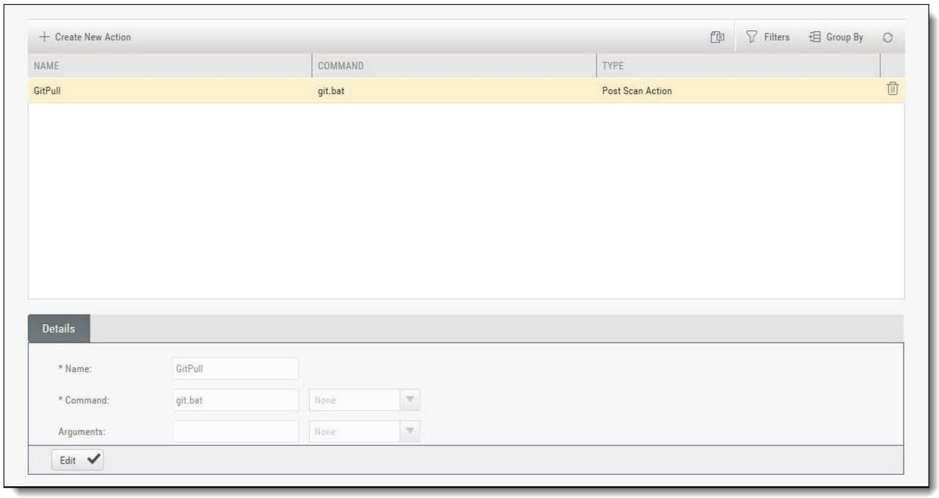


The Adding Engine Server window includes the following properties:

- **Server Name**: The name of the server you are appointing as Engine Server
- **Server URI**: The address of the server
- **Scan LOC limits**: The Scan limits is not a mandatory field, in the event the fields are left empty assume the value From to include: All to: All. Define the lower and higher limits for size of projects that this engine can accept for scanning.
  - When the range is defined and the user clicks OK, the system performs a check of range continuity. In the event there is no continuity between ranges of all engines defined at that moment, a pop-up message is displayed: "Line 1: "Notice: Projects including the following ranges: line 2 : XXX – YYY line 3: more then 1000 Line 4: Will not be scanned."
  - In the event the scan size falls out of defined engine ranges, the scan fails and the following message is displayed: "Scan has failed due to falling outside of the defined engines scan ranges".
  - After defining the scan engine range, in order to activate the user has to Restart the scan manager service.

Configuring Pre & Post Scan Action

1. Go to **Settings** > **Scan Settings** > **Pre & Post Scan Actions**. The **Pre & Post Scan Action** window is displayed.

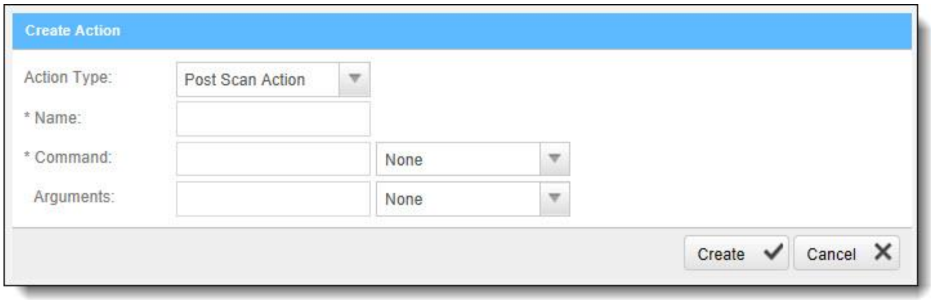


NAME	COMMAND	TYPE
GitPull	git.bat	Post Scan Action

* Name:	GitPull	
* Command:	git.bat	None
Arguments:		None

2. Click **Create New Action**.

   The **Create Action** window is displayed.



Action Type:	Post Scan Action	
* Name:		
* Command:		None
Arguments:		None

3. Configure the following parameters:
   - **Action Type** - select Pre-scan Action / Post Scan Action
   - **Name** - enter the Pre/Post scan Action name
   - **Command** - enter the command (e.g. pull batch file's exact name)
   - **Arguments** - leave empty
4. Click **Create** and **Finish**.

User Management

This section explains aspects of the user management.

User Administration

Checkmarx Access Control is a user management solution for user administration. Using Access Control, user administration managers are provided with a universal view of user access rights and a centralized management console to define unified access control management for all Checkmarx users. Access Control also provides the AuditTrail database table – an audit log that can be used for tracking user actions. In upcoming releases Access Control will be integrated into the CxPlatform, to deliver a fully featured user interface for access control and user management across the entire Checkmarx product offering.

For more information about Access Control for this version, refer to the Access Control User Guide.

For more information about CxSAST/CxOSA roles and permissions, see CxSAST / CxOSA Roles and Permissions.

CxSAST / CxOSA Roles and Permissions

This section describes the roles and permissions associated with CxSAST / CxOSA that are effective after performing the data migration procedure and upgrading to CxSAST/CxOSA v9.0.0 and up.

Provided CxSAST / CxOSA Roles

The following table lists the predefined roles that are provided for CxSAST / CxOSA v9.0.0 and up, along with their respective permissions:

Provided roles cannot be updated or deleted.

Provided Roles for CxSAST / CxOSA	Description	Permissions per Role
Scanner	Permissions to create and manage projects, and run scans	save-sast-scan save-osa-scan open-issue-tracking-tickets save-project create-project

Provided Roles for CxSAST / CxOSA	Description	Permissions per Role
		view-failed-sast-scan download-scan-log see-support-link
Reviewer	Read-only permissions to view scan results and generate reports	manage-result-comment manage-data-analysis-templates generate-scan-report export-scan-results see-support-link
Auditor	Permissions to manage vulnerability queries and use CxAudit	use-cxaudit create-preset update-and-delete-preset manage-custom-description save-sast-scan save-project
Results Updater	Permissions to update the properties of scan results	manage-results-state-and-assignee manage-result-comment manage-result-severity
Results Verifier	Permissions to set the state of scan results to "Not Exploitable"	manage-result-exploitability
Data Cleaner	Permissions to delete projects and scans	delete-sast-scan delete-project
SAST Admin	Full permissions	All SAST permissions, excluding use-cxaudit

CxSAST / CxOSA Permissions

The following table describes the permissions associated with CxSAST / CxOSA v9.0.0 and up:

Permission	Category	Description
save-sast-scan	Projects & Scans	Run new CxSAST scan Create scan subset Save results from CxAudit

Permission	Category	Description
delete-sast-scan	Projects & Scans	Delete CxSAST scan Lock/unlock scan
save-project	Projects & Scans	Create new project Update project Branch project Duplicate project Save local project from CxAudit
delete-project	Projects & Scans	Delete project
view-failed-sast-scan	Projects & Scans	View faild scans
save-osa-scan	Projects & Scans	Run CxOSA scan
download-scan-log	Projects & Scans	Download scan log
manage-result-state-and-assignee	Scan Results	Change result state (excluding NE) Assign user
manage-result-comment	Scan Results	Add new result comment
manage-result-exploitability	Scan Results	Set result state to NE (all other states will be available as well)
manage-result-severity	Scan Results	Change result severity
open-issue-tracking-tickets	Scan Results	Create ticket for result
manage-data-analysis-templates	Reports	create and delete templates
generate-scan-report	Reports	Generate scan reports
export-scan-results	Reports	Export to CSV from the results viewer
manage-custom-description	Vulnerability Queries	Manage custom query descriptions (create, export and import)
create-preset	Vulnerability Queries	Create a new preset, save it, update it, delete it
update-and-delete-preset	Vulnerability Queries	Edit and delete all presets (including Cx out-of-the-box presets)
use-cxaudit	Vulnerability Queries	Login to CxAudit

Permission	Category	Description
		Note: This permission is counted against the license.
manage-data-retention	System Configuration	Manage data retention
manage-engine-servers	System Configuration	Manage engine servers
manage-system-settings	System Configuration	Download application logs View utilization dashboard View license details View installation details View and edit general settings View and edit CxOSA settings Manage source control users Export/import preset
manage-external-services-settings	System Configuration	Configure external service settings
manage-custom-fields	System Configuration	Create/update/delete custom fields
manage-issue-tracking-systems	System Configuration	Manage issue-tracking system
manage-pre-post-scan-actions	System Configuration	Configure pre- and post-scan actions
download-system-logs	System Configuration	View installation details page Download application logs Note: only available from 9.0 HF1
use-odata	API	Fetch all data via OData API (no filter per current user's team)
see-support-link	Other	View and use "Services & Support" button
view-results	Scan Results	This permission separates the view-results ability from any other permission. This is added to any predefined role and is available from CxSAST 9.0 HF5

Permissions per User Interface Screen

The following permissions are required to open the following CxSAST / CxOSA user interface screens.

UI Screen	Required permission to open the screen
Dashboard/Project state	-
Dashboard/Failed scans	view-failed-sast-scan
Dashboard/Utilization	manage-system-settings
Dashboard/Risk	-
Dashboard/Data Analysis	
Projects & Scans/Create new project	
Projects & Scans/Queue	
Projects & Scans/Projects	-
Projects & Scans/All scans	-
Management/Scan settings/Query viewer	-
Management/Scan settings/Preset manager	-
Management/Scan settings/Pre-post actions	manage-pre-post-scan-actions
Management/Scan settings/Source control users	manage-system-settings
Management/Application settings/General	manage-system-settings
Management/Application settings/License	manage-system-settings
Management/Application settings/OSA settings	manage-system-settings
Management/Application settings/Installation	manage-system-settings
Management/Application settings/External services	manage-external-services-settings

UI Screen	Required permission to open the screen
Management/Application settings/Engine management	manage-engine-servers
Management/Application settings/Data retention	manage-data-retention
Management/Application settings/Issue tracking	manage-issue-tracking-systems
Management/Manage custom fields	manage-custom-fields
Access Control	manage-users (AC permission)
M&O/Analytics	view-analytics (M&O permission)
M&O/Remediation Intelligence	(M&O permission)
M&O/Policy Violations	-
M&O/Policy Manager	-
My Profile	-
Services & Support	see-support-link