CxSAST v9.3.0

User Guide

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

Once CxSAST has been installed, you have to create an Administrator user account before logging in for the first time. The Admin user, who will be a member of the CxServer Team (the top level in the hierarchy) has full permissions to manage all applicable users, roles, teams, server settings, and projects.

Registering a new User

- 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 enter **http://<server>/cxwebclient/login.aspx** where **<server>** reflects the IP address or resolvable hostname of the CxSAST server.

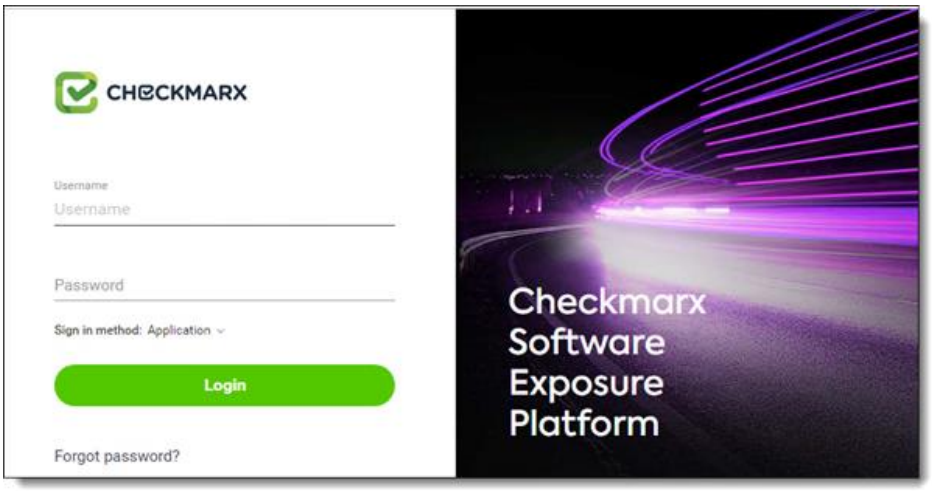
- If '3rd party cookies' are disabled in your browser, you will not be able to log into the CxSAST Web Interface via '**http://localhost**'. In this case, you have to use '**http://<FQDN>**', where **<FQDN>** stands for **Fully Qualified Domain Name** and consists of both the hostname and the domain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

1. Enter the required Administrator user account information.
2. Define the required password according to the following requirements:
    - 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. Click <**Register**>. You are directed to the Checkmarx Login page.

Logging In

To log in, do the following:

1. Access the Checkmarx portal as explained above.
2. Enter the user name and password that you defined when registering as a new user.



- The 'Login' and 'Change Password' pages appear always in English regardless of the selected local language.
- Starting with Access Control 2.1, the logo and the login banner can be replaced with images of your own as explained.
- You can subsequently change the Administrator password and add CxSAST users.

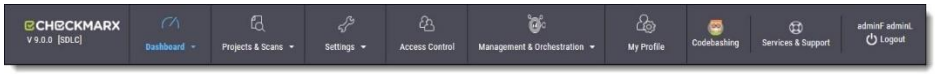
Session Timeout

A session timeout warning message appears when two thirds of the default idle time (default = 5 mins) have passed. Click <**OK**> to continue the current session. If the entire default idle time as passed, clicking <**OK**> redirects you to the login page and a new login is 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:

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 at 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

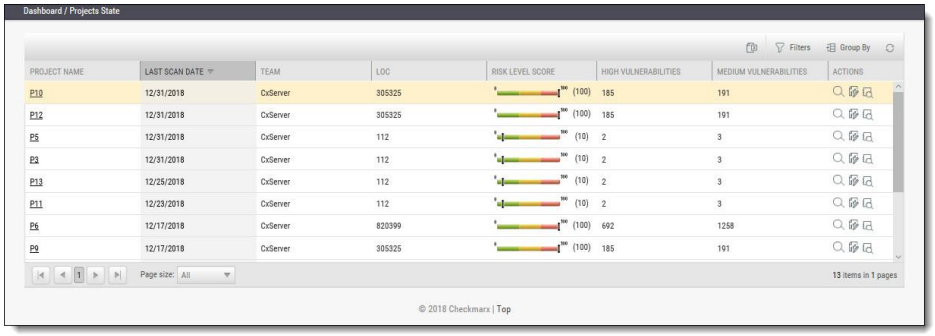
As a manager (Server, Company or Service Provider manager) you can view high-level information such as the state of your projects, scan status, utilization and risk and data analysis in the Dashboard Menu.

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 display the Project State window, go to **Dashboard > Project State**.



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)

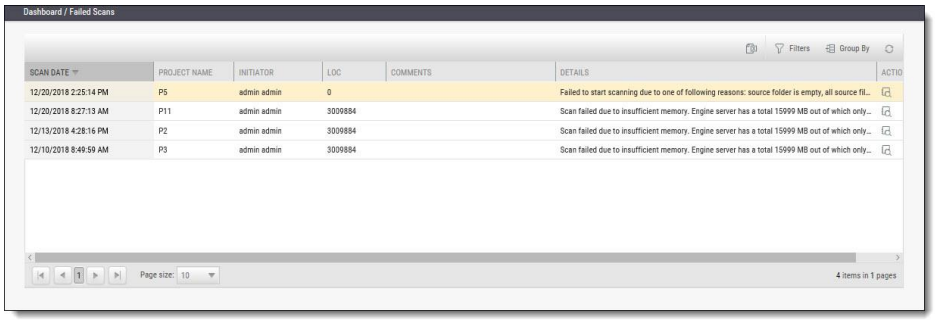
You can Export as CSV File , use the Filter and Group By tools as well as Refresh the current view.

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

Failed Scans

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

- To display the Failed Scans window, go to **Dashboard > Failed Scans**.



The Failed Scans window includes the following information:

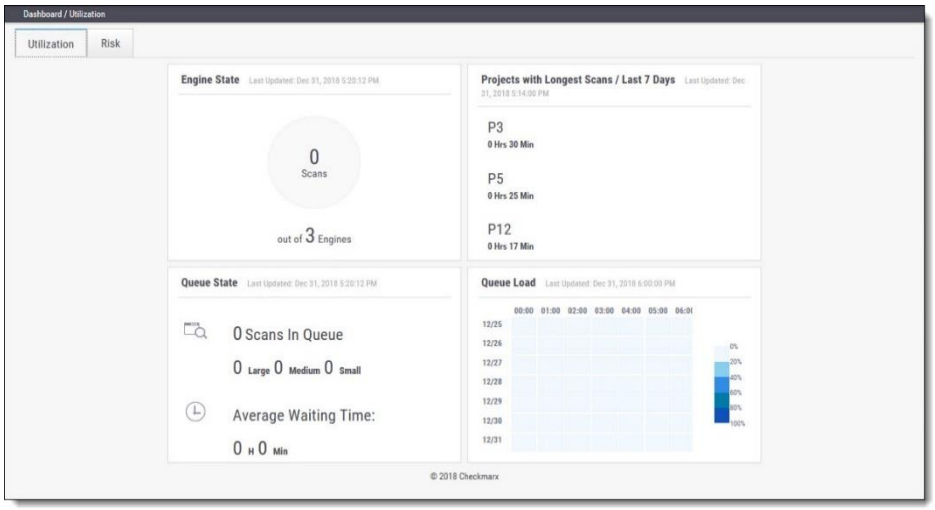
- **Scan Date**
- **Project Name**
- **Initiator**
- **LOC**
- **Comments** (as in The Queue (v8.9.0 to v9.3.0))
- **Details**
- **Actions** (Download scan logs)

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 display the Utilization window, Go to **Dashboard > Utilization**.



The Utilization window includes the following information:

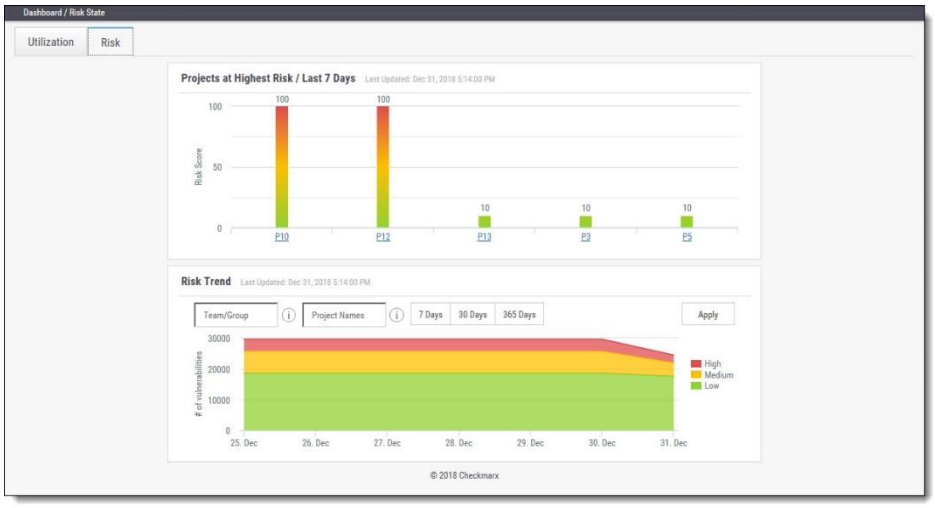
- **Engine State** - number of scans to engine ratio
- **Queue State** - number of scans in the queue and their LOC size / average waiting time
- **Projects with Longest Scans** - top 3 scans in the longest waiting time category
- **Queue Load** - queue load over a 7 day period:
    - The darker the 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 display the Risk State window, go to **Dashboard > Risk State**.



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

You can filter by **Team/Group**, **Project Name** and **Number of Days**. Click <**Apply**> to confirm.

Roll-over the graph to get the project risk and vulnerabilities scores according to date.

Click **Project Name** to view the Project State summary.

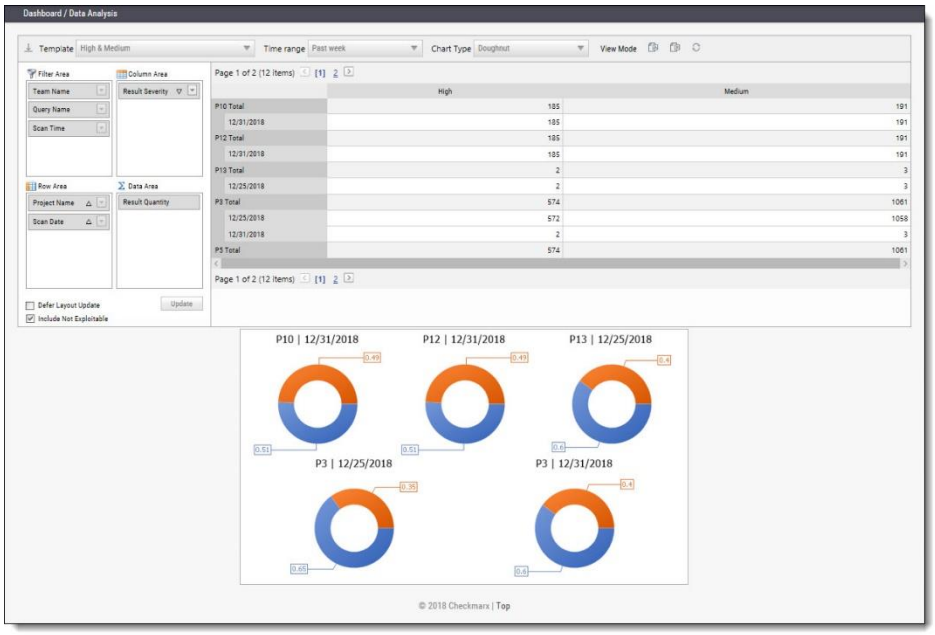
Click the legend to display/hide the respective vulnerabilities (High, Medium, Low).

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.

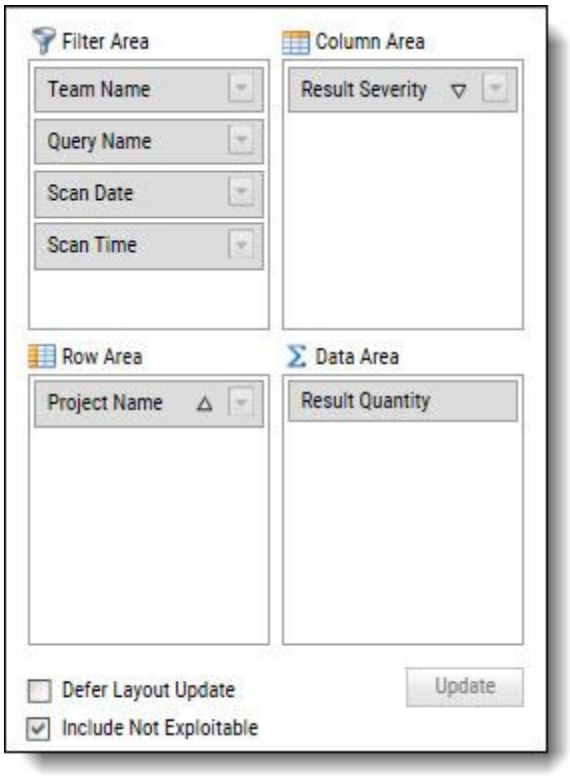
- To display the Data Analysis window, go to **Dashboard > Data Analysis**.



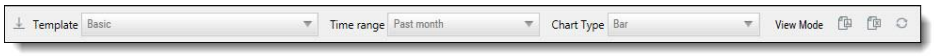
The data can be presented in several predefined configurations and you can also create your own tables.

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 Filter area to Column, Row or Data area



- 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.



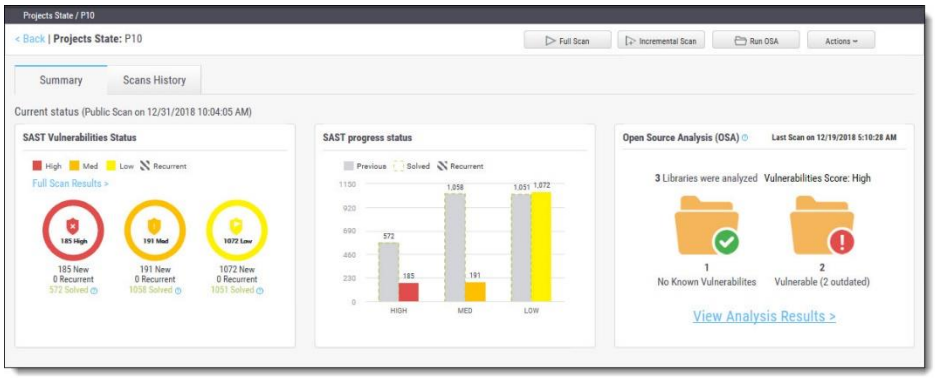
- To save a custom table as a template, click <**Save**>.

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.



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.

• Note that a purchased or 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 Vulnerabilities Status

Provides a graph with the status of each vulnerability severity.


- All new vulnerability instances discovered accorsding to severity (high, medium and low)


- Recurring vulnerability instances from previous scan

Solved is defined as 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.

Click the **Full Scan Results** link to display the Scan List for this project.

SAST Progress 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. Click on 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, see 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.

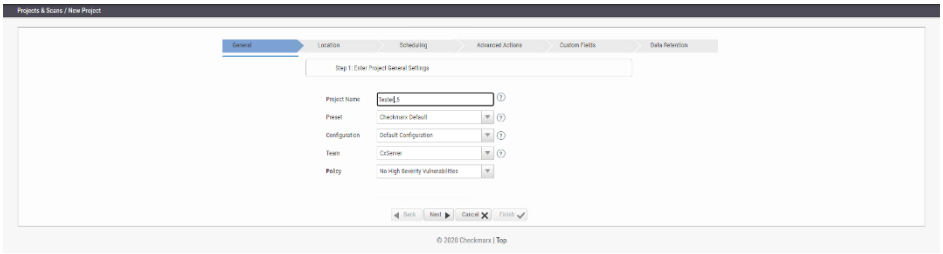
For Continuous Integration development methodology, if a new branch is created for each iteration, update the code location within the existing project (rather than creating a new project) so that all the results will reside within a single project. Scanning of projects that include multiple code languages 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 a Project

To create a CxSAST project, do the following:

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



2. Configure the following **General** project properties:
    - **Project Name -** should indicate the source code to be scanned and tracked.

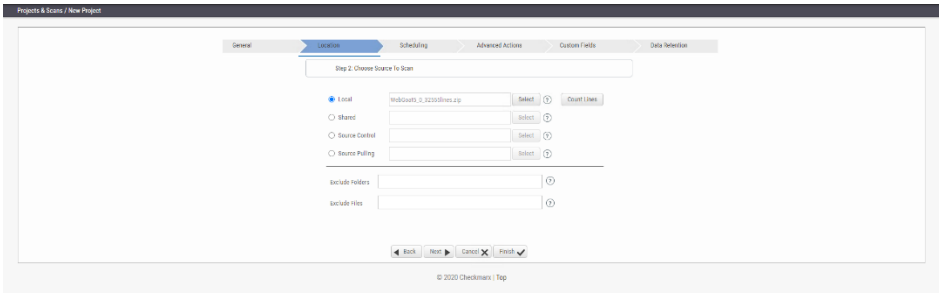
- Project names cannot include the following characters: **: ? ! \ / * " < > | ; & # $ ^**

    - **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** (optional) - 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**>. You are asked for the location of the source code.



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

- **Local -** Click <**Select**> to browse to a local file that contains the code. Future scans to the project are also performed 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.
- The supported max. file size of zipped files is 1GB and the max size of uncompressed files is 2GB. Larger files cannot be uploaded, even if the **MaxFileSize** key is set accordingly. To modify the MaxFileSize key in web.config, refer to the end of this section.
- To create a smaller zip file that only includes files with specified extensions, use the CxZip utility.
- Zip files generated in a Linux environment may not respond properly.
- If a zip file is uploaded that contains a file path longer than 255 characters, the file is not sent for scanning. Shorten the file path and try again.
- If the zip file contains another zip file inside, the internal zip file is not sent for scanning. Extract the content 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. Extract the content 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 is included under the Source Control field.
- Files inside a zip file that are located inside a repository are not sent for scanning. Extract the content 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:

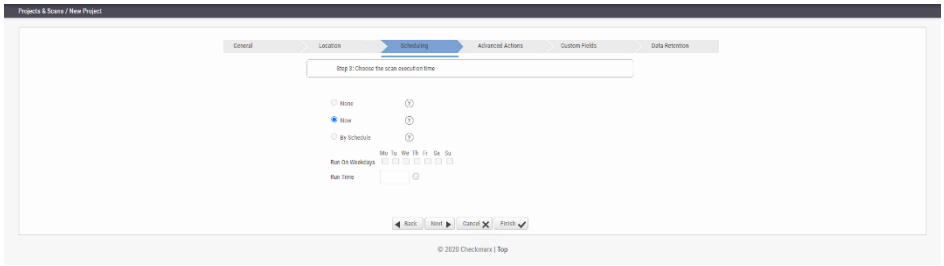
```
|+ add-ons
| |+ connectors
| | |+ cvc3.js
| | |+ spass.js
| | + z3.js
| | - lib
| | | - readme.txt
| | | - smt_solver.js
| + src
| +doc
| - readme.txt
+ src
- lib
|- find_sql_injections.js
|- jquery.js
+ logic.js
```

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

5. Click <**Count Lines**> to display the number of lines in the current project.

- The Java Script is enhanced during the scan process. The real count of lines might therefore be larger than the result displayed by running **Count Lines** or the Cx CMD Line Counter.

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



- 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.

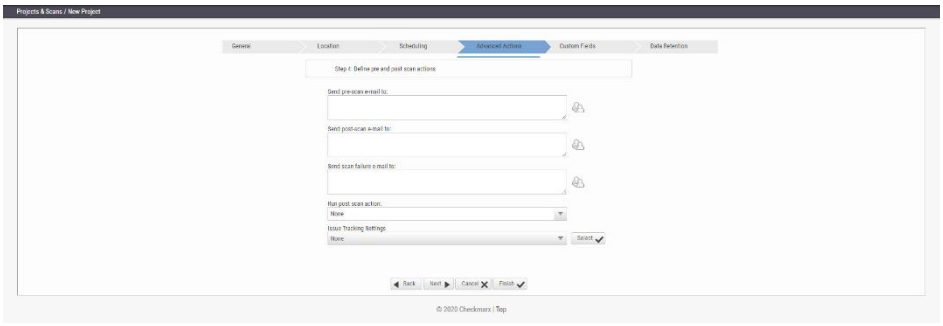
7. Configure the following scan execution **Scheduling** properties:
    - **None** - no schedule, you have to manually run the scan.
    - **Now** - defines an immediate scan.
    - **By Schedule** - define an automatic weekly scan according to the specified time.

    - **Run on Weekdays** - define on which day to run the periodic scan.
    - **Run Time** - define at what time to run the periodic scan.

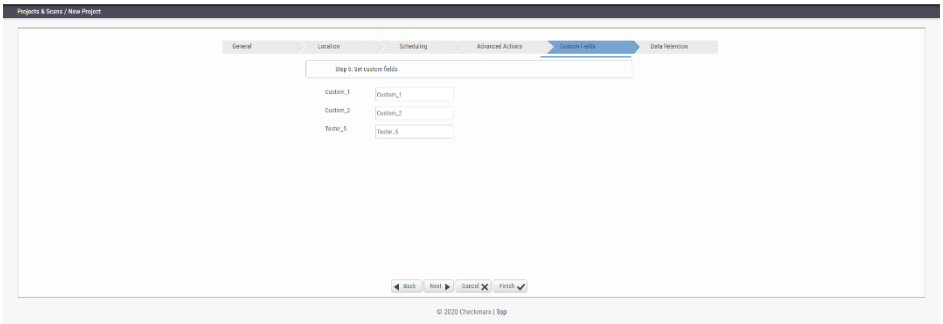
        - To support continuous integration development methodology, it is recommended to schedule periodic scanning of source files, so they can be checked after modifications. This can be automated via the CLI in the Build file, but it does not have to be done this way because CxSAST scans source code and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

- The next steps of the wizard are optional. To skip them all or some of them, click <**Finish**> after the last step you wish to configure.

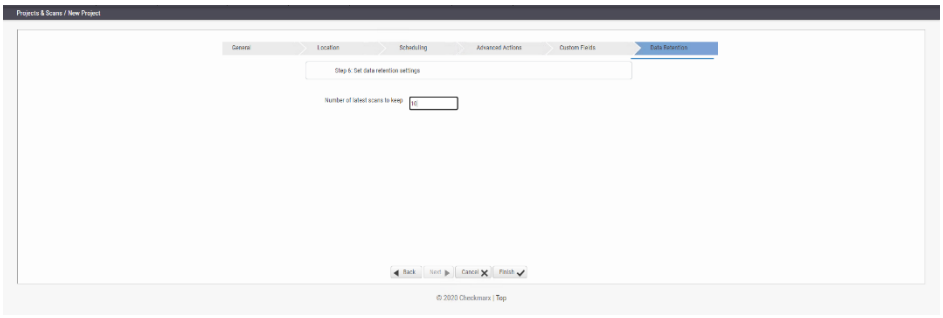
8. Click <**Next**>. to configure additional advanced options.



9. Configure the following **Advanced Action** properties:
    - **Send pre-scan email to** - define to which email address to send a pre-scan notification.
    - **Send post-scan email to** - define to which email address to send a post-scan notification.
    - **Send scan failure email to** - define to which email address 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).
10. Click <**Next**> to define custom fields.



11. Configure the **Custom Field** properties according to the available custom fields (see Custom Field Management).
12. Click <**Next**> to configure data retention.



13. Configure the **Data Retention** properties:
    - **Number of latest scans to keep** - Define the number of latest scans to be kept (see Data Retention Management).
14. Click <**Finish**> and check the scan status (see The Queue (v8.9.0 to v9.3.0)).

➢ **To modify the MaxFileSize key in web.config:**

1. Open the web.config file in the installation folder of the Web Portal installation, which is located **at** <Installation folder>\Checkmarx\CheckmarxWebPortal\Web, usually **C:\Program Files\Checkmarx\CheckmarxWebPortal\Web**
2. Navigate to the **MaxFileSize** key.
3. Set the MaxFileSize key to the desired max. file size in MB (max. 2000 for uncompressed files) and then click **Save** to save the web.config file.

Configuring the Connection to a Source Control System

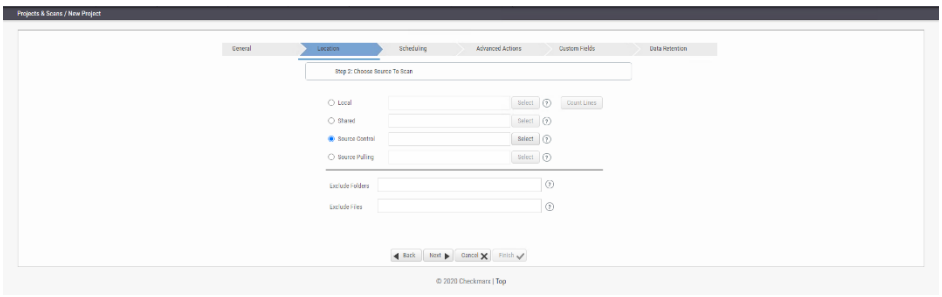
One of the options for source locations is **Source Control**. Selecting this option enables you to select and connect to one of the following source control types:

- TFS
- SVN
- GIT
- Preforce

To connect to a source control system, do the following:

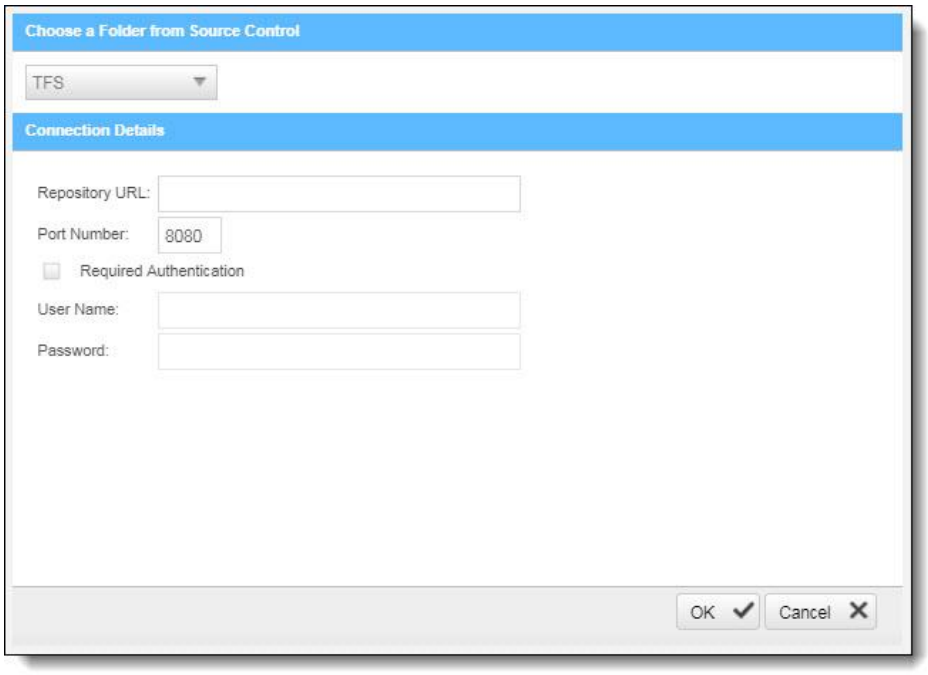
1. When creating a project, select **Source Control** as location for the source code to be scanned.
2. Click <**Select**>. The Source Control window is displayed with a drop down menu to select the desired source control type.

- Files inside a zip file that are located inside a repository are not sent for scanning. Extract the content 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.



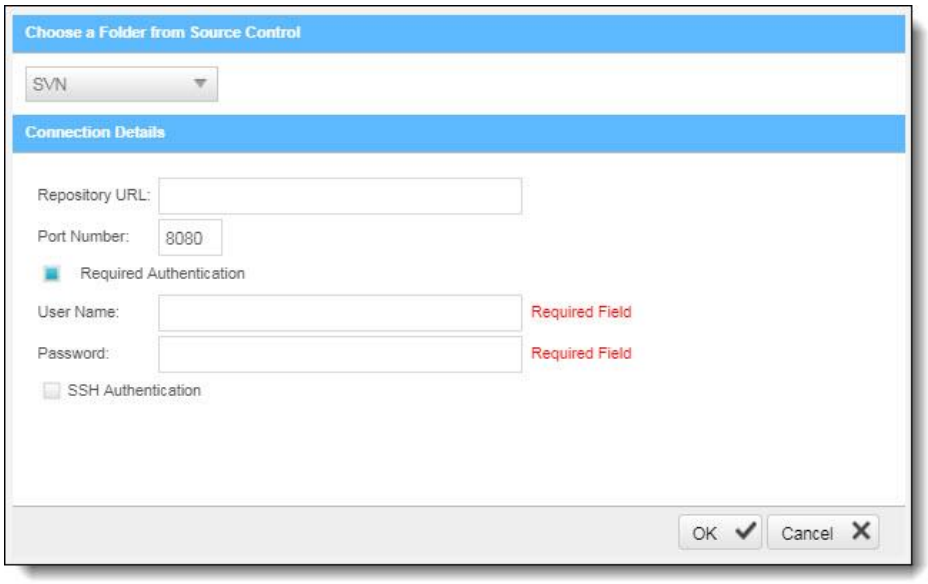
The TFS Connection Details panel includes the following parameters:

- **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.



2. 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

3. 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
4. Click <**OK**>.

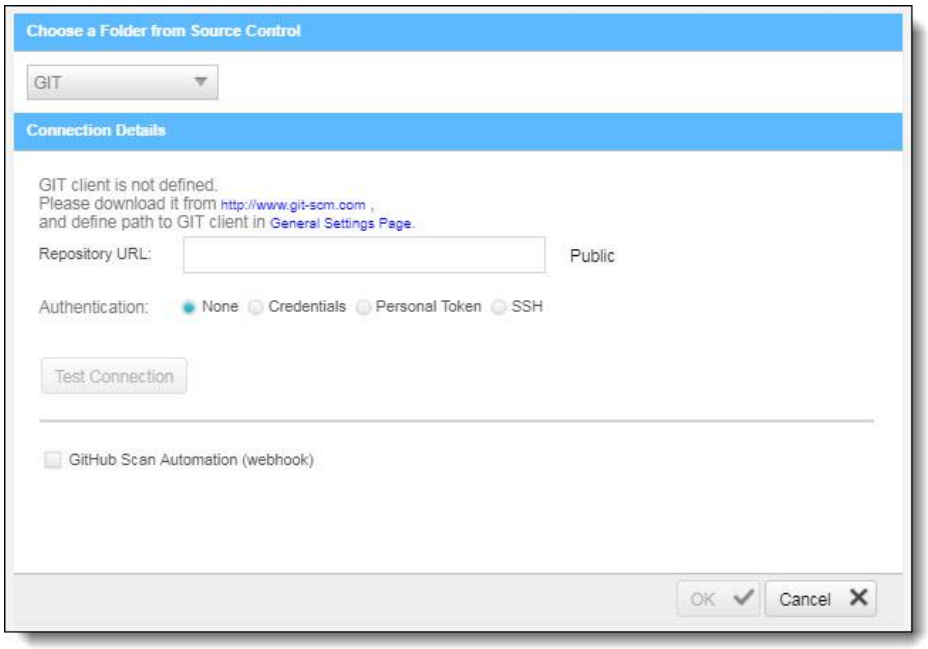
- Checkmarx does not support SSH keys with a passphrase.
- For best results, use ssh-keygen, per these instructions, and not PuTTYgen.

Defining Source Control for GIT

Requirements for using GIT repository:

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

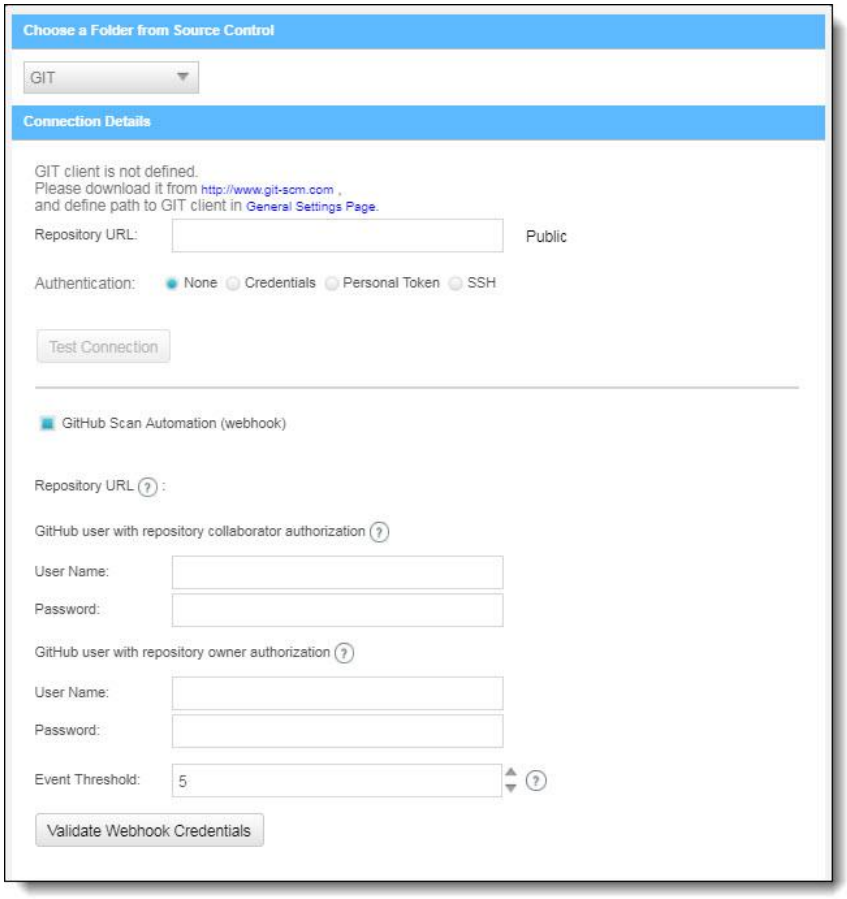
1. Select **GIT** from the drop-down. The GIT Connection Details panel is displayed.



2. 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.

- 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

    - Click **Test Connection**. Once the 'Connection Successful' message is displayed you can continue.
    - **GitHub Scan Automation** - select to include GitHub Integration.



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

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

4. 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.

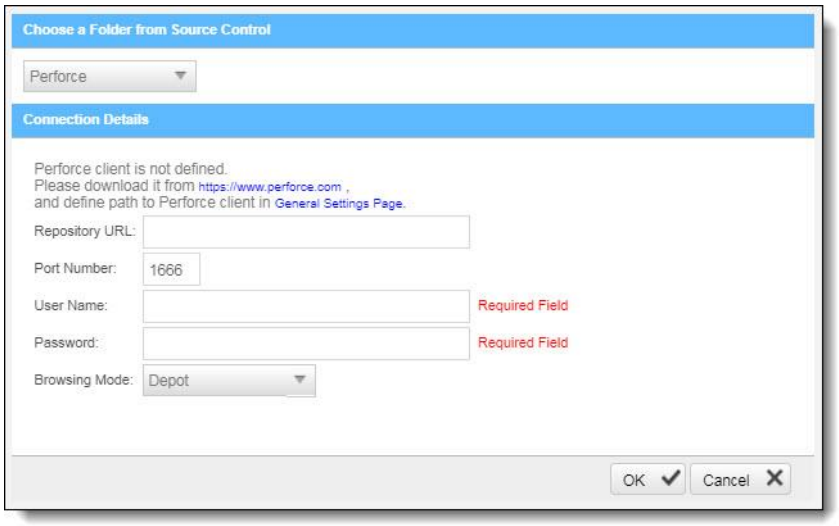
5. Click <**Validate Webhook Credentials**> to confirm authentication to the GitHub webhooks works correctly. A 'Server Connection Verified Successfully' message is displayed.
6. Click <**OK**> to complete procedure.

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.



   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**>.

- To set the Perforce client executable path, refer to the Path to P4 command line client executable parameter in the Server Settings.

You can now continue to configure the project.

- 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 and Duplicating Existing Projects

CxSAST gives you the capability to branch or 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 or duplicated, you can treat it as a separate project with separate issues to manage. Projects are duplicated or branched as follows:

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**
- **Advanced Actions** (email notifications on pre-scan, post-scan and scan failure).

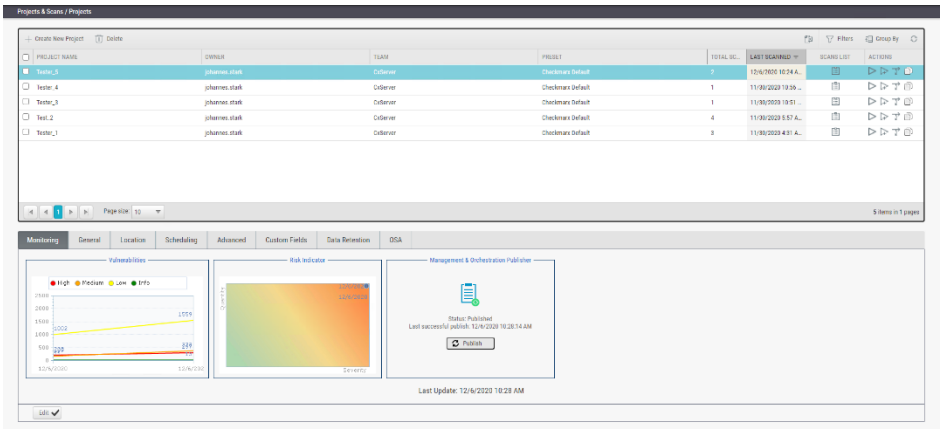
Branch Project - similar to copying a project, except that it copies the following set of properties:

- **Preset**
- **Team**
- Last scan from the source project with all results and remarks.

- When branching a project, the branch must be started from the last successful scan. Successful scan means the 'last real scan' that was performed, instead of an attempted scan, which changed the date of the scan start, but was never performed because there was no change in the code.

➢ **To open the Projects list**

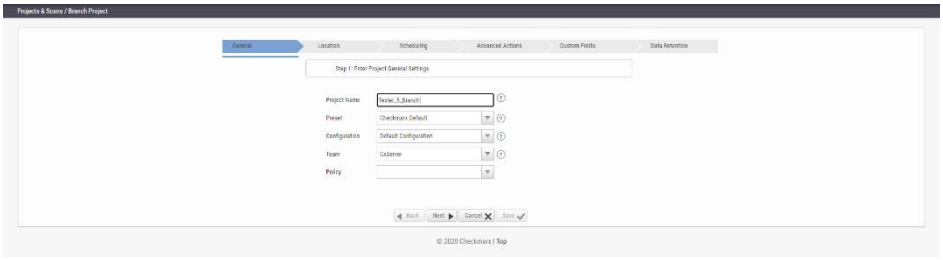
- Go to **Projects & Scans and** select **Projects**.



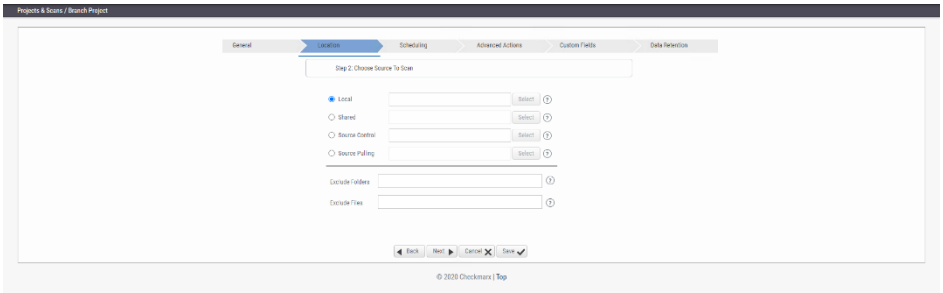
➢ **To branch an existing project**

- These instructions guide you through the workflow of branching a project. For further information on parameters, refer to the instructions on creating a new project.

1. Select the desired project from the list and click **Branch Project** to start.

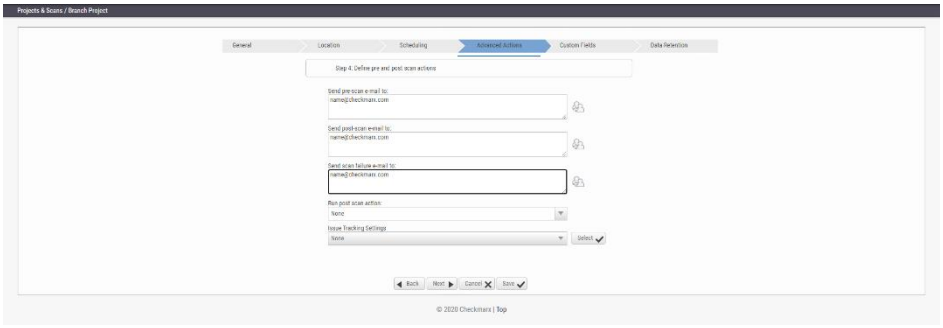


2. Assign a name that indicates that it is a branch to your selected project.
3. Click <**Next**> to continue.

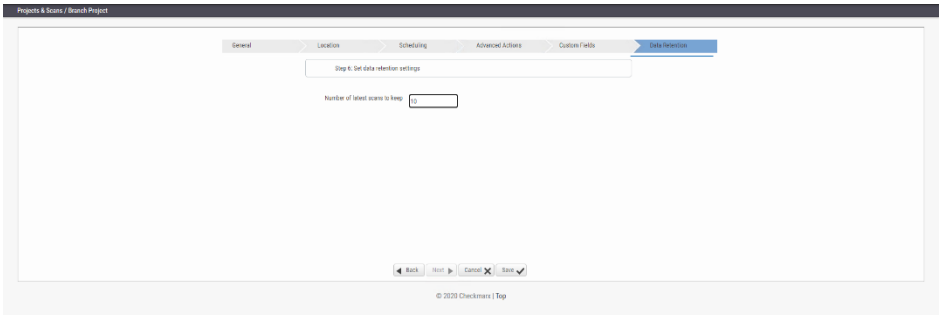


4. Keep the source set as for the original project or define the new location of the same source code.
5. The source code in the project branch must be the same as for the original project, although it can be in a different location.

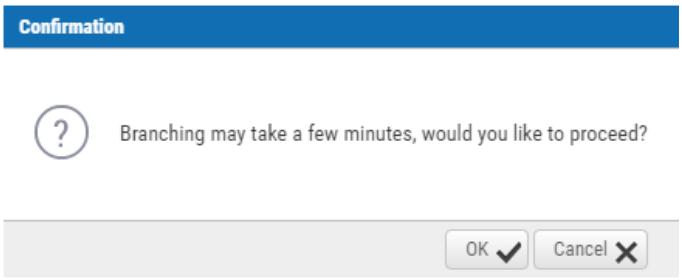
6. Do one of the following, depending on whether you wish to reconfigure the email notification settings:
    - If you don't intend to reconfigure the email notification settings. Click <**Save**> to generate the branch.
    - If you wish to configure or reconfigure email notification settings, click <**Next**> to continue the wizard. The Scheduling dialog appears, but settings are unavailable as the branch uses the original project settings.
7. Click <**Next**> again to access the Advanced Actions dialog.
8. Define the email address for notifications and click <**Next**> to continue. The Custom Fields dialog appears with the settings for the original project, which cannot be modified.



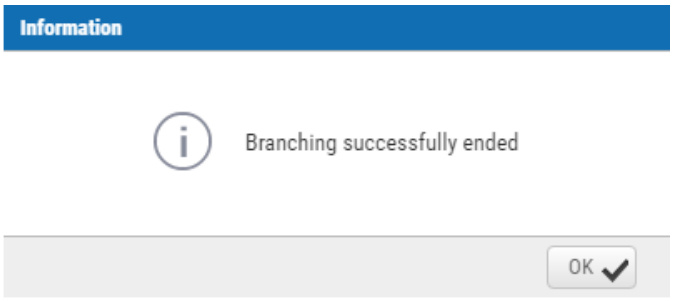
9. Click <**Next**> again to define the number of latest scans to keep in the Data Retention dialog.



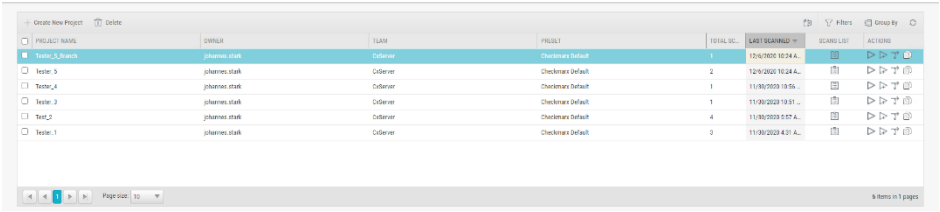
10. Define Data Retention settings and click <**Next**>.
11. Once complete, click <**Save**> and then <**OK**> to start branching the project.



You are notified once the branching has been completed.



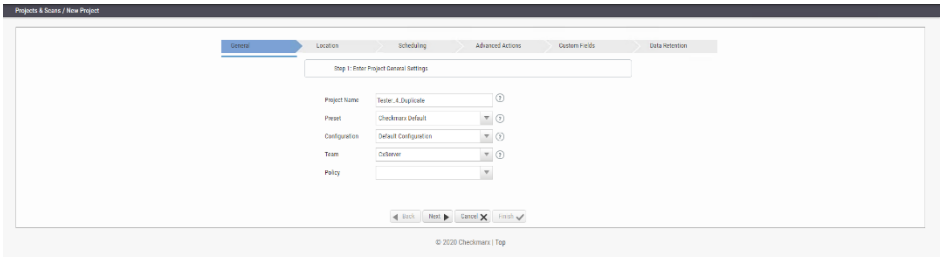
12. Click <**OK**> to return to the Projects list. The branch is listed in the Projects list.



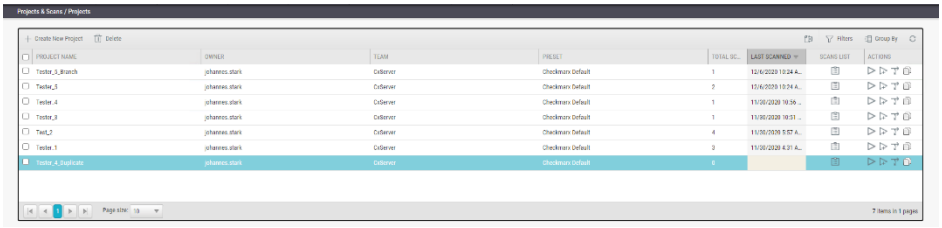
- Branched projects are not counted as additional projects according to the Checkmarx licensing structure. This means that you are not allowed to create new projects once you have reached the maximum project threshold, but you are able to open branches of existing projects without requiring additional licenses.

➢ **To duplicate a project**

1. Select the desired project from the list and click **Duplicate Project** to start.

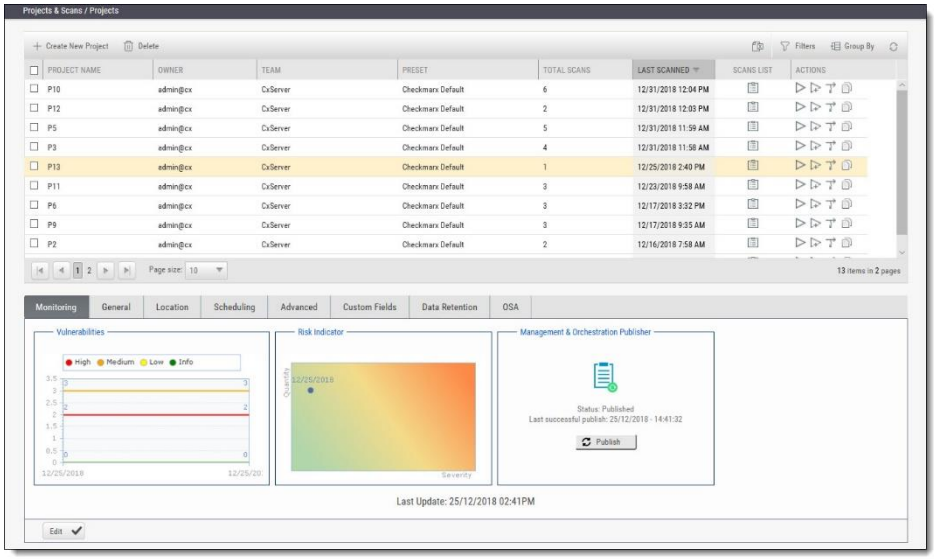


2. Continue following the instructions on creating a new project. Once completed, the new duplicated project appears listed in the Projects list.



Managing Projects and Running Scans

This section displays the user interface and explains the available tools and options.



Scan List/Actions

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

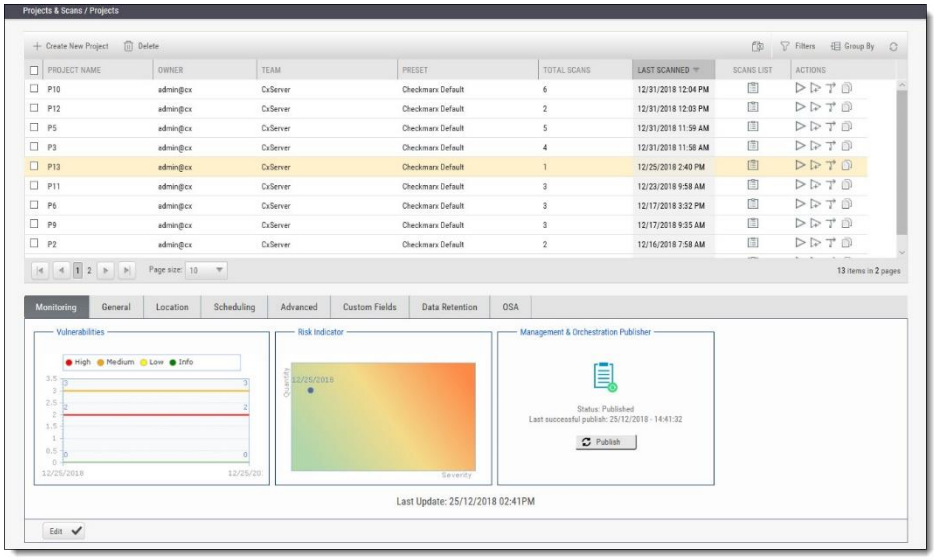
	**Scan List**	Displays the project in the individual project path, e.g. Projects & Scans/View Project Scans/My Java Projects.
	**Full Scan**	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.

	**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

If a zip file is uploaded that contains file path consisting of more than 255 characters, the file is not sent for scanning. Shorten the file path and try again.		
	**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 **Advanced Actions** (email notifications on pre-scan, post-scan and scan failure).
	**Branch Project**	Similar to copying a project, except that it copies the following set of properties: • Preset • Team Last scan from the source project with all results and remarks.

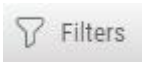
Managing Tables

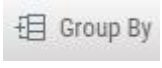
The various tables in the web interface provide navigation and pagination controls:



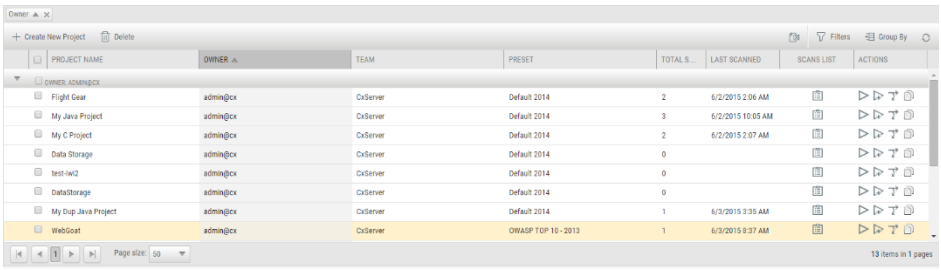
The following actions are available from the table's header bar:

- **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 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.



- 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

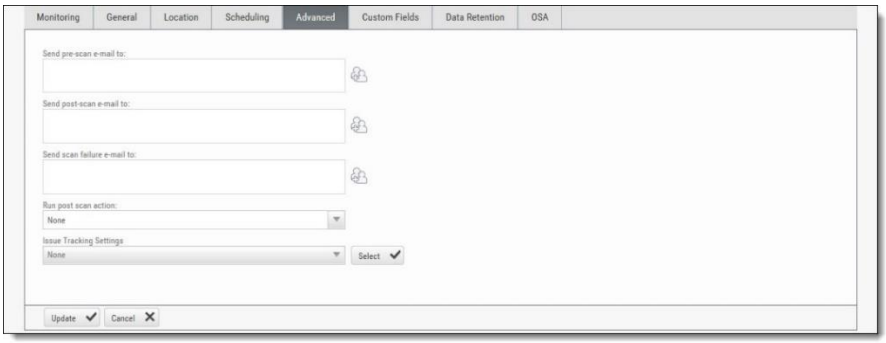
CxSAST can automatically perform configurable actions with each scan. The available types of **Advanced Actions** are:

- 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 sending automatic emails, do the following:

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



2. Click  and add recipients. Separate email addresses with semicolons (;).

- Click <**Finish**>.
  Email actions require SMTP settings to be configured.

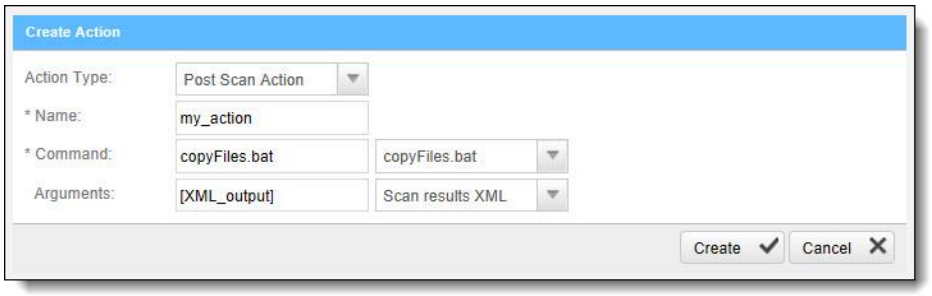
Configuring an Executable Action

To configure CxSAST to run an executable before or after a scan, do the following:

1. Upload an executable: To ensure the integrity of the system and to restrict access, executable files must be uploaded manually by approved personnel.

- The location used by CxSAST for executable files appears in **Settings > Application Settings > General > Executables Folder**.

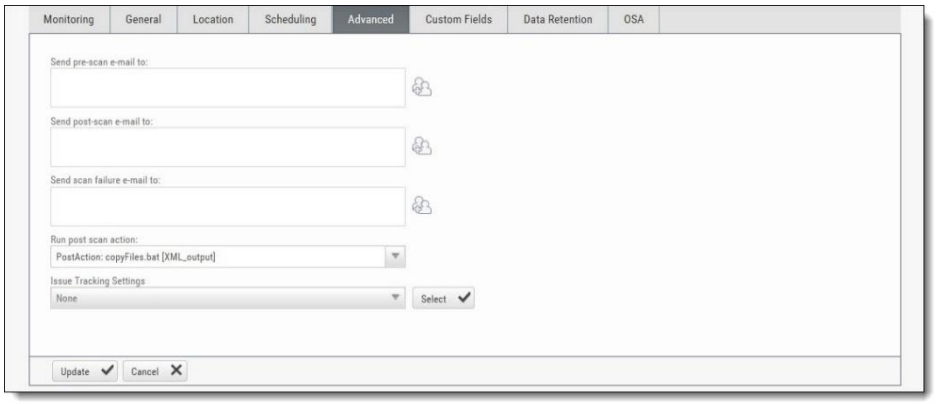
2. Define an Action for the executable: Go to **Settings > Scan Settings > Pre & Post Scan Actions > Create New Action**, and configure the following:



- **Action Type:** Pre-scan or Post-scan.
- **Name:** This will appear 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.

- The command must use the same name that is used for the file located in the 'Executables' folder as defined in **Settings > Application Settings > General > Executables Folder**. Files in the 'Executables' folder appear in the drop-down list.

3. Enter the arguments required by the command.
4. For post-scan actions, you can also select whether the scan results should be XML or CSV.
5. Assign the action to a project: In a project's Advanced Actions tab, select an action from the list:

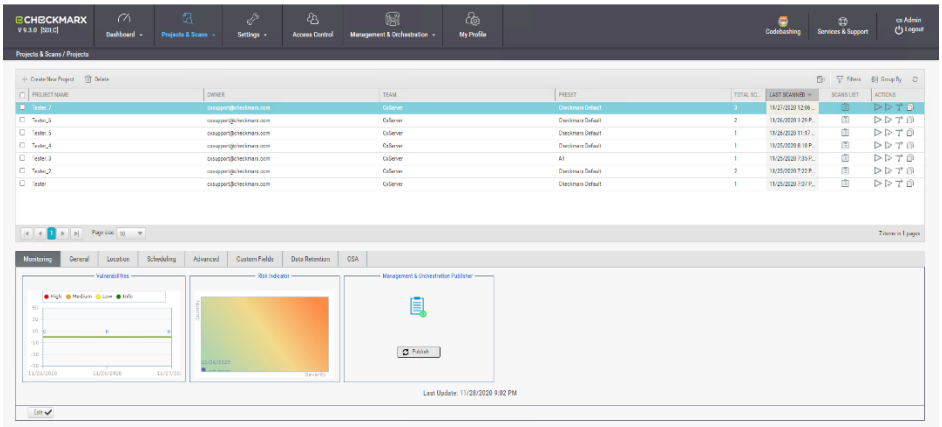


6. Click <**Finish**>.

Viewing Project Details

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

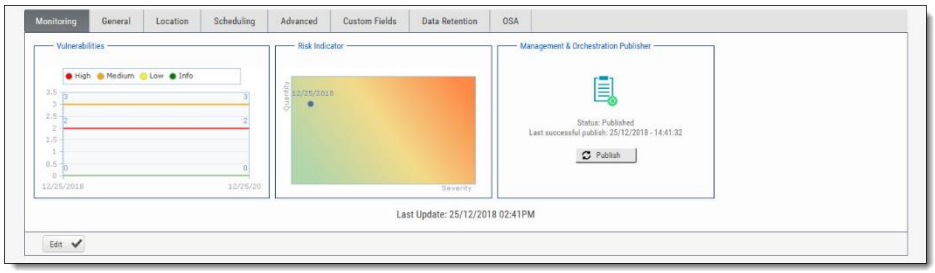
- To open the Projects window, go to **Projects & Scans > Projects**. The Projects window is displayed.



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.



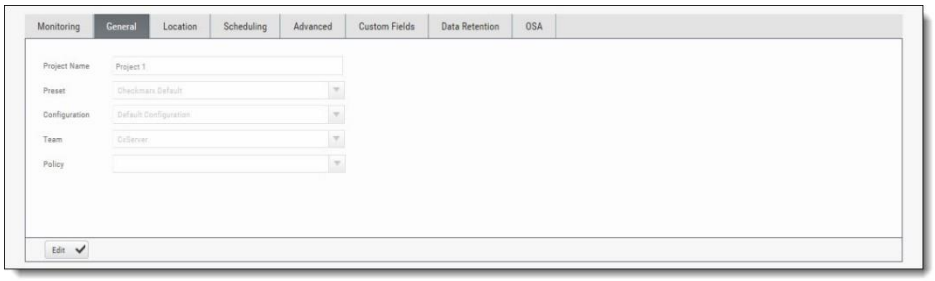
The Monitoring tab represents the evolution of the project last 10 scans focusing on the numbers of found vulnerabilities and overall risk.

- 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.

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

General Properties

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

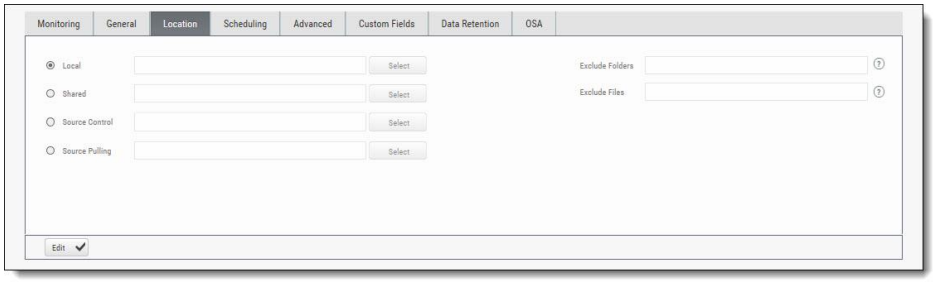


The General tab represents the project name, defined preset, configuration, associated team and policy assigned to the project.

- For more information about defining these properties refer to section about General properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Location Properties

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

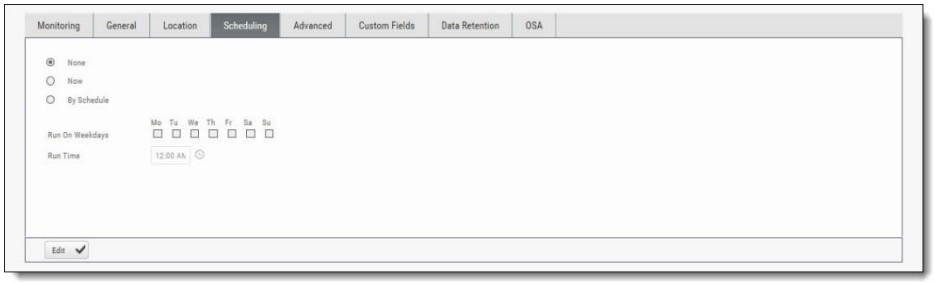


The Location tab represents the various options for locating and pulling the source code for scanning.

- For more information about defining these properties refer to section about Location properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Scheduling Properties

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



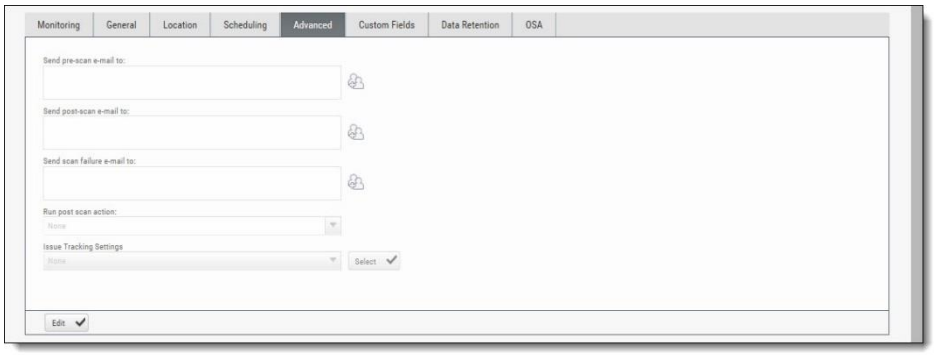
The Scheduling tab represents the various options for scheduling the automatic scans.

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.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Advanced Properties

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

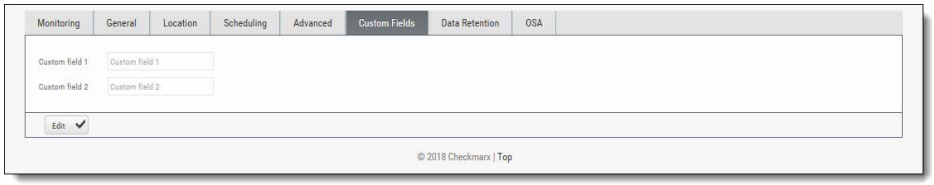


The Advanced tab represents the various options for pre/post scan actions and issue tracking settings.

- For more information about defining these properties refer to section about Advanced properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Custom Fields Properties

- 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.

- For more information about defining these properties refer to section about Custom Field properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Data Retention Properties

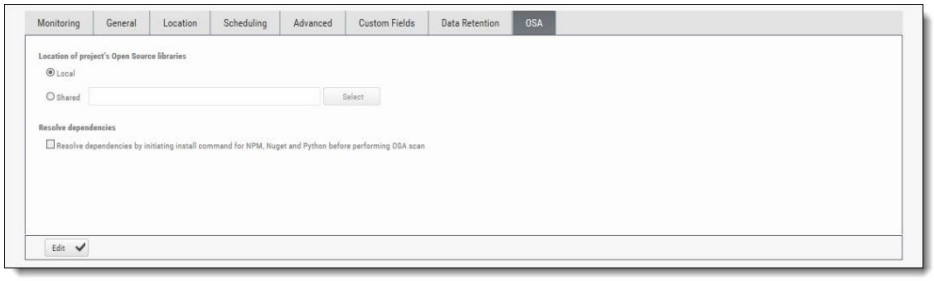
- Click the **Data Retention** tab to display its properties.

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.

- For more information about defining these properties refer to section about Data Retention properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

CxOSA Properties

- 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.

- For more information about defining these properties refer to section about Open Source Analysis properties in Creating and Configuring Projects.
- Click <**Edit**> to change settings and then click <**Update**> to save the changes.

Managing Queries

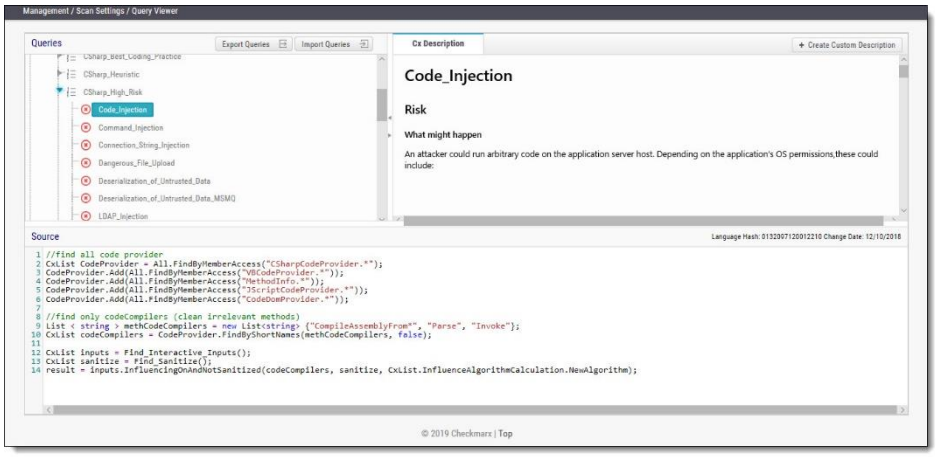
You can import and export CxSAST code queries as XML files. You can manage sets of queries known as **Presets** to be selected per-project to be used.

Viewing, Importing, and Exporting Queries

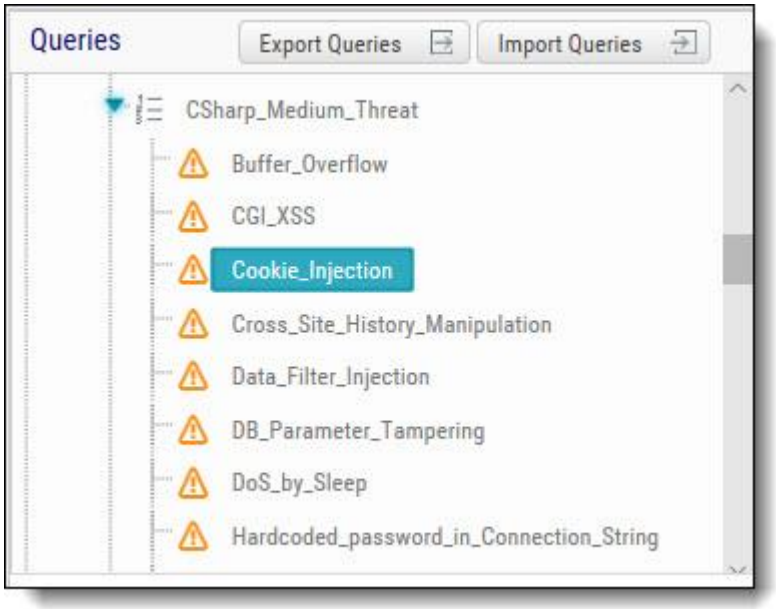
The **Query Viewer** displays all Checkmarx default queries and custom queries, with their descriptions and source code. You can import and export custom queries as XML files.

To export queries, do the following:

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



2. 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.
3. To view a query's **Description** and **Source** code, select the query.
4. Select organizational custom queries to be exported



5. Click **Export Queries**.
6. Save the exported XML file.

➢ **To import queries:**

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

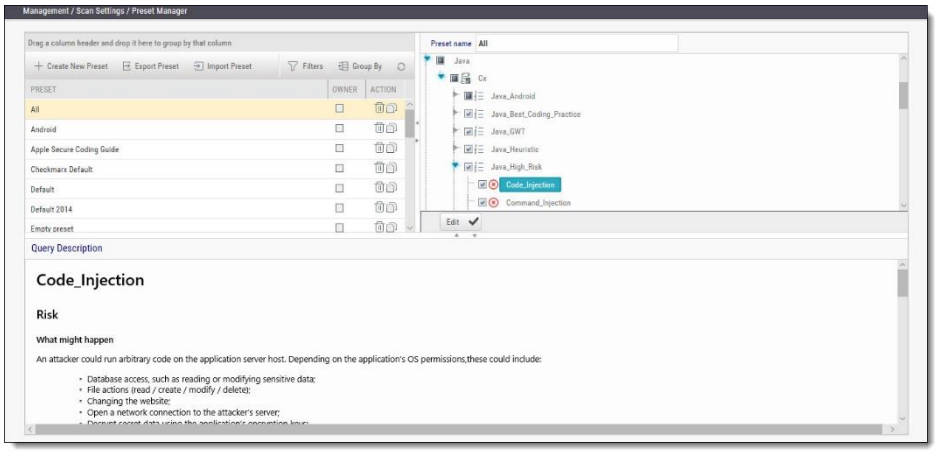
• If the imported query has the same name as an existing one, the existing query will be overridden.

Managing Query Presets (v9.0.0 and up)

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**>.



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.

➢ **To import a preset:**

1. Go to **Settings** > **Scan Settings**, and click **Import Preset**.
2. Choose the preset XML file to be imported.

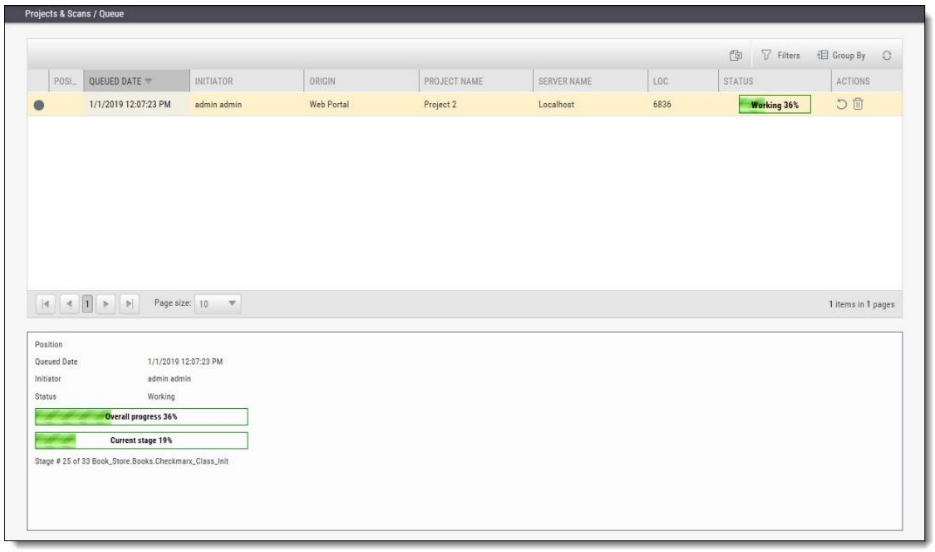
- If the imported preset includes a query that has the same name as an existing one, the existing query will be overridden.

The Queue

The Queue lists the scan that is currently queued or running and the order in which the following scans are going to be executed. You can manage the table.

➢ **To access the queue:**

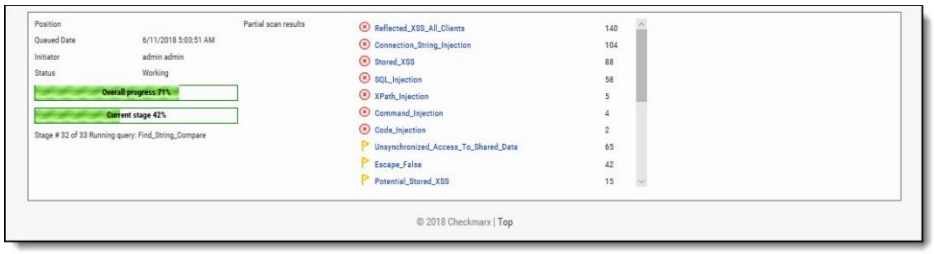
- Go to **Projects & Scans > Queue**.



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).

- 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.
- 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:



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

This chapter explains how to view and handle scan results.

Viewing Results from All Scans

You can view the results for one selected scan. Depending on your choice, you can either view a list of all scans or individually per selected project.

➢ **To view a list of all scans:**

- Go to **Projects & Scans > All Scans**. A list with all scans of all projects is displayed.

➢ **To view a list of scans for a selected project:**

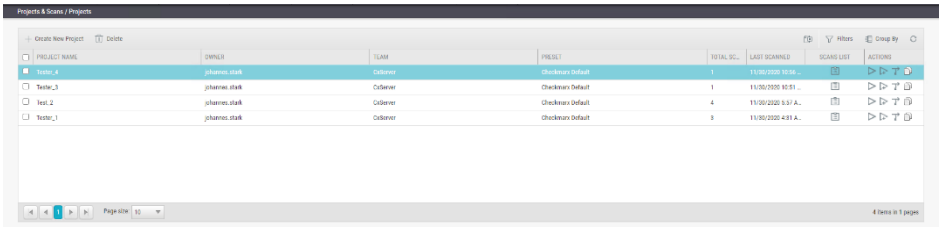
1. To view a list of all scans of one project, go to **Projects & Scans > Projects**. A list of all projects is displayed.
2. Select the desired project and display its scan list .

➢ **To view the scan results of a scan:**

- Select the desired scan from the scan list and then open the results viewer to display the results.

Projects and Scan Options

Under **Projects & Scans > Projects**, various scan and project-related actions are available. For information and instructions on creating and configuring projects, refer to Creating and Configuring Projects.

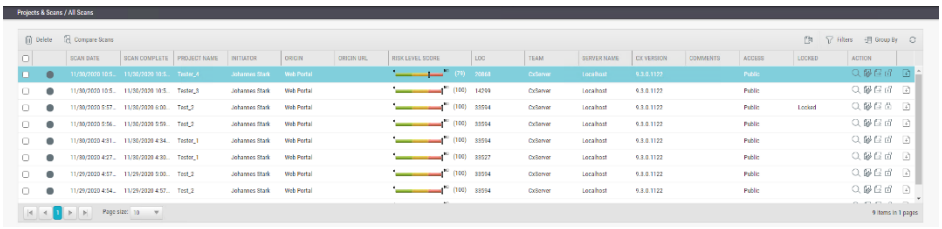


The table below illustrates and explains the content of the table columns.

Column	Action	Description
Project selector	Check to select project	Selects a project to perform one of the available actions outlined.
Project Name		Lists the name of the project.
Team		Lists the team to which this project is assigned.
Preset		The preset you selected when creating the project
Total Scans		Number of scans run for this project.
Last Scanned		Date and time of the last scan run for the project.
Scans 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	Scans the entire project. If the project is configured for a local location, you have to upload a zip file with the updated source code.
	Incremental Scan	Scans only new and modified files since the last 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

Under **Projects & Scans > All Scans**, all scan results appear in a table with each row representing an individual scan result set. You can sort tables according to **Scan Date**, **Scan Complete Date**, **Project Name** or **Risk Level Score**. Additional options are available under Managing Tables.



The list below illustrates and explains the content of the table columns.

- **Scan selector**: Check to select a scan to perform one of the available actions outlined at the bottom of this list.

- **Scan indicator**:
  - indicates a full scan
  - indicates an incremental scan
  - indicates a partial scan. Information on why only a partial scan was performed is provided in Scan Summary. For more information about partial scans, refer to the FAQ section
  - indicates scan in process
- **Scan Date**: The date when the scan was started
- **Scan Complete**: The date when the scan was completed.
- **Project Name**: The project for which the scan was performed.
- **Initiator**: The user who activated the scan
- **Origin**: The system from which the scan was activated
- **Origin URL**: The triggered URL of origin (e.g. Jenkins URL)
- **Risk Level Score**. A risk indicator bar 

indicates the overall risk calculation of all vulnerabilities found in this scan (between 0% and 100%).
- **LOC** (Lines Of Code): The number of lines that the code in the project consists of.
- **Team**: The team that the scan is assigned to
- **Server Name**: The CxEngine server that performed the scan
- **Cx Version**: The CxSAST version 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**: If a scan is locked , this column marks it as **Locked** to avoid automated purging of important scan data. Locked scans cannot be deleted. There is no entry in tis column for unlocked scans.
- **Action**. The following can be performed for selected scans:
  - displays the scan results
  - generates a scan report
  - creates a summary of the scan
  - locks the scan to prevent it from being deleted
  - downloads the scan logs for the selected scan

Summary of All Scans

- If a scan has been initiated for a non-local project or if an incremental scan has been initiated for a local project with no code changes since the previous scan, the **Comments** indicate that the scan was not actually performed.
- Under **Monitoring**, scan details are displayed for a selected scan in the table as illustrated below:

The Monitoring tab provides two graphical summaries of found vulnerabilities:

- **Top 5 Vulnerabilities**. This chart displays the five most common high and medium vulnerabilities detected in this scan.
- **Risk Indicator**. This 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 Results

- You can view the results of one scan at the time.

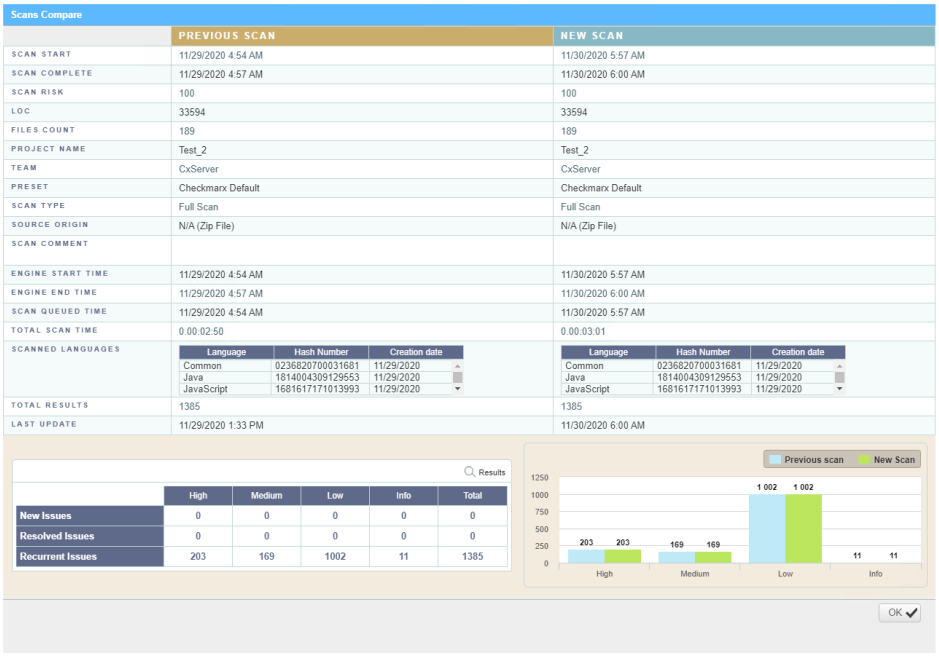
To view scan results for the desired scan, do the following:

1. Display all scans or the scans of a certain project as explained above.
2. Select the desired scan in the list and click . The scan results appear.
3. For detailed information on the scan results, refer to Navigating Scan Results.

Comparing Scans

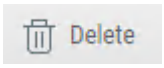
To compare two scans, do the following:

1. Display all scans or the scans of a certain project as explained above.
2. Select  two scans and click **Compare Scans**  . The Scans Compare screen is displayed.
3. Click <**Results**> in order to see a 'file compare' showing the code differences in each file, grouped by vulnerability/scan result.



Deleting Scans

Delete one or more scans as follows:

1. Select  the rows of the requested scans.
2. Click 

. You are asked to confirm your request.
3. Click <**OK**> to confirm the delete request.

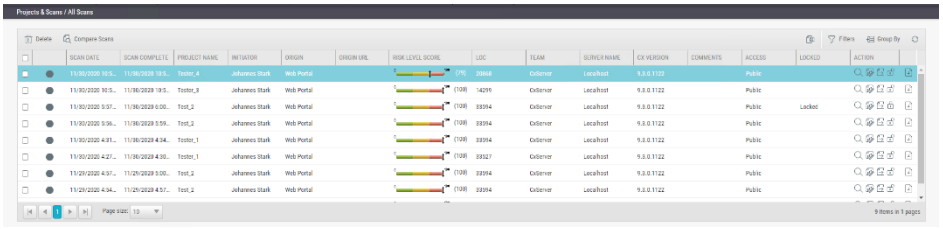
- If the user does not have the authorization required for deleting scans, no scan will be deleted.
- Locked scans are not deleted. If, for example, one scan out of three is locked  , a message appears indicating that only 2 of the 3 scans have been deleted successfully.
- To display the details of a locked scan, click **Export as CSV File**  to download the DeleteErrors.csv file, which displays the details of the locked scan.
- Unlocking all scans indicated in the report enables full deletion of the project.

Scan Result Actions

The following pages describe the scan result actions:

Navigating All Scans

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

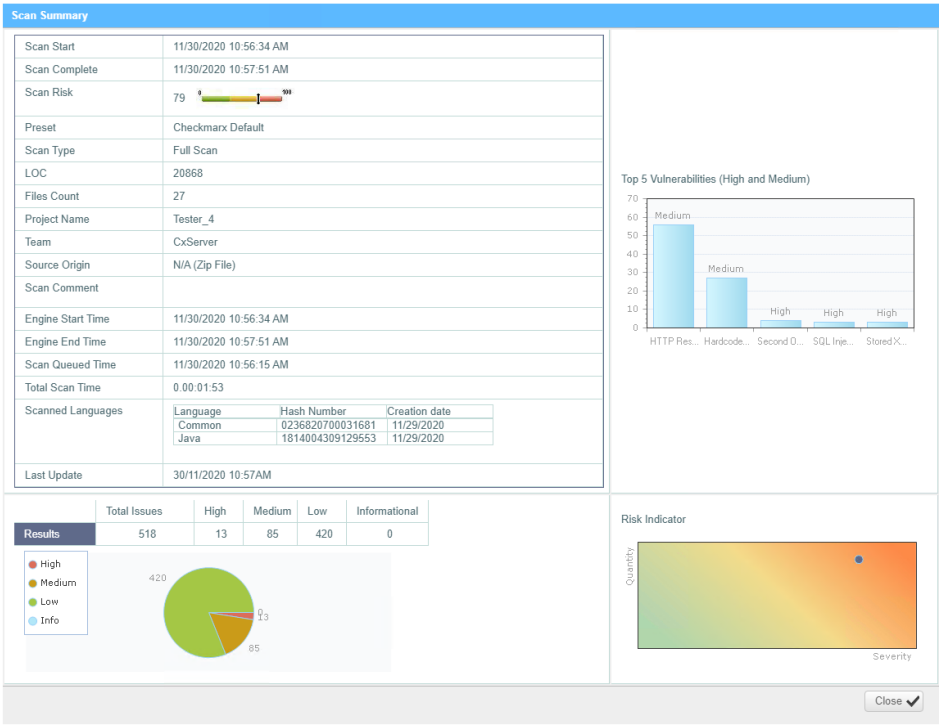


Column	Action	Description
Action		View Scan Results
		Create Report
		Open Scan Summary
		Download Scan Logs (requires the 'download_scan_log' permission)

Viewing the Scan Summary

You can view the scan summary as follows:

1. Under **Projects & Scans > All Scan**, click **Open Scan Summary** . The Scan Summary window is displayed.



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.

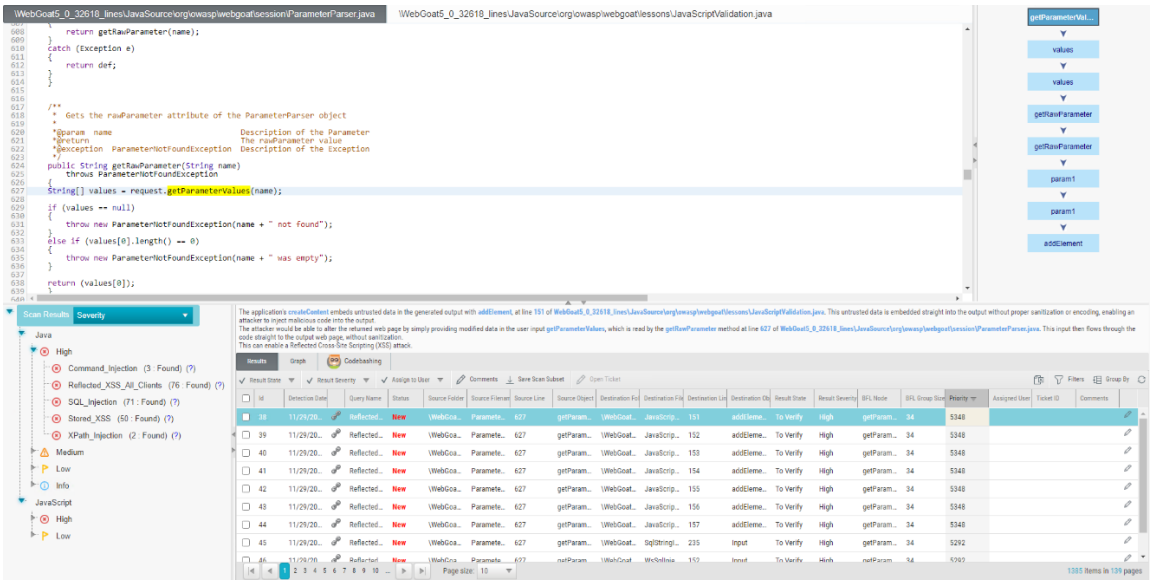
Navigating Scan Results

When viewing scan results in the web interface, the scan results overview appears and you can browse through the results The scan results summary consists of four panes with various levels of information as illustrated below. You can drill down from a comprehensive list to the actual code elements by moving through the panes in the order outlined below.

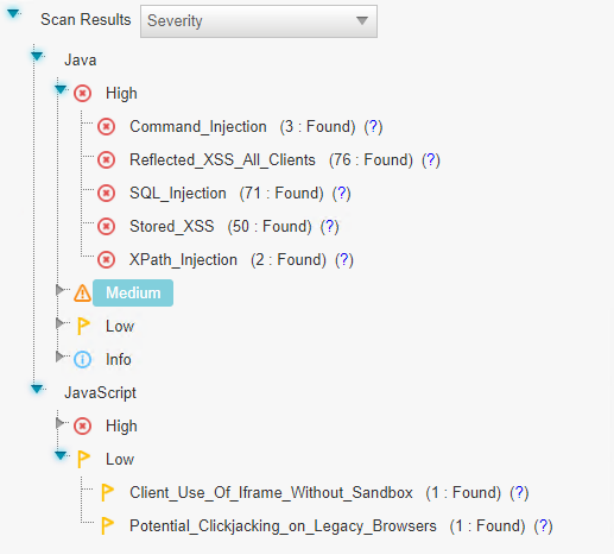
The result summary is divided into the following four panes:

- **Code Pane**. Displays the code with detected vulnerability highlighted in the code.
- **Path Pane**. Displays the full path of 'vulnerable' code elements with
- **Queries Pane**. Defines how to present the query results.
- **Results Pane**. Displays the result as table or graph. In addition, background information is available on detected vulnerabilities.

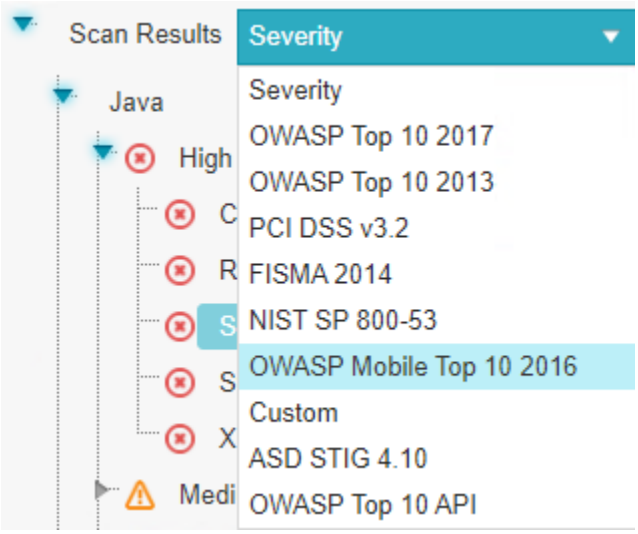
- The Queries pane is covered first as it defines how results are presented. The Queries pane is followed by the Results pane as you have to select the results here to locate them in the code and gain additional information.



Lower left pane: Each item in the list is a specific type of vulnerability for which CxSAST queries the scanned code. Each item is listed with the number of detected instances of the respective vulnerability. The queries are sorted by code language, category, and severity.



The drop-down menu lets you select the desired method for displaying the detected vulnerabilities as illustrated below.

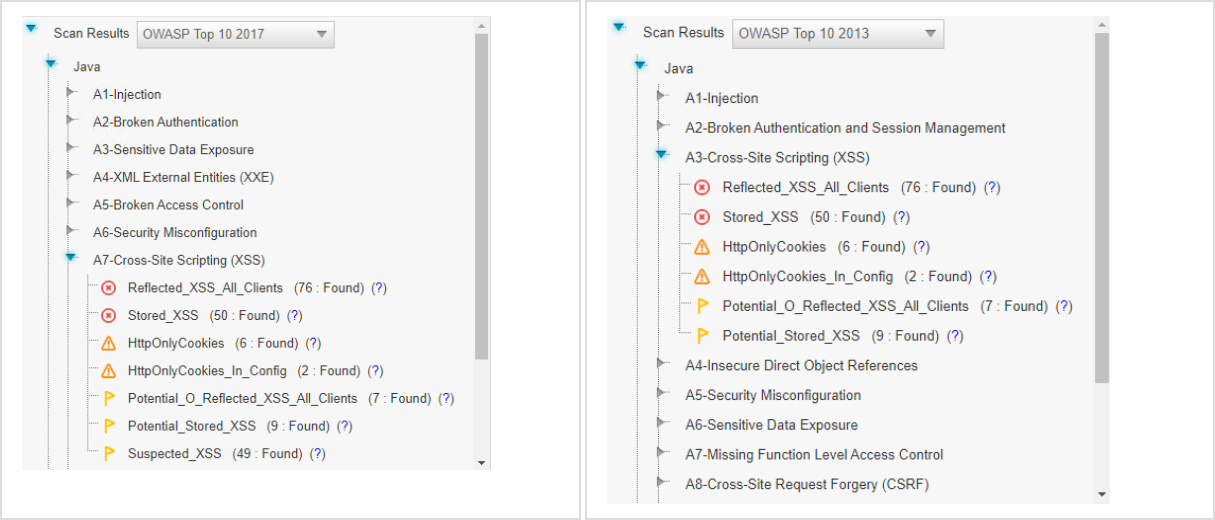


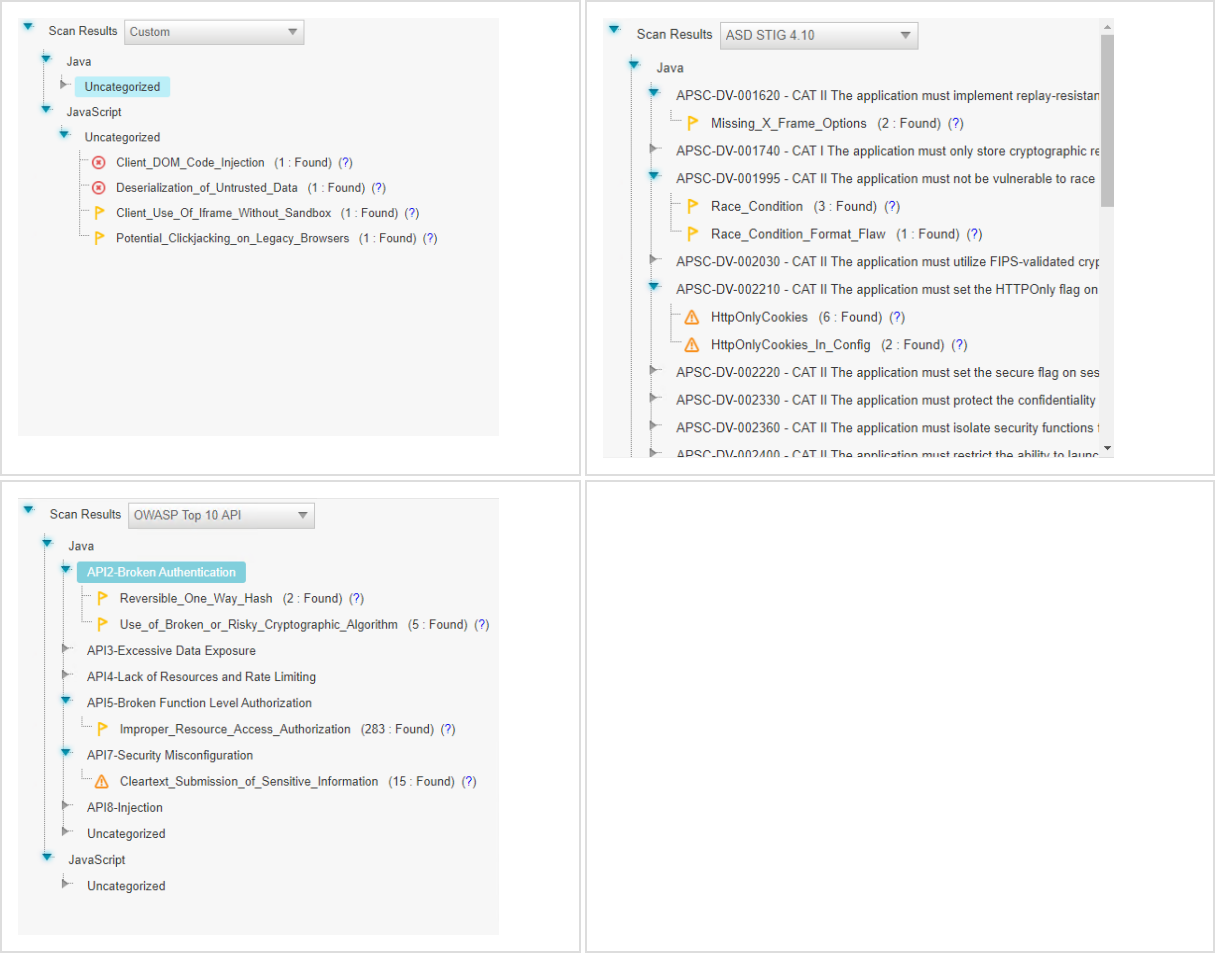
- **Severity** - displays application security risks (vulnerabilities) by severity (**High**, **Medium**, **Low** and **Info**).

- **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 listed as **Uncategorized**.
- **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 listed as **Uncategorized**.
- **PCI DSS v3.2** - 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 listed as **Uncategorized**.
- **FISMA 2014** - 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 listed as **Uncategorized**.
- **NIST SP 800-53** - 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 listed as **Uncategorized**.
- **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 listed as **Uncategorized**.
- **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.
- **ASD STIG 4 10** - displays vulnerabilities categorized by the DISA Application and Development STIG once the STIG post-installation script has been run.
- **OWASP Top 10 API**

The following images illustrate the methods for displaying the detected vulnerabilities.

To learn more about each vulnerability, click **(?)** to view additional information on it provided by Codebashing.


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 (76 : Found) (?)
Stored_XSS (50 : Found) (?)
HttpOnlyCookies (6 : Found) (?)
HttpOnlyCookies_In_Config (2 : Found) (?)
Potential_O_Reflected_XSS_All_Clients (7 : Found) (?)
Potential_Stored_XSS (9 : Found) (?)
Suspected_XSS (49 : Found) (?)
Scan Results
OWASP Top 10 2013
Java
A1-Injection
A2-Broken Authentication and Session Management
A3-Cross-Site Scripting (XSS)
Reflected_XSS_All_Clients (76 : Found) (?)
Stored_XSS (50 : Found) (?)
HttpOnlyCookies (6 : Found) (?)
HttpOnlyCookies_In_Config (2 : Found) (?)
Potential_O_Reflected_XSS_All_Clients (7 : Found) (?)
Potential_Stored_XSS (9 : 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
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 (76 : Found) (?)
Stored_XSS (50 : Found) (?)
HTTP_Response_Splitting (10 : Found) (?)
HttpOnlyCookies (6 : Found) (?)
HttpOnlyCookies_In_Config (2 : Found) (?)
Potential_O_Reflected_XSS_All_Clients (7 : Found) (?)
Potential_Stored_XSS (9 : Found) (?)
PCI DSS (3.2) - 6.5.8 - Improper access control
Scan Results
FISMA 2014
Java
Access Control
Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKey (2 : Found) (?)
Incorrect_Permission_Assignment_For_Critical_Resources (19 : Found) (?)
Configuration Management
Identification And Authentication
Media Protection
System And Information Integrity
Uncategorized
JavaScript
Configuration Management
Uncategorized
Scan Results
NIST SP 800-53
Java
AC-3 Access Enforcement (P1)
SC-13 Cryptographic Protection (P1)
Use_of_a_One_Way_Hash_with_a_Predictable_Salt (8 : Found) (?)
Reversible_One_Way_Hash (2 : Found) (?)
Use_of_Broken_or_Risky_Cryptographic_Algorithm (5 : Found) (?)
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)
Scan Results
OWASP Mobile Top 10 2016
Java
M7-Client Code Quality
Command_Injection (3 : Found) (?)
SQL_Injection (71 : Found) (?)
Input_Path_Not_Canonicalized (10 : Found) (?)
M9-Reverse Engineering
Uncategorized
JavaScript
Uncategorized



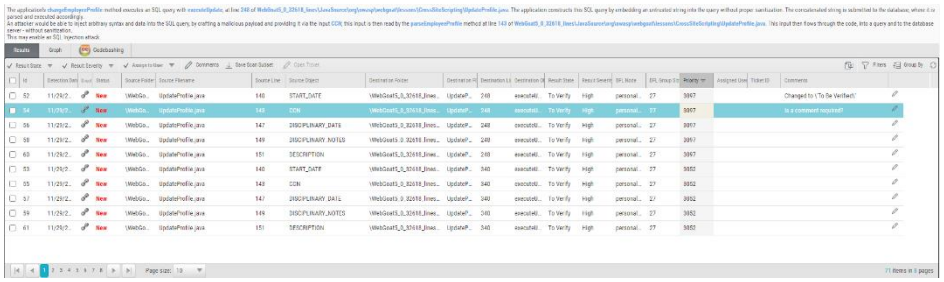
Results Summary

Lower right pane: The lower right section hosts the result summary with tutorial as follows:

- **Results**: View a list of detected vulnerabilities and select them for further action.
- **Graph**: View a graphical display that displays affected code elements and the relationship between them.
- **Codebashing**: Learn more about detected instances using Codebashing.

Results

To view a list of detected instances and details, select **Results**. The highlighted instance's code element details appear at the top. You can navigate the results using pagination controls.



Select an instance node (Graph tab) or a listed result (Results tab) to change the following (depending on your user permission):

Result State	Useful for disregarding false positives or just for planning what issues to handle • **To Verify** (default) – instance 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. • **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. • 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. • When the state of an instance is changed (for example 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. If enabled, issuing a comment is required when either changing the state of scan results to **Not Exploitable** or to any different severity change, depending on the option you enabled.
Result Severity	Useful for defining the priority level of the selected issue. • **High** • **Medium** • **Low** • **Info**

Assign to User	Useful for planning who should handle the selected issue.
Comments	Add a comment to an instance. This metadata is maintained for the project when performing future scans and for instances that continue to be found. When adding a comment, it is logged with date and time into the comment history.
Save Scan Subset	Use this option for selected instances to appear in the results list as an independent result set.
Open Ticket	Click to open a ticket in a bug tracing system, for example in Jira.

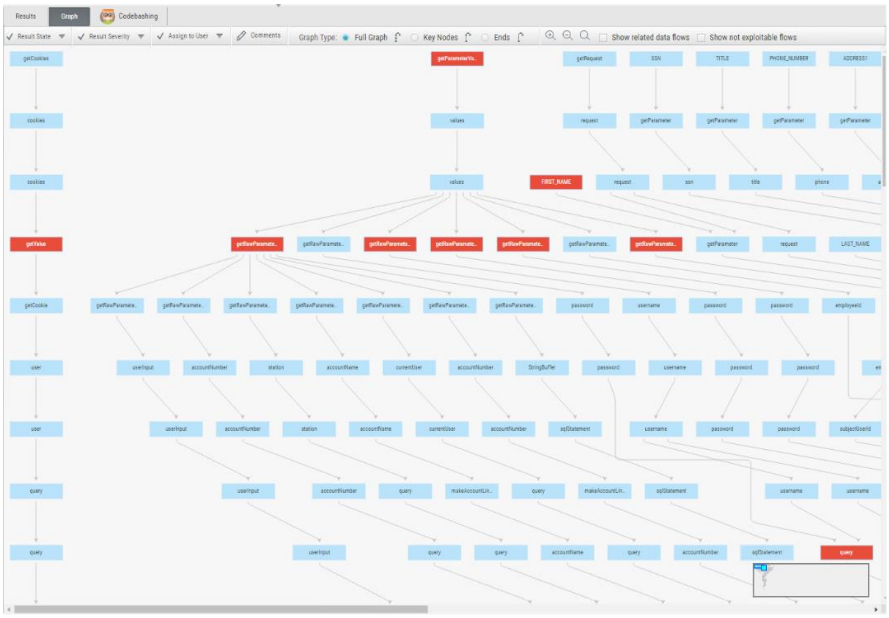
The results are listed with the following parameters:

- Selector: Check to select the desired result to perform the tasks listed above.
- **Id**: The ID of the respective scan.
- **Detection Date**: The date on which the vulnerability was detected for the first time in the scanned code.
- **Direct**: Click to copy the direct URL of this vulnerability to the clipboard. You are able to log on from a different host and directly access CxSAST and this vulnerability report.
- **Query Name**: The name associated with the query of the source code.
- **Status**: The status of the result, for example **New** (newly detected).
- **Source Folder**: The folder of the resource with the detected vulnerability.
- **Source File Name**: The name of the resource file in which the vulnerability was detected.
- **Source Line**: The line number in the source code where the vulnerability was detected.
- **Source Object**: The object where the vulnerability was detected. Once you select the list entry, the object appears highlighted in the resource available in the upper left window.
- **Destination Folder**: The destination of the resource.
- **Destination File Name**: The name of the destination file for the resource with the vulnerability.
- **Destination Line**: The line number in the destination.
- **Destination Object**: The destination object, for example the output of the source.
- **Result State**: The status of the result. The result state can be updated. For available status options, refer to the table above. Updating the result state automatically adds a comment to the comment section.

- **Result Severity**: The severity of the result. The severity can be updated. For available severities, refer to the table above. Updating the result severity automatically adds a comment to the comment section.
- **BFL Node**: BFL stands for Best Fix Location. This parameter defines the node where the fix of the vulnerability should be implemented.
- **BFL Group Size**: Defines the group size that the fix should have.
- **Priority**: Defines the priority at which the vulnerability should be handled.
- **Assigned User**: Lists the user to whom this vulnerability has been assigned. To assign a user, refer to the table above.
- **Ticket ID**: The ID of the ticket, if assigned. For additional information on opening a ticket, refer to the table above.
- **Comments**: Free text you may add. If updating result severity or result state, a comment is added automatically. To add a comment, click  and enter the comment into the Comment field. Once the comment is saved, it is logged with date and time under **Comments History**.

Graph

To display the first and last code elements of each detected instance with the relationships between them, select **Graph**.



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.

Codebashing

To learn more about code vulnerabilities, why they happen, and how to eliminate them, select **Codebashing** to enter the interactive Checkmarx learning platform. Codebashing provides developers with an in-context learning platform that helps understand vulnerabilities and write secure code. Codebashing comes as a free version with basic capabilities. Additional learning material and in-depth information is available with the full version.

The free edition of Codebashing covers the following:

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

The full version includes over 20 lessons and additional languages:

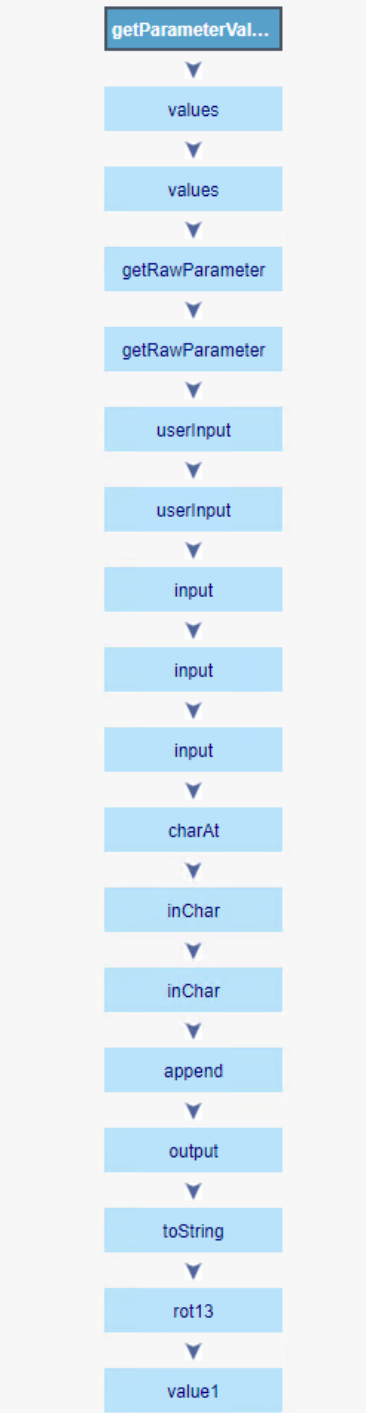
- **Lessons**: Session fixation, Use of insufficiently random values, Reflected XSS, Command Injection, DOM XSS, Directory (Path) Traversal, Privileged Interface Exposure, Leftover Debug Code, Session Exposure in URL, User Enumeration, Horizontal Privilege Escalation, Vertical Privilege Escalation, Authentication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

The Path Pane

The Path Pane displays the full path of code elements that constitute the vulnerability instance selected in the **Results** pane. This path represents the full attack vector for the vulnerability instance.

➢ To view the attack vector:

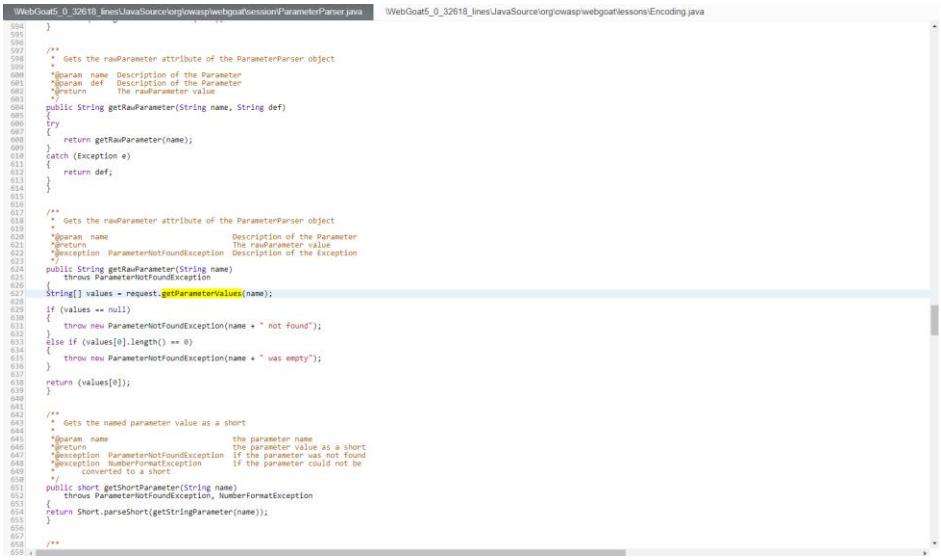
- Select an instance in the **Results** pane (**Results** or **Graph** tab) and view its attack vector in the **Path** pane. The code line containing the element that has been selected in the **Path** pane is highlighted.



- 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.
- When using the CxSAST IDE plugins, you can immediately fix the code in place!

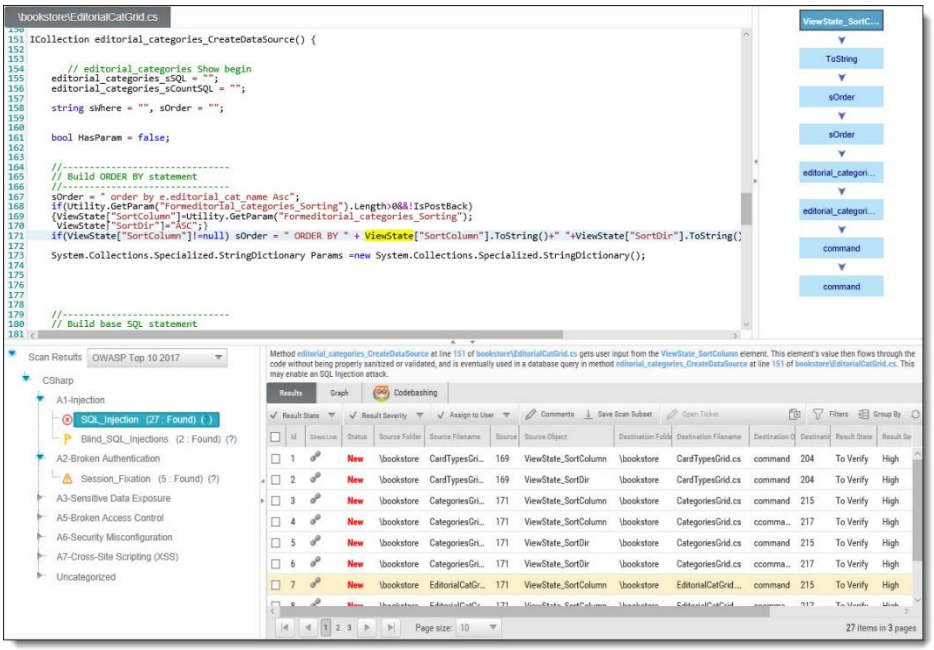
The Code Pane

The Code Pane displays the source code of your scanned resource with the detected vulnerabilities marked. Use the Path pane or Results pane to highlight detected vulnerabilities in the code.



Scan Results Example

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



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.

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

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.

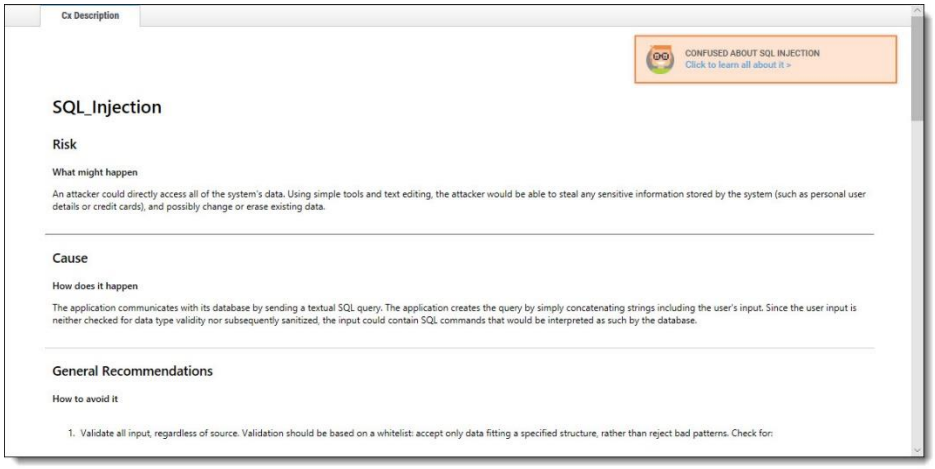
Codebashing is currently available as a free limited edition to all users. This version includes a free edition of Codebashing covering:

- **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 full general information for the SQL_Injection, including risk, cause and recommendations with code examples.



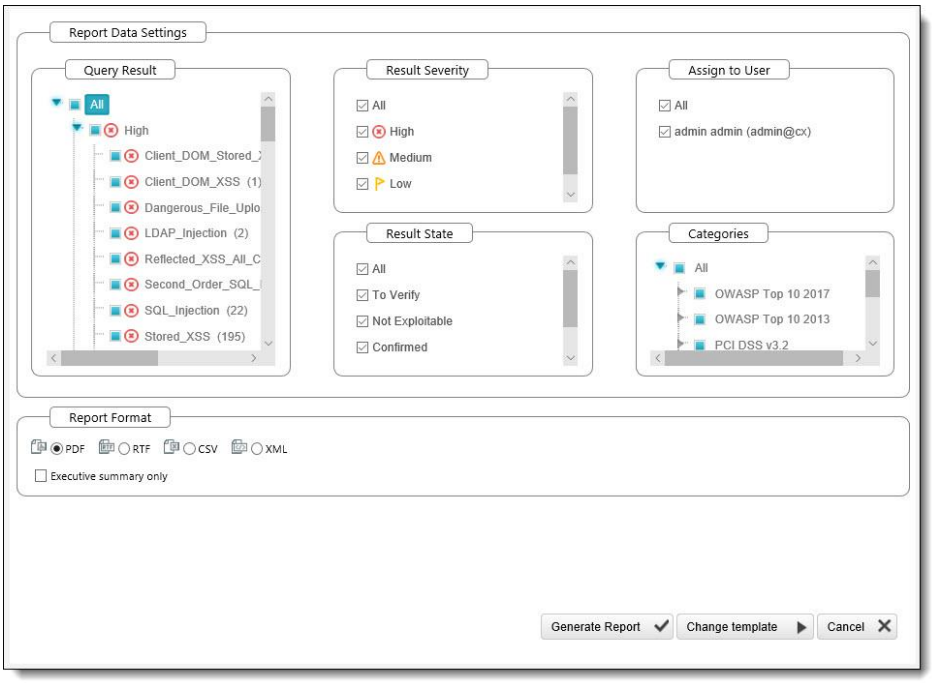
Selecting a specific instance of the vulnerability in the **Results** pane (bottom, center and right) displays the instance's code details at the top of the pane, and displays the path of component code elements in the **Path** pane (top-right). The Path pane shows all the code elements leading from 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, select the desired scan and click **Create Report** . The report settings are displayed.



2. Filter the results for the generated report and select the report file format. To filter the results, clear the report data settings that you don't want and keep only the desired ones checked. The report data settings are the following ones:
    - **Query Results**: Select or clear query results such as **SQL_Injection**, **LDAP_Injection** etc. sorted according to their severity.
    - **Result Severity**: Select or clear the severity, which means **High**, **Medium**, **Low**, **Info**.
    - **Result State**: Select or clear the result status.
    - **Assign to User**: Select or clear to show reports assigned to specific users only.
    - **Categories**: Select or clear to select report categories.

- By default, all report data settings are selected to be included in the report.

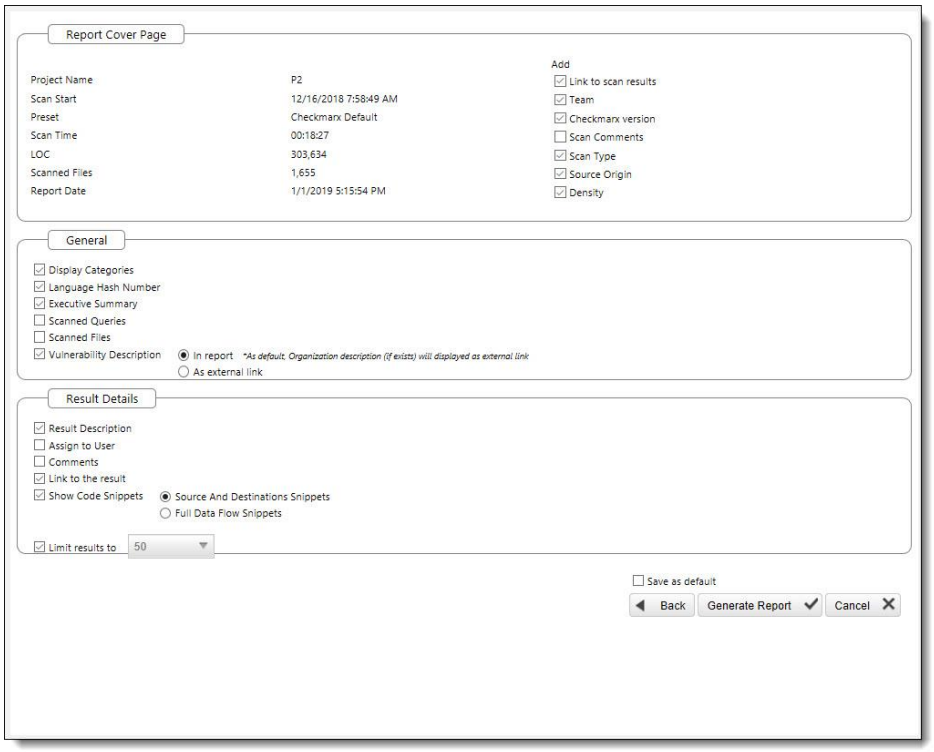
➢ **To customize categories:**

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

3. 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.

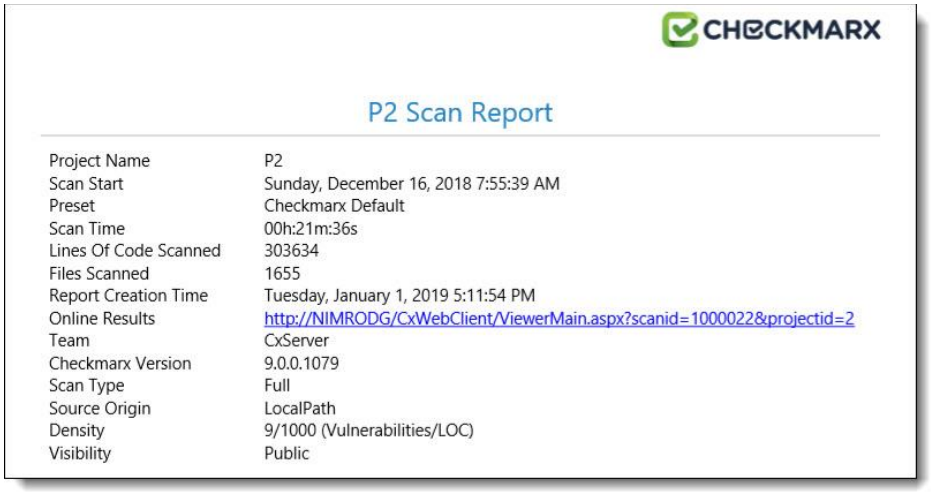
➢ **To change the report template:**

1. Click <**Change Template**>. The template setting are displayed.



2. Select the details to be presented on the report cover page, in the report itself and the details to be shown for each result.
3. Select **Save as default** 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 in the Scan Report section at the beginning of the PDF file, as illustrated below.



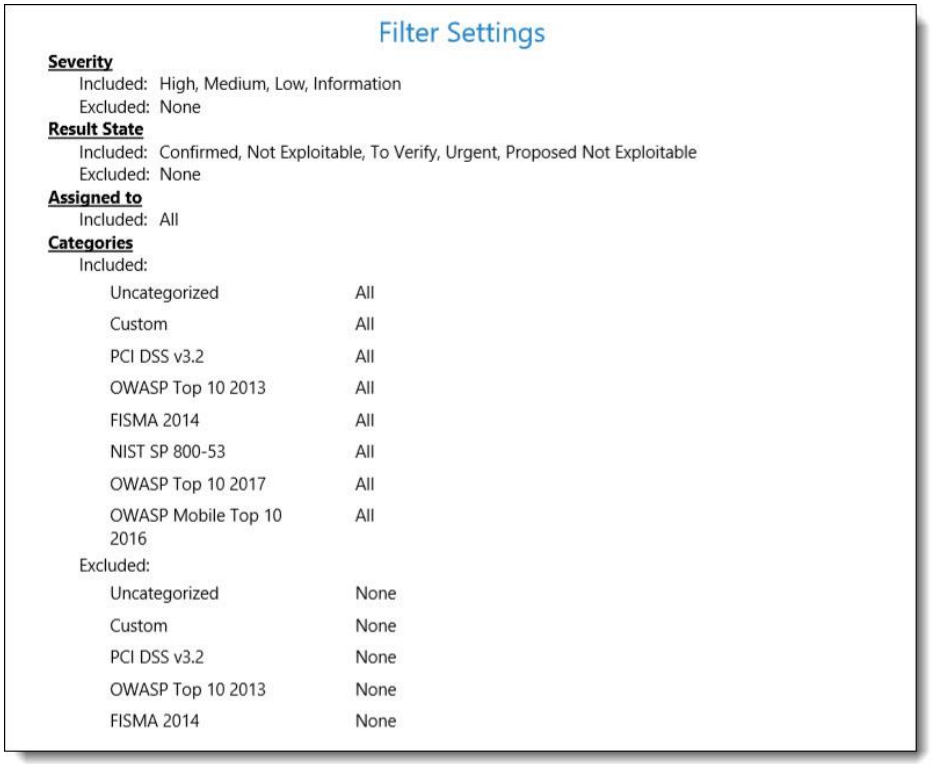
CHECKMARX

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 in the Filter Setting section, as illustrated 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

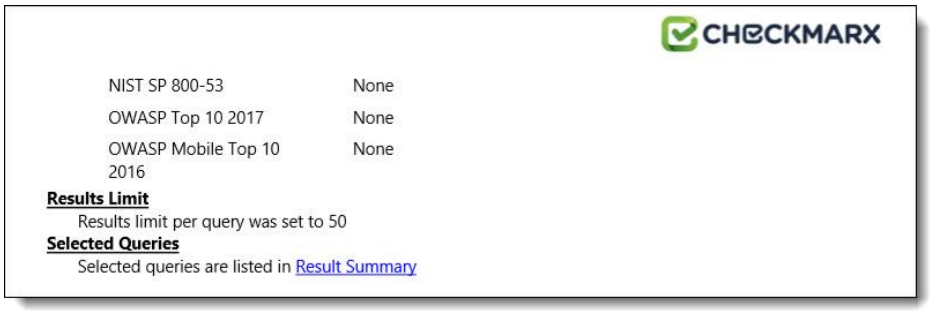
Assigned to
Included: All

Categories
Included:

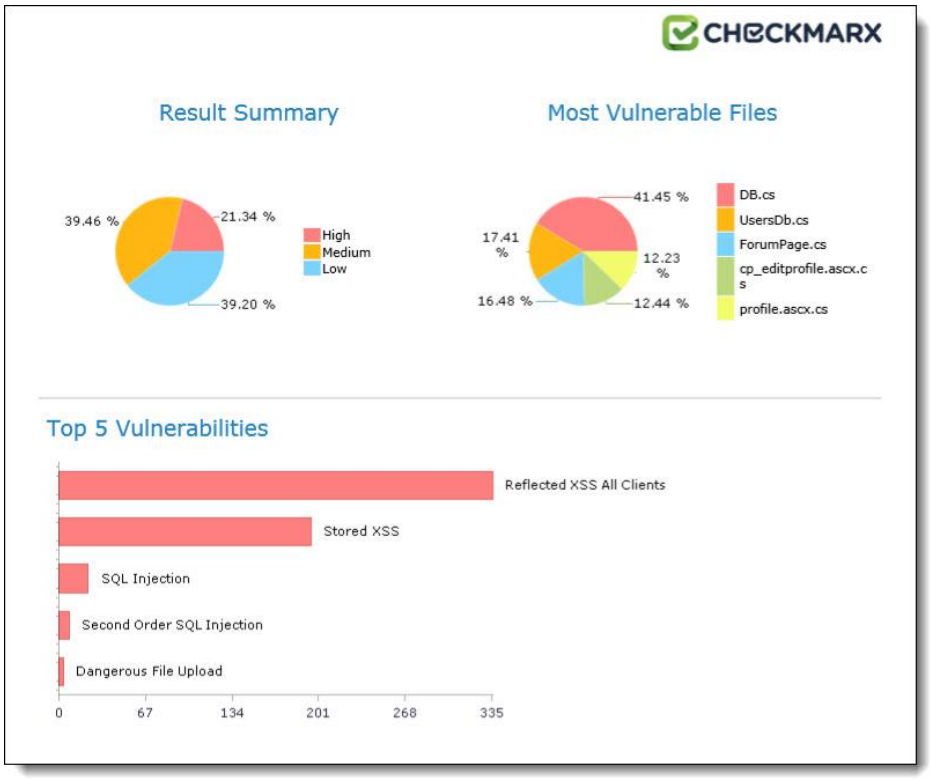
Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

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



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

CHECKMARX

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.

CHECKMARX

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.

CHECKMARX

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

CHECKMARX

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.

CHECKMARX

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 list is a basic description of the fields provided in the .csv report result, which is generated by **Create Report**, if the selected format is **.csv**:

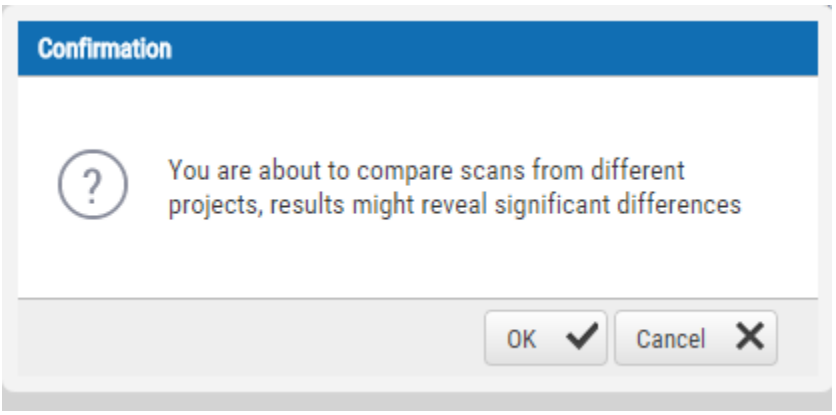
- **SrcFileName** – file name of the first node of the result
- **Line** – line of the first node of the result
- **Column** – column of the first node of the result
- **NodeId** – internal id to be able to identify the query in the first node
- **Name** – text of the first node of the result
- **DestFileName**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

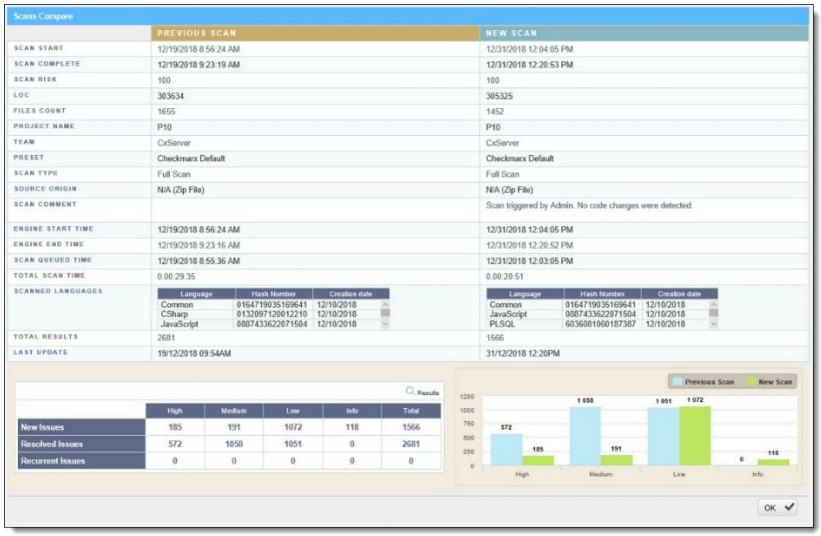
You can now compare the results of two scans in separate projects. CxSAST provides a summary of differences, and an interactive interface similar to the interface for results of single scan.

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"



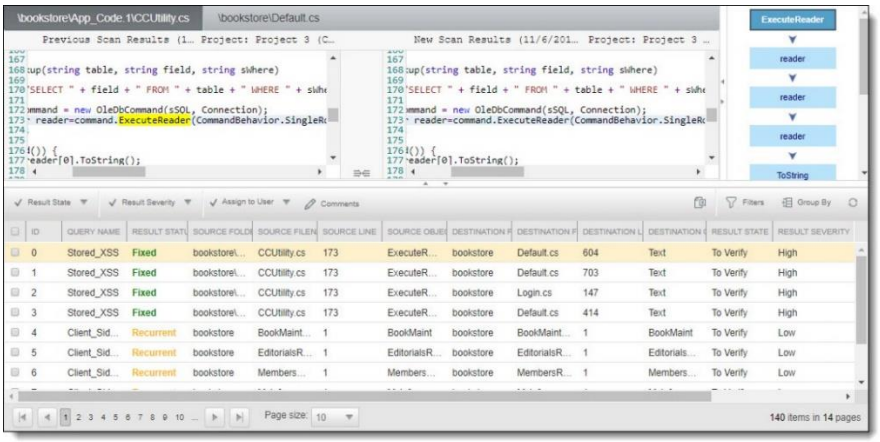
A comparison summary is displayed:



The comparison summary includes the following:

- 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:



Displaying CxSCA Scan Results in CxSAST

- Support for displaying CxSCA scan results in CxSAST is going to be added by a hotfix. Make sure to have always the latest available hotfix installed.

To enable users to easily compare scan results generated with scans by two different engines, it is now possible to display CxSCA results in the summary page of CxSAST. To display the CxSCA results in CxSAST, do the following:

1. Enable the option by editing the **IsScaEnabled** feature flag in the database.
2. Enable your user to log in to CxSAST and CxSCA by setting up the Primary Access Control.
3. Define the CxSCA URL and the tenant name in CxSAST.
4. To view scan results of CxSCA in CxSAST, log in to CxSAST and, from the menu, select **Dashboard > Projects State**.

Enabling Displaying CxSCA in the Database

You have to first enable this option in the database as follows:

1. Open **SQL Server Management Studio**.
2. In the Object Explorer, navigate to **Databases > CxDB > Tables > dbo.CxComponentConfiguration**.
3. Right-click **dbo.CxComponentConfiguration** and select **Edit Top 200 Rows**. The associated keys appear listed.
4. Navigate to **IsScaEnabled** and set it to **true**.

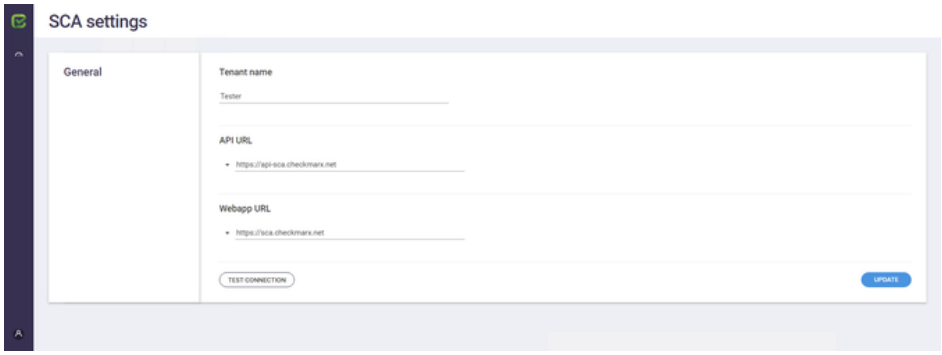
Enabling Access Control to Authenticate Users for CxSAST and CxSCA

In a second step, you have to enable Access Control to authenticate users for CxSAST and CxSCA at the same time by setting up the Primary Access Control as explained.

Defining the CxSCA Properties in CxSAST

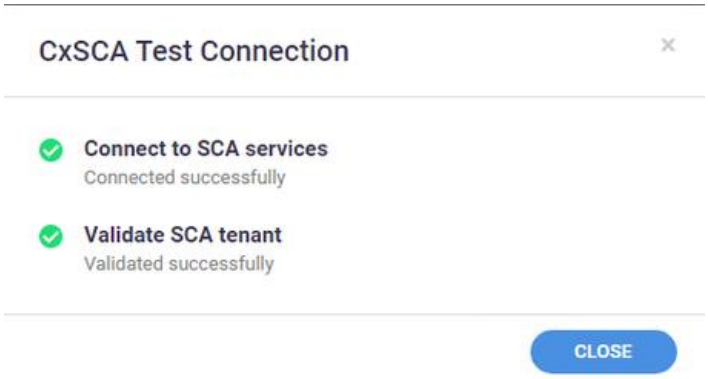
By default, CxSAST displays the CxOSA settings on the dashboard, if the license for CxOSA was accepted. Users can choose to display CxSCA results in this space instead. To do so, you have to define the CxSCA URL and the tenant name in CxSAST as follows:

1. In CxSAST, from the menu, go to **Settings > Application Settings** and select **SCA Settings** from the menu.



- If **OSA Settings** is displayed instead, this feature has not been enabled in the database.

2. Edit the SCA text display according to the feature flag configuration.
3. Under **Webapp URL**, enter the CxSCA URL.
4. Under **Tenant Name**, enter the tenant name.
5. Click <**TEST CONNECTION**> to verify that your settings are correct.



6. Click <**CLOSE**> and refresh the page.

All connection test results must be labeled for the CxSCA results to be displayed on the Dashboard.

Viewing the CxSCA Results in CxSAST

If enabled and configured as explained in this section, a summary of results obtained by scanning source code in CxSCA is displayed side by side with a summary of CxSAST scan results in the CxSAST Dashboard as illustrated in this section.

By default, a summary or place holder of CxOSA scan results is displayed.

Requirements

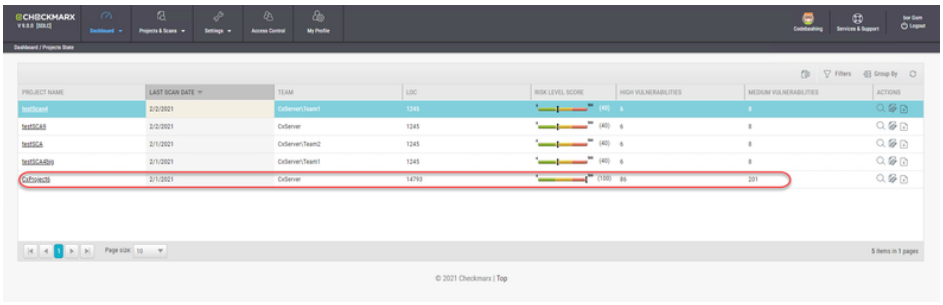
To view summaries of CxSAST and CxSCA results side by side in the CxSAST Dashboard, the following is required:

- The user must have a license activated for both CxSAST and CxSCA.
- The respective projects in CxSAST and CxSCA must have the same name.
- Both projects must have been scanned by CxSAST and CxSCA.
- The relevant CxSAST user must have full access to CxSCA.
- Displaying CxSCA must be enabled in the database as explained above.
- Access Control must be configured to log in to both CxSAST and CxSCA.

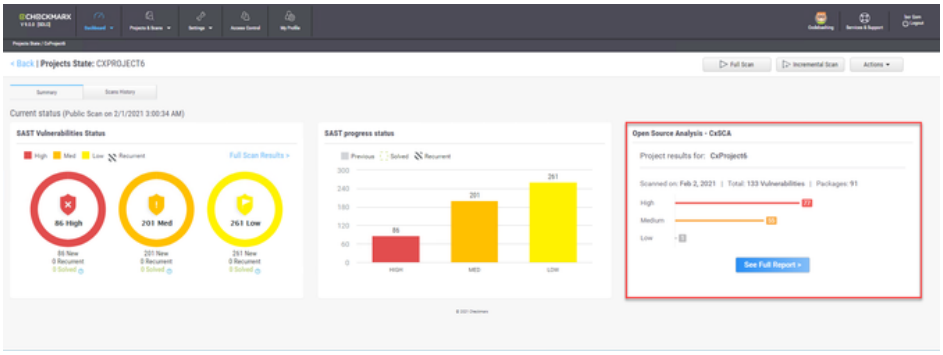
Displaying the Summary for CxSAST and CxSCA

To display the summary of test results for CxSAST and CxSCA, do the following:

1. Log in to CxSAT and CxSCA using the Primary Access Control that you configured earlier.
2. Go to **Dashboard > Projects State**.



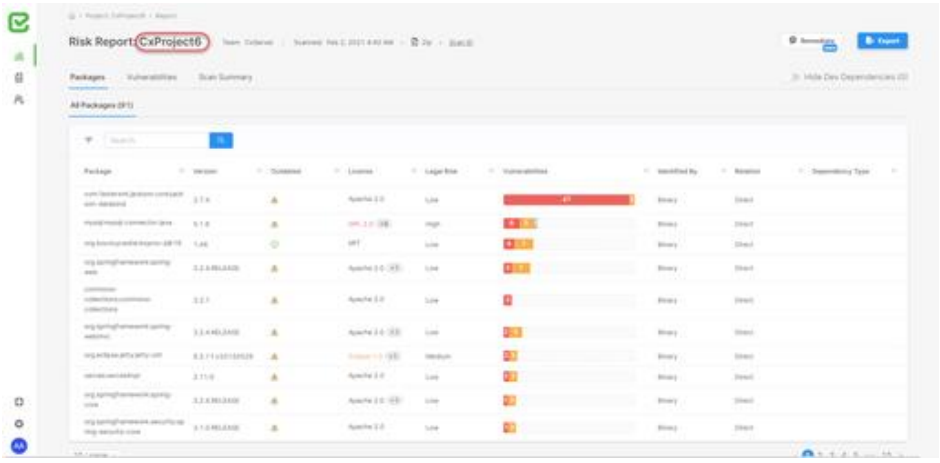
3. Click the project for which you want to view the scan summaries, for example **CXPROJECT6**. The scan summary appears for both the CxSAST and the CxSCA scans.



Full Report for the CxSCA Results

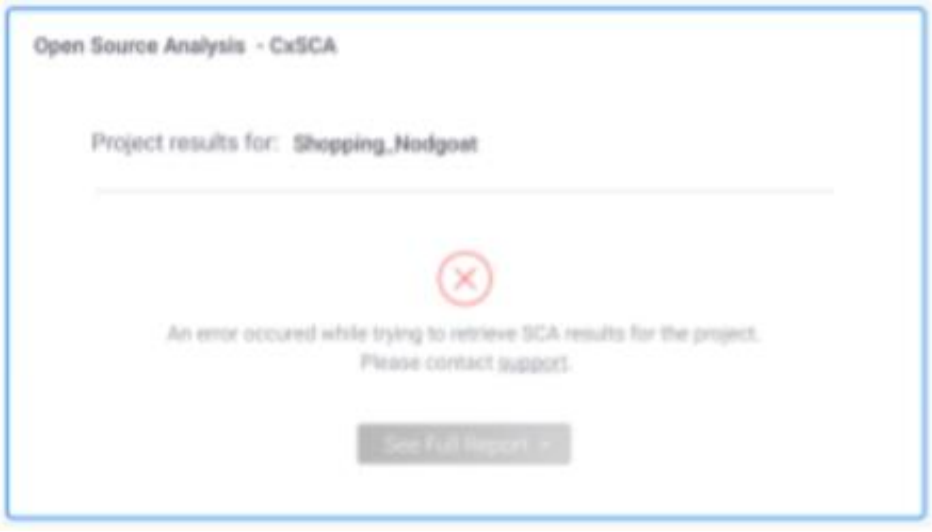
➢ **To view a full report for the CxSCA results, do the following:**

1. Click <**See Full Report**>. The CxSCA application opens in a new tab with a full report on the selected project, for example **CXPROJECT6**.
2. For additional information and instructions on working with CxSCA, refer to the CxSCA Documentation.



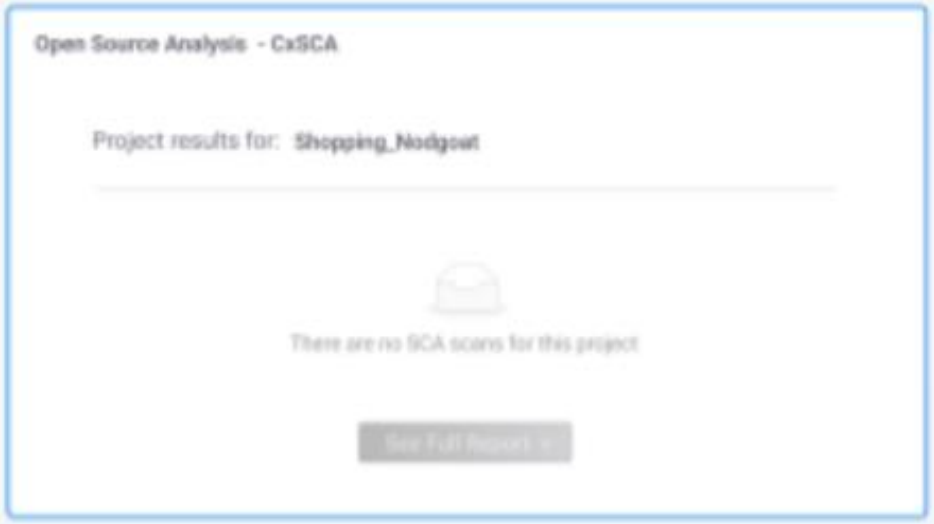
Possible Errors

If there is another SAST project scan with the same name



- Verify that the CxSAST project and the corresponding CxSCA project have the same name.
- Verify that no other CxSAST project in the network has been assigned the same name.

If no scans have been performed yet for the corresponding CxSCA project

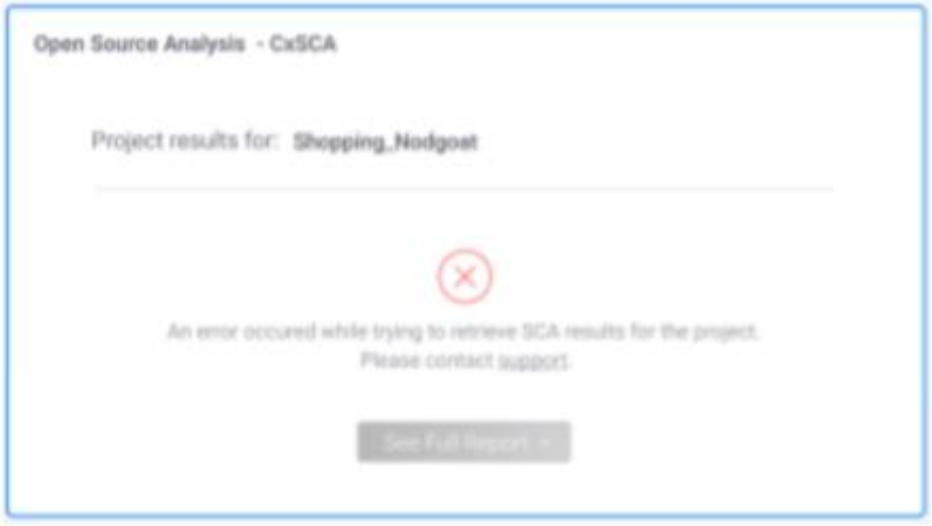


- Perform a scan for the corresponding CxSCA project.

If the corresponding CxSCA project does not exist

- Make sure that there is a CxSCA scan with the same project name.
- Return to the SCA settings page,
- Make sure that your tenant name and the URLs are correct.
- Test the connection.
- Update if needed.

In case, the connection cannot be established or results cannot be retrieved otherwise, a general error is reported



- Return to the CxSCA settings page.
- Verify that your tenant name and the URLs are correct.
- Test the connection.
- Update if needed.

Dashboard Data Analysis

For additional information on Data Analysis, refer to Getting to Know the System Dashboard.

System Management

This chapter covers system management and user management.

Management Settings

This section addresses authentication settings, application settings, maintenance settings, custom field management and profile settings.

Authentication Settings

From v9.0.0 and up, for LDAP and SAML management, see 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, please 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

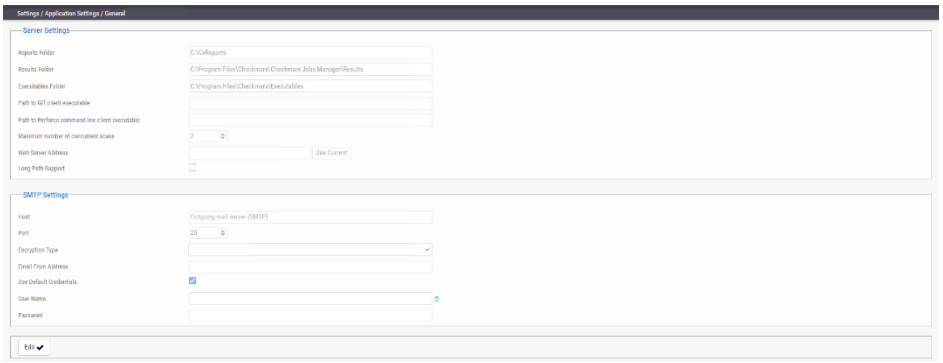
From v9.0.0 and up, for SMTP and Domain Management settings, see Access Control Settings.

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.

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.

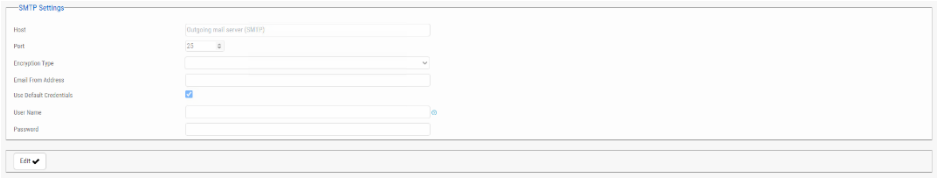
- **Path to P4 command line client executable** - Set the Perforce client executable path
  (e.g. **C:\Program Files\Perforce\p4.exe**)

> - 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 take effect.
- **Time remaining until task completion (min)** - Set the time remaining until the task is complete.
- **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.



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 are used.
- **User Name** - Enter the user name.
- **Password** - Enter the password.

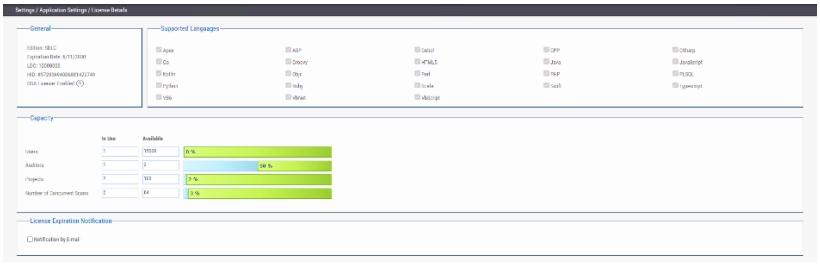
CxOSA Settings

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

License Details

CxSAST lets you view the details of the license you obtained. To view the license details, do the following:

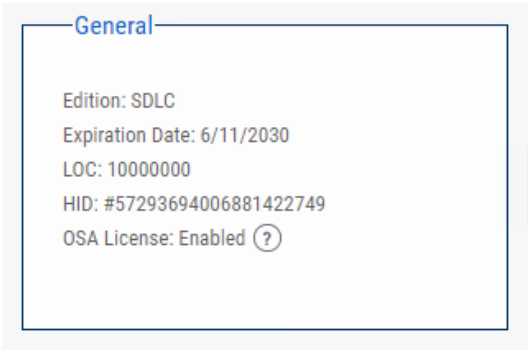
- Select **Settings** > **Application Settings** > **License Details.** The **License Details** window is displayed.



The License Details screen is divided into the following windows:

General

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



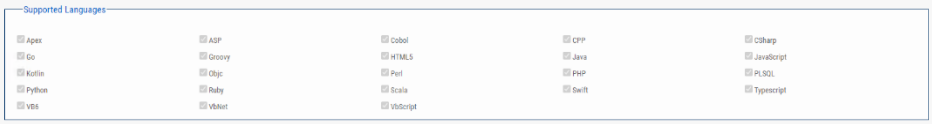
This includes the following information:

- **Edition -** CxSAST license edition (SDLC or Security Gate). To learn more about the different editions please refer to License Editions Overview.
- **Expiration Date** - Lense 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.



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.

This 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.

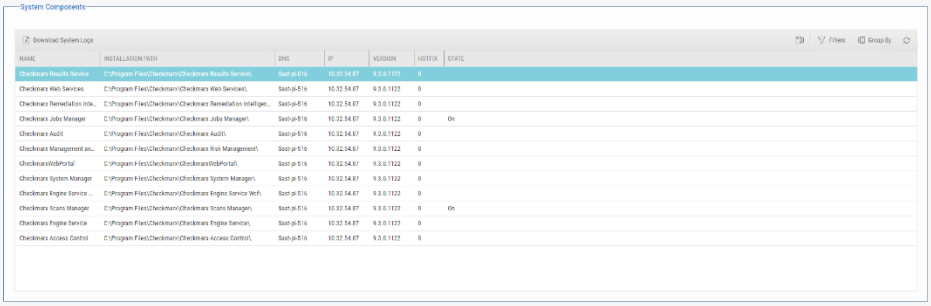
- **Notification by E-mail** - If checked, a notification email is automatically sent to the CxSAST Administrator User on a weekly basis, starting 90 days (defined in the database) before the actual license is set to expire.

The Notification by email address is defined under Email Notifications in the Server SMTP Setting.

Installation Information

The Installation Information screen provides a list of all the CxSAST components installed with their characteristic parameters. To display the installation information, do the following:

1. Select **Settings** > **Application Settings** > **Installation Information**.
   The **Installation Information** window is displayed with the following information:
   - **Installation Path**: Location of the installation.
   - **Version:** The CxSAST version with build#.
   - **DNS**: System name of the host where the component is installed This information also indicates, if the system is a centralized or a distributed installation.
   - **IP**: The IP address of the host where the component is installed.
   - **Hotfix**: The Hotfix number. **0**, if no hotfix has been installed.
   - **State**: Current state of the respective component.



2. Click the **Download System Log** button to download the system log file.

Content Pack version

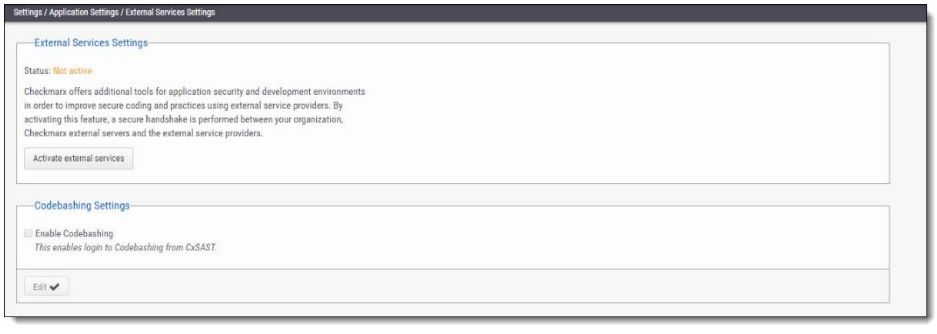
- The permission (**download_system_logs**) is required to perform the 'Download System Log' task.
- The latest queries pack version is also listed in cases where a content pack is installed. For additional information on the Content Pack for your version, refer to the relevant version release notes 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.



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.

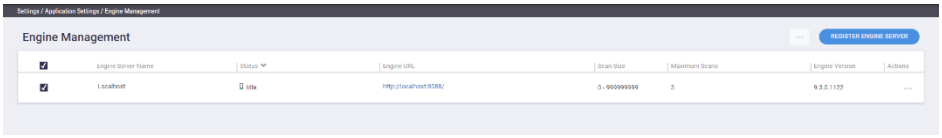
3. Click <**Edit**>. The **Codebashing Settings** fields are enabled.
    - **Enable Codebashing** - If selected, enables **anonymous data collection** in order to provide user analytics. The second checkbox, enables **non-anonymous data collection** in order to provide user analytics. This option, if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

Engine Management

Engine Server Management provides an interface for viewing real-time engine server status information that includes the number of engine servers in the system, their status, location (URL) and scan size. Available actions on the Engine Management interface include registering, editing, blocking/unblocking and unregistering engine servers as explained below.

➢ **To open the Engine Management:**

- Select **Settings** > **Application Settings** > **Engine Management**.
  The **Engine Management** window is displayed.



The Engine Server Management screen refreshes 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
Selector	Select ☑ all engines in case you want to unregister all of them.
Engine Sever Name	Name of the engine server
Status	Status of the engine server: • Scanning: The engine server is running one or more scans. • Idle: The engine server is waiting to receive scan requests. • Blocked: The engine server is blocked and unable to receive scan requests. • Offline: The engine server is unable to communicate with the system because the host may be down, a service stopped, connectivity issues, etc.

Field	Description
	• Scanning & Blocked: The engine server is blocked and completes running scans that have been requested before the engine server has been blocked.
Engine URL	URL of the engine server
Scan Size	The range of the number of lines (LOC) allowed to be scanned on this engine.
Maximum Scans	The max number of concurrent scans allowed on this engine.
Engine Version	Engine version number
Actions	The following actions are available: • Edit • Unregister • Block • Unblock

Performing Engine Sever Management Actions

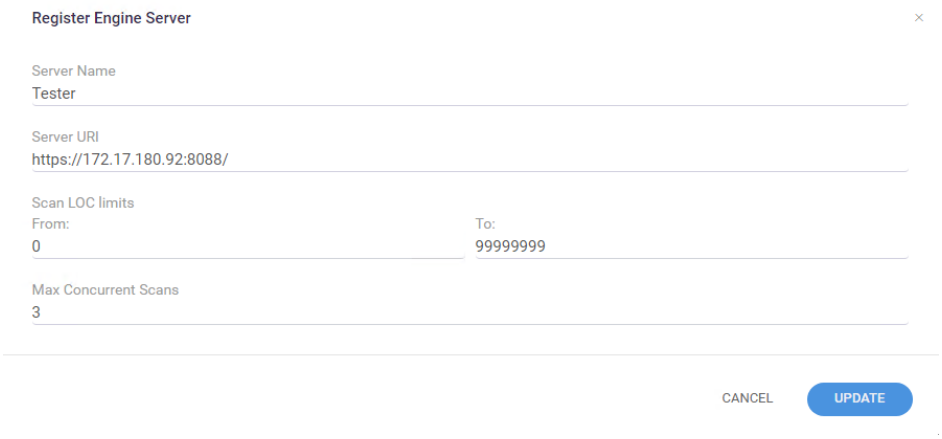
The Engine Management interface allows you to perform the following:

- Registering a new engine server
- Editing an engine server
- Blocking/unblocking an engine server
- Unregistering an engine server

Registering a New Engine Server

You can register (add) a new engine server to the system as follows:

1. Click <**REGISTER ENGINE SERVER**> to display the Register Engine Server dialog.
2. Define the server attributes illustrated and listed below.
3. Click <**UPDATE**> to save the changes. The new engine server is added to the engine list.

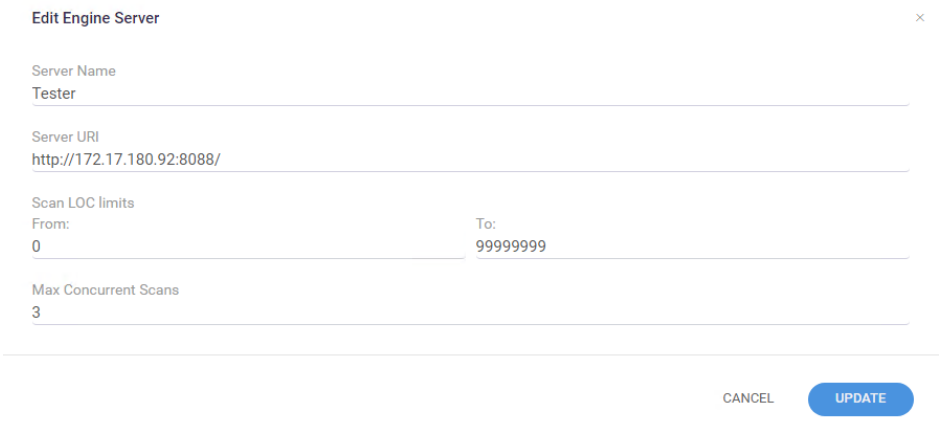


Parameter	Description
Server Name	Enter the name of the engine server. Each engine server should have a unique name.
Server URI	Enter the URI address of the engine server. The URL looks as follows: http(s)://<host name or IP address>:<port>, for example http://172.17.180.92:8088
Scan LOC Limit	Enter the scan LOC (lines of code) limit. The 'From' and 'To' definition must be a whole number between 0 - 999,999,999.
Max Concurrent Scans	Enter the allowed max number of concurrent scans, which must be a whole number between 1 - 999,999,999. The max number you can enter depends on the resources of your system.

Editing an Engine Server

You can edit an existing engine server's attributes in the system as follows:

1. In the Engine Server table, under **Actions**, click ⋯ and select **Edit**. The Edit Engine Server dialog is displayed.

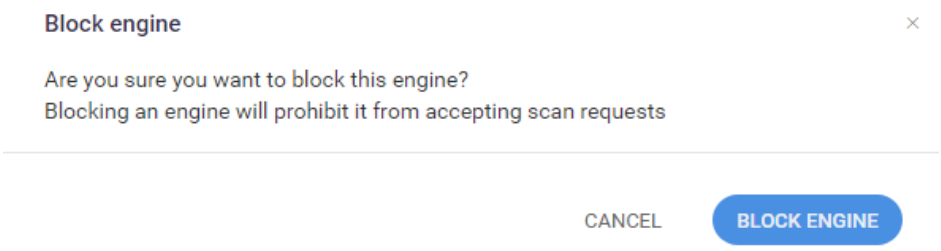


2. Modify the engine parameters accordingly. For additional information on parameters, refer to **Registering a New Engine Server**.
3. Click <**UPDATE**> to save the changes.

Blocking/Unblocking an Engine Server

Blocking prevents the engine server from accepting any new scan requests from the system. Scans requested by the system before the engine server has been blocked, continue uninterrupted until they are completed. To block an engine server, do the following:

1. In the Engine Server table, under **Actions**, click ⋯ and select **Block**. The Block Engine Server dialog is displayed.



2. Click <**BLOCK ENGINE**>. The status of the engine server switches to **Blocked** in the list.

To unblock an engine server, do the following:

- Follow the instructions above and select **Unblock**. Once the engine server is unblocked, the status of the engine server returns to the previous status, usually **Idle**, and resumes accepting new scan requests from the system.

➢ **To block multiple engine servers:**

1. Select at least two engine servers. You are now able to perform a batch job.
2. Click and then select **Block** from the menu. The selected engine servers in the list are blocked.

➢ **To unblock multiple engine servers:**

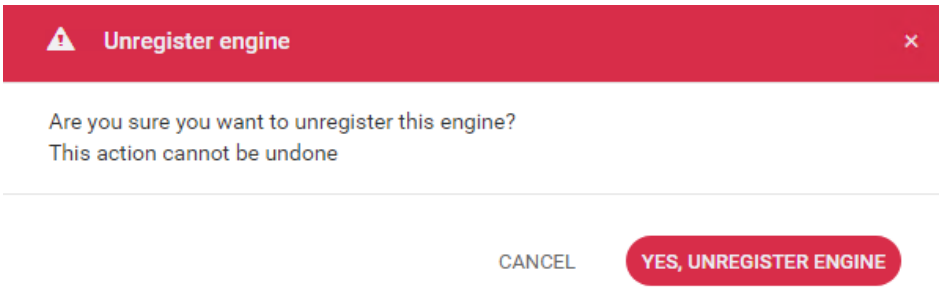
1. Select at least two engine servers. You are now able to perform a batch job.
2. Click and then select **Unblock** from the menu. The selected engine servers in the list are unblocked.

In order to block (unblock) engine servers as a batch job, all the selected engine servers must be unblocked (blocked), otherwise the **Block**/ **Unblock** command is unavailable.

Unregistering an Engine Server

You can unregister (remove) an engine server from the system as follows:

1. In the Engine Server table, under **Actions**, click and select and select **Unregister**. The Unregister Engine Server dialog is displayed.
2. Click <**YES, UNREGISTER ENGINE**> to remove the engine server from the Engine Management list.



➢ **To block multiple engine servers:**

1. Select ☑ at least two engine servers. You are now able to perform a batch job ⋯.
2. Click ⋯ and then select 🗑 **Unregister** from the menu. You are asked to confirm your request.
3. Click <**YES, UNREGISTER ENGINES**> to remove the selected engine servers from the list.

- You cannot unregister engine servers that are currently running a scan.
- If you run a batch job and some of the selected engine servers are currently running a scan, you are notified that the scanning engine servers cannot be unregistered. If you still want to unregister these engine servers, you have to repeat the unregistering process for them.

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.

Warning - Scanned data is purged from the file system as well as the database, therefore, once deleted cannot be reversed. See **Data Retention Purged Data**, below.

Using our CxSAST (REST) API for Data Retention, this process can be automated (v8.8.0 and up).

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.

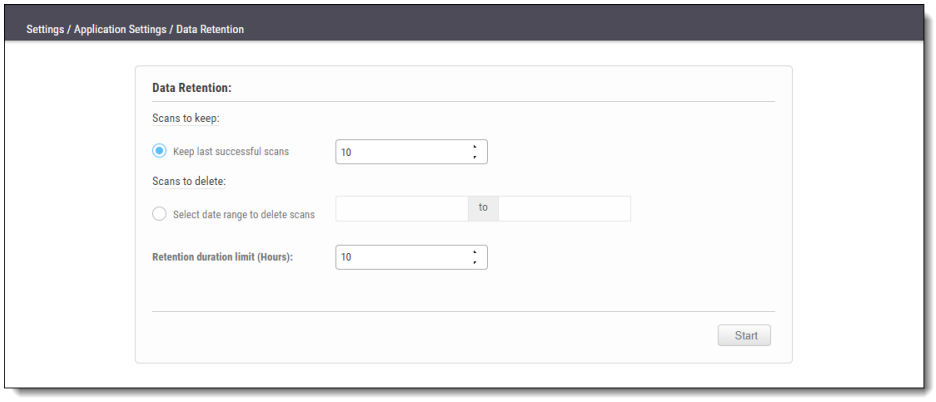
Specific scans may be marked as “Locked” to avoid automated purging of important scan data.

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. Refer to Unlocking Scans (v9.0.0 to v9.2.0) or Unlocking Scans (v9.3.0 and up) respectively.

Defining Data Retention Settings

To define the data retention settings, do the following:

Select **Settings** > **Application Settings** > **Data Retention**. The Data Retention window is displayed.

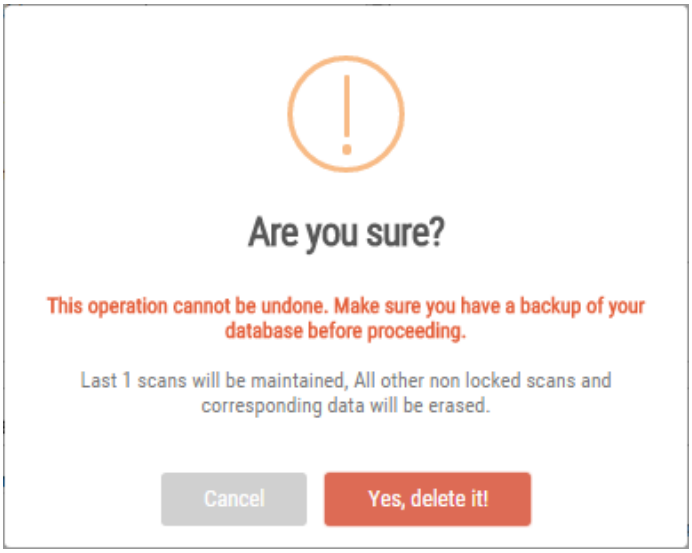


The Data Retention window includes the following settings:

- **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.

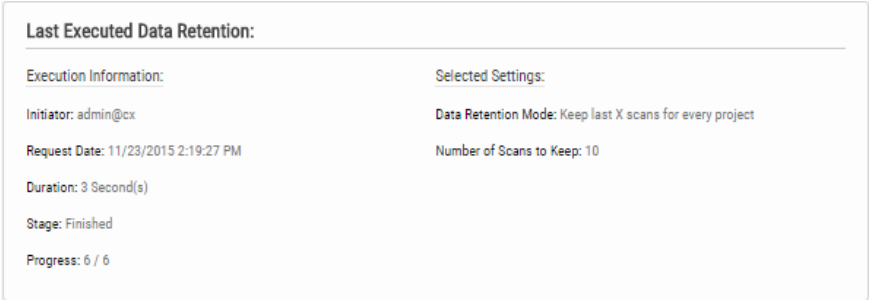
Click **Start**. The following message appears:



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.

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



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

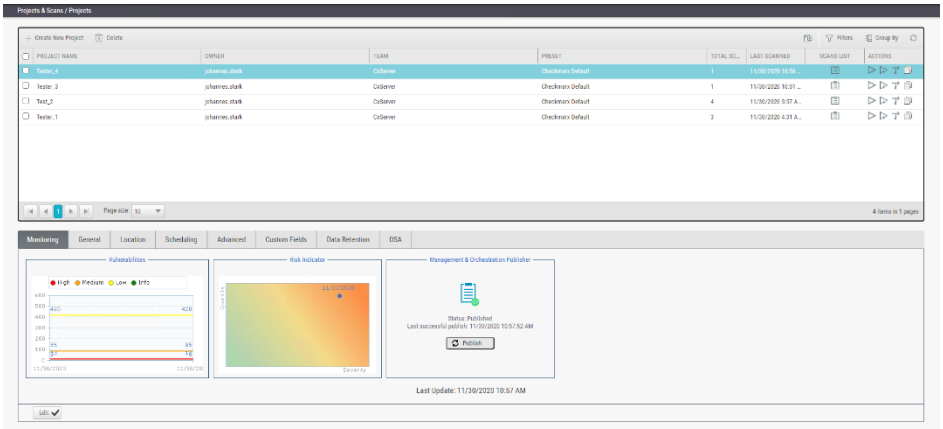
File System

- 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

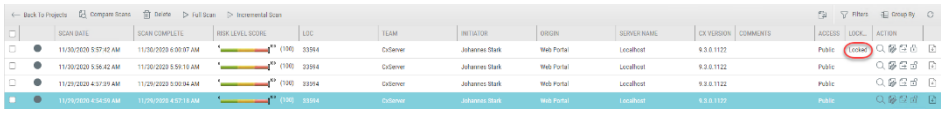
One of the most common reasons for having no scans deleted is that one or more of the scans are locked. This can be modified by unlocking the scans as follows:

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



2. Select the requested project. If many projects exist, filter the project list as follows:
   - Click **Filters** on the right.
   - Type one or more identifying criteria for the project, such as the project name, owner or team.
   - Press <**Enter**> to only see the projects listed that match the filter criteria you entered.

3. Under **Scans List**, click **View Projects Scans**. The scans run by the selected project appear listed.
4. Locate the locked scan. Locked scans are labeled **Locked** in the LOCKED column as illustrated below. Unlocked scans do not have an entry in that column.



5. Click to unlock the scan.

➢ **To lock a scan:**

- Go to the desired scan in the list and click . The **Locked** indicator appears in the LOCKED column.

Issue Tracking Settings

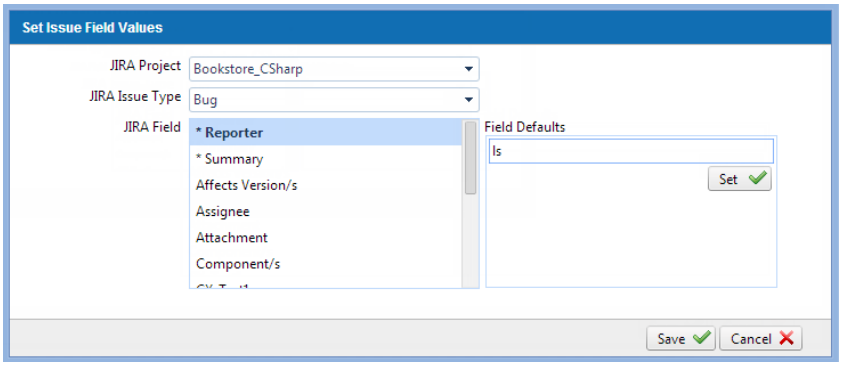
Issue tracking for CxSAST can be performed using JIRA integration. JIRA is a proprietary issue tracking product that allows bug tracking and agile project management.

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 (in a distributed deployment: on CxManager), 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 and 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**

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. Back in the CxSAST project, click **Finish**.

License Editions Overview

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

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

Custom Field Management

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

Implementing and consuming project attributes by using the Custom Fields capability is a process that consists of three steps:

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.**

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.

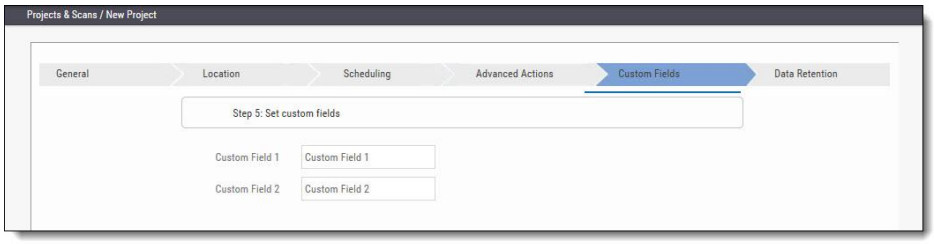
➢ **To edit the custom field's name:**

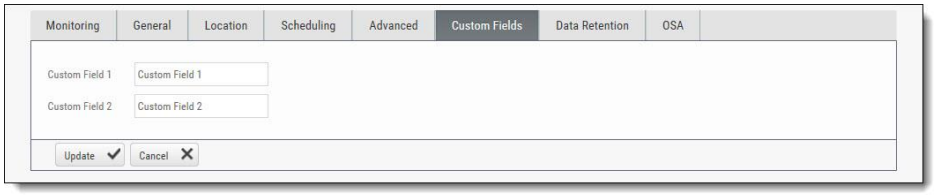
1. Click **+** to the left of the field name.
2. Make the requested change in the editable row that appears.
3. Click <**Save**>.

➢ **To delete a custom field row:**

1. Click **Delete** next to the desired custom field and confirm your request when prompted.
2. Click <**Save**>.

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.





My Profile Settings

Since v9.0.0, My Profile settings are handled from the Access Control portal, and clicking <**My Profile**> on the CxSAST Dashboard navigates you to the 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

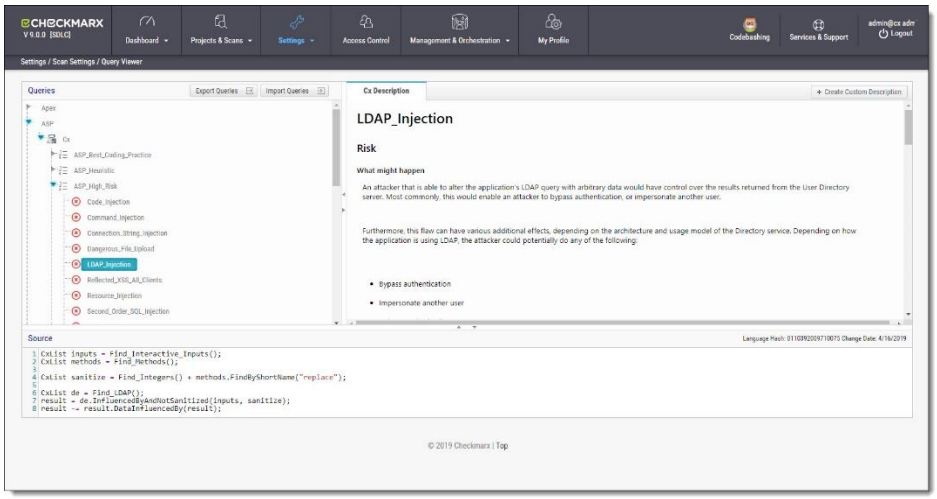
This section addresses the query viewer, preset management, limiting engine scans and configuring pre- and post-scan actions.

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.



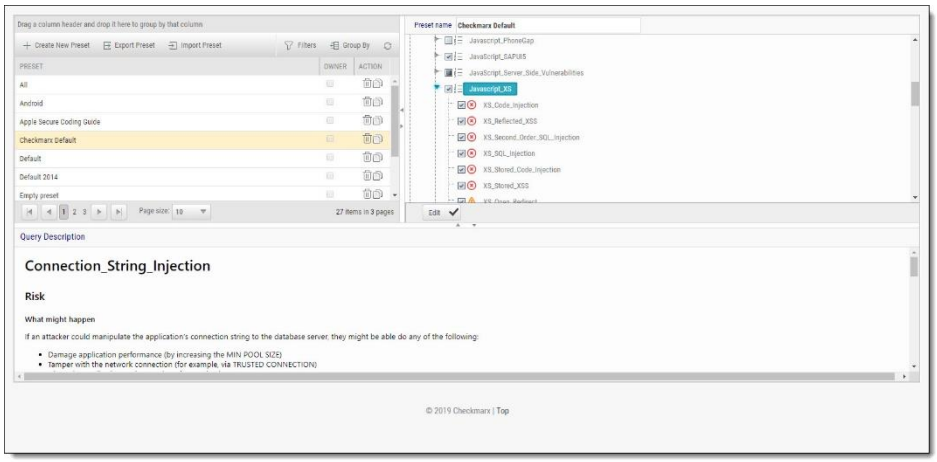
2. Select a **Query** in the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk. The source code for the query is displayed in the **Source** pane at the bottom of the window.

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.



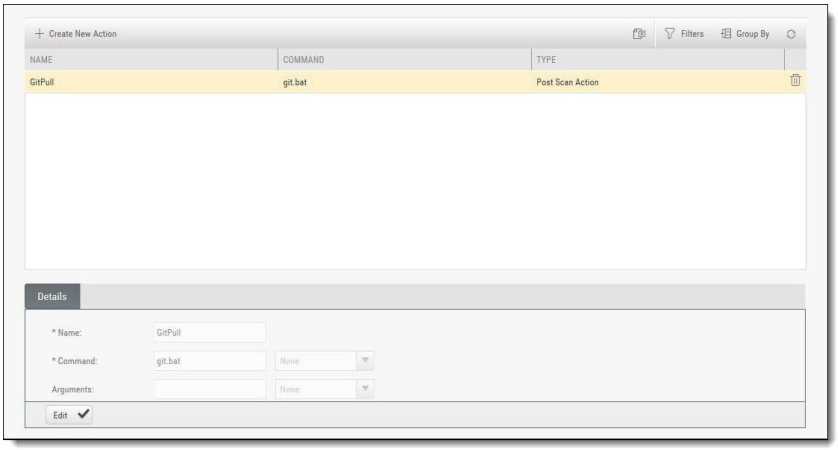
2. Select a **Preset** in the **Presets** pane. Select a **Query** from the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk.
3. Click **Create New Preset** to create a new preset.

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.



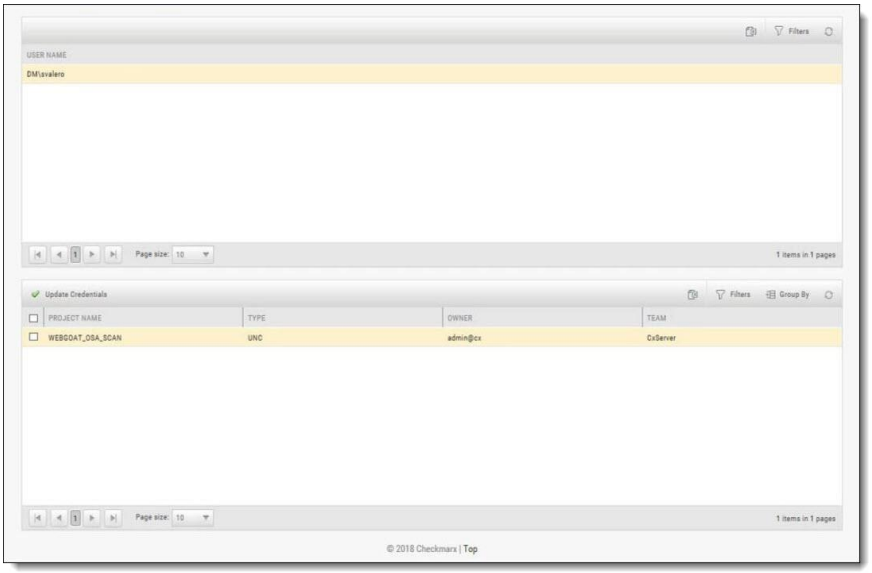
2. Select an **Action** from the **Actions** pane. The definitions of the selected action are displayed in the **Details** pane at the bottom of the window.
3. Click <**Edit**> to update the selected action details.

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:**

1. Go to **Settings** > **Scan Settings** > **Source Control Users**. The **Source Control User** window is displayed.



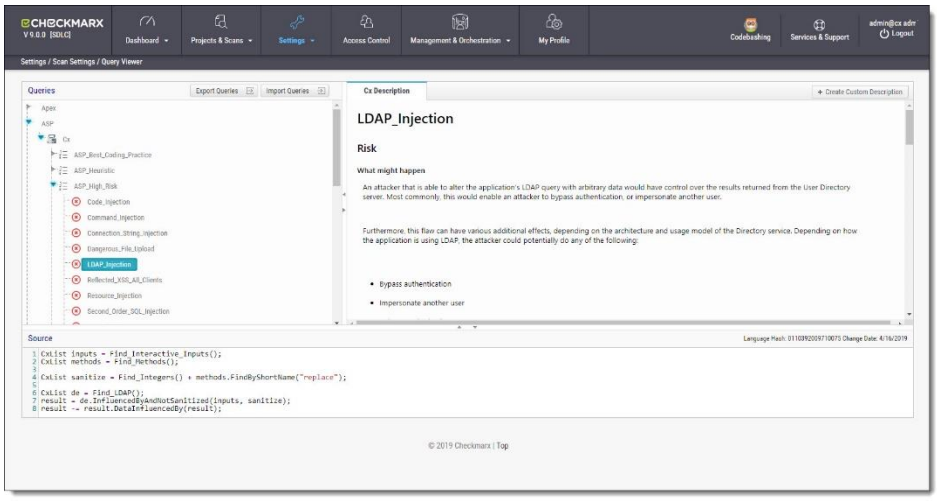
2. Select the **User** from the **Users** pane. The credentials of the selected user are displayed in the **Credentials** pane at the bottom of the window.
3. Click <**Update Credentials**> to update the selected user credentials.

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.



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.

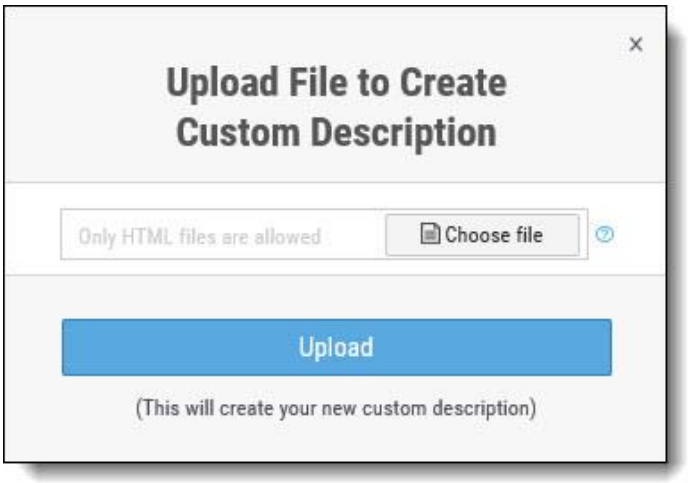
Creating a Custom Description

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.



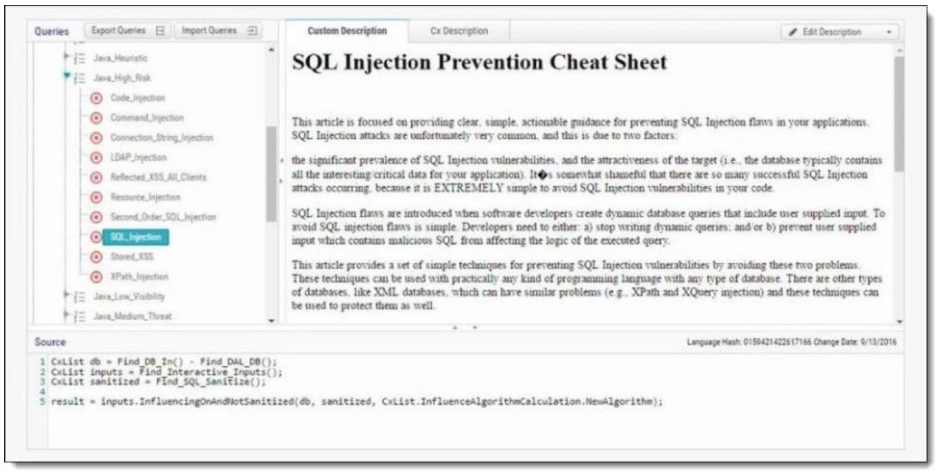
3. Click <**Choose File**>, navigate to the custom description file (.HTML) and click **Open**.

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 will not be saved.

4. Click <**Upload**>. The **Custom Description** tab is displayed in the **Description** pane.



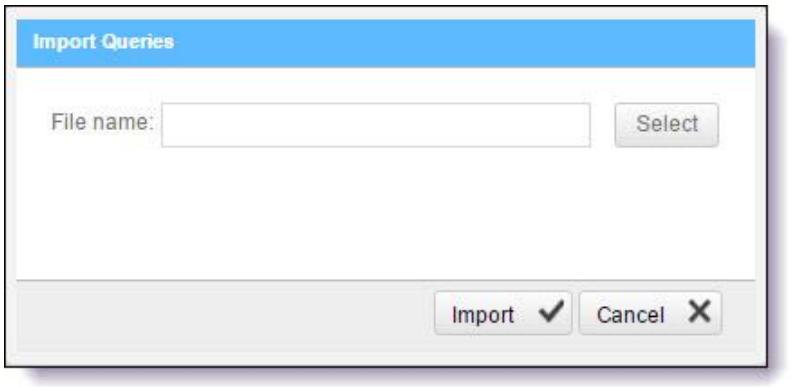
You can replace or delete the custom description by clicking **Edit Description** and selecting **Update Description** or **Delete Description** accordingly.

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.



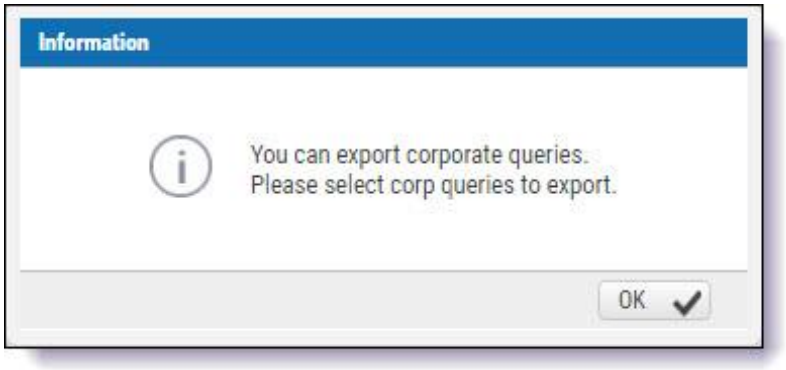
2. Click <**Import**>, navigate to the query file (.XML) and click <**Open**>. The query is displayed in the **Queries** pane.

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.



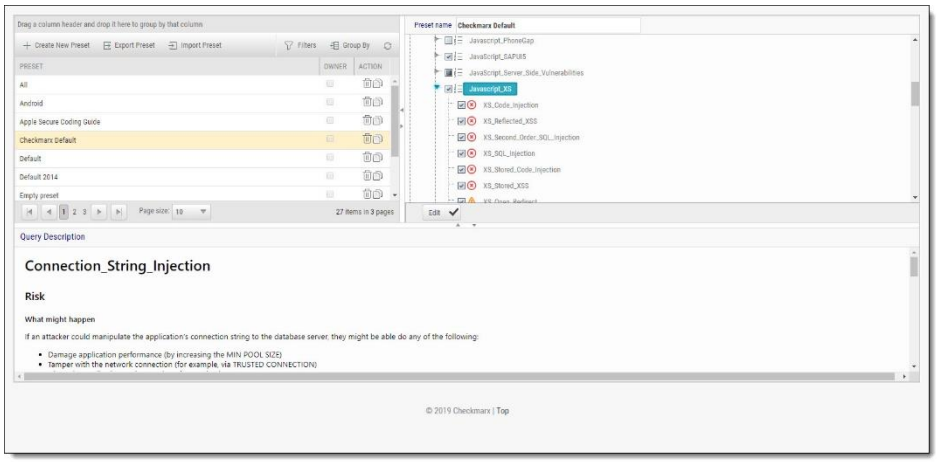
2. Click <**OK**>.

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:**

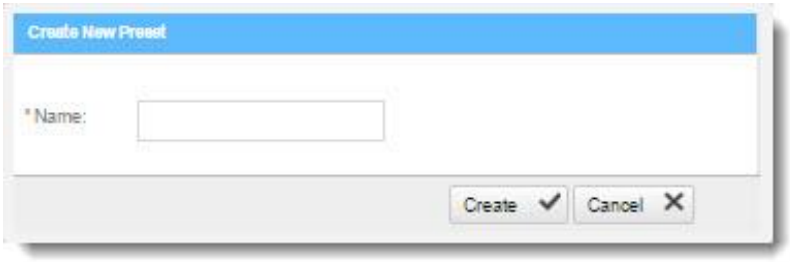
- 1. Go to **Settings > Scan Settings > Preset Manager**. The Presets Manager window is displayed.



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

➢ **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**>.

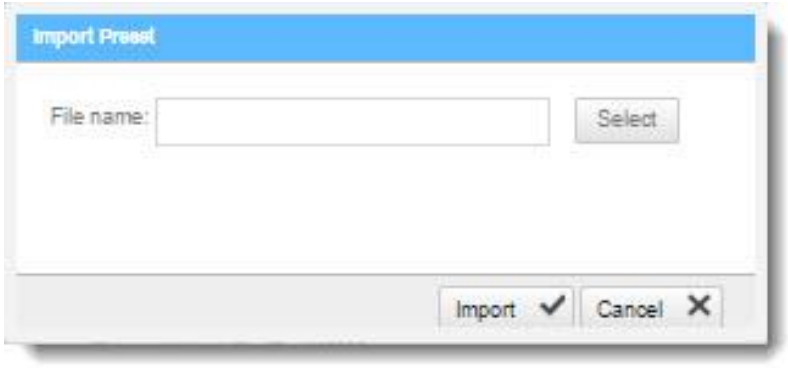
➢ **To modify an existing preset:**

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.
4. Click <**Save**>.

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.

➢ **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. Click <**Import**>. The Preset is displayed in the Preset pane.



If the imported preset has the same name as an existing one, the existing preset will be overridden.

➢ **To export a preset:**

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

➢ **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

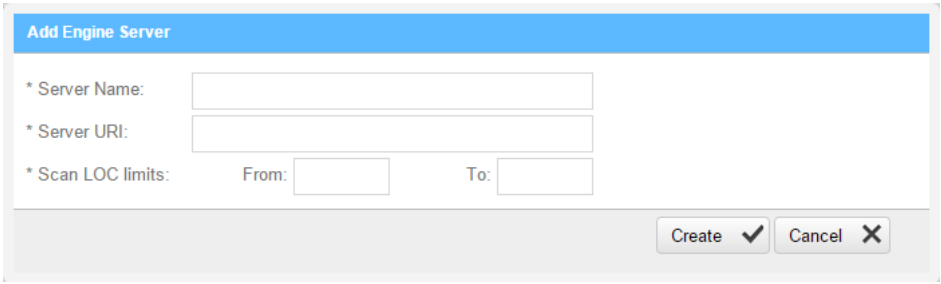
Preset	Usage	Includes vulnerability queries for....
Android	For Android related application security risks	Groovy, Java and Kotlin coding languages
Apple Secure Coding Guide	For IOS related application security risks	ObjectiveC coding language
Checkmarx Default	The Checkmarx Default preset essentially 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
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

Preset	Usage	Includes vulnerability queries for....
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:

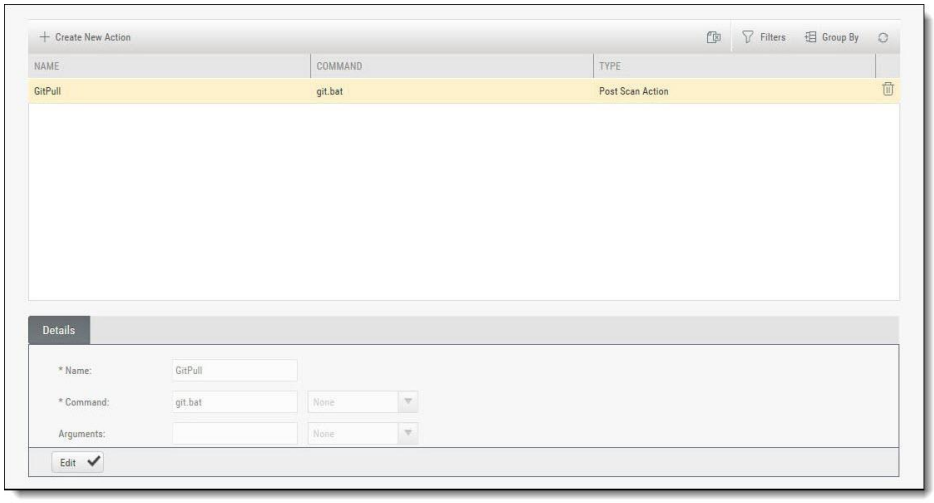
- **Server Name**: The name of the server you are appointing as Engine Server
- **Server URI**: The address of the server
- **Scan LOC limits**: The Scan limits is not a mandatory field, in the event the fields are left empty assume the value From to include: All to: All. Define the lower and higher 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.

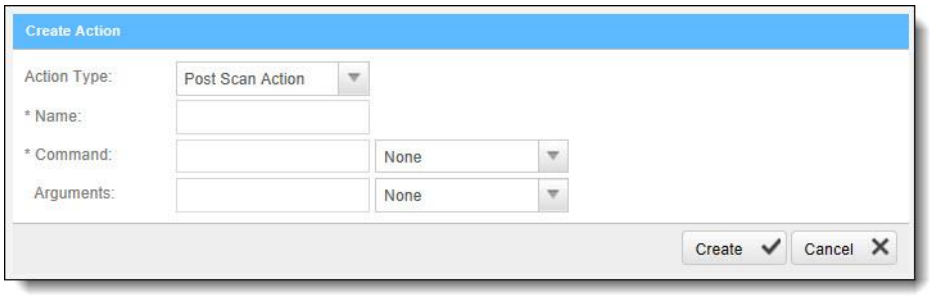
Configuring Pre & Post Scan Action

➢ **To create Pre & Post Scan actions:**

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



2. Click **Create New Action**. The **Create Action** window is displayed.



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 then <**Finish**>.

User Management

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, please refer to 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 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

Provided Roles for CxSAST / CxOSA	Description	Permissions per Role
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
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

Permission	Category	Description
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 • 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
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

Working with Logs

This section outlines the structure of the CxSAST logs and explains how to work with them.

Downloading and Viewing Logs

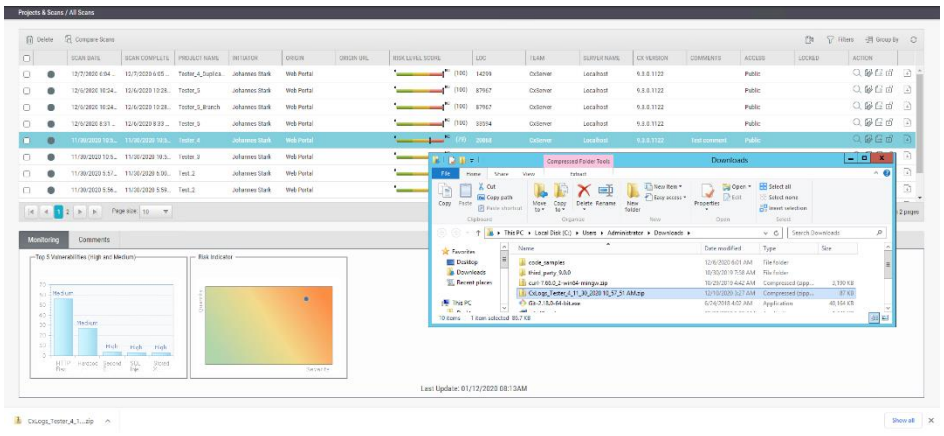
Scan logs consist of general system information and information related to the scan results and the scan process itself. Logs can be downloaded from the Scan and Projects State lists as zip archives for viewing and further treatment. A typical scan log downloads in the following format: **CxLogs_<project name>_<date of the latest scan>_<time of the latest scan>.zip**, for example **CxLogs_Tester_4_11_30_2020 10_57_51 AM.zip** for a project called **Tester_4** that has been scanned last on **November 30th, 2020**. The zip archive contains the pre-defined type(s) of the scan log, which may be one or both of the two following ones:

- The 'regular' one in the Checkmarx plain text format
- A new type in JSON format that reflects the log structure required for ELK analysis.

For further information on the log structure, ELK analysis etc., refer to Analyzing Logs Using ELK.

➢ **To download the log:**

1. In the Project State list or a scan list, navigate to the desired scan and click . The scan log of the desired scan is downloaded to the default download folder (usually the Download folder) and appears listed in your browser.
2. Navigate to the log file and copy it to the desired location on your host.



Enabling the JSON Format for Log Files

In order to obtain logs in JSON format, you first have to enable the JSON format in the config files for each log that provides this option.

For example for the Scans Manager logs, you have to enter the bin folder (**C:\Program Files\Checkmarx\Checkmarx Scans Manager\bin**) and locate the logging config file, in this case **ScansManager.logging.config** and set **"jsonFormat"** to **true**. You are able to generate logs in JSON format and the plain text format or just in JSON format. In addition, you can define, which elements of the log structure to show or hide.

- **To generate the log in JSON format only:**

1. Navigate to the relevant bin folder, for example **C:\Program Files\Checkmarx\Checkmarx Scans Manager\bin** and open the logging config file, in this case **ScansManager.logging.config** with your text editor.
2. Set **"jsonFormat"** to **true**.
3. To show results for the desired elements of the JSON log, set them to **true** as well, for example to display the Correlation results, set **"showCorrelation"** to **true**.
4. Save the file.

- **To generate the log in plain text and JSON format:**

1. Duplicate the relevant code section, for example

```
{
  "path": "$rootDir$/../../Logs/ScansManager",
   ...
    "period": "Infinite"
  }
}
```

2. In the duplicated section, under **"path"**, define a different path for example for the JSON log. The path might be something like **"path": "$rootDir$/../../Logs/ScansManager/JSON"** while the path in the example above specifies the location for the log in plain text format.
3. Set **"jsonFormat"** to **true** and enable the elements of the JSON log that you want to be displayed as outlined above.
4. Save the file.

- To display part or some aspects of the log (for example ERROR level in JSON format and the rest in plain text format, set **"minimumLevel"** to the respective level. For example, for JSON format, set **"minimumLevel"** to **"ERROR"** and for the part to be generated in plain text format, set it to **"Information"**.

Example for the Scans Manager log:

```
{
  "service": {
    "identifier": "ScansManager"
  },
  "persistence": {
    "File": [
      {
        "path": "$rootDir$/../../Logs/ScansManager",
        "fileName": "CxScanManager",
        "dateTimeFormat": "yyyy-MM-dd HH:mm:ss,fff",
        "minimumLevel": "Error",
        "jsonFormat": true,
        "showCaller": true,
        "showCorrelation": true,
        "showService": true,
        "showGuid": true,
        "retention": 5,
        "rotation": {
          "size": 10,
          "period": "Infinite"
        }
      },
      {
        "path": "$rootDir$/../../Logs/ScansManager/Trace",
        "fileName": "CxScanManagerAll",
        "dateTimeFormat": "yyyy-MM-dd HH:mm:ss,fff",
        "minimumLevel": "Information",
        "jsonFormat": false,
        "showCaller": false,
        "showCorrelation": false,
        "showService": false,
        "showGuid": false,
        "retention": 5,
        "rotation": {
          "size": 10,
          "period": "Infinite"
        }
      }
    ]
  }

}
```

Analyzing Logs Using ELK

Scan logs are downloaded as zip archives for viewing and further treatment in the previously illustrated format.

The Log Structures

The table below compares a typical line of a log in plain text format with a line from a log in the new JSON format.

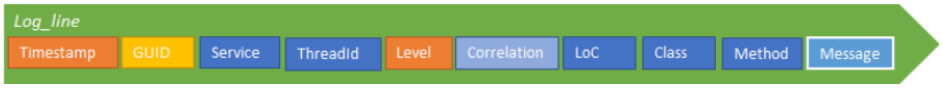
Log Format	A Typical Line
Legacy	2020-11-12 11:25:25,968 [38] ERROR - Failed to fetch engine server information with server id 1 reason:Operation returned an invalid status code 'Unauthorized'
JSON	{"Timestamp":"2020-12-23 09:25:09,251","GUID":"de73292e-1558-4454-8013-3a79d27ca102","Service":"ScansManager","ThreadId":24,"Level":"INFO","Correlation": {"ScanRequest":"1000004","Project":"4","Scan": "645cd5cf-6e89-4405-97b5-267029f54b2b" },"CallerInfo": {"Line":501,"Class":"C:\\CxCode\\CxApplication\\Source\\Common\\CxDAL\\ScanRequests\\ScanRequestDataProvider.cs","Method": "ExecuteUpdate" },"Message":"Tried to update ScanRequest id: 1000004. Sucess? True"}

- To analyze logs using ELK, you have to use the JSON format of the respective log.
- The log is available in JSON format along with the plain text format or instead of it, depending on the enabled log format.

The Log Structure of the Log in JSON Format

Every line in the log consists of the following type of information as illustrated and explained for the log line below:

{"Timestamp":"2020-12-23 09:25:09,251"**,"GUID":**"de73292e-1558-4454-8013-3a79d27ca102"**,"Service":**"ScansManager"**,"ThreadId":**24**,"Level":**"INFO"**,**"Correlation"**:**{"ScanRequest":"1000004","Project":"4","Scan":"645cd5cf-6e89-4405-97b5-267029f54b2b"**},{"Line":**501**,"Class":**"C:\\CxCode\\CxApplication\\Source\\Common\\CxDAL\\ScanRequests\\ScanRequestDataProvider.cs"**,"Method":**"ExecuteUpdate"**},**"Message"**:**"Tried to update ScanRequest id: 1000004. Sucess? True"**}**



- **Timestamp:** Timestamp for each log line entry.
- **GUID:** Unique identifier, which allows you to view all logs related to a specific component/service.
- **Service:** Component identifier, this can be customized in the config file, by default it is the name of the component, e.g. **JobsManager**
- **ThreadId:** Thread/process identifier.
- **Level:** Logs with different severities can be logged at different levels. The visibility can be limited to a single level, displaying only logs at a certain severity or above, for example only logs of **ERROR**.
- **CorrelationID:** Provides the ability to correlate logs in a certain flow/request. Being able to see all the logs relevant to a particular request or a particular event, helps you to drill down to the relevant information for a specific request. (e.g.: **ScanId**, is the same across several services)
- **Correlation**: Provides the ability to correlate logs in a certain flow/request. Being able to see all the logs relevant to a particular request or a particular event helps you to drill down to the relevant information for a specific request. (e.g.: **ScanId**, is the same across several services). Please note that **Correlation** is an attribute that aggregates relevant properties such as **ScanRequest**, **Project**, **ScanId**, etc.
- **Line:** Number with lines of code where the log entry is. The scheme refers to it as **LoC**.
- **Class:** Class name where the log entry is.
- **Method:** Method name where the log entry is.
- **Message:** A free text string with contextual information.

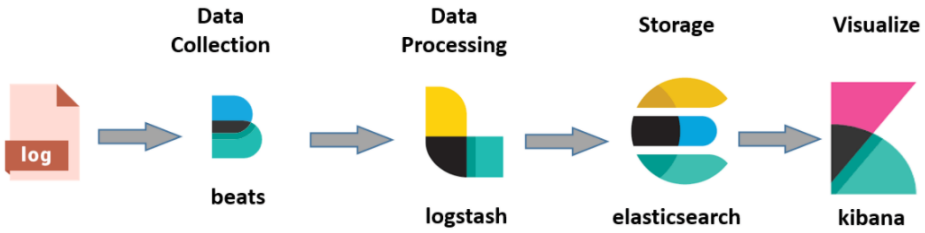
Analyzing Logs

ELK stands for the combined use of three open source projects, Elastic Search, LogStash and Kibana. They work together as follows:

- **E**: Stands for Elastic Search and is used for storing logs.
- **L**: Stands for LogStash and is used for both shipping as well as processing and storing logs.
- **K**: Stands for Kibana, which is a web-based visualization tool hosted by Nginx or Apache.

ELK provides centralized logging that can be useful when attempting to identify problems with servers or applications. It allows you to search all your logs in a single place. It also helps to identify issues in multiple servers by connecting the respective server logs during a specific time frame.

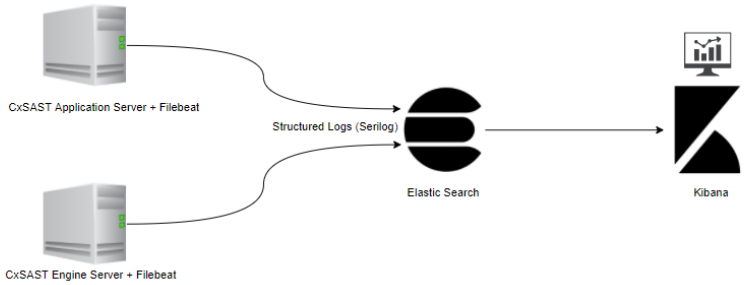
The ELK components are used as illustrated in the simple diagram below:



The components are the following:

- **Logs**: Server logs in JSON format that are subject to be analyzed. These logs are generated together with the legacy logs and reside in the separate JSON folder.
- **Beats**: For example Filebeat: It is responsible for collecting log data and forwarding it to the Logstash or directly to Elastic Search.
- **Logstash**: Parses and transforms data received from the beats (for example Filebeat).
- **Elastic Search**: Indexes and stores the data received from the beats or Logstash.
- **Kibana**: Uses the Elasticsearch database to explore, visualize and share the log data.

To simplify the system, the Checkmarx ELK system does not use the Logstash and forwards data straight to the Elasic Search as illustrated below.



The ELK Components Used To Analyze CxSAST Logs

Checkmarx uses and supports Filebeat, Elastic Search and Kibana. The components are located as follows:

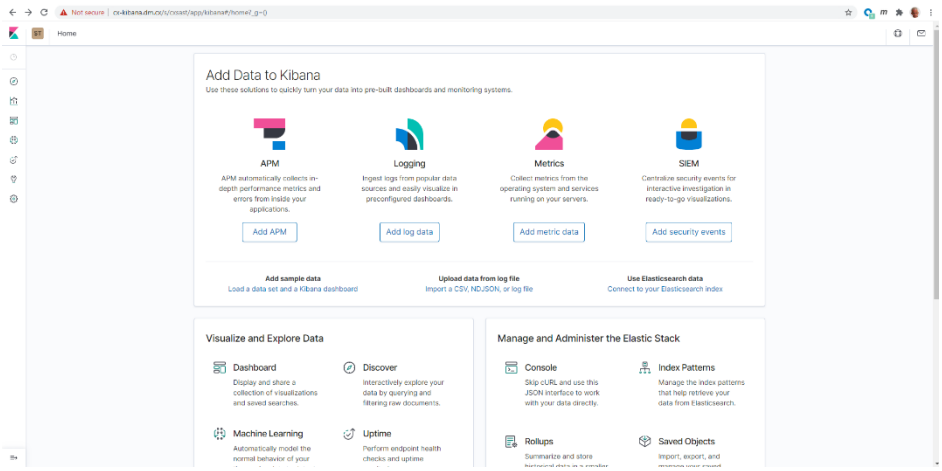
- **Filebeat** on the host that hosts your CxSAST Engine server or the CxSAST application server. For further information and instructions, refer to Getting Started with Filebeat.
- **Elastic Search** on a dedicated server. For further information and instructions, refer to the Elastic Search installation instructions.
- **Kibana** on a dedicated server. For further information and instructions, refer to the Kibana installation instructions.

Analyzing a Log

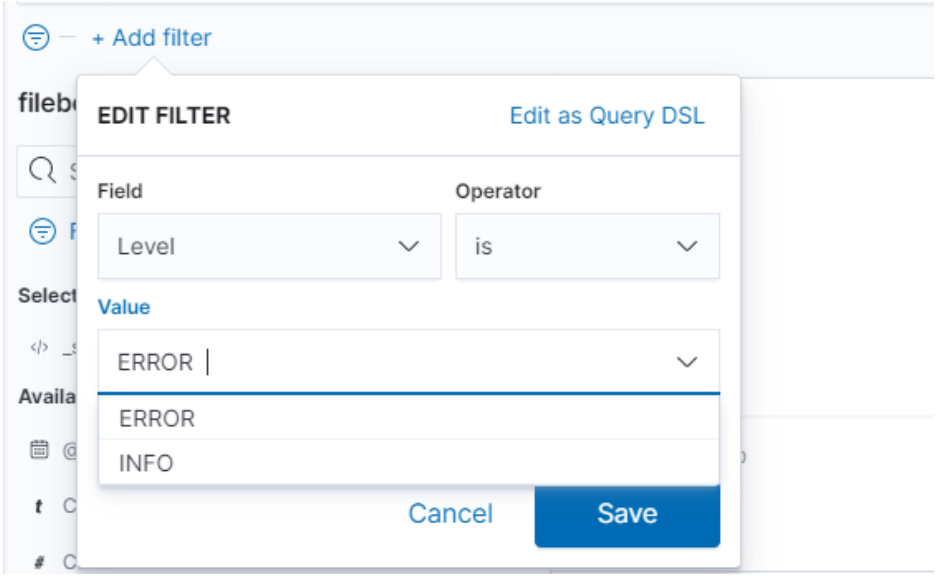
To analyze a log, you have to enter your Kibana space via the Kibana interface that you created while installing Kibana.

➢ **To enter the Kibana space:**

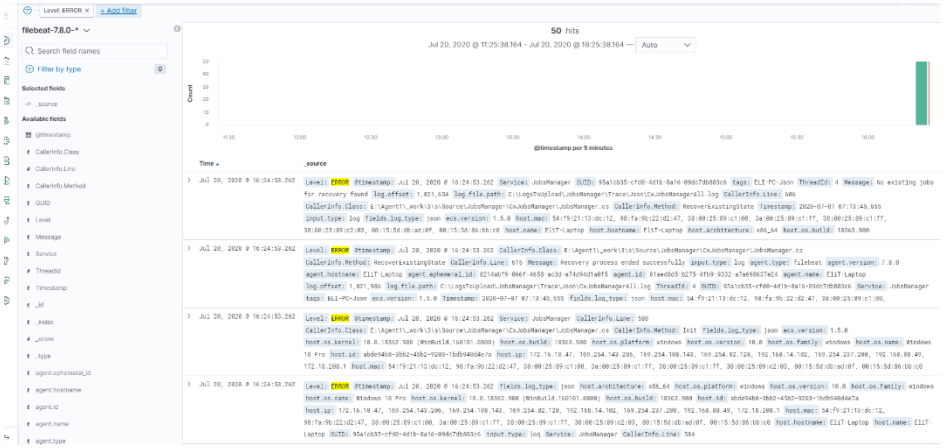
1. Open your Internet browser and enter the URL of your Kibana space, which is something like **http://{FQDN or IP}/{folder}/kibana#/home**, for example **https://cx-kibana.dm.cx/s/cxsast/app/kibana#/home?_g=()**.



2. Click <**Add Log Data**> to import a scan log.
3. Filter the log for Level **ERROR** as illustrated below.



The results are displayed as follows:



4. Follow the onscreen instructions and options to continue illustrating the log results.