

Lab Exercise 19

Setting up Snyc for SAST in Jenkins

Name-Misha

SAP ID- 500119679

Batch-2

Objective: To demonstrate the setup of the Snyc plugin in Jenkins for Static Application Security Testing (SAST), to automatically detect vulnerabilities in their codebase during development, thereby enhancing application security before deployment

Tools required: Snyc

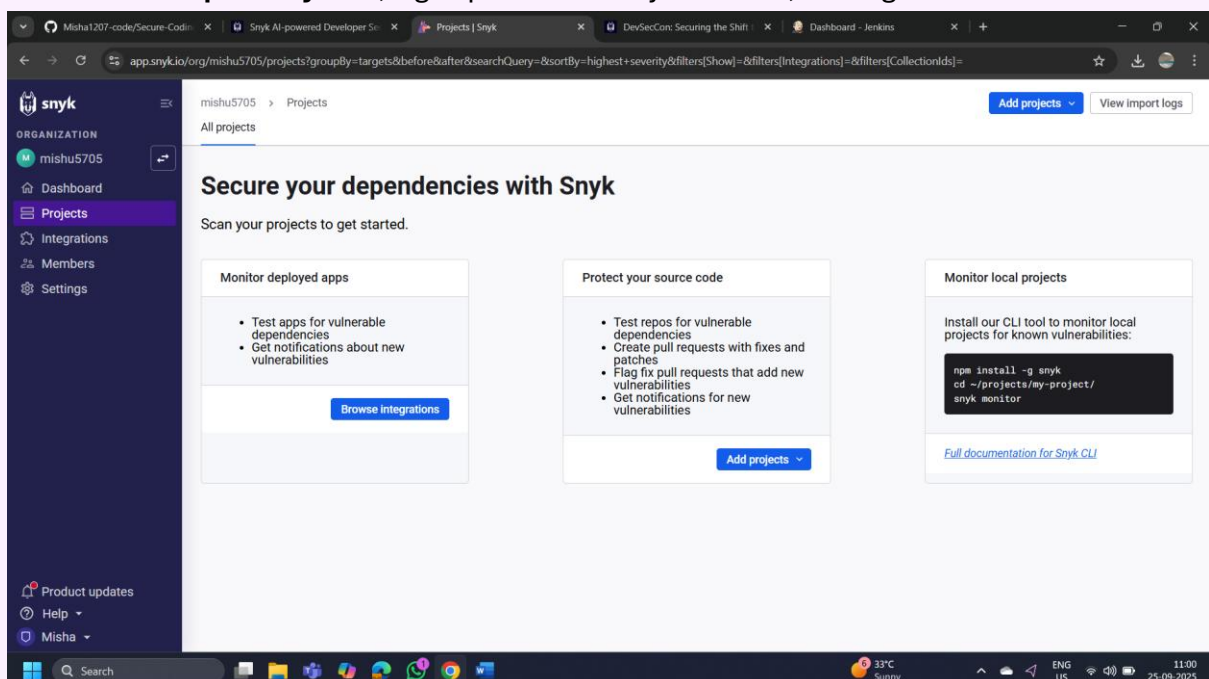
Prerequisites: None

Steps to be followed:

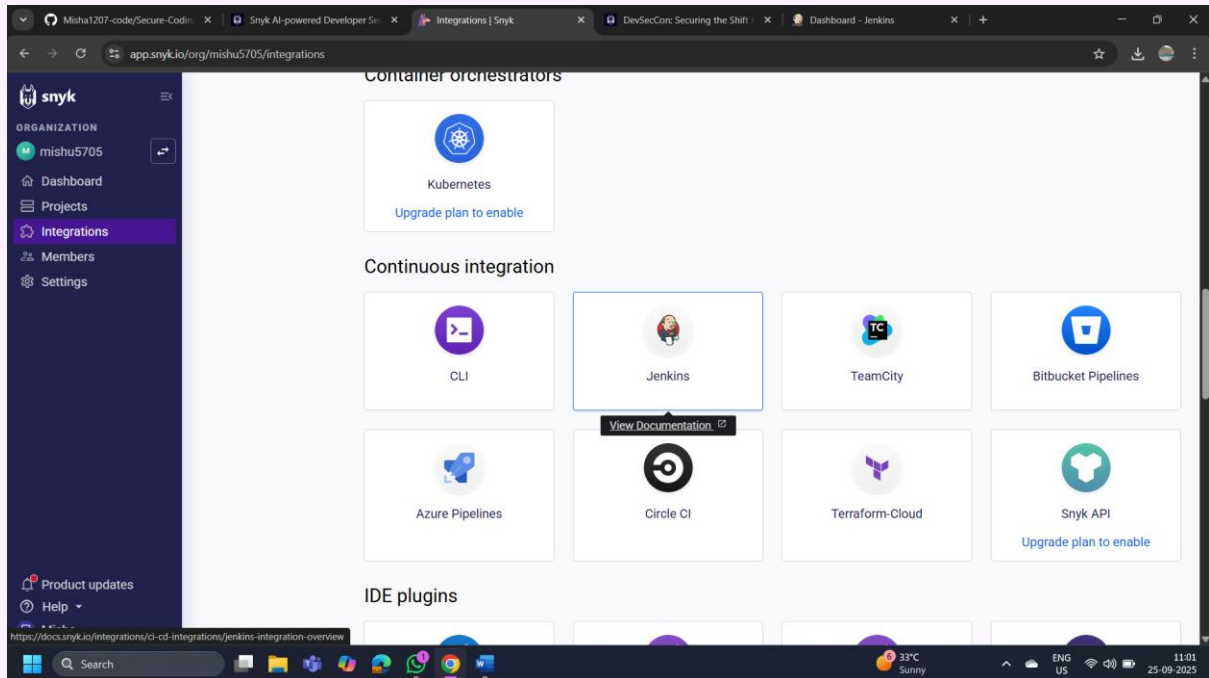
1. Configure Snyc as a SAST scan tool
2. Create and configure a Jenkins job for Snyc integration
3. Manage Snyc API and Jenkins credentials
4. Configure the Jenkins job for scanning

Step 1: Configure Snyc as a SAST scan tool

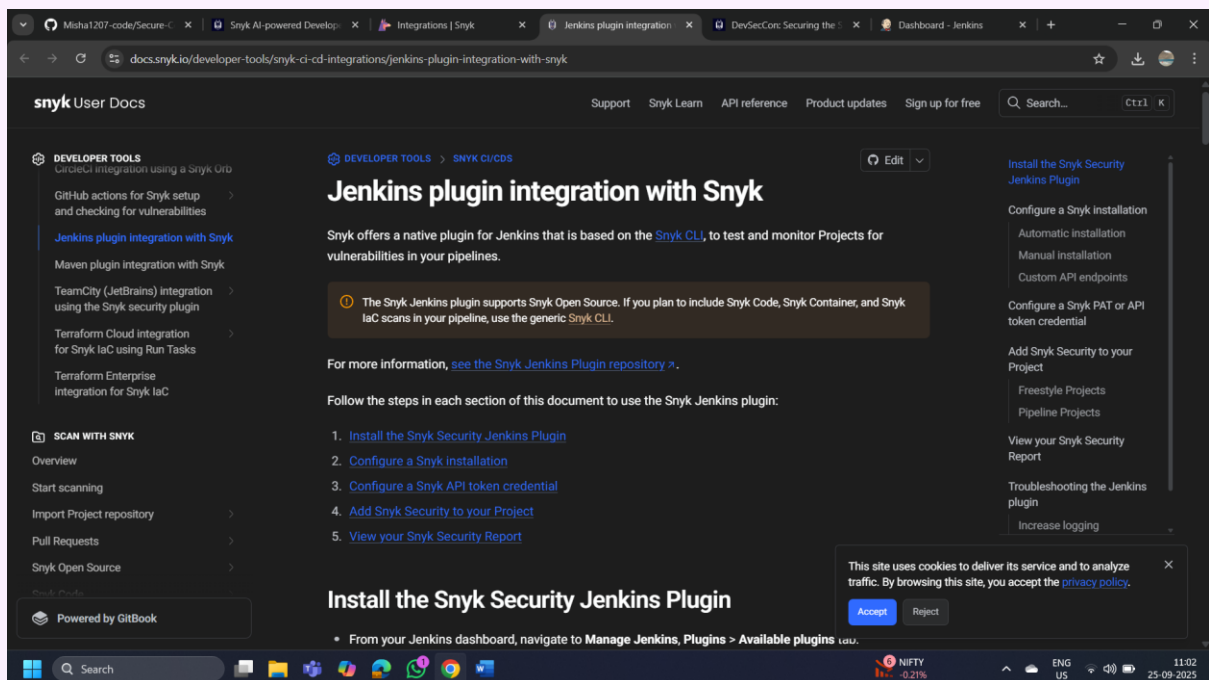
1.1 Visit <https://snyk.io/>, sign up for a new Snyc account, and log in



1.2 Navigate to **Integrations** and select **Jenkins**



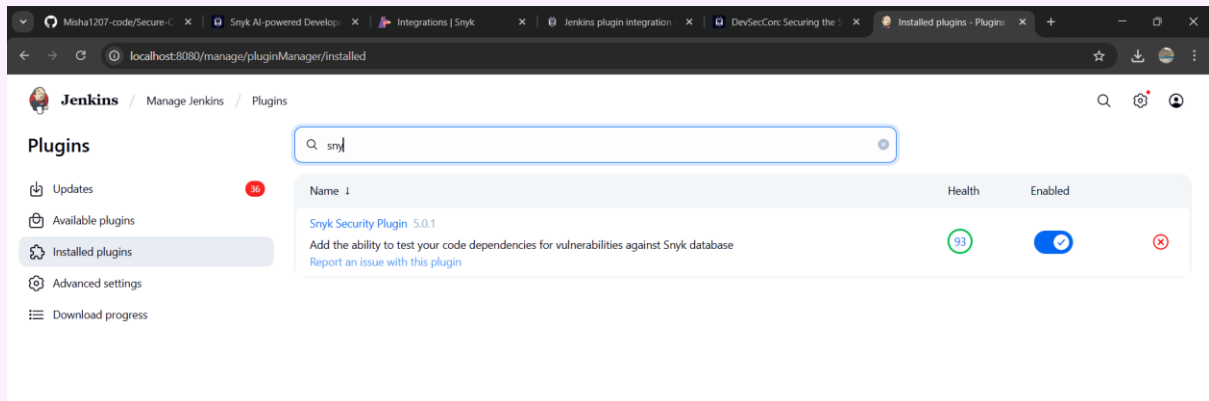
This will direct you to the documentation for integrating Snyk with Jenkins.



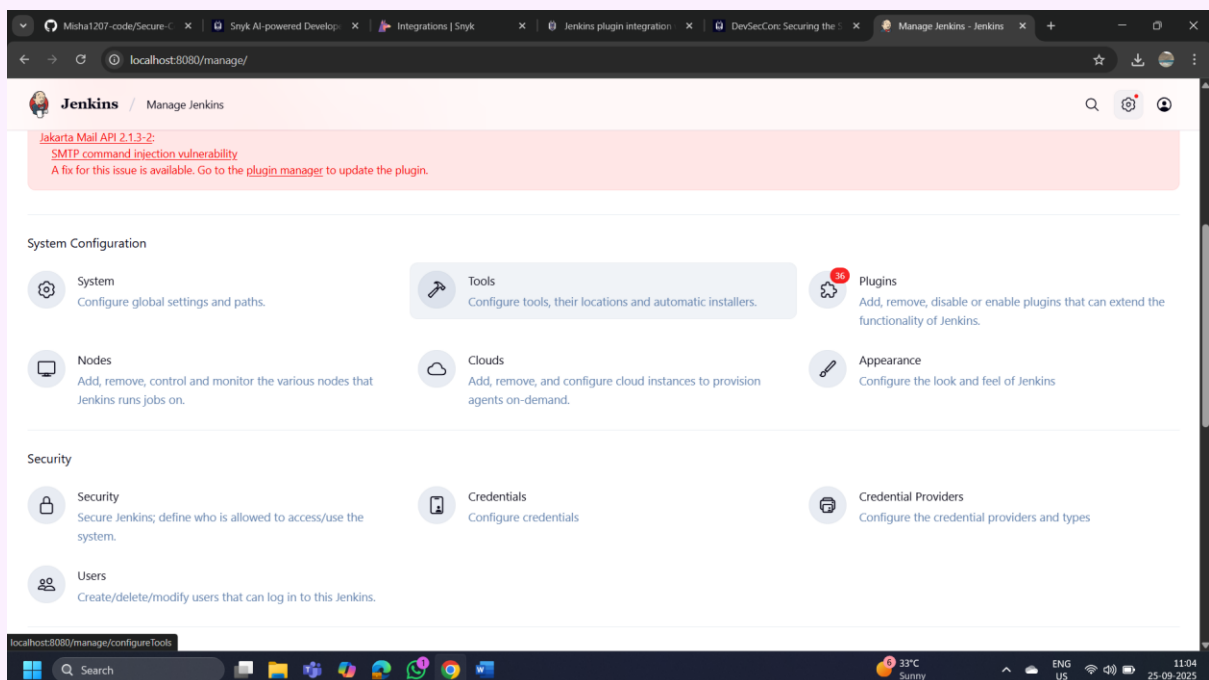
Step 2: Create and configure a Jenkins job for Snyk integration

2.1 Open Jenkins and log in to the Jenkins account:

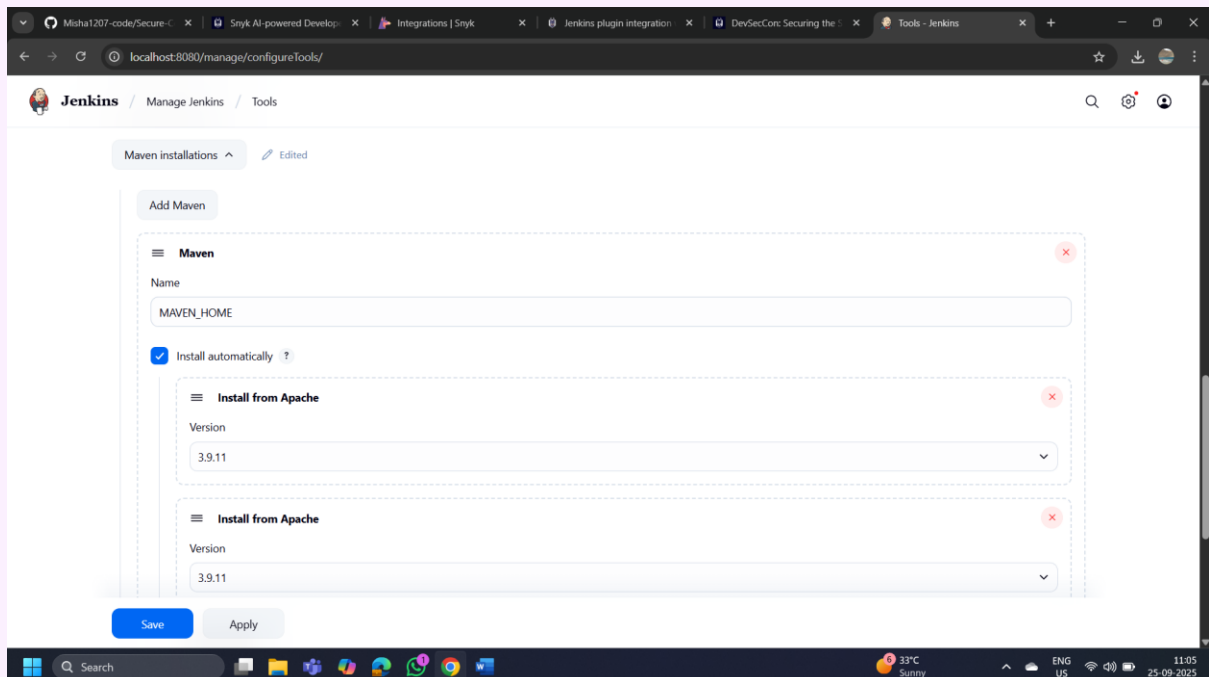
2.2 To install the Snyk plugin, navigate to **Manage Jenkins** and click **Available Plugins**, search for **Snyk Security** plugin, and then click **Install**



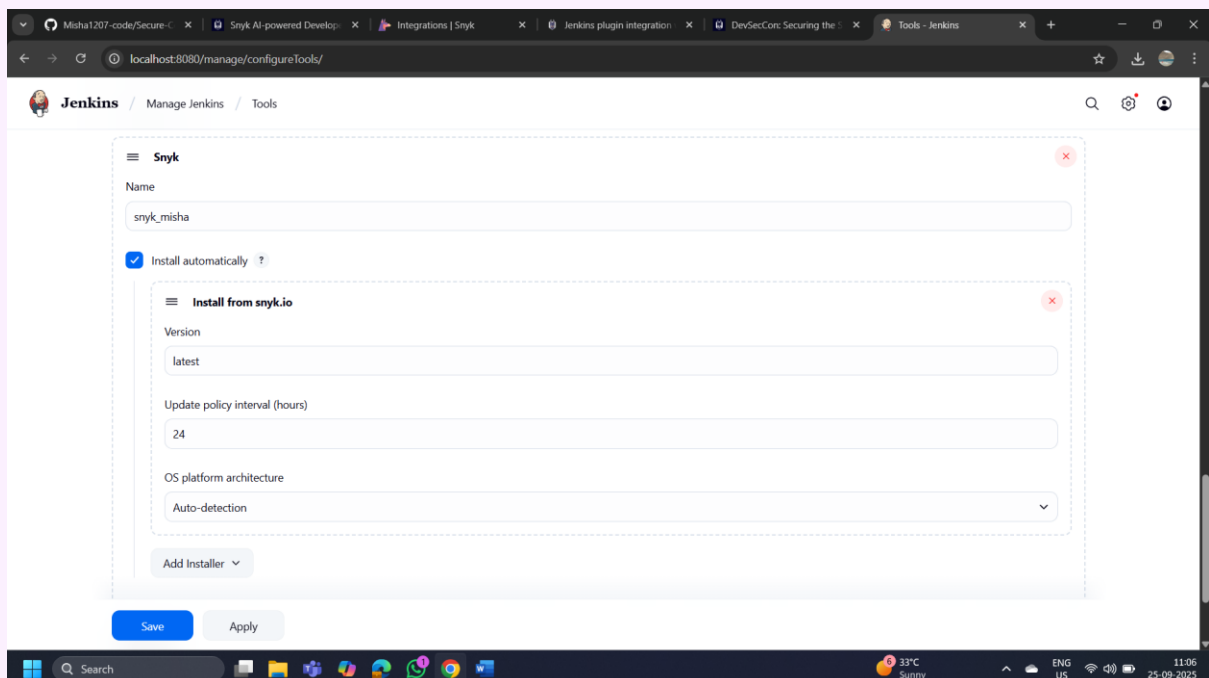
2.3 To configure Maven and Snyk in the **Global Tool Configuration**, click on **Tools** inside **Manage Jenkins**



2.4 To add Maven, click on **Add Maven** under **Maven installations** and enter **Maven** as the **Name**

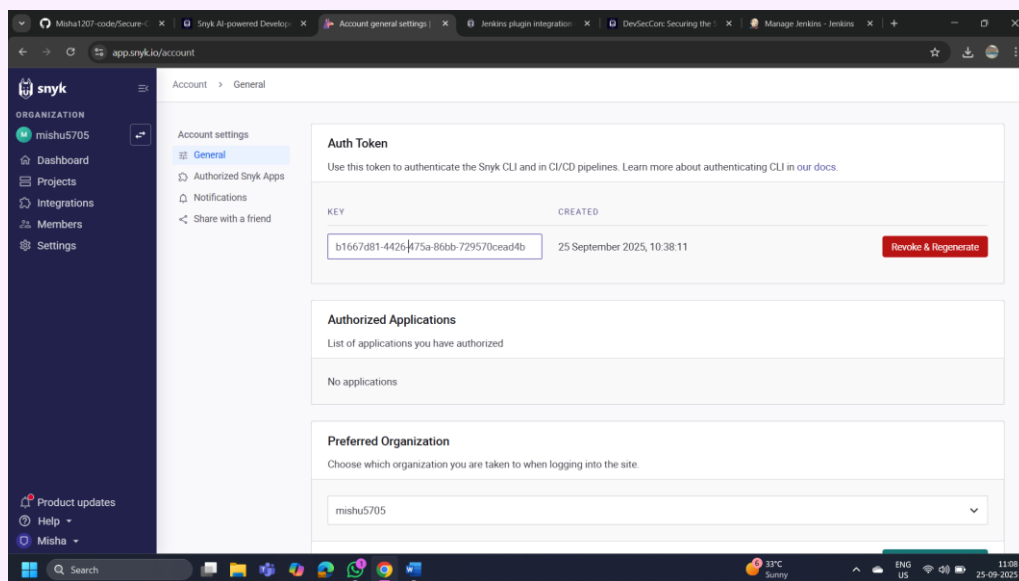
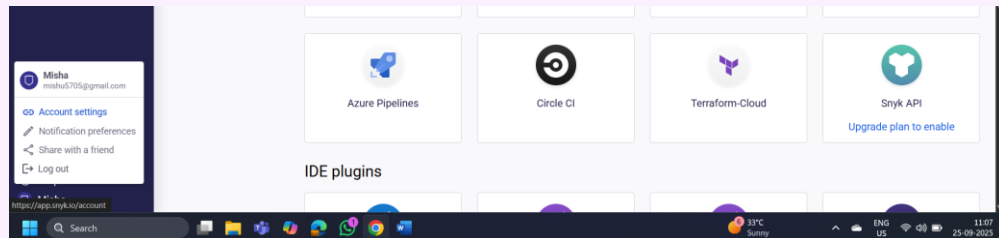


2.5 To add Snky, click on **Add Snky** under **Snyk Installations**, add **Name** as **Snyk**, and click on the **Save** button

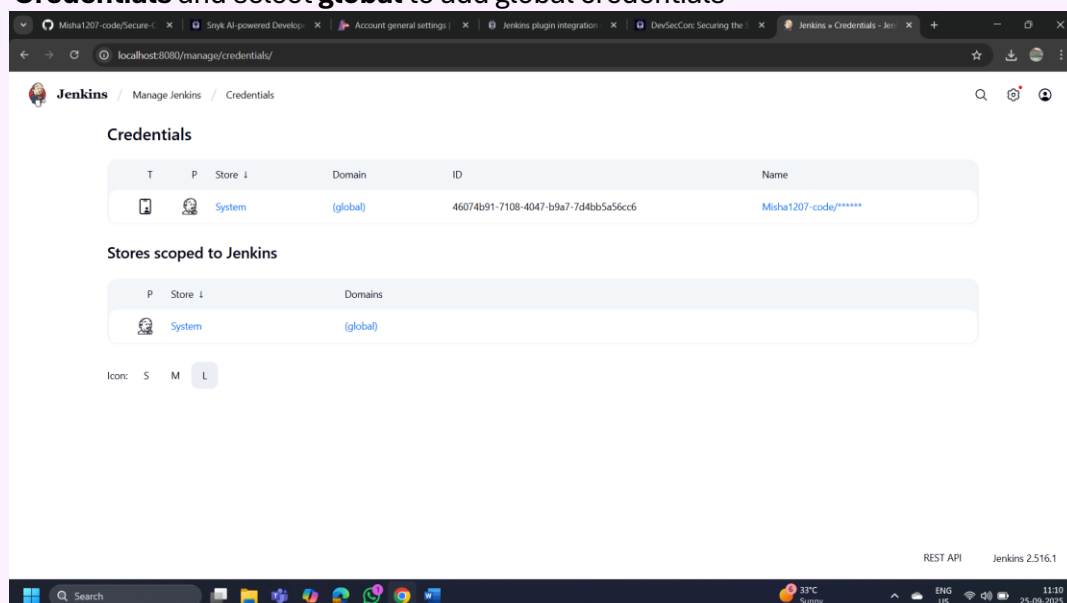


Step 3: Manage Snky API and Jenkins credentials

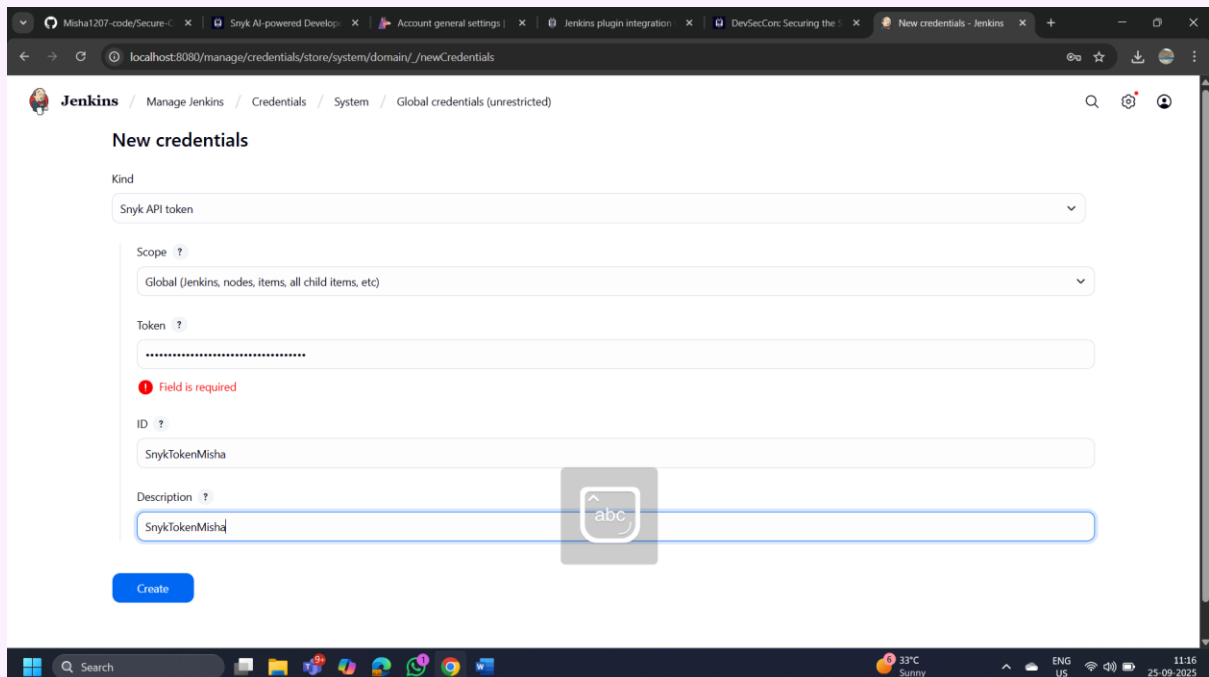
3.1 To retrieve your Snky API token, go to **Account Settings** in your Snky account, click on **Click to show** under the Auth Token key field, and copy the token for further reference



3.2 In the Jenkins interface, go to **Manage Jenkins**, select **Security**, then choose **Credentials** and select **global** to add global credentials



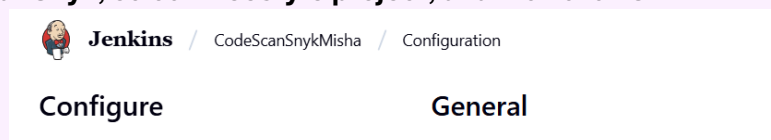
3.3 Click on **Add Credentials**, select the **Snyk API token** from the **Kind** field, paste the copied token from step 3.1 into the **Token** field, and then click the **Create** button



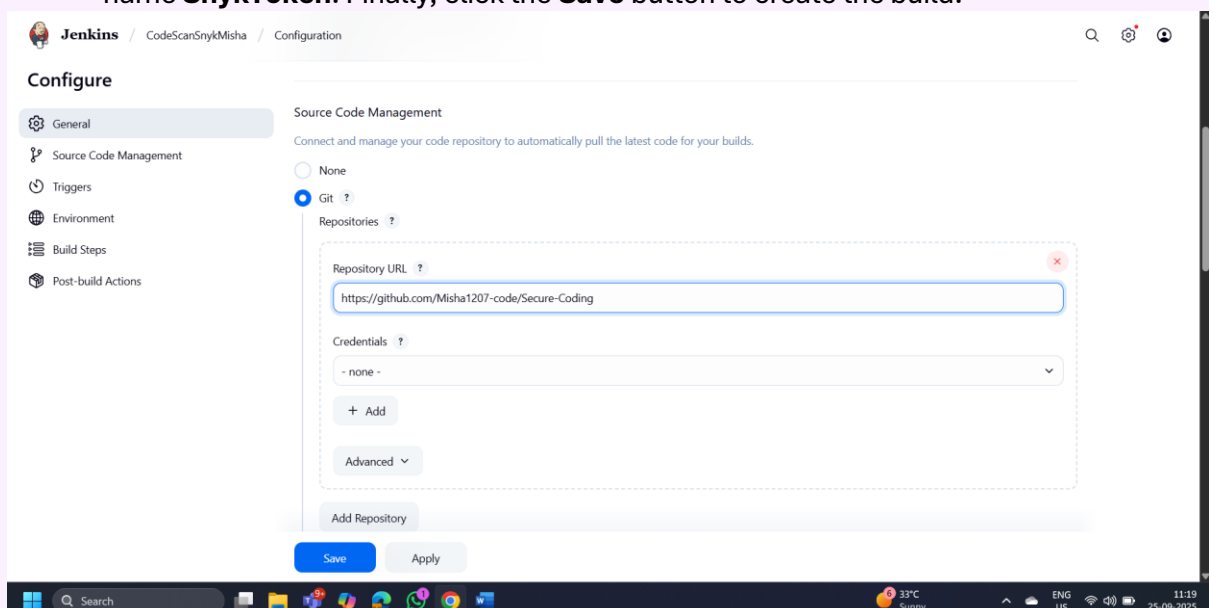
The screenshot shows the Jenkins 'New credentials' page. The 'Kind' dropdown is set to 'Snyk API token'. The 'Scope' dropdown is set to 'Global (Jenkins, nodes, items, all child items, etc)'. The 'Token' field is empty, and a red error message 'Field is required' is displayed below it. The 'ID' field contains 'SnykTokenMisha'. The 'Description' field contains 'SnykTokenMisha'. A 'Create' button is at the bottom left.

Step 4: Configure the Jenkins job for scanning

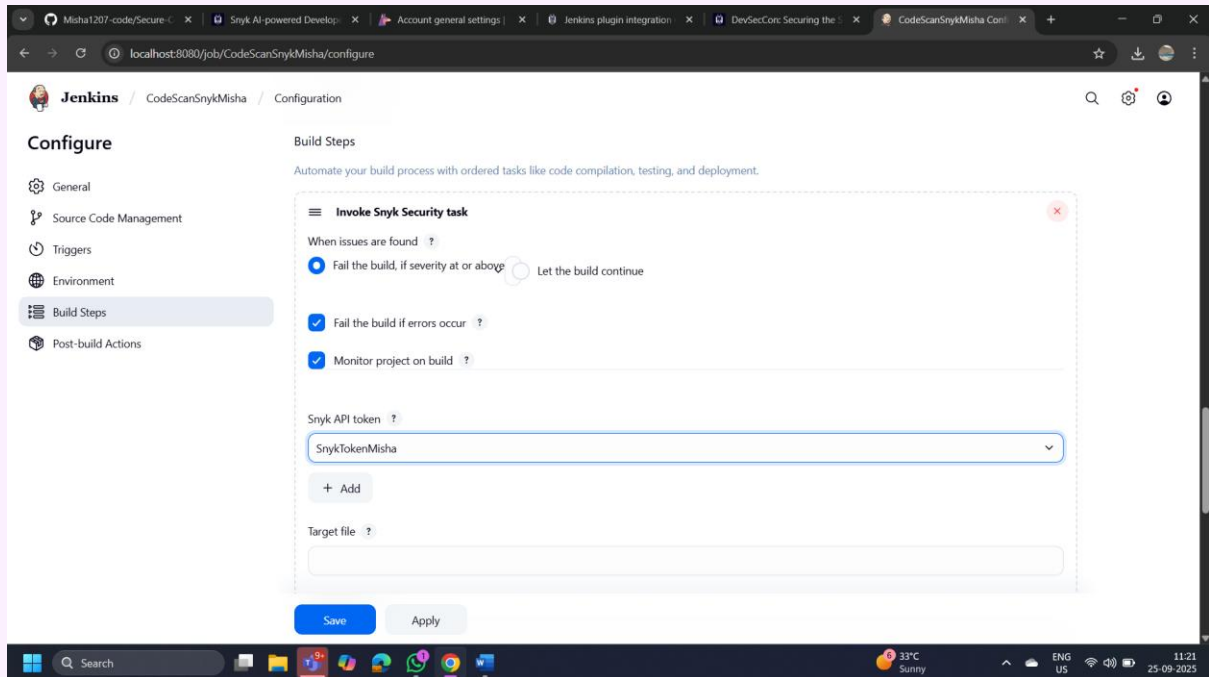
4.1 To create a new Jenkins job, click on **New Item**, enter the item name as **CodeScanSnyk**, select **Freestyle project**, and then click **OK**



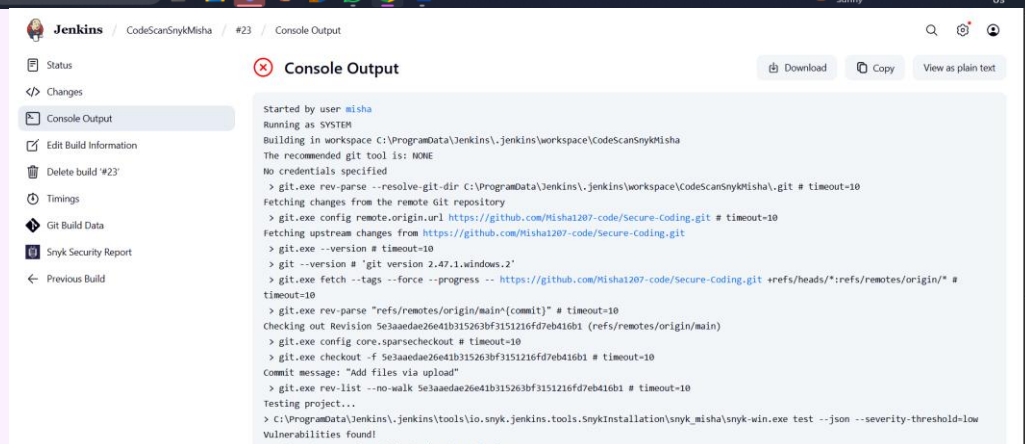
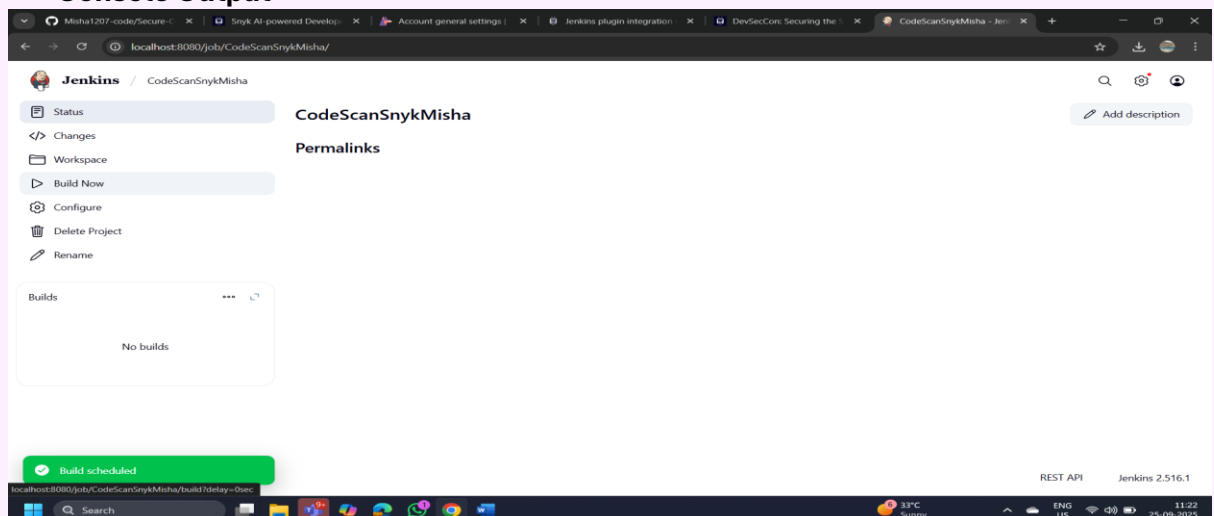
4.2 After creating a job, go to **Source Code Management** and enter the GitHub repository URL. Then, under **Build Steps**, add the build step **Invoke Snyk Security task** with the name **SnykToken**. Finally, click the **Save** button to create the build.



The screenshot shows the Jenkins 'Configure' page for a job named 'CodeScanSnykMisha'. The 'Source Code Management' section is expanded, showing the 'Repository URL' field with the value 'https://github.com/Misha1207-code/Secure-Coding'. The 'Credentials' dropdown is set to 'none'. The 'Save' button is at the bottom.



4.3 To check the build status, click on the build link under **Permalinks**. After that, click on **Console Output**



4.4 To navigate to the Snky tool to review code, scan reports under the **Projects** section

The top screenshot displays the Snyk web interface for organization 'mishu5705' under the 'Projects' section. It shows a list of projects, including 'Misha1207-code/Secure-Coding'. Below the project name, there is a table with columns: Project, Imported, Tested, and Issues. The project 'demo.secure.code.db:demo.secure.code.db' is listed with 'a minute ago' for both Imported and Tested, and a score of 0. Below the table, there is a prompt: 'Ready to import another project? Secure your entire stack with Snyk' with an 'Add projects' button.

The bottom screenshot shows the detailed view of a specific issue. The issue is titled 'commons-lang:commons-lang - Uncontrolled Recursion' with a score of 654. It is categorized as 'VULNERABILITY' with a severity of 'High'. The issue was introduced through 'org.sonarsource.scanner.maven:sonar-maven-plugin@3.9.0.2155'. The interface also shows a 'Show more detail' link and an 'Ignore' button.

By following the above steps, you have successfully demonstrated the setup of the Snyk plugin in Jenkins for static application security testing (SAST), to automatically detect vulnerabilities in their codebase during development, thereby enhancing application security before deployment.