**Lesson 09 Demo 02**

**Integrating SCA Tools into Jenkins for Enhanced Vulnerability Detection**

**Objective:** To automate SCA scans by integrating the Snyk plugin with Jenkins, enhancing the efficiency of vulnerability detection within Jenkins build jobs

**Tools required:** Jenkins, Snyk Plugin

**Prerequisites:** Basic knowledge of Jenkins and Snyk

Steps to be followed:

1. Install Snyk and Maven plugins in the Jenkins
2. Configure the Maven and Snyk installations
3. Create a new Jenkins pipeline job

**Step 1: Install Snyk and Maven plugins in the Jenkins**

* 1. Log in to your Jenkins dashboard and click on **Manage Jenkins**

A screenshot of a computer

Description automatically generated

* 1. Navigate to **System Configuration** and click on **Plugins**

A screenshot of a computer

Description automatically generated

* 1. In the **Available Plugins** section, enter **snyk** in the search bar, select the **Snyk Security** plugin, and click **Install**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The **Snyk Security** plugin is successfully installed.

* 1. Go to **Manage Jenkins** in the Jenkins dashboard

A screenshot of a computer

Description automatically generated

* 1. Navigate to **System Configuration** and click on **Plugins**

A screenshot of a computer

Description automatically generated

* 1. In the **Available Plugins** section, enter **maven** in the search bar, select the **Maven Integration** plugin, and click **Install**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The **Maven Integration** plugin is successfully installed.

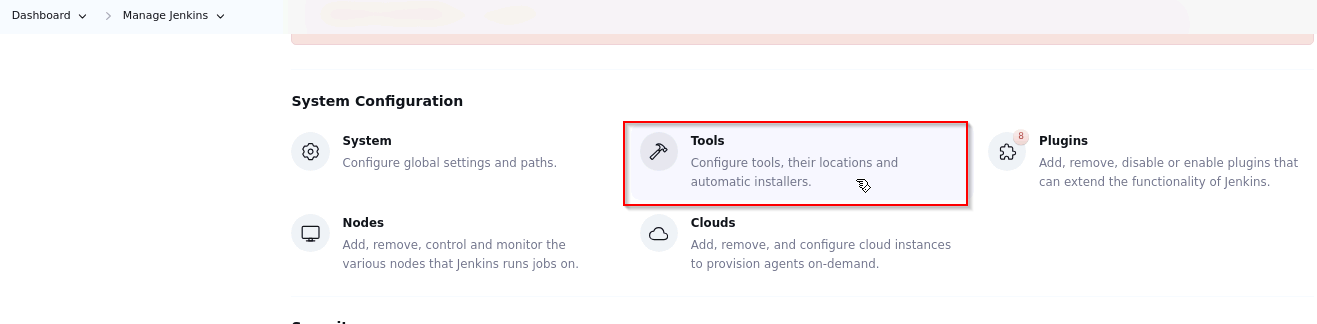
**Step 2: Configure the Maven and Snyk installations**

* 1. Go tothe Jenkins dashboard and click on **Manage Jenkins**

A screenshot of a computer

Description automatically generated

* 1. Navigate to **System Configuration** and click on **Tools**



* 1. Under **Maven Installations**, click on **Add Maven**

A screenshot of a computer

Description automatically generated

* 1. Type **Maven** in the **Name** field and then click on **Save**

A screenshot of a computer

Description automatically generated

* 1. Under **Snyk Installations,** click on **Add Snyk**

A white rectangular object with blue and green lines

Description automatically generated with medium confidence

* 1. Type **Snyk** in the **Name** field and then click on **Save**

A screenshot of a computer

Description automatically generated

Now you need to get the API token from Snyk, so follow the below steps for getting the API token.

* 1. Visit **https://snyk.io/** and create a new Snyk account

A screenshot of a website

Description automatically generated

* 1. Click on the **Account settings** option

A screenshot of a computer

Description automatically generated

* 1. Under the **Auth Token** section, click the **click to show** button under the **KEY** field to reveal the hidden token key

A screenshot of a computer

Description automatically generated

* 1. Under the **Auth Token** section, click the **Click to Show button** under the **KEY** field to reveal the hidden token key

A screenshot of a computer

Description automatically generated

* 1. Copy the Snyk authentication token

A screenshot of a computer

Description automatically generated

* 1. Navigate back to the Jenkins dashboard and click on **Manage Jenkins**

A screenshot of a computer

Description automatically generated

* 1. Select the **Credentials** option under **Manage Jenkins**

A screenshot of a computer

Description automatically generated

* 1. Click on the **global** option under the **Domains** column

A screenshot of a computer

Description automatically generated

* 1. Select **Snyk API token** under the **Kind** field, paste the copied key from step 2.11 in the **Token** field, select ID as **SnykToken,** and click on **Create**

A screenshot of a computer

Description automatically generated

**Step 3: Create a new Jenkins pipeline job**

* 1. Go to the Jenkins dashboard and click on **New Item**

A screenshot of a computer

Description automatically generated

* 1. Enter the item name as **SCAPipeline**, select the type as **Pipeline,** and click on the **OK** button

A screenshot of a computer

Description automatically generated

* 1. Enter the below code in the pipeline script and click on **Save**:

**pipeline {**

**agent any**

**tools {**

**maven "Maven"**

**snyk "Snyk"**

**}**

**stages {**

**stage('Build & Test Automation') {**

**steps {**

**// Get some code from a GitHub repository**

**git 'https://github.com/anujdevopslearn/SonarQubeCoverageJava/'**

**// Run Maven on a Unix agent.**

**sh "mvn -Dmaven.test.failure.ignore=true clean package"**

**}**

**post {**

**success {**

**junit '\*\*/target/surefire-reports/\*.xml'**

**archiveArtifacts 'target/\*.jar'**

**}**

**}**

**}**

**stage('SCA Scan') {**

**steps {**

**snykSecurity snykInstallation: 'Snyk', snykTokenId: 'SnykToken'**

**}**

**}**

**}**

**}**

A screenshot of a computer

Description automatically generated

* 1. Click on the **Build Now** option to execute the job

A screenshot of a phone

Description automatically generated

The output of the build will be as shown below:

A screenshot of a computer

Description automatically generated

* 1. Navigate to the Synk interface and click on the **Projects** tab

A screenshot of a computer

Description automatically generated

You can review code scan reports. In case of any vulnerabilities, it would be mentioned on the portal. You can validate the vulnerability report from Snyk to understand the security-related bugs.

A screenshot of a computer

Description automatically generated

By following these steps, you have effectively demonstrated how to automate SCA scans by integrating the Snyk plugin with Jenkins, enhancing the efficiency of vulnerability detection within Jenkins build jobs.