Lab Exercise 19
Setting up Snyk for SAST in Jenkins

Objective: To demonstrate 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

Tools required: Snyk

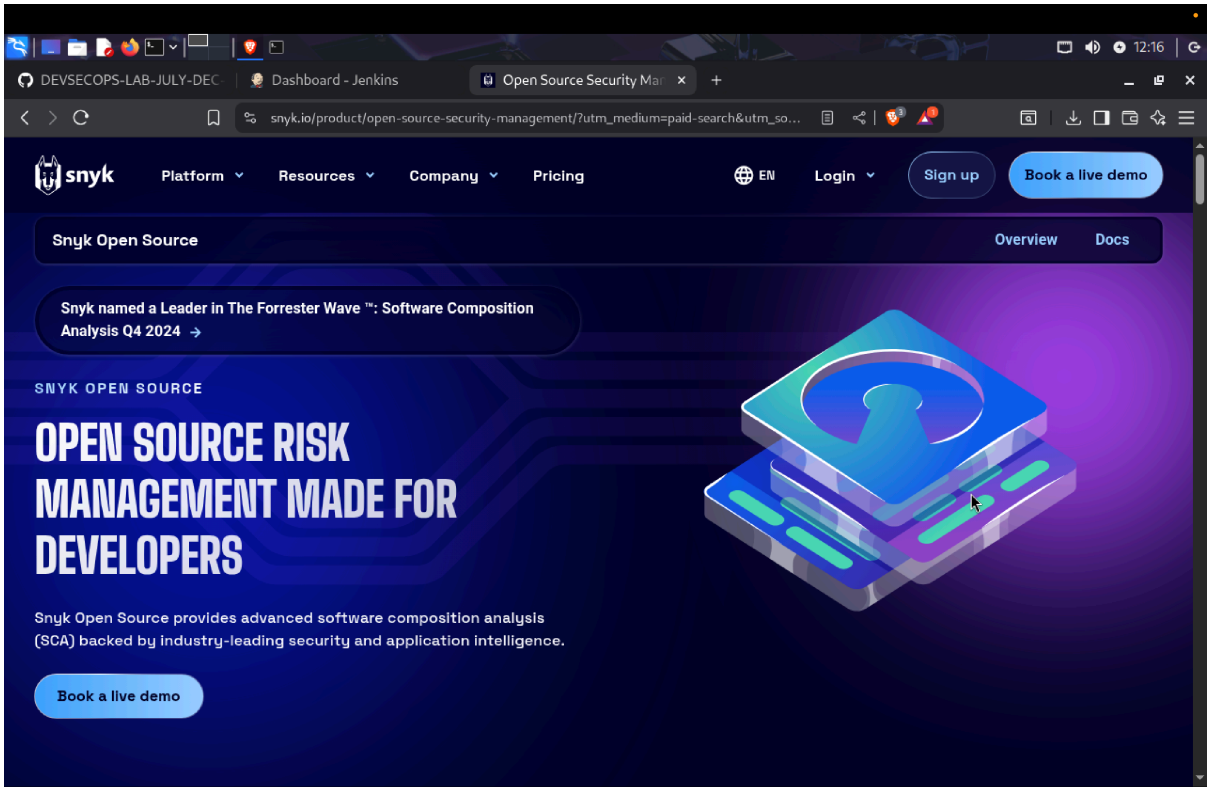
Prerequisites: None

Steps to be followed:

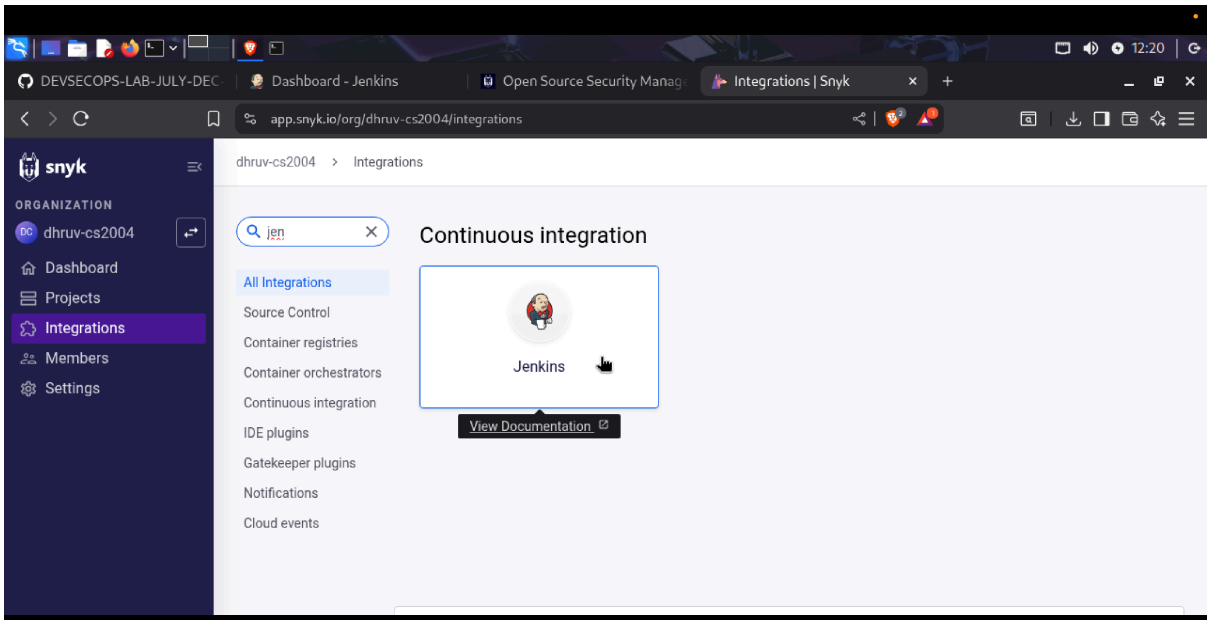
1. Configure Snyk as a SAST scan tool
2. Create and configure a Jenkins job for Snyk integration
3. Manage Snyk API and Jenkins credentials
4. Configure the Jenkins job for scanning

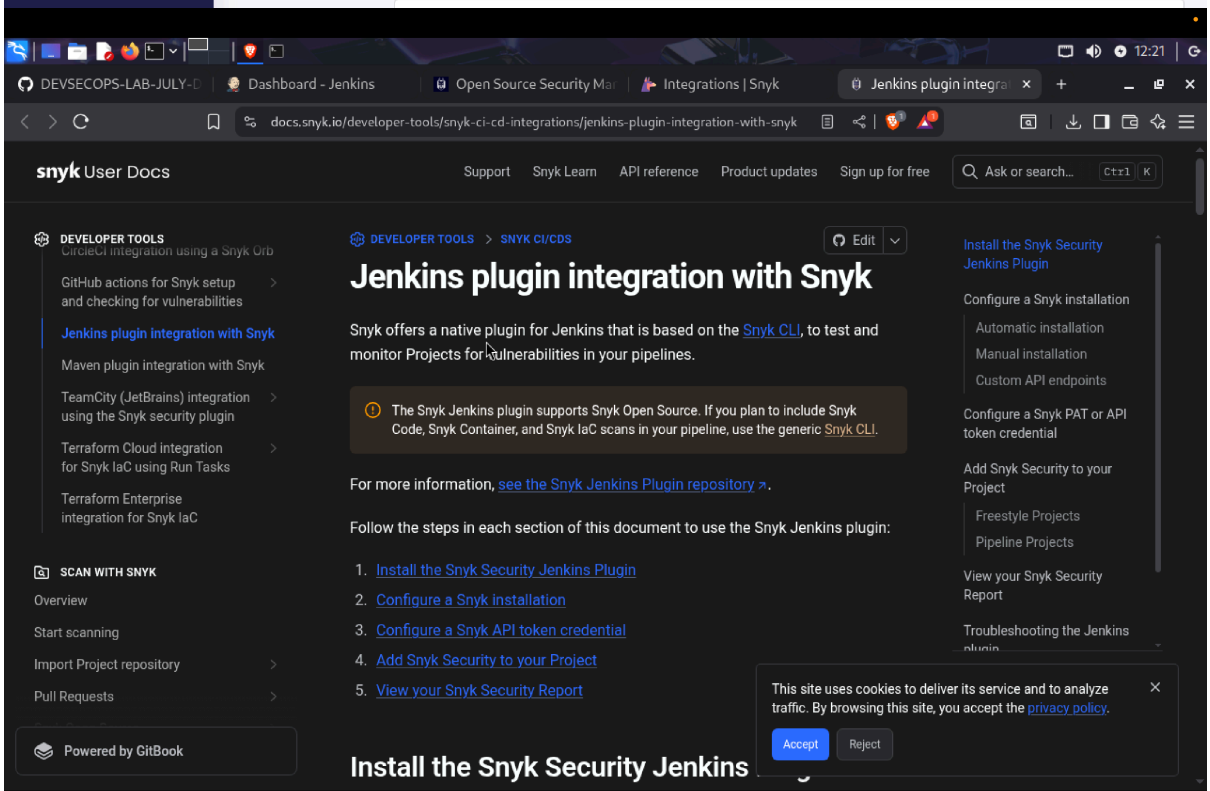
Step 1: Configure Snyk as a SAST scan tool

1. Visit **https://snyk.io/**, sign up for a new Snyk account, and log in



2. Navigate to **Integrations** and select **Jenkins**

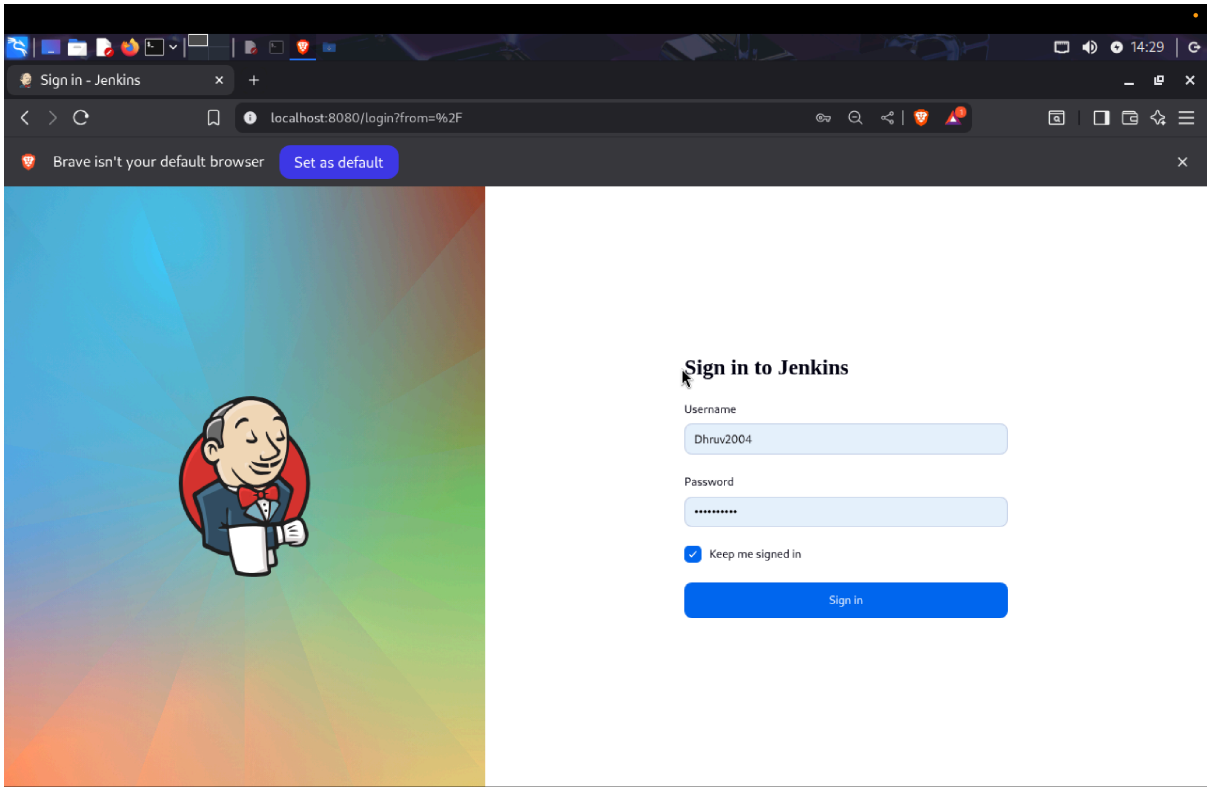




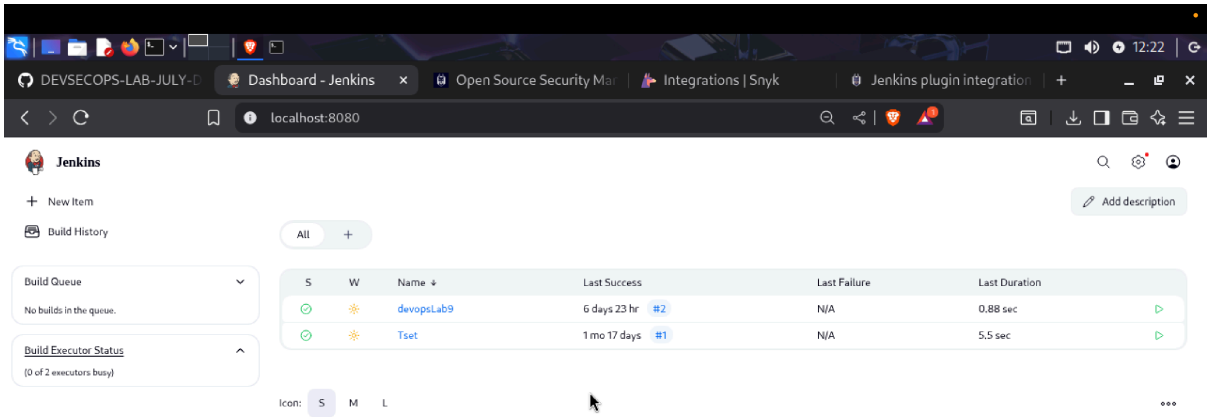
This will direct you to the documentation for integrating Snyk with Jenkins.

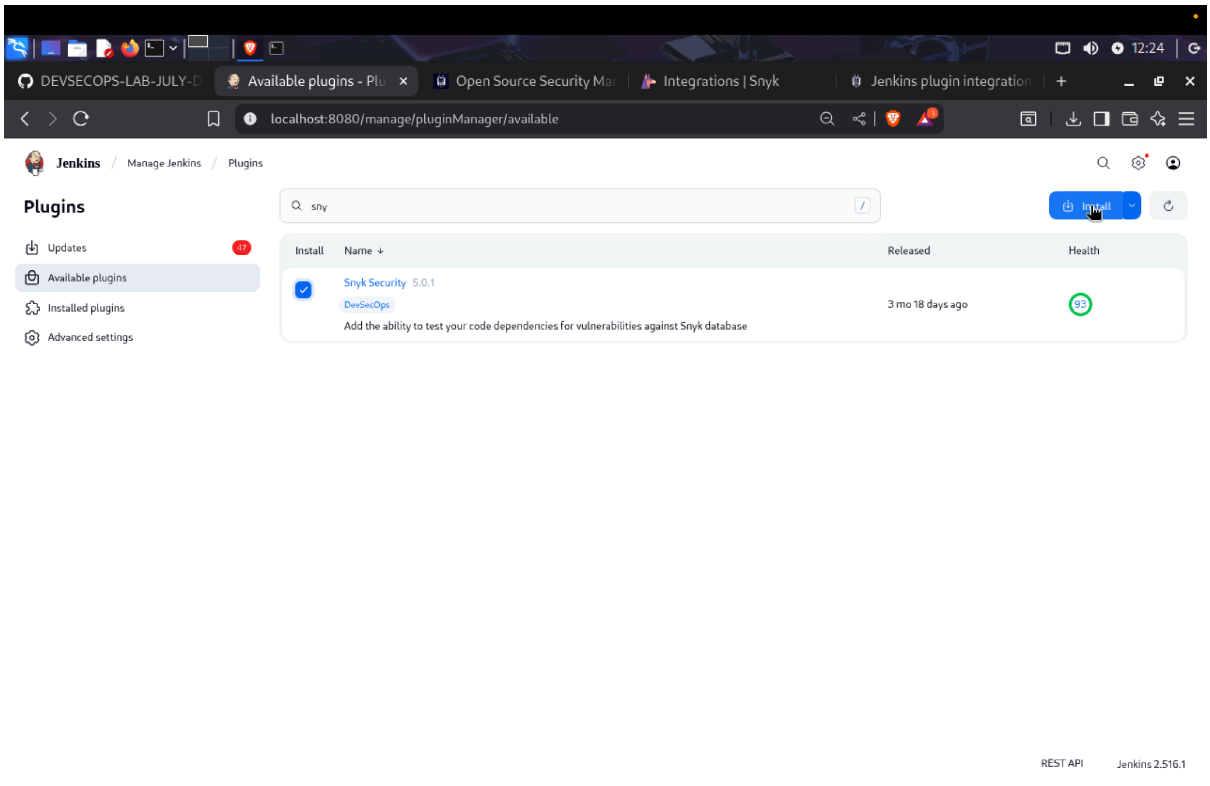
Step 2: Create and configure a Jenkins job for Snyk integration

1. Open Jenkins and log in to the Jenkins account:

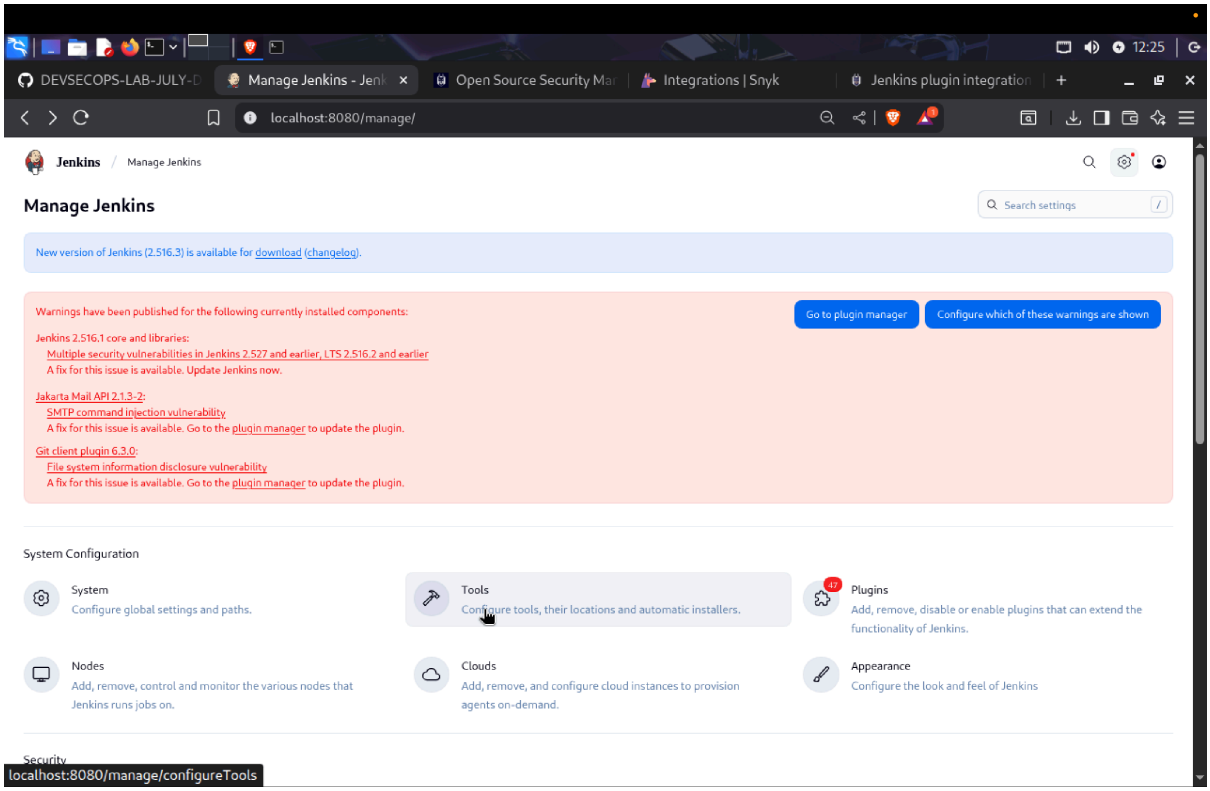


To install the Snyk plugin, navigate to **Manage Jenkins** and click **Available Plugins**, search for **Snyk Security** plugin, and then click **Install**

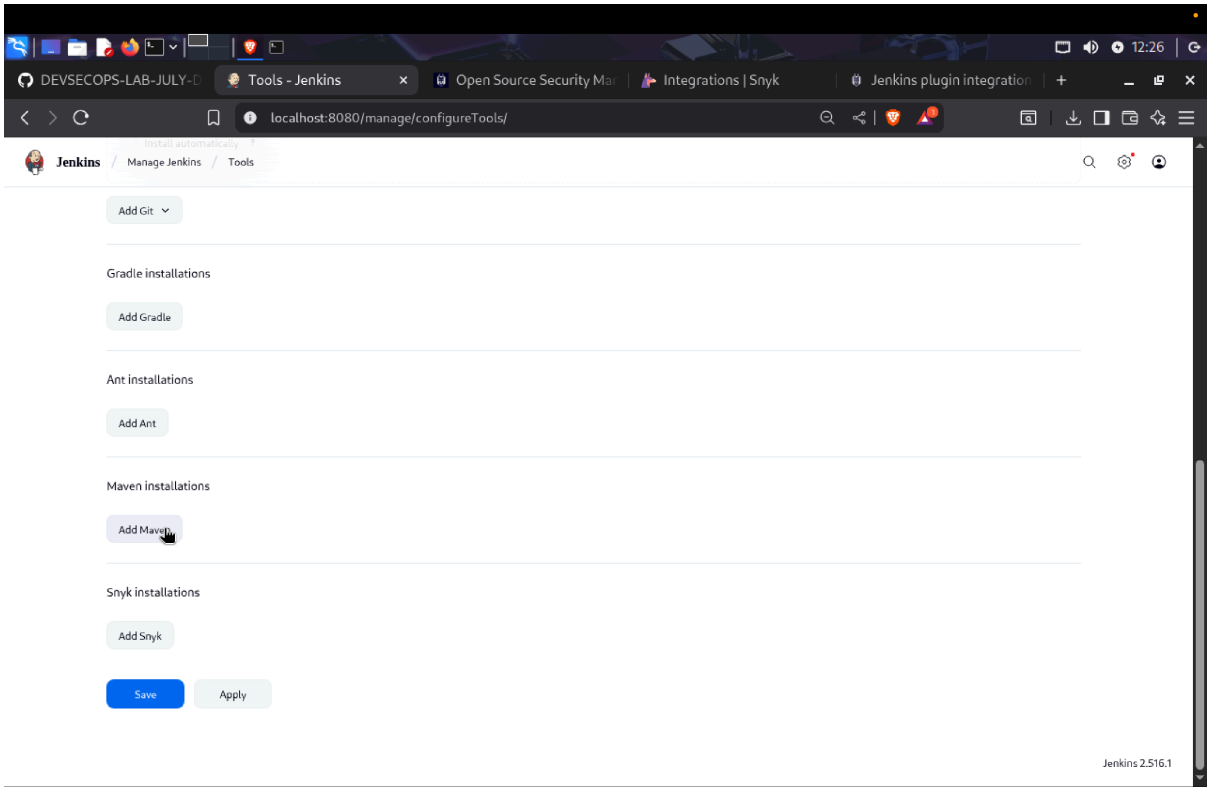


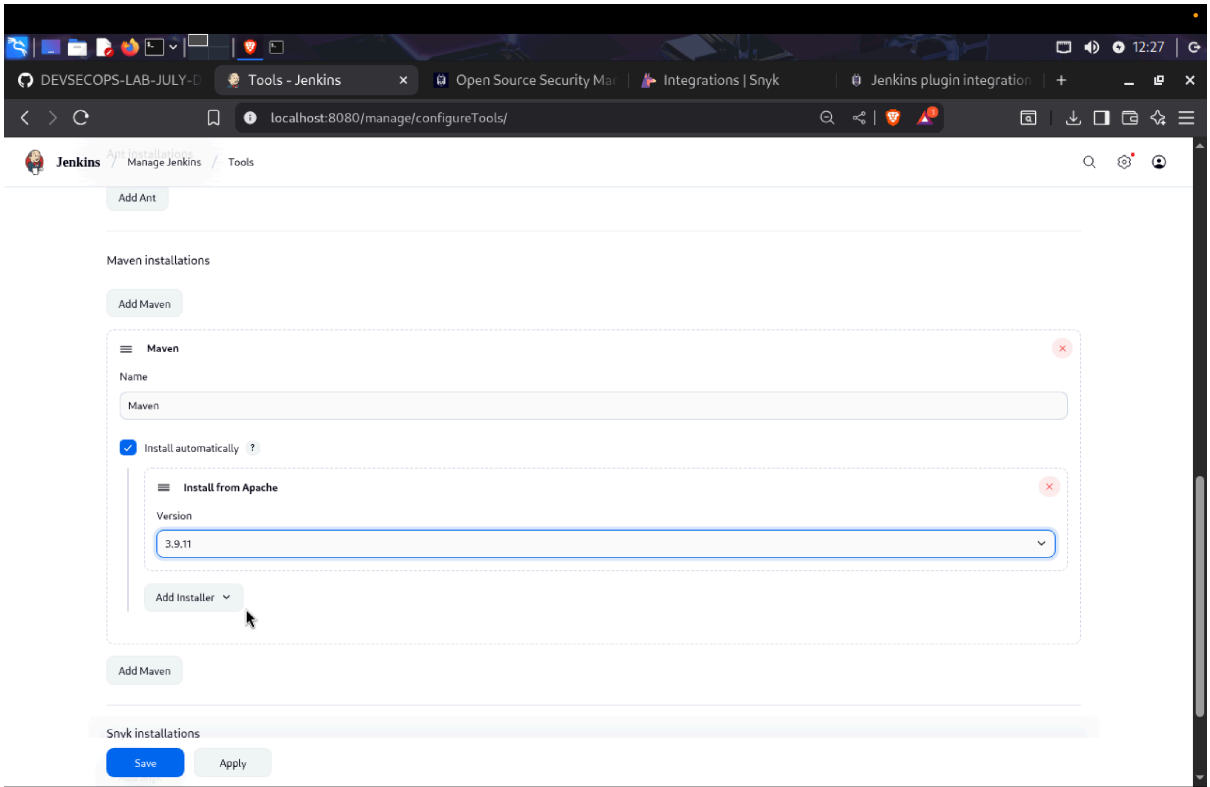


2. To configure Maven and Snyk in the **Global Tool Configuration**, click on **Tools** inside **Manage Jenkins**

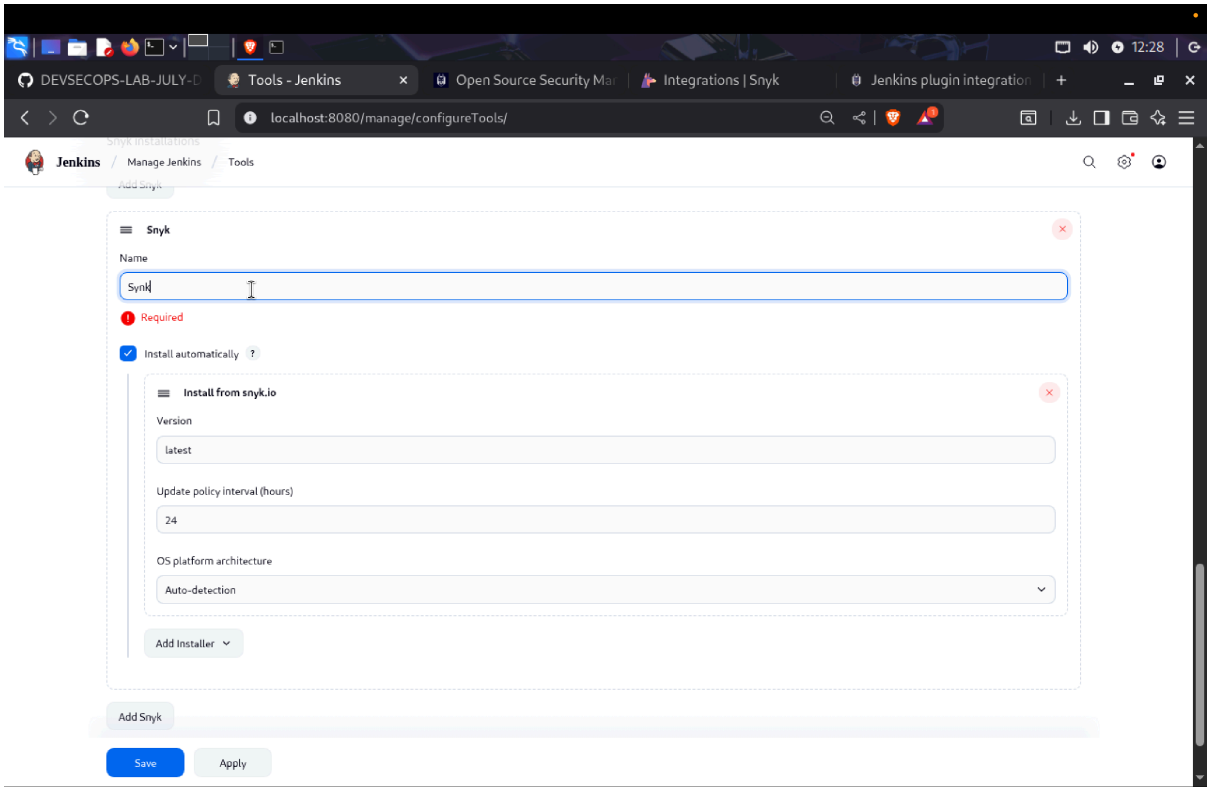


3. To add Maven, click on **Add Maven** under **Maven installations** and enter **Maven** as the **Name**



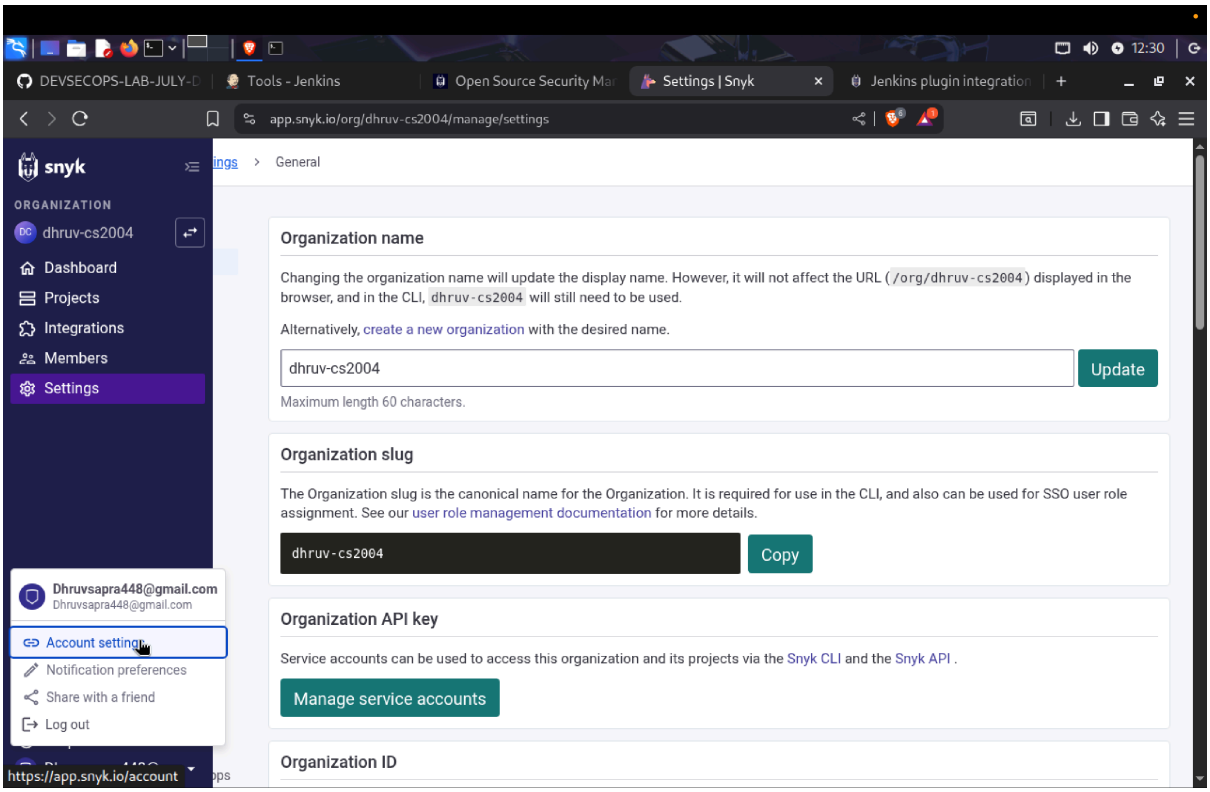


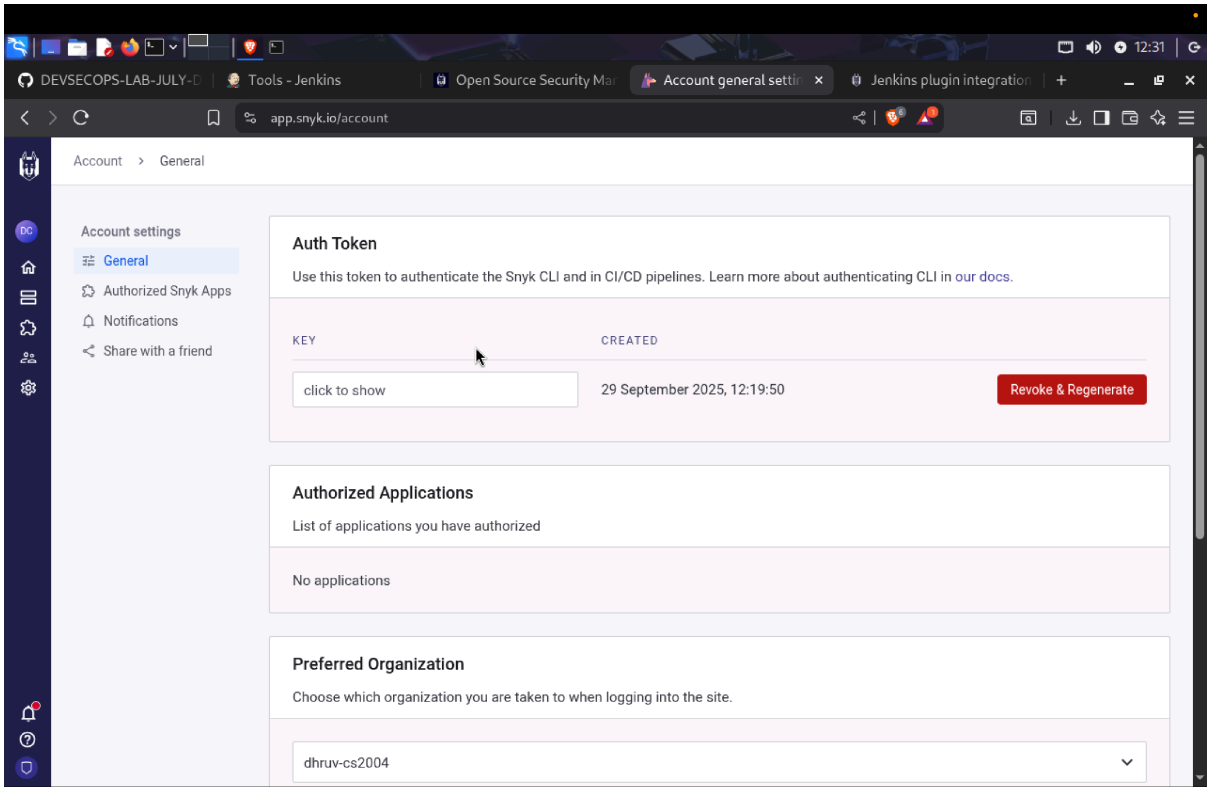
4. To add Snyk, click on **Add Snyk** under **Snyk Installations,** add **Name** as **Synk,** and click on the **Save** button

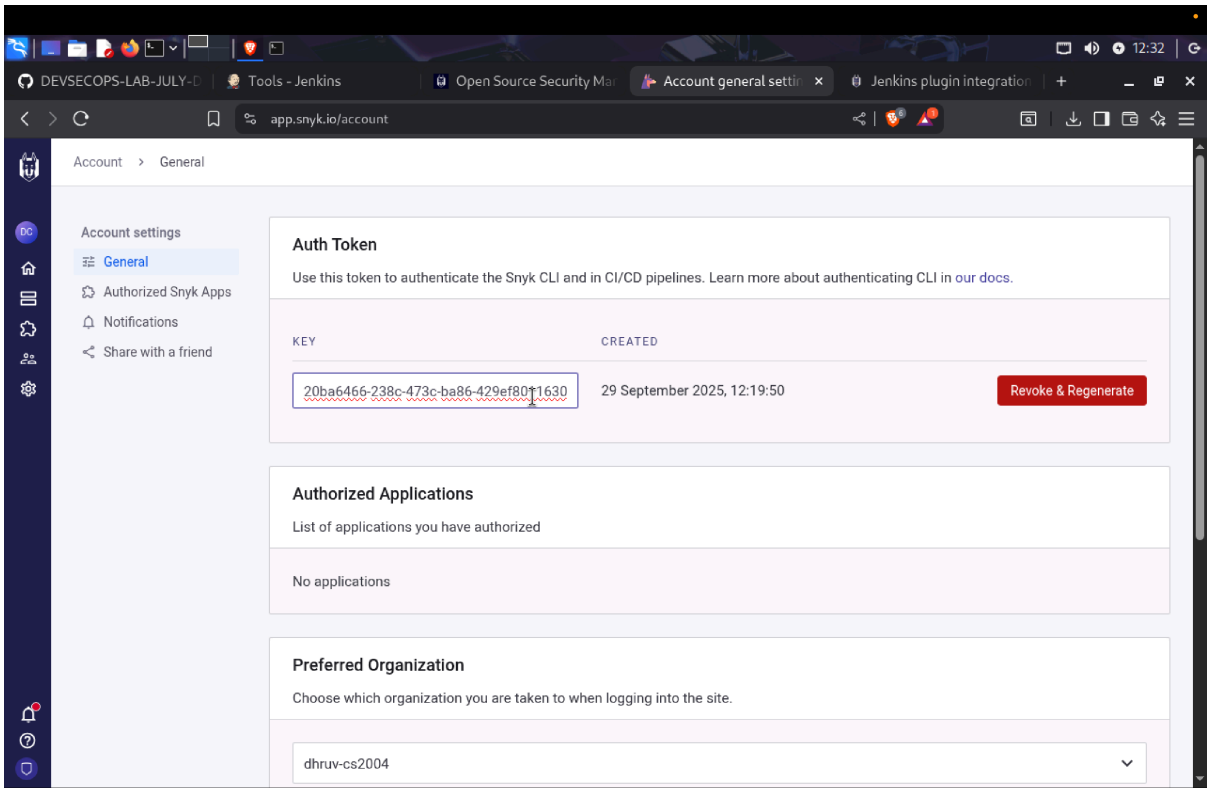


Step 3: Manage Snyk API and Jenkins credentials

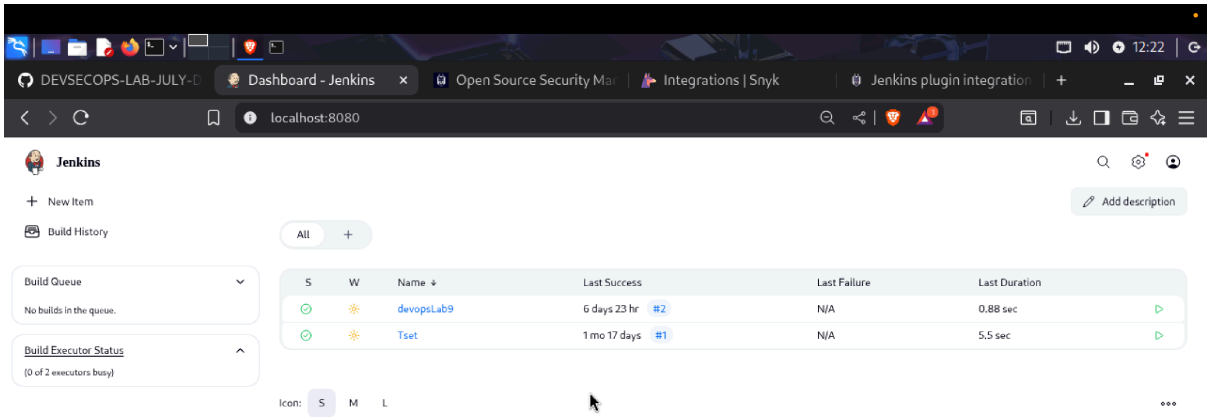
1. To retrieve your Snyk API token, go to **Account Settings** in your Snyk account, click on **Click to show** under the Auth Token key field, and copy the token for further reference

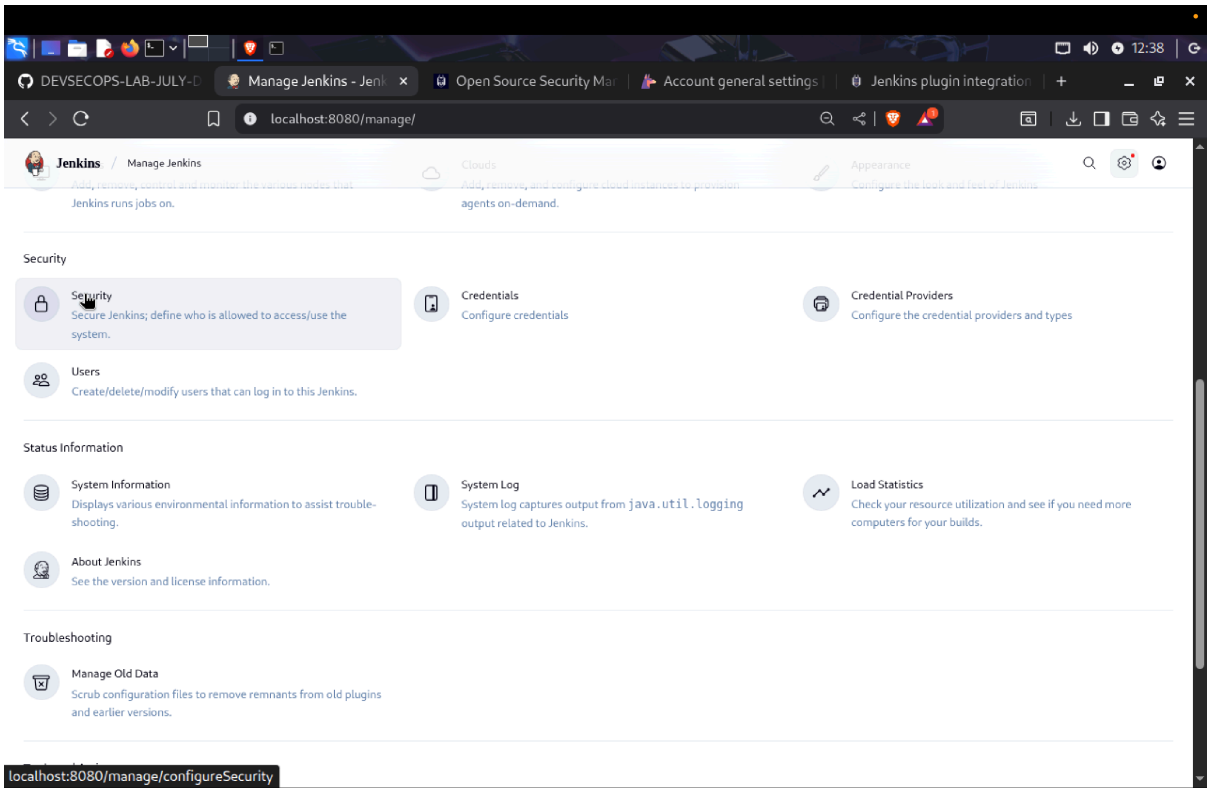


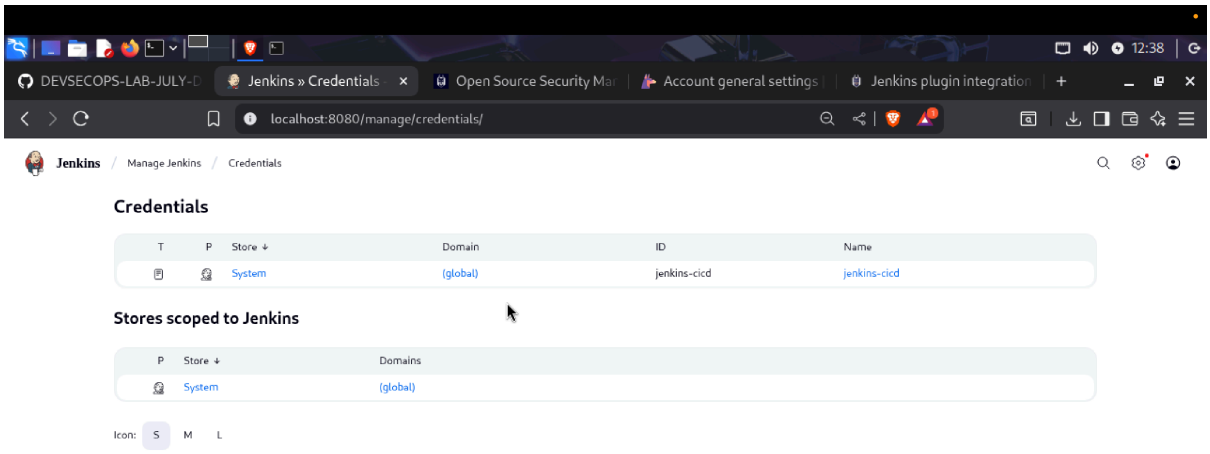




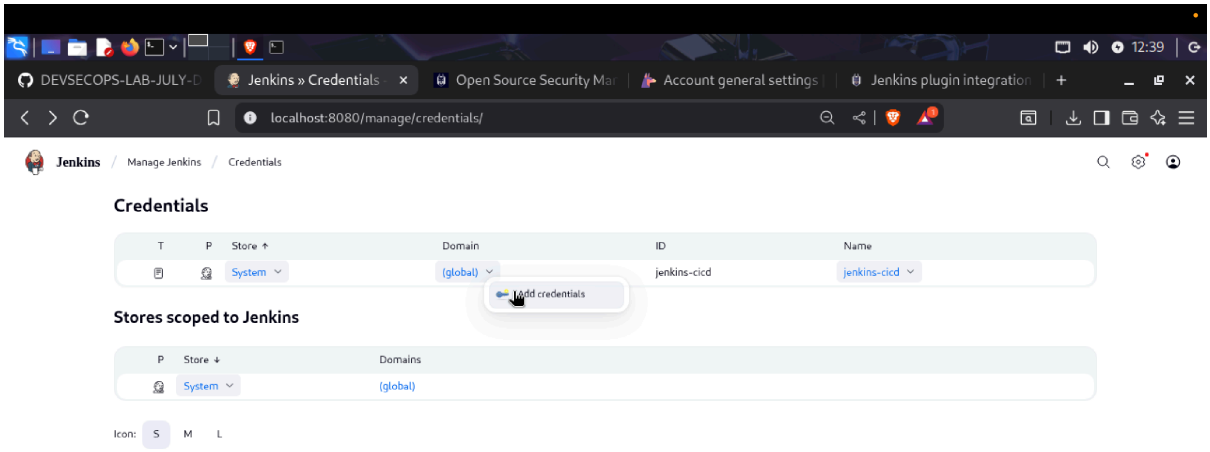
2. In the Jenkins interface, go to **Manage Jenkins,** select **Security**, then choose **Credentials** and select **global** to add global credentials

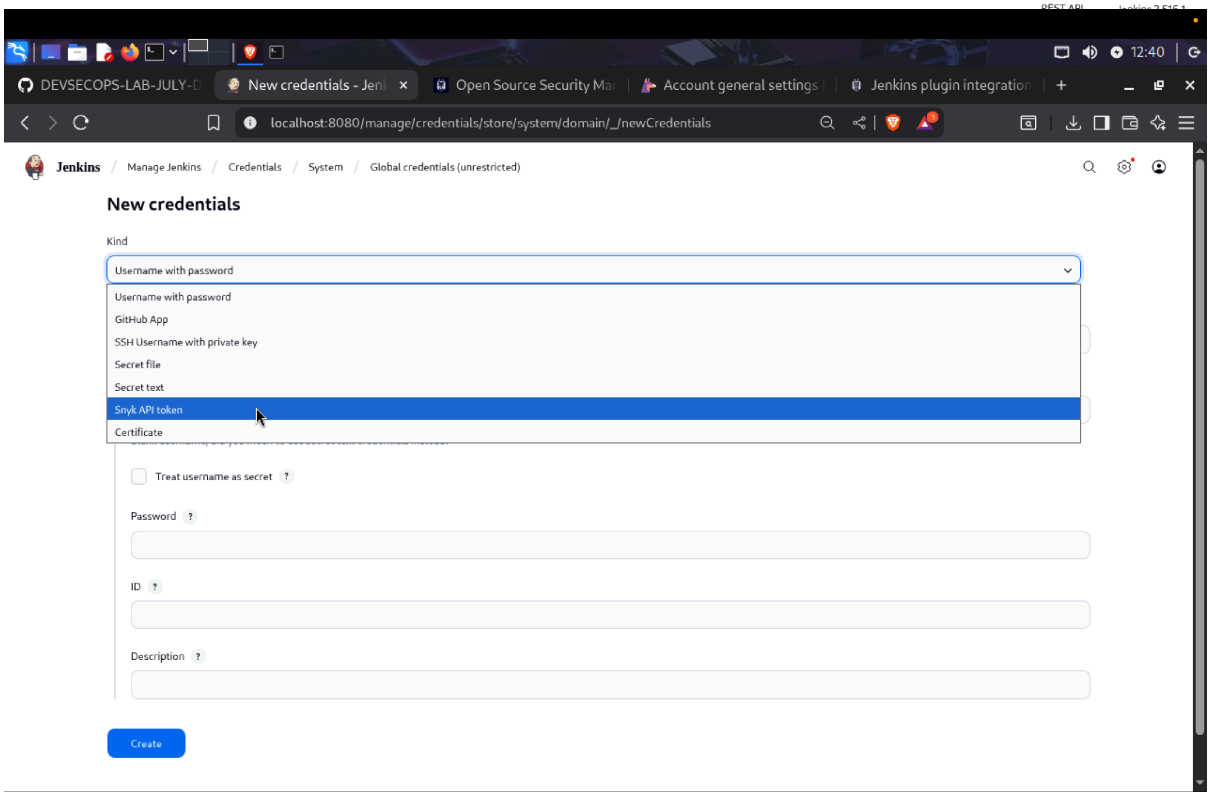


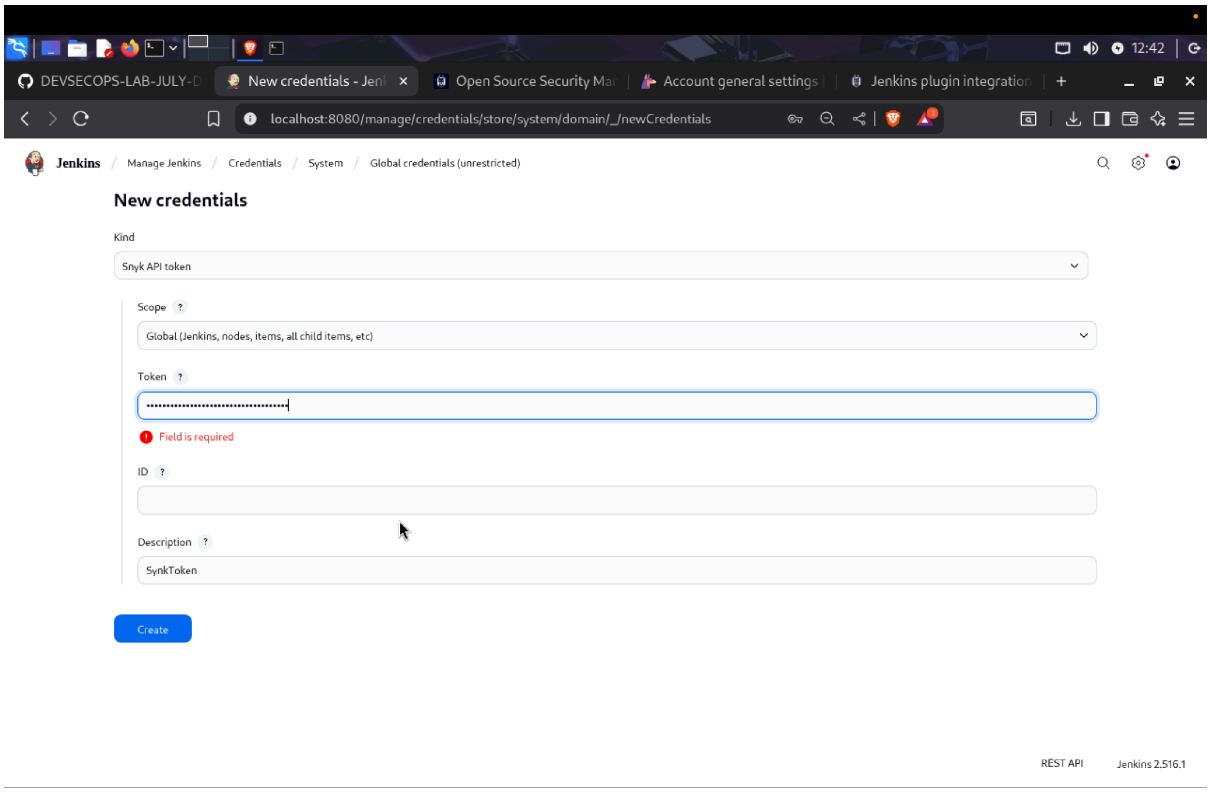

DEVSECOPS-LAB-JULY-D
Manage Jenkins - Jenk
Open Source Security Mar
Account general settings
Jenkins plugin integration
12:38
localhost:8080/manage/
Jenkins / Manage Jenkins
Jenkins runs jobs on.
Clouds
agents on-demand.
Appearance
Security
Security
Secure Jenkins; define who is allowed to access/use the system.
Credentials
Configure credentials
Credential Providers
Configure the credential providers and types
Users
Create/delete/modify users that can log in to this Jenkins.
Status Information
System Information
Displays various environmental information to assist trouble-shooting.
System Log
System log captures output from java.util.logging output related to Jenkins.
Load Statistics
Check your resource utilization and see if you need more computers for your builds.
About Jenkins
See the version and license information.
Troubleshooting
Manage Old Data
Scrub configuration files to remove remnants from old plugins and earlier versions.
localhost:8080/manage/configureSecurity

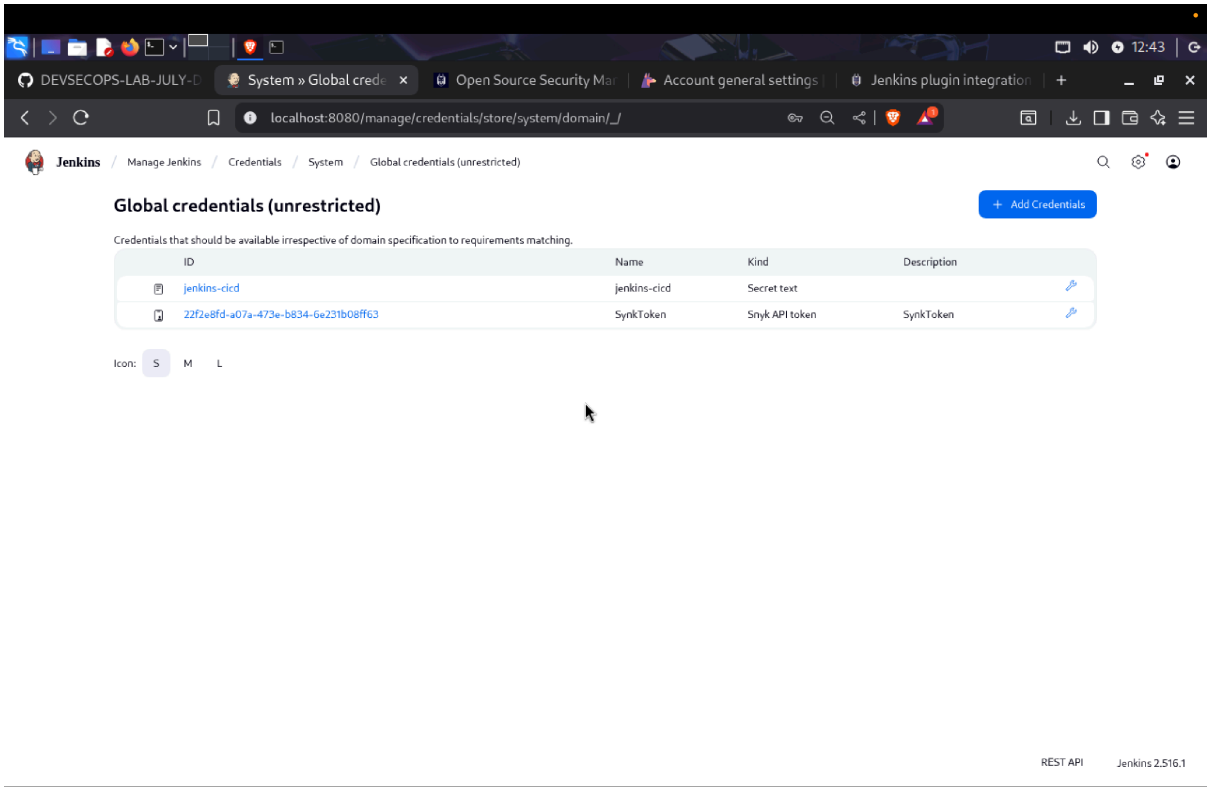

DEVSECOPS-LAB-JULY-D
Jenkins » Credentials
Open Source Security Mar
Account general settings
Jenkins plugin integration
12:38
localhost:8080/manage/credentials/
Jenkins / Manage Jenkins / Credentials
Credentials
T
P
Store
Domain
ID
Name
System
(global)
jenkins-cicd
jenkins-cicd
Stores scoped to Jenkins
P
Store
Domains
System
(global)
Icon: S M L

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

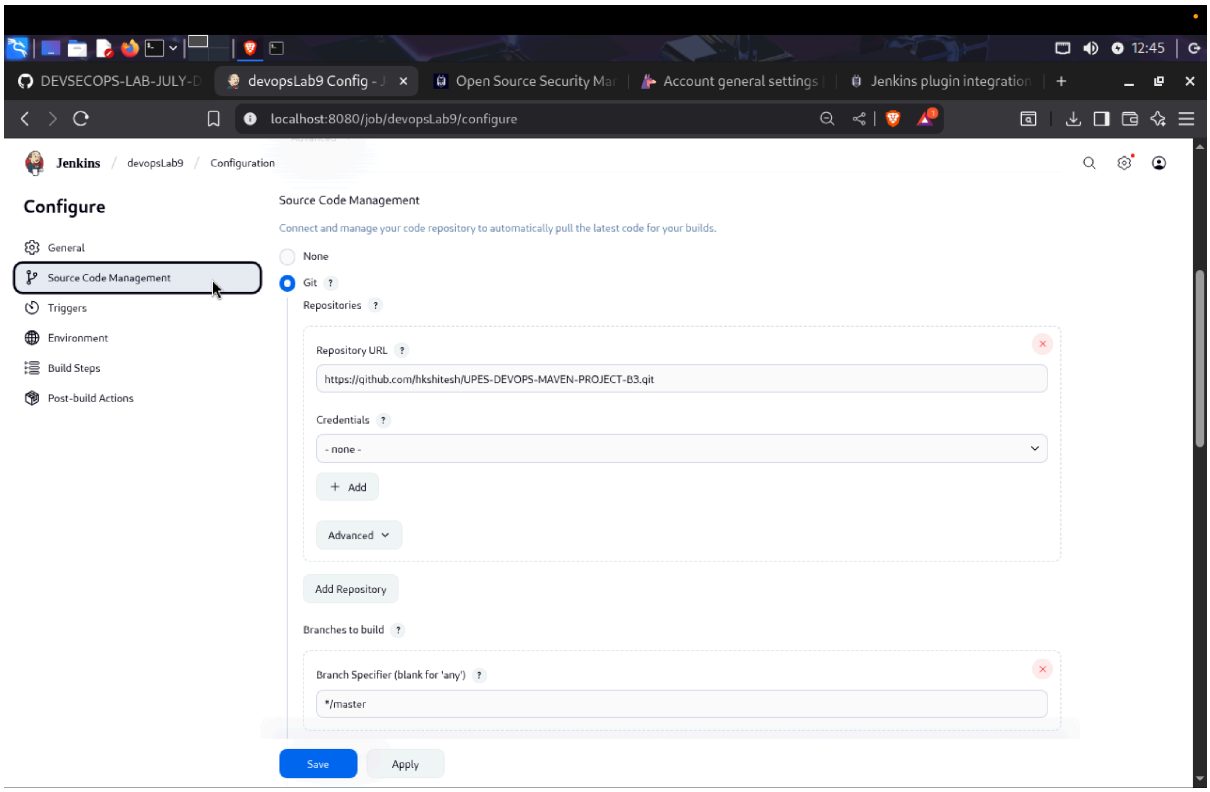


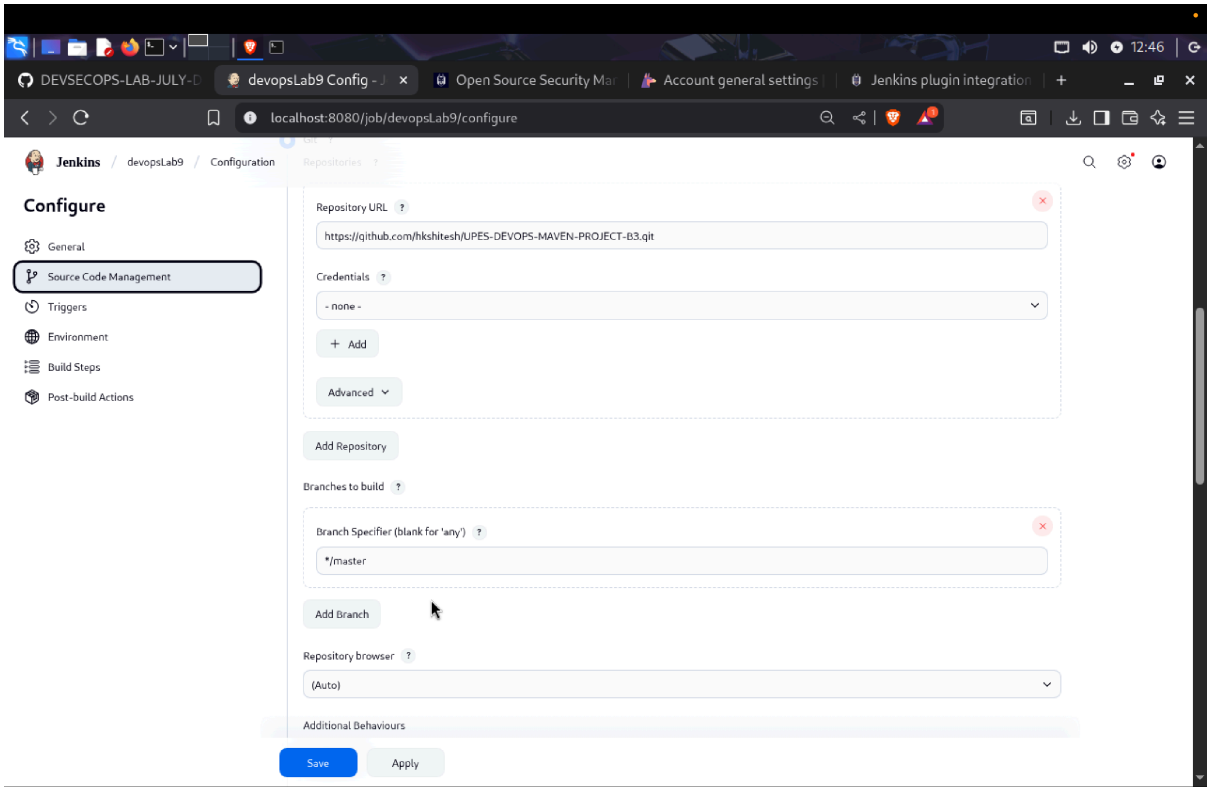



12:42
DEVSECOPS-LAB-JULY-D
New credentials - Jenk
Open Source Security Mar
Account general settings
Jenkins plugin integration
localhost:8080/manage/credentials/store/system/domain/_/newCredentials
Jenkins / Manage Jenkins / Credentials / System / Global credentials (unrestricted)
New credentials
Kind
Snyk API token
Scope
Global (Jenkins, nodes, items, all child items, etc)
Token
Field is required
ID
Description
SynkToken
Create
REST API
Jenkins 2.516.1

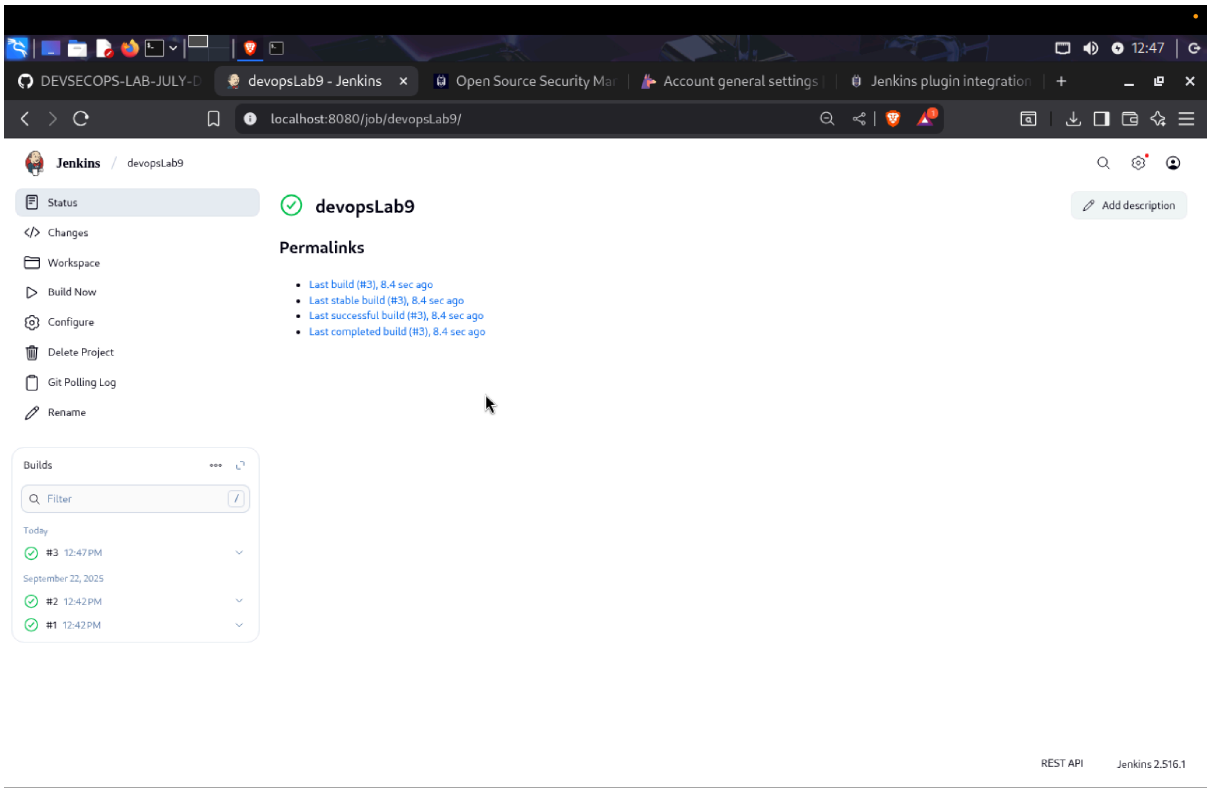

12:43
DEVSECOPS-LAB-JULY-D
System » Global cred
Open Source Security Mar
Account general settings
Jenkins plugin integration
localhost:8080/manage/credentials/store/system/domain/_/
Jenkins / Manage Jenkins / Credentials / System / Global credentials (unrestricted)
Global credentials (unrestricted)
Add Credentials
Credentials that should be available irrespective of domain specification to requirements matching.
ID
Name
Kind
Description
jenkins-cicd
jenkins-cicd
Secret text
22f2e8fd-a07a-473e-b834-6e231b08ff63
SynkToken
Snyk API token
SynkToken
Icon: S M L
REST API
Jenkins 2.516.1

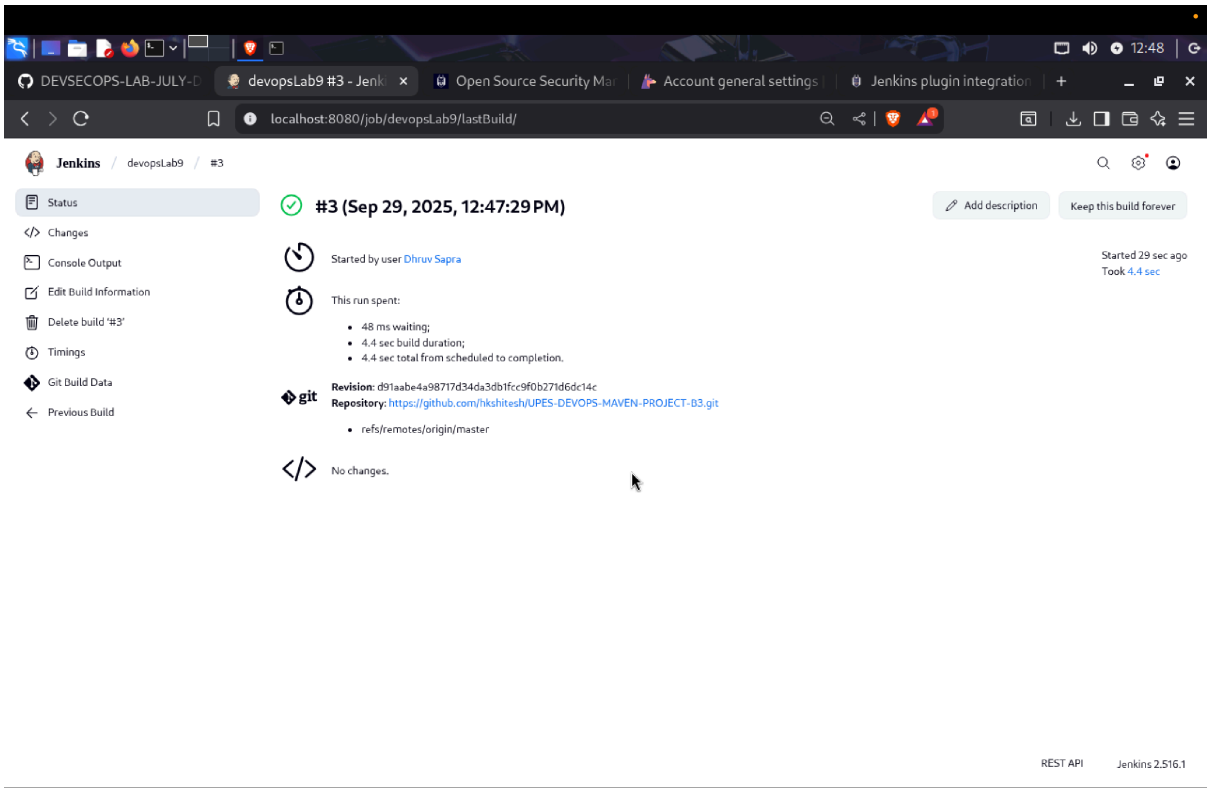
1. After creating a job, go to **Source Code Management** and enter the GitHub repository URL. Then, under **Build Steps**, add the build step **Invoke Snyk Security task** with the name **SnykToken**. Finally, click the **Save** button to create the build.

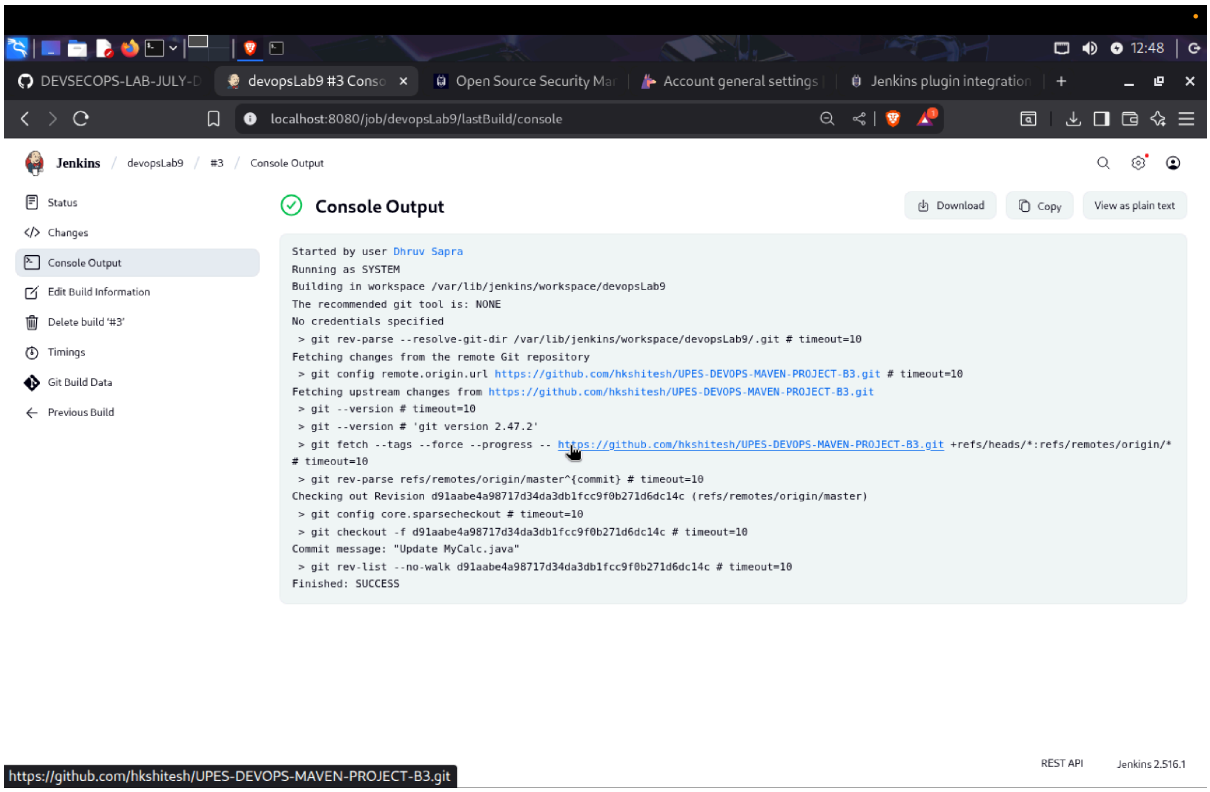




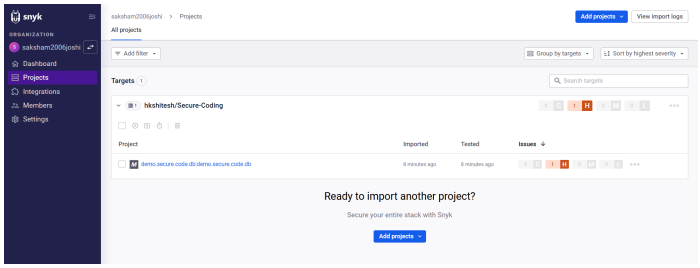
2. To check the build status, click on the build link under **Permalinks.** After that, click on **Console Output**







3. To navigate to the Snyk tool to review code, scan reports under the **Projects** section

4. 

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.