# Jenkins and Snyk – a SAST plugin

## Introduction

1. Jenkins:

Jenkins is a Continuous Integration (CI) or Continuous Delivery (CD) tool, which provides many plugins to support it. Jenkins builds and tests software projects continuously to make it easier for developers to integrate changes to the project, and make it easier for users to obtain a fresh build [3]. To do the Continuous Delivery, a substantial number of testing and deployment plugins are available in Jenkins [3]. Besides, Jenkins can install Google Compute Engine (GCE) plugin to communicate with GCP.

1. Snyk:

Snyk is an open-source SAST tool. It can scan source code and identify vulnerabilities behind it. It supports JAVA, JAVASCRIPT, PYTHON and so on [4]. It also provides integration plugins to facilitate vulnerability scans while building projects. It has an open-source version and an enterprise-paid version. In this project, we just use its open-source version [1].

## How does Jenkins work?

<https://www.jenkins.io/doc/book/installing/linux/>

## How does Snyk work?

First, install the Snyk Security plugin by clicking “Manage Jenkins” on the dashboard, then ”Manage Plugins”-> ”Available”. Search “Snyk Security Plugin” and then install it. After installation, go to “Dashboard” -> “Manage jenkins” -> “Global Tool Configuration” to add a Snyk installation.

Second, get our Snyk API Token. To achieve this, we first register an account in snyk.io website, then visit <https://app.snyk.io/account> page, and copy the auth token in the “Key” input field.

Third, configure the Snyk Security plugin in the Jenkins surface as below [2]:

* Go to "Manage Jenkins" > "Manage Credentials"
* Choose a Store
* Choose a Domain
* Go to "Add Credentials"
* Select "Snyk API Token"
* Configure the Credentials
* Casually input an "ID" but remember because it is needed when configuring the build step.
* Go to "Manage Jenkins" > "Configure System"->”Global properties”, check “Environment variables”, and then add two environment variables as below:

|  |  |
| --- | --- |
| name | values |
| SNYK\_API | https://snyk.io/api/v1 |
| SNYK\_TOKEN | <Snyk API Token>\* |

\* its value varies from different Snyk accounts.

Fourth, configure building a project as below [2]:

* Select a project
* Go to "Configure"
* Under "Build Steps", select "Add build step" then select "Invoke Snyk Security Task" and configure as needed. Here we only configure Snyk API token field and Snyk installation field.
* Under " Source Code Management", select "Git" then fill in “Repository URL” field as whichever our company’s valid git address is(e.g., <https://github.com/redbackoperations/website-frontend>). Fill in other fields as needed

## Review of Snyk

Snyk is a professional SAST tool. It analyses and tests the static code and gives reports showing a detailed analysis of the code and a list of all bugs. More importantly, its open-source version is enough for our team to use. Another famous SAST tool is called Checkmarx, which also has its Jenkins integration plugin. After the plugin installs, and before compilation begins, source code analysis of Checkmarx can be executed to identify security vulnerabilities. However, this tool is commercial and has to be paid for. Therefore, from the price point of view, this software is also more suitable.

By using Snyk to analyse and test the source code of website-frontend of redbackoperations, a vulnerability report is generated. The report says that there are 2 high-risk vulnerabilities and 4 medium-risk vulnerabilities in this project. One vulnerability is detailed as below:



## Conclusion

The Jenkins integrated with Snyk is very convenient for developers to discover security flaws before building and submitting their projects to their production environment. Snyk can give a detailed report, which gives users an insight into the security of their project. Therefore, it is recommendable for this solution to be used in our development of projects in our company.

## Reference List

[1] A. Agarwal, “DevSecOps: Static Application Security Testing Sast using SNYK in Jenkins,” *Medium*, 10-Feb-2021. [Online]. Available: https://toashishagarwal.medium.com/devsecops-static-application-security-testing-sast-using-snyk-in-jenkins-57ce3d992945. [Accessed: 21-Nov-2022].

[2] Jenkinsci, “Jenkinsci/SNYK-security-scanner-plugin: Test and monitor your projects for vulnerabilities with Jenkins. this plugin is officially maintained by Snyk.,” *GitHub*. [Online]. Available: https://github.com/jenkinsci/snyk-security-scanner-plugin. [Accessed: 21-Nov-2022].

[3] Saurabh, “What is Jenkins?: Jenkins for continuous integration,” *Edureka*, 15-Nov-2022. [Online]. Available: https://www.edureka.co/blog/what-is-jenkins/. [Accessed: 22-Nov-2022].

[4] “SNYK code - supported languages and Frameworks,” *Snyk Code - Supported languages and frameworks - Snyk User Docs*. [Online]. Available: https://docs.snyk.io/products/snyk-code/snyk-code-language-and-framework-support. [Accessed: 22-Nov-2022].