

Hands-on Lab: Using SNYK to scan your code repository

Estimated Time: 30 minutes

In this lab, you will become familiar with SNYK, pronounced as **Sneak**, to scan your code repository.

Learning Objectives:

After completing this exercise, you will be able to:

- Perform a scan of your code repository
- Analyze the code repository report

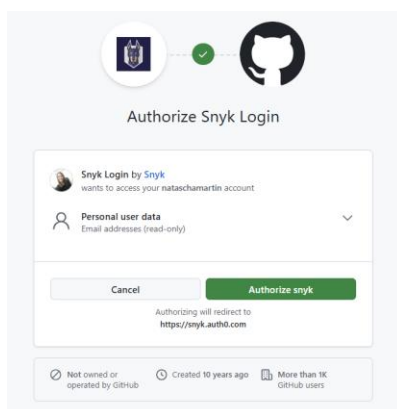
Pre-requisites

- You must have a GitHub account. If you don't have a GitHub account go to [this link](#), follow the instructions and sign-up. **COMPLETED**
- You should have some public and private repositories in your GitHub. If you don't have any, then let's create one. For example, if you want to create a copy of another public repository, <https://github.com/bitnami/containers>, go to the repository. Click **Fork** to fork the repository into your account. This will make a copy of the repository for you. **COMPLETED**

Adding a project to SNYK

SNYK software has many capabilities. But we will focus on the code repository vulnerability check which is offered as a free service.

1. Go to <https://app.snyk.io/login> and click login with GitHub.



2. If you are already logged into GitHub in your browser, go to next step. Otherwise, login with your Github credentials.

3. Provide permission and authorize snyk to use your GitHub credentials to login.
4. The first time you login, it asks if you want to subscribe for information on product releases and feature updates. Click **No, not right now**.
5. Choose the location of the code you want to test. For this exercise, choose Github. You are free to choose BitBucket if you have an account already.

***Note:** Step 5 was skipped automatically since I had already authenticated GitHub during the login process and Snyk detected my existing GitHub integration.*


6. You are presented with options to choose between using both public and private repositories (or repos) or just the public repos. Choose **Public repos only**.
7. Check and select all the types of scans you would like snyk to do and click **Authenticate Github**.
8. Github requires you to explicitly allow snyk to use your public repos. Click **Authorize snyk** to do so.
9. It takes you to the **Dashboard**, where you can click **Add Projects**. You have options to choose from.



- Github
 - CLI
 - Monitor public Github repos
 - Other sources (BitBucket, Cloud, etc.,)
10. Click **Github** to see all your public repos listed. You can scan one of your public repos.
 11. You can choose your repos and Add the selected repos to scan.

Personal and Organization repositories


☐ nataschamartin

☐ bitnami  ☐ cybersecurity-portfolio ☐ lab-agile-planning








☐ test

Settings

add custom file location (optional)
 to add a dependency from a non-default path, add it below:

Select a repository 

exclude folders (Supported for Snyk Open Source and Snyk Container only, optional)
 specify the names of the folders that you want to exclude from the search (maximum 10 folders).
 separate names with commas.

Search        100%

Depending on the size of your repo, scan might take time.

12. Click **Add Project** again and choose, **Monitor public Github repos** option.

13. Type the name of a public url. For example, the image below shows <https://github.com/bitnami/containers>. Click **Add repo** and then click **Import 1 repository**.

14. Once the repo is imported, the scanning begin for vulnerabilities. This take a few seconds, after which a report is generated showing how many projects in the repository were scanned and how many **Critical**, **High** priority, **Medium** priority and **Low** priority vulnerabilities were found in these.

Today	
> bitnami/containers <small>main</small>	Import triggered at 12:30:01
> nataschamartin/bitnami <small>main</small>	Import triggered at 12:28:17
> nataschamartin/cybersecurity-portfolio <small>main</small>	Import triggered at 12:28:17
> nataschamartin/test <small>main</small>	Import triggered at 12:28:17
> nataschamartin/lab-agile-planning <small>main</small>	Import triggered at 12:28:17

Targets 5		Search targets
> 270 bitnami/containers	0 C 0 H 16 M 18 L	...
> 270 nataschamartin/bitnami	0 C 0 H 16 M 18 L	...
> 0 nataschamartin/cybersecurity-portfolio	0 C 0 H 0 M 0 L	...
> 1 nataschamartin/test	0 C 0 H 0 M 0 L	...
> 0 nataschamartin/lab-agile-planning	0 C 0 H 0 M 0 L	...

Summary of my lab status:

Repository	Scanned?	Issues Found	Action Needed?
bitnami/containers	Yes	Yes	None
nataschamartin/bitnami	Yes	Yes	None
nataschamartin/test	Yes	No issues	None
nataschamartin/cybersecurity-portfolio	No	—	No scannable content
nataschamartin/lab-agile-planning	No	—	No scannable content

Lab Summary: Scanning for Code Vulnerabilities with Snyk

In this lab, I used Snyk to scan my GitHub repositories for known code vulnerabilities. The lab required connecting my GitHub account to Snyk, granting repository access, and allowing Snyk to perform automated testing on supported repositories.

I skipped the earlier GitHub account creation steps since I already had an existing account. I started directly with the Snyk setup and repository process.

Steps Completed:

1. Connected Snyk to GitHub

- Authorized OAuth access
- Enabled both public and private repo scanning
- Checked all Snyk automation settings (PR checks, auto upgrades, etc.)

2. Imported Repositories for Scanning:

- bitnami/containers
- nataschamartin/bitnami
- nataschamartin/test
- nataschamartin/cybersecurity-portfolio
- nataschamartin/lab-agile-planning

3. Successfully Scanned Repos:

- bitnami/containers → Issues detected (High/Medium/Low)

- nataschamartin/bitnami → Issues detected (High/Medium/Low)
- nataschamartin/test → Scanned successfully, **no issues found**

4. Repositories Not Scanned:

- nataschamartin/cybersecurity-portfolio
- nataschamartin/lab-agile-planning

These repos contain no scannable code files (like package managers or dependency files), so no vulnerabilities were detected. This is expected behavior.

Notes:

- No errors occurred during authorization or repo selection.
- No re-imports were needed, all activity shows properly in the Snyk dashboard.
- Only code-based repos with scannable files return results in Snyk.