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.

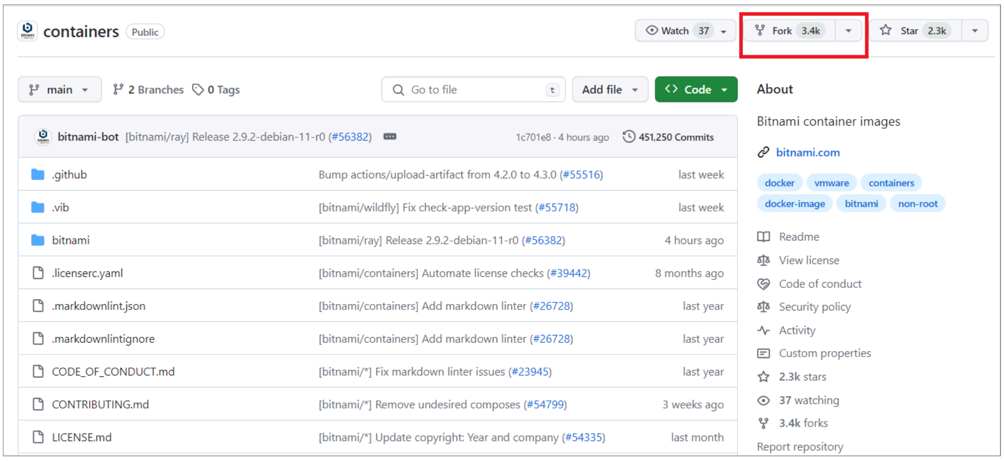
Learning Objectives:

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.
- 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.



bitnami-bot [bitnami/ray] Release 2.9.2-debian-11-r0 (#56382) 1c701e8 · 4 hours ago 451,250 Commits

.github	Bump actions/upload-artifact from 4.2.0 to 4.3.0 (#55516)	last week
.vib	[bitnami/wildfly] Fix check-app-version test (#55718)	last week
bitnami	[bitnami/ray] Release 2.9.2-debian-11-r0 (#56382)	4 hours ago
.licenserc.yaml	[bitnami/containers] Automate license checks (#39442)	8 months ago
.markdownlint.json	[bitnami/containers] Add markdown linter (#26728)	last year
.markdownlintignore	[bitnami/containers] Add markdown linter (#26728)	last year
CODE_OF_CONDUCT.md	[bitnami/*] Fix markdown linter issues (#23945)	last year
CONTRIBUTING.md	[bitnami/*] Remove undesired composes (#54799)	3 weeks ago
LICENSE.md	[bitnami/*] Update copyright: Year and company (#54335)	last month

About

Bitnami container images

bitnami.com

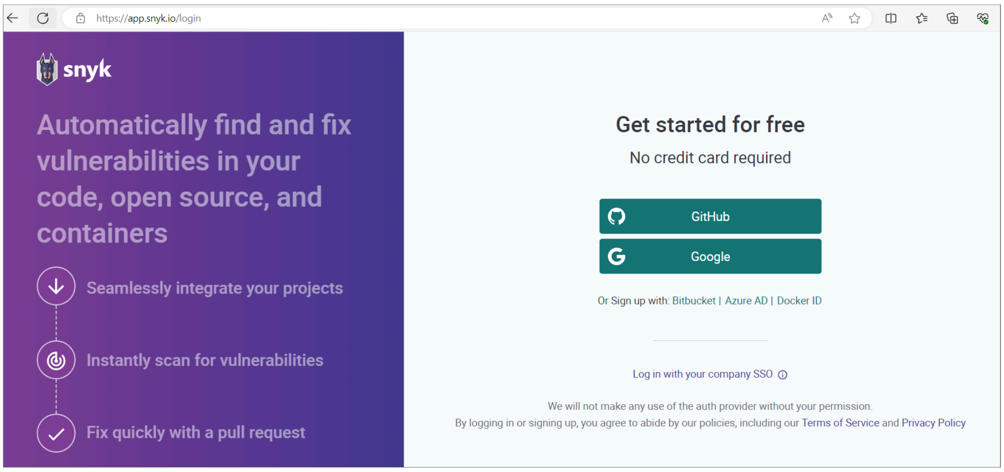
docker vmware containers docker-image bitnami non-root

Readme
View license
Code of conduct
Security policy
Activity
Custom properties
2.3k stars
37 watching
3.4k forks
Report repository

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.



Automatically find and fix vulnerabilities in your code, open source, and containers

Seamlessly integrate your projects

Instantly scan for vulnerabilities

Fix quickly with a pull request

Get started for free

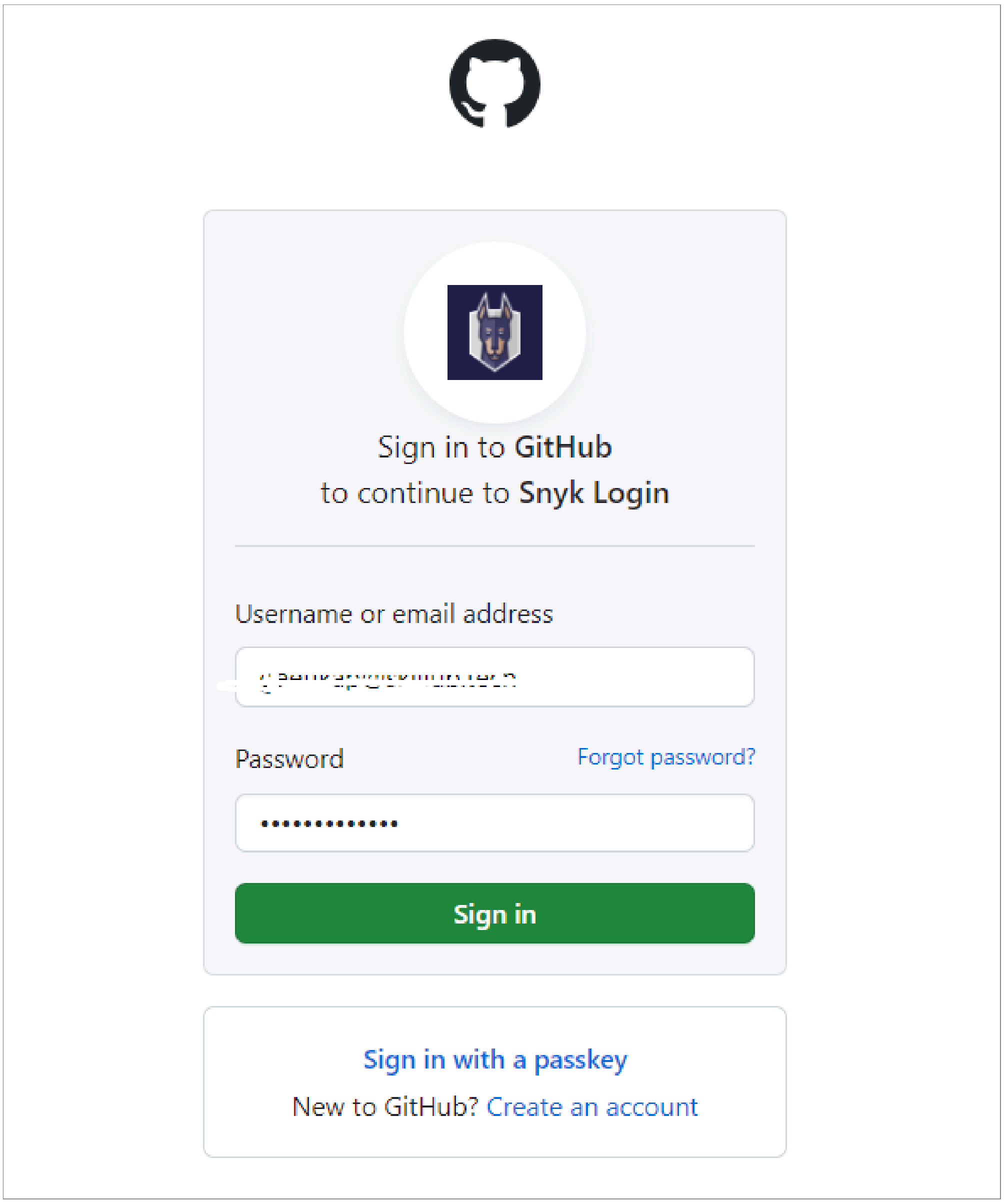
No credit card required

Or Sign up with: Bitbucket | Azure AD | Docker ID

Log in with your company SSO

We will not make any use of the auth provider without your permission.
By logging in or signing up, you agree to abide by our policies, including our Terms of Service and Privacy Policy

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



Sign in to **GitHub**
to continue to **Snyk Login**

Username or email address

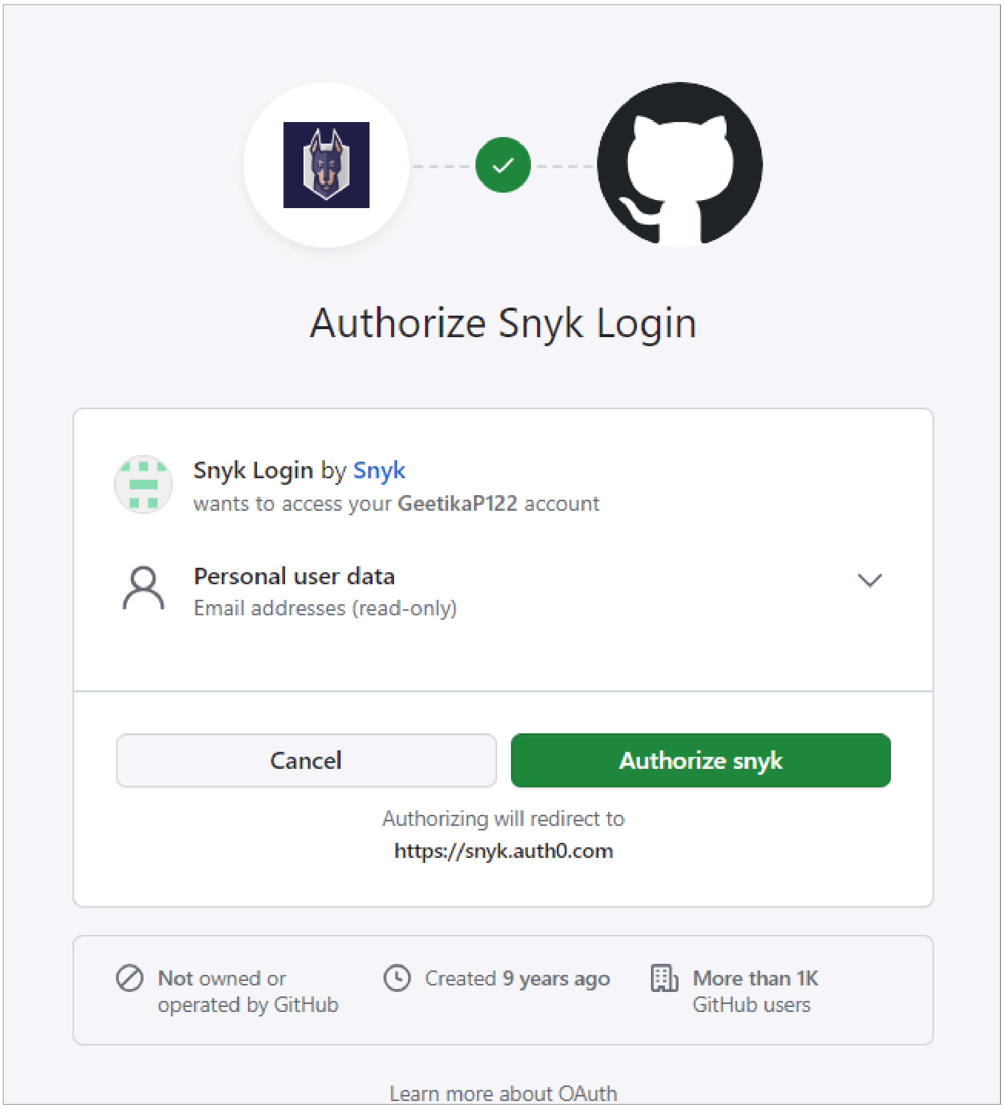
[redacted]

Password — Forgot password?

•••••••••••••

New to GitHub? Create an account

3. Provide permission and authorize snyk to use your GitHub credentials to login.



Authorize Snyk Login

Snyk Login by Snyk
wants to access your GeetikaP122 account

Personal user data
Email addresses (read-only)

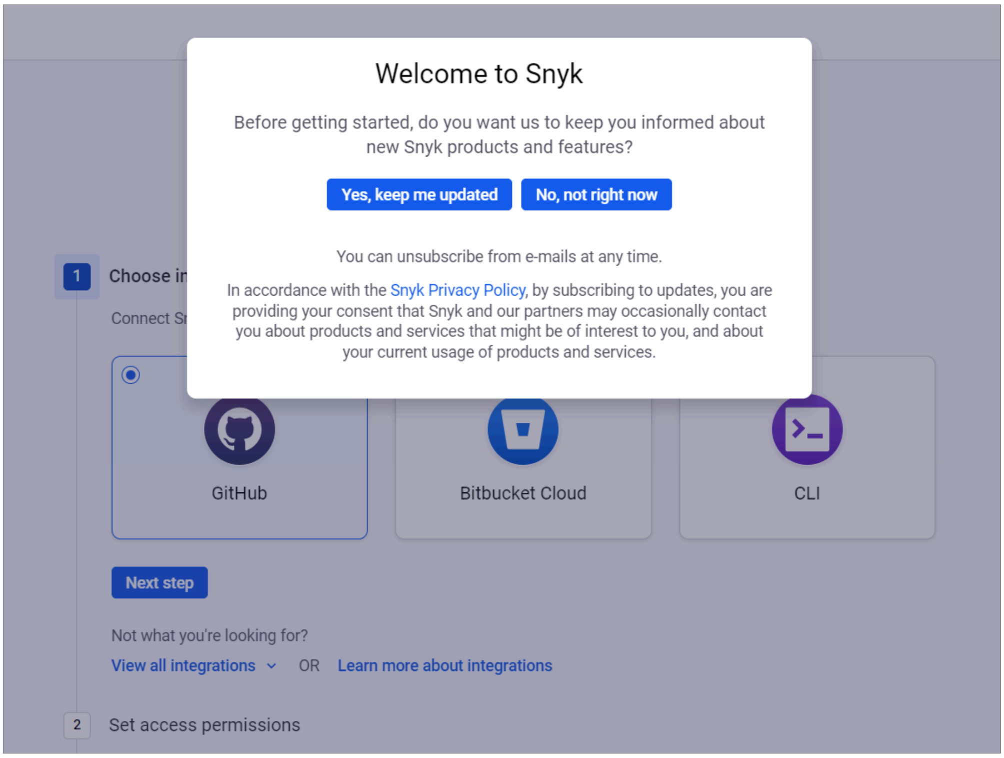
Authorizing will redirect to
https://snyk.auth0.com

Not owned or operated by GitHub

Created 9 years ago

More than 1K GitHub users

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**.



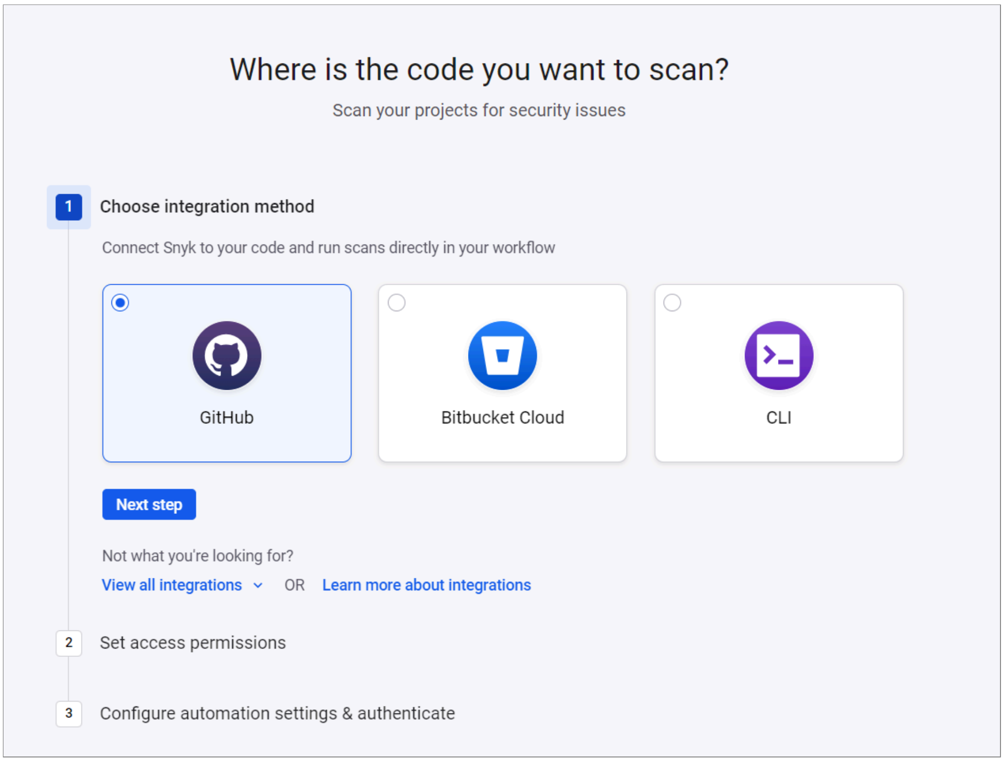
Welcome to Snyk

Before getting started, do you want us to keep you informed about new Snyk products and features?

You can unsubscribe from e-mails at any time.

In accordance with the Snyk Privacy Policy, by subscribing to updates, you are providing your consent that Snyk and our partners may occasionally contact you about products and services that might be of interest to you, and about your current usage of products and services.

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.



Where is the code you want to scan?

Scan your projects for security issues

1 Choose integration method

Connect Snyk to your code and run scans directly in your workflow

● GitHub

○ Bitbucket Cloud

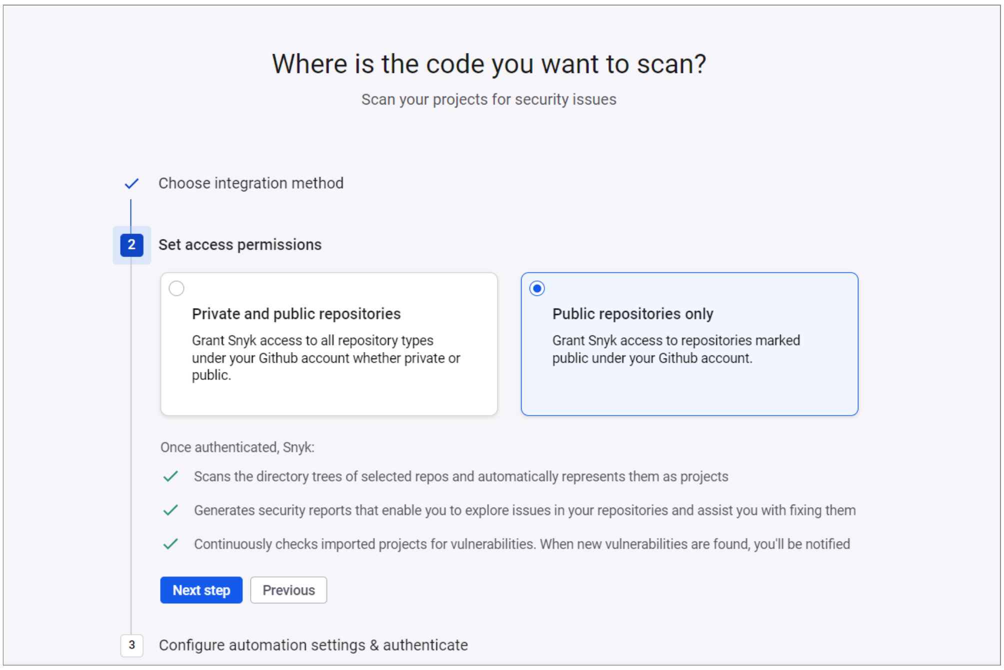
○ CLI

Not what you're looking for?

2 Set access permissions

3 Configure automation settings & authenticate

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**.



Where is the code you want to scan?

Scan your projects for security issues

✓ Choose integration method

2 Set access permissions

○ **Private and public repositories**
Grant Snyk access to all repository types under your Github account whether private or public.

● **Public repositories only**
Grant Snyk access to repositories marked public under your Github account.

Once authenticated, Snyk:

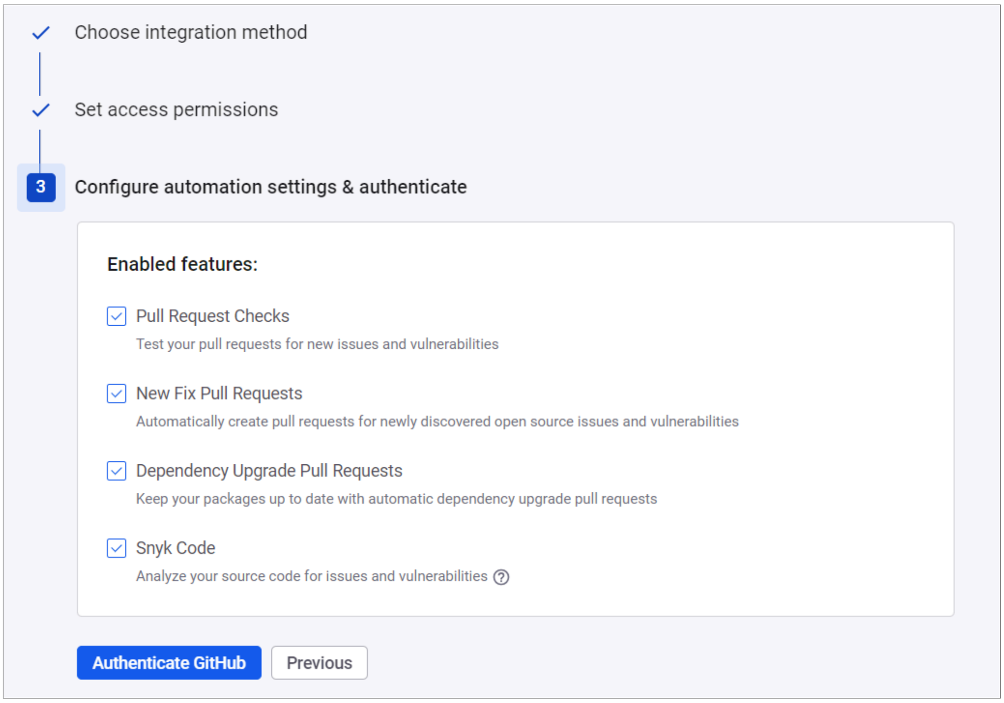
✓ Scans the directory trees of selected repos and automatically represents them as projects

✓ Generates security reports that enable you to explore issues in your repositories and assist you with fixing them

✓ Continuously checks imported projects for vulnerabilities. When new vulnerabilities are found, you'll be notified

3 Configure automation settings & authenticate

7. Check and select all the types of scans you would like snyk to do and click **Authenticate Github**.



✓ Choose integration method

✓ Set access permissions

3 Configure automation settings & authenticate

Enabled features:

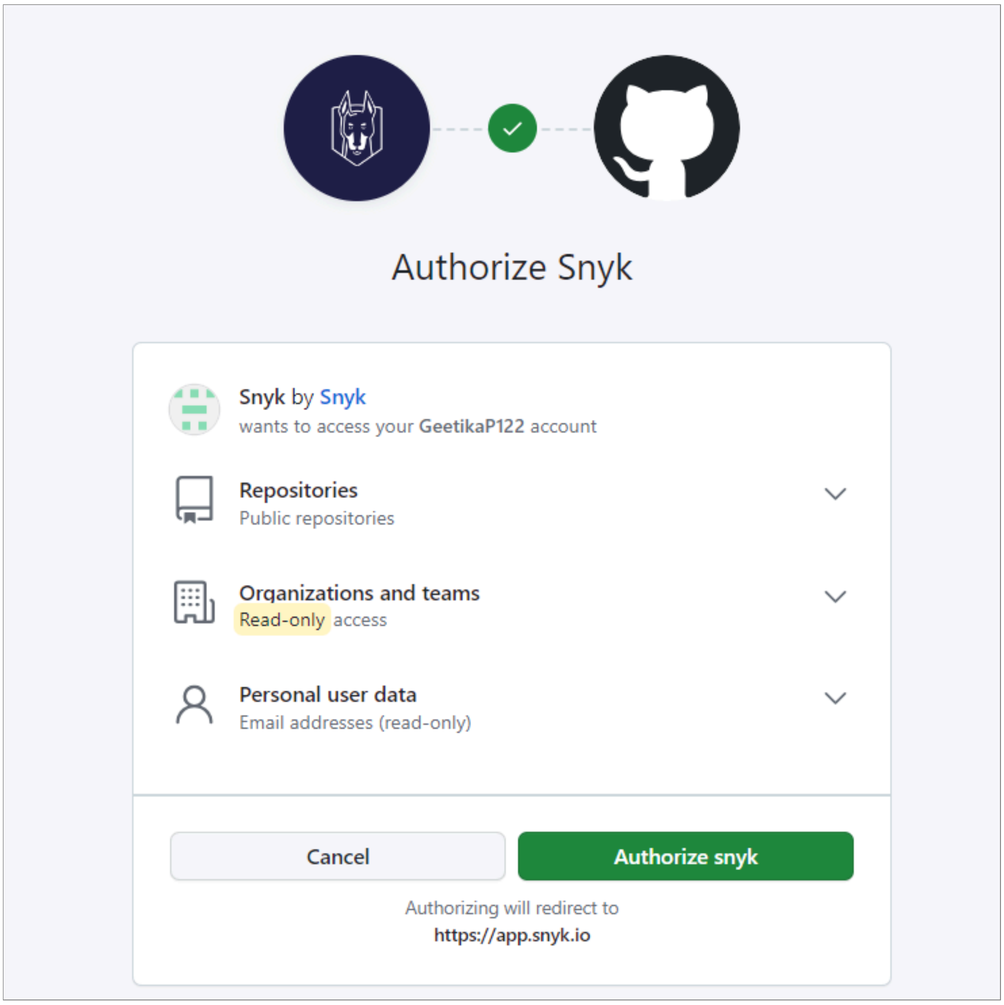
☑ Pull Request Checks
Test your pull requests for new issues and vulnerabilities

☑ New Fix Pull Requests
Automatically create pull requests for newly discovered open source issues and vulnerabilities

☑ Dependency Upgrade Pull Requests
Keep your packages up to date with automatic dependency upgrade pull requests

☑ Snyk Code
Analyze your source code for issues and vulnerabilities

8. Github requires you to explicitly allow snyk to use your public repos. Click **Authorize snyk** to do so.



Authorize Snyk

Snyk by Snyk
wants to access your GeetikaP122 account

Repositories
Public repositories

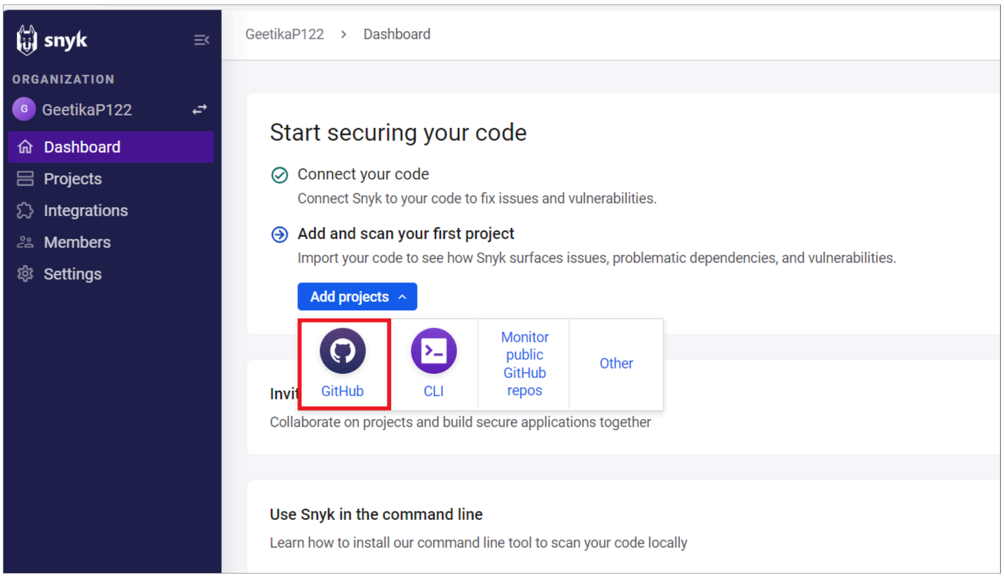
Organizations and teams
Read-only access

Personal user data
Email addresses (read-only)

Authorizing will redirect to
https://app.snyk.io

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.,)



Start securing your code

Connect your code
Connect Snyk to your code to fix issues and vulnerabilities.

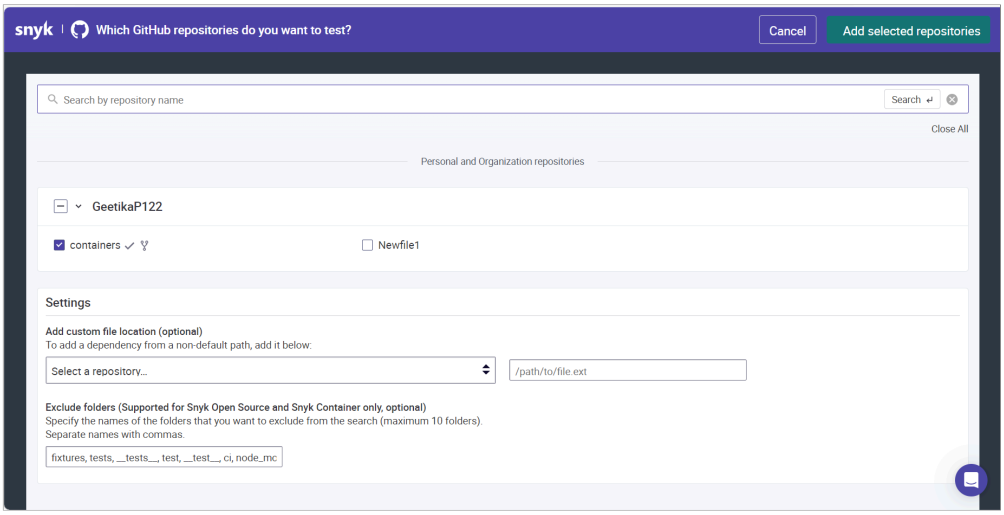
Add and scan your first project
Import your code to see how Snyk surfaces issues, problematic dependencies, and vulnerabilities.

Collaborate on projects and build secure applications together

Use Snyk in the command line
Learn how to install our command line tool to scan your code locally

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.


snyk | Which GitHub repositories do you want to test?
Cancel
Add selected repositories
Search by repository name
Search
Close All
Personal and Organization repositories
GeetikaP122

☑ containers ✓
□ Newfile1

Settings

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

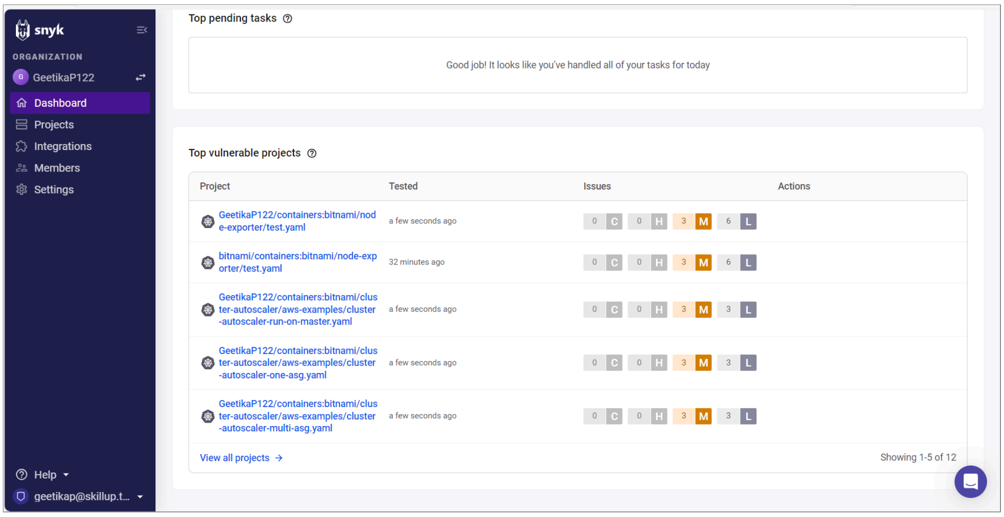
Select a repository... /path/to/file.ext

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.

fixtures, tests, __tests__, test, __test__, ci, node_mc

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

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



Top pending tasks

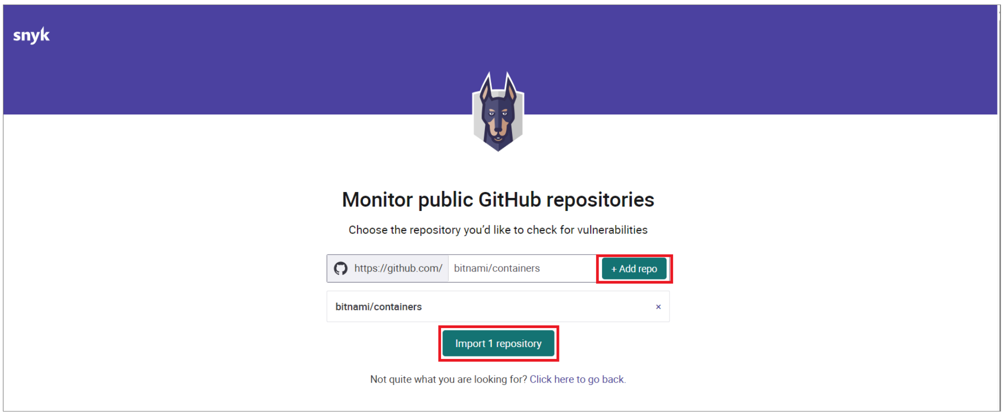
Good job! It looks like you've handled all of your tasks for today

Top vulnerable projects

Project	Tested	Issues	Actions
GeetikaP122/containers:bitnami/node-exporter/test.yaml	a few seconds ago	0 C 0 H 3 M 6 L	
bitnami/containers:bitnami/node-exporter/test.yaml	32 minutes ago	0 C 0 H 3 M 6 L	
GeetikaP122/containers:bitnami/cluster-autoscaler/aws-examples/cluster-autoscaler-run-on-master.yaml	a few seconds ago	0 C 0 H 3 M 3 L	
GeetikaP122/containers:bitnami/cluster-autoscaler/aws-examples/cluster-autoscaler-one-asg.yaml	a few seconds ago	0 C 0 H 3 M 3 L	
GeetikaP122/containers:bitnami/cluster-autoscaler/aws-examples/cluster-autoscaler-multi-asg.yaml	a few seconds ago	0 C 0 H 3 M 3 L	

View all projects → Showing 1-5 of 12

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**.



snyk

Monitor public GitHub repositories

Choose the repository you'd like to check for vulnerabilities

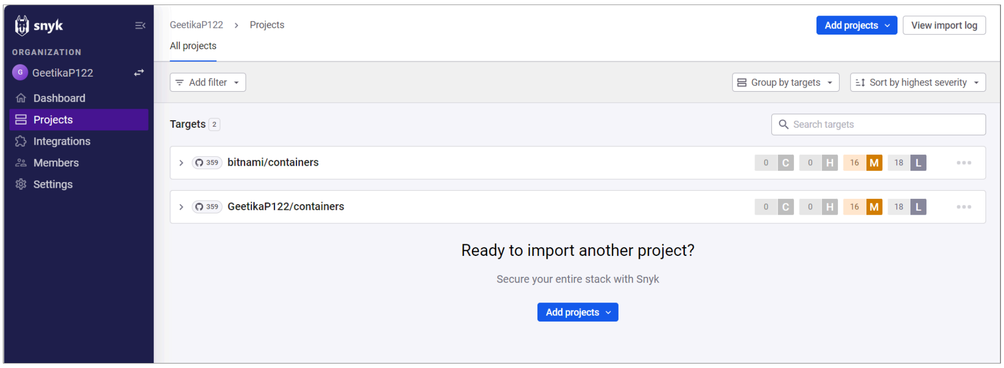
https://github.com/ bitnami/containers + Add repo

bitnami/containers ×

Import 1 repository

Not quite what you are looking for? Click here to go back.

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.



Targets 2

	C	H	M	L
359 bitnami/containers	0	0	16	18
359 GeetikaP122/containers	0	0	16	18

Ready to import another project?

Secure your entire stack with Snyk

Add projects

Congratulations! You just learned how to scan code with Snyk.

You may try to run this code scan on your own repos or other public GitHub repositiries for practice.

Author(s)

Lavanya T S

Skills Network