Secure Programming
Static Code Analysis

In this lab you will use a static code analyser to analyse the Coffeshop application. We will use Snyk CLI as the analyser. Note: this is available as a plugin for most of the major IDE platforms, so you can choose to install this way. (See documentation: IDE plugins | Snyk)

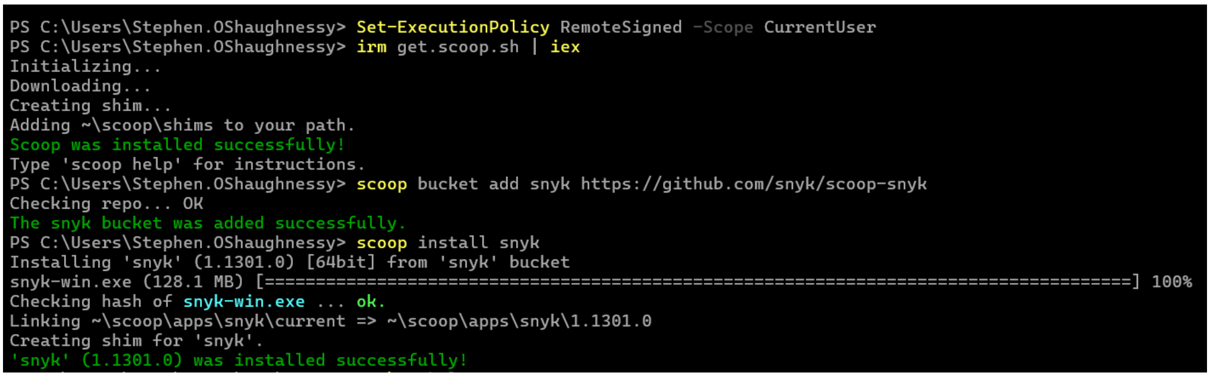
1. Set up a Snyk account (https://app.snyk.io/login) - You cans sign up through Google or Github/ Bitbucket etc. It will link automatically to those accounts. You can integrate Snyk into your Github projects for real-time scanning.

2. Download Snyk:
Windows:
Open PowerShell and type the following:

```
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
irm get.scoop.sh | iex
```

Then type: **scoop install snyk**

You should see a similar output to this:



```
PS C:\Users\Stephen.OShaughnessy> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
PS C:\Users\Stephen.OShaughnessy> irm get.scoop.sh | iex
Initializing...
Downloading...
Creating shim...
Adding ~\scoop\shims to your path.
Scoop was installed successfully!
Type 'scoop help' for instructions.
PS C:\Users\Stephen.OShaughnessy> scoop bucket add snyk https://github.com/snyk/scoop-snyk
Checking repo... OK
The snyk bucket was added successfully.
PS C:\Users\Stephen.OShaughnessy> scoop install snyk
Installing 'snyk' (1.1301.0) [64bit] from 'snyk' bucket
snyk-win.exe (128.1 MB) [=====================================================================================] 100%
Checking hash of snyk-win.exe ... ok.
Linking ~\scoop\apps\snyk\current => ~\scoop\apps\snyk\1.1301.0
Creating shim for 'snyk'.
'snyk' (1.1301.0) was installed successfully!
```

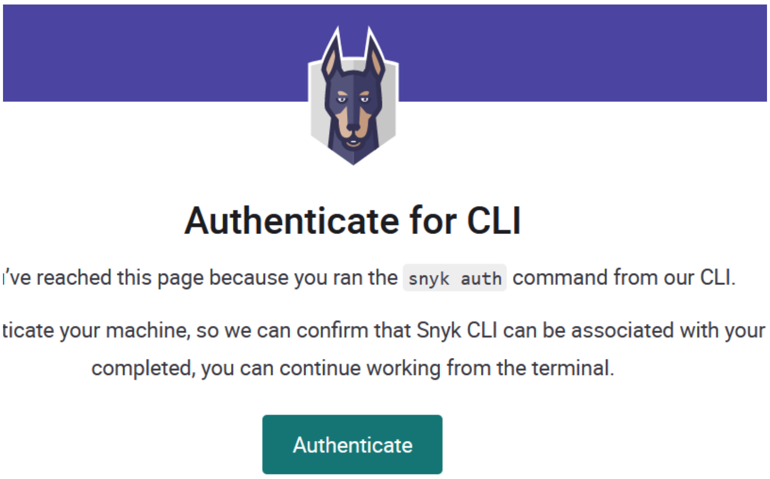
Linux/ Mac:
In a terminal type the following:

```
brew tap snyk/tap
brew install snyk
```

Or if you have Node.js installed: **npm install snyk -g**

4. Authenticate your CLI app by typing **snyk auth.**

You will be re-directed to an authenticate page as below. Ensure you are logged into your account you created in step 1:

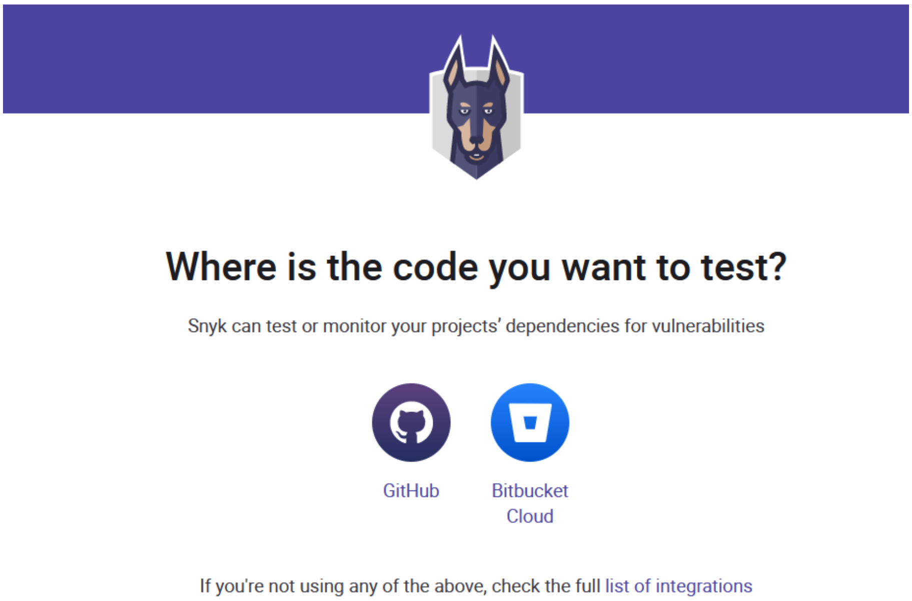


Authenticate for CLI

've reached this page because you ran the `snyk auth` command from our CLI.

ticate your machine, so we can confirm that Snyk CLI can be associated with your completed, you can continue working from the terminal.

Next, we will need to enable Snyk code to analyse the source code. In Snyk, when you log in, you will be presented with the page below. Choose the "list of integrations" link, which will take you to the dashboard.

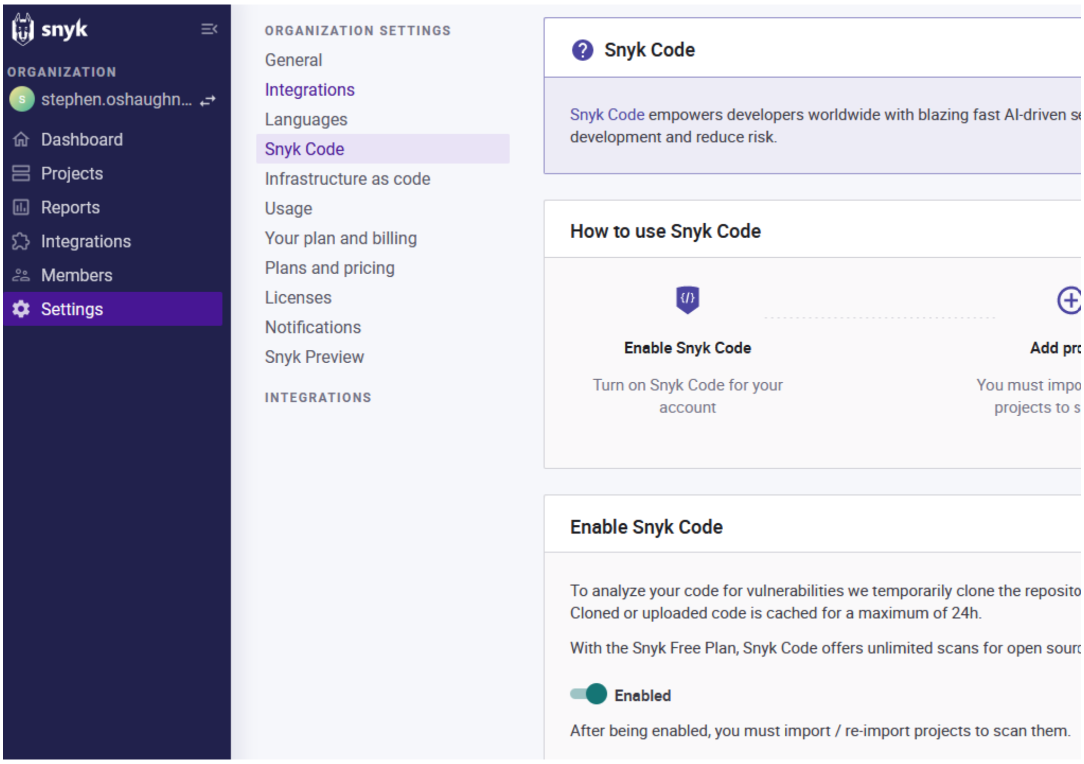


Where is the code you want to test?

Snyk can test or monitor your projects' dependencies for vulnerabilities

If you're not using any of the above, check the full list of integrations

Click on settings and under Organization Settings, enable Synk Code:



Snyk Code empowers developers worldwide with blazing fast AI-driven se
development and reduce risk.

Turn on Snyk Code for your account

You must impo projects to s

To analyze your code for vulnerabilities we temporarily clone the reposito
Cloned or uploaded code is cached for a maximum of 24h.

With the Snyk Free Plan, Snyk Code offers unlimited scans for open sourc

● Enabled

After being enabled, you must import / re-import projects to scan them.

You can test if Snyk has installed by running it against a dependency or library, e.g.,

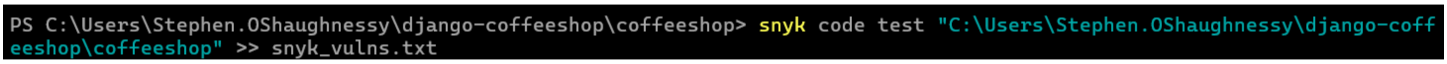
snyk test ionic

This should output several vulnerabilities currently in the ionic library.

Scanning the Coffeeshop Site

Run the following command: **snyk code test <path-to-your-django-coffeeshop>**.

This will scan the source code for vulnerabilities. You can redirect the output to a text file for clarity, e.g.,



```
PS C:\Users\Stephen.OShaughnessy\django-coffeeshop\coffeeshop> snyk code test "C:\Users\Stephen.OShaughnessy\django-coff
eeshop\coffeeshop" >> snyk_vulns.txt
```

Examine the contents of the source code analysis. Choose 3 vulnerabilities (one low, one medium, one critical) that we have not covered in the labs and fix them.

Note: You can open the code up in an IDE to make the changes. There is no need to run the code. Once you have applied the code fix, run the Snyk analysis again and check that the vulnerabilities no longer appear in the listing.

Deliverables

Upload the Snyk text file listing (after the fixes have been implemented) and the source code files – you only have to include the class files you have fixed.