

Cisco Enterprise Networking Use Case Guide:

**Cisco-DNA-Center-with-Cisco-PSIRT-API-integration**

**Walk** – Run – Fly



**Author: David Fernandez**

**APO Programmability Team**

[APO-Programmability@cisco.com](mailto:APO-Programmability@cisco.com)

**Introduction**

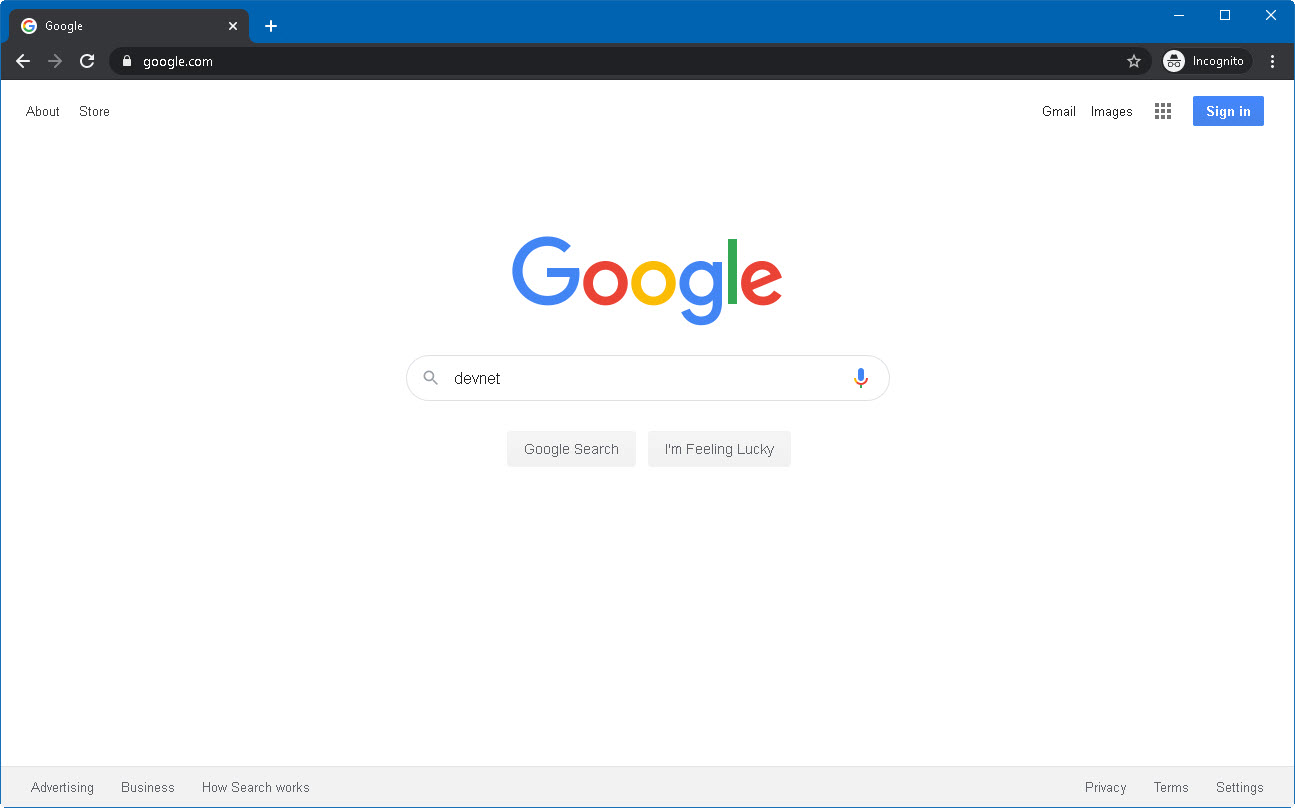
Use Case: Cisco DNA Center integration with Cisco PSIRT API

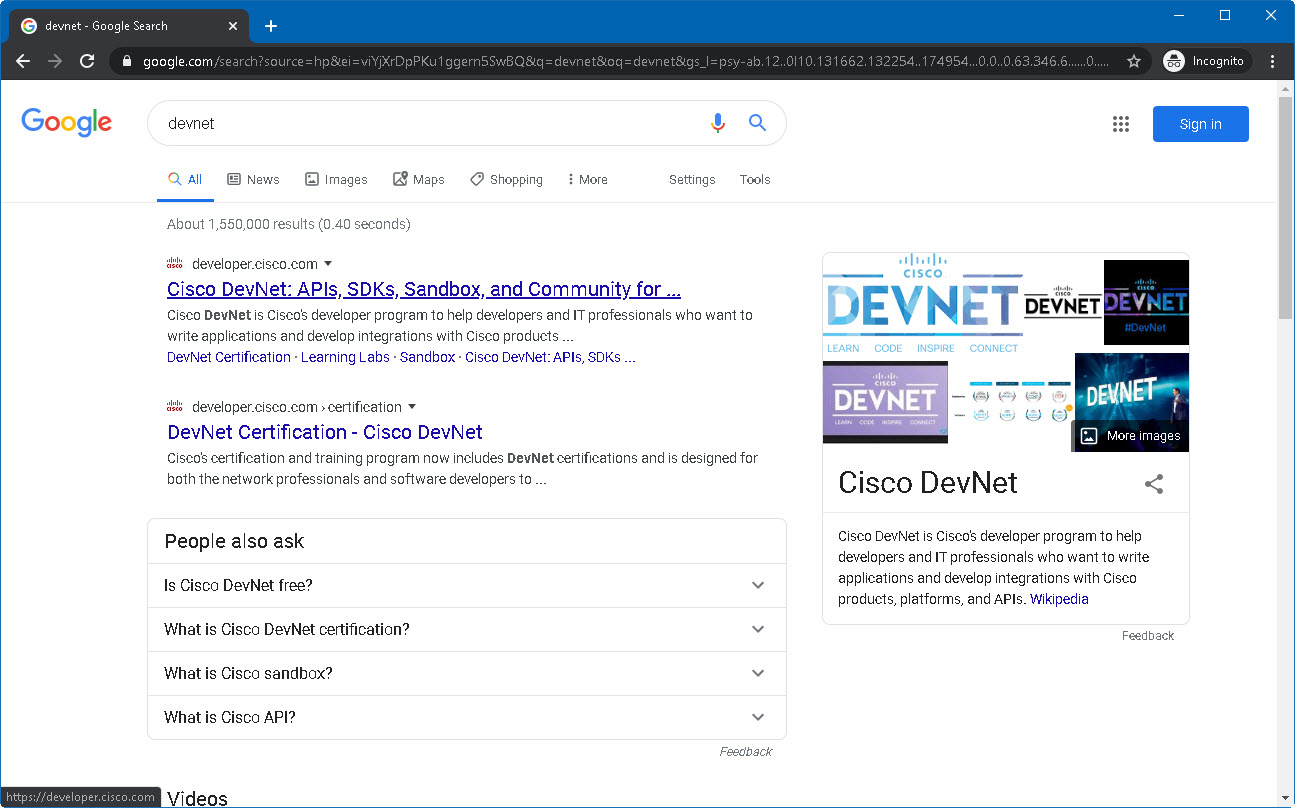
The purpose of this guide is to take you from zero to running the Enterprise Networking’s Use Case in under 30 minutes, regardless of Operating System or Python availability.

The script’s goal is to generate a CSV file containing all the vulnerabilities that affect the devices that are part of a Cisco DNA Center managed network.

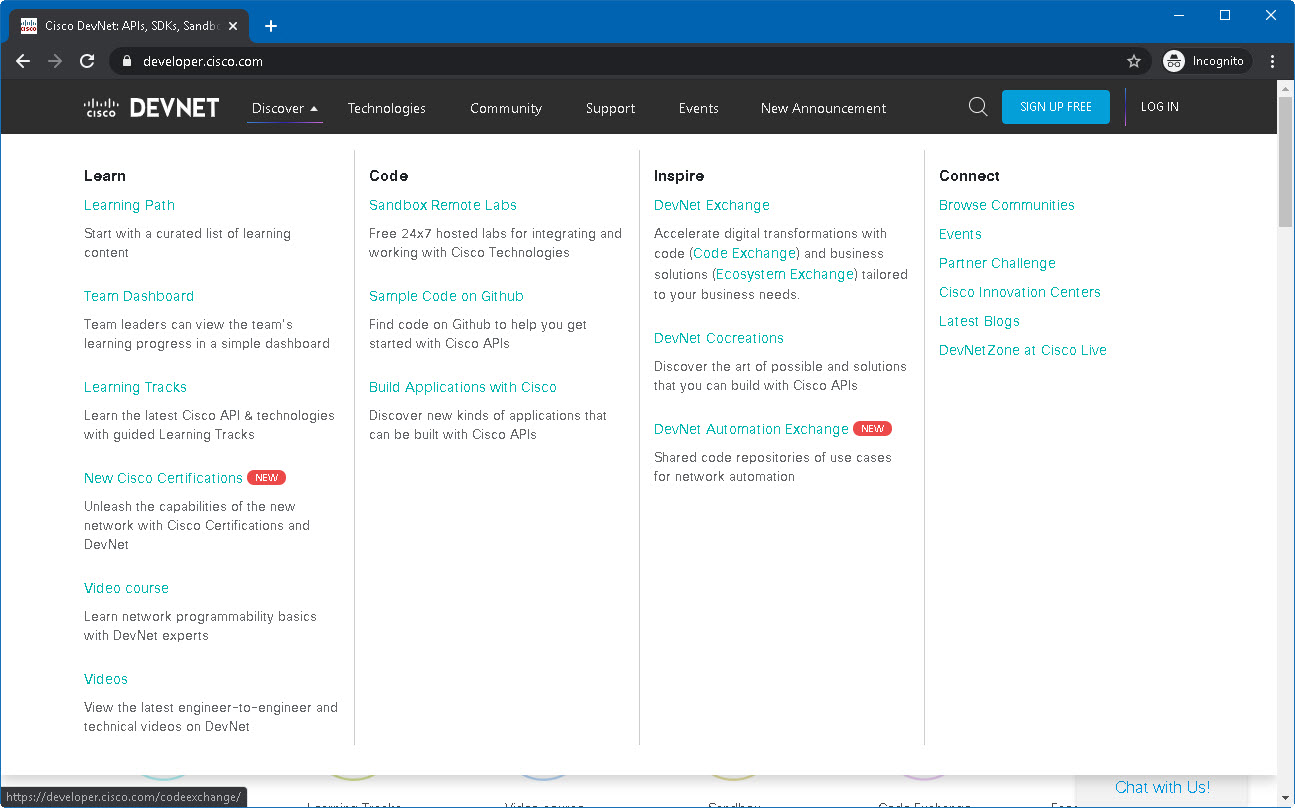
In this implementation of the application, the author has included the Cisco PSIRT database of vulnerabilities as of June-05-2019 in the vulnerabilities.json file in the repo.

Let’s get started!

Google **DevNet**

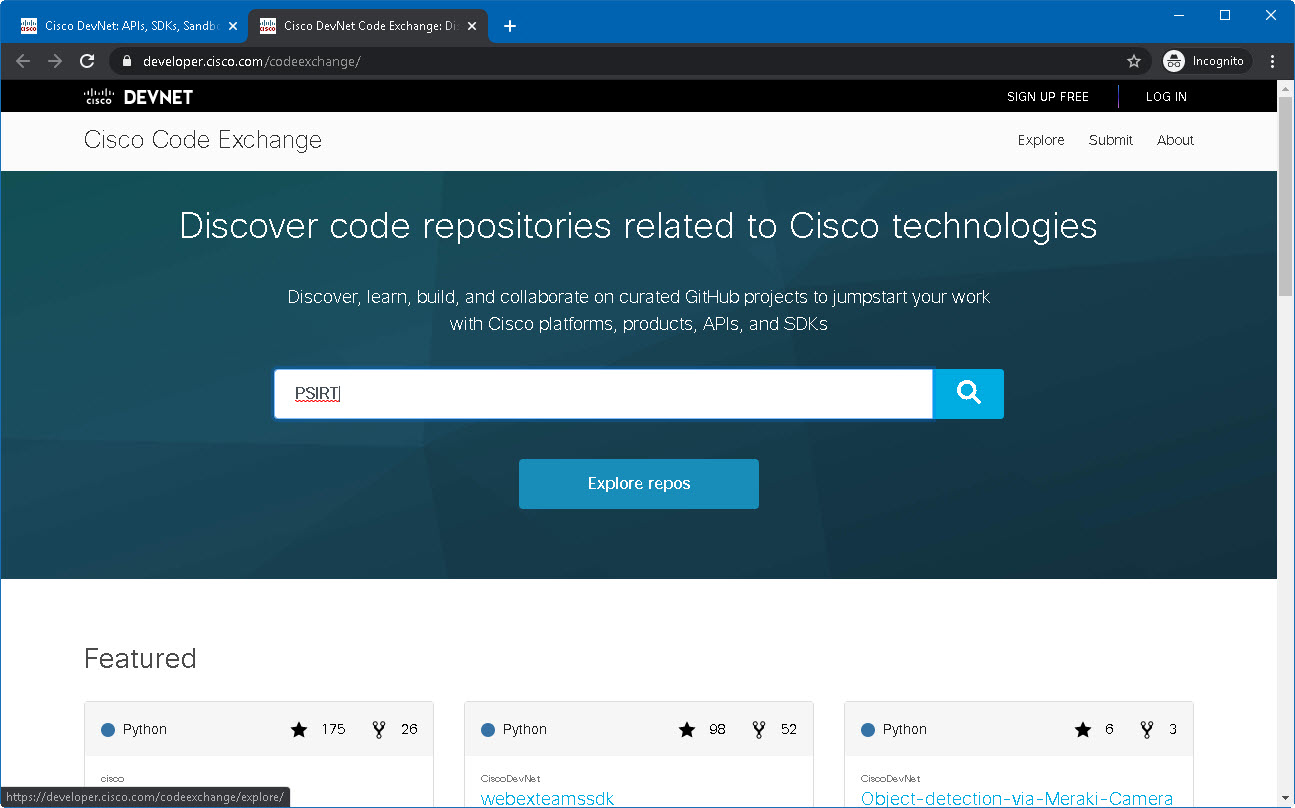
Open the first link, which should be **http://developer.cisco.com/** 

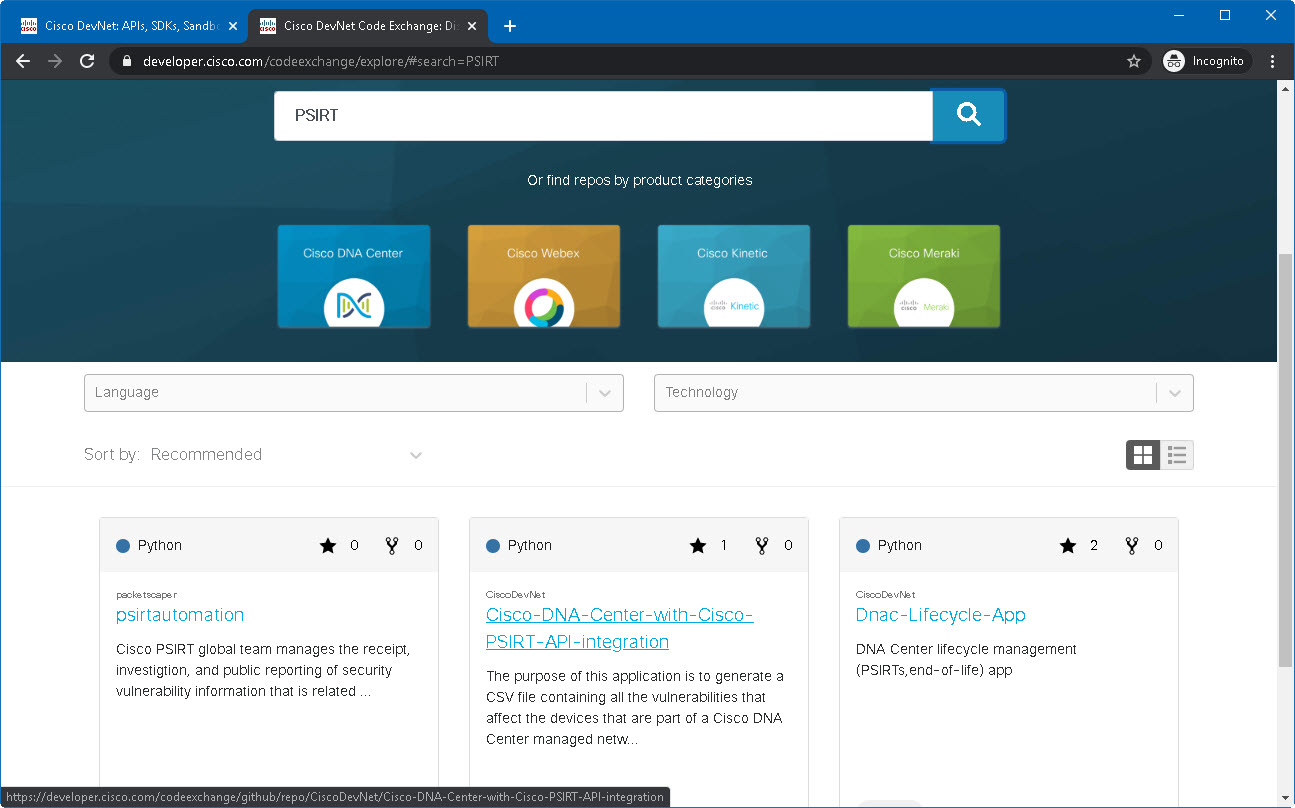
This will open the Cisco DevNet portal, one of the best resources to start or continue learning, with a significant amount of enablement resources. Feel free to explore the website, create a profile and join the community, also, we are here for you!

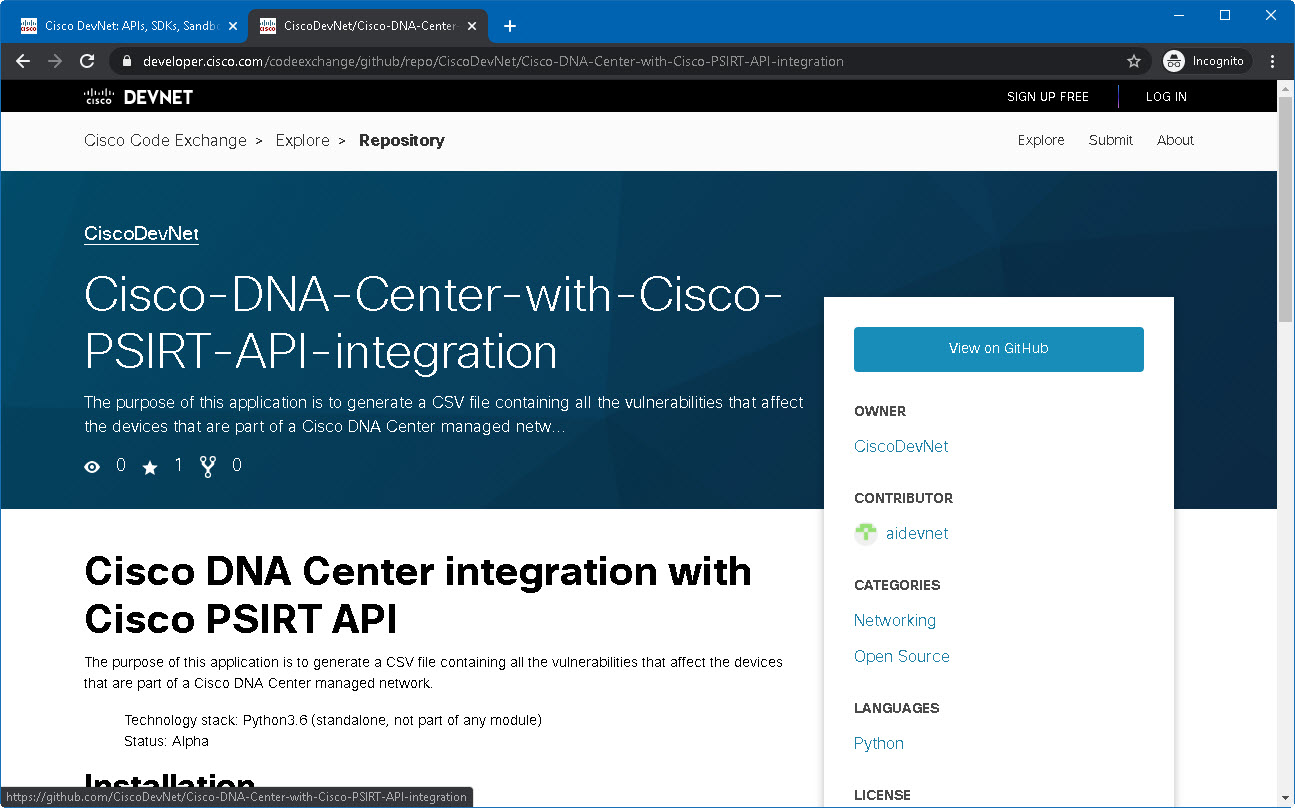
Click on **Discover tab**, then click on **Code Exchange**

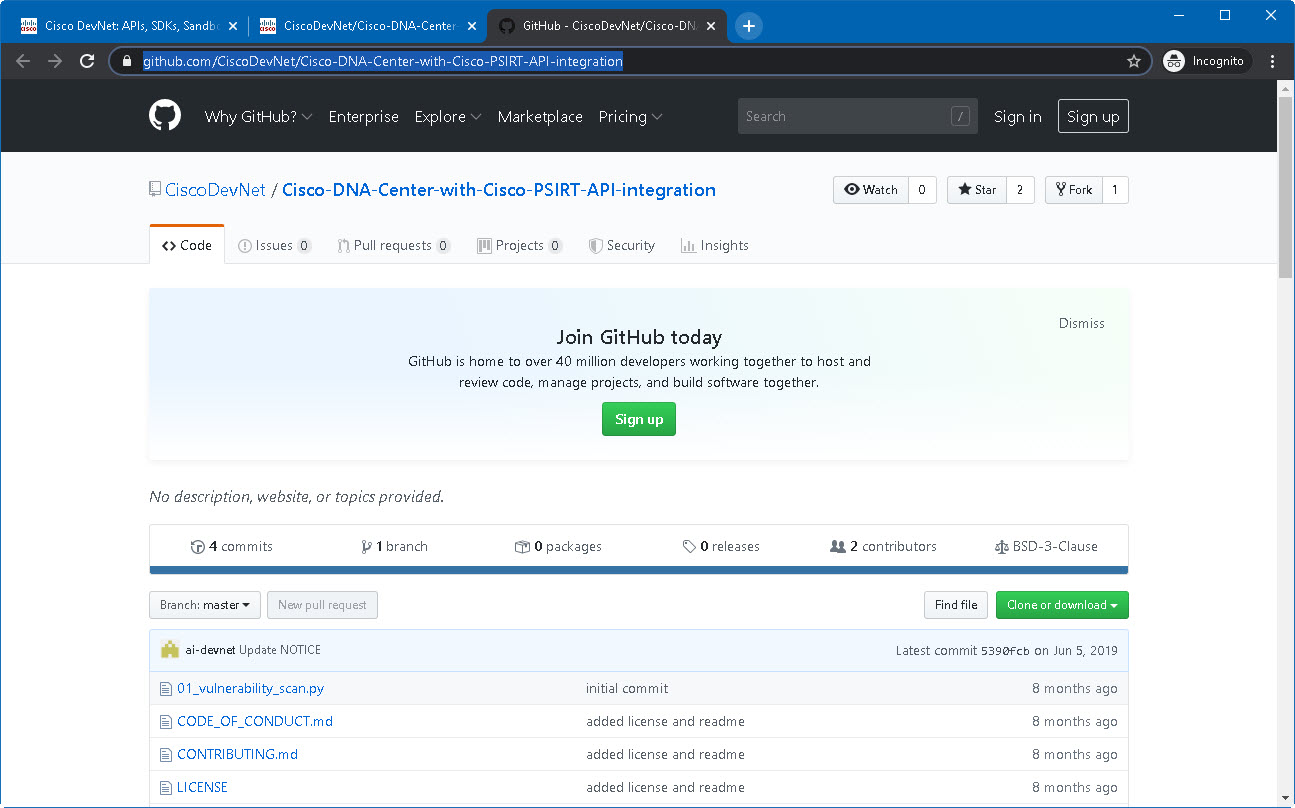
2

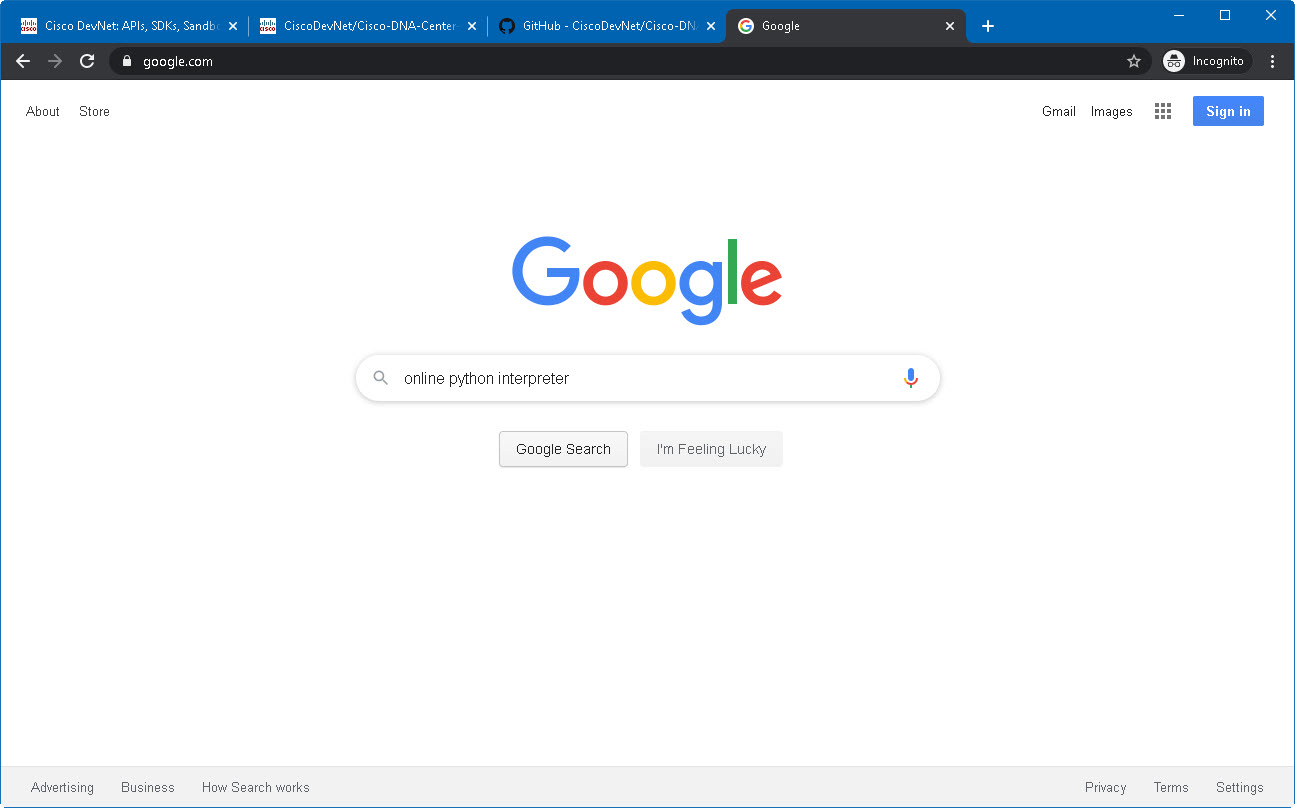
1

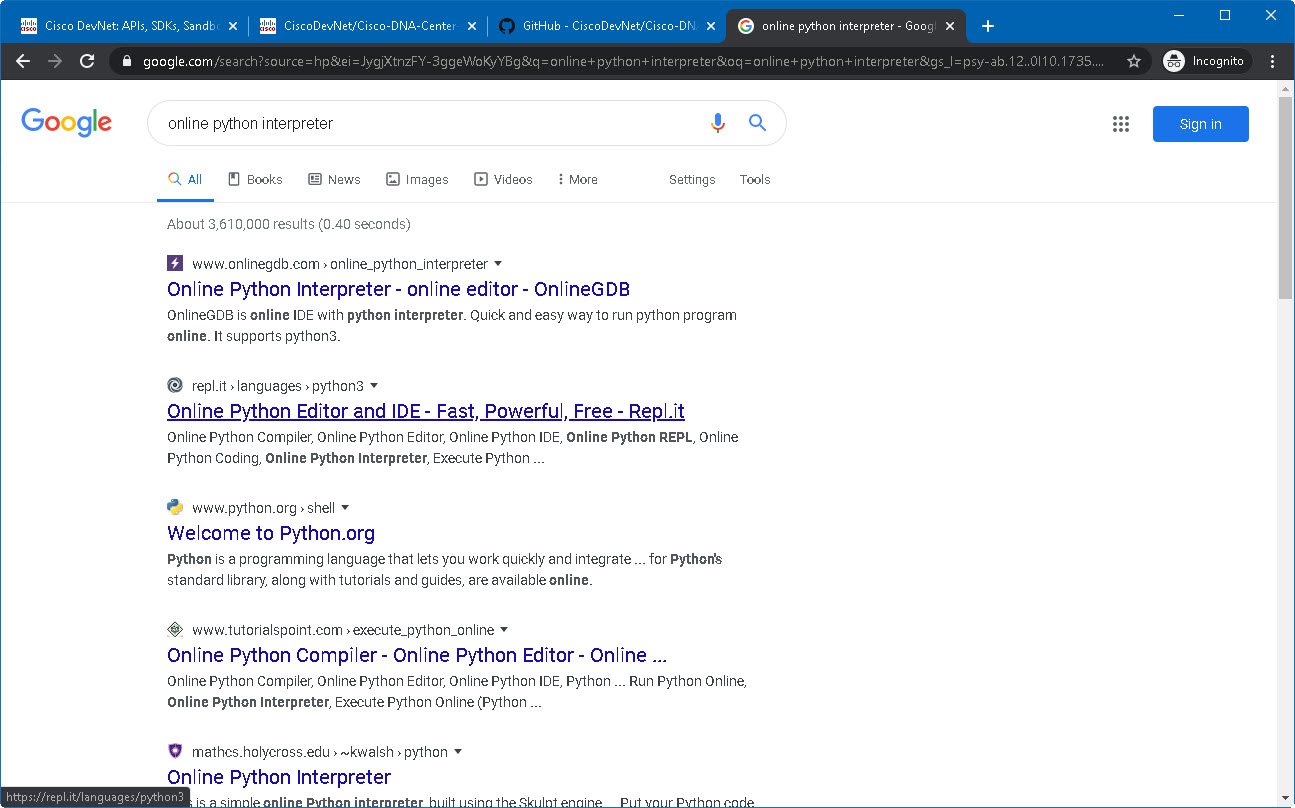
Our use case is a DNAC – PSIRT combination through APIs, so search for **PSIRT**

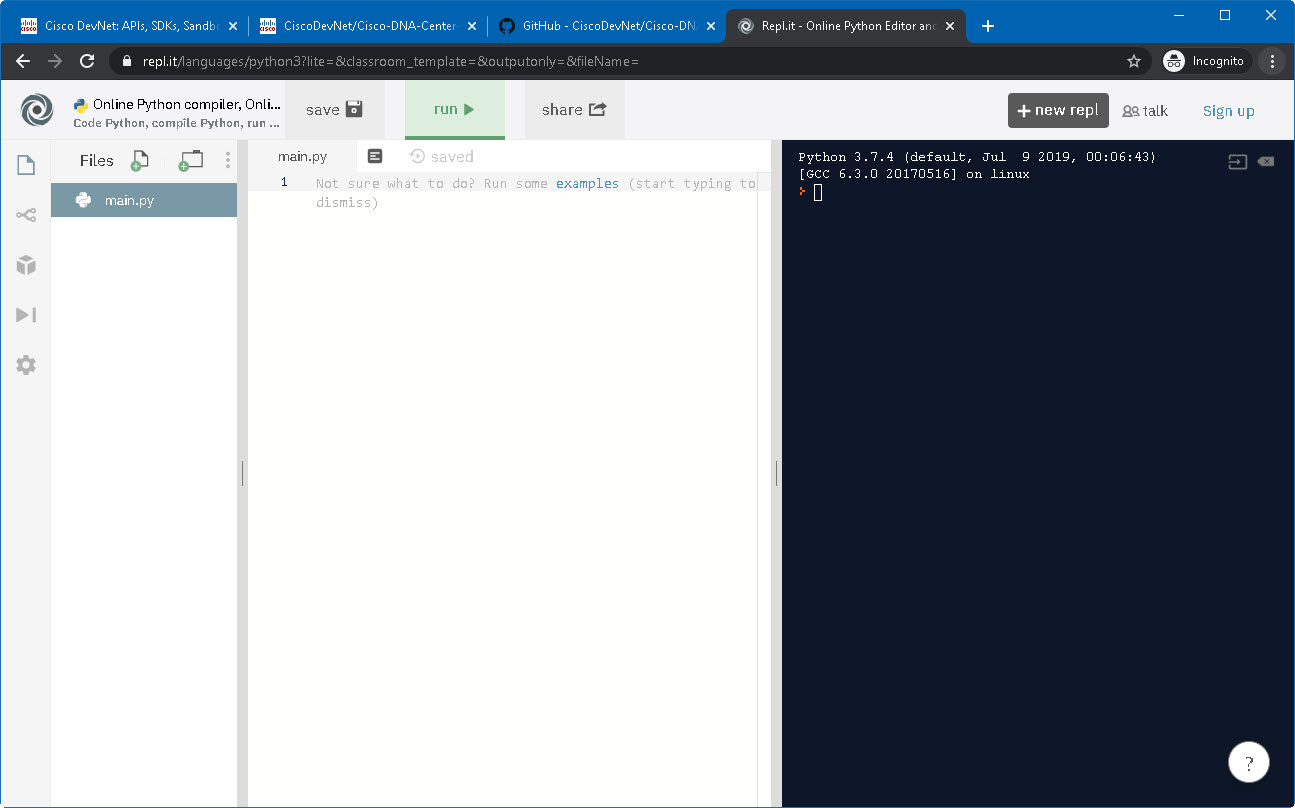
Open the **Cisco-DNA-Center-with-Cisco-PSIRT-API-integration** use case

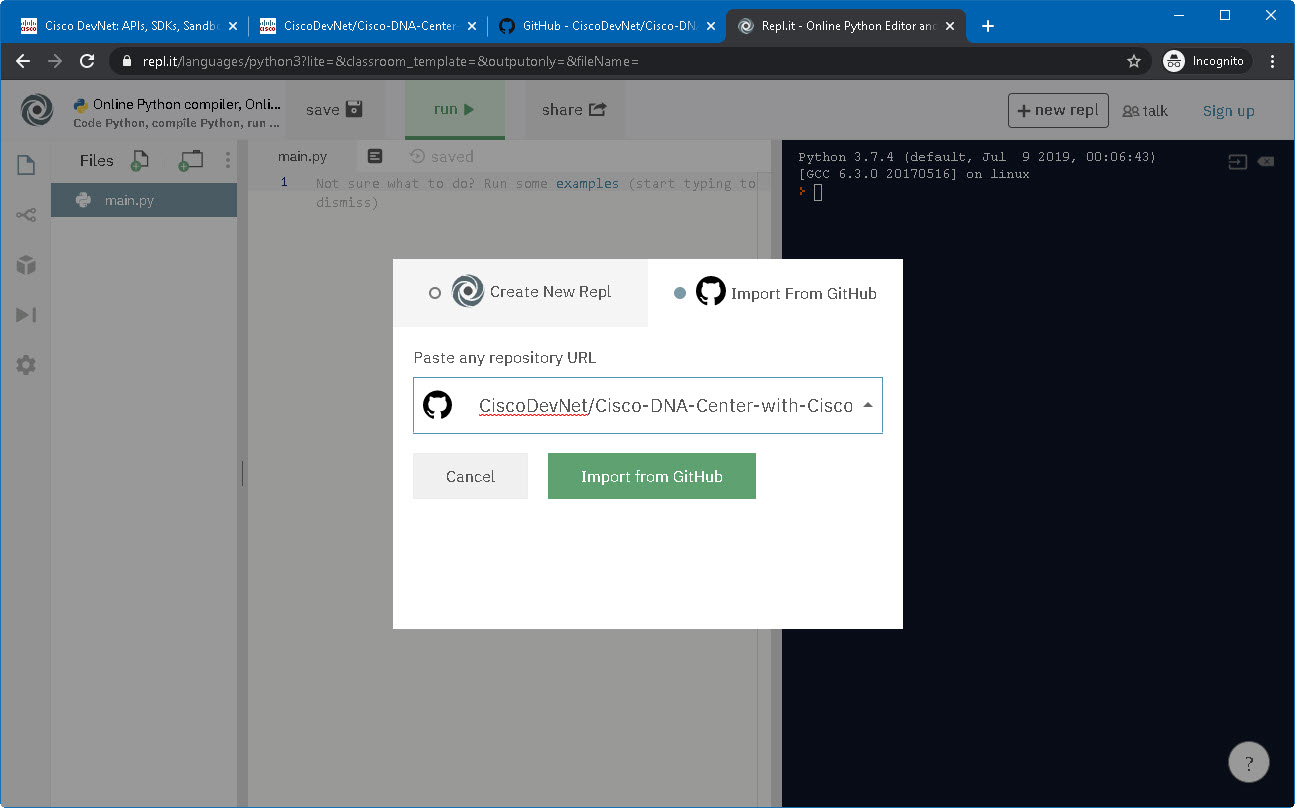
Feel free to glance through the Use Case and its instructions for local installation (highly recommended). But in this case, we want to run it in any PC regardless of operating system, so we’re going to borrow some computing power from the cloud. Click on **View on Github**

This is where the Use Case’s code is. Feel free to explore all the files in it, then select the **https://github.com/CiscoDevNet/Cisco-DNA-Center-with-Cisco-PSIRT-API-integration** URL at your browser’s address bar and **copy** it into the clipboard

We have a GitHub repo (collection of files someone else coded for us) and we need to run it. The recommended way is to install Python locally and set up a developer environment, however, for this guide we’re going to take a quick approach: Open a google window and search for **online python intepreter**

Among the top results should be the interpreter from **repl.it** it’s a great online tool to quickly run Python scripts, click on that **link**

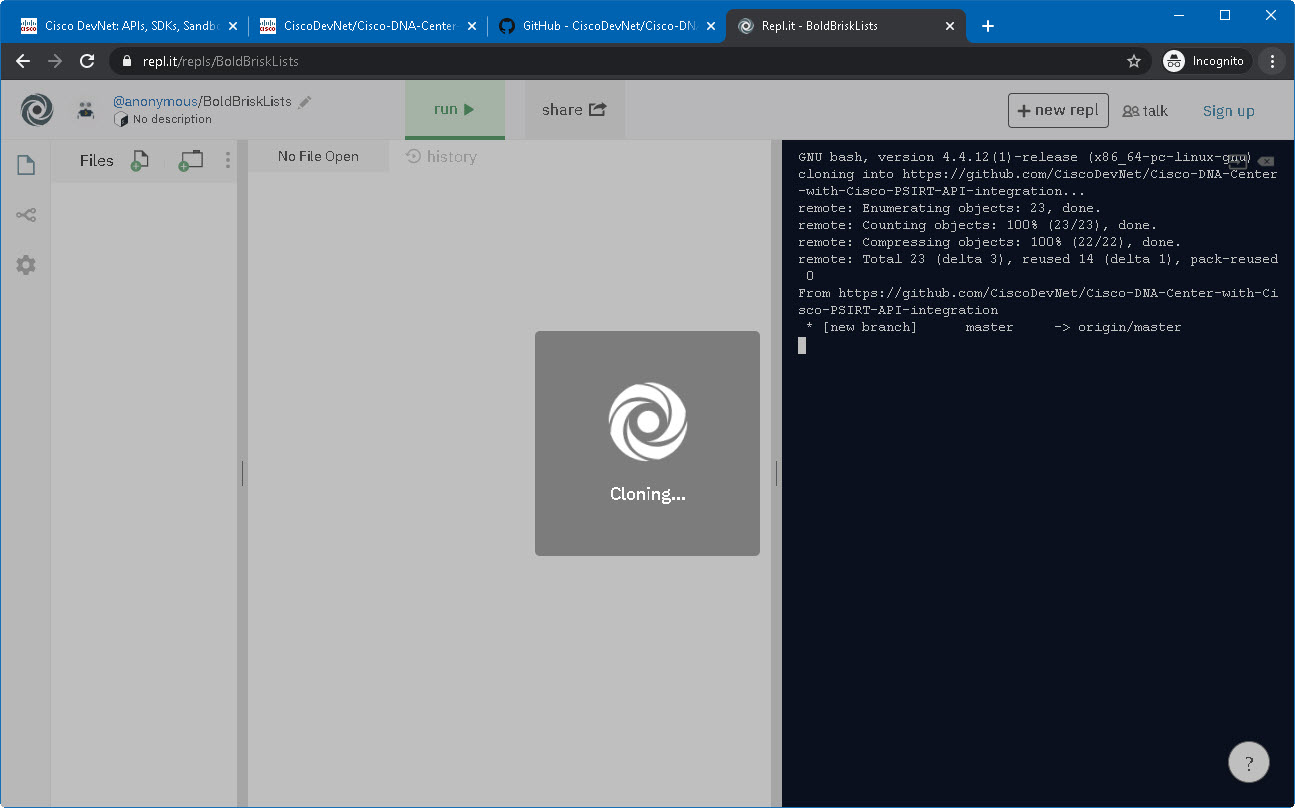
You will be presented with a brand-new online environment ready to run Python 3.7.x scripts. Click on the **+ new repl** button

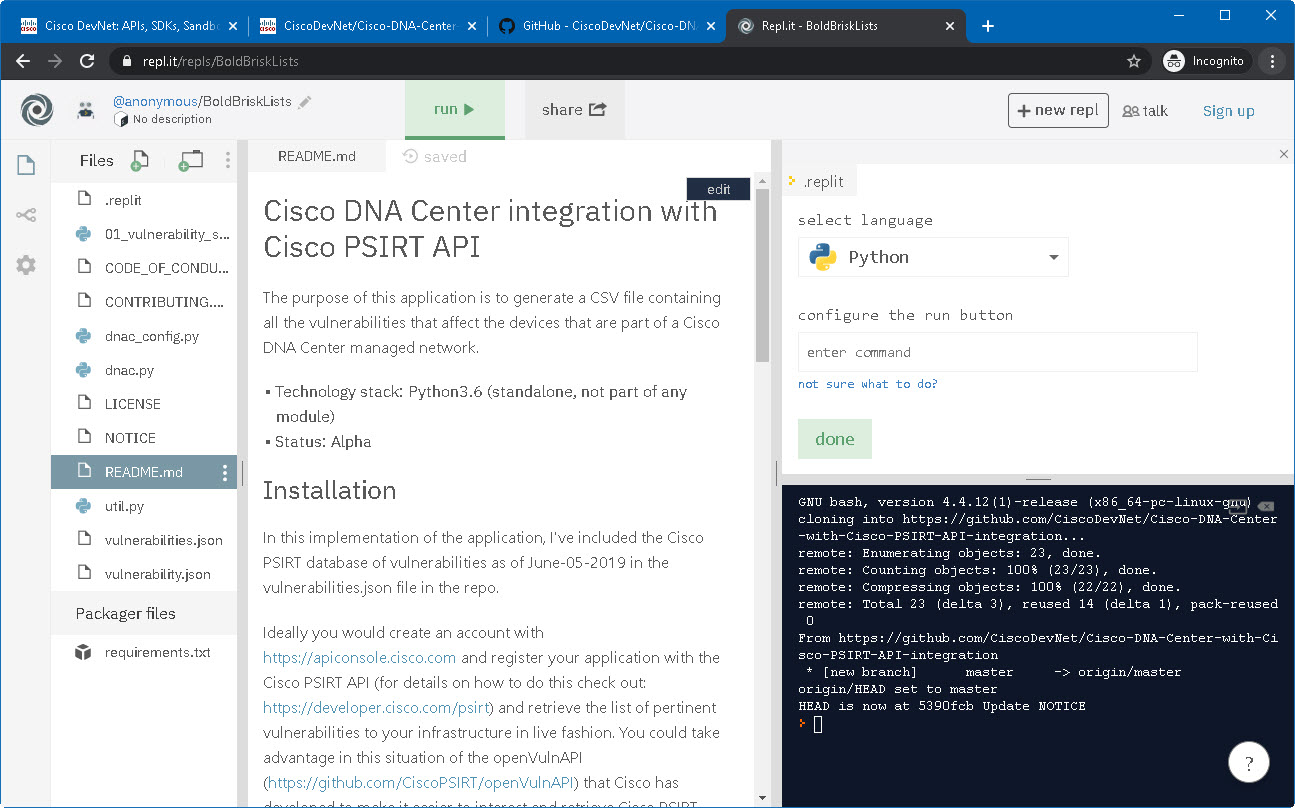
Click the **Import from GitHub** **(1)** tab and paste the **URL** **(2)** from the GitHub repo you copied earlier, then click on **Import from GitHub (3)**  
You might get prompted by the browser that changes made to the site may not be saved, this is because repl.it started a new interpreter for you and does not want you to lose any progress. Click **Leave** if prompted

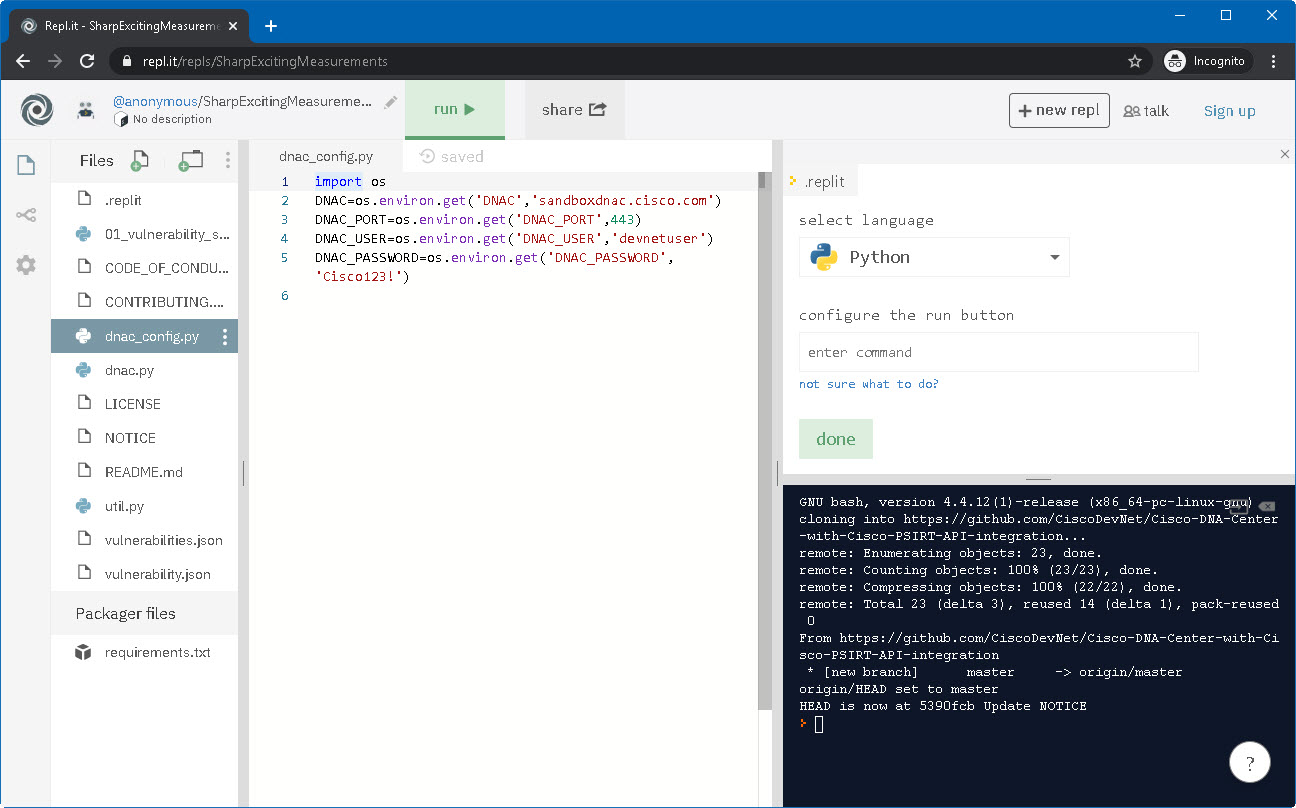
3

2

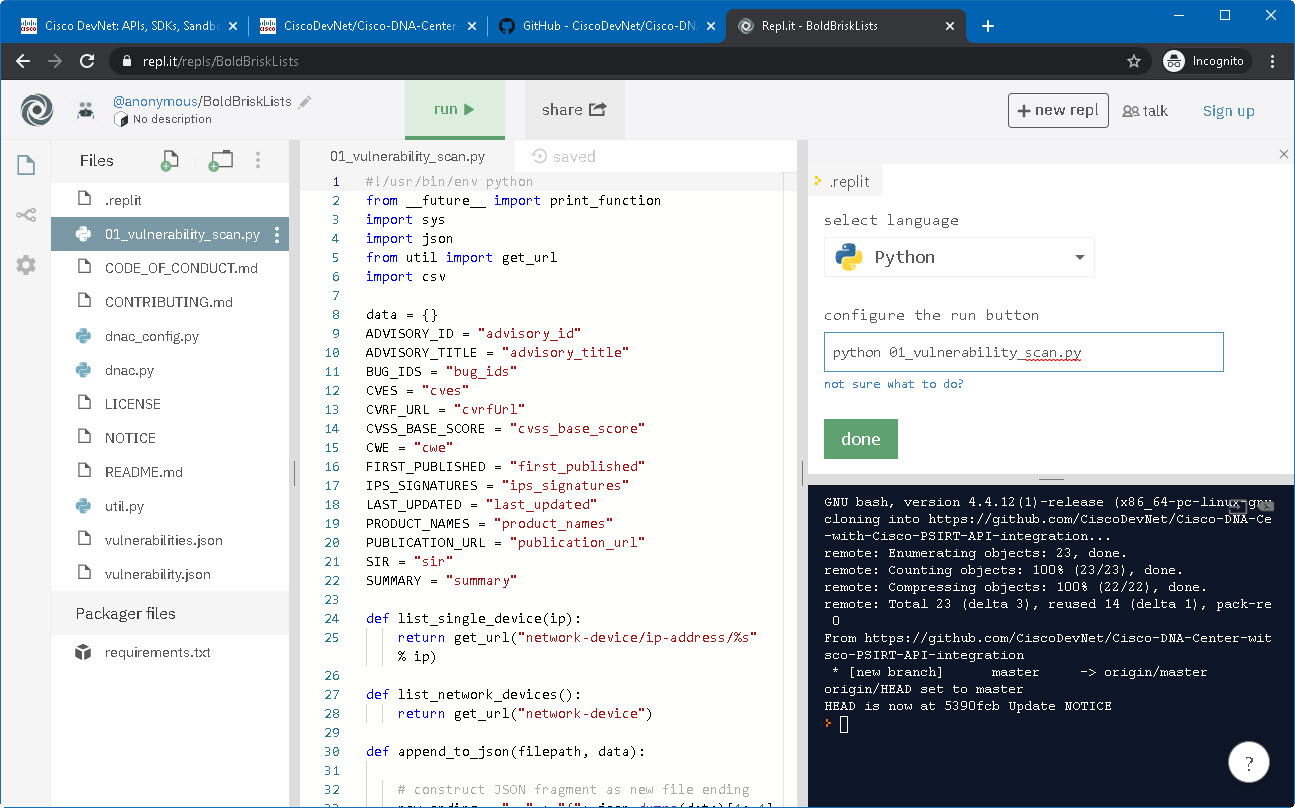
1

The GitHub repo will be side-loaded from GitHub into the repl.it environment. Wait until the file tab indicator says **saved** before continuing

Feel free to explore the **files** on the left

One of the files on the left is **dnac\_config.py**. There are 5 lines of code that will tell the Python interpreter where the target DNA Center is, if you want to test the Use Case against your own DNA Center, feel free to edit this file accordingly. Otherwise, the sandboxdnac.cisco.com is a great always-on resource from DevNet to learn this and many other use cases. 

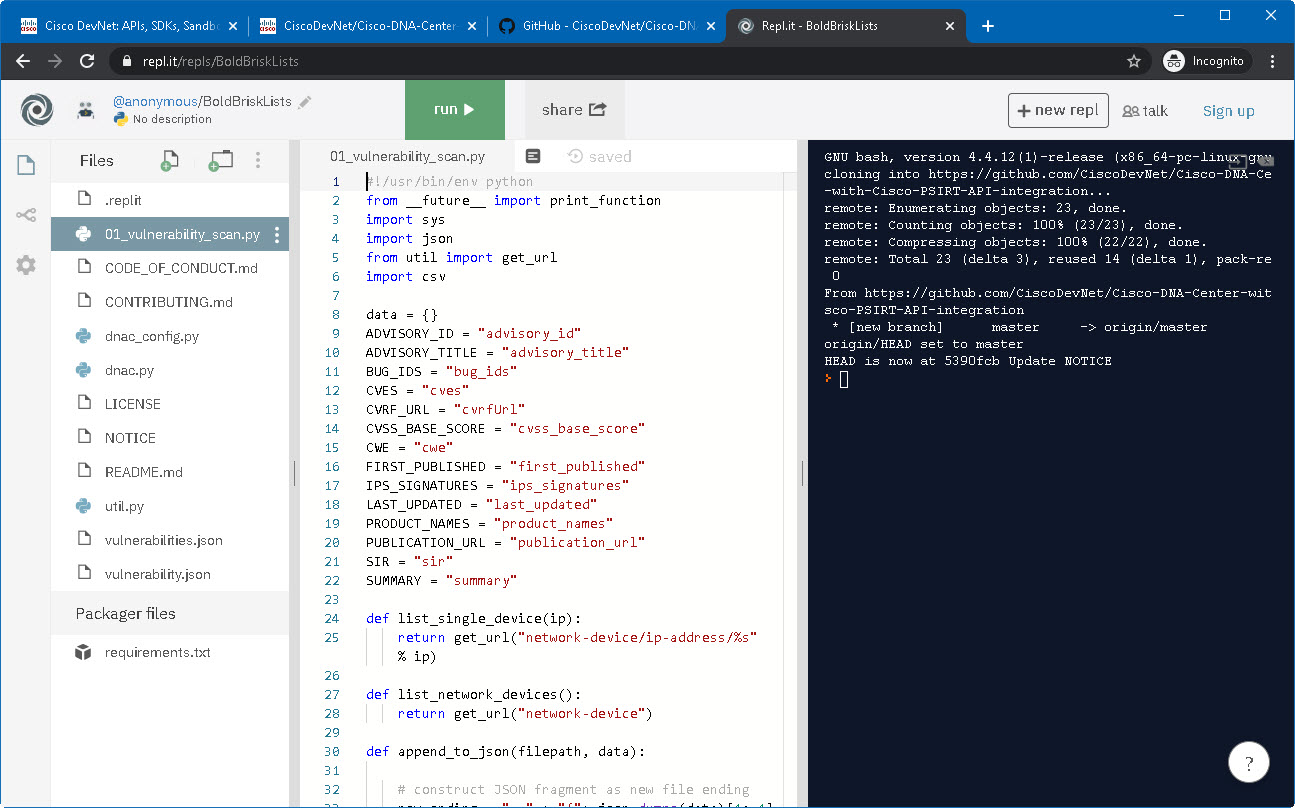
Click on the **01\_vulnerability\_scan.py** file **(1)** andexamineits contents. This is the main script. It will import the other Python (**.py**) files to function properly, but the bulk of the work is being done in these 90 lines. We are not ready to run the script just yet, because there are several files and the repl.it engine doesn’t know which is the main one.

Enter the text **python** **01\_vulnerability\_scan.py** in the top right dialog **(2)** as shown, and click **done (3)**. This means that when the run button is clicked, it should execute that command, which will run the main script

2

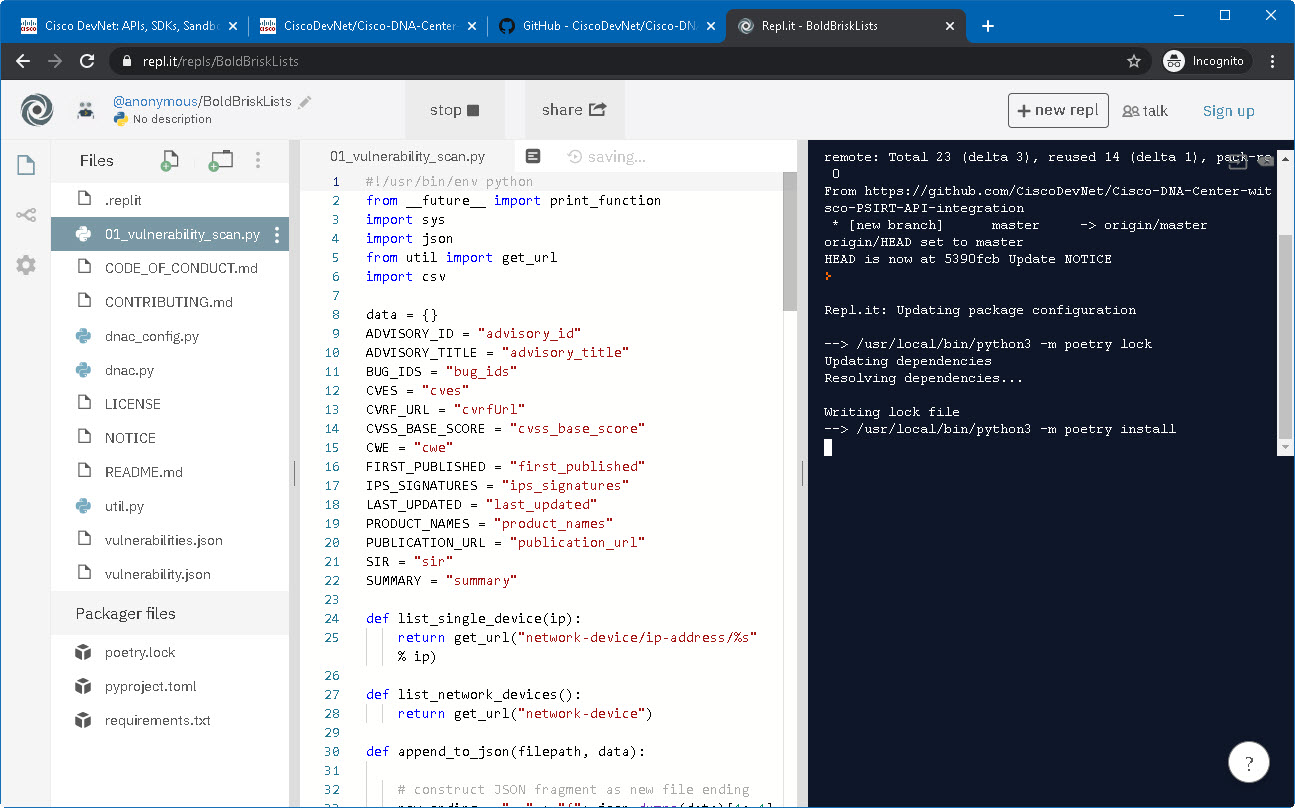
3

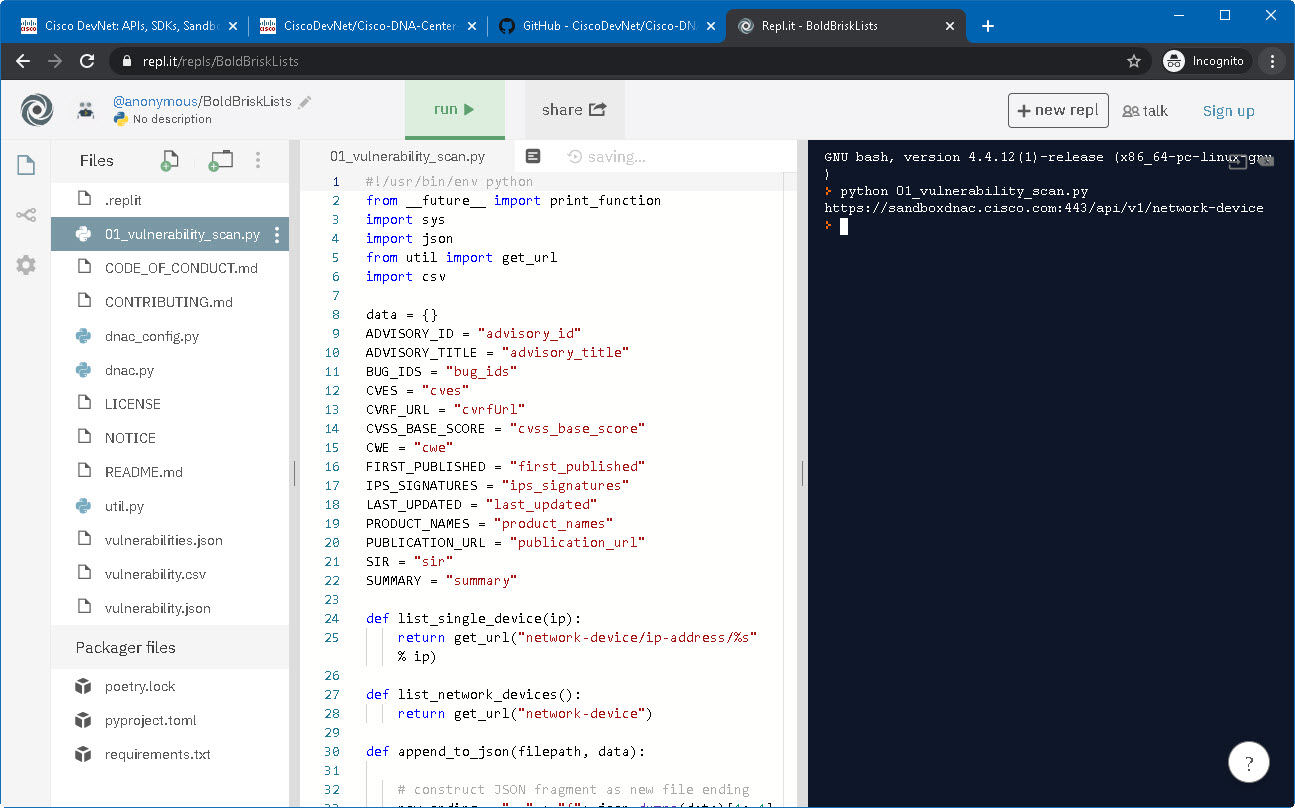
1

At this point we are ready to run our script. Click the green **run** button

**Wait** for the script to run. Because Python is trying to import packages that repl.it doesn’t have, it will automatically install them for you. This might take a few seconds.

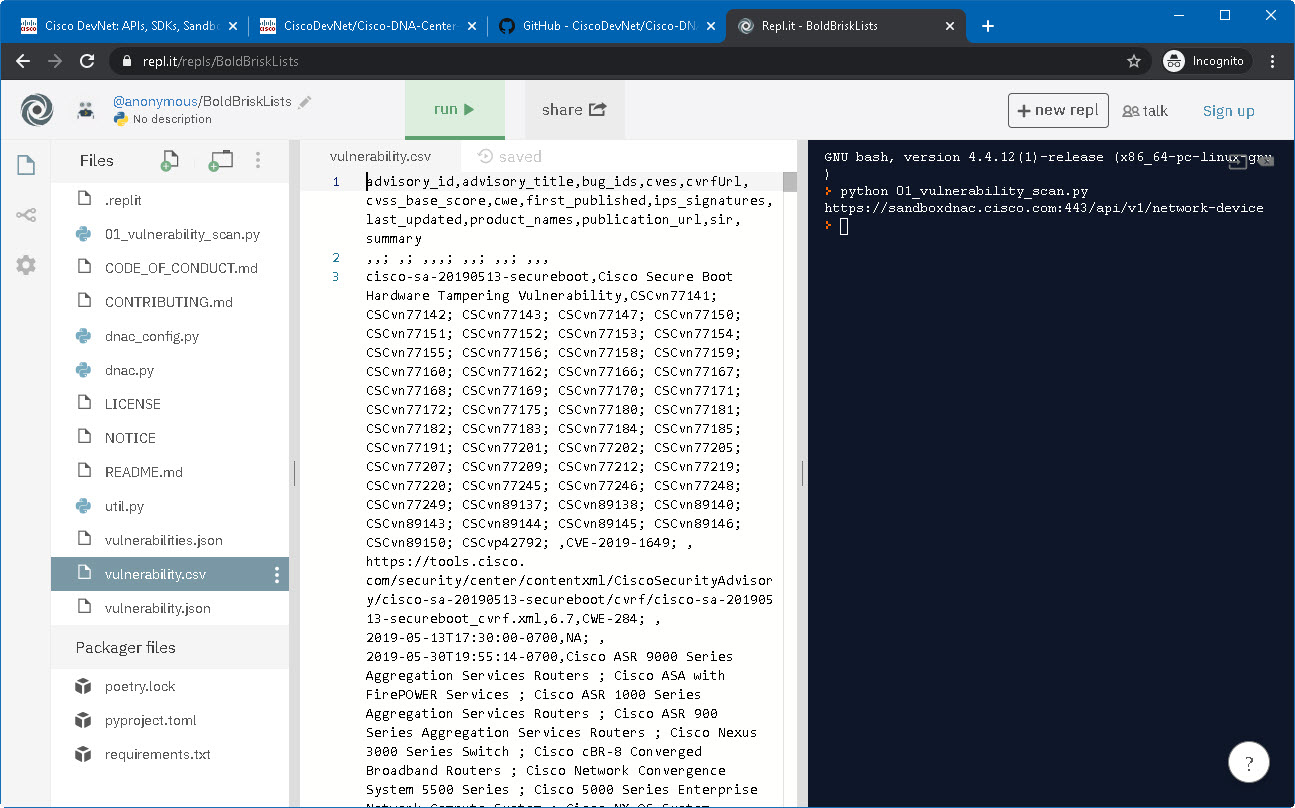
At this point, the script is running through the code, which is telling Python to go fetch DNA Center information, grab all the devices that are in its domain, and compare them against a known vulnerability list to see which devices might be in that list. Then it will create a comma-separated-values (CSV) file with the results.

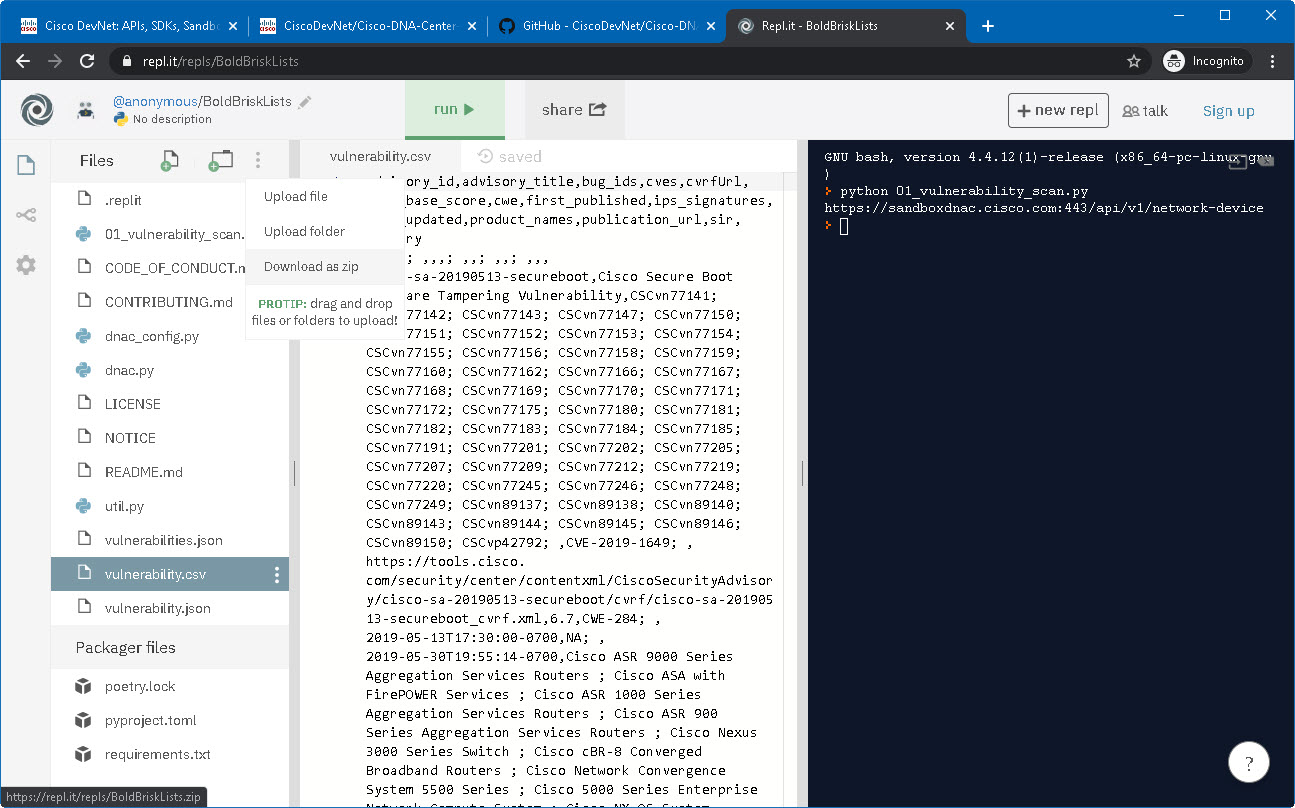
Note that there is no **.csv** file anywhere on the file list on the left. 

When the script finishes running, you will notice in the console that it just prints the address of the DNA Center and the API path it targeted to get the device information **(1)**, nothing more. This is because the Script was designed to capture a significant amount of vulnerability data that is better managed through a spreadsheet. So, its output will be the newly-created **vulnerability.csv** file you will see on the left panel **(2)** 

1

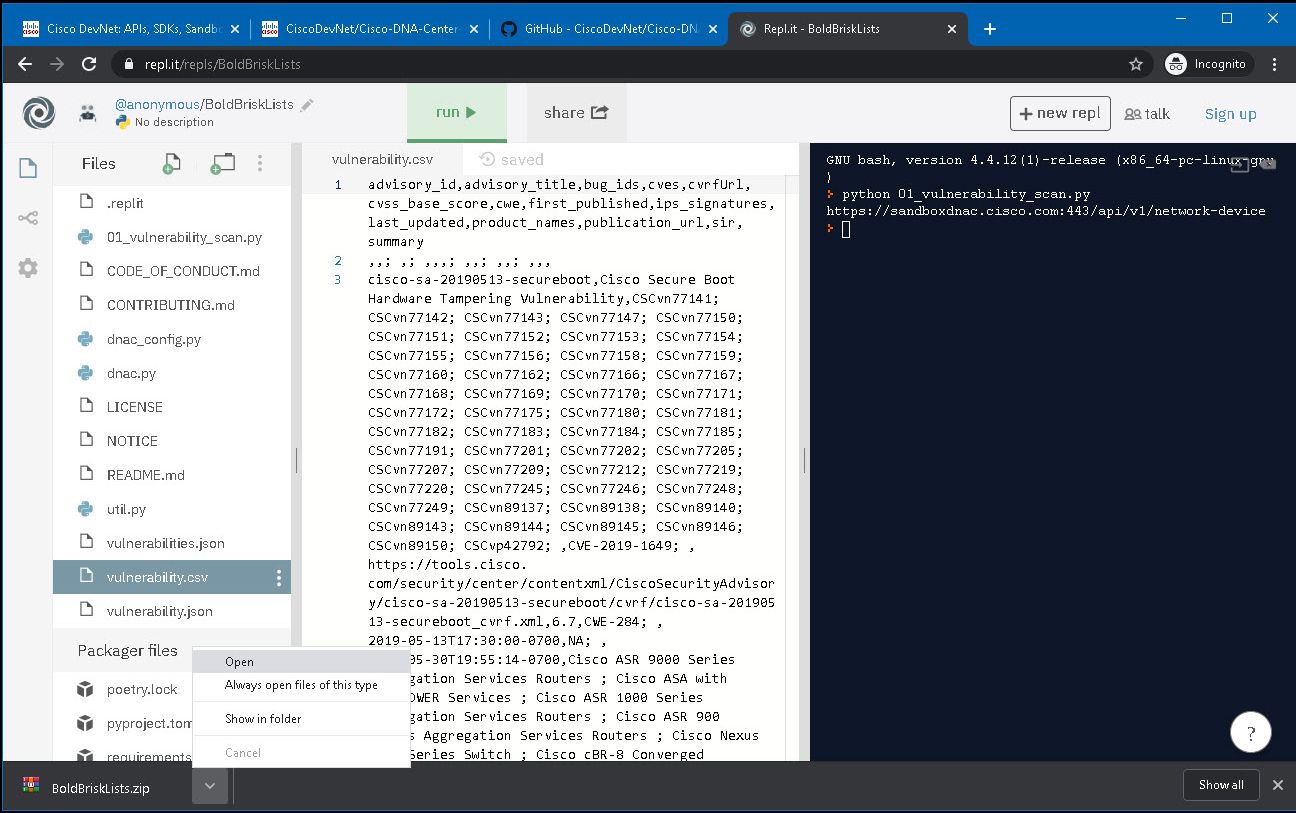
2

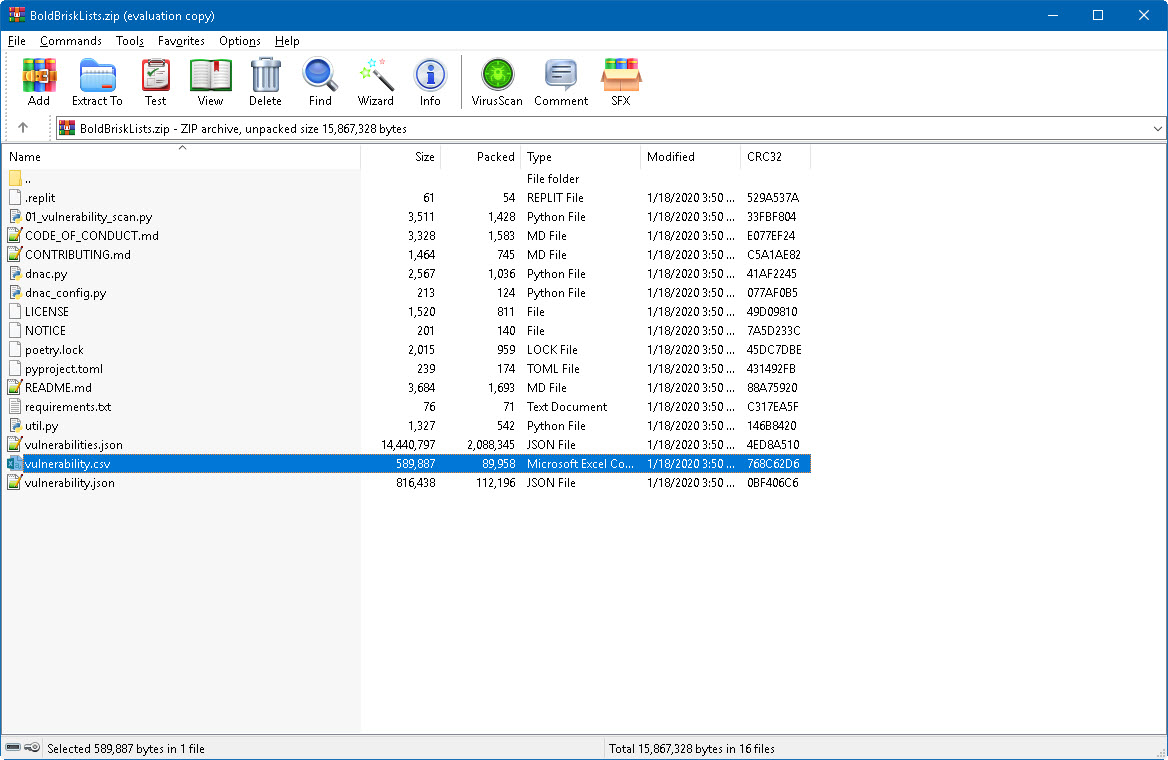
Click on the **vulnerability.csv** file and check its contents. It’s not very readable, perhaps downloading the files and opening it in Excel is better

Click on the **three dots** of the left panel**(1)**, and then **Download as zip (2)**

1

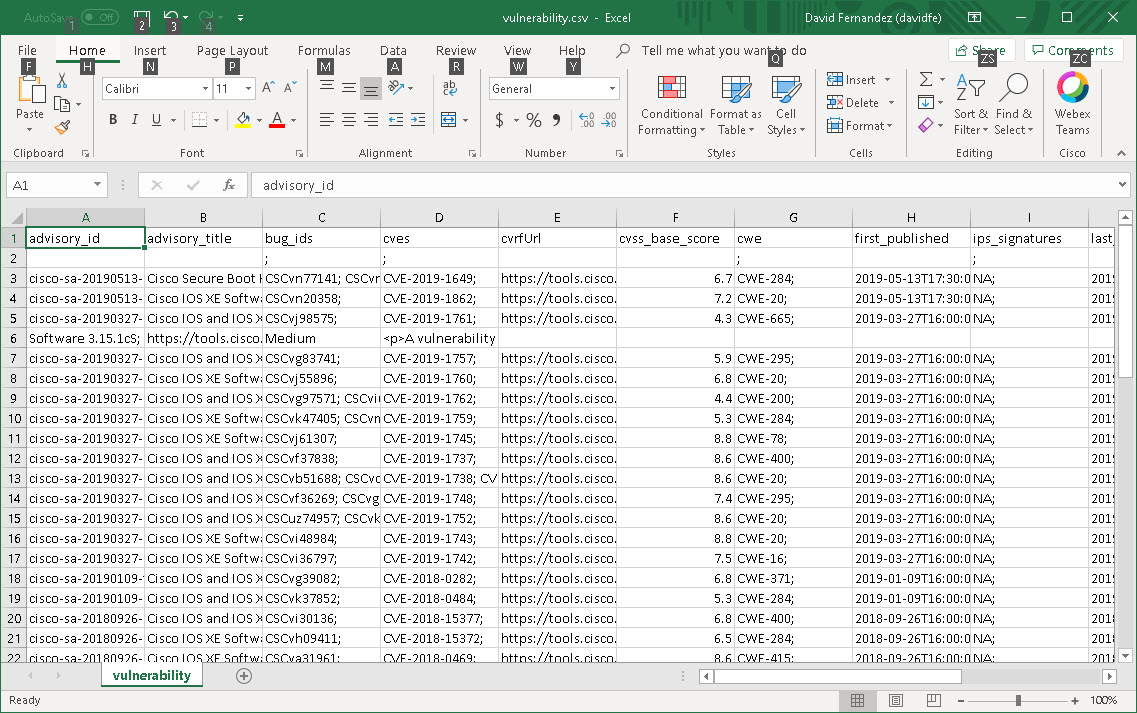
2

Note that repl.it generates random phrases for its environments so that they’re unique. Your environment and filename will be different. Once the file downloads, **open** the zip file

Open the **vulnerability.csv** file

There it is! The result of the script is the correlation between all your devices in DNA Center’s view, and the associated vulnerabilities that may affect them. From here, you may sort the data, send it to a team of analysts, or even generate alarms when some of these vulnerabilities are above a certain threshold.

Continue below for the final step!



*The beauty of programmability is that it elevates your status from the doer of the work to the designer of the work. Make the machines work, not your fingers!*

Hope you enjoyed the guide and don’t hesitate to contact me for any questions!

David Fernandez – [davidfe@cisco.com](mailto:davidfe@cisco.com)