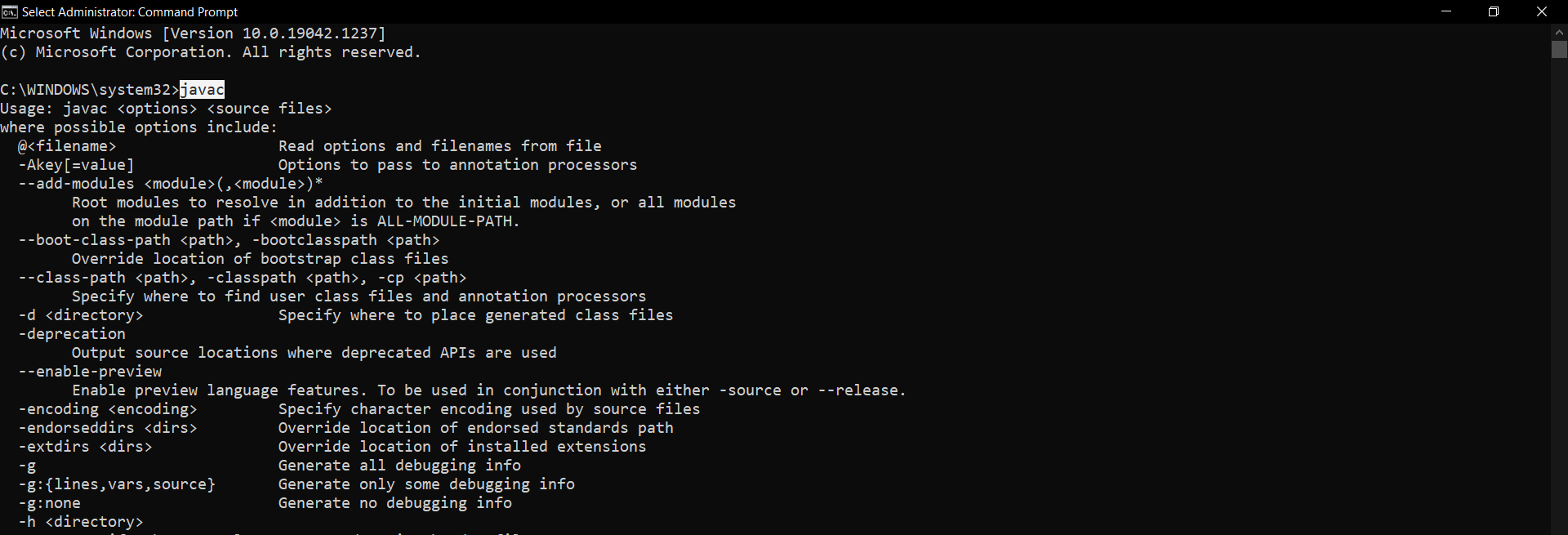
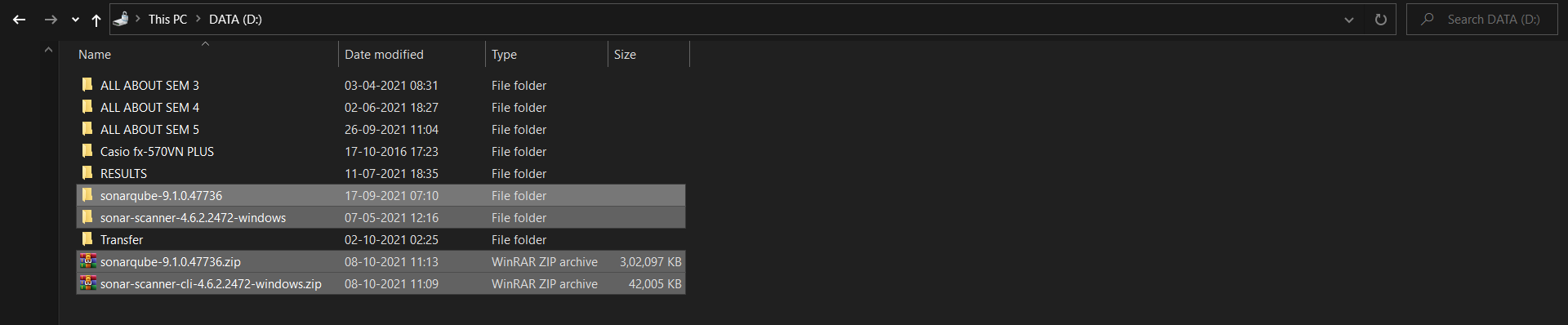
**Aim:**  To understand Static Analysis SAST process and learn to integrate SAST to SonarQube.

**Screenshots:**

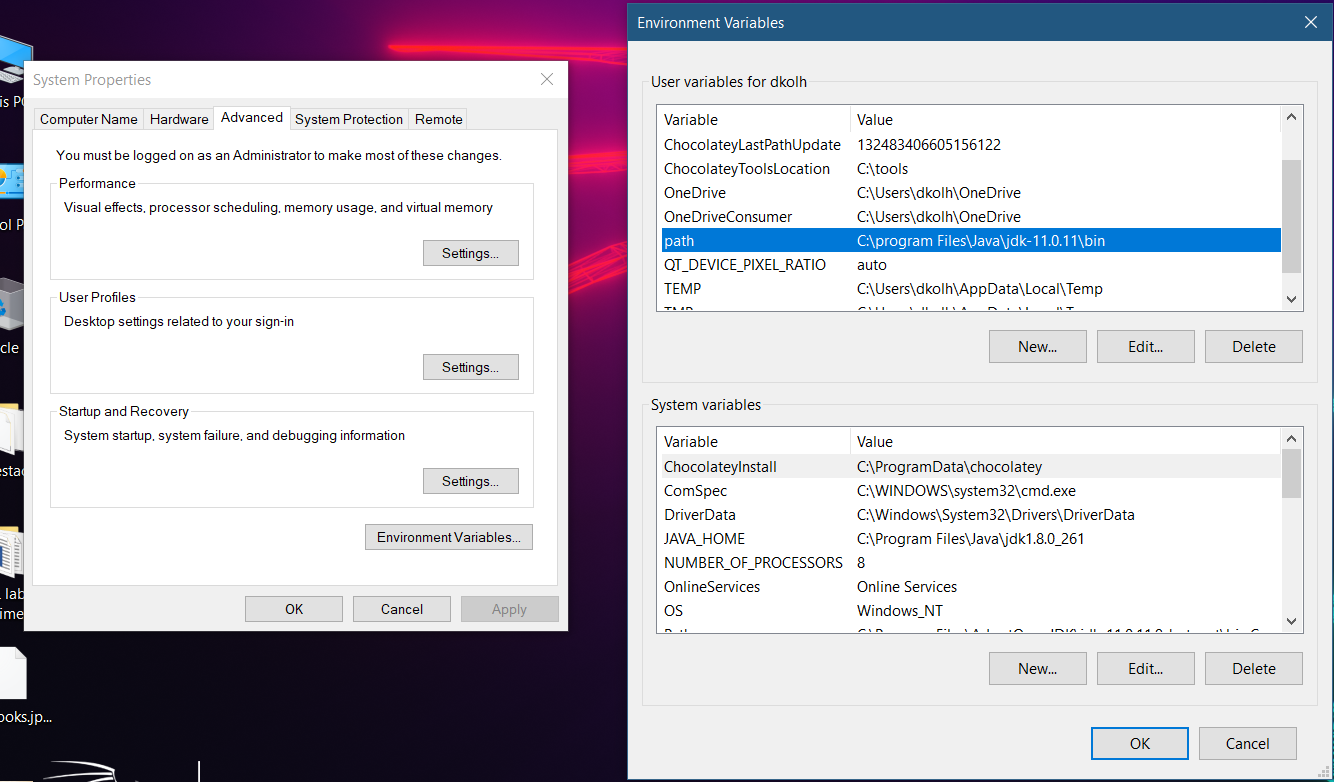
* For performing this practical we need jdk 11 or latest version in our system.



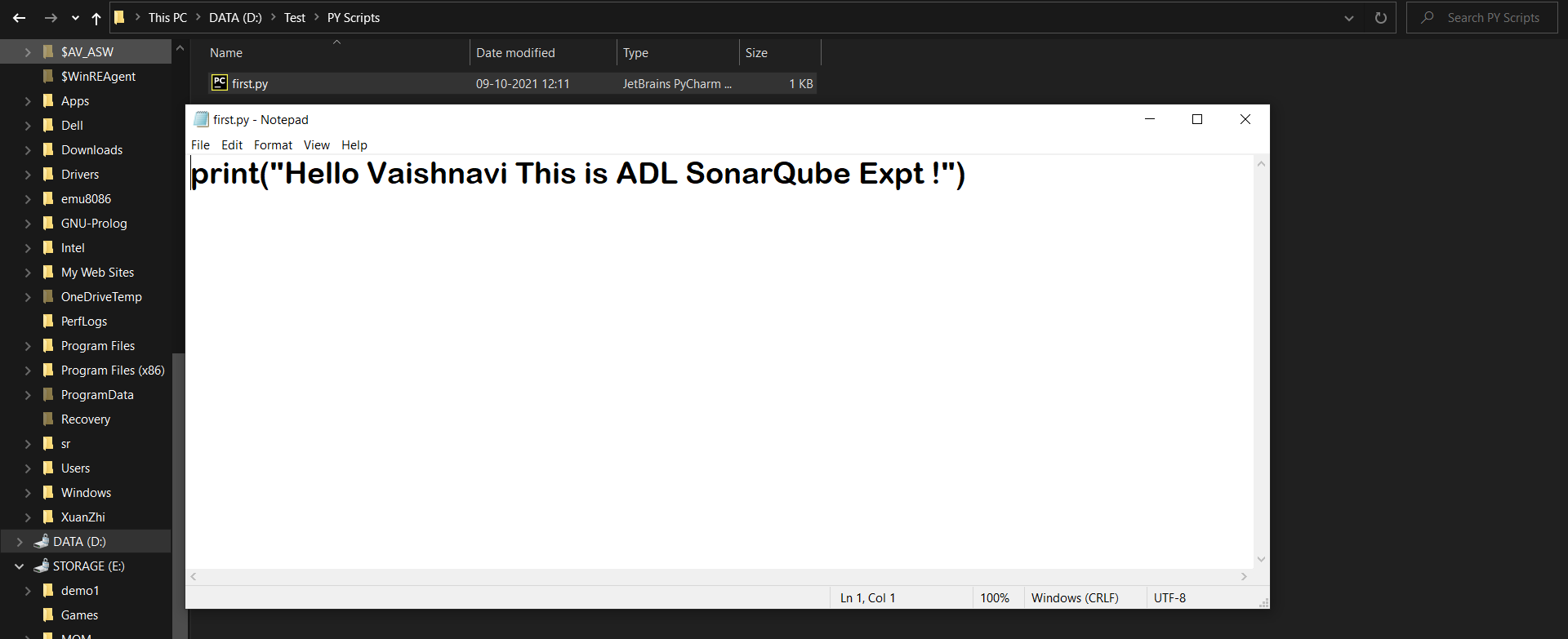
* Download **SonarQube** and **SonarScanner** zip file and extract it in a folder.



* Java Path added in environment variables

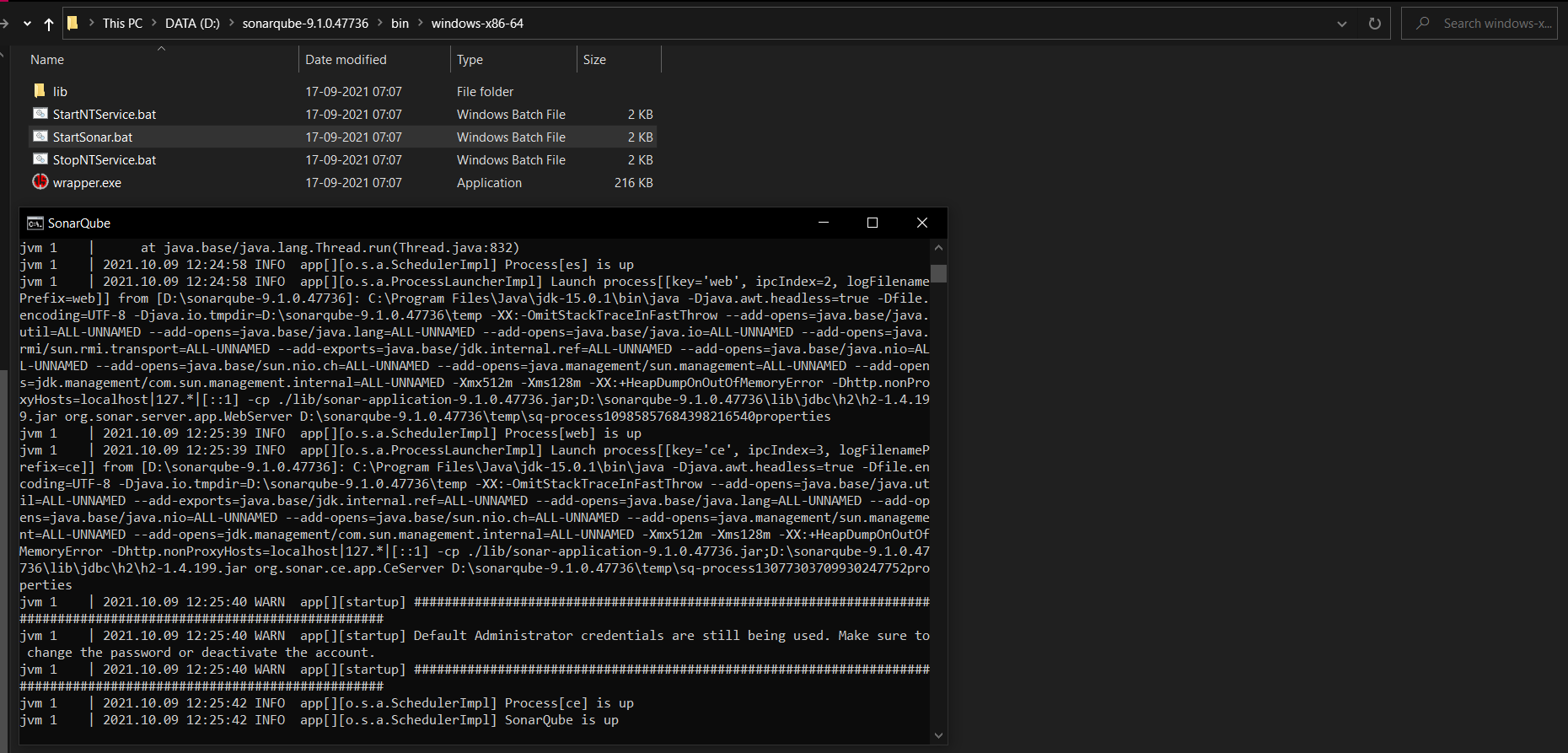


* Copy-Pasting the path of SonarQube till folder in user variables environment
* Create a new folder in that create one more folder and add the program which you want to test. (Here I have added a simple python program for testing)

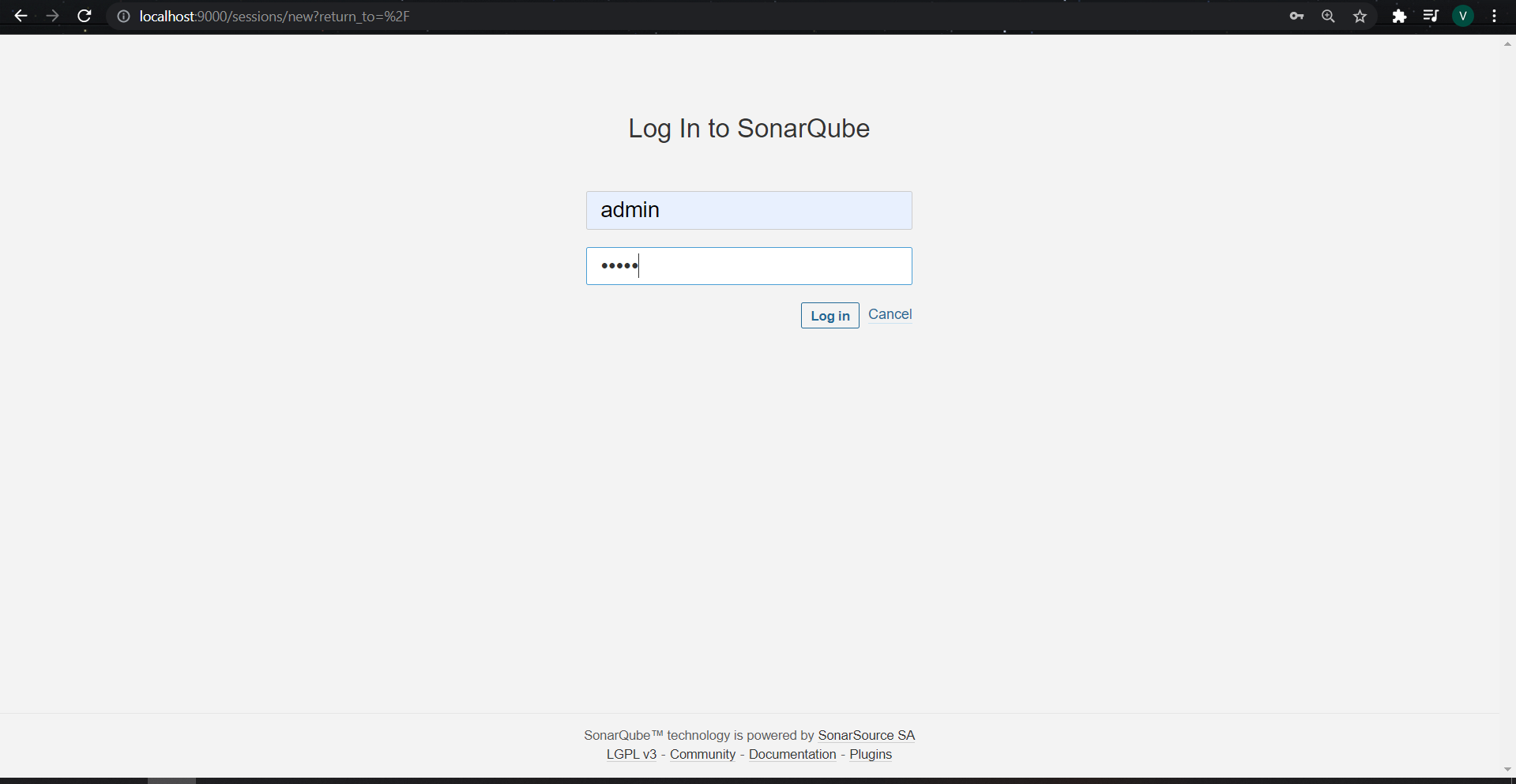


* In the SonarQube folder click on 🡪 windows folder and then click on 🡪Start Sonar

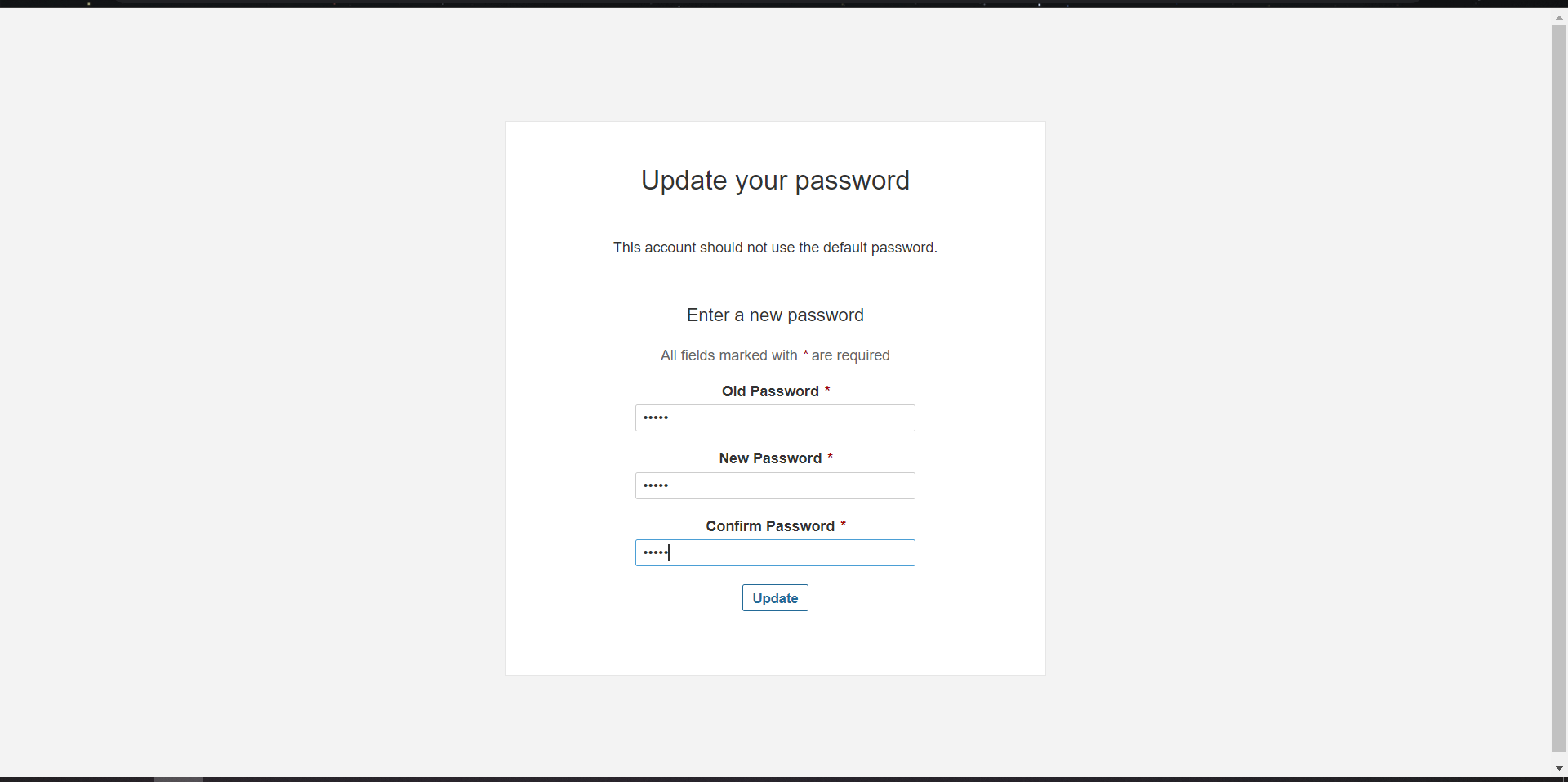
Keep the command prompt open all the time while performing the experiment



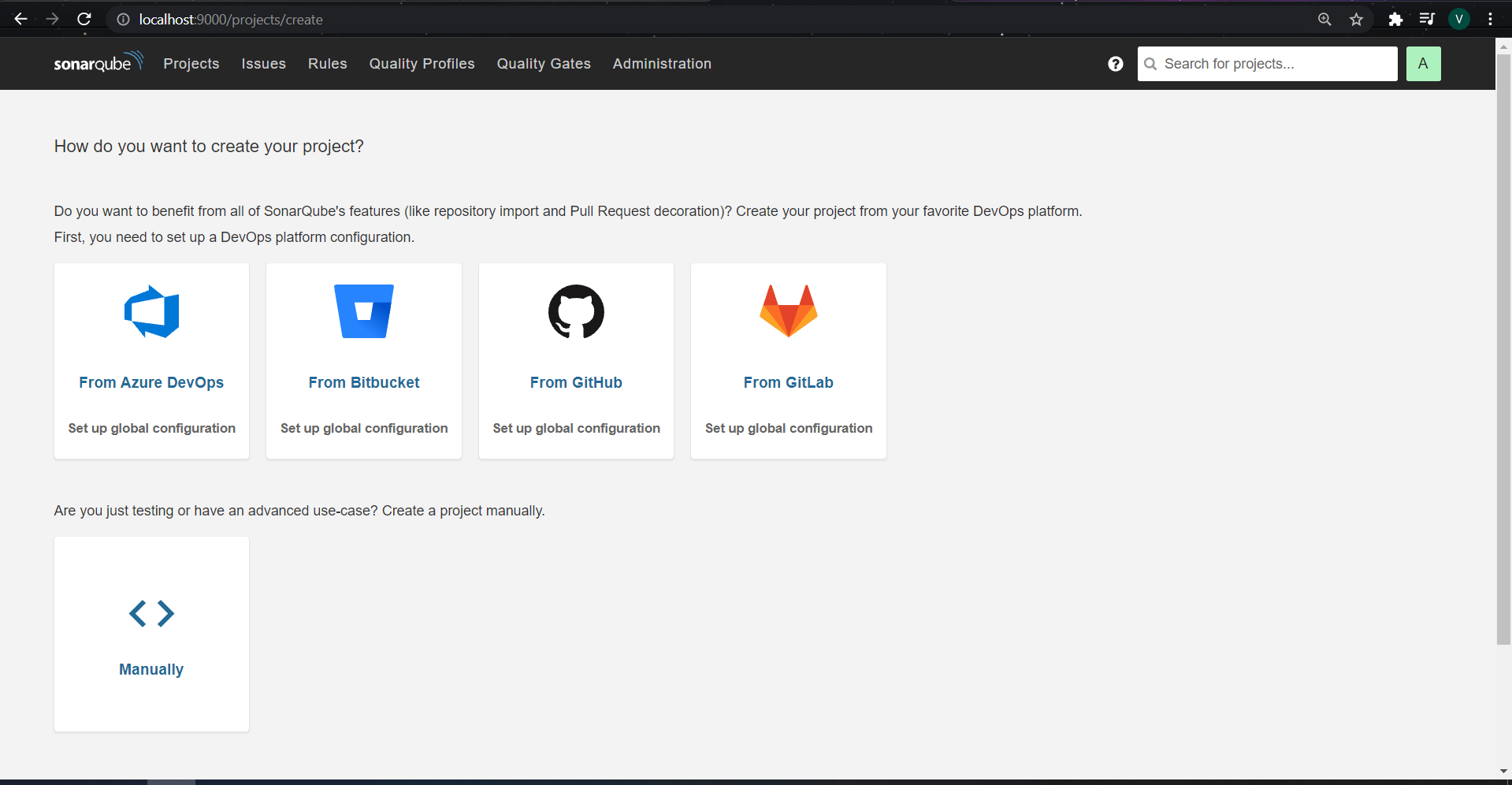
* To run SonarQube open the URL <https://localhost:9000> and type username and password which is by default (admin)



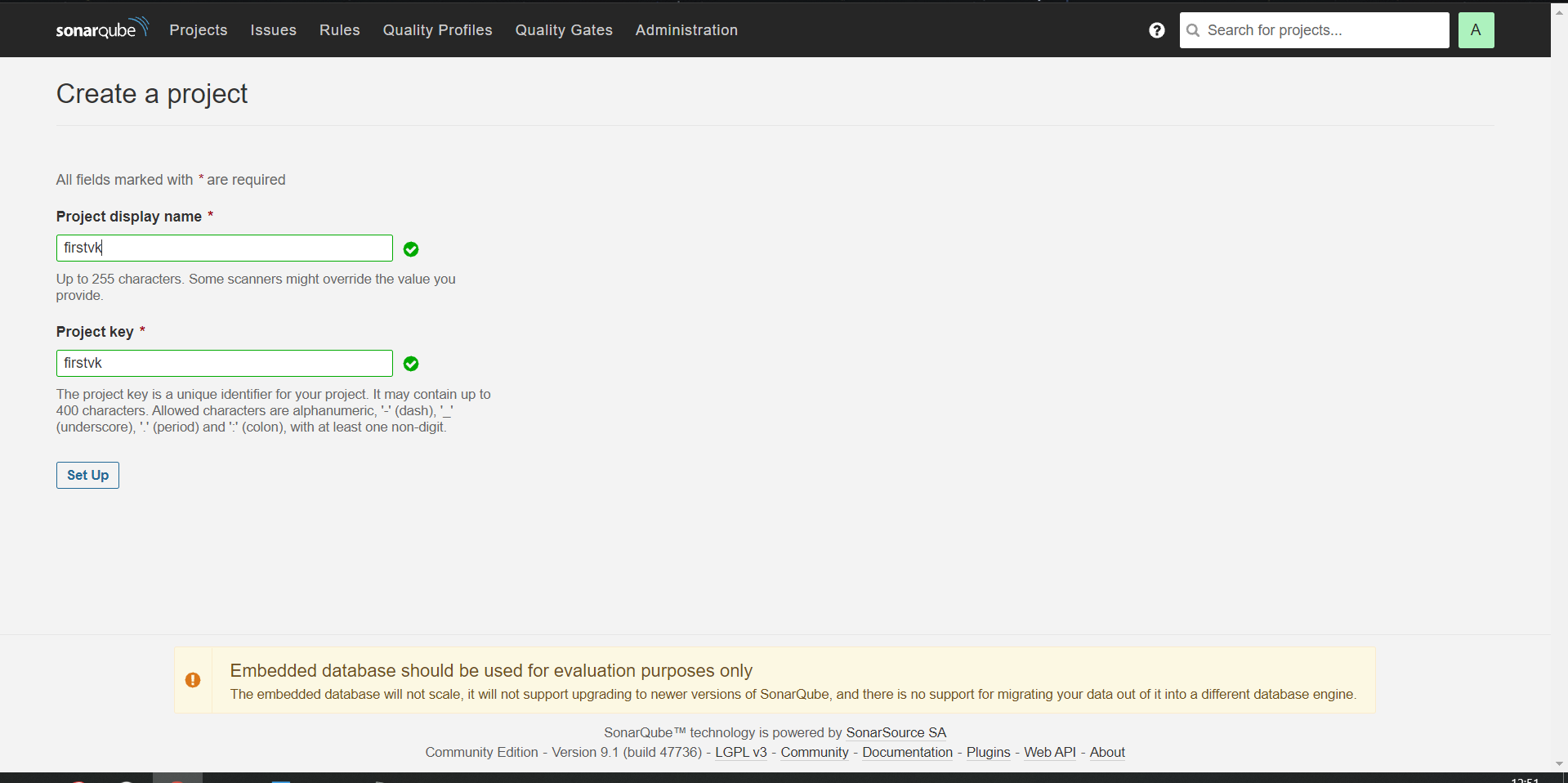
* After login it will ask to change the password for admin to something else



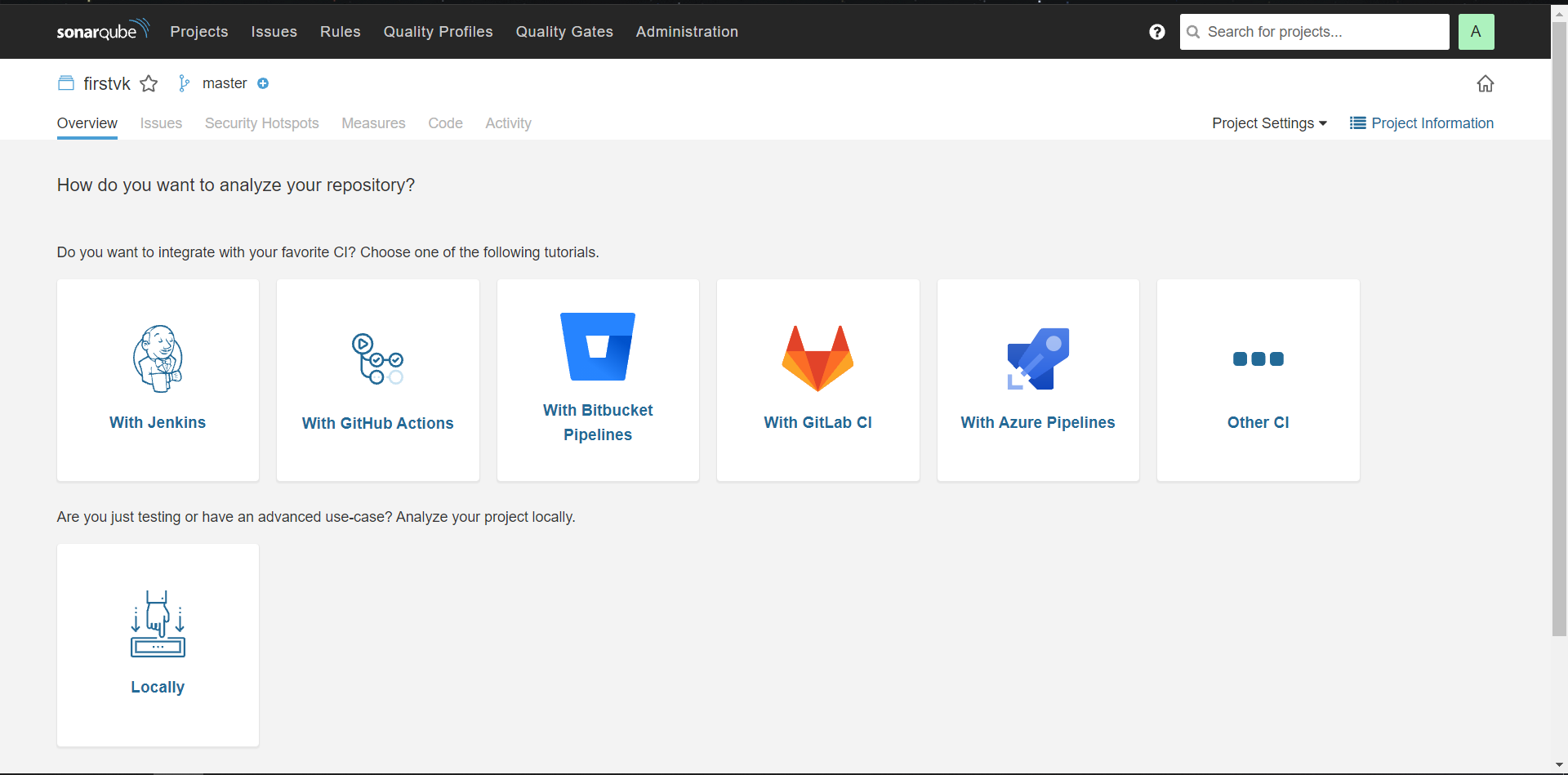
* After changing password, the SonarQube dashboard will get opened



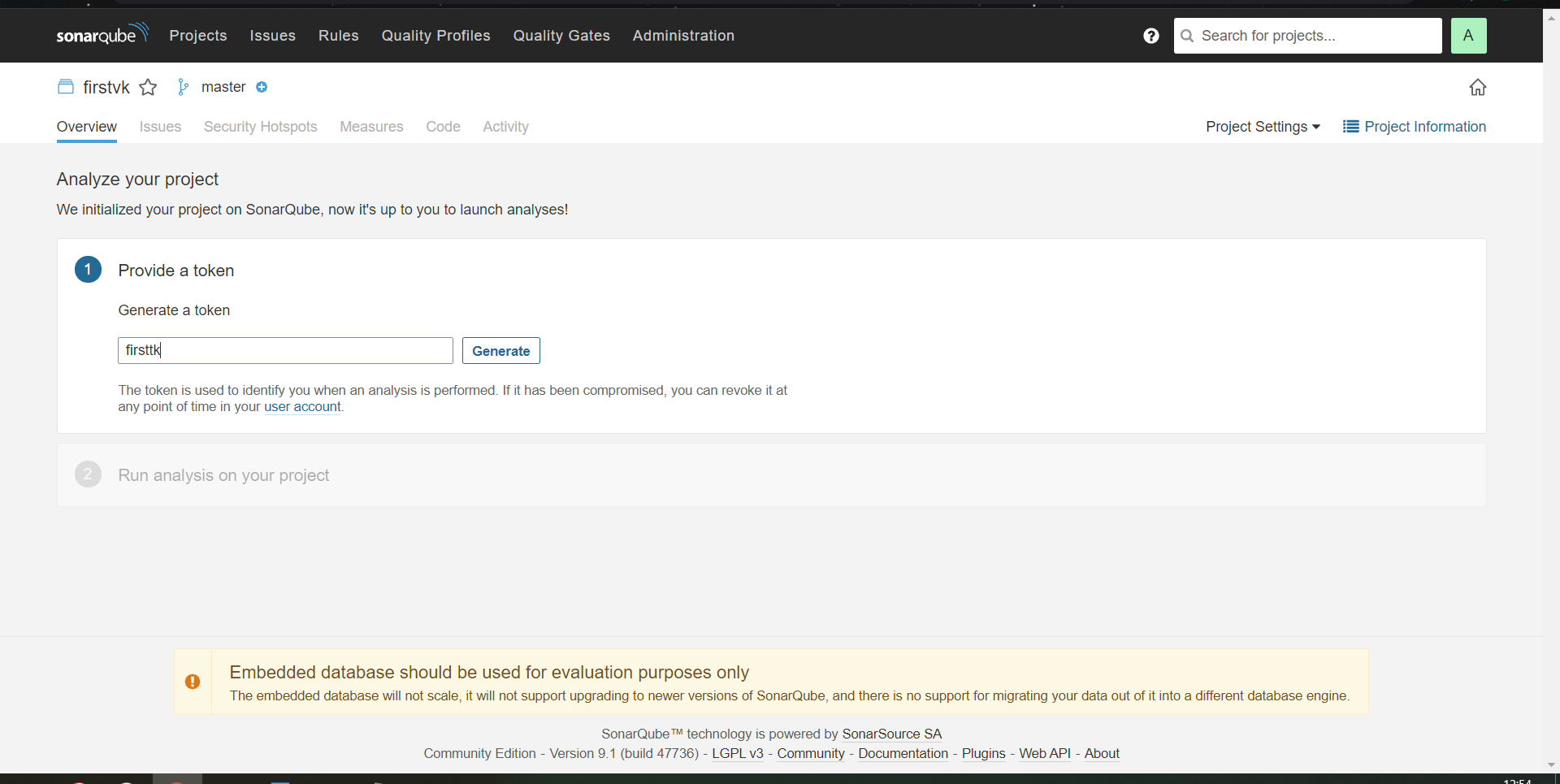
* Now we have to change some configurations files for sonar scanner before that in sonar scanner click on create project manually and give a name to the project**(firstvk)**



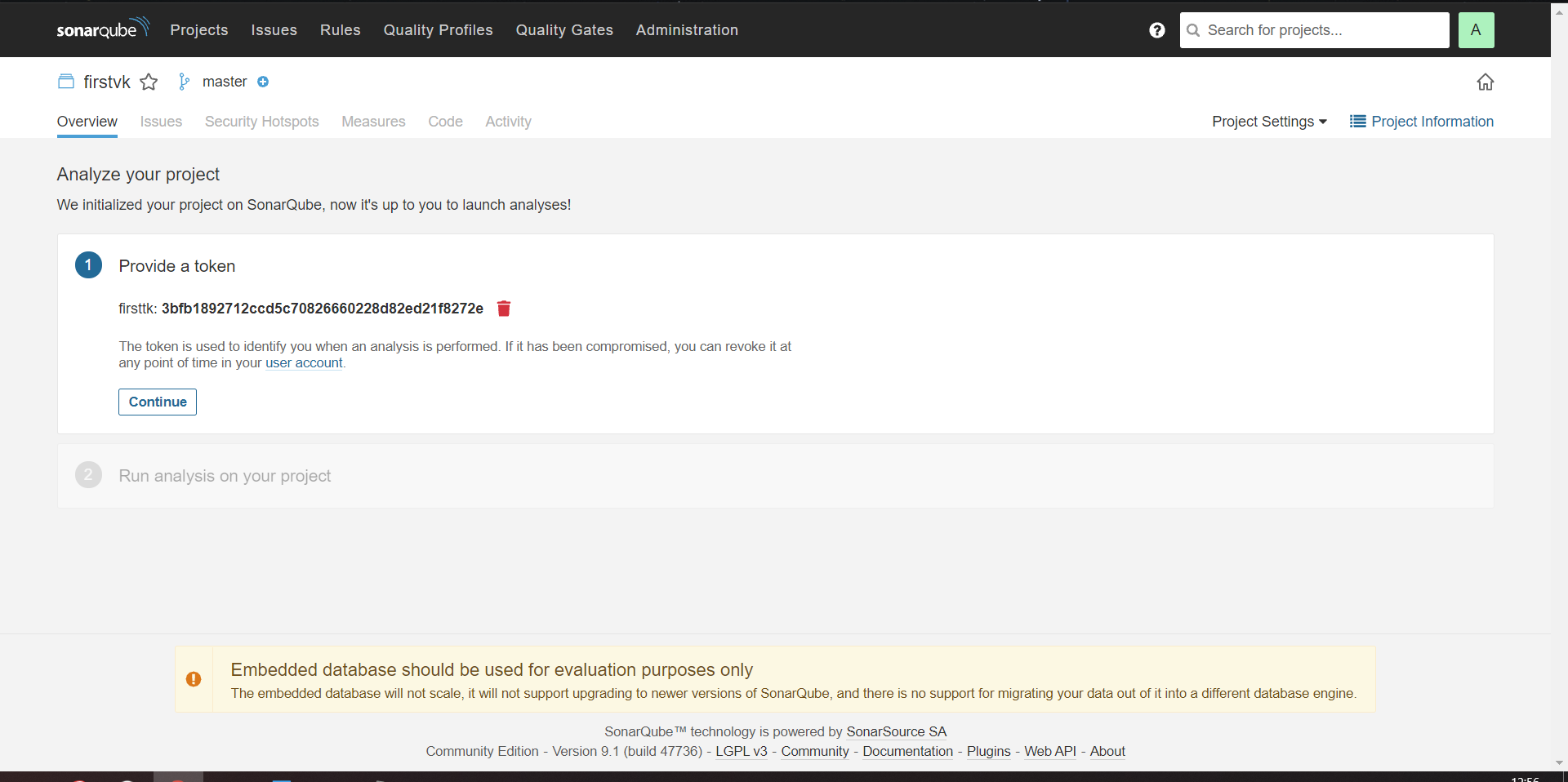
* After entering the name of project click on Set Up button and then click on Locally box on the screen



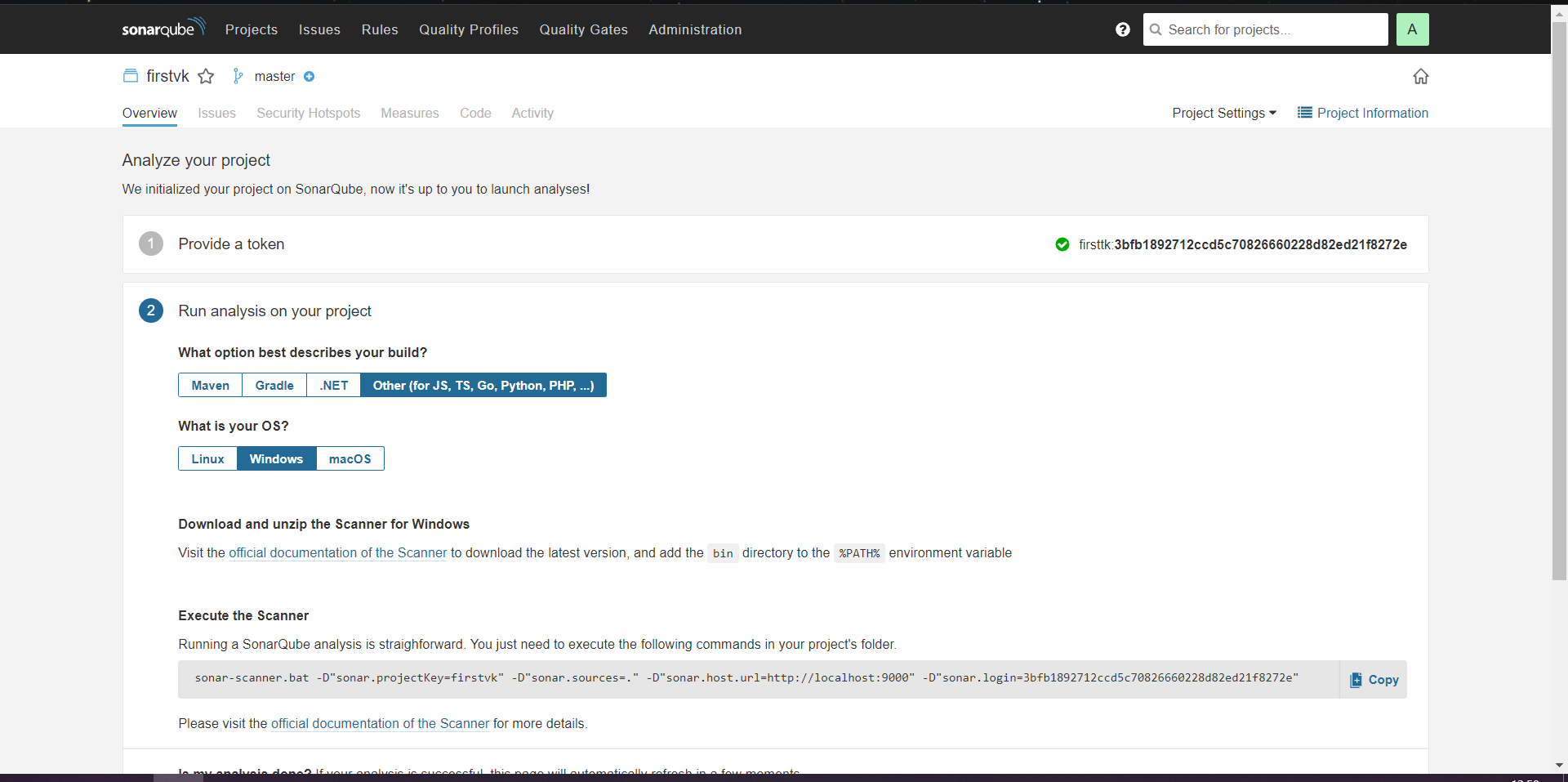
* Now it will ask to generate token, give a name**(firsttk)** for the token and then click on generate button.



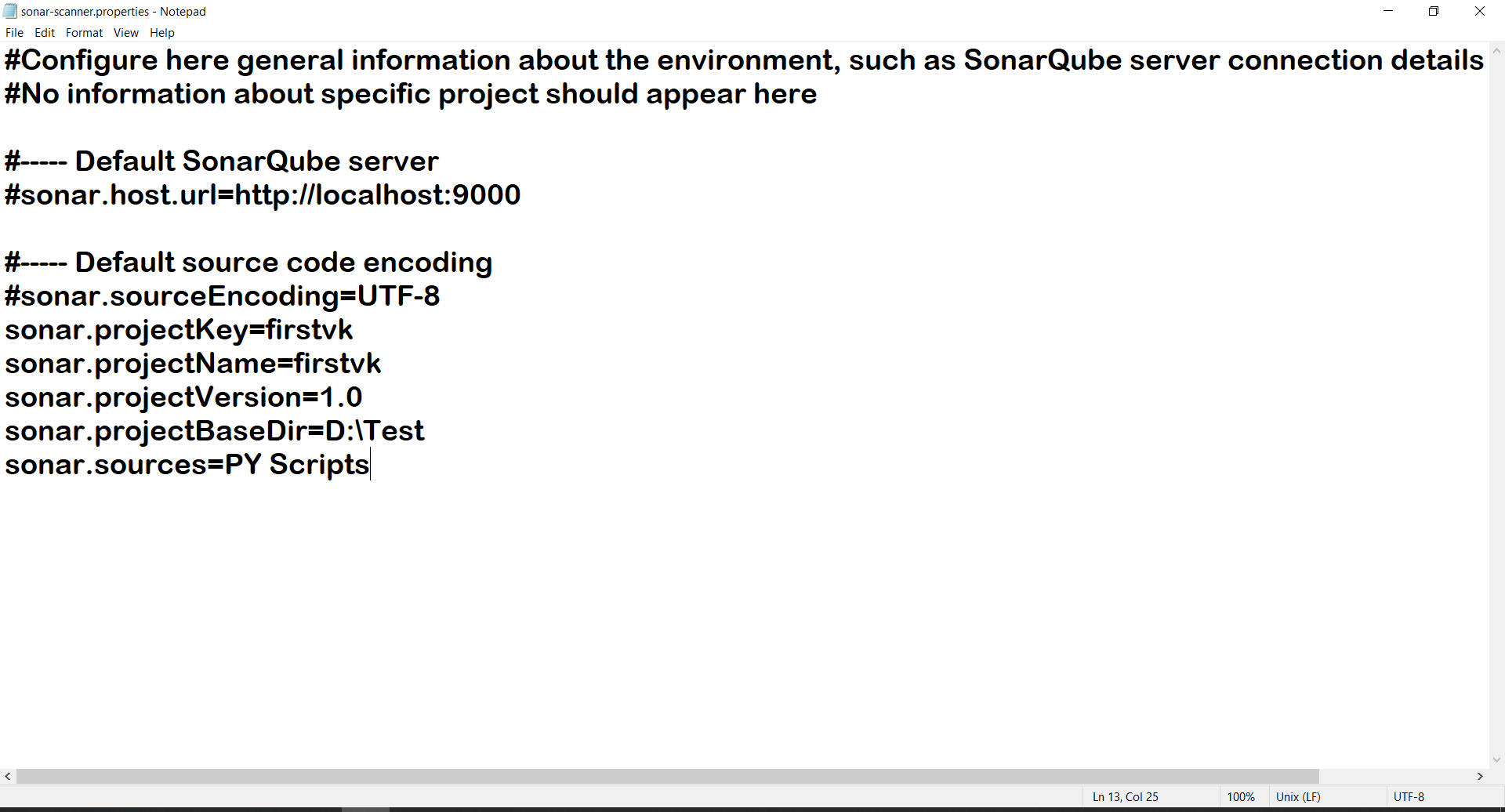
* Token will be generated (firsttk: **3bfb1892712ccd5c70826660228d82ed21f8272e**) then click on continue button



* After that select the type of program file which you created for testing and then select the operating system



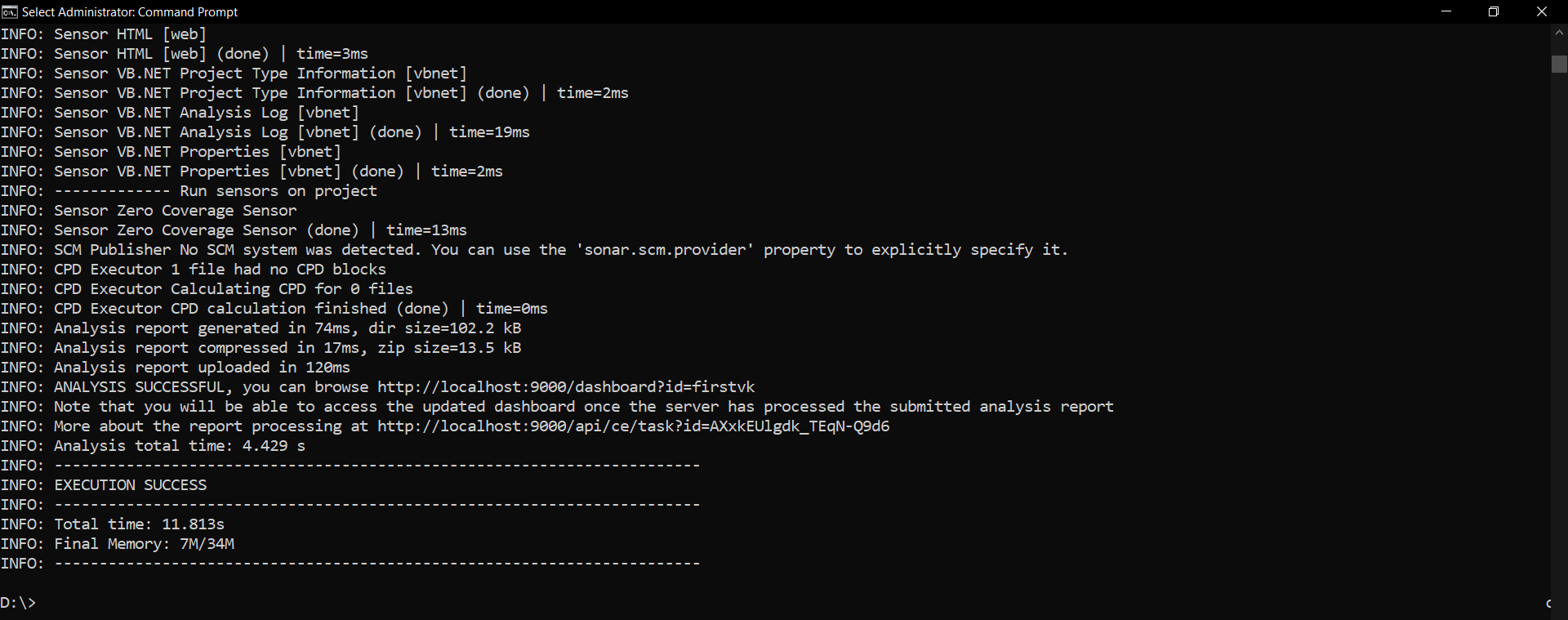
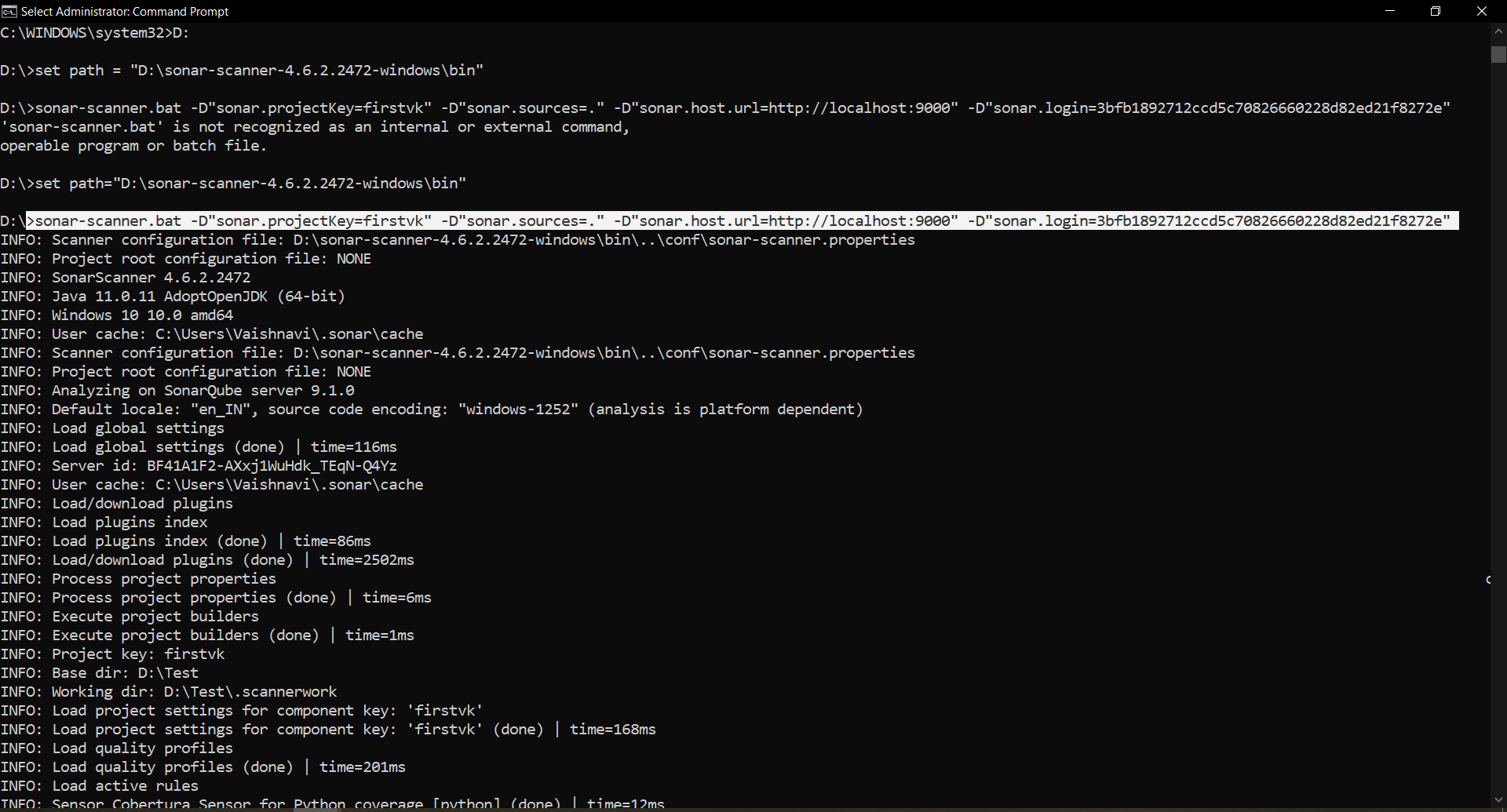
* After this enter the required details in **sonar-scanner. Properties** file



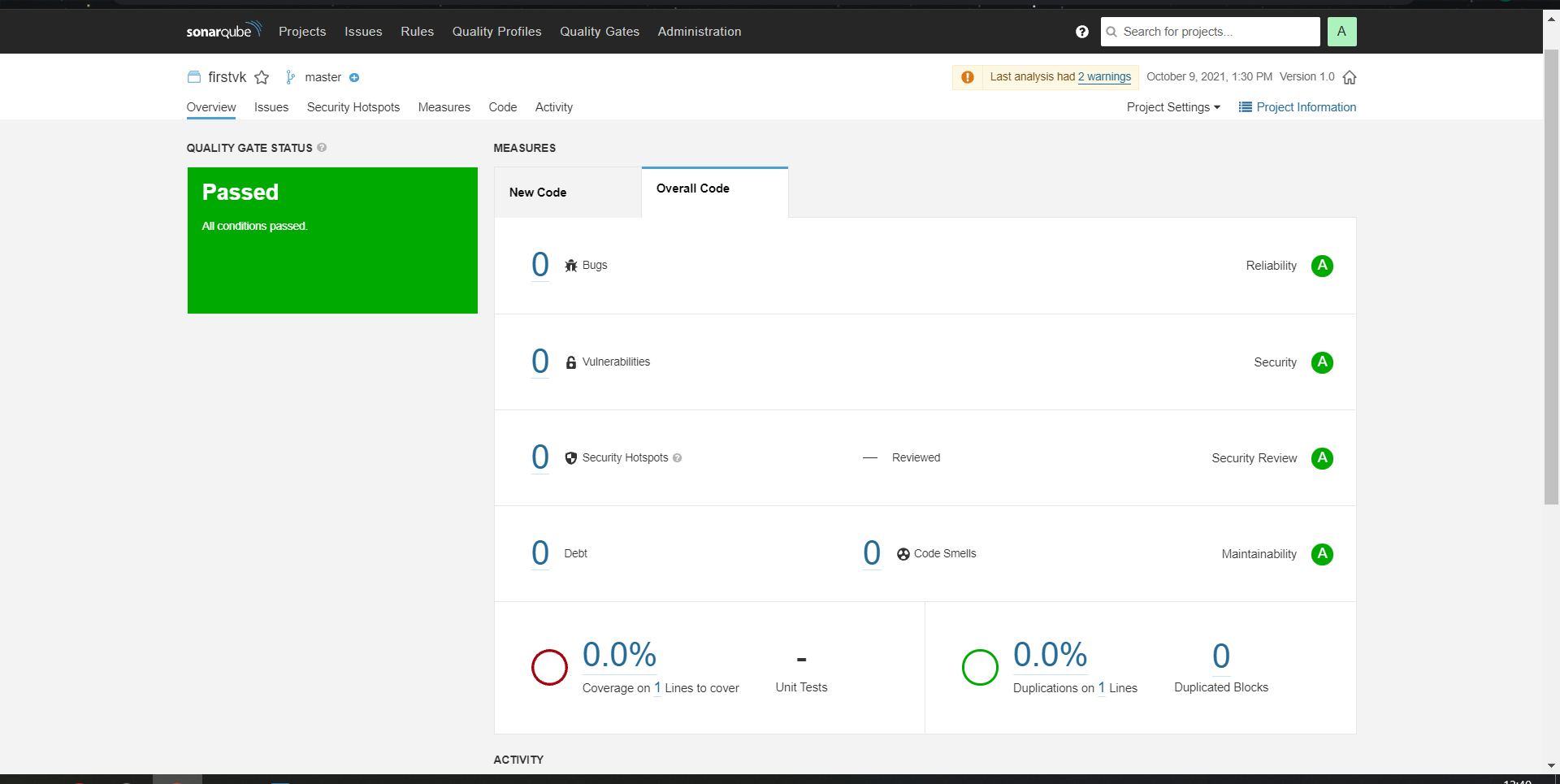
* After this step open command prompt and run it as administrator and type these commands in it to set the path🡪set the path of SonarQube bin folder

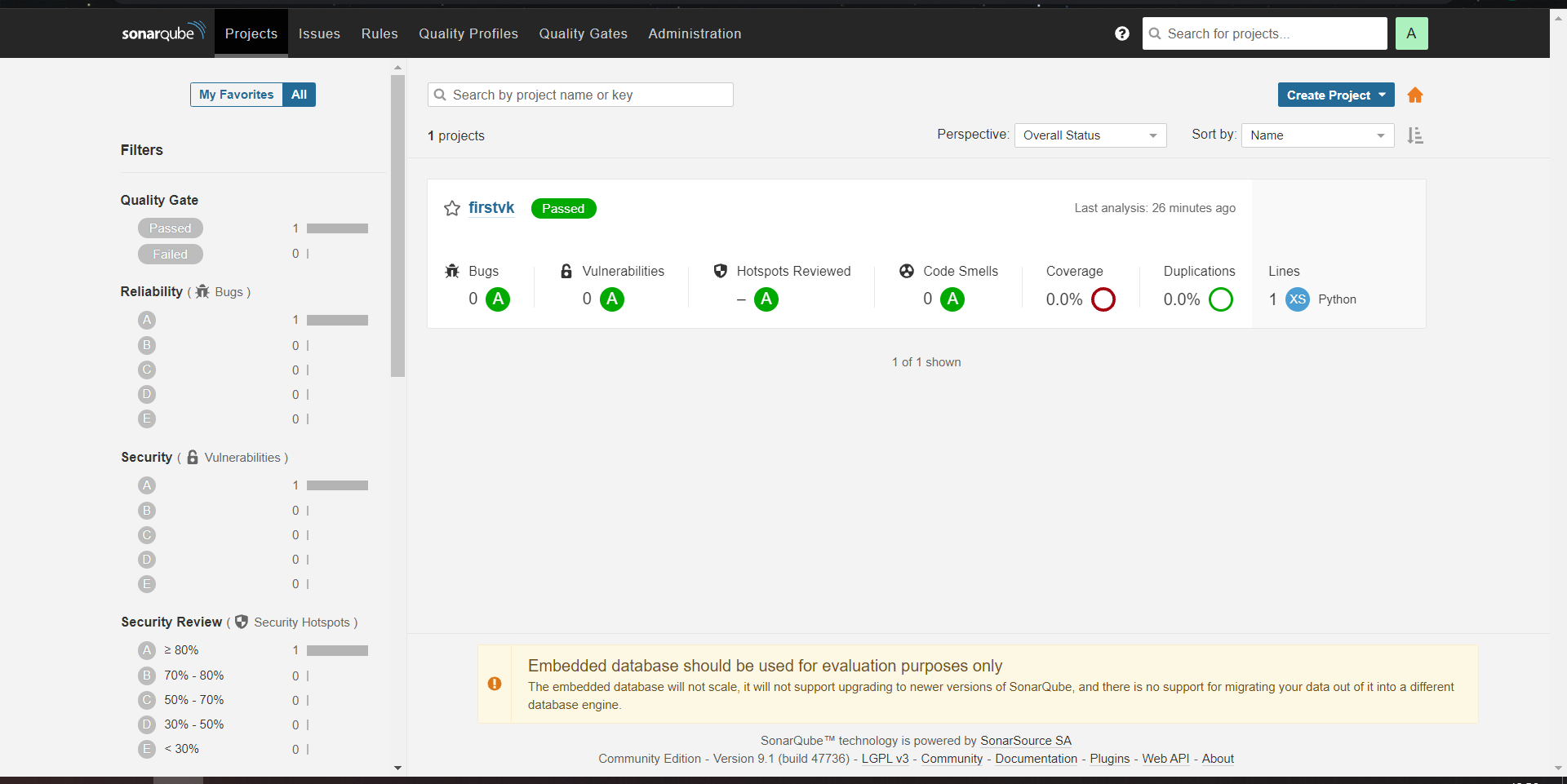


* Then copy the command of your project form SonarQube dashboard and paste it in command prompt after setting the path



* After execution of this path, you will now see the project got executed in SonarQube dashboard which will display bugs, Vulnerabilities and all the information related to the project as below





This will be the final output for the SonarQube project execution

**Conclusion:**

Successfully created a project on SonarQube platform which show the bugs Vulnerabilities and all the information related to the project.

**Lab Outcome: ITL504.4**  
To identify and remediate application vulnerabilities earlier and help integrate security in the development process using SAST Techniques.