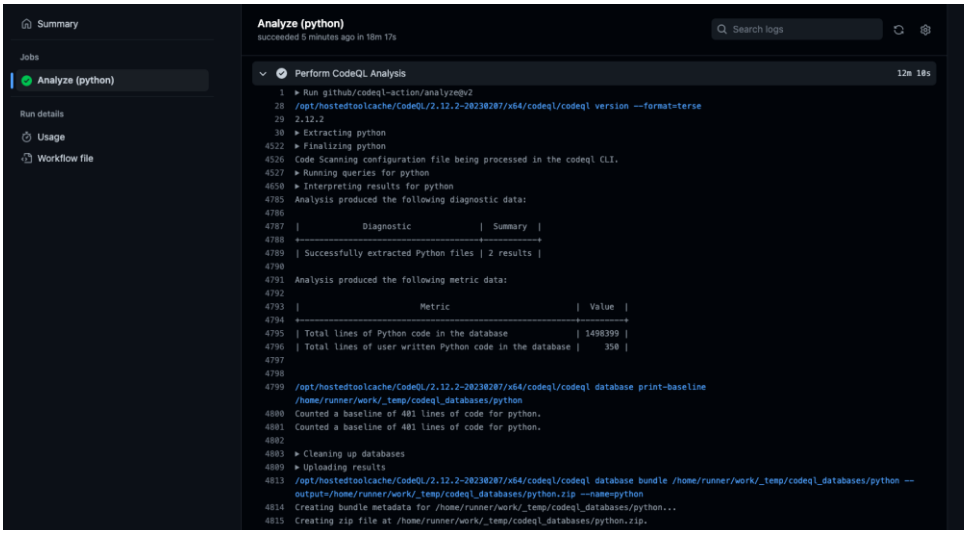
REPORT:

SAAD JAFAR (19I-1691)

MOIZ GOHAR (19I-1906)

AI-J

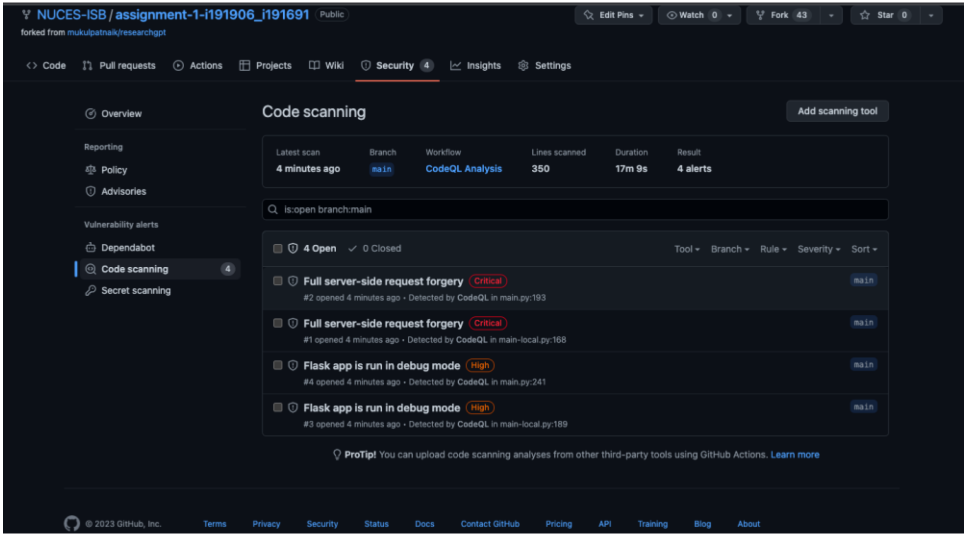
We conducted a codeql analysis for our repo. The codeql analysis for the Python codebase produced some valuable metric data, including a total of 1,498,399 lines of Python code in the database and 350 lines of user-written Python code. However, the analysis also uncovered some security alerts that require attention, including two instances of full server-side request forgery and two instances of Flask app being run in debug mode. These issues were identified as critical and high severity respectively and should be addressed promptly to ensure the security of the codebase.



Analyze (python)
succeeded 5 minutes ago in 18m 17s

Perform CodeQL Analysis 12m 10s

```
▶ Run github/codeql-action/analyze@v2
/opt/hostedtoolcache/CodeQL/2.12.2-20230207/x64/codeql/codeql version --format=terse
2.12.2
▶ Extracting python
▶ Finalizing python
Code Scanning configuration file being processed in the codeql CLI.
▶ Running queries for python
▶ Interpreting results for python
Analysis produced the following diagnostic data:

|            Diagnostic              |  Summary  |
+------------------------------------+-----------+
| Successfully extracted Python files | 2 results |

Analysis produced the following metric data:

|                         Metric                          |  Value  |
+---------------------------------------------------------+---------+
| Total lines of Python code in the database              | 1498399 |
| Total lines of user written Python code in the database |     350 |


/opt/hostedtoolcache/CodeQL/2.12.2-20230207/x64/codeql/codeql database print-baseline
/home/runner/work/_temp/codeql_databases/python
Counted a baseline of 401 lines of code for python.
Counted a baseline of 401 lines of code for python.

▶ Cleaning up databases
▶ Uploading results
/opt/hostedtoolcache/CodeQL/2.12.2-20230207/x64/codeql/codeql database bundle /home/runner/work/_temp/codeql_databases/python --
output=/home/runner/work/_temp/codeql_databases/python.zip --name=python
Creating bundle metadata for /home/runner/work/_temp/codeql_databases/python...
Creating zip file at /home/runner/work/_temp/codeql_databases/python.zip.
```



NUCES-ISB / assignment-1-i191906_i191691 Public
forked from mukulpatnaik/researchgpt

Code scanning

| Latest scan | Branch | Workflow | Lines scanned | Duration | Result |
|---|---|---|---|---|---|
| 4 minutes ago | main | CodeQL Analysis | 350 | 17m 9s | 4 alerts |

is:open branch:main

4 Open ✓ 0 Closed

□ Full server-side request forgery Critical main
#2 opened 4 minutes ago • Detected by CodeQL in main.py:193

□ Full server-side request forgery Critical main
#1 opened 4 minutes ago • Detected by CodeQL in main-local.py:168

□ Flask app is run in debug mode High main
#4 opened 4 minutes ago • Detected by CodeQL in main.py:241

□ Flask app is run in debug mode High main
#3 opened 4 minutes ago • Detected by CodeQL in main-local.py:189

ProTip! You can upload code scanning analyses from other third-party tools using GitHub Actions. Learn more