SAST

Code can be found here: https://github.com/c2003-tamu/413

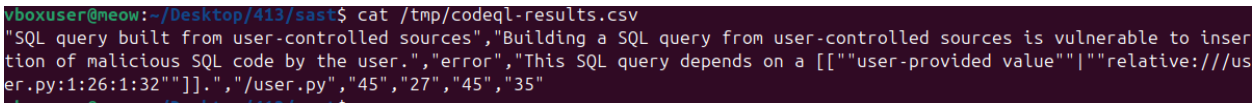
Environment Setup

- Clone git repository
- Ensure docker is installed on your machine
    - sudo apt install docker.io
- Navigate to 413/sast directory

Running Locally

NOTE: For this assignment, I decided to analyze my sql injection assignment code.

- Navigate to 413/sast directory
- Run command: docker build -t codeql-python .
- Run command: docker run –rm -it -v “$(pwd):/opt/src” -v “/tmp:/opt/results” codeql-python
- After above command finishes, run command: cat /tmp/codeql-results.csv, results should be as follows:



As seen above, locally running codeql correctly identified our SQL injection vulnerability.

Github Actions

My github actions run can be found here:
https://github.com/c2003-tamu/413/actions/runs/14181153212/job/39727335833

Needless to say, my github action failed :(

I ran CodeQL against my repository for all assignments for the class (specifically all python files), and it found quite a few vulnerabilities, as seen below:

```
at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-queries/Security/
CWE-079/ReflectedXss.bqrs.
  Interpreted pathproblem query "NoSQL Injection" (py/nosql-injection) at path /home/runner/wor
_temp/codeql_databases/python/results/codeql/python-queries/Security/CWE-943/NoSqlInjection.bqr
  Interpreted problem query "Incomplete URL substring sanitization" (py/incomplete-url-substrin
sanitization) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-
queries/Security/CWE-020/IncompleteUrlSubstringSanitization.bqrs.
  Interpreted pathproblem query "Construction of a cookie using user-supplied input" (py/cookie
injection) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-querie
Security/CWE-020/CookieInjection.bqrs.
  Interpreted problem query "Incomplete regular expression for hostnames" (py/incomplete-hostna
regexp) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-queries/
Security/CWE-020/IncompleteHostnameRegExp.bqrs.
  Interpreted problem query "Overly permissive regular expression range" (py/overly-large-range
at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-queries/Security/
CWE-020/OverlyLargeRange.bqrs.
  Interpreted pathproblem query "XPath query built from user-controlled sources" (py/xpath-
injection) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-querie
Security/CWE-643/XpathInjection.bqrs.
  Interpreted problem query "Flask app is run in debug mode" (py/flask-debug) at path /home/
runner/work/_temp/codeql_databases/python/results/codeql/python-queries/Security/CWE-215/
FlaskDebug.bqrs.
  Interpreted pathproblem query "LDAP query built from user-controlled sources" (py/ldap-
injection) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/python-querie
Security/CWE-090/LdapInjection.bqrs.
  Interpreted pathproblem query "Code injection" (py/code-injection) at path /home/runner/work/
_temp/codeql_databases/python/results/codeql/python-queries/Security/CWE-094/CodeInjection.bqrs
  Interpreted pathproblem query "URL redirection from remote source" (py/url-redirection) at pa
/home/runner/work/_temp/codeql_databases/python/results/codeql/python-queries/Security/CWE-601/
UrlRedirect.bqrs.
  Interpreted pathproblem query "Clear-text storage of sensitive information" (py/clear-text-
storage-sensitive-data) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/
python-queries/Security/CWE-312/CleartextStorage.bqrs.
  Interpreted pathproblem query "Clear-text logging of sensitive information" (py/clear-text-
logging-sensitive-data) at path /home/runner/work/_temp/codeql_databases/python/results/codeql/
python-queries/Security/CWE-312/CleartextLogging.bqrs.
  Interpreted problem query "Accepting unknown SSH host keys when using Paramiko" (py/paramiko-
missing-host-key-validation) at path /home/runner/work/_temp/codeql_databases/python/results/
codeql/python-queries/Security/CWE-295/MissingHostKeyValidation.bqrs.
```