Mark Smith, Jonathan Seibert, Shafqat Rana

Term Project

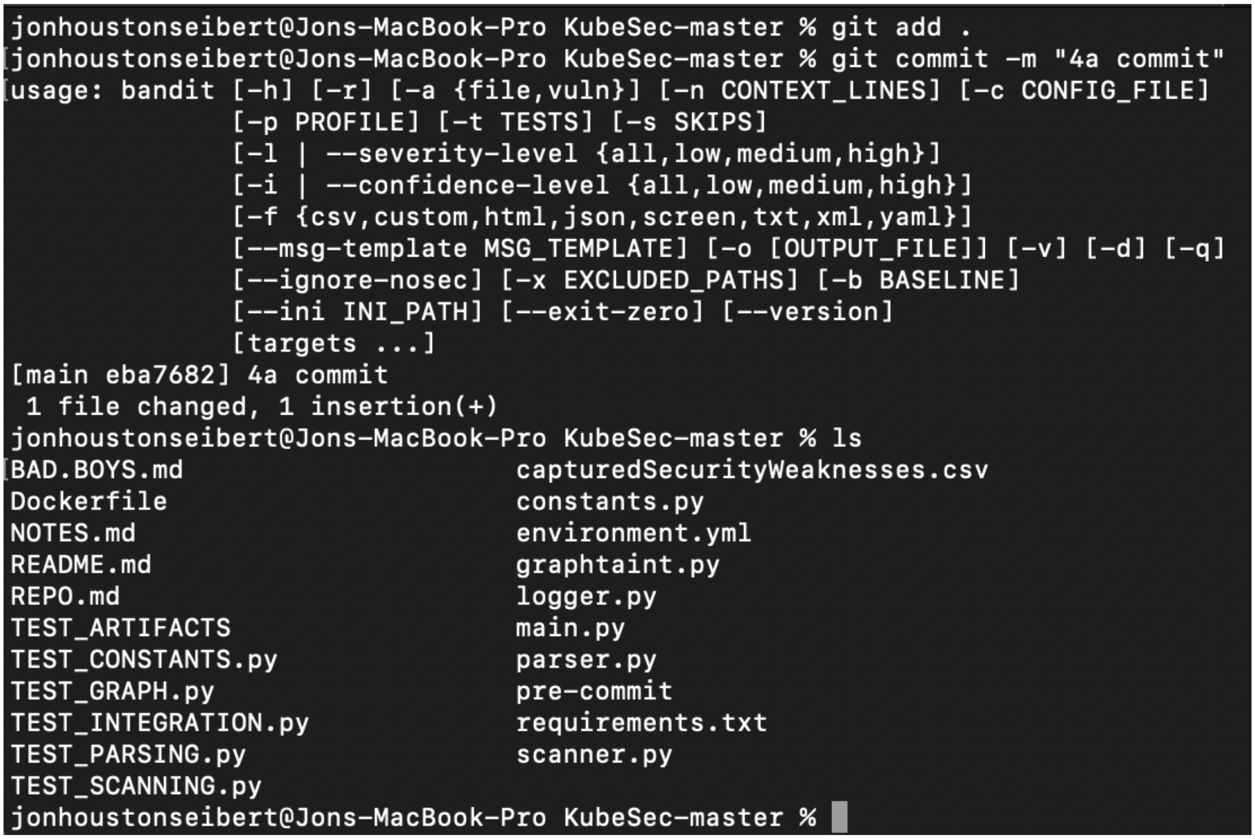
COMP 5710

Dec 1, 2023

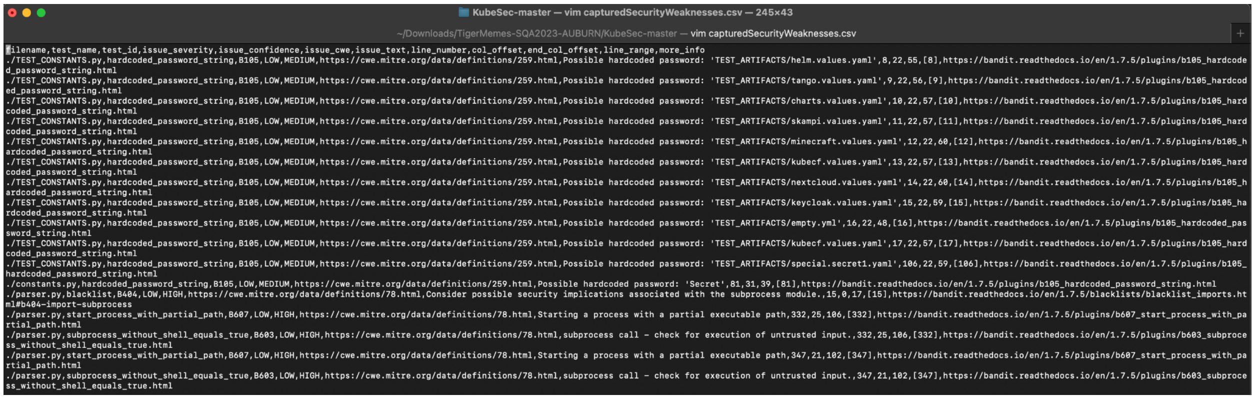
Part 4a git hooks — Jonathan Seibert

The task of this assignment was to create a Git Hook that will run and report all security weaknesses in the project in a CSV file whenever a Python file is changed and committed. By using the hooks directory in the .git folder, we can create a pre-commit hook from the provided pre-commit.sample file that runs before every commit. The file was modified to use the line bandit -r -f "csv" -o "capturedSecurityWeaknesses.csv" so that way all the bandit security weaknesses could be output when the script runs to the capturedSecurityWeaknesses.csv file. To use this feature, you can clone the repository, copy the pre-commit file to the .git/hooks directory, and make a commit or you can run it manually by going into the pre-commit file itself and run the script manually to just get the output file. I learned how to use bash scripts to automatically run bandit in a repo to report security vulnerabilities and tie it into the project to run when commits are made. This is a useful tool because it can warn a developer about their latest code changes before merging to master.

4a Screenshots of running git hook



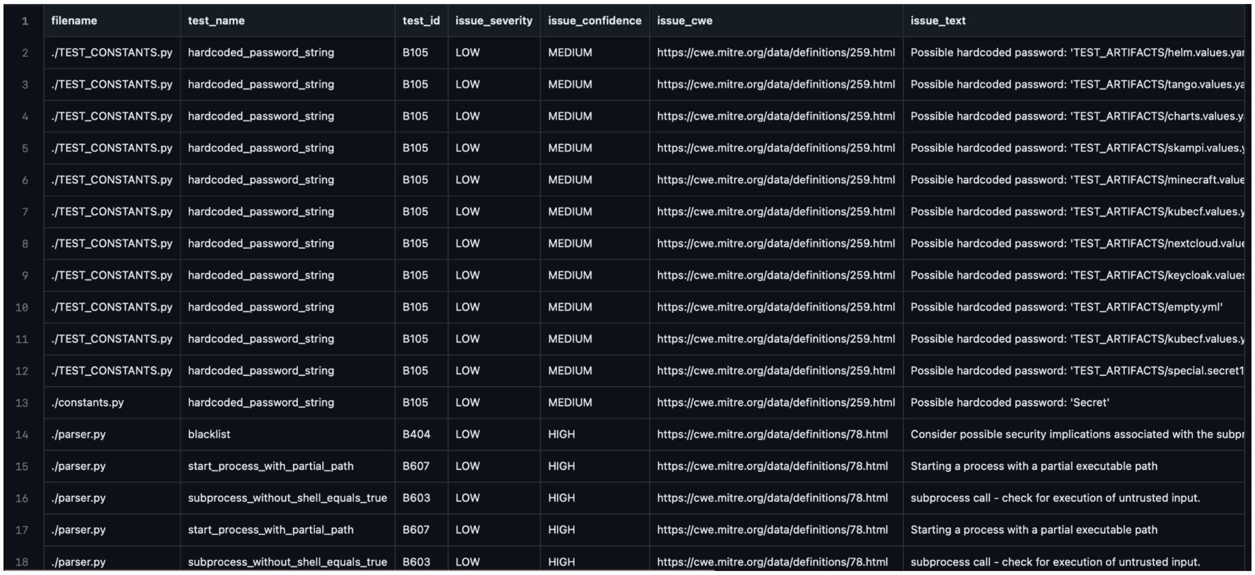
```
jonhoustonseibert@Jons-MacBook-Pro KubeSec-master % git add .
[jonhoustonseibert@Jons-MacBook-Pro KubeSec-master % git commit -m "4a commit"
[usage: bandit [-h] [-r] [-a {file,vuln}] [-n CONTEXT_LINES] [-c CONFIG_FILE]
              [-p PROFILE] [-t TESTS] [-s SKIPS]
              [-l | --severity-level {all,low,medium,high}]
              [-i | --confidence-level {all,low,medium,high}]
              [-f {csv,custom,html,json,screen,txt,xml,yaml}]
              [--msg-template MSG_TEMPLATE] [-o [OUTPUT_FILE]] [-v] [-d] [-q]
              [--ignore-nosec] [-x EXCLUDED_PATHS] [-b BASELINE]
              [--ini INI_PATH] [--exit-zero] [--version]
              [targets ...]
[main eba7682] 4a commit
 1 file changed, 1 insertion(+)
jonhoustonseibert@Jons-MacBook-Pro KubeSec-master % ls
[BAD.BOYS.md                     capturedSecurityWeaknesses.csv
Dockerfile                      constants.py
NOTES.md                        environment.yml
README.md                       graphtaint.py
REPO.md                         logger.py
TEST_ARTIFACTS                  main.py
TEST_CONSTANTS.py               parser.py
TEST_GRAPH.py                   pre-commit
TEST_INTEGRATION.py             requirements.txt
TEST_PARSING.py                 scanner.py
TEST_SCANNING.py
jonhoustonseibert@Jons-MacBook-Pro KubeSec-master %
```



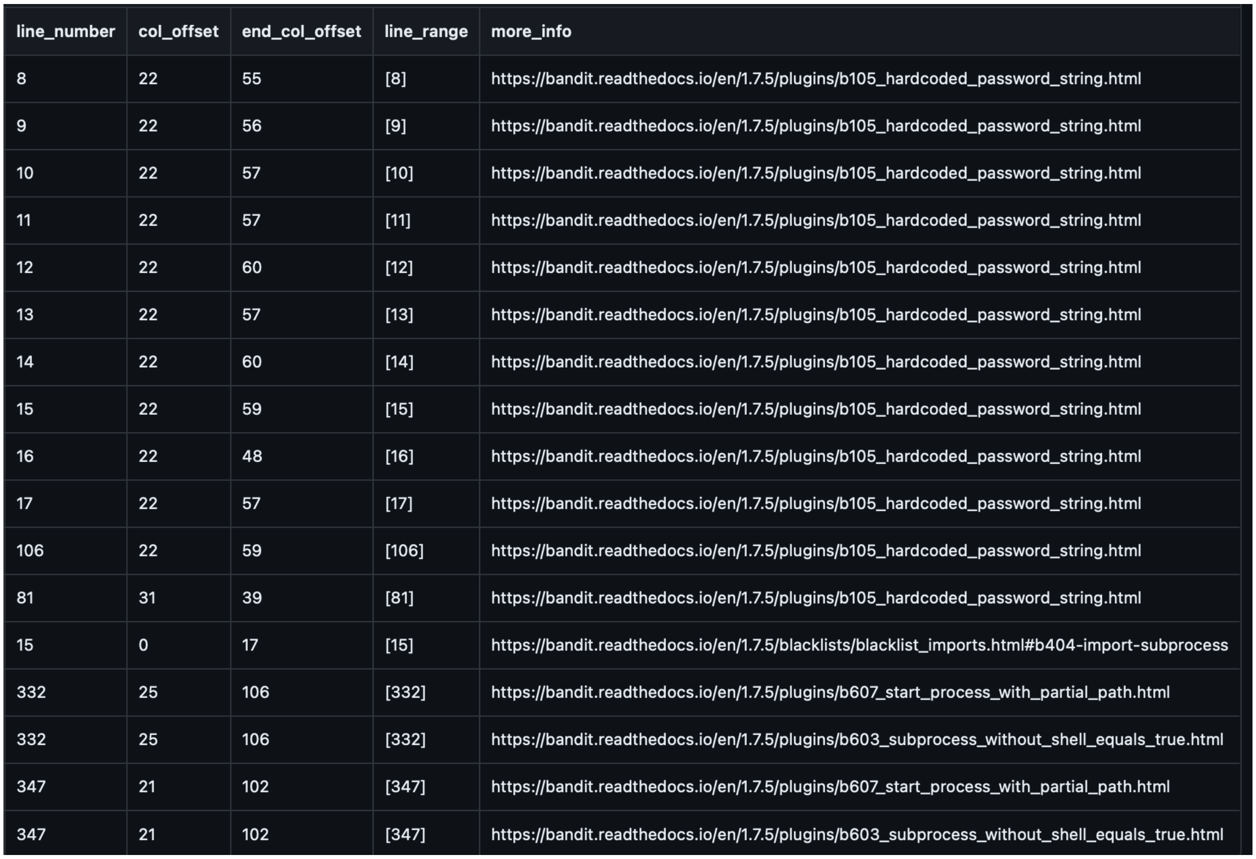
KubeSec-master — vim capturedSecurityWeaknesses.csv — 245×43
~/Downloads/TigerMemes-SQA2023-AUBURN/KubeSec-master — vim capturedSecurityWeaknesses.csv

```
filename,test_name,test_id,issue_severity,issue_confidence,issue_cwe,issue_text,line_number,col_offset,end_col_offset,line_range,more_info
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/helm.values.yaml',8,22,55,[8],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcode
d_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/tango.values.yaml',9,22,56,[9],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcod
ed_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/charts.values.yaml',10,22,57,[10],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hard
coded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/skampi.values.yaml',11,22,57,[11],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hard
coded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/minecraft.values.yaml',12,22,60,[12],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_h
ardcoded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/kubecf.values.yaml',13,22,57,[13],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hard
coded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/nextcloud.values.yaml',14,22,60,[14],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_h
ardcoded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/keycloak.values.yaml',15,22,59,[15],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_ha
rdcoded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/empty.yml',16,22,48,[16],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_pas
sword_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/kubecf.values.yaml',17,22,57,[17],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hard
coded_password_string.html
./TEST_CONSTANTS.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'TEST_ARTIFACTS/special.secret1.yaml',106,22,59,[106],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_
hardcoded_password_string.html
./constants.py,hardcoded_password_string,B105,LOW,MEDIUM,https://cwe.mitre.org/data/definitions/259.html,Possible hardcoded password: 'Secret',81,31,39,[81],https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
./parser.py,blacklist,B404,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,Consider possible security implications associated with the subprocess module.,15,0,17,[15],https://bandit.readthedocs.io/en/1.7.5/blacklists/blacklist_imports.ht
ml#b404-import-subprocess
./parser.py,start_process_with_partial_path,B607,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,Starting a process with a partial executable path,332,25,106,[332],https://bandit.readthedocs.io/en/1.7.5/plugins/b607_start_process_with_pa
rtial_path.html
./parser.py,subprocess_without_shell_equals_true,B603,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,subprocess call - check for execution of untrusted input.,332,25,106,[332],https://bandit.readthedocs.io/en/1.7.5/plugins/b603_subproce
ss_without_shell_equals_true.html
./parser.py,start_process_with_partial_path,B607,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,Starting a process with a partial executable path,347,21,102,[347],https://bandit.readthedocs.io/en/1.7.5/plugins/b607_start_process_with_pa
rtial_path.html
./parser.py,subprocess_without_shell_equals_true,B603,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,subprocess call - check for execution of untrusted input.,347,21,102,[347],https://bandit.readthedocs.io/en/1.7.5/plugins/b603_subproce
ss_without_shell_equals_true.html
```

4a CSV output



filename	test_name	test_id	issue_severity	issue_confidence	issue_cwe	issue_text
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/helm.values.yar
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/tango.values.ya
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/charts.values.y
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/skampi.values.y
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/minecraft.value
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/kubecf.values.y
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/nextcloud.value
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/keycloak.values
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/empty.yml'
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/kubecf.values.y
./TEST_CONSTANTS.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'TEST_ARTIFACTS/special.secret1
./constants.py	hardcoded_password_string	B105	LOW	MEDIUM	https://cwe.mitre.org/data/definitions/259.html	Possible hardcoded password: 'Secret'
./parser.py	blacklist	B404	LOW	HIGH	https://cwe.mitre.org/data/definitions/78.html	Consider possible security implications associated with the subpr
./parser.py	start_process_with_partial_path	B607	LOW	HIGH	https://cwe.mitre.org/data/definitions/78.html	Starting a process with a partial executable path
./parser.py	subprocess_without_shell_equals_true	B603	LOW	HIGH	https://cwe.mitre.org/data/definitions/78.html	subprocess call - check for execution of untrusted input.
./parser.py	start_process_with_partial_path	B607	LOW	HIGH	https://cwe.mitre.org/data/definitions/78.html	Starting a process with a partial executable path
./parser.py	subprocess_without_shell_equals_true	B603	LOW	HIGH	https://cwe.mitre.org/data/definitions/78.html	subprocess call - check for execution of untrusted input.



line_number	col_offset	end_col_offset	line_range	more_info
8	22	55	[8]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
9	22	56	[9]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
10	22	57	[10]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
11	22	57	[11]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
12	22	60	[12]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
13	22	57	[13]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
14	22	60	[14]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
15	22	59	[15]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
16	22	48	[16]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
17	22	57	[17]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
106	22	59	[106]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
81	31	39	[81]	https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
15	0	17	[15]	https://bandit.readthedocs.io/en/1.7.5/blacklists/blacklist_imports.html#b404-import-subprocess
332	25	106	[332]	https://bandit.readthedocs.io/en/1.7.5/plugins/b607_start_process_with_partial_path.html
332	25	106	[332]	https://bandit.readthedocs.io/en/1.7.5/plugins/b603_subprocess_without_shell_equals_true.html
347	21	102	[347]	https://bandit.readthedocs.io/en/1.7.5/plugins/b607_start_process_with_partial_path.html
347	21	102	[347]	https://bandit.readthedocs.io/en/1.7.5/plugins/b603_subprocess_without_shell_equals_true.html

Part 4b Fuzzing -- Shafqat Rana

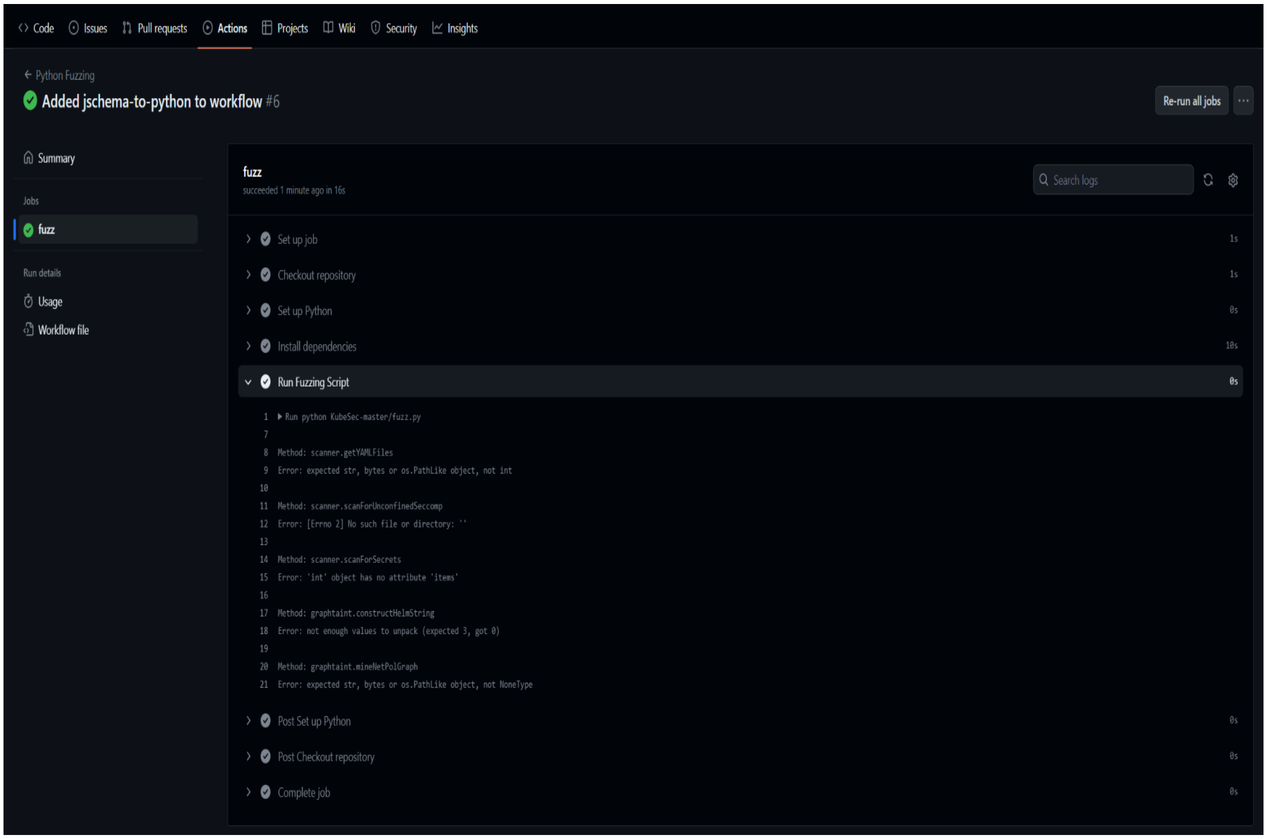
I created a fuzz.py file that has a FuzzFunctions method which is called in the main method of the fuzz.py file. The FuzzFunctions method calls five separate methods across two different files using inputs that should throw errors when calling them. The functions that I called with their inputs were:

- getYAMLFiles(1)
- scanForUnconfinedSeccomp('')
- getItemFromSecret(0, 0)
- constructHelmString({})
- mineNetPolGraph(None, None, None, None)

The errors varied from invalid types, No such file or directory, and not enough values to unpack. To get the Github Actions to be executed automatically, a .yml file was added within the .github/workflows directory that installed needed directories that would allow for the fuzz.py file to be run. Calling these methods with inputs that would test their boundaries allowed for testing of the code to check for any obvious downsides of the code and made me consider how to best implement error handling for these types of situations.

The link to the GitHub actions logs can be found here
https://pipelinesghubeus11.actions.githubusercontent.com/ZmKOYFLjEDc0jTM4iMeVsYXFPppcCCQoJFK6v1gnBK1M0vsmNC/_apis/pipelines/1/runs/13/signedlogcontent/2?urlExpires=2023-12-01T02%3A00%3A25.4941864Z&urlSigningMethod=HMACV1&urlSignature=4c9LHShcG37k2h6WxO8mNx7fjA9D9rcCDuo%2FtmsoCEI%3D

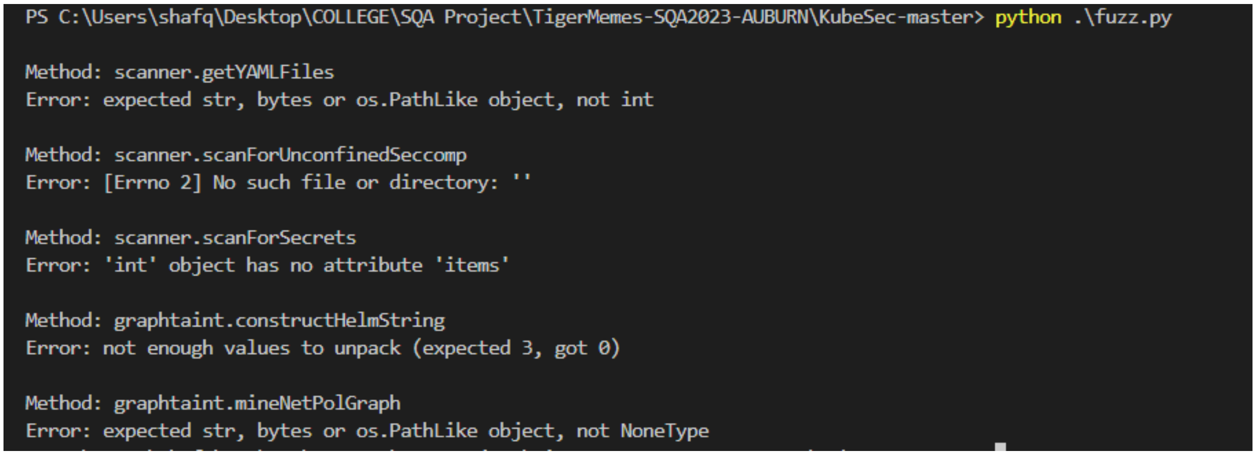
Screenshots of the file running in Github Actions and locally from my terminal.



Added jschema-to-python to workflow #6

fuzz
succeeded 1 minute ago in 16s

```
Set up job              1s
Checkout repository     1s
Set up Python           0s
Install dependencies    10s
Run Fuzzing Script      0s
▶ Run python KubeSec-master/fuzz.py

Method: scanner.getYAMLFiles
Error: expected str, bytes or os.PathLike object, not int

Method: scanner.scanForUnconfinedSeccomp
Error: [Errno 2] No such file or directory: ''

Method: scanner.scanForSecrets
Error: 'int' object has no attribute 'items'

Method: graphtaint.constructHelmString
Error: not enough values to unpack (expected 3, got 0)

Method: graphtaint.mineNetPolGraph
Error: expected str, bytes or os.PathLike object, not NoneType
Post Set up Python      0s
Post Checkout repository 0s
Complete job            0s
```



```
PS C:\Users\shafq\Desktop\COLLEGE\SQA Project\TigerMemes-SQA2023-AUBURN\KubeSec-master> python .\fuzz.py

Method: scanner.getYAMLFiles
Error: expected str, bytes or os.PathLike object, not int

Method: scanner.scanForUnconfinedSeccomp
Error: [Errno 2] No such file or directory: ''

Method: scanner.scanForSecrets
Error: 'int' object has no attribute 'items'

Method: graphtaint.constructHelmString
Error: not enough values to unpack (expected 3, got 0)

Method: graphtaint.mineNetPolGraph
Error: expected str, bytes or os.PathLike object, not NoneType
```

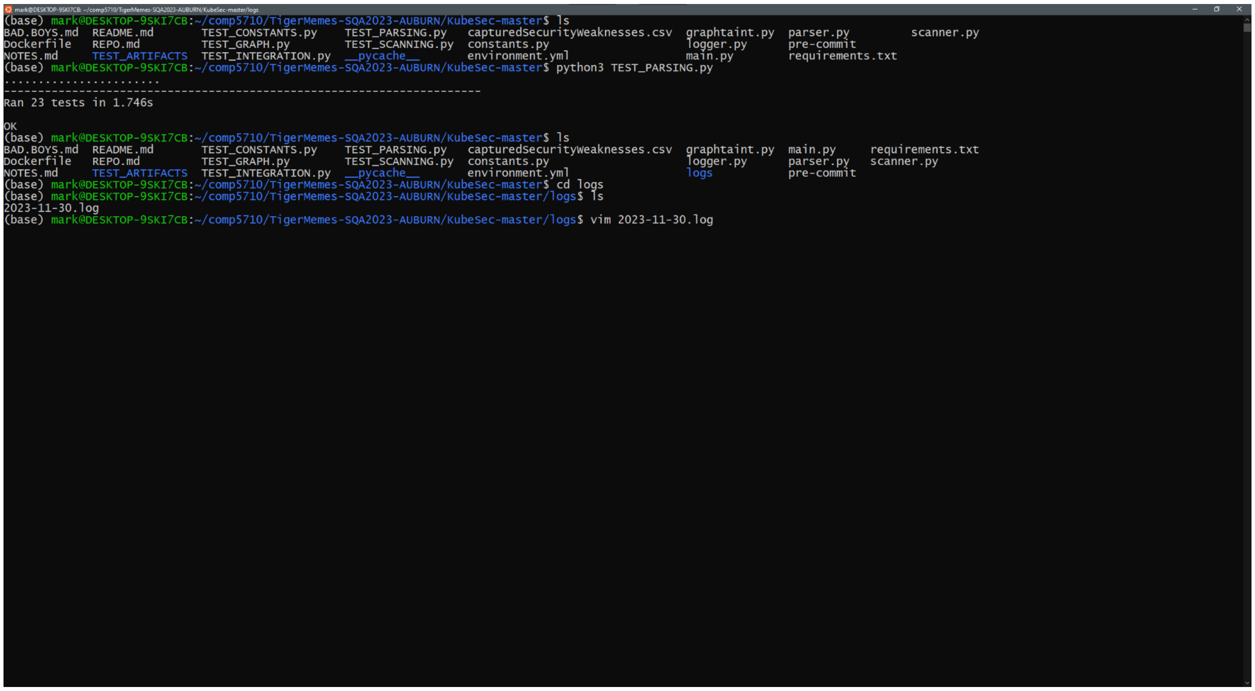
4c Forensics - Mark Smith

I created a simple logging class with a single function that returns a logger. The logger creates a new file for that day that will contain every log that occurs on that day. The log's themselves provide a timestamp, configurable message, and a log level when used. Added some test code in the file to make sure the logger is working. Added forensics to the following methods in the TestParsing class to test the log as well as provide info:

- testKeyExtraction
- testKeyPathLength
- testKeyPath1
- testKeyPath2
- testKeyCount

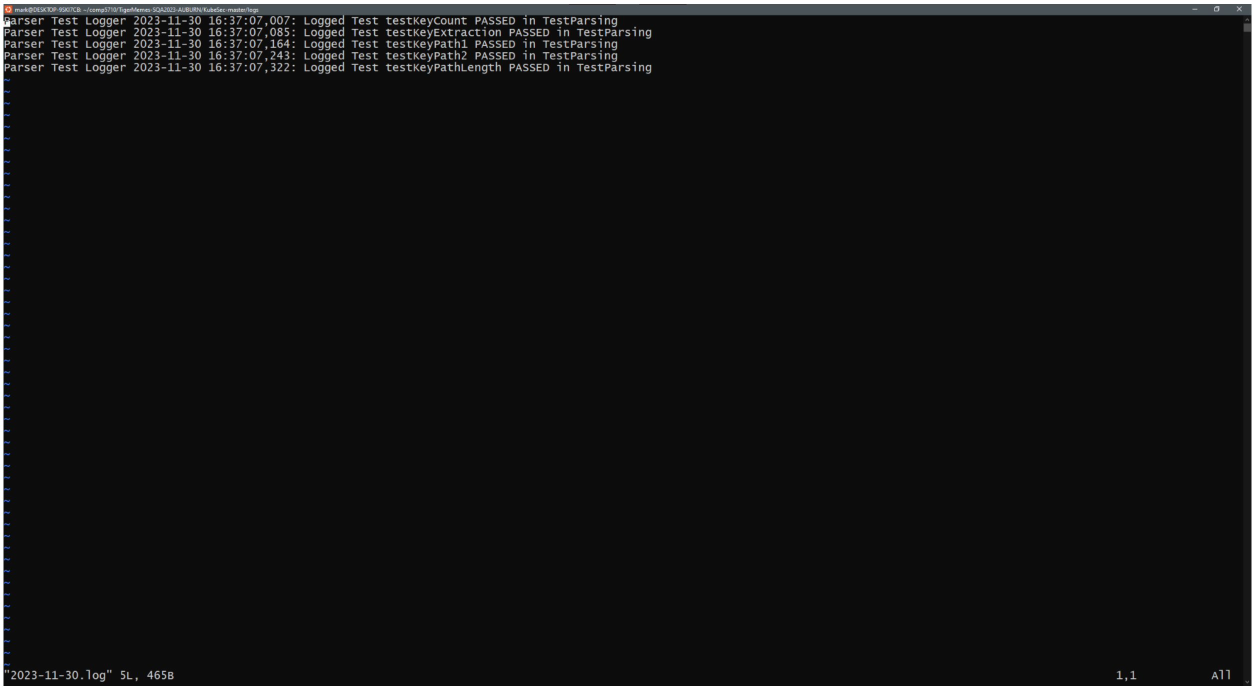
While this is only for a few methods of the whole repo, it outlines how the class I made could be used to log information that could be relevant after the fact when analyzing code. In the cases above it is just to log when testing occurs, but the message could be changed to fit any section of the code. This would be useful when going back over the code when a security issue occurred. Working on this example, it made me think about where I should place code that will be used for forensics. Additionally, it made me think about what kind of information I should include in a log. Specifically, what kind of level each log should be, the code's status, where it occurred etc. I also gained experience working with pythons logging class which I will be able to use for work I might do in the future that involves python.

Running the python file that has the logs as part of the methods. Log directory and log is created


mark@DESKTOP-9SKI7CB: ~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master/logs

```
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master$ ls
BAD.BOYS.md  README.md       TEST_CONSTANTS.py    TEST_PARSING.py   capturedSecurityWeaknesses.csv  graphtaint.py  parser.py         scanner.py
Dockerfile   REPO.md         TEST_GRAPH.py        TEST_SCANNING.py  constants.py                    logger.py      pre-commit
NOTES.md     TEST_ARTIFACTS  TEST_INTEGRATION.py  __pycache__       environment.yml                 main.py        requirements.txt
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master$ python3 TEST_PARSING.py
.......................
----------------------------------------------------------------------
Ran 23 tests in 1.746s

OK
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master$ ls
BAD.BOYS.md  README.md       TEST_CONSTANTS.py    TEST_PARSING.py   capturedSecurityWeaknesses.csv  graphtaint.py  main.py     requirements.txt
Dockerfile   REPO.md         TEST_GRAPH.py        TEST_SCANNING.py  constants.py                    logger.py      parser.py   scanner.py
NOTES.md     TEST_ARTIFACTS  TEST_INTEGRATION.py  __pycache__       environment.yml                 logs           pre-commit
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master$ cd logs
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master/logs$ ls
2023-11-30.log
(base) mark@DESKTOP-9SKI7CB:~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master/logs$ vim 2023-11-30.log
```

Checking the information in the log.



mark@DESKTOP-9SKI7CB: ~/comp5710/TigerMemes-SQA2023-AUBURN/KubeSec-master/logs

```
Parser Test Logger 2023-11-30 16:37:07,007: Logged Test testKeyCount PASSED in TestParsing
Parser Test Logger 2023-11-30 16:37:07,085: Logged Test testKeyExtraction PASSED in TestParsing
Parser Test Logger 2023-11-30 16:37:07,164: Logged Test testKeyPath1 PASSED in TestParsing
Parser Test Logger 2023-11-30 16:37:07,243: Logged Test testKeyPath2 PASSED in TestParsing
Parser Test Logger 2023-11-30 16:37:07,322: Logged Test testKeyPathLength PASSED in TestParsing
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"2023-11-30.log" 5L, 465B                                                                    1,1           All
```