

SCREENSHOTS OF WORK DONE

Activity 1 : Git Hooks

```
jabrewster@MSI: ~/JORTZ-FA × + v
jabrewster@MSI:~$ cd JORTZ-FALL2024-SQA/.git/hooks/
jabrewster@MSI:~/JORTZ-FALL2024-SQA/.git/hooks$ ls -al
total 80
drwxr-xr-x 2 jabrewster jabrewster 4096 Dec  3 21:29 .
drwxr-xr-x 8 jabrewster jabrewster 4096 Nov 29 15:43 ..
-rw-r--r-- 1 jabrewster jabrewster 192 Nov 29 11:49 .pre-commit-config.yaml
-rwxr-xr-x 1 jabrewster jabrewster 478 Nov 13 13:46 applypatch-msg.sample
-rwxr-xr-x 1 jabrewster jabrewster 896 Nov 13 13:46 commit-msg.sample
-rwxr-xr-x 1 jabrewster jabrewster 4655 Nov 13 13:46 fsmonitor-watchman.sample
-rwxr-xr-x 1 jabrewster jabrewster 189 Nov 13 13:46 post-update.sample
-rwxr-xr-x 1 jabrewster jabrewster 424 Nov 13 13:46 pre-applypatch.sample
-rwxr-xr-x 1 jabrewster jabrewster 621 Nov 29 11:50 pre-commit
-rwxr-xr-x 1 jabrewster jabrewster 1664 Nov 29 11:35 pre-commit.legacy
-rwxr-xr-x 1 jabrewster jabrewster 1643 Nov 29 15:11 pre-commit.sample
-rwxr-xr-x 1 jabrewster jabrewster 416 Nov 13 13:46 pre-merge-commit.sample
-rwxr-xr-x 1 jabrewster jabrewster 1374 Nov 13 13:46 pre-push.sample
-rwxr-xr-x 1 jabrewster jabrewster 4898 Nov 13 13:46 pre-rebase.sample
-rwxr-xr-x 1 jabrewster jabrewster 544 Nov 13 13:46 pre-receive.sample
-rwxr-xr-x 1 jabrewster jabrewster 1492 Nov 13 13:46 prepare-commit-msg.sample
-rwxr-xr-x 1 jabrewster jabrewster 2783 Nov 13 13:46 push-to-checkout.sample
-rwxr-xr-x 1 jabrewster jabrewster 3650 Nov 13 13:46 update.sample
jabrewster@MSI:~/JORTZ-FALL2024-SQA/.git/hooks$ |
```

Made the files, pre-commit, .pre-commit-config.yaml

```
jabrewster@MSI: ~/JORTZ-FA × + v
- repo: https://github.com/Reid-Roberts/JORTZ-FALL2024-SQA.git
  rev: v1.0.5
  hooks:
    - id: python-bandit-vulnerability-check
      args: [--skip, "B101", --recursive, clumper]
```

Code in .pre-commit-config.yaml so bandit knows what repo to look at and what file type to look for

```
#!/bin/sh
bandit -r |.
```

Added code it the pre-commit file so bandit checks the entire repo


```

[main] INFO     profile include tests: None
[main] INFO     profile exclude tests: None
[main] INFO     cli include tests: None
[main] INFO     cli exclude tests: None
[main] INFO     running on Python 3.10.9
Run started:2024-12-04 15:27:19.520020

Test results:
>> Issue: [B404:blacklist] Consider possible security implications associated with the subprocess module.
Severity: Low   Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist\_imports.html#b404-import-subprocess
Location: ./MLForensics-farzana/empirical/dataset.stats.py:12:0
11     from datetime import datetime
12     import subprocess
13     from collections import Counter

-----
>> Issue: [B607:start_process_with_partial_path] Starting a process with a partial executable path
Severity: Low   Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b607\_start\_process\_with\_partial\_path.html
Location: ./MLForensics-farzana/empirical/dataset.stats.py:59:24
58
59     author_emails = str(subprocess.check_output(['bash', '-c', command2Run]))
60     author_emails = author_emails.split('\n')

-----
>> Issue: [B603:subprocess_without_shell_equals_true] subprocess call - check for execution of untrusted input.
Severity: Low   Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b603\_subprocess\_without\_shell\_equals\_true.html
Location: ./MLForensics-farzana/empirical/dataset.stats.py:59:24
58
59     author_emails = str(subprocess.check_output(['bash', '-c', command2Run]))
60     author_emails = author_emails.split('\n')

-----
>> Issue: [B404:blacklist] Consider possible security implications associated with the subprocess module.
Severity: Low   Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist\_imports.html#b404-import-subprocess
Location: ./MLForensics-farzana/mining/git.repo.miner.py:10:0
9         import csv
10         import subprocess
11         import numpy as np

-----
>> Issue: [B408:blacklist] Using minidom to parse untrusted XML data is known to be vulnerable to XML attacks. Replace minidom with lxml. minidom.b() is called.
Severity: Low   Confidence: High
CWE: CWE-20 (https://cwe.mitre.org/data/definitions/20.html)
More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist\_imports.html#b408-import-xml-minidom
Location: ./MLForensics-farzana/mining/git.repo.miner.py:15:0
14     from git import exc

```

Static testing output when committing

Activity 2 : fuzzing

```

def generateRandomFileName(Length=10):
    # Generates a random name for a file
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(Length)) + '.py'

```

Method used in fuzzing to generate random file names

```

FileNotFoundError: [Errno 2] No such file or directory: 'JRoUMorL2P.py'
PS C:\Users\Zamarian\OneDrive\Desktop\COMP5710\MLForensics\MLForensics-farzana\FAME-ML>

```

One error given when fuzzing

```

> python3 lint_engine.py
Traceback (most recent call last):
  File "/Users/reidroberts/JORTZ-FALL2024-SQA/MLForensics-farzana/FAME-ML/lint_engine.py", line 839, in <module>
    simpleFuzzer()
  File "/Users/reidroberts/JORTZ-FALL2024-SQA/MLForensics-farzana/FAME-ML/lint_engine.py", line 834, in simpleFuzzer
    result = fuzzing(py_file)
  File "/Users/reidroberts/JORTZ-FALL2024-SQA/MLForensics-farzana/FAME-ML/lint_engine.py", line 824, in fuzzing
    res1 = getDataLoadCount(name)
  File "/Users/reidroberts/JORTZ-FALL2024-SQA/MLForensics-farzana/FAME-ML/lint_engine.py", line 23, in getDataLoadCount
    py_tree = py_parser.getPythonParseObject(py_file)
  File "/Users/reidroberts/JORTZ-FALL2024-SQA/MLForensics-farzana/FAME-ML/py_parser.py", line 82, in getPythonParseObject
    full_tree = ast.parse( open( pyFile ).read())
FileNotFoundError: [Errno 2] No such file or directory: 'cuVACCsBsP.py'

```

Output when fuzzing that reveals vulnerability in source code:

```

def fuzzing(name):
    res1 = getDataLoadCount(name)
    res2 = getDataLoadCountb(name)
    res3 = getDataLoadCountc(name)
    res4 = getModelLoadCounta(name)
    res5 = getModelLoadCountb(name)
    return res1, res2, res3, res4, res5

def simpleFuzzer(tests=10):
    for _ in range(tests):
        py_file = generateRandomFileName()
        result = fuzzing(py_file)

```

Methods fuzzed, and tested a given amount of times (10)

Activity 3 : Forensics

```

## same logger from in class workshop to be now implemented in project

import logging

def giveMeLoggingObject():
    format_str = '%(asctime)s: %(message)s'
    file_name = 'PROJECT-LOGGER.log'
    logging.basicConfig(format=format_str, filename=file_name, level=logging.INFO)
    loggerObj = logging.getLogger('simple-logger')
    return loggerObj

```

projectLogger.py added to be able to create logging objects

```

18  def getDataLoadCount( py_file ):
19      logobj = projectLogger.giveMeLoggingObject ()
20      logobj.info("First Data Load Counter Method Activated")
21      data_load_count = 0
22      logobj.info("The data load count is initialized to {}".format(data_load_count))
23      py_tree = py_parser.getPythonParseObject(py_file)
24      func_def_list = py_parser.getPythonAttributeFuncs( py_tree )
25

```

Example of lint engine modification

 PROJECT-LOGGER.log

Project logger file created when lint_engine is ran

```

1      2024-12-04 09:42:35,023:First Data Load Counter Method Activated
2      2024-12-04 09:42:35,023:The data load count is initialized to 0
3      2024-12-04 10:05:36,988:First Data Load Counter Method Activated
4      2024-12-04 10:05:36,989:The data load count is initialized to 0

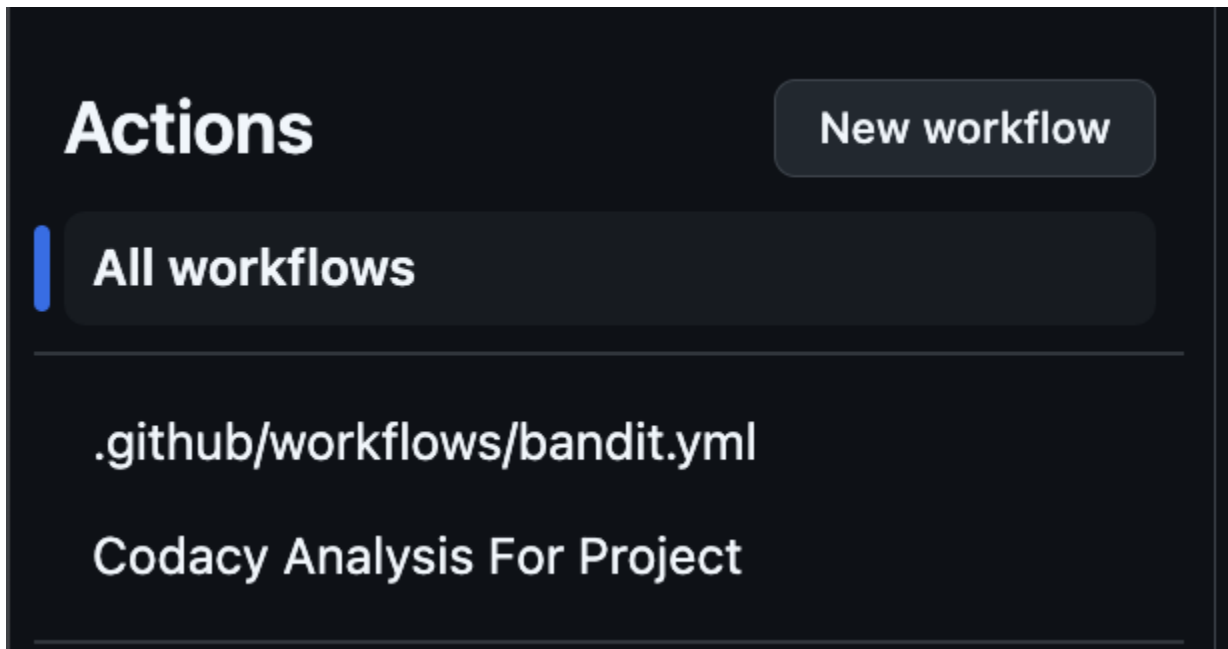
```

Outputs to the logger file that show the code encounters an error when logging (the error is revealed by the fuzzing displayed previously)


































Activity 4 : CI

```
1  name: Codacy Analysis For Project
2
3  on: ["push"]
4
5  jobs:
6    codacy-analysis-cli:
7      name: Codacy Analysis CLI
8      runs-on: ubuntu-latest
9      steps:
10       - name: Checkout code
11         uses: actions/checkout@main
12
13       - name: Run Codacy Analysis CLI
14         uses: codacy/codacy-analysis-cli-action@master
```

Codacy-analysis.yaml file added



New action present

 Update lint_engine.py Codacy Analysis For Project #10: Commit 254264c pushed by Reid-Roberts	main	 33 minutes ago  3m 6s	...
 Update lint_engine.py .github/workflows/bandit.yml #15: Commit 254264c pushed by Reid-Roberts	main	 33 minutes ago  Failure	...
 Update lint_engine.py Codacy Analysis For Project #9: Commit 57147a5 pushed by Reid-Roberts	main	 38 minutes ago  3m 45s	...
 Update lint_engine.py .github/workflows/bandit.yml #14: Commit 57147a5 pushed by Reid-Roberts	main	 38 minutes ago  Failure	...
 Update lint_engine.py Codacy Analysis For Project #8: Commit 0823019 pushed by Reid-Roberts	main	 40 minutes ago  3m 58s	...
 Update lint_engine.py .github/workflows/bandit.yml #13: Commit 0823019 pushed by Reid-Roberts	main	 40 minutes ago  Failure	...
 Update lint_engine.py Codacy Analysis For Project #7: Commit 0d0f5c7 pushed by Reid-Roberts	main	 18 hours ago  3m 3s	...
 Update lint_engine.py .github/workflows/bandit.yml #12: Commit 0d0f5c7 pushed by Reid-Roberts	main	 18 hours ago  Failure	...
 minor changes Codacy Analysis For Project #6: Commit 81eb849 pushed by Reid-Roberts	main	 5 days ago  3m 20s	...
 minor changes .github/workflows/bandit.yml #11: Commit 81eb849 pushed by Reid-Roberts	main	 5 days ago  Failure	...
 minor changes Codacy Analysis For Project #5: Commit b7fe708 pushed by Reid-Roberts	main	 5 days ago  4m 35s	...

A list of the different commits made available by the Codacy CI integrations