BigSwag Project Report

Brenden Rice, John Mulligan, Moe Salaam

1. Git Hooks

A pre-commit hook was added that would run bandit on the repo and print the results in an output.csv. Because the .git directory isn’t tracked it is explained that you need to add the pre-commit file to the .git/hooks directory for it to run. This saves a output.csv file in the root directory, something I realized that caused some issues with being able to push changes. After an output.csv is made it needs to be moved from the folder before you can do a new commit, otherwise the commit gets blocked. Here is an example of the output.csv:

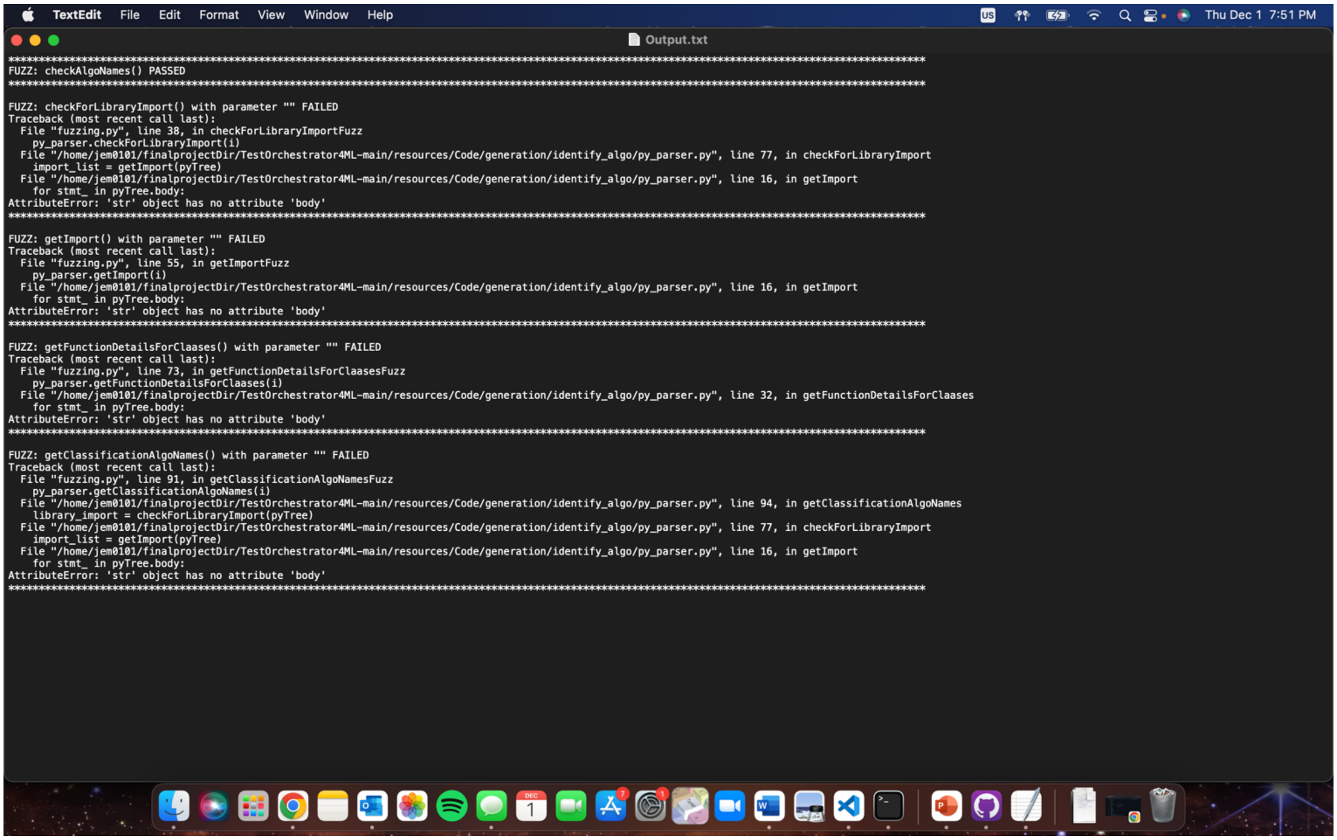
```
filename,test_name,test_id,issue_severity,issue_confidence,issue_cwe,issue_text,line_number,col_offset,line_range,more_info
../BigSwag-SQA2022-AUBURN/TestOrchestrator4ML/TestOrchestrator4ML-main/generation/probability_based_label_perturbation.py,blacklist,B311,LOW,HIGH,https://cwe.mitre.org/data/definitions/330.html,Standard pseudo-random generators are not suitable for security/cryptographic purposes.,28,40,[28],https://bandit.readthedocs.io/en/1.7.4/blacklists/blacklist_calls.html#b311-random
../BigSwag-SQA2022-AUBURN/TestOrchestrator4ML/TestOrchestrator4ML-main/label_perturbation_attack/probability_based_label_perturbation.py,blacklist,B311,LOW,HIGH,https://cwe.mitre.org/data/definitions/330.html,Standard pseudo-random generators are not suitable for security/cryptographic purposes.,28,40,[28],https://bandit.readthedocs.io/en/1.7.4/blacklists/blacklist_calls.html#b311-random
../BigSwag-SQA2022-AUBURN/TestOrchestrator4ML/TestOrchestrator4ML-main/select_repos/dev_count.py,blacklist,B404,LOW,HIGH,https://cwe.mitre.org/data/definitions/78.html,Consider possible security implications associated with the subprocess module.,7,0,[7],https://bandit.readthedocs.io/en/1.7.4/blacklists/blacklist_imports.html#b404-import-subprocess
../BigSwag-SQA2022-AUBURN/TestOrchestrator4ML/TestOrchestrator4ML-main/select_repos/dev_count.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,26,24,[26],https://bandit.readthedocs.io/en/1.7.4/plugins/b607_start_process_with_partial_path.html
../BigSwag-SQA2022-AUBURN/TestOrchestrator4ML/TestOrchestrator4ML-main/select_repos/dev_count.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.,26,24,[26],https://bandit.readthedocs.io/en/1.7.4/plugins/b603_subprocess_without_shell_equals_true.html
```

2. Fuzzing

Implemented fuzzing for 5 methods:

1. checkAlgoNames:
2. checkForLibraryImport
3. getImport
4. getFunctionDetailsForClaases
5. getClassificationAlgoNames

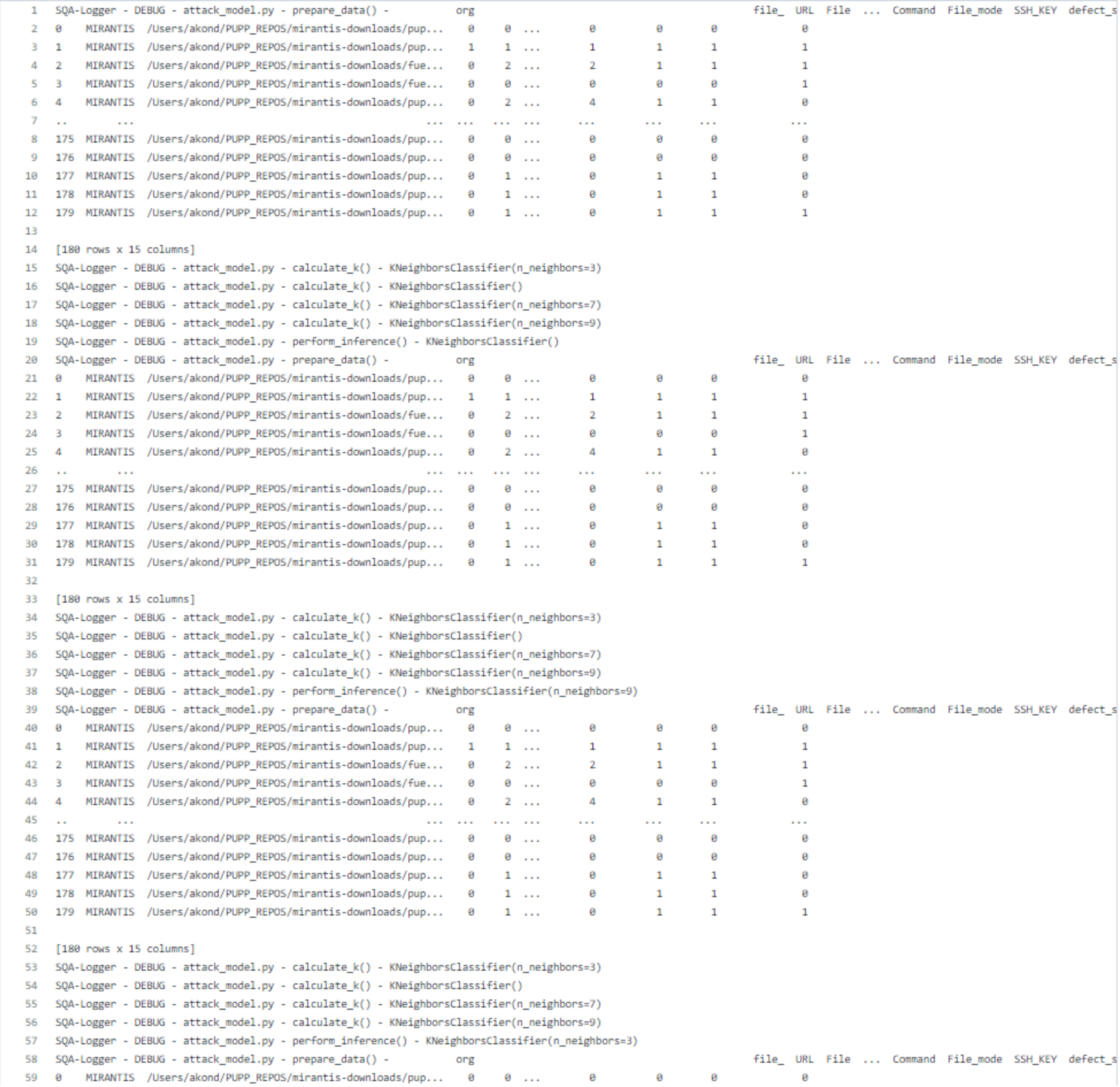
Made sure that all the methods are tested by cross-referencing “blns.json” and either passed or failled the parameters. Output is printed out along with stack traceback where error was found. Learned about what given values are passed or failed and the reasons why they failed, acceptable parameters and insfficient ones.



```
****************************************************************************************************************************
FUZZ: checkAlgoNames() PASSED
****************************************************************************************************************************

FUZZ: checkForLibraryImport() with parameter "" FAILED
Traceback (most recent call last):
  File "fuzzing.py", line 38, in checkForLibraryImportFuzz
    py_parser.checkForLibraryImport(i)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 77, in checkForLibraryImport
    import_list = getImport(pyTree)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 16, in getImport
    for stmt_ in pyTree.body:
AttributeError: 'str' object has no attribute 'body'
****************************************************************************************************************************

FUZZ: getImport() with parameter "" FAILED
Traceback (most recent call last):
  File "fuzzing.py", line 55, in getImportFuzz
    py_parser.getImport(i)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 16, in getImport
    for stmt_ in pyTree.body:
AttributeError: 'str' object has no attribute 'body'
****************************************************************************************************************************

FUZZ: getFunctionDetailsForClaases() with parameter "" FAILED
Traceback (most recent call last):
  File "fuzzing.py", line 73, in getFunctionDetailsForClaasesFuzz
    py_parser.getFunctionDetailsForClaases(i)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 32, in getFunctionDetailsForClaases
    for stmt_ in pyTree.body:
AttributeError: 'str' object has no attribute 'body'
****************************************************************************************************************************

FUZZ: getClassificationAlgoNames() with parameter "" FAILED
Traceback (most recent call last):
  File "fuzzing.py", line 91, in getClassificationAlgoNamesFuzz
    py_parser.getClassificationAlgoNames(i)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 94, in getClassificationAlgoNames
    library_import = checkForLibraryImport(pyTree)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 77, in checkForLibraryImport
    import_list = getImport(pyTree)
  File "/home/jem0101/finalprojectDir/TestOrchestrator4ML-main/resources/Code/generation/identify_algo/py_parser.py", line 16, in getImport
    for stmt_ in pyTree.body:
AttributeError: 'str' object has no attribute 'body'
****************************************************************************************************************************
```

3. Forensics

Logging forensics was added to two files in the GitHub repo. 4 logging snippets were added in /resources/Code/generate/generate_attack.py to provide logging for various functions to log potential security vulnerabilities in the ML code such as poisoning attacks and model tricking. Another logging snippet was added into /label_pertubation_attack/knn.py to log a potential point for a poisoning attack. The logs output the information about the python file, the python function, and either the model or the dataset which could be attacked. Running the repo through /resources/code/generate/main.py will output these logs to a file “app.log” in the directory /resources/Output/app.log. Here is a screenshot of the results:



```
SQA-Logger - DEBUG - attack_model.py - prepare_data() -            org                                              file_  URL  File  ...  Command  File_mode  SSH_KEY  defect_s
0    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
1    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     1     1  ...        1          1        1              1
2    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     2  ...        2          1        1              1
3    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     0  ...        0          0        0              1
4    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     2  ...        4          1        1              0
..        ...                                                 ...  ...   ...  ...      ...        ...      ...            ...
175  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
176  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
177  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
178  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
179  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              1

[180 rows x 15 columns]
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=3)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier()
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=7)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=9)
SQA-Logger - DEBUG - attack_model.py - perform_inference() - KNeighborsClassifier()
SQA-Logger - DEBUG - attack_model.py - prepare_data() -            org                                              file_  URL  File  ...  Command  File_mode  SSH_KEY  defect_s
0    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
1    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     1     1  ...        1          1        1              1
2    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     2  ...        2          1        1              1
3    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     0  ...        0          0        0              1
4    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     2  ...        4          1        1              0
..        ...                                                 ...  ...   ...  ...      ...        ...      ...            ...
175  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
176  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
177  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
178  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
179  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              1

[180 rows x 15 columns]
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=3)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier()
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=7)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=9)
SQA-Logger - DEBUG - attack_model.py - perform_inference() - KNeighborsClassifier(n_neighbors=9)
SQA-Logger - DEBUG - attack_model.py - prepare_data() -            org                                              file_  URL  File  ...  Command  File_mode  SSH_KEY  defect_s
0    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
1    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     1     1  ...        1          1        1              1
2    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     2  ...        2          1        1              1
3    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/fue...     0     0  ...        0          0        0              1
4    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     2  ...        4          1        1              0
..        ...                                                 ...  ...   ...  ...      ...        ...      ...            ...
175  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
176  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
177  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
178  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              0
179  MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     1  ...        0          1        1              1

[180 rows x 15 columns]
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=3)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier()
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=7)
SQA-Logger - DEBUG - attack_model.py - calculate_k() - KNeighborsClassifier(n_neighbors=9)
SQA-Logger - DEBUG - attack_model.py - perform_inference() - KNeighborsClassifier(n_neighbors=3)
SQA-Logger - DEBUG - attack_model.py - prepare_data() -            org                                              file_  URL  File  ...  Command  File_mode  SSH_KEY  defect_s
0    MIRANTIS  /Users/akond/PUPP_REPOS/mirantis-downloads/pup...     0     0  ...        0          0        0              0
```