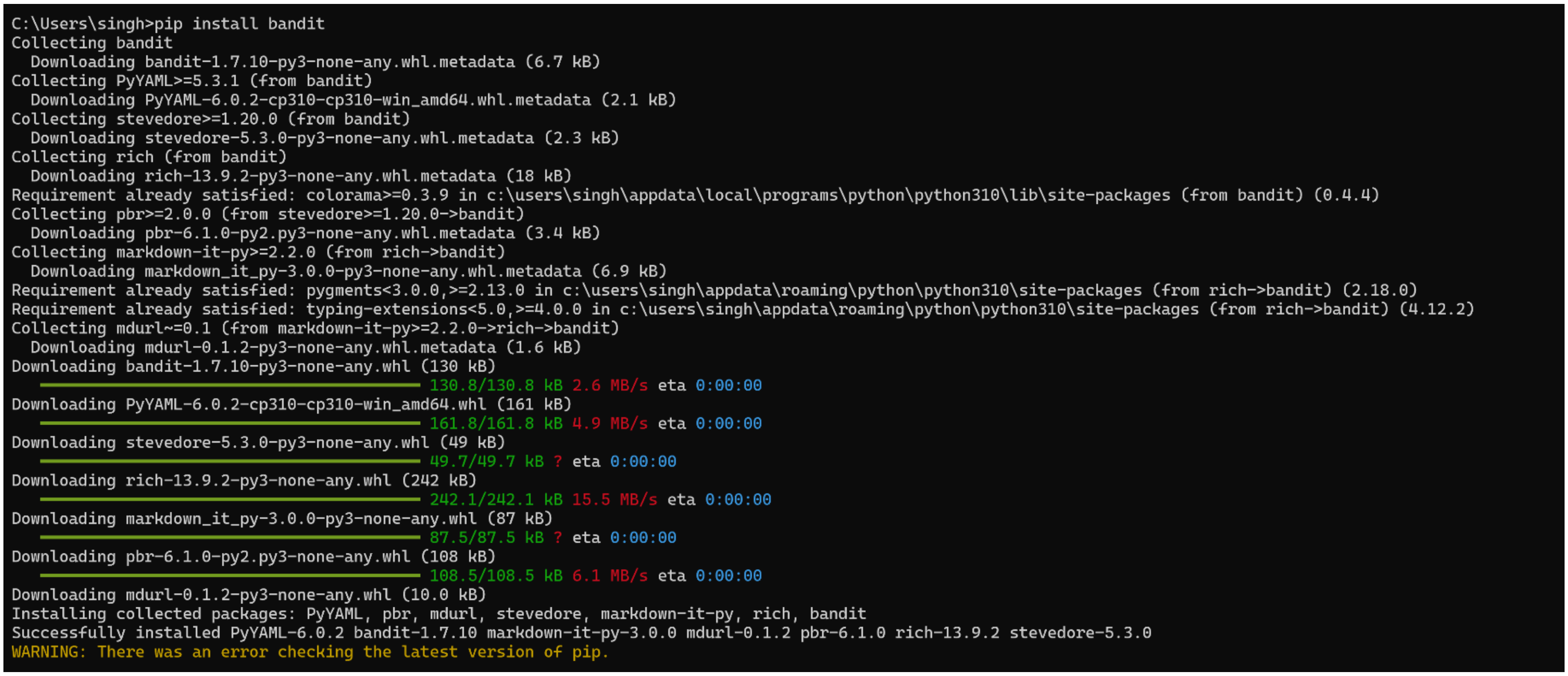
Ankush Singh

WorkShop_6

Screenshot's for the WorkShop



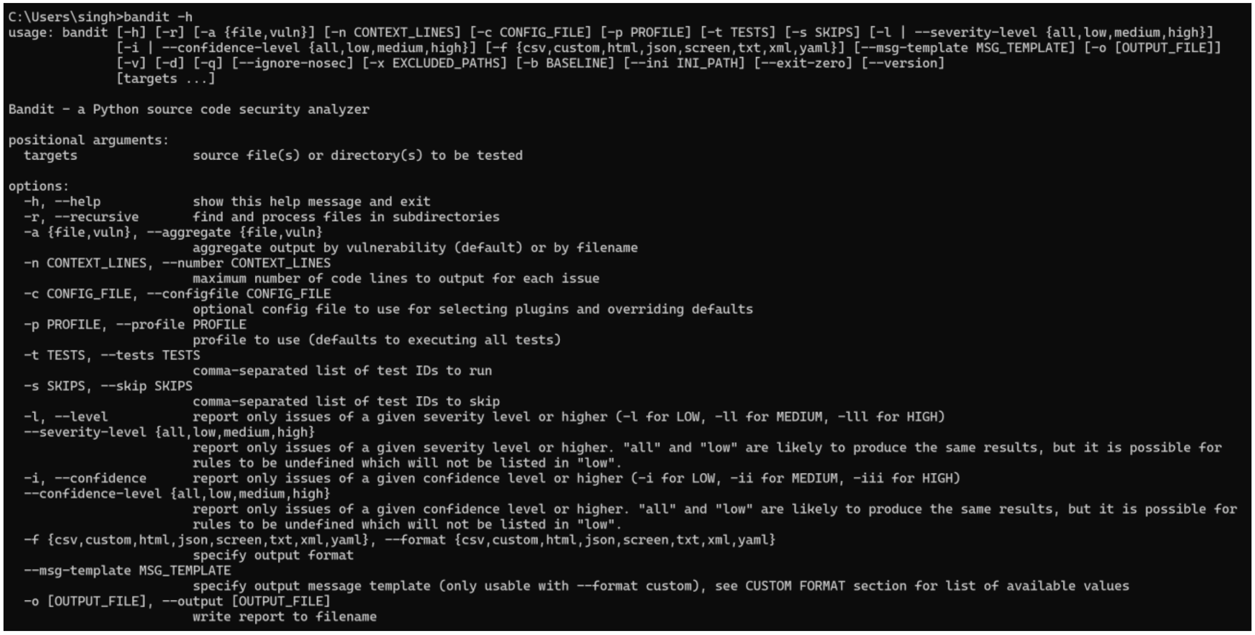
```
C:\Users\singh>pip install bandit
Collecting bandit
  Downloading bandit-1.7.10-py3-none-any.whl.metadata (6.7 kB)
Collecting PyYAML>=5.3.1 (from bandit)
  Downloading PyYAML-6.0.2-cp310-cp310-win_amd64.whl.metadata (2.1 kB)
Collecting stevedore>=1.20.0 (from bandit)
  Downloading stevedore-5.3.0-py3-none-any.whl.metadata (2.3 kB)
Collecting rich (from bandit)
  Downloading rich-13.9.2-py3-none-any.whl.metadata (18 kB)
Requirement already satisfied: colorama>=0.3.9 in c:\users\singh\appdata\local\programs\python\python310\lib\site-packages (from bandit) (0.4.4)
Collecting pbr>=2.0.0 (from stevedore>=1.20.0->bandit)
  Downloading pbr-6.1.0-py2.py3-none-any.whl.metadata (3.4 kB)
Collecting markdown-it-py>=2.2.0 (from rich->bandit)
  Downloading markdown_it_py-3.0.0-py3-none-any.whl.metadata (6.9 kB)
Requirement already satisfied: pygments<3.0.0,>=2.13.0 in c:\users\singh\appdata\roaming\python\python310\site-packages (from rich->bandit) (2.18.0)
Requirement already satisfied: typing-extensions<5.0,>=4.0.0 in c:\users\singh\appdata\roaming\python\python310\site-packages (from rich->bandit) (4.12.2)
Collecting mdurl~=0.1 (from markdown-it-py>=2.2.0->rich->bandit)
  Downloading mdurl-0.1.2-py3-none-any.whl.metadata (1.6 kB)
Downloading bandit-1.7.10-py3-none-any.whl (130 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 130.8/130.8 kB 2.6 MB/s eta 0:00:00
Downloading PyYAML-6.0.2-cp310-cp310-win_amd64.whl (161 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 161.8/161.8 kB 4.9 MB/s eta 0:00:00
Downloading stevedore-5.3.0-py3-none-any.whl (49 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 49.7/49.7 kB ? eta 0:00:00
Downloading rich-13.9.2-py3-none-any.whl (242 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 242.1/242.1 kB 15.5 MB/s eta 0:00:00
Downloading markdown_it_py-3.0.0-py3-none-any.whl (87 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 87.5/87.5 kB ? eta 0:00:00
Downloading pbr-6.1.0-py2.py3-none-any.whl (108 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 108.5/108.5 kB 6.1 MB/s eta 0:00:00
Downloading mdurl-0.1.2-py3-none-any.whl (10.0 kB)
Installing collected packages: PyYAML, pbr, mdurl, stevedore, markdown-it-py, rich, bandit
Successfully installed PyYAML-6.0.2 bandit-1.7.10 markdown-it-py-3.0.0 mdurl-0.1.2 pbr-6.1.0 rich-13.9.2 stevedore-5.3.0
WARNING: There was an error checking the latest version of pip.
```

Above screenshot, installing the bandit with the command of 'pip install bandit'

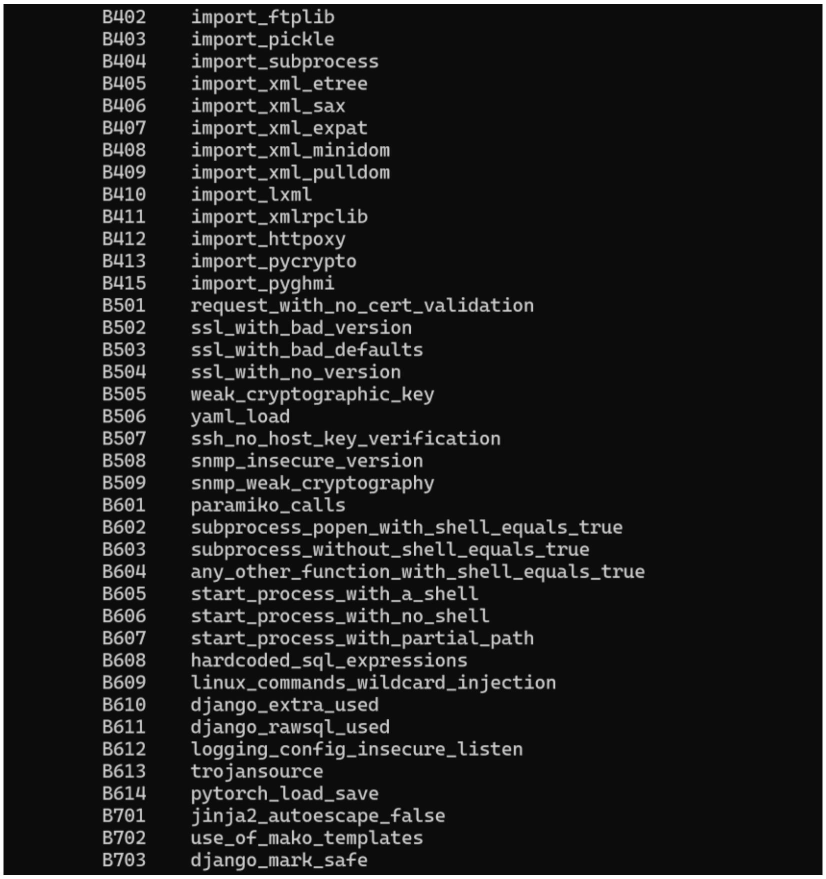
Ankush Singh

WorkShop_6

Screenshot's for the WorkShop



```
C:\Users\singh>bandit -h
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 ...]

Bandit - a Python source code security analyzer

positional arguments:
  targets               source file(s) or directory(s) to be tested

options:
  -h, --help            show this help message and exit
  -r, --recursive       find and process files in subdirectories
  -a {file,vuln}, --aggregate {file,vuln}
                        aggregate output by vulnerability (default) or by filename
  -n CONTEXT_LINES, --number CONTEXT_LINES
                        maximum number of code lines to output for each issue
  -c CONFIG_FILE, --configfile CONFIG_FILE
                        optional config file to use for selecting plugins and overriding defaults
  -p PROFILE, --profile PROFILE
                        profile to use (defaults to executing all tests)
  -t TESTS, --tests TESTS
                        comma-separated list of test IDs to run
  -s SKIPS, --skip SKIPS
                        comma-separated list of test IDs to skip
  -l, --level           report only issues of a given severity level or higher (-l for LOW, -ll for MEDIUM, -lll for HIGH)
  --severity-level {all,low,medium,high}
                        report only issues of a given severity level or higher. "all" and "low" are likely to produce the same results, but it is possible for
                        rules to be undefined which will not be listed in "low".
  -i, --confidence      report only issues of a given confidence level or higher (-i for LOW, -ii for MEDIUM, -iii for HIGH)
  --confidence-level {all,low,medium,high}
                        report only issues of a given confidence level or higher. "all" and "low" are likely to produce the same results, but it is possible for
                        rules to be undefined which will not be listed in "low".
  -f {csv,custom,html,json,screen,txt,xml,yaml}, --format {csv,custom,html,json,screen,txt,xml,yaml}
                        specify output format
  --msg-template MSG_TEMPLATE
                        specify output message template (only usable with --format custom), see CUSTOM FORMAT section for list of available values
  -o [OUTPUT_FILE], --output [OUTPUT_FILE]
                        write report to filename
```



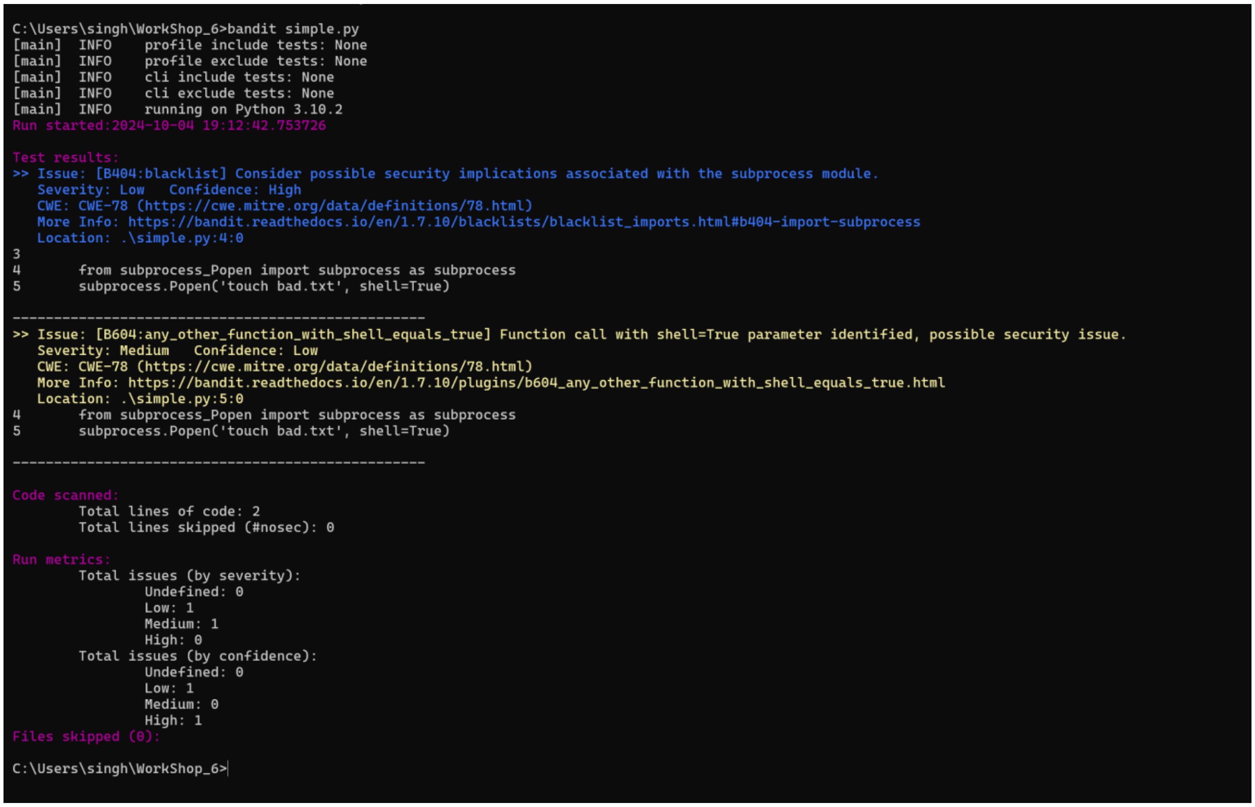
```
        B402    import_ftplib
        B403    import_pickle
        B404    import_subprocess
        B405    import_xml_etree
        B406    import_xml_sax
        B407    import_xml_expat
        B408    import_xml_minidom
        B409    import_xml_pulldom
        B410    import_lxml
        B411    import_xmlrpclib
        B412    import_httpoxy
        B413    import_pycrypto
        B415    import_pyghmi
        B501    request_with_no_cert_validation
        B502    ssl_with_bad_version
        B503    ssl_with_bad_defaults
        B504    ssl_with_no_version
        B505    weak_cryptographic_key
        B506    yaml_load
        B507    ssh_no_host_key_verification
        B508    snmp_insecure_version
        B509    snmp_weak_cryptography
        B601    paramiko_calls
        B602    subprocess_popen_with_shell_equals_true
        B603    subprocess_without_shell_equals_true
        B604    any_other_function_with_shell_equals_true
        B605    start_process_with_a_shell
        B606    start_process_with_no_shell
        B607    start_process_with_partial_path
        B608    hardcoded_sql_expressions
        B609    linux_commands_wildcard_injection
        B610    django_extra_used
        B611    django_rawsql_used
        B612    logging_config_insecure_listen
        B613    trojansource
        B614    pytorch_load_save
        B701    jinja2_autoescape_false
        B702    use_of_mako_templates
        B703    django_mark_safe
```

Above screenshot's, verifies that bandit is installed. Using the command 'bandit -h'

Ankush Singh

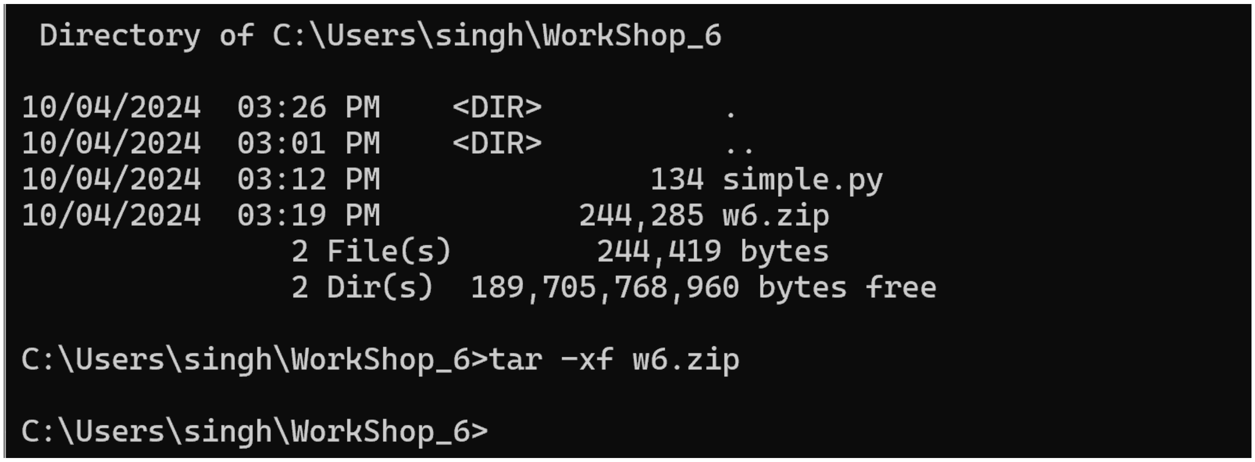
WorkShop_6

Screenshot's for the WorkShop



```
C:\Users\singh\WorkShop_6>bandit simple.py
[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 3.10.2
Run started:2024-10-04 19:12:42.753726

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: .\simple.py:4:0
3
4       from subprocess_Popen import subprocess as subprocess
5       subprocess.Popen('touch bad.txt', shell=True)

--------------------------------------------------
>> Issue: [B604:any_other_function_with_shell_equals_true] Function call with shell=True parameter identified, possible security issue.
   Severity: Medium   Confidence: Low
   CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b604_any_other_function_with_shell_equals_true.html
   Location: .\simple.py:5:0
4       from subprocess_Popen import subprocess as subprocess
5       subprocess.Popen('touch bad.txt', shell=True)

--------------------------------------------------

Code scanned:
        Total lines of code: 2
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 1
                Medium: 1
                High: 0
        Total issues (by confidence):
                Undefined: 0
                Low: 1
                Medium: 0
                High: 1
Files skipped (0):

C:\Users\singh\WorkShop_6>
```

Above screenshot, used the same code as professor had in his recording, screenshot is about running the command 'bandit simple.py' which runs the simple.py file.



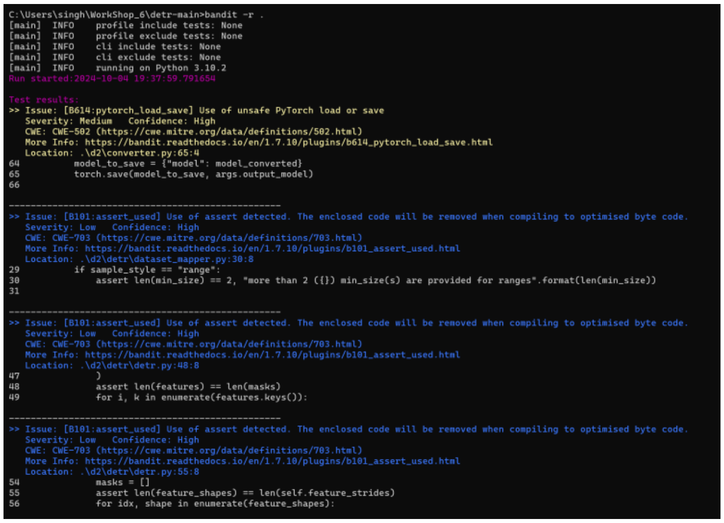
```
 Directory of C:\Users\singh\WorkShop_6

10/04/2024  03:26 PM    <DIR>          .
10/04/2024  03:01 PM    <DIR>          ..
10/04/2024  03:12 PM               134 simple.py
10/04/2024  03:19 PM           244,285 w6.zip
               2 File(s)        244,419 bytes
               2 Dir(s)  189,705,768,960 bytes free

C:\Users\singh\WorkShop_6>tar -xf w6.zip

C:\Users\singh\WorkShop_6>
```

Above screenshot, downloaded the 'w6.zip' folder and unzipped the folder.

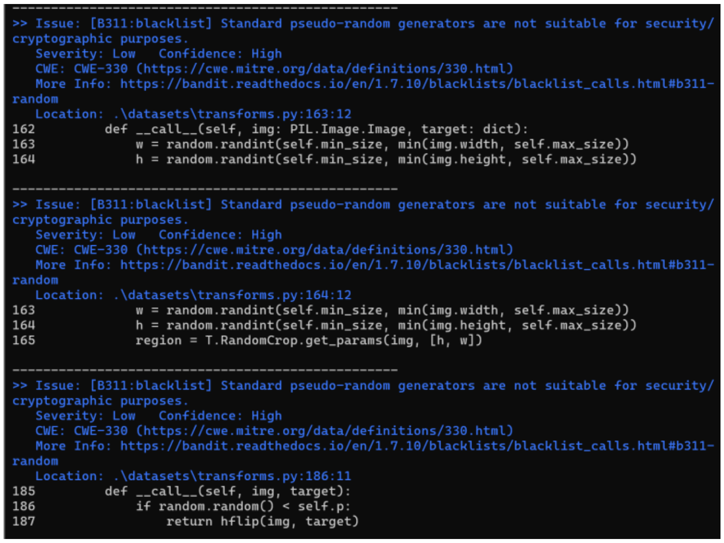
Ankush Singh

WorkShop_6

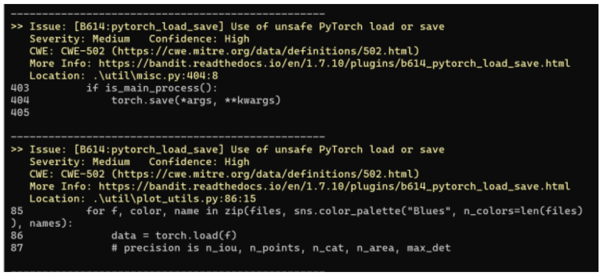
Screenshot’s for the WorkShop



```
C:\Users\singh\WorkShop_6\detr-main>bandit -r .
[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 3.10.2
Run started:2024-10-04 19:37:59.791654

Test results:
>> Issue: [B614:pytorch_load_save] Use of unsafe PyTorch load or save
   Severity: Medium   Confidence: High
   CWE: CWE-502 (https://cwe.mitre.org/data/definitions/502.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b614_pytorch_load_save.html
   Location: .\d2\converter.py:65:4
64          model_to_save = {"model": model_converted}
65          torch.save(model_to_save, args.output_model)
66

--------------------------------------------------
>> Issue: [B101:assert_used] Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
   Severity: Low   Confidence: High
   CWE: CWE-703 (https://cwe.mitre.org/data/definitions/703.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b101_assert_used.html
   Location: .\d2\detr\dataset_mapper.py:30:8
29          if sample_style == "range":
30              assert len(min_size) == 2, "more than 2 ({}) min_size(s) are provided for ranges".format(len(min_size))
31

--------------------------------------------------
>> Issue: [B101:assert_used] Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
   Severity: Low   Confidence: High
   CWE: CWE-703 (https://cwe.mitre.org/data/definitions/703.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b101_assert_used.html
   Location: .\d2\detr\detr.py:48:8
47              )
48              assert len(features) == len(masks)
49              for i, k in enumerate(features.keys()):

--------------------------------------------------
>> Issue: [B101:assert_used] Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
   Severity: Low   Confidence: High
   CWE: CWE-703 (https://cwe.mitre.org/data/definitions/703.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b101_assert_used.html
   Location: .\d2\detr\detr.py:55:8
54              masks = []
55              assert len(feature_shapes) == len(self.feature_strides)
56              for idx, shape in enumerate(feature_shapes):
```



```
--------------------------------------------------
>> Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/
cryptographic purposes.
   Severity: Low   Confidence: High
   CWE: CWE-330 (https://cwe.mitre.org/data/definitions/330.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist_calls.html#b311-
random
   Location: .\datasets\transforms.py:163:12
162         def __call__(self, img: PIL.Image.Image, target: dict):
163             w = random.randint(self.min_size, min(img.width, self.max_size))
164             h = random.randint(self.min_size, min(img.height, self.max_size))

--------------------------------------------------
>> Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/
cryptographic purposes.
   Severity: Low   Confidence: High
   CWE: CWE-330 (https://cwe.mitre.org/data/definitions/330.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist_calls.html#b311-
random
   Location: .\datasets\transforms.py:164:12
163             w = random.randint(self.min_size, min(img.width, self.max_size))
164             h = random.randint(self.min_size, min(img.height, self.max_size))
165             region = T.RandomCrop.get_params(img, [h, w])

--------------------------------------------------
>> Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/
cryptographic purposes.
   Severity: Low   Confidence: High
   CWE: CWE-330 (https://cwe.mitre.org/data/definitions/330.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/blacklists/blacklist_calls.html#b311-
random
   Location: .\datasets\transforms.py:186:11
185         def __call__(self, img, target):
186             if random.random() < self.p:
187                 return hflip(img, target)
```



```
--------------------------------------------------
>> Issue: [B614:pytorch_load_save] Use of unsafe PyTorch load or save
   Severity: Medium   Confidence: High
   CWE: CWE-502 (https://cwe.mitre.org/data/definitions/502.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b614_pytorch_load_save.html
   Location: .\util\misc.py:404:8
403         if is_main_process():
404             torch.save(*args, **kwargs)
405

--------------------------------------------------
>> Issue: [B614:pytorch_load_save] Use of unsafe PyTorch load or save
   Severity: Medium   Confidence: High
   CWE: CWE-502 (https://cwe.mitre.org/data/definitions/502.html)
   More Info: https://bandit.readthedocs.io/en/1.7.10/plugins/b614_pytorch_load_save.html
   Location: .\util\plot_utils.py:86:15
85          for f, color, name in zip(files, sns.color_palette("Blues", n_colors=len(files)
), names):
86              data = torch.load(f)
87              # precision is n_iou, n_points, n_cat, n_area, max_det
```

Above screenshot’s, after unzipping the folder ran the command ‘bandit -r .’ to scan files.