SET Lab ESE

Name : Sagar Nameshwar Rahangdale

Batch : T7

Subject : SET LAB ESE

Perform source code testing using Bandit for your code written in python language for any security flaws

After performing analysis create a report which will contain below points

f. Number of hits

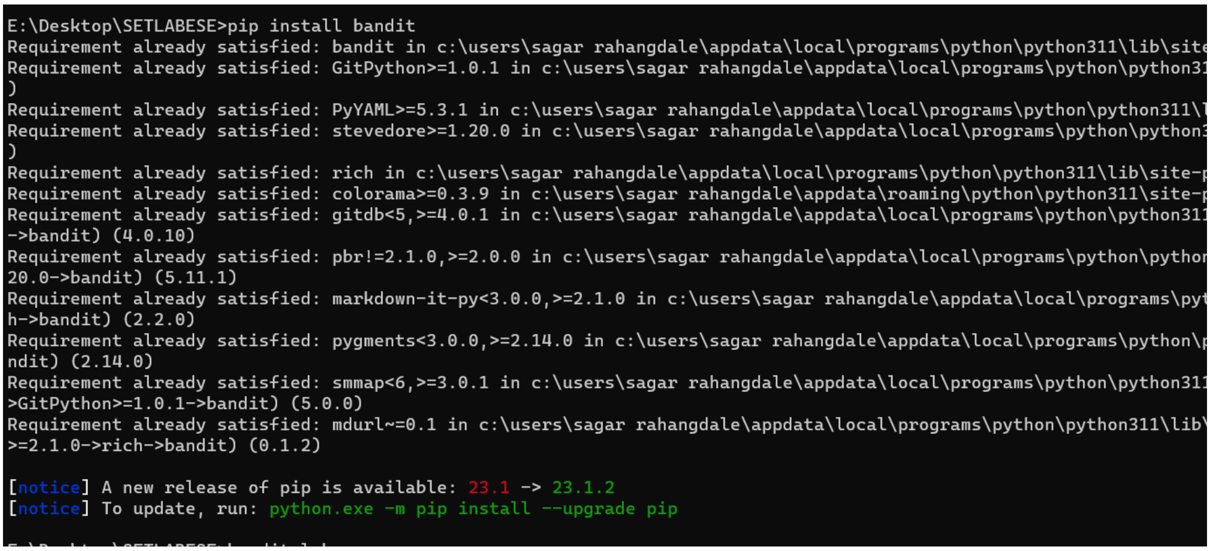
g. Potential risks

h. Suggested alternatives for the risks

i. Updating the code as per suggestions

j. Re-execution of code after updating the changes

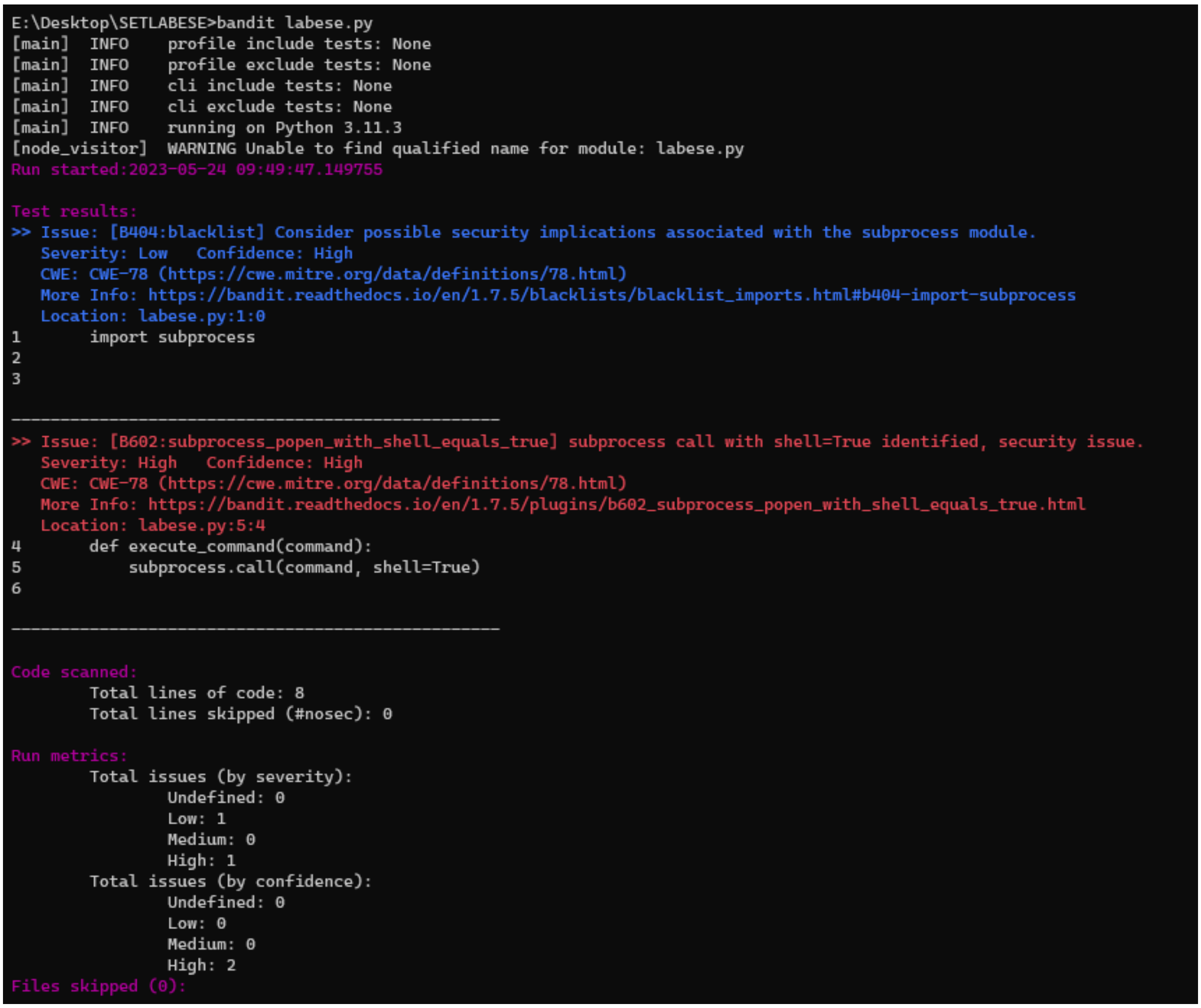
Step 1. Install the bandit .



```
E:\Desktop\SETLABESE>pip install bandit
Requirement already satisfied: bandit in c:\users\sagar rahangdale\appdata\local\programs\python\python311\lib\site
Requirement already satisfied: GitPython>=1.0.1 in c:\users\sagar rahangdale\appdata\local\programs\python\python31
)
Requirement already satisfied: PyYAML>=5.3.1 in c:\users\sagar rahangdale\appdata\local\programs\python\python311\l
Requirement already satisfied: stevedore>=1.20.0 in c:\users\sagar rahangdale\appdata\local\programs\python\python3
)
Requirement already satisfied: rich in c:\users\sagar rahangdale\appdata\local\programs\python\python311\lib\site-p
Requirement already satisfied: colorama>=0.3.9 in c:\users\sagar rahangdale\appdata\roaming\python\python311\site-p
Requirement already satisfied: gitdb<5,>=4.0.1 in c:\users\sagar rahangdale\appdata\local\programs\python\python311
->bandit) (4.0.10)
Requirement already satisfied: pbr!=2.1.0,>=2.0.0 in c:\users\sagar rahangdale\appdata\local\programs\python\python
20.0->bandit) (5.11.1)
Requirement already satisfied: markdown-it-py<3.0.0,>=2.1.0 in c:\users\sagar rahangdale\appdata\local\programs\pyt
h->bandit) (2.2.0)
Requirement already satisfied: pygments<3.0.0,>=2.14.0 in c:\users\sagar rahangdale\appdata\local\programs\python\p
ndit) (2.14.0)
Requirement already satisfied: smmap<6,>=3.0.1 in c:\users\sagar rahangdale\appdata\local\programs\python\python311
>GitPython>=1.0.1->bandit) (5.0.0)
Requirement already satisfied: mdurl~=0.1 in c:\users\sagar rahangdale\appdata\local\programs\python\python311\lib\
>=2.1.0->rich->bandit) (0.1.2)

[notice] A new release of pip is available: 23.1 -> 23.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
```

Step 2. Run the file using the Bandit



```
E:\Desktop\SETLABESE>bandit labese.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 3.11.3
[node_visitor]  WARNING Unable to find qualified name for module: labese.py
Run started:2023-05-24 09:49:47.149755

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/1.7.5/blacklists/blacklist_imports.html#b404-import-subprocess
   Location: labese.py:1:0
1       import subprocess
2
3

--------------------------------------------------
>> Issue: [B602:subprocess_popen_with_shell_equals_true] subprocess call with shell=True identified, security issue.
   Severity: High   Confidence: High
   CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
   More Info: https://bandit.readthedocs.io/en/1.7.5/plugins/b602_subprocess_popen_with_shell_equals_true.html
   Location: labese.py:5:4
4       def execute_command(command):
5           subprocess.call(command, shell=True)
6

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

Code scanned:
        Total lines of code: 8
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 1
                Medium: 0
                High: 1
        Total issues (by confidence):
                Undefined: 0
                Low: 0
                Medium: 0
                High: 2
Files skipped (0):
```

f. Number of hits

One low severity issue: [B404:blacklist]

One high severity issue: [B602:subprocess_popen_with_shell_equals_true]

g. Potential risks

Security vulnerabilities due to the use of the subprocess module.

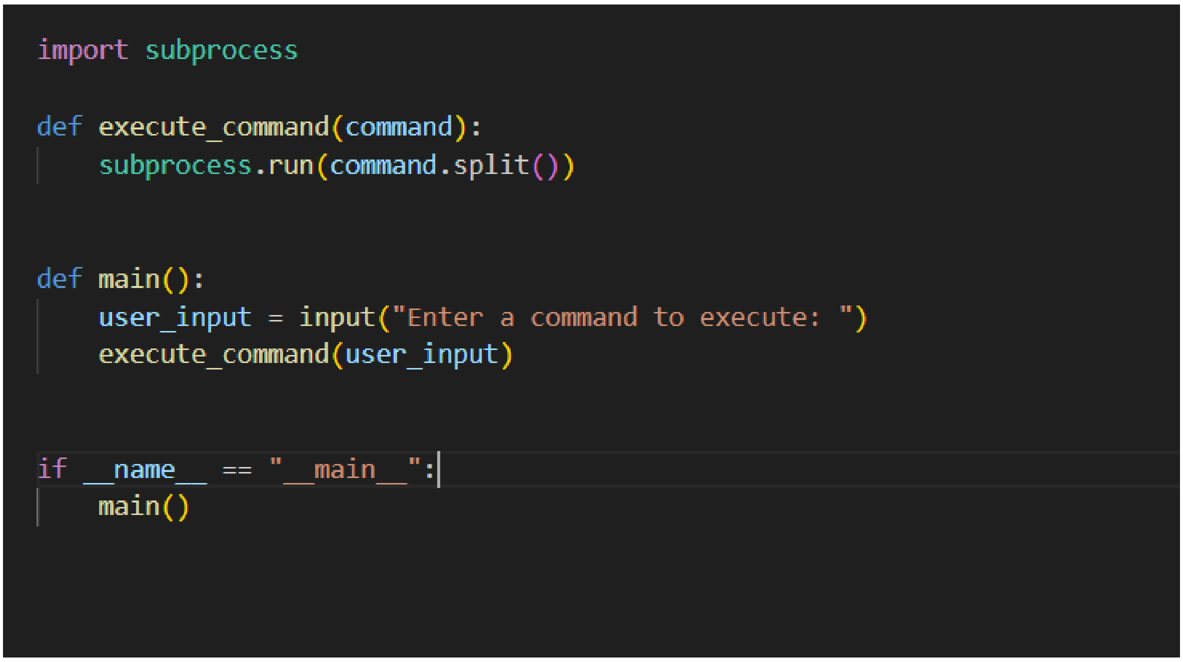
Command injection vulnerability due to the use of subprocess.call with shell=True.

h. Suggested alternatives for the risks

For the subprocess module, be cautious when executing commands and ensure proper input validation and sanitization.

Replace subprocess.call with subprocess.run to avoid command injection vulnerabilities. Pass the command as a list of arguments instead of using shell=True.

i. Updating the code as per suggestions



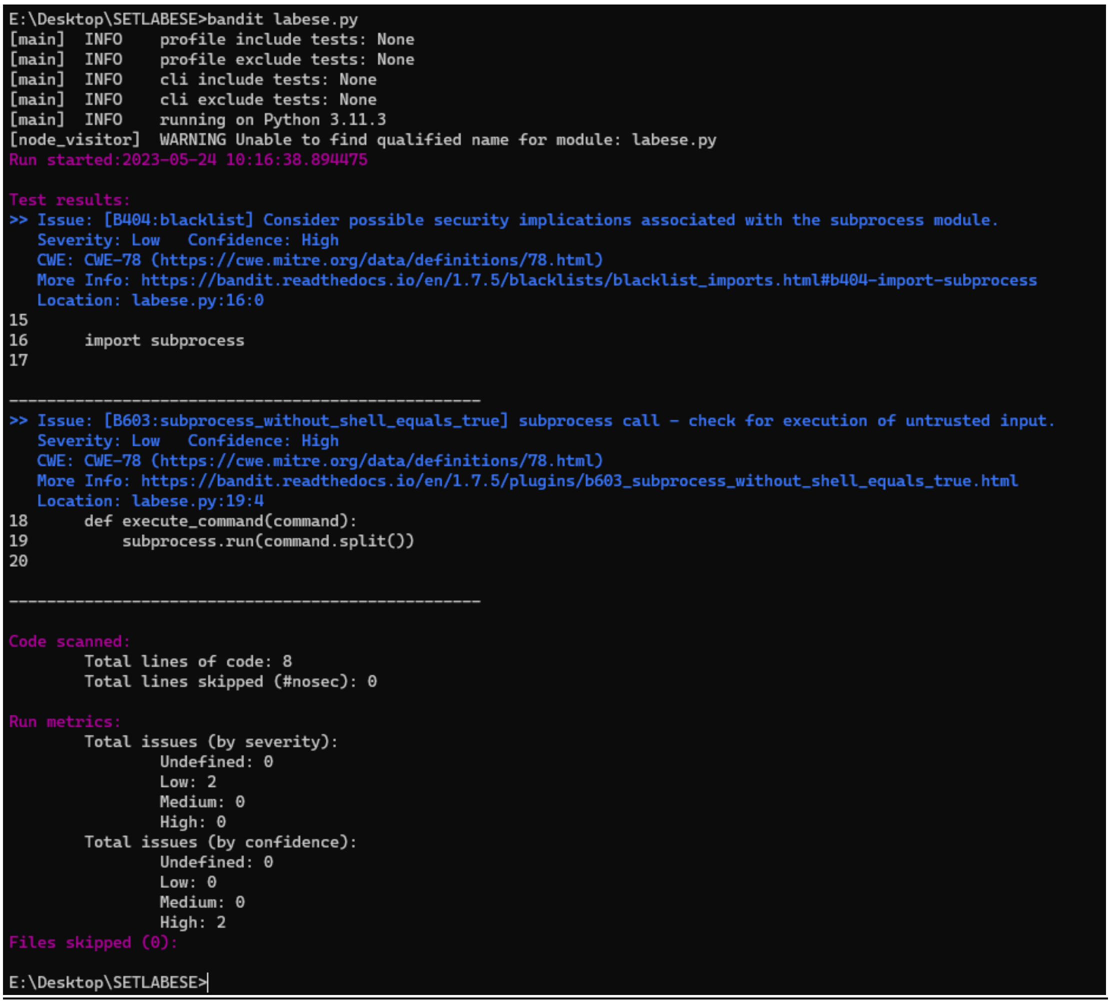
```python
import subprocess

def execute_command(command):
    subprocess.run(command.split())


def main():
    user_input = input("Enter a command to execute: ")
    execute_command(user_input)


if __name__ == "__main__":
    main()
```

j. Re-execution of code after updating the changes



```
E:\Desktop\SETLABESE>bandit labese.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 3.11.3
[node_visitor]  WARNING Unable to find qualified name for module: labese.py
Run started:2023-05-24 10:16:38.894475

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/1.7.5/blacklists/blacklist_imports.html#b404-import-subprocess
   Location: labese.py:16:0
15
16      import subprocess
17

--------------------------------------------------
>> 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/1.7.5/plugins/b603_subprocess_without_shell_equals_true.html
   Location: labese.py:19:4
18      def execute_command(command):
19          subprocess.run(command.split())
20

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

Code scanned:
        Total lines of code: 8
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 2
                Medium: 0
                High: 0
        Total issues (by confidence):
                Undefined: 0
                Low: 0
                Medium: 0
                High: 2
Files skipped (0):

E:\Desktop\SETLABESE>
```