

Pysa Experiment (Task – 4)

Refer to the below step-by-step guide if you are not able to run Pysa or Dynamic debugger.

Sub Task – 1

For the Sub Task-1, you must go through all the files in the task-4 directory and answer the questions. Below are all the files.

Views.py

```
views.py x
Task-4 > views.py > ...
1  import requests
2  from collections import defaultdict
3
4  def solve(value):
5      if value in {"+", "-", "*", "/"}:
6          result = eval(f"8 {value} 4")
7          return result
8      else:
9          return -1
10
11 base_url = 'https://pysa-api-2598d-default-rtdb.firebaseio.com/opr.json'
12 operators = requests.get(base_url)
13 opr_json = operators.json()
14 operator = opr_json["mul"]
15
16 d = defaultdict(list)
17 d[1].append(operator)
18 operators = d[1]
19
20 result = solve(operator)
21
22 print(result)
```

Taint.config

```
taint.config X
Task-4 > taint.config
1 {
2   "sources": [
3     {
4       "name": "CustomUserControlled",
5       "comment": "use to annotate user input"
6     },
7     {
8       "name": "WebUserConrtrolled",
9       "comment": "use to annotate user input"
10    }
11  ],
12
13  "sinks": [
14    {
15      "name": "CodeExecution",
16      "comment": "use to annotate execution of python code"
17    }
18  ],
19
20  "features": [],
21
22  "rules": [
23    {
24      "name": "Possible RCE:",
25      "code": 5001,
26      "sources": [ "CustomUserControlled" ],
27      "sinks": [ "CodeExecution" ],
28      "message_format": "User specified data may reach a code execution sink"
29    },
30    {
31      "name": "Possible RCE2:",
32      "code": 5002,
33      "sources": [ "WebUserConrtrolled" ],
34      "sinks": [ "CodeExecution" ],
35      "message_format": "User specified data from web may reach a code execution sink"
36    }
37  ]
38 }
39
```

sources_sinks.pysa

```
sources_sinks.pysa X
Task-4 > sources_sinks.pysa
1 def requests.api.get() -> TaintSource[WebUserConrtrolled]: ...
2
3 def eval(__source: TaintSink[CodeExecution], __globals, __locals): ...
4
```

.pyre_configuration

```
{ } .pyre_configuration X
Task-4 > { } .pyre_configuration > ...
1  {
2    "source_directories": [
3      |   "."
4    ],
5    "taint_models_path": [
6      |   "."
7    ],
8    "search_path": [
9      |   "../../stubs/"
10   ],
11   "exclude": [
12     |   ".*integration_test.*"
13   ]
14 }
15
```

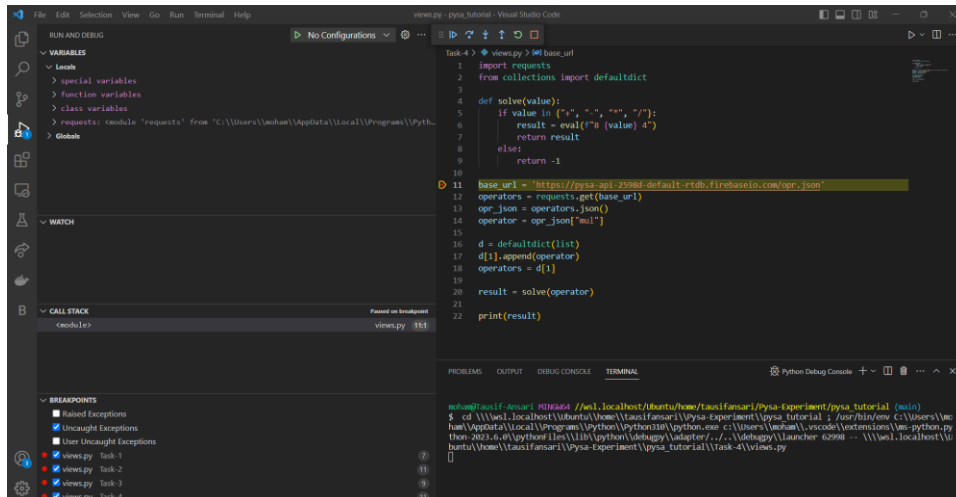
Sub Task – 2

For the Sub Task-2, you will run Pysa (Static Analyzer) and by going through its output you will answer the questions. Below is the Pysa Output for Task-3

```
[
  {
    "line": 20,
    "column": 15,
    "stop_line": 20,
    "stop_column": 23,
    "path": "views.py",
    "code": 5002,
    "name": "Possible RCE2:",
    "description": "Possible RCE2: [5002]: User specified data from web may reach a code execution sink",
    "define": "views.$toplevel"
  }
]
```

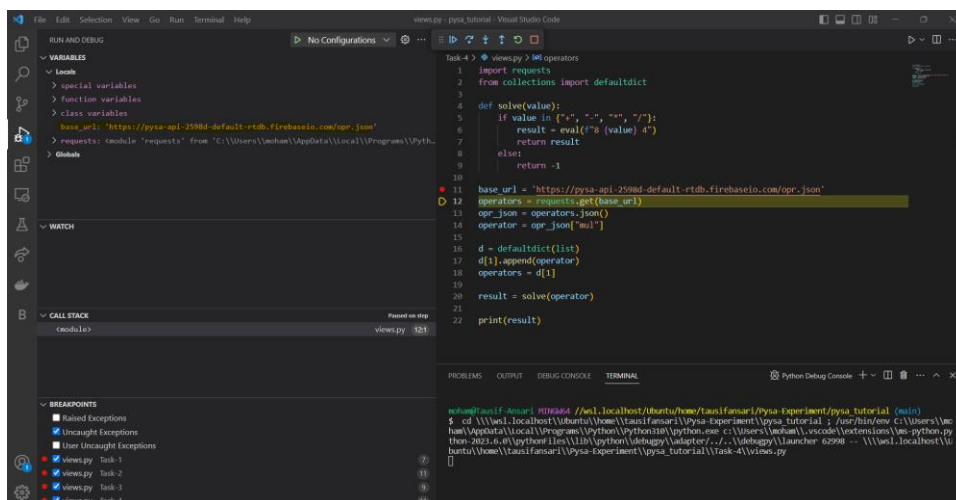
Sub Task – 3

For the Sub Task-3, you will run the dynamic debugger and try to track the flow of data. In this Sub Task you will use the Output of Pysa along with the Output of the dynamic debugger and then try to answer the questions. Below is the Output of the debugger.



```
task-4 > views.py > 111 base_url
1 import requests
2 from collections import defaultdict
3
4 def solve(value):
5     if value in {"+", "-", "*", "/"}:
6         result = eval(f"8 {value} 4")
7         return result
8     else:
9         return -1
10
11 base_url = "https://pysa-api-2598d-default-rtb.firebaseio.com/opr_json"
12 operators = requests.get(base_url)
13 opr_json = operators.json()
14 operator = opr_json["mul"]
15
16 d = defaultdict(list)
17 d[1].append(operator)
18 operators = d[1]
19
20 result = solve(operator)
21
22 print(result)
```

```
shubham@shubham-HP: /mnt/localhost/shubham/tanvifansari/Pysa-Experiment/pysa_tutorial (main)
$ cd /mnt/localhost/shubham/tanvifansari/Pysa-Experiment/pysa_tutorial ; /usr/bin/env C:\Users\shubham\AppData\Local\Programs\Python\Python310\python.exe c:\Users\shubham\vscode\extensions\ms-python.python-2023.6.0\python\lib\python\python\debugpy\adapter\../.\\debugpy\launcher 62980 -- \\mnt.localhost\shubham\home\tanvifansari\Pysa-Experiment\pysa_tutorial\Task-4\views.py
```



```
task-4 > views.py > 121 operators
1 import requests
2 from collections import defaultdict
3
4 def solve(value):
5     if value in {"+", "-", "*", "/"}:
6         result = eval(f"8 {value} 4")
7         return result
8     else:
9         return -1
10
11 base_url = "https://pysa-api-2598d-default-rtb.firebaseio.com/opr_json"
12 operators = requests.get(base_url)
13 opr_json = operators.json()
14 operator = opr_json["mul"]
15
16 d = defaultdict(list)
17 d[1].append(operator)
18 operators = d[1]
19
20 result = solve(operator)
21
22 print(result)
```

```
shubham@shubham-HP: /mnt/localhost/shubham/tanvifansari/Pysa-Experiment/pysa_tutorial (main)
$ cd /mnt/localhost/shubham/tanvifansari/Pysa-Experiment/pysa_tutorial ; /usr/bin/env C:\Users\shubham\AppData\Local\Programs\Python\Python310\python.exe c:\Users\shubham\vscode\extensions\ms-python.python-2023.6.0\python\lib\python\python\debugpy\adapter\../.\\debugpy\launcher 62980 -- \\mnt.localhost\shubham\home\tanvifansari\Pysa-Experiment\pysa_tutorial\Task-4\views.py
```