

Inspection Task 1

Imagine you are an expert in taint analysis and you want to evaluate a new Android taint analysis tool **X**. Tool **X** analyzes an Android app called **save_me.apk** and outputs 3 taint flows in the file **plain.xml**.

Below is an explanation about the format used in **plain.xml** :

```
<answer>
  <flows>
    <flow> // information of a taint flow
      <reference type="to"> // Information about the sink
        <statement>
          // the sink statement in Jimple
        </statement>
        <method>
          // the method in which the sink statement exists
        </method>
        <classname>
          // the class in which the sink statement exists
        </classname>
        ....
      </reference>
      <reference type="from"> // Information about the source
        ...
      </reference>
      <attributes>
        <attribute>
          <name>FlowID</name>
          <value>1</value> // the FlowID
        </attribute>
      </attributes>
    </flow>
    ....
  </flows>
</answer>
```

To evaluate the precision of **X**, you have to decide if these 3 taint flows in **plain.xml** are true positives or false positives.

Your Task:

1. Start Visual Studio Code, disable the extension TB-Viewer in Visual Studio Code if you have it enabled. Restart Visual Studio Code.
2. In Visual Studio Code, click **File >> Open Workspace >> Select myworkspace.code-workspace** in the folder **save_me**. This folder contains the decompiled source code project. Java source code is located in the **src** folder.
3. Inspect the taint flows in **plain.xml** with the source code in Visual Studio Code.
4. Document your judgement with Yes or No for each flow in the spreadsheet.
https://docs.google.com/spreadsheets/d/1mZu835VaMUZhzGMLKIEJJwxV11vAGhKw_MS06Iq9jgw/edit?usp=sharing
5. **Tell me when you start!**
6. **Tell me when you finish!**