**CWE476 Null Pointer Dereference** Detections of Infer, SonarQube, and SpotBugs

—-------------------------------------------------------------------------------------------------

1. **Shared, Unique, and Missed True Positives**

—-----------------------------------------------------------------------

**106** are *shared* detections of all the tools, they are:

Name\_id to id= # Detections

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_01 to 17 = 17

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_01 to 17 = 17

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 1 to 11, 13 to 17, 31, 41= 18

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_1 tol 11, 13 to 17, 31, 41 = 18

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 1 to 11, 13 to 17, 31, 41= 18

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 1 to 11, 13 to 17, 31 41= 18

The test cases design

1: Baseline

2: Control flow: if(true) and if(false)

3: Control flow: if(5==5) and if(5!=5)

4: Control flow: if(PRIVATE\_STATIC\_FINAL\_TRUE) and if(PRIVATE\_STATIC\_FINAL\_FALSE)

5: Control flow: if(privateTrue) and if(privateFalse)

6: Control flow: if(PRIVATE\_STATIC\_FINAL\_FIVE==5) and if(PRIVATE\_STATIC\_FINAL\_FIVE!=5)

7: Control flow: if(privateFive==5) and if(privateFive!=5)

8: Control flow: if(privateReturnsTrue()) and if(privateReturnsFalse())

9: Control flow: if(IO.STATIC\_FINAL\_TRUE) and if(IO.STATIC\_FINAL\_FALSE)

10: Control flow: if(IO.staticTrue) and if(IO.staticFalse)

11: Control flow: if(IO.staticReturnsTrue()) and if(IO.staticReturnsFalse())

13: Control flow: if(IO.STATIC\_FINAL\_FIVE==5) and if(IO.STATIC\_FINAL\_FIVE!=5)

14: Control flow: if(IO.staticFive==5) and if(IO.staticFive!=5)

15: Control flow: switch(7)

16: Control flow: while(true)

17: Control flow: for loops

31: Data flow: make a copy of data within the same method

41: Data flow: data passed as an argument from one method to another in the same class

—-------------------------------------------------------------------------------------------------------

**25** are *unique* detections of Infer, these are:

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 22a,45,61a., **67a,\_68a,**74b =6

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_22a,45,61a., **67a,\_68a,**74b =6

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 22a,45,61a., **67a,\_68a,**74b ,81a =7

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 22a,45,61a., **67a,\_68a,**74b =6

22: Control flow: Flow controlled by the value of a public static variable. Sink functions are in a separate file from sources.

45: Data flow: data passed as a private class member variable from one function to another in the same class

61: Data flow: data returned from one method to another in different classes in the same package

67: Data flow: data passed in a class from one method to another in different source files in the same package

68: Data flow: data passed as a member variable in the "a" class, which is used by a method in another class in the same package

74: Data flow: data passed in a HashMap from one method to another in different source files in the same package

—---------------------------------------------------------------------------------------------------------------------------

**12** are *shared* detections of Infer and Sonar, these are:

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_12 \_21, \_42 = 3

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_12 \_21, \_42 = 3

CWE476\_NULL\_Pointer\_Dereference\_\_String\_12 \_21, \_42 = 3

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_12 \_21, \_42 = 3

12: Control flow: if(IO.staticReturnsTrueOrFalse())

21: Control flow: Flow controlled by the value of a private variable. All functions are contained in one file.

42: Data flow: data returned from one method to another in the same class

—--------------------------------------------------------------------------------------------------------------------

**23** are *shared* detections of Infer and SpotBugs, these are:

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_51a, \_52a., \_53a., \_54a, **\_71a**, \_81a =6

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_51a, \_52a., \_53a., \_54a, **\_71a**, \_81a =6

CWE476\_NULL\_Pointer\_Dereference\_\_String\_51a, \_52a., \_53a., \_54a, **\_71a**, =5

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_51a, \_52a., \_53a., \_54a, **\_71a**, \_81a =6

51: Data flow: data passed as an argument from one function to another in different classes in the same package

52: Data flow: data passed as an argument from one method to another to another in three different classes in the same package

53: Data flow: data passed as an argument from one method through two others to a fourth; all four functions are in different classes in the same package

54: Data flow: data passed as an argument from one method through three others to a fifth; all five functions are in different classes in the same package

71: Data flow: data passed as an Object reference argument from one method to another in different classes in the same package

81: Data flow: data passed in a parameter to an abstract method

—---------------------------------------------------------------------------------------------------------------------------

**15 test cases** were *missed* by Infer and all the tools, these are:

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ **72**, 73, 75, = 3

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_66, **72**, 73, 75, = 4

CWE476\_NULL\_Pointer\_Dereference\_\_String\_66, **72**, 73, 75, = 4

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_66, **72**, 73, 75, = 4

66: Data flow: data passed in an array from one method to another in different source files in the same package

72: Data flow: data passed in a Vector from one method to another in different source files in the same package

73: Data flow: data passed in a LinkedList from one method to another in different source files in the same package

75: Data flow: data passed in a serialized object from one method to another in different source files in the same package

1. **Shared, and Unique False Positives**

—-----------------------------------------------------------

**12 FP OF Infer**

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_**05** (line 74), 10 (line **67)**, 74b (line 40), = 3

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_**05** (line 74) , 10 (line **67**), 74b (line 40) = 3

CWE476\_NULL\_Pointer\_Dereference\_\_String\_**\_05** (line 74) , 10 (line **67**), 74b (line 40) = 3

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_**05**(line 74), 10 (line **67**), 74b (line 40) = 3

**80 FP OF Sonar**

**Integer, String, StringBuilder, and int\_array**

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_03(line 67, 90)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_04(line 74)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_**05**(line **74**)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_06(72,95)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_07(72,95)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_09( 67, 90)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_**10**(**67**, 90)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_11( 67, 91)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_13( 67, 90)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_14( 67, 90)

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_15(76,107)

**8 FP** are *shared* between Infer and Sonar, these are:

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_**05** (line 74), **10** (line **67)** = 2

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_**05** (line 74) , **10** (line **67**) = 2

CWE476\_NULL\_Pointer\_Dereference\_\_String\_**\_05** (line 74) , **10** (line **67**) = 2

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_**05**(line 74), **10** (line **67**) = 2

**For checking these test cases please find Java Test Cases of Juliet Test Suite here:** [**https://samate.nist.gov/SARD/test-suites**](https://samate.nist.gov/SARD/test-suites)