**Analyzing CWE476\_Null Pointer Dereference Test Cases of Juliet Test Suite by All The Tools**

1. **By Facebook Infer**

There are 2 checkers that target this weakness in Infer:

The first one is: biabduction -> NULL\_DEREFERENCE

The second one is : pulse -> NULLPTR\_DEREFERENCE

The first checker works by default

**Infer command:** ant clean

~/Downloads/infer/infer/bin/infer --pulse -- ant

**Results:**

| Positives | Negatives | Infer Detector name | #All Detections | # TP | # FP | # Duplicated detections |
| --- | --- | --- | --- | --- | --- | --- |
| 181 | 466 | pulse | 132 | 20 | 0 | 112 |
| biabduction | 158 | 146 | 12 | 0 |
| Total | 290 | 166 | 12 | 112 |

**The used command:**

~/Downloads/infer/infer/bin/infer --pulse -- ant

**Steps:**

ant clean

~/Downloads/infer/infer/bin/infer --pulse -- ant

cd infer-out/

grep "Null Dereference" report.txt > onlyNullDere.txt

cat onlyNullDere.txt | cut -d '.' -f 1 | sort | uniq -c | wc -l

168-2 = 166 -> TP detections

290-166 = 124

**For presenting them:**

cat onlyNullDere.txt | cut -d '.' -f 1 | sort | uniq -c

**—---------------------------------------------------------------------------------------------------------------------------**

**~/Downloads/infer/infer/bin/infer run -- ant =>** Null Dereference(NULL\_DEREFERENCE): 158

**TP Detected = 146**

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\_\_int\_array\_01 to 17 \_21, \_22a \_41 \_42 \_51a, \_52a., \_53a., \_54a, \_61a., \_74b \_81a = 28

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_01 to 17, \_21., \_22a, \_41, \_42, \_51a, \_52a, \_53a, \_54a, \_61a, \_74b, \_81a = 28

CWE476\_NULL\_Pointer\_Dereference\_\_String\_01 till 17, \_21., \_22a, \_41, \_42, \_51a, \_52a, \_53a, \_54a, \_61a, \_74b, \_81a = 28

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_01 till 17, \_21, \_22a, \_41, \_42, \_51a till \_54a, \_61a, \_74b, \_81a = 28

**FP Detected = 12**

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

**Missed Test cases: FN = 35**

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_31, 45, 67, 68, 71, 72, 73, 75, = 8

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 31, 45, 66, 67, 68, 71, 72, 73, 75, = 9

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 31, 45, 66, 67, 68, 71, 72, 73, 75, = 9

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_ 31, 45, 66. 67, 68, 71, 72, 73, 75, = 9

**Missed Test cases: but does not considered FN = 17**

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

**—---------------------------------------------------------------------------------------------------**

**~/Downloads/infer/infer/bin/infer --pulse -- ant = 290 detections**

**—----------------------------------------------------------------------------------------**

**TP Detected = 166**

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\_\_int\_array\_01 to 17 \_21, \_22a,\_**31,** \_41 \_42 , **45,** \_51a, \_52a., \_53a., \_54a, \_61a., **67a,\_68a,\_71a**, \_74b \_81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_01 to 17, \_21., \_22a, **31,** \_41, \_42, **45,** \_51a, \_52a, \_53a, \_54a, \_61a, \_**67a,\_68a,\_71a**,\_74b, \_81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_String\_01 till 17, \_21., \_22a, **31,** \_41, \_42,**45,** \_51a, \_52a, \_53a, \_54a, \_61a,\_**67a,\_68a,\_71a**, \_74b, \_81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_01 till 17, \_21., \_22a, **31,** \_41, \_42,**45,** \_51a, \_52a, \_53a, \_54a, \_61a,\_**67a,\_68a,\_71a**, \_74b, \_81a = 33

The highlighted are unique detections for Infer

**Duplicate TP detections = 112**

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 1 2 3 4 6 8 9 11 13 15 16 17 21 22a 41 42 51a 52a 53a 54a 61a 81a = 22

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_01,02,03,04,06,08,09,11, 13, 15,16,17 = 12

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_01,02,03,04,06,08,09,11, 13, 15,16,17 = 12

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 1 2 3 4 6 8 9 11 13 15 16 17 21 22a 41 42 51a 52a 53a 54a 61a 81a = 22

CWE476\_NULL\_Pointer\_Dereference\_\_String\_1 2 3 4 6 8 9 11 13 15 16 17 21 22a 41 42 51a 52a 53a 54a 61a 81a = 22

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_1 2 3 4 6 8 9 11 13 15 16 17 21 22a 41 42 51a 52a 53a 54a 61a 81a = 22

**FP Detected = 12**

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

**Missed Test cases: FN = 15**

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_72, 73, 75 = 3

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 72, 73, 75, = 3

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 66, 72, 73, 75, = 4

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_ 66., 72, 73, 75, = 4

**Missed Test cases: but does not considered FN = 17**

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

1. **By SonarQube**

There are 1 checkers that target this weakness in Sonar: Null pointers should not be dereferenced

**Sonar running command:** sonarqube-8.6.1.40680/bin/linux-x86-64/sonar.sh console

**Sonar analysis command :** sonar-scanner -Dsonar.projectKey=CWE476 -Dsonar.sources=$HOME/Juliet1.3Last/src/testcases/CWE476\_NULL\_Pointer\_Dereference -Dsonar.java.binaries=$HOME/Juliet1.3Last/src/testcases/CWE476\_NULL\_Pointer\_Dereference/antbuild/testcases/CWE476\_NULL\_Pointer\_Dereference -Dsonar.host.url=http://localhost:9000 -Dsonar.login=cd12b14274749caf2dd50d2e97b166b1cb31593a -X

**Results:**

| Positives | Negatives | #All Detections | # TP | # FP | # Duplicated detections |
| --- | --- | --- | --- | --- | --- |
| 181 | 466 | 188 | 118 | 80 | 0 |

**TP Detected = 118**

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 1 till 17 21 31 41 42 = 21

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_1 till 17 21 31 41 42 = 21

CWE476\_NULL\_Pointer\_Dereference\_\_String\_1 till 17 21 31 41 42 = 21

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 1 till 17 21 31 41 42 = 21

**FP Detected = 80**

A(b) -> A is the file ID, while b is the number of fp there

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 3(2), 4(1), 5(1), 6(2), 7(2),9(2),10(2),11(2), 13(2),14(2),15(2)= 20

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_3(2), 4(1), 5(1), 6(2), 7(2),9(2),10(2),11(2), 13(2),14(2),15(2)= 20

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 3(2), 4(1), 5(1), 6(2), 7(2),9(2),10(2),11(2), 13(2),14(2),15(2)= 20

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 3(2), 4(1), 5(1), 6(2), 7(2),9(2),10(2),11(2), 13(2),14(2),15(2)= 20

1. **By SpotBugs**

The following table contains different detections of Spotbugs in CWE476 of Juliet according to the priority level; High, high and normal, and all.

**Results:**

| Positives | Negatives | SpotBugs Priority | #All Detections | #TP | #FP | #Duplicate Detections |
| --- | --- | --- | --- | --- | --- | --- |
| 181 | 466 | high | 106 | 106 | 0 | 0 |
| High & normal | 129+17=146 | 129 | 0 | 17 |
| All | 129+445=574 |  |  |  |

Yellow : detections from Correctness checkers

Green : detections from style checkers

**SpotBugs(h)**

**—-------------**

106 TP:

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

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_ 1 till 11, 13 till 17, 31,41= 18

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

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_1 till 17 = 17 (without FP)

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

0 FP:

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

**SpotBugs(h&n)**

129 TP:

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 1 till 11, 13 till 17, 31,41,51a, 52a, 53a, 54a, 71a, 81a = 24

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_ 1 till 11, 13 till 17, 31,41,51a, 52a, 53a, 54a, 71a, 81a= 24

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 1 till 11, 13 till 17, 31,41, 51a, 52a, 53a, 54a, 71a= 23

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 1 till 11, 13 till 17, 31,41, 51a, 52a, 53a, 54a, 71a, 81a = 24

0 FP:

17 Duplicate detections:

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_1 till 17 = 17

**SpotBugs(all)**

129 TP:

37 TP:

Total = 166

CWE476\_NULL\_Pointer\_Dereference\_\_Integer\_ 1 till 11, 13 till 17, 21,22a,31,41,45.51a, 52a, 53a, 54a, 66a,67a,71a, 72,73,74,75,81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_StringBuilder\_ 1 till 11, 13 till 17, 21,22a,31,41,45.51a, 52a, 53a, 54a, 66a,67a,71a, 72,73,74,75,81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_String\_ 1 till 11, 13 till 17, 21,22a,31,41,45.51a, 52a, 53a, 54a, 66a,67a,71a, 72,73,74,75,81a = 33

CWE476\_NULL\_Pointer\_Dereference\_\_binary\_if\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_deref\_after\_check\_1 till 17 = 17 (without FP)

CWE476\_NULL\_Pointer\_Dereference\_\_int\_array\_ 1 till 11, 13 till 17, 21,22a,31,41,45.51a, 52a, 53a, 54a, 66a,67a,71a, 72,73,74,75,81a = 33

264 FP:

Duplicate detections: 24\*4 = 96 , 17 \* 2= 34 -> 96 + 34 = 130 - 1 = 129, there are also other 15 detections inside the bad() methods , these also considered as duplicate conditions . These are shown as test cases with 4 detections for each. -> Total = 129 + 15 = 144

TOTAL DETECTIONS = TP + FP + DUPLICATE

= 166 + 264 + 144

= 574