Results for SCA Tools
Using Java Juliet Test Cases

01/01/2018

Contents

1. Summary

Table1 summaries the number of flaws that each SCA tool successfully highlights, the number of flaws that each SCA tool fails to highlight, and the number of the fake warnings that each SCA tool emits. Additionally, Table1 shows the number of test cases / CWEs that were used to evaluate the SCA tools.

Table1. General Results for SCA Tools

Tools	**# of CWEs**	**True Positive (Detected Flaws)**	**False Negative (Undetected Flaws)**	**False Positive (Fake Flaws)**
Tool4	91	437	51579	108528
Tool5	91	323	46248	8729

2. Weaknesses (CWEs) Results

In this section the SCA tools evaluation results in the context of the software engineering metrics.

2.1. CWE-23: Relative Path Traversal

Table2. General Results for SCA Tools based on CWE-23

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1512	0	1512	0
Tool5	1512	19	1493	1226

2.2. CWE-369: Divide by Zero

Table3. General Results for SCA Tools based on CWE-369

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	8900	100	8800	213
Tool5	8900	53	8847	134

2.3. CWE-80: Basic XSS

Table4. General Results for SCA Tools based on CWE-80

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2268	0	2268	0
Tool5	2268	0	2268	293

2.4. CWE-81: XSS Error Message

Table5. General Results for SCA Tools based on CWE-81

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1134	0	1134	0
Tool5	1134	19	1115	137

2.5. CWE-83: Unlock Not Locked

Table6. General Results for SCA Tools based on CWE-83

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	3	0	3	0
Tool5	3	0	3	0

2.6. CWE-89: SQL Injection

Table7. General Results for SCA Tools based on CWE-89

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	10689	9	10680	95481
Tool5	10689	0	10689	0

2.7. CWE-90: LDAP Injection

Table8. General Results for SCA Tools based on CWE-90

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1512	0	1512	0
Tool5	1512	0	1512	158

2.8. CWE-113: HTTP Response Splitting

Table9. General Results for SCA Tools based on CWE-113

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	6408	0	6408	0
Tool5	6408	38	925	6370

2.9. CWE-134: Uncontrolled Format String

Table10. General Results for SCA Tools based on CWE-134

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	3204	0	3204	0
Tool5	3204	0	3204	0

2.10. CWE-190: Integer Overflow

Table11. General Results for SCA Tools based on CWE-190

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	12282	0	12282	0
Tool5	12282	0	12282	0

2.11. CWE-252: Unchecked Return Value

Table12. General Results for SCA Tools based on CWE-252

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	0	17	148
Tool5	17	0	17	0

2.12. CWE-253: Incorrect Check of Function Return Value

Table13. General Results for SCA Tools based on CWE-253

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	0	17	0
Tool5	17	0	17	0

2.13. CWE-256: Plaintext Storage of Password

Table14. General Results for SCA Tools based on CWE-256

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	178	0	178	0
Tool5	178	0	178	8

2.14. CWE-259: Hard Coded Password

Table15. General Results for SCA Tools based on CWE-259

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	540	0	540	0
Tool5	540	0	540	0

2.15. CWE-382: Use of System Exit

Table16. General Results for SCA Tools based on CWE-382

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	34	34	0	204
Tool5	34	17	17	2

2.16. CWE-383: Direct Use of Threads

Table17. General Results for SCA Tools based on CWE-383

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	16	16	0	97
Tool5	16	0	16	0

2.17. CWE-390: Error Without Action

Table18. General Results for SCA Tools based on CWE-390

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	34	17	17	880
Tool5	34	0	34	0

2.18. CWE-396: Catch Generic Exception

Table19. General Results for SCA Tools based on CWE-396

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	34	17	17	164
Tool5	34	0	34	8

2.19. CWE-398: Poor Code Quality

Table20. General Results for SCA Tools based on CWE-398

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	137	0	137	0
Tool5	137	0	137	0

2.20. CWE-404: Improper Resource Shutdown or Release

Table21. General Results for SCA Tools based on CWE-404

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	5	0	5	39
Tool5	5	1	4	7

2.21. CWE-476: NULL Pointer Dereference

Table22. General Results for SCA Tools based on CWE-476

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	759	0	759	0
Tool5	759	102	657	316

2.22. CWE-478: Missing Default Case in Switch

Table23. General Results for SCA Tools based on CWE-478

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	17	0	347
Tool5	17	17	0	1

2.23. CWE-481: Assigning instead of Comparing

Table24. General Results for SCA Tools based on CWE-481

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	0	17	0
Tool5	17	0	17	0

2.24. CWE-483: Incorrect Block Delimitation

Table25. General Results for SCA Tools based on CWE-483

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	19	19	0	329
Tool5	19	0	19	0

2.25. CWE-484: Omitted Break Statement in Switch

Table26. General Results for SCA Tools based on CWE-484

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	17	0	191
Tool5	17	17	0	1

2.26. CWE-486: Comparison of Classes by Name

Table27. General Results for SCA Tools based on CWE-486

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	0	17	0
Tool5	17	0	17	0

2.27. CWE-500: Public Static Field Not Marked Final

Table28. General Results for SCA Tools based on CWE-500

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1	0	1	5
Tool5	1	1	0	0

2.28. CWE-561: Dead Code

Table29. General Results for SCA Tools based on CWE-561

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1	0	1	0
Tool5	1	0	1	0

2.29. CWE-563: Unused Variable

Table30. General Results for SCA Tools based on CWE-563

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	932	130	802	2941
Tool5	932	1	931	57

2.30. CWE-568: Finalize Without Super

Table31. General Results for SCA Tools based on CWE-568

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2	2	0	40
Tool5	2	1	1	1

2.31. CWE-570: Expression Always False

Table32. General Results for SCA Tools based on CWE-570

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	16	1	15	66
Tool5	16	0	16	3

2.32. CWE-571: Expression Always True

Table33. General Results for SCA Tools based on CWE-571

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	16	0	16	0
Tool5	16	0	16	2

2.33. CWE-572: Call to Thread run Instead of start

Table34. General Results for SCA Tools based on CWE-572

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	17	0	174
Tool5	17	17	0	0

2.34. CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session

Table35. General Results for SCA Tools based on CWE-579

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1	0	1	0
Tool5	1	0	1	1

2.35. CWE-580: Clone() Method Without Super.clone()

Table36. General Results for SCA Tools based on CWE-580

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1	1	0	10
Tool5	1	0	1	0

2.36. CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined

Table37. General Results for SCA Tools based on CWE-581

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2	2	0	36
Tool5	2	1	1	0

2.37. CWE-584: Return Inside Finally Block

Table38. General Results for SCA Tools based on CWE-584

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	17	0	90
Tool5	17	0	17	0

2.38. CWE-585: Empty Synchronized Block

Table39. General Results for SCA Tools based on CWE-585

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2	2	0	18
Tool5	2	2	0	0

2.39. CWE-586: Explicit Call to Finalize( )

Table40. General Results for SCA Tools based on CWE-586

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	17	0	196
Tool5	17	17	0	1

2.40. CWE-597: Wrong Operator String Comparison

Table41. General Results for SCA Tools based on CWE-597

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	17	0	17	0
Tool5	17	0	17	0

2.41. CWE-601: Open Redirect

Table42. General Results for SCA Tools based on CWE-601

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1134	0	1134	6847
Tool5	1134	0	1134	0

2.42. CWE-609: Double Checked Locking

Table43. General Results for SCA Tools based on CWE-609

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2	2	0	12
Tool5	2	0	2	2

2.43. CWE-674: Uncontrolled Recursion

Table44. General Results for SCA Tools based on CWE-674

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	2	0	2	0
Tool5	2	0	2	0

2.44. CWE-681: Incorrect Conversion Between Numeric Types

Table45. General Results for SCA Tools based on CWE-681

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	51	0	51	0
Tool5	51	0	51	0

2.45. CWE-832: Unlock Not Locked

Table46. General Results for SCA Tools based on CWE-832

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	3	0	3	0
Tool5	3	0	3	1

2.46. CWE-833: Deadlock

Table47. General Results for SCA Tools based on CWE-833

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	6	0	6	0
Tool5	6	0	6	0

2.47. CWE-835: Infinite Loop

Table48. General Results for SCA Tools based on CWE-835

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	6	0	6	0
Tool5	6	0	6	0

2.48. CWE-762: Mismatched Memory Management Routines

Table48. General Results for SCA Tools based on CWE-762

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool4	1787	0	1787	0
Tool5	1787	0	1787	0

- We evaluated both Tool4 and Tool5 using the rest of the CWEs and the True Positive and False Positive rates were zero.

Appendix A

Software Engineering Metrics

The software engineering metrics that were used in this research in order to evaluate the SCA tools, will be illustrated.

- **CountInput (aka FANIN).** Software engineering metric measures the number of calling subprograms plus global variables read.
- **Countline (aka NL).** Software engineering metric counts the number of all lines in the function.
- **CountLineBlank (aka BLOC).** Software engineering metric counts the number of blank lines in the function.
- **CountLineCode (aka LOC).** Software engineering metric counts the number of lines containing source code in the function.
- **CountLineCodeDecl.** Software engineering metric counts the number of lines containing declarative source code.
- **CountLineCodeExe.** Software engineering metric counts the number of lines containing executable source code.
- **CountLineComment (aka CLOC).** Software engineering metric counts the number of lines containing comment.
- **CountLineInactive.** Software engineering metric counts the number of inactive lines.
- **CountLinePreprocessor.** Software engineering metric counts the number of preprocessor lines.
- **CountSemicolon.** Software engineering metric counts the number of semicolons.
- **CountStmt.** Software engineering metric counts the number of statements.
- **CountStmtDecl.** Software engineering metric counts the number of Declarative Statements.
- **CountStmtEmpty.** Software engineering metric counts the number of Empty statements.
- **CountStmtExe.** Software engineering metric counts the number of executable statements.
- **CountPath (aka NPATH).** Software engineering metric counts the number of possible paths, not counting abnormal exits or goto(s).
- **Cyclomatic.** Software engineering metric measures the Cyclomatic Complexity.
- **CyclomaticModified.** Software engineering metric measures the Modified Cyclomatic Complexity.
- **CyclomaticStrict.** Software engineering metric measures the Strict Cyclomatic Complexity.
- **Essential (aka Essential Complexity, EV (G)).**
- **Knots.** Software engineering metric measures of overlapping jumps.
- **MaxNesting.** Software engineering metric measures the maximum nesting level of control constructs.
- **RatioCommentToCode.** Software engineering metric measures the Ratio of Comment lines to code lines.
- **CountOutput (aka FANOUT).** Software engineering metric measures the number of called subprograms plus global variables set.
- **CountPathLog.**