Results for SCA Tools
Using C++\C 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)**
Tool1	91	3015	181435	11740
Tool2	91	39297	145198	167566
Tool3	91	26663	157832	18325

2. Weaknesses (CWEs) Results

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

2.1. CWE-124:Buffer Underwrite ('Buffer Underflow')

Table2. General Results for SCA Tools based on CWE-124

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	5088	0	5088	1312
Tool2	5088	1223	3865	2198
Tool3	5088	260	4828	1420

2.2. CWE-126: Buffer Over-read

Table3. General Results for SCA Tools based on CWE-126

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	3867	20	3847	179
Tool2	3867	487	3380	2652
Tool3	3867	74	3793	2312

2.3. CWE-134: Uncontrolled Format String

Table4. 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)
Tool1	5530	4	5526	870
Tool2	5530	1	5529	15697
Tool3	5530	756	4774	712

2.4. CWE-36: Absolute Path Traversal

Table5. General Results for SCA Tools based on CWE-36

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	1870	0	1870	0
Tool2	1870	1	1869	20
Tool3	1870	0	1870	0

2.5. CWE-773: Missing Reference to Active File Descriptor or Handle

Table6. General Results for SCA Tools based on CWE-773

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	5530	4	5526	870
Tool2	5530	1	5529	15697
Tool3	5530	756	4774	712

2.6. CWE-775: Missing Release File Descriptor/Handle after Effective Lifetime

Table7. General Results for SCA Tools based on CWE-775

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	570	0	570	44
Tool2	570	46	524	53
Tool3	570	75	495	110

2.7. CWE-606: Unchecked Input for Loop Condition

Table8. General Results for SCA Tools based on CWE-606

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	1390	0	1390	0
Tool2	1390	1	1389	0
Tool3	1390	90	1300	746

2.8. CWE-605: Multiple Binds to the Same Port

Table9. General Results for SCA Tools based on CWE-605

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	1	48	0
Tool3	49	0	49	0

2.9. CWE-570: Expression is Always False

Table10. 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)
Tool1	6	0	6	0
Tool2	6	3	3	42
Tool3	6	2	4	3

2.10. CWE-478: Missing Default Case in Switch Statement

Table11. 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)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.11. CWE-685: Function Call With Incorrect Number of Arguments

Table12. General Results for SCA Tools based on CWE-685

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	18	31	0
Tool2	49	0	49	0
Tool3	49	19	30	10

2.12. CWE-123: Write-what-where Condition

Table13. General Results for SCA Tools based on CWE-123

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	561	0	561	0
Tool2	561	3	558	11
Tool3	561	3	558	0

2.13. CWE-122: Heap-based Buffer Overflow

Table14. General Results for SCA Tools based on CWE-122

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	15176	0	15176	847
Tool2	15176	4252	10924	14
Tool3	15176	794	14382	32

2.14. CWE-680:Integer Overflow to Buffer Overflow

Table15. General Results for SCA Tools based on CWE-680

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	2136	0	2136	38
Tool2	2136	620	1516	1
Tool3	2136	87	2049	100

2.15. CWE-121: Stack-based Buffer Overflow

Table16. General Results for SCA Tools based on CWE-121

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	13585	0	13585	1313
Tool2	13585	2269	11316	
Tool3	13585	593	12992	0

2.16. CWE-476: NULL Pointer Dereference

Table17. 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)
Tool1	1334	37	1297	163
Tool2	1334	352	982	146
Tool3	1334	180	1154	334

2.17. CWE-127: Buffer Under-read

Table18. General Results for SCA Tools based on CWE-127

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	5088	0	5088	1223
Tool2	5088	1223	3865	21018
Tool3	5088	444	4644	0

2.18. CWE-480: Use of Incorrect Operator

Table19. General Results for SCA Tools based on CWE-480

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	20	29	6
Tool3	49	22	27	98

2.19. CWE-481: Assigning instead of Comapring

Table20. 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)
Tool1	49	0	49	0
Tool2	49	1	48	0
Tool3	49	19	30	0

2.20. CWE-482: Comparing instead of Assigning

Table21. General Results for SCA Tools based on CWE-482

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	21	28	30

2.21. CWE-483: Incorrect Block Delimitation

Table22. 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)
Tool1	51	0	51	1
Tool2	51	22	29	10
Tool3	51	21	30	98

2.22. CWE-484: Omitted Break Statement in Switch

Table23. 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)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.23. CWE-489: Leftover Debug Code

Table24. General Results for SCA Tools based on CWE-489

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.24. CWE-761: Free of Pointer not at Start of Buffer

Table25. General Results for SCA Tools based on CWE-761

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	1110	1	1109	212
Tool2	1110	338	772	4797
Tool3	1110	1	1109	21

2.25. CWE-762: Mismatched Memory Management Routines

Table26. 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)
Tool1	19104	1607	17497	16
Tool2	19104	18510	594	41794
Tool3	19104	17721	1383	231

2.26. CWE-617: Reachable Assertion

Table27. General Results for SCA Tools based on CWE-617

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	1173	0	1173	38
Tool2	1173	52	1119	1
Tool3	1173	24	1147	51

2.27. CWE-563: Unused Variable

Table28. 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)
Tool1	1742	0	1742	96
Tool2	1742	115	1627	2324
Tool3	1742	1	1741	0

2.28. CWE-562: Return of Stack Variable Address

Table29. General Results for SCA Tools based on CWE-562

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	3	0	3	0
Tool2	3	3	0	0
Tool3	3	1	2	0

2.29. CWE-561: Dead Code

Table30. 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)
Tool1	1	0	1	0
Tool2	1	0	1	0
Tool3	1	1	0	0

2.30. CWE-560: Use of umask() with chmod-style Argument

Table31. General Results for SCA Tools based on CWE-560

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	1	48	0

2.31. CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')

Table32. General Results for SCA Tools based on CWE-400

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	2780	0	2780	276
Tool2	2780	264	2516	7658
Tool3	2780	101	2679	874

2.32. CWE-401: Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Table33. General Results for SCA Tools based on CWE-401

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	7741	180	7522	219
Tool2	7741	643	7098	20639
Tool3	7741	277	7464	1568

2.33. CWE-404: Improper Resource Shutdown or Release

Table34. 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)
Tool1	555	0	555	66
Tool2	555	0	555	0
Tool3	555	123	432	0

2.34. CWE-196: Unsigned to Signed Conversion Error

Table35. General Results for SCA Tools based on CWE-196

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.35. CWE-197: Numeric Truncation Error

Table36. General Results for SCA Tools based on CWE-197

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	3366	0	3366	114
Tool2	3366	494	2872	121
Tool3	3366	72	3294	153

2.36. CWE-194: Unexpected Sign Extension

Table37. General Results for SCA Tools based on CWE-194

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	4488	0	4488	170
Tool2	4488	407	4081	0
Tool3	4488	172	4316	1952

2.37. CWE-195: Signed to Unsigned Conversion Error

Table38. General Results for SCA Tools based on CWE-195

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	4488	100	4388	170
Tool2	4488	407	4081	0
Tool3	4488	172	4316	2036

2.38. CWE-190: Integer Overflow or Wraparound

Table39. 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)
Tool1	15012	135	14877	276
Tool2	15012	895	14117	0
Tool3	15012	532	14480	1746

2.39. CWE-191: Integer Underflow(Wrap or Wraparound)

Table40. General Results for SCA Tools based on CWE-191

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	9174	75	9099	184
Tool2	9174	553	8621	0
Tool3	9174	322	8852	0

2.40. CWE-416: Use After Free

Table41. General Results for SCA Tools based on CWE-416

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	2505	0	2505	293
Tool2	2505	189	2316	5151
Tool3	2505	155	2350	210

2.41. CWE-415: Double Free

Table42. General Results for SCA Tools based on CWE-415

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	3704	307	3397	114
Tool2	3704	724	2980	10355
Tool3	3704	428	3276	136

2.42. CWE-665: Improper Initialization

Table43. General Results for SCA Tools based on CWE-665

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	374	0	374	0
Tool2	374	106	268	0
Tool3	374	0	374	0

2.43. CWE-666: Operation on Resource in Wrong Phase of Lifetime

Table44. General Results for SCA Tools based on CWE-666

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	245	0	245	0
Tool2	245	0	245	750
Tool3	245	0	245	0

2.44. CWE-188: Reliance on Data/Memory Layout

Table45. General Results for SCA Tools based on CWE-188

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	98	0	98	0
Tool2	98	1	97	0
Tool3	98	0	98	34

2.45. CWE-789: Uncontrolled Memory Allocation

Table46. General Results for SCA Tools based on CWE-789

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	2690	0	2690	184
Tool2	2690	884	1806	10814
Tool3	2690	108	2582	10

2.46. CWE-690: Unchecked Return Value to NULL Pointer Dereference

Table47. General Results for SCA Tools based on CWE-690

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	2590	0	2590	212
Tool2	2590	0	2590	0
Tool3	2590	28	2562	0

2.47. CWE-426: Untrusted Search Path

Table48. General Results for SCA Tools based on CWE-426

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	374	0	374	0
Tool2	374	228	146	1138
Tool3	374	1	373	0

2.48. CWE-427: Uncontrolled Search Path Element

Table49. General Results for SCA Tools based on CWE-427

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	935	0	935	0
Tool2	935	1	934	0
Tool3	935	11	924	8

2.49. CWE-835: Infinite Loop

Table50. 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)
Tool1	6	0	6	0
Tool2	6	3	3	3
Tool3	6	0	6	1

2.50. CWE-479: Single Handler Use of a Non-reentrant Function

Table51. General Results for SCA Tools based on CWE-479

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	19	0	19	0
Tool2	19	0	19	0
Tool3	19	0	19	2

2.51. CWE-832: Unlock a Resource that is not Locked

Table52. 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)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	1

2.52. CWE-571: Expression is Always True

Table53. 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)
Tool1	6	0	6	0
Tool2	6	3	3	43
Tool3	6	3	3	0

2.53. CWE-672: Operation on a Resource after Expiration or Release

Table54. General Results for SCA Tools based on CWE-672

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	252	0	252	0
Tool2	252	68	184	949
Tool3	252	2	250	1

2.54. CWE-547: Use of Hard-coded, Security-relevant Constants

Table55. General Results for SCA Tools based on CWE-547

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	1	48	0
Tool3	49	0	49	0

2.55. CWE-546: Suspicious Comment

Table56. General Results for SCA Tools based on CWE-546

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	245	0	245	0
Tool2	245	0	245	0
Tool3	245	1	244	21

2.56. CWE-676: Use of Potentially Dangerous Function

Table57. General Results for SCA Tools based on CWE-676

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.57. CWE-675: Duplicate Operations on Resource

Table58. General Results for SCA Tools based on CWE-675

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	834	0	834	63
Tool2	834	207	627	1685
Tool3	834	69	765	0

2.58. CWE-674: Uncontrolled Recursion

Table59. 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)
Tool1	38	0	38	0
Tool2	38	2	36	10
Tool3	38	0	38	1

2.59. CWE-475: Undefined Behavior for Inout to API

Table60. General Results for SCA Tools based on CWE-475

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	2

2.60. CWE-377: Insecure Temporary File

Table61. General Results for SCA Tools based on CWE-377

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	147	0	147	0
Tool2	147	0	147	301
Tool3	147	0	147	0

2.61. CWE-374: Mutable Objects Passes by Reference

Table62. General Results for SCA Tools based on CWE-374

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.62. CWE-688: Function Call With Incorrect Variable or Reference as Argument

Table63. General Results for SCA Tools based on CWE-688

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	19	30	0
Tool3	49	19	30	4

2.63. CWE-242: Use of Inherently Dangerous Function

Table64. General Results for SCA Tools based on CWE-242

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.64. CWE-369: Divide By Zero

Table65. 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)
Tool1	5004	280	4724	184
Tool2	5004	894	4110	1106
Tool3	5004	528	4476	438

2.65. CWE-364: Single Handler Race Condition

Table66. General Results for SCA Tools based on CWE-364

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.66. CWE-367:Time-of-check Time-of-use (TOC TOU) Race Condition

Table67. General Results for SCA Tools based on CWE-367

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	98	0	98	102
Tool2	98	1	97	307
Tool3	98	0	98	0

2.67. CWE-366: Race Condition within a Thread

Table68. General Results for SCA Tools based on CWE-366

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	38	0	38	0
Tool2	38	0	38	0
Tool3	38	0	38	0

2.68. CWE-390: Detection of Error Condition Without Action

Table69. 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)
Tool1	196	0	196	0
Tool2	196	42	154	0
Tool3	196	2	194	5

2.69. CWE-391: Unchecked Error Condition

Table70. General Results for SCA Tools based on CWE-391

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	147	0	147	0
Tool2	147	0	147	0
Tool3	147	0	147	0

2.70. CWE-392: Failure to Report Error in Status Code

Table71. General Results for SCA Tools based on CWE-392

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	38	0	30	0
Tool2	38	2	36	0
Tool3	38	0	38	1

2.71. CWE-396: Declaration of Catch for Generic Exception

Table72. 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)
Tool1	147	0	147	0
Tool2	147	0	147	0
Tool3	147	0	147	0

2.72. CWE-397: Declaration of Throws for Generic Exception

Table73. General Results for SCA Tools based on CWE-397

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.73. CWE-398: Indicator of Poor Code Quality

Table74. 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)
Tool1	246	0	246	0
Tool2	246	0	246	0
Tool3	246	38	208	13

2.74. CWE-252: Unchecked Return Value

Table75. 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)
Tool1	735	0	735	0
Tool2	735	61	674	0
Tool3	735	10	725	61

2.75. CWE-78: OS Command Injection

Table76. General Results for SCA Tools based on CWE-78

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	3740	0	3740	0
Tool2	3740	946	2794	0
Tool3	3740	44	3696	21

2.76. CWE-590: Free of Memory not on the Heap

Table77. General Results for SCA Tools based on CWE-590

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	8110	247	7863	380
Tool2	8110	907	7203	0
Tool3	8110	52	8058	180

2.77. CWE-510: Trapdoor

Table78. General Results for SCA Tools based on CWE-510

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	190	0	190	0
Tool2	190	0	190	0
Tool3	190	0	190	0

2.78. CWE-511: Login/Time Bomb

Table79. General Results for SCA Tools based on CWE-511

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	147	0	147	0
Tool2	147	4	143	0
Tool3	147	147	0	0

2.79. CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior

Table80. General Results for SCA Tools based on CWE-758

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	1275	0	1275	324
Tool2	1275	1	1274	0
Tool3	1275	0	1275	0

2.80. CWE-304: Missing Critical Step in Authentication

Table81. General Results for SCA Tools based on CWE-304

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	49	0	12
Tool3	49	0	49	0

2.81. CWE-457: Use of Uninitialized Variable

Table82. General Results for SCA Tools based on CWE-457

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	7022	0	7022	1173
Tool2	7022	564	6458	18
Tool3	7022	360	6662	759

2.82. CWE-459: Incomplete Cleanup

Table83. General Results for SCA Tools based on CWE-459

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.83. CWE-588: Attempt to Access Child of a Non-structure Pointer

Table84. General Results for SCA Tools based on CWE-588

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	317	0	317	14
Tool2	317	48	269	0
Tool3	317	3	314	32

2.84. CWE-23: Relative Path Traversal

Table85. 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)
Tool1	1870	0	1870	0
Tool2	1870	1	1869	0
Tool3	1870	0	1870	0

2.85. CWE-587: Assignment of a Fixed Address to a Pointer

Table86. General Results for SCA Tools based on CWE-587

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	1	48	0
Tool3	49	0	49	0

2.86. CWE-506: Embedded Malicious Code

Table87. General Results for SCA Tools based on CWE-506

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	92	0	92	0
Tool2	92	2	90	0
Tool3	92	0	92	1

2.87. CWE-468: Incorrect Pointer Scaling

Table88. General Results for SCA Tools based on CWE-468

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	99	0	99	0
Tool2	99	21	78	0
Tool3	99	22	77	13

2.88. CWE-469: Public Data Assigned to Private Array-Typed Field

Table89. General Results for SCA Tools based on CWE-469

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	49	0	49	0
Tool2	49	0	49	0
Tool3	49	0	49	0

2.89. CWE-134: Uncontrolled Format String

Table90. 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)
Tool1	5530	0	5530	0
Tool2	5530	15	5515	25
Tool3	5530	756	4774	712

2.90. CWE-467: Use of sizeof() on a Pointer Type

Table91. General Results for SCA Tools based on CWE-467

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	561	0	561	0
Tool2	561	48	513	0
Tool3	561	139	422	309

2.91. CWE-464: Addition of Data Structure Sentinel

Table92. General Results for SCA Tools based on CWE-464

Tools	Actual # of Flaws in test cases	True Positive (Detected Flaws)	False Negative (Undetected Flaws)	False Positive (Fake Flaws)
Tool1	187	0	187	0
Tool2	187	47	140	0
Tool3	187	0	187	0

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.**