DEPARTAMENTO DE
ENGENHARIA INFORMÁTICA
FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA

Departamento de Engenharia Informática
Faculdade de Ciências e Tecnologia
Universidade de Coimbra

Performance Results Tables "Evaluation of static analysis tools in detecting the OWASP Top 10 vulnerabilities"

Inês Martins Marçal

Dissertation in the context of the Masters in Informatics Security,
advised by Professor Marcos Vieira and Professor Bruno Sousa and
presented to the Department of Informatics Engineering
of the Faculty of Sciences and Technology of the University of Coimbra.

September 2024

Contents

Glossary

FN False Negative. 6

FP False Positive. 4, 6, 43

OWASP Open Worldwide Application Security Project. 3, 4, 6, 19

SAST Static Application Security Testing. 3, 4, 6, 16, 19, 43

TN True Negative. 6

TP True Positive. 6, 43

Chapter 1

Introduction

The purpose of this document is to complement and provide better insight into the conclusions drawn in the section 'Benchmark results' of the thesis "Evaluation of static analysis tools in detecting the Open Worldwide Application Security Project (OWASP) Top 10 vulnerabilities" and in the article called "A Benchmarking Methodology for Application Security Testing". In it, the following details are outlined:

- Characterization of the workload in terms of number of instances;
- Results achieved individually by the Static Application Security Testing (SAST) tools in each web application;
- Results achieved by the SAST tools combinations of 2 and 3 in each web application;
- Results obtained from combinations of two tools per vulnerability, based on the newly developed SAST tool combination strategy with assigned weights;
- Agreement between pairs of tools

Chapter 2

Characterization of the workload

The following tables, tables 2.1 and 2.2, illustrate the vulnerable and non-vulnerable instances of the various projects that compose the workload concerning the vulnerabilities selected within each OWASP Top 10 category. It should be noted that the third column called NN corresponds to the occurrences in the SAST tools output that have been classified as False Positive (FP)s, but which nevertheless do not fall within the non-vulnerable classification of the category in which they were identified.

Vulnerability	WebGoat			Juice Shop			Mutillidae			OWASP Bench.			Juliet T. Suite		
	P	N	NN	P	N	NN	P	N	NN	P	N	NN	P	N	NN
A01: Broken Access Control															
Bypassing authorization	5	0	0	10	1	0	1	2	0	0	0	0	233	372	1535
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	17	30	0
Path Traversal	9	4	11	11	3	0	7	9	0	133	135	879	230	378	0
Cross-site Request Forgery	1	7	0	1	46	0	18	4	2	0	0	0	0	0	0
A02: Cryptographic Failures															
Use of Old/Insecure algorithms	14	3	0	5	1	0	10	0	0	130	116	0	34	60	494
Deprecated Hash Functions	5	2	3	8	3	0	5	2	7	129	107	0	51	90	0
Use of Weak PRNG	16	2	0	5	1	0	11	0	0	218	275	0	34	60	17
Seeds Hard-Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	17	30	0
A03: Injection															
Command Injection	0	0	0	0	0	0	9	6	0	126	125	0	252	411	0
SQL Injection	15	10	2	47	25	0	19	7	0	272	232	236	260	863	223
LDAP Injection	0	0	0	0	0	0	1	0	0	27	32	0	265	433	0
Cross-site Scripting	31	6	20	15	1	1	107	75	2	246	209	1023	196	323	44
XPath Injection	0	0	0	0	0	0	2	0	0	15	20	0	263	850	0
HTTP Response Splitting	2	4	13	0	0	0	0	4	0	0	0	0	389	1266	115
A04: Insecure Design															
Improper Error Handling	84	51	0	4	32	0	104	0	0	185	6377	0	90	155	2063
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	11	3	0	0	0	0	110	45	0	83	43	493	0	0	0
A05: Security Misconfiguration															
XML External Entities	4	0	0	1	0	0	2	2	0	0	0	0	0	0	0
Bad Programming of Cookies	17	3	0	32	0	0	24	24	0	1536	1516	0	17	30	0
Insecure Use of Hard-Coded Constants	13	0	0	3	0	5	2	3	2	0	0	0	37	52	0
A06: Vulnerable and Outdated Components															
Vulnerable Third-party components	6	0	0	13	0	0	2	0	0	0	0	0	68	120	364
A07: Identification and Authentication Failures															
Bypassing authentication	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0
Hard-coded credentials	26	1	5	0	0	2	3	2	12	0	0	0	111	156	75
A08: Software and data integrity failures															
Insecure Deserialization	3	1	0	1	1	0	1	0	0	0	0	0	0	0	0
A09: Security Logging and Monitoring Failures															
Improper Output Neutralization for Logs	96	143	2	11	23	0	102	0	5	0	0	0	51	90	53
A10: Server-side Request Forgery															
Server-side Request Forgery	4	0	4	1	0	0	11	0	1	0	0	0	0	0	0

Table 2.1: Vulnerabilities present in the testing web applications

Vulnerability	Piwigo			Shopizer Shop			PeerTube			Metafresh		
	P	N	NN	P	N	NN	P	N	NN	P	N	NN
A01: Broken Access Control												
Bypassing authorization	0	9	0	0	2	0	0	16	6	0	0	1
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	0	110	0	6	3	33	4	55	81	1	34	2
Cross-site Request Forgery	57	25	0	4	0	0	194	0	0	3	0	0
A02: Cryptographic Failures												
Use of Old/Insecure algorithms	4	0	1	3	0	0	0	0	0	28	0	0
Deprecated Hash Functions	41	8	0	7	10	2	4	1	0	126	4	14
Use of Weak PRNG	9	1	0	0	0	0	2	3	0	16	0	0
Seeds Hard-Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0
A03: Injection												
Command Injection	0	15	0	0	0	0	0	7	0	0	5	0
SQL Injection	2	5	1	0	11	0	0	19	0	0	262	217
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0
Cross-site Scripting	11	32	15	0	316	6	0	28	1	7	223	21
XPath Injection	0	0	0	0	0	0	0	0	0	0	3	0
HTTP Response Splitting	1	11	0	3	0	17	0	0	0	0	7	1
A04: Insecure Design												
Improper Error Handling	17	0	0	289	260	0	0	0	0	112	71	0
Trust Boundary Violation	0	13	0	0	5	0	0	0	0	0	0	0
Method Tampering	27	0	0	0	0	0	0	0	0	1	0	0
A05: Security Misconfiguration												
XML External Entities	1	1	0	0	0	0	0	0	0	2	22	0
Bad Programming of Cookies	28	7	0	0	0	0	3	1	0	8	0	0
Insecure Use of Hard-Coded Constants	0	0	0	2	0	0	3	0	2	2	0	0
A06: Vulnerable and Outdated Components												
Vulnerable Third-party components	4	2	0	0	5	0	194	0	0	1	0	0
A07: Identification and Authentication Failures												
Bypassing authentication	0	0	0	0	0	0	0	0	0	0	0	0
Hard-coded credentials	0	0	5	0	0	51	0	0	43	4	4	73
A08: Software and data integrity failures												
Insecure Deserialization	1	25	0	0	0	0	0	0	0	1	4	1
A09: Security Logging and Monitoring Failures												
Insertion of Sensitive Information into Log File	0	0	0	0	0	0	0	0	0	0	0	0
Improper Output Neutralization for Logs	16	35	4	187	97	0	0	0	0	274	370	51
A10: Server-side Request Forgery												
Server-side Request Forgery	0	20	3	0	4	0	1	6	0	0	0	0

Table 2.2: Vulnerabilities present in the real open-source web applications

Chapter 3

Performance results for all SAST Tools

This section covers the accomplishment of the SAST tools results stage as part of the stipulated benchmarking methodology. The outputs of the SAST tools have been classified into True Positive (TP), FP, True Negative (TN) and False Negative (FN) within the scope of the issues contained in each web application or test cases that compose the workload. The detection capacity demonstrated by the SAST tools in identifying the vulnerabilities covered by the OWASP Top 10, among the various vulnerable and non-vulnerable instances contained in the workload, is detailed below, with each set of two tables referring to the same test component included in the latter. As the key conclusions drawn from the analysis of the results obtained have already been highlighted in section 5.1.1.1, providing these tables constitutes a reference to the observations made.

Results obtained in WebGoat

Vulnerability				Tools															
Name	Total			Snyk				Fortify				Semgrep				SpotBugs			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	5	0	0	0	5	0	0	0	5	0	0	0	5	0	0	0	5	0	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	9	4	11	6	3	0	15	1	8	0	15	4	5	0	15	6	3	10	5
Cross-Site Request Forgery	1	7	0	1	0	0	7	0	1	0	7	1	0	5	2	1	0	5	2
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	14	3	0	0	14	0	3	0	14	0	3	0	14	0	3	0	14	0	3
Deprecated Hash Functions	5	2	3	1	4	0	5	1	4	0	5	1	4	0	5	1	4	0	5
Use of Weak PRNG	16	2	0	5	11	0	2	11	5	0	2	6	10	0	2	11	5	0	2
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	15	10	2	15	0	0	12	15	0	0	12	14	1	0	12	15	0	0	12
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	31	6	20	10	21	2	24	0	31	0	26	18	13	5	21	0	31	0	26
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	2	4	13	1	1	1	16	0	2	0	17	0	2	0	17	0	2	13	4
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	84	51	0	0	84	0	51	39	45	0	51	0	84	0	51	0	84	0	51
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	11	3	0	0	11	0	3	0	11	0	3	0	11	0	3	0	11	0	3
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	4	0	0	2	2	0	0	0	4	0	0	0	4	0	0	1	3	0	0
Bad Programming of Cookies	17	3	0	0	17	0	3	0	17	0	3	13	4	0	3	0	17	0	3
Insecure Use of Hard Coded Constants	13	0	0	13	0	0	0	4	9	0	0	0	13	0	0	0	13	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	6	0	0	0	6	0	0	0	6	0	0	1	5	0	0	0	6	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
Hard Coded Credentials	26	1	5	18	8	1	5	7	19	0	6	0	26	0	6	2	24	1	5
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	3	1	0	2	1	0	1	0	3	0	1	2	1	0	1	2	1	0	1
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	96	143	2	0	96	0	145	9	87	0	145	4	92	0	145	9	87	3	142
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	4	0	4	1	3	0	4	0	4	0	4	3	1	0	4	1	3	0	4

Table 3.1: SAST tools output in relation to the WebGoat - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	5	0	0	0	5	0	0	0	5	0	0	0	5	0	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	9	4	11	6	3	0	15	6	3	1	14	0	9	0	15
Cross-Site Request Forgery	1	7	0	1	0	0	7	1	0	0	7	0	1	0	7
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	14	3	0	1	13	1	2	0	14	0	3	14	0	0	3
Deprecated Hash Functions	5	2	3	1	4	2	3	1	4	1	4	1	4	0	5
Use of Weak PRNG	16	2	0	1	15	0	2	2	14	0	2	10	6	0	2
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	15	10	2	13	2	0	12	12	3	0	12	3	12	2	10
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	31	6	20	1	30	0	26	1	30	15	11	0	31	0	26
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	2	4	13	0	2	0	17	0	2	0	17	0	2	0	17
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	84	51	0	0	84	0	51	1	83	0	51	3	81	0	51
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	11	3	0	0	11	0	3	0	11	0	3	0	11	0	3
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	4	0	0	1	3	0	0	1	3	0	0	0	4	0	0
Bad Programming of Cookies	17	3	0	0	17	0	3	0	17	0	3	0	17	0	3
Insecure Use of Hard Coded Constants	13	0	0	3	10	0	0	3	10	0	0	3	10	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	6	0	0	0	6	0	0	1	5	0	0	5	1	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
Hard Coded Credentials	26	1	5	0	26	0	6	6	20	4	2	2	24	0	6
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	3	1	0	2	1	0	1	1	2	0	1	0	3	0	1
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	96	143	2	0	96	3	142	9	87	0	145	0	96	0	145
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	4	0	4	1	3	0	4	1	3	4	0	0	4	0	4

Table 3.2: SAST tools output concerning the WebGoat - Part2

Results obtained in Juice Shop

Vulnerability				Tools											
Name	Total			Snyk				Fortify				Semgrep			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	10	1	0	0	10	0	1	0	10	0	1	1	9	1	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	11	3	0	2	9	0	3	0	11	0	3	8	3	3	0
Cross-Site Request Forgery	1	46	0	1	0	0	46	0	1	0	46	1	0	0	46
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	5	1	0	0	5	0	1	0	5	0	1	0	5	0	1
Deprecated Hash Functions	8	3	0	1	7	0	3	0	8	0	3	0	8	0	3
Use of Weak PRNG	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	47	25	0	6	41	0	25	0	47	0	25	7	40	1	24
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	15	1	1	10	5	0	2	0	15	0	2	4	11	1	1
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	4	32	0	0	4	0	32	0	4	0	32	0	4	0	32
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
Bad Programming of Cookies	32	0	0	0	32	0	0	2	30	0	0	0	32	0	0
Insecure Use of Hard Coded Constants	3	0	5	3	0	0	5	0	3	0	5	2	1	0	5
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	13	0	0	1	12	0	0	0	13	0	0	1	12	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	2	0	0	0	2	0	0	0	2	0	0	0	2
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	11	23	0	0	11	0	23	0	11	0	23	0	11	0	23
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	1	0	0	1	0	0	0	0	1	0	0	1	0	0	0

Table 3.3: SAST tools output in relation to the JuiceShop - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	10	1	0	0	10	0	1	0	10	0	1	0	10	0	1
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	11	3	0	0	11	0	3	0	11	0	3	0	11	0	3
Cross-Site Request Forgery	1	46	0	0	1	0	46	0	1	0	46	0	1	0	46
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	5	1	0	0	5	0	1	0	5	0	1	0	5	0	1
Deprecated Hash Functions	8	3	0	1	7	0	3	0	8	0	3	1	7	0	3
Use of Weak PRNG	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	47	25	0	0	47	0	25	0	47	0	25	0	47	0	25
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	15	1	1	7	8	1	1	1	14	0	2	0	15	0	2
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	4	32	0	0	4	0	32	0	4	0	32	0	4	0	32
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
Bad Programming of Cookies	32	0	0	0	32	0	0	0	32	0	0	0	32	0	0
Insecure Use of Hard Coded Constants	3	0	5	0	3	5	0	0	3	0	5	0	3	0	5
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	13	0	0	0	13	0	0	0	13	0	0	0	13	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	2	0	0	0	2	0	0	0	2	0	0	2	0
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	11	23	0	0	11	0	23	0	11	0	23	0	11	0	23
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0

Table 3.4: SAST tools output in relation to the JuiceShop - Part2

Results obtained in Mutillidae II

Vulnerability				Tools											
Name	Total			Snyk				Fortify				Semgrep			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	7	9	0	4	3	0	9	2	5	0	9	1	6	0	9
Cross-Site Request Forgery	18	4	2	0	18	0	6	4	14	2	4	0	18	0	6
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	10	0	0	0	10	0	0	0	10	0	0	0	10	0	0
Deprecated Hash Functions	5	2	7	4	1	7	2	5	0	0	9	0	5	0	9
Use of Weak PRNG	11	0	0	0	11	0	0	11	0	0	0	0	11	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	9	6	0	5	4	0	6	6	3	0	6	9	0	0	6
SQL Injection	19	7	0	0	19	0	7	0	19	0	7	1	18	0	7
LDAP Injection	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
Cross-Site Scripting	107	75	2	60	47	9	68	45	62	14	63	37	70	11	66
XPath Injection	2	0	0	1	1	0	0	0	2	0	0	0	2	0	0
HTTP Response Splitting	0	4	0	0	0	0	4	0	0	0	4	0	0	0	4
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	104	0	0	0	104	0	0	4	100	0	0	4	100	0	0
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	110	45	0	0	110	0	45	0	110	0	45	0	110	0	45
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	2	2	0	2	0	0	2	0	2	0	2	0	2	0	2
Bad Programming of Cookies	24	24	0	20	4	4	20	24	0	12	12	11	13	4	20
Insecure Use of Hard Coded Constants	2	3	2	0	2	0	5	0	2	0	5	0	2	0	5
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	2	0	0	0	2	0	0	0	2	0	0	2	0	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
Hard Coded Credentials	3	2	12	2	1	0	14	0	3	9	5	0	3	0	14
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	102	0	5	81	21	0	5	1	101	5	0	5	97	0	5
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	11	0	1	3	8	0	1	0	11	0	1	2	9	1	0

Table 3.5: SAST tools output in relation to the Mutillidae II - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	1	2	0	0	1	0	2	0	1	1	1	0	1	0	2
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	7	9	0	2	5	0	9	1	6	0	9	0	7	0	9
Cross-Site Request Forgery	18	4	2	0	18	0	6	0	18	2	4	0	18	0	6
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	10	0	0	0	10	0	0	0	10	0	0	0	10	0	0
Deprecated Hash Functions	5	2	7	4	1	0	9	1	4	0	9	0	5	0	9
Use of Weak PRNG	11	0	0	11	0	0	0	1	10	0	0	0	11	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	9	6	0	0	9	0	6	5	4	0	6	0	9	0	6
SQL Injection	19	7	0	0	19	0	7	0	19	0	7	0	19	0	7
LDAP Injection	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
Cross-Site Scripting	107	75	2	0	107	0	77	47	60	7	70	0	107	0	77
XPath Injection	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
HTTP Response Splitting	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	104	0	0	0	104	0	0	0	104	0	0	0	104	0	0
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	110	45	0	0	110	0	45	110	0	0	45	0	110	0	45
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	2	2	0	0	2	0	2	0	2	0	2	0	2	0	2
Bad Programming of Cookies	24	24	0	20	4	0	24	0	24	0	24	0	24	0	24
Insecure Use of Hard Coded Constants	2	3	2	1	1	2	3	0	2	0	5	0	2	0	5
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	2	0	0	0	2	0	0	0	2	0	0	1	1	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
Hard Coded Credentials	3	2	12	0	3	3	11	1	2	1	13	2	1	0	14
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	102	0	5	0	102	0	5	5	97	0	5	0	102	0	5
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	11	0	1	0	11	0	1	1	10	0	1	0	11	0	1

Table 3.6: SAST tools output in relation to the Mutillidae II - Part2

Results obtained in OWASP Benchmark

Vulnerability				Tools															
Name	Total			Snyk				Fortify				Semgrep				Spotbugs			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	133	135	879	133	0	66	948	122	11	667	347	123	10	118	896	133	0	484	530
Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	130	116	0	130	0	0	116	130	0	0	116	130	0	0	116	130	0	0	116
Deprecated Hash Functions	129	107	0	89	40	0	107	89	40	0	107	89	40	0	107	89	40	0	107
Use of Weak PRNG	218	275	0	218	0	0	275	218	0	52	223	218	0	0	275	218	0	0	275
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	126	125	0	126	0	45	80	126	0	125	0	117	9	109	16	126	0	111	14
SQL Injection	272	232	236	272	0	87	381	185	87	154	314	253	19	170	298	272	0	210	258
LDAP Injection	27	32	0	27	0	13	19	27	0	31	1	26	1	28	4	27	0	27	5
Cross-Site Scripting	246	209	1023	231	15	110	1122	215	31	68	1164	46	200	26	1206	246	0	696	536
XPath Injection	15	20	0	15	0	7	13	14	1	15	5	14	1	13	7	15	0	19	1
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trust Boundary Violation	83	43	493	76	7	24	512	31	52	12	524	69	14	26	510	83	0	35	501
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	1536	1516	0	170	1366	82	1434	62	1474	190	1326	856	680	163	1353	170	1366	82	1434
Insecure Use of Hard Coded Constants	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8 Software and data integrity failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.7: SAST tools output in relation to the OWASP Benchmark - Part1

Vulnerability				Tools											
Name	Total			Synopsys				Kiuwan				Horusec			
Name	Total			Synopsys				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	133	135	879	0	133	0	1014	118	15	110	904	0	133	0	1014
Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	130	116	0	97	33	0	116	130	0	40	76	97	33	66	50
Deprecated Hash Functions	129	107	0	89	40	0	107	89	40	0	107	28	101	0	107
Use of Weak PRNG	218	275	0	218	0	0	275	0	218	0	275	193	25	52	223
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	126	125	0	115	11	67	58	126	0	125	0	0	126	0	125
SQL Injection	272	232	236	272	0	128	340	263	9	119	349	199	73	414	54
LDAP Injection	27	32	0	27	0	15	17	24	3	8	24	2	25	7	25
Cross-Site Scripting	246	209	1023	246	0	561	671	246	0	844	388	15	231	4	1228
XPath Injection	15	20	0	15	0	15	5	15	0	5	15	15	0	20	0
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trust Boundary Violation	83	43	493	83	0	30	506	72	11	509	27	0	83	0	536
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	1536	1516	0	686	850	81	1435	0	1536	0	1516	0	1536	36	1480
Insecure Use of Hard Coded Constants	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8 Software and data integrity failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.8: SAST tools output in relation to the OWASP Benchmark - Part2

Results obtained in Juliet Test Suite

Vulnerability				Tools															
Name	Total			Snyk				Fortify				Semgrep				Spotbugs			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	233	372	1535	152	81	0	1907	32	201	480	1427	9	224	9	1898	196	37	1099	808
Insufficient Session Expiration	17	30	0	0	17	0	30	0	17	0	30	0	17	0	30	0	17	0	30
Path Traversal	230	378	0	160	70	0	378	230	0	4	374	53	177	24	354	213	17	188	190
Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	34	60	494	34	0	298	256	18	16	0	554	34	0	0	554	34	0	298	256
Deprecated Hash Functions	51	90	0	51	0	0	90	51	0	0	90	34	17	0	90	51	0	0	90
Use of Weak PRNG	34	60	17	0	34	0	77	34	0	0	77	0	34	0	77	34	0	0	77
Seeds Hard Coded in PRNG	17	30	0	0	17	0	30	0	17	0	30	0	17	0	30	0	17	0	30
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	252	411	0	164	88	0	411	252	0	411	0	60	192	9	402	252	0	411	0
SQL Injection	260	863	223	144	116	22	1064	260	0	126	960	226	34	358	728	260	0	861	225
LDAP Injection	265	433	0	176	89	0	433	265	0	61	372	265	0	423	10	265	0	433	0
Cross-Site Scripting	196	323	44	115	81	0	367	96	100	0	367	41	155	0	367	16	180	0	367
XPath Injection	263	850	0	0	263	0	850	263	0	18	832	54	209	288	562	263	0	850	0
HTTP Response Splitting	389	1266	115	249	140	0	1381	137	252	307	1074	0	389	0	1381	368	21	861	520
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	90	155	2063	0	90	0	2218	51	39	2123	95	0	90	0	2218	0	90	0	2218
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	17	30	638	17	0	0	668	17	0	30	638	17	0	0	668	16	1	0	668
Insecure Use of Hard Coded Constants	37	52	2	22	15	0	54	0	37	0	54	2	35	2	52	17	20	0	54
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	68	120	364	0	68	0	484	34	34	364	120	0	68	0	484	0	68	0	484
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	111	156	75	78	33	106	125	21	90	51	180	36	75	51	180	56	55	0	231
A8 Software and data integrity failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	51	90	53	17	34	0	143	0	51	0	143	34	17	0	143	0	51	0	143
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.9: SAST tools output in relation to the Juliet Test Suit - Part1

Vulnerability				Tools											
Name	Total			Synopsys				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	233	372	1535	87	146	0	1907	106	127	105	1802	0	233	0	1907
Insufficient Session Expiration	17	30	0	17	0	0	30	0	17	0	30	0	17	0	30
Path Traversal	230	378	0	0	230	0	378	149	81	0	378	0	230	0	378
Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	34	60	494	34	0	388	166	17	17	0	554	34	0	164	390
Deprecated Hash Functions	51	90	0	51	0	0	90	51	0	0	90	51	0	0	90
Use of Weak PRNG	34	60	17	0	34	0	77	0	34	17	60	17	17	0	77
Seeds Hard Coded in PRNG	17	30	0	17	0	0	30	0	17	0	30	17	0	0	30
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	252	411	0	98	154	0	411	142	110	0	411	252	0	0	411
SQL Injection	260	863	223	125	135	0	1086	242	18	356	730	260	0	217	869
LDAP Injection	265	433	0	265	0	432	1	151	114	0	433	264	1	0	433
Cross-Site Scripting	196	323	44	86	110	0	367	194	2	0	367	0	196	44	323
XPath Injection	263	850	0	105	158	175	675	164	99	310	540	0	263	0	850
HTTP Response Splitting	389	1266	115	0	389	0	1381	168	221	32	1349	0	389	0	1381
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	90	155	2063	0	90	0	2218	20	70	33	2185	0	90	0	2218
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	17	30	638	0	17	0	668	0	17	0	668	0	17	0	668
Insecure Use of Hard Coded Constants	37	52	2	35	2	0	54	26	11	0	54	0	37	0	54
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	68	120	364	0	68	0	484	0	68	0	484	0	68	0	484
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	111	156	75	102	9	3	228	70	41	104	127	0	111	75	156
A8 Software and data integrity failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	51	90	53	0	51	0	143	34	17	4	139	0	51	49	94
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.10: SAST tools output in relation to the Juliet Test Suit - Part2

Results obtained in Shopizer

Vulnerability				Tools															
Name	Total			Snyk				Fortify				Semgrep				SpotBugs			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2	0	0	2	0
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	6	3	33	0	6	0	36	0	6	0	36	0	6	0	36	1	5	25	11
Cross-Site Request Forgery	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0	4	0	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	3	0	0	1	2	0	0	1	2	0	0	1	2	0	0	1	2	0	0
Deprecated Hash Functions	7	10	2	0	7	0	12	0	7	0	12	0	7	0	12	0	7	0	12
Use of Weak PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	0	11	0	0	0	0	11	0	0	0	11	0	0	0	11	0	0	11	0
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	0	316	6	0	0	10	312	0	0	0	322	0	0	0	322	0	0	0	322
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	3	0	17	3	0	0	17	2	1	0	17	0	3	0	17	3	0	0	17
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	289	260	0	0	289	0	260	248	41	0	260	0	289	0	260	0	289	0	260
Trust Boundary Violation	0	5	0	0	0	0	5	0	0	0	5	0	0	0	5	0	0	5	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Insecure Use of Hard Coded Constants	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0	1	1	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	0	5	0	0	0	0	5	0	0	0	5	0	0	0	5	0	0	0	5
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	51	0	0	0	51	0	0	16	35	0	0	0	51	0	0	0	51
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	187	97	0	0	187	0	97	129	58	1	96	7	180	0	97	4	183	0	97
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	4	0	0	0	0	4	0	0	0	4	0	0	0	4	0	0	3	1

Table 3.11: SAST tools output in relation to the Shopizer - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	6	3	33	5	1	9	27	0	6	3	33	0	6	0	36
Cross-Site Request Forgery	4	0	0	2	2	0	0	4	0	0	0	0	4	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	3	0	0	1	2	0	0	0	3	0	0	0	3	0	0
Deprecated Hash Functions	7	10	2	0	7	0	12	0	7	0	12	6	1	11	1
Use of Weak PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SQL Injection	0	11	0	0	0	0	11	0	0	0	11	0	0	0	11
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	0	316	6	0	0	0	322	0	0	106	216	0	0	0	322
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	3	0	17	0	3	0	17	3	0	17	0	0	3	0	17
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	289	260	0	0	289	0	260	0	289	0	260	5	284	0	260
Trust Boundary Violation	0	5	0	0	0	0	5	0	0	0	5	0	0	0	5
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Insecure Use of Hard Coded Constants	2	0	0	0	2	0	0	1	1	0	0	0	2	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	0	5	0	0	0	0	5	0	0	0	5	0	0	0	5
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	51	0	0	0	51	0	0	27	24	0	0	8	43
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	187	97	0	0	187	0	97	7	180	0	97	0	187	0	97
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	4	0	0	0	0	4	0	0	1	3	0	0	0	4

Table 3.12: SAST tools output in relation to the Shopizer - Part2

Results obtained in Piwigo

Vulnerability				Tools											
Name	Total			Snyk				Fortify				Semgrep			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	9	0	0	0	2	7	0	0	0	9	0	0	0	9
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	0	110	0	0	0	25	85	0	0	38	72	0	0	54	56
Cross-Site Request Forgery	57	25	0	0	57	0	25	3	54	0	25	0	57	0	25
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	4	0	1	0	4	0	1	3	1	1	0	0	4	0	1
Deprecated Hash Functions	41	8	0	34	7	0	8	32	9	2	6	0	41	0	8
Use of Weak PRNG	9	1	0	0	9	0	1	8	1	0	1	0	9	0	1
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	15	0	0	0	0	15	0	0	15	0	0	0	15	0
SQL Injection	2	5	1	2	0	0	6	2	0	0	6	0	2	4	2
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	11	32	15	3	8	29	18	0	11	10	37	0	11	1	46
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	1	11	0	0	1	0	11	0	1	6	5	0	1	0	11
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	17	0	0	0	17	0	0	0	17	0	0	0	17	0	0
Trust Boundary Violation	0	13	0	0	0	0	13	0	0	0	13	0	0	0	13
Method Tampering	27	0	0	0	27	0	0	0	27	0	0	0	27	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1
Bad Programming of Cookies	28	7	0	14	14	0	7	16	12	0	7	0	28	0	7
Insecure Use of Hard Coded Constants	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	4	2	0	0	4	0	2	0	4	0	2	0	4	0	2
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	5	0	0	0	5	0	0	0	5	0	0	0	5
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	25	0	0	1	0	25	0	1	0	25	1	0	25	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	16	35	4	0	16	0	39	3	13	15	24	0	16	0	39
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	20	3	0	0	4	19	0	0	0	23	0	0	14	9

Table 3.13: SAST tools output in relation to the Piwigo - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	9	0	0	0	0	9	0	0	0	9	0	0	0	9
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	0	110	0	0	0	0	110	0	0	2	108	0	0	0	110
Cross-Site Request Forgery	57	25	0	0	57	0	25	0	57	0	25	0	57	0	25
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	4	0	1	1	3	0	1	3	1	0	1	0	4	0	1
Deprecated Hash Functions	41	8	0	25	16	2	6	35	6	2	6	0	41	0	8
Use of Weak PRNG	9	1	0	7	2	0	1	2	7	0	1	1	8	0	1
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	15	0	0	0	0	15	0	0	0	15	0	0	0	15
SQL Injection	2	5	1	0	2	0	6	0	2	0	6	0	2	1	5
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	11	32	15	0	11	0	47	1	10	6	41	0	11	0	47
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	1	11	0	0	1	0	11	0	1	2	9	0	1	0	11
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	17	0	0	0	17	0	0	0	17	0	0	0	17	0	0
Trust Boundary Violation	0	13	0	0	0	0	13	0	0	13	0	0	0	0	13
Method Tampering	27	0	0	0	27	0	0	26	1	0	0	0	27	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1
Bad Programming of Cookies	28	7	0	16	12	1	6	0	28	0	7	0	28	0	7
Insecure Use of Hard Coded Constants	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	4	2	0	0	4	0	2	0	4	0	2	4	0	2	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	5	0	0	0	5	0	0	0	5	0	0	5	0
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	25	0	0	1	0	25	0	1	2	23	0	1	0	25
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	16	35	4	0	16	0	39	0	16	3	36	0	16	0	39
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	20	3	0	0	0	23	0	0	0	23	0	0	0	23

Table 3.14: SAST tools output in relation to the Piwigo - Part2

Results obtained in Peertube

Vulnerability				Tools											
Name	Total			Snyk				Fortify				Semgrep			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	16	6	0	0	1	21	0	0	0	22	0	0	0	22
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	4	55	81	2	2	15	121	0	4	0	136	4	0	124	12
Cross-Site Request Forgery	194	0	0	0	194	0	0	3	191	0	0	0	194	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Deprecated Hash Functions	4	1	0	1	3	0	1	1	3	0	1	0	4	0	1
Use of Weak PRNG	2	3	0	0	2	0	3	0	2	0	3	0	2	0	3
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	7	0	0	0	0	7	0	0	0	7	0	0	0	7
SQL Injection	0	19	0	0	0	0	19	0	0	0	19	0	0	0	19
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	0	28	1	0	0	7	22	0	0	0	29	0	0	28	1
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	3	1	0	3	0	1	0	0	3	0	1	0	3	0	1
Insecure Use of Hard Coded Constants	3	0	2	3	0	1	1	0	3	0	2	0	3	0	2
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	194	0	0	0	194	0	0	3	191	0	0	0	194	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	43	0	0	2	41	0	0	14	29	0	0	0	43
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	1	6	0	0	1	3	3	0	1	0	6	0	1	0	6

Table 3.15: SAST tools output in relation to the PeerTube - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	16	6	0	0	0	22	0	0	9	13	0	0	5	17
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	4	55	81	0	4	0	136	0	4	0	136	0	4	0	136
Cross-Site Request Forgery	194	0	0	0	194	0	0	194	0	0	0	0	194	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Deprecated Hash Functions	4	1	0	1	3	0	1	0	4	0	1	4	0	0	1
Use of Weak PRNG	2	3	0	0	2	0	3	0	2	0	3	2	0	3	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
OS Command Injection	0	7	0	0	0	0	7	0	0	0	7	0	0	5	2
SQL Injection	0	19	0	0	0	0	19	0	0	0	19	0	0	0	19
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	0	28	1	0	0	0	29	0	0	0	29	0	0	0	29
XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bad Programming of Cookies	3	1	0	0	3	0	1	0	3	0	1	0	3	0	1
Insecure Use of Hard Coded Constants	3	0	2	0	3	0	2	0	3	0	2	2	1	1	1
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	194	0	0	0	194	0	0	194	0	0	0	0	194	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	0	0	43	0	0	4	39	0	0	0	43	0	0	23	20
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	1	6	0	0	1	0	6	0	1	0	6	0	1	0	6

Table 3.16: SAST tools output in relation to the PeerTube - Part2

Results obtained in Metafresh

Vulnerability				Tools															
Name	Total			Snyk				Fortify				Semgrep				SpotBugs			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	1	34	2	1	0	6	30	0	1	25	11	0	1	2	34	0	1	0	36
Cross-Site Request Forgery	3	0	0	3	0	0	0	0	3	0	0	2	1	0	0	0	3	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	28	0	0	0	28	0	0	0	28	0	0	0	28	0	0	0	28	0	0
Deprecated Hash Functions	126	4	14	4	122	0	18	3	123	0	18	3	123	0	18	0	126	0	18
Use of Weak PRNG	16	0	0	1	15	0	0	14	2	0	0	3	13	0	0	0	16	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	5	0	0	0	0	5	0	0	4	1	0	0	1	4	0	0	0	5
SQL Injection	0	262	217	0	0	17	462	0	0	38	441	0	0	47	432	0	0	2	477
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	7	223	21	0	7	4	240	0	7	142	102	0	7	1	243	0	7	0	244
XPath Injection	0	3	0	0	0	0	3	0	0	3	0	0	0	0	3	0	0	0	3
HTTP Response Splitting	0	7	1	0	0	5	3	0	0	3	5	0	0	0	8	0	0	0	8
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	112	71	0	0	112	0	71	59	53	71	0	0	112	0	71	0	112	0	71
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	2	22	0	1	1	2	20	0	2	16	6	1	1	12	10	0	2	0	22
Bad Programming of Cookies	8	0	0	6	2	0	0	4	4	0	0	6	2	0	0	0	8	0	0
Insecure Use of Hard Coded Constants	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	4	4	73	4	0	2	75	0	4	19	58	0	4	0	77	0	4	0	77
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	4	1	0	1	0	5	0	1	0	5	0	1	1	4	0	1	0	5
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	274	370	51	32	242	12	409	203	71	284	137	130	144	1	420	1	273	0	421
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.17: SAST tools output in relation to the Metafresh - Part1

Vulnerability				Tools											
Name	Total			Synopsis				Kiuwan				Horusec			
A1 Broken Access Control	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authorization	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1
Insufficient Session Expiration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path Traversal	1	34	2	0	1	0	36	1	0	8	28	0	1	4	32
Cross-Site Request Forgery	3	0	0	1	2	0	0	3	0	0	0	0	3	0	0
A2 Cryptographic Failure	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Use of Old/Insecure algorithms	28	0	0	1	27	0	0	0	28	0	0	28	0	0	0
Deprecated Hash Functions	126	4	14	3	123	0	18	3	123	0	18	125	1	18	0
Use of Weak PRNG	16	0	0	0	16	0	0	6	10	0	0	3	13	0	0
Seeds Hard Coded in PRNG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3 Injection	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Command Injection	0	5	0	0	0	0	5	0	0	0	5	0	0	0	5
SQL Injection	0	262	217	0	0	1	478	0	0	0	479	0	0	380	99
LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cross-Site Scripting	7	223	21	7	0	15	229	6	1	11	233	0	7	0	244
XPath Injection	0	3	0	0	0	0	3	0	0	0	3	0	0	0	3
HTTP Response Splitting	0	7	1	0	0	0	8	0	0	4	4	0	0	0	8
A4 Insecure Design	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Error Handling	112	71	0	0	112	0	71	0	112	0	71	53	59	0	71
Trust Boundary Violation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Method Tampering	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A5 Security Misconfiguration	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
XML External Entities	2	22	0	0	2	0	22	0	2	9	13	0	2	5	17
Bad Programming of Cookies	8	0	0	3	5	0	0	0	8	0	0	1	7	0	0
Insecure Use of Hard Coded Constants	2	0	0	1	1	0	0	1	1	0	0	0	2	0	0
A6 Vulnerable and Outdated Components	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Vulnerable Third-Party Components	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
A7 Identification and Authentication Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Bypassing Authentication	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hard Coded Credentials	4	4	73	0	4	0	77	3	1	0	77	0	4	56	21
A8 Software and Data Integrity Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Insecure Deserialization	1	4	1	1	0	4	1	0	1	0	5	0	1	0	5
A9 Security Logging and Monitoring Failures	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Improper Output Neutralization for Logs	274	370	51	18	256	120	301	78	196	0	421	0	274	0	421
A10 Server-Side Request Forgery	P	N	NN	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
Server-Side Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.18: SAST tools output in relation to the Metafresh - Part2

Chapter 4

Performance results for all Combinations of 2 and 3 SAST Tools using the 1st strategy

This section includes the results achieved by applying the strategy demonstrated in example 1 of the "Combinations of tools" step, which was incorporated into Methodology stage 4.1.4.4. The established approach involves the disjunction of the SAST tools' outputs obtained individually and was extended to the combinations of 2, table 4.1, and 3, table 4.2. As the latter were characterized on the basis of representative metrics for different vulnerability detection scenarios, the rankings derived make it possible to observe the progression of the SAST tool combination ranking over different contexts. Due to the proximity of certain performance values reached through the main metric, this was used in conjunction with a tiebreaker metric in order to break the tie between those within the same 5% range.

Results obtained in Combinations of 2 Tools

Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FP	TN	FN	Recall	Precison	Comb.	TP	FP	TN	FN	Rec.*Infor.	Recall
C, A	5072	7615	12708	3249	60.95%	39.98%	A, E	4821	4411	15912	3500	39.47%	57.94%
C, F	5054	7781	12542	3267	60.74%	39.38%	B, A	4628	2901	17422	3693	39.31%	55.62%
C, E	5098	8398	11925	3223	61.27%	37.77%	C, E	5098	8398	11925	3223	36.74%	61.27%
B, A	4628	2901	17422	3693	55.62%	61.47%	C, A	5072	7615	12708	3249	37.63%	60.95%
F, E	4650	4154	16169	3671	55.88%	52.82%	C, F	5054	7781	12542	3267	37.19%	60.74%
A, E	4821	4411	15912	3500	57.94%	52.22%	B, C	4919	6815	13508	3402	37.12%	59.12%
B, C	4919	6815	13508	3402	59.12%	41.92%	A, D	4824	6856	13467	3497	36.01%	57.97%
A, D	4824	6856	13467	3497	57.97%	41.3%	F, E	4650	4154	16169	3671	37.84%	55.88%
E, D	4643	7030	13293	3678	55.8%	39.78%	E, D	4643	7030	13293	3678	33.82%	55.8%
C, D	4774	10907	9416	3547	57.37%	30.44%	F, D	4444	6954	13369	3877	31.83%	53.41%
B, F	4191	2693	17630	4130	50.37%	60.88%	B, F	4191	2693	17630	4130	34.53%	50.37%
G, E	4165	4534	15789	4156	50.05%	47.88%	G, E	4165	4534	15789	4156	31.97%	50.05%
F, D	4444	6954	13369	3877	53.41%	38.99%	B, E	4096	3719	16604	4225	32.22%	49.22%
C, G	4282	7524	12799	4039	51.46%	36.27%	A, F	4036	3354	16969	4285	32.01%	48.5%
A, F	4036	3354	16969	4285	48.5%	54.61%	C, D	4774	10907	9416	3547	29.75%	57.37%
B, E	4096	3719	16604	4225	49.22%	52.41%	C, G	4282	7524	12799	4039	29.45%	51.46%
B, D	4157	7181	13142	4164	49.96%	36.66%	B, D	4157	7181	13142	4164	28.63%	49.96%
G, D	3896	7642	12681	4425	46.82%	33.77%	G, D	3896	7642	12681	4425	25.57%	46.82%
F, G	3604	3536	16787	4717	43.31%	50.48%	A, G	3686	3683	16640	4635	27.95%	44.3%
A, G	3686	3683	16640	4635	44.3%	50.02%	F, G	3604	3536	16787	4717	27.27%	43.31%
B, G	3317	2530	17793	5004	39.86%	56.73%	B, G	3317	2530	17793	5004	25.4%	39.86%
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FP	TN	FN	F-measure	Recall	Comb.	TP	FP	TN	FN	Markedness	Precision
B, A	4628	2901	17422	3693	58.4%	55.62%	B, A	4628	2901	17422	3693	71.99%	61.47%
B, F	4191	2693	17630	4130	55.13%	50.37%	B, F	4191	2693	17630	4130	70.95%	60.88%
A, E	4821	4411	15912	3500	54.93%	57.94%	B, G	3317	2530	17793	5004	67.39%	56.73%
F, E	4650	4154	16169	3671	54.31%	55.88%	A, F	4036	3354	16969	4285	67.23%	54.61%
B, E	4096	3719	16604	4225	50.77%	49.22%	F, E	4650	4154	16169	3671	67.16%	52.82%
A, F	4036	3354	16969	4285	51.38%	48.5%	B, E	4096	3719	16604	4225	66.06%	52.41%
C, E	5098	8398	11925	3223	46.73%	61.27%	A, E	4821	4411	15912	3500	67.1%	52.22%
C, A	5072	7615	12708	3249	48.29%	60.95%	F, G	3604	3536	16787	4717	64.27%	50.48%
C, F	5054	7781	12542	3267	47.78%	60.74%	A, G	3686	3683	16640	4635	64.12%	50.02%
B, C	4919	6815	13508	3402	49.06%	59.12%	G, E	4165	4534	15789	4156	63.52%	47.88%
A, D	4824	6856	13467	3497	48.24%	57.97%	B, C	4919	6815	13508	3402	60.9%	41.92%
E, D	4643	7030	13293	3678	46.44%	55.8%	A, D	4824	6856	13467	3497	60.34%	41.3%
F, D	4444	6954	13369	3877	45.07%	53.41%	C, A	5072	7615	12708	3249	59.81%	39.98%
G, E	4165	4534	15789	4156	48.94%	50.05%	E, D	4643	7030	13293	3678	59.05%	39.78%
A, G	3686	3683	16640	4635	46.99%	44.3%	C, F	5054	7781	12542	3267	59.36%	39.38%
F, G	3604	3536	16787	4717	46.62%	43.31%	F, D	4444	6954	13369	3877	58.25%	38.99%
B, G	3317	2530	17793	5004	46.82%	39.86%	C, E	5098	8398	11925	3223	58.25%	37.77%
C, G	4282	7524	12799	4039	42.55%	51.46%	B, D	4157	7181	13142	4164	56.3%	36.66%
B, D	4157	7181	13142	4164	42.29%	49.96%	C, G	4282	7524	12799	4039	56.14%	36.27%
C, D	4774	10907	9416	3547	39.78%	57.37%	G, D	3896	7642	12681	4425	53.95%	33.77%
G, D	3896	7642	12681	4425	39.24%	46.82%	C, D	4774	10907	9416	3547	51.54%	30.44%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 4.1: Ranking of Combination of 2 SAST tools by scenario

Results obtained in Combinations of 3 Tools

Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FP	TN	FN	Recall	Precison	Comb.	TP	FP	TN	FN	Rec.*Infor.	Recall
B, C, A	5866	8265	12058	2455	70.5%	41.51%	C, A, E	6077	9553	10770	2244	46.02%	73.03%
C, A, E	6077	9553	10770	2244	73.03%	38.88%	B, C, A	5866	8265	12058	2455	45.76%	70.5%
C, F, E	5923	9438	10885	2398	71.18%	38.56%	B, A, E	5540	4979	15344	2781	47.3%	66.58%
B, A, E	5540	4979	15344	2781	66.58%	52.67%	C, F, E	5923	9438	10885	2398	44.4%	71.18%
A, E, D	5562	7431	12892	2759	66.84%	42.81%	C, A, D	5789	10724	9599	2532	40.63%	69.57%
F, E, D	5427	7407	12916	2894	65.22%	42.29%	B, C, E	5628	9040	11283	2693	41.65%	67.64%
B, C, F	5572	8265	12058	2749	66.96%	40.27%	B, C, F	5572	8265	12058	2749	42.29%	66.96%
C, A, F	5554	8698	11625	2767	66.75%	38.97%	A, E, D	5562	7431	12892	2759	43.54%	66.84%
B, C, E	5628	9040	11283	2693	67.64%	38.37%	C, A, F	5554	8698	11625	2767	41.37%	66.75%
C, A, D	5789	10724	9599	2532	69.57%	35.06%	F, E, D	5427	7407	12916	2894	41.99%	65.22%

C, E, D	5546	11369	8954	2775	66.65%	32.79%	A, G, E	5243	5863	14460	3078	42.27%	63.01%
C, F, D	5467	11296	9027	2854	65.7%	32.61%	B, F, E	5193	4598	15725	3128	43.62%	62.41%
B, A, G	5025	4438	15885	3296	60.39%	53.1%	A, F, E	5182	4924	15399	3139	42.99%	62.28%
B, F, E	5193	4598	15725	3128	62.41%	53.04%	F, G, E	5052	5543	14780	3269	40.51%	60.71%
A, F, E	5182	4924	15399	3139	62.28%	51.28%	B, A, G	5025	4438	15885	3296	41.84%	60.39%
F, G, E	5052	5543	14780	3269	60.71%	47.68%	C, E, D	5546	11369	8954	2775	36.89%	66.65%
A, G, E	5243	5863	14460	3078	63.01%	47.21%	C, F, D	5467	11296	9027	2854	36.17%	65.7%
B, A, D	5079	6506	13817	3242	61.04%	43.84%	C, A, G	5398	9042	11281	2923	39.05%	64.87%
A, G, D	5110	7414	12909	3211	61.41%	40.8%	C, G, E	5382	9807	10516	2939	37.65%	64.68%
B, C, G	5181	8171	12152	3140	62.26%	38.8%	C, F, G	5342	9127	11196	2979	38.29%	64.2%
C, A, G	5398	9042	11281	2923	64.87%	37.38%	B, C, G	5181	8171	12152	3140	38.0%	62.26%
C, F, G	5342	9127	11196	2979	64.2%	36.92%	A, G, D	5110	7414	12909	3211	38.36%	61.41%
C, G, E	5382	9807	10516	2939	64.68%	35.43%	B, A, D	5079	6506	13817	3242	39.38%	61.04%
B, C, D	5113	11186	9137	3208	61.45%	31.37%	B, E, D	4992	7287	13036	3329	37.24%	59.99%
C, G, D	5040	11402	8921	3281	60.57%	30.65%	B, G, E	4921	5220	15103	3400	39.46%	59.14%
B, A, F	4674	3774	16549	3647	56.17%	55.33%	A, F, D	4915	6571	13752	3406	37.43%	59.07%
B, F, G	4642	4118	16205	3679	55.79%	52.99%	G, E, D	4912	8140	12183	3409	35.12%	59.03%
B, G, E	4921	5220	15103	3400	59.14%	48.53%	B, F, D	4834	6954	13369	3487	35.98%	58.09%
A, F, D	4915	6571	13752	3406	59.07%	42.79%	B, A, F	4674	3774	16549	3647	38.65%	56.17%
B, F, D	4834	6954	13369	3487	58.09%	41.01%	B, F, G	4642	4118	16205	3679	37.8%	55.79%
B, E, D	4992	7287	13036	3329	59.99%	40.65%	A, F, G	4499	4753	15570	3822	35.33%	54.07%
G, E, D	4912	8140	12183	3409	59.03%	37.63%	B, C, D	5113	11186	9137	3208	32.69%	61.45%
F, G, D	4699	8030	12293	3622	56.47%	36.92%	C, G, D	5040	11402	8921	3281	31.64%	60.57%
A, F, G	4499	4753	15570	3822	54.07%	48.63%	F, G, D	4699	8030	12293	3622	33.02%	56.47%
B, G, D	4424	7209	13114	3897	53.17%	38.03%	B, G, D	4424	7209	13114	3897	31.29%	53.17%
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FP	TN	FN	F-measure	Recall	Comb.	TP	FP	TN	FN	Markedness	Precision
B, A, E	5540	4979	15344	2781	58.81%	66.58%	B, A, F	4674	3774	16549	3647	68.63%	55.33%
B, F, E	5193	4598	15725	3128	57.34%	62.41%	B, A, G	5025	4438	15885	3296	67.96%	53.1%
A, F, E	5182	4924	15399	3139	56.24%	62.28%	B, F, E	5193	4598	15725	3128	68.22%	53.04%
B, A, G	5025	4438	15885	3296	56.51%	60.39%	B, F, G	4642	4118	16205	3679	67.24%	52.99%
B, A, F	4674	3774	16549	3647	55.75%	56.17%	B, A, E	5540	4979	15344	2781	68.66%	52.67%
C, A, E	6077	9553	10770	2244	50.75%	73.03%	A, F, E	5182	4924	15399	3139	67.17%	51.28%
C, F, E	5923	9438	10885	2398	50.02%	71.18%	B, G, E	4921	5220	15103	3400	65.08%	48.53%
B, C, A	5866	8265	12058	2455	52.25%	70.5%	A, F, G	4499	4753	15570	3822	64.46%	48.63%
B, C, F	5572	8265	12058	2749	50.29%	66.96%	F, G, E	5052	5543	14780	3269	64.79%	47.68%
A, E, D	5562	7431	12892	2759	52.19%	66.84%	A, G, E	5243	5863	14460	3078	64.83%	47.21%
F, E, D	5427	7407	12916	2894	51.31%	65.22%	B, A, D	5079	6506	13817	3242	62.42%	43.84%
A, G, E	5243	5863	14460	3078	53.98%	63.01%	A, E, D	5562	7431	12892	2759	62.59%	42.81%
B, A, D	5079	6506	13817	3242	51.03%	61.04%	A, F, D	4915	6571	13752	3406	61.47%	42.79%
F, G, E	5052	5543	14780	3269	53.42%	60.71%	F, E, D	5427	7407	12916	2894	61.99%	42.29%
B, G, E	4921	5220	15103	3400	53.31%	59.14%	B, C, A	5866	8265	12058	2455	62.3%	41.51%
B, F, G	4642	4118	16205	3679	54.35%	55.79%	B, F, D	4834	6954	13369	3487	60.16%	41.01%
A, F, G	4499	4753	15570	3822	51.2%	54.07%	A, G, D	5110	7414	12909	3211	60.44%	40.8%
C, A, D	5789	10724	9599	2532	46.62%	69.57%	B, E, D	4992	7287	13036	3329	60.16%	40.65%
B, C, E	5628	9040	11283	2693	48.96%	67.64%	B, C, F	5572	8265	12058	2749	60.85%	40.27%
C, A, F	5554	8698	11625	2767	49.21%	66.75%	C, A, E	6077	9553	10770	2244	60.82%	38.88%
C, A, G	5398	9042	11281	2923	47.43%	64.87%	C, F, E	5923	9438	10885	2398	60.25%	38.56%
C, G, E	5382	9807	10516	2939	45.78%	64.68%	C, A, F	5554	8698	11625	2767	59.87%	38.97%
C, F, G	5342	9127	11196	2979	46.88%	64.2%	B, C, G	5181	8171	12152	3140	59.13%	38.8%
B, C, G	5181	8171	12152	3140	47.81%	62.26%	B, C, E	5628	9040	11283	2693	59.55%	38.37%
A, G, D	5110	7414	12909	3211	49.03%	61.41%	B, G, D	4424	7209	13114	3897	57.56%	38.03%
B, E, D	4992	7287	13036	3329	48.47%	59.99%	G, E, D	4912	8140	12183	3409	57.89%	37.63%
A, F, D	4915	6571	13752	3406	49.63%	59.07%	C, A, G	5398	9042	11281	2923	58.4%	37.38%
G, E, D	4912	8140	12183	3409	45.96%	59.03%	C, F, G	5342	9127	11196	2979	57.95%	36.92%
B, F, D	4834	6954	13369	3487	48.08%	58.09%	F, G, D	4699	8030	12293	3622	57.08%	36.92%
C, E, D	5546	11369	8954	2775	43.95%	66.65%	C, G, E	5382	9807	10516	2939	56.8%	35.43%
C, F, D	5467	11296	9027	2854	43.59%	65.7%	C, A, D	5789	10724	9599	2532	57.09%	35.06%
B, C, D	5113	11186	9137	3208	41.54%	61.45%	C, E, D	5546	11369	8954	2775	54.56%	32.79%
C, G, D	5040	11402	8921	3281	40.71%	60.57%	C, F, D	5467	11296	9027	2854	54.3%	32.61%
F, G, D	4699	8030	12293	3622	44.65%	56.47%	B, C, D	5113	11186	9137	3208	52.69%	31.37%
B, G, D	4424	7209	13114	3897	44.34%	53.17%	C, G, D	5040	11402	8921	3281	51.88%	30.65%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 4.2: Ranking of Combination of 3 SAST tools by scenario

Chapter 5

Performance results for all Combinations of 2 Tools using the 2nd strategy

In order to refine the analysis already carried out in the combined execution of SAST tools and, consequently, understand the impact of this approach on the vulnerabilities contained within each category of the OWASP Top 10, a new strategy was implemented in which the performance of the tools dictates their weight in the combination. Since the application of this strategy involves assigning a weight to the SAST tools according to their position in the ranking against a given vulnerability and scenario, as shown in example 2 of the "Combinations of tools" step in the Methodology stage 4.1.4.4, the weights obtained according to their performance in relation to this scope are shown in table 5.1. The results of combining two SAST tools' outputs based on them are displayed in the present section from table 5.2 to table 5.21, each of which refers to a specific OWASP Top 10 category. For a given vulnerability contained in the latter, the rankings achieved with regard to the metrics associated with different vulnerability detection contexts are provided.

Weights of tools for each scenario regarding all different vulnerabilities

Vulnerability	Bypassing Authorization				Vulnerability	Insufficient Session Expiration			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1529	0.1529	0.1579	0.1529	Snyk	0.1404	0.1404	0.1404	0.1404
Fortify	0.1379	0.1379	0.1379	0.1329	Fortify	0.1404	0.1404	0.1404	0.1404
Semgrep	0.1329	0.1329	0.1329	0.1429	Semgrep	0.1404	0.1404	0.1404	0.1404
Synopsis	0.1429	0.1429	0.1529	0.1579	Synopsis	0.1579	0.1579	0.1579	0.1579
Horusec	0.1279	0.1279	0.1279	0.1279	Horusec	0.1404	0.1404	0.1404	0.1404
Kiuwan	0.1479	0.1479	0.1479	0.1479	Kiuwan	0.1404	0.1404	0.1404	0.1404
SpotBugs	0.1579	0.1579	0.1429	0.1379	SpotBugs	0.1404	0.1404	0.1404	0.1404
Vulnerability	Path Traversal				Vulnerability	Cross-Site Request Forgery			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1479	0.1529	0.1579	0.1579	Snyk	0.1529	0.1479	0.1479	0.1529
Fortify	0.1529	0.1479	0.1479	0.1329	Fortify	0.1429	0.1529	0.1529	0.1429
Semgrep	0.1379	0.1379	0.1379	0.1429	Semgrep	0.1379	0.1429	0.1429	0.1379
Synopsis	0.1329	0.1329	0.1329	0.1479	Synopsis	0.1479	0.1329	0.1329	0.1479
Horusec	0.1304	0.1304	0.1304	0.1304	Horusec	0.1279	0.1279	0.1279	0.1279
Kiuwan	0.1429	0.1429	0.1529	0.1529	Kiuwan	0.1579	0.1579	0.1579	0.1579
SpotBugs	0.1579	0.1579	0.1429	0.1379	SpotBugs	0.1329	0.1379	0.1379	0.1329
Vulnerability	Use of Old/Insecure algorithms				Vulnerability	Deprecated Hash Functions			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1454	0.1354	0.1354	0.1354	Snyk	0.1379	0.1529	0.1529	0.1329
Fortify	0.1379	0.1529	0.1529	0.1529	Fortify	0.1529	0.1479	0.1479	0.1479
Semgrep	0.1529	0.1579	0.1579	0.1579	Semgrep	0.1279	0.1279	0.1279	0.1529
Synopsis	0.1279	0.1279	0.1279	0.1279	Synopsis	0.1429	0.1379	0.1379	0.1379
Horusec	0.1579	0.1479	0.1429	0.1429	Horusec	0.1579	0.1579	0.1579	0.1279
Kiuwan	0.1329	0.1429	0.1479	0.1479	Kiuwan	0.1479	0.1429	0.1429	0.1429
SpotBugs	0.1454	0.1354	0.1354	0.1354	SpotBugs	0.1329	0.1329	0.1329	0.1579
Vulnerability	Seeds Hard Coded in PRNG				Vulnerability	Use of Weak PRNG			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1379	0.1379	0.1379	0.1379	Snyk	0.1379	0.1379	0.1379	0.1429
Fortify	0.1379	0.1379	0.1379	0.1379	Fortify	0.1579	0.1579	0.1579	0.1379
Semgrep	0.1379	0.1379	0.1379	0.1379	Semgrep	0.1429	0.1429	0.1429	0.1479
Synopsis	0.1554	0.1554	0.1554	0.1554	Synopsis	0.1479	0.1479	0.1479	0.1529
Horusec	0.1554	0.1554	0.1554	0.1554	Horusec	0.1329	0.1329	0.1329	0.1329
Kiuwan	0.1379	0.1379	0.1379	0.1379	Kiuwan	0.1279	0.1279	0.1279	0.1279
SpotBugs	0.1379	0.1379	0.1379	0.1379	SpotBugs	0.1529	0.1529	0.1529	0.1579
Vulnerability	OS Command Injection				Vulnerability	SQL Injection			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1479	0.1579	0.1579	0.1529	Snyk	0.1329	0.1379	0.1579	0.1579
Fortify	0.1529	0.1529	0.1379	0.1279	Fortify	0.1429	0.1429	0.1479	0.1479
Semgrep	0.1279	0.1279	0.1279	0.1379	Semgrep	0.1479	0.1479	0.1379	0.1379
Synopsis	0.1329	0.1329	0.1429	0.1479	Synopsis	0.1279	0.1329	0.1529	0.1529
Horusec	0.1379	0.1379	0.1529	0.1579	Horusec	0.1379	0.1279	0.1279	0.1279
Kiuwan	0.1429	0.1429	0.1479	0.1429	Kiuwan	0.1529	0.1579	0.1429	0.1429
SpotBugs	0.1579	0.1479	0.1329	0.1329	SpotBugs	0.1579	0.1529	0.1329	0.1329
Vulnerability	LDAP Injection				Vulnerability	Cross-Site Scripting			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1329	0.1479	0.1479	0.1479	Snyk	0.1529	0.1529	0.1579	0.1579
Fortify	0.1579	0.1579	0.1529	0.1429	Fortify	0.1479	0.1479	0.1529	0.1479
Semgrep	0.1479	0.1329	0.1279	0.1329	Semgrep	0.1329	0.1329	0.1379	0.1529
Synopsis	0.1529	0.1429	0.1379	0.1379	Synopsis	0.1429	0.1429	0.1429	0.1429
Horusec	0.1304	0.1304	0.1304	0.1304	Horusec	0.1279	0.1279	0.1279	0.1279
Kiuwan	0.1279	0.1279	0.1429	0.1529	Kiuwan	0.1579	0.1579	0.1479	0.1379
SpotBugs	0.1429	0.1379	0.1329	0.1279	SpotBugs	0.1379	0.1379	0.1329	0.1329
Vulnerability	XPath Injection				Vulnerability	HTTP Response Splitting			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1329	0.1479	0.1479	0.1479	Snyk	0.1529	0.1529	0.1579	0.1579
Fortify	0.1579	0.1579	0.1579	0.1579	Fortify	0.1429	0.1429	0.1429	0.1429
Semgrep	0.1379	0.1379	0.1379	0.1279	Semgrep	0.1329	0.1329	0.1329	0.1329
Synopsis	0.1429	0.1429	0.1479	0.1379	Synopsis	0.1329	0.1329	0.1329	0.1329
Horusec	0.1554	0.1554	0.1554	0.1554	Horusec	0.1329	0.1329	0.1329	0.1329
Kiuwan	0.1479	0.1479	0.1529	0.1479	Kiuwan	0.1479	0.1479	0.1529	0.1529
SpotBugs	0.1529	0.1529	0.1429	0.1329	SpotBugs	0.1579	0.1579	0.1479	0.1479
Vulnerability	Improper Error Handling				Vulnerability	Trust Boundary Violation			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1329	0.1329	0.1329	0.1329	Snyk	0.1479	0.1479	0.1479	0.1579
Fortify	0.1579	0.1579	0.1579	0.1429	Fortify	0.1329	0.1329	0.1379	0.1429

Semgrep	0.1479	0.1429	0.1429	0.1529	Semgrep	0.1379	0.1429	0.1429	0.1479
Synopsis	0.1329	0.1329	0.1329	0.1329	Synopsis	0.1579	0.1579	0.1579	0.1529
Horusec	0.1304	0.1304	0.1304	0.1304	Horusec	0.1279	0.1279	0.1279	0.1279
Kiuwan	0.1429	0.1479	0.1479	0.1479	Kiuwan	0.1429	0.1379	0.1329	0.1329
SpotBugs	0.1329	0.1329	0.1329	0.1329	SpotBugs	0.1529	0.1529	0.1529	0.1379
Vulnerability	Method Tampering				Vulnerability	XML External Entities			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1379	0.1379	0.1379	0.1379	Snyk	0.1579	0.1579	0.1579	0.1529
Fortify	0.1379	0.1379	0.1379	0.1379	Fortify	0.1304	0.1304	0.1304	0.1279
Semgrep	0.1529	0.1529	0.1529	0.1529	Semgrep	0.1529	0.1529	0.1529	0.1429
Synopsis	0.1379	0.1379	0.1379	0.1379	Synopsis	0.1429	0.1429	0.1429	0.1479
Horusec	0.1379	0.1379	0.1379	0.1379	Horusec	0.1304	0.1304	0.1304	0.1329
Kiuwan	0.1479	0.1429	0.1429	0.1429	Kiuwan	0.1379	0.1379	0.1379	0.1379
SpotBugs	0.1379	0.1379	0.1379	0.1379	SpotBugs	0.1479	0.1479	0.1479	0.1579
Vulnerability	Bad Programming of Cookies				Vulnerability	Insecure Use of Hard Coded Constants			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1479	0.1479	0.1479	0.1479	Snyk	0.1579	0.1579	0.1579	0.1579
Fortify	0.1379	0.1379	0.1379	0.1379	Fortify	0.1379	0.1329	0.1329	0.1429
Semgrep	0.1579	0.1579	0.1579	0.1529	Semgrep	0.1279	0.1279	0.1279	0.1279
Synopsis	0.1529	0.1529	0.1529	0.1579	Synopsis	0.1529	0.1529	0.1529	0.1379
Horusec	0.1329	0.1329	0.1329	0.1329	Horusec	0.1329	0.1379	0.1379	0.1329
Kiuwan	0.1279	0.1279	0.1279	0.1279	Kiuwan	0.1479	0.1479	0.1479	0.1529
SpotBugs	0.1429	0.1429	0.1429	0.1429	SpotBugs	0.1429	0.1429	0.1429	0.1479
Vulnerability	Vulnerable Third-Party Components				Vulnerability	Bypassing Authentication			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1404	0.1354	0.1354	0.1454	Snyk	0.1429	0.1429	0.1429	0.1429
Fortify	0.1579	0.1579	0.1579	0.1579	Fortify	0.1429	0.1429	0.1429	0.1429
Semgrep	0.1479	0.1429	0.1429	0.1529	Semgrep	0.1429	0.1429	0.1429	0.1429
Synopsis	0.1529	0.1429	0.1379	0.1379	Synopsis	0.1429	0.1429	0.1429	0.1429
Horusec	0.1329	0.1479	0.1479	0.1379	Horusec	0.1429	0.1429	0.1429	0.1429
Kiuwan	0.1579	0.1579	0.1579	0.1579	Kiuwan	0.1429	0.1429	0.1429	0.1429
SpotBugs	0.1479	0.1479	0.1479	0.1579	SpotBugs	0.1429	0.1429	0.1429	0.1429
Vulnerability	Hard Coded Passwords				Vulnerability	Insecure Deserialization			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1529	0.1529	0.1529	0.1479	Snyk	0.1454	0.1504	0.1504	0.1554
Fortify	0.1329	0.1329	0.1329	0.1329	Fortify	0.1304	0.1304	0.1304	0.1354
Semgrep	0.1379	0.1379	0.1379	0.1429	Semgrep	0.1529	0.1429	0.1379	0.1279
Synopsis	0.1579	0.1579	0.1579	0.1529	Synopsis	0.1579	0.1579	0.1579	0.1479
Horusec	0.1279	0.1279	0.1279	0.1279	Horusec	0.1304	0.1304	0.1304	0.1354
Kiuwan	0.1479	0.1479	0.1429	0.1379	Kiuwan	0.1379	0.1379	0.1429	0.1429
SpotBugs	0.1429	0.1429	0.1479	0.1579	SpotBugs	0.1454	0.1504	0.1504	0.1554
Vulnerability	Improper Output Neutralization for Logs				Vulnerability	Server-Side Request Forgery			
Tool	1	2	3	4	Tool	1	2	3	4
Snyk	0.1429	0.1429	0.1429	0.1479	Snyk	0.1529	0.1529	0.1529	0.1529
Fortify	0.1579	0.1579	0.1579	0.1379	Fortify	0.1304	0.1304	0.1304	0.1304
Semgrep	0.1529	0.1529	0.1529	0.1579	Semgrep	0.1579	0.1579	0.1579	0.1429
Synopsis	0.1329	0.1379	0.1379	0.1329	Synopsis	0.1429	0.1429	0.1429	0.1579
Horusec	0.1279	0.1279	0.1279	0.1279	Horusec	0.1304	0.1304	0.1304	0.1304
Kiuwan	0.1479	0.1479	0.1479	0.1479	Kiuwan	0.1479	0.1479	0.1479	0.1479
SpotBugs	0.1329	0.1329	0.1329	0.1579	SpotBugs	0.1379	0.1379	0.1379	0.1379
1 - Business Critical | 2 - Heightened Critical | 3 - Best Effort | 4 - Minimum Effort									

Table 5.1: Weights of each tool for each scenario regarding all the vulnerabilities

Results obtained in A1: Broken Access Control

A1: Broken Access Control													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Path Traversal													
C, D	392	9	782	828	97.76%	33.39%	B, C	378	23	112	1498	88.28%	94.26%
B, D	385	16	782	828	96.01%	32.99%	B, E	340	61	112	1498	75.39%	84.79%
B, C	366	35	732	878	91.27%	33.33%	C, D	392	9	782	828	72.92%	97.76%
C, A	364	37	732	878	90.77%	33.21%	B, D	385	16	782	828	70.78%	96.01%
C, E	363	38	732	878	90.52%	33.15%	E, D	380	21	782	828	69.27%	94.76%
E, D	380	21	782	828	94.76%	32.7%	F, D	375	26	782	828	67.77%	93.52%
F, D	375	26	782	828	93.52%	32.41%	A, D	375	26	782	828	67.77%	93.52%
A, D	375	26	782	828	93.52%	32.41%	G, D	375	26	782	828	67.77%	93.52%
G, D	375	26	782	828	93.52%	32.41%	C, A	364	37	732	878	65.95%	90.77%
C, F	355	46	732	878	88.53%	32.66%	C, E	363	38	732	878	65.66%	90.52%
C, G	355	46	732	878	88.53%	32.66%	B, A	308	93	112	1498	65.23%	76.81%
B, E	340	61	112	1498	84.79%	75.22%	B, F	308	93	112	1498	65.23%	76.81%
B, A	308	93	112	1498	76.81%	73.33%	B, G	308	93	112	1498	65.23%	76.81%
B, F	308	93	112	1498	76.81%	73.33%	C, F	355	46	732	878	63.33%	88.53%
B, G	308	93	112	1498	76.81%	73.33%	C, G	355	46	732	878	63.33%	88.53%
A, E	289	112	123	1487	72.07%	70.15%	A, E	289	112	123	1487	59.25%	72.07%
F, E	275	126	123	1487	68.58%	69.1%	F, E	275	126	123	1487	55.18%	68.58%
G, E	275	126	123	1487	68.58%	69.1%	G, E	275	126	123	1487	55.18%	68.58%
A, F	193	208	228	1382	48.13%	45.84%	A, F	193	208	228	1382	32.24%	48.13%
A, G	193	208	228	1382	48.13%	45.84%	A, G	193	208	228	1382	32.24%	48.13%
F, G	13	388	1	1609	3.24%	92.86%	F, G	13	388	1	1609	1.67%	3.24%
Bypassing Authorization													
C, D	239	10	294	1643	95.98%	44.84%	C, D	239	10	294	1643	86.77%	95.98%
F, D	207	42	294	1643	83.13%	41.32%	F, D	207	42	294	1643	69.81%	83.13%
B, D	207	42	294	1643	83.13%	41.32%	B, D	207	42	294	1643	69.81%	83.13%
A, D	207	42	294	1643	83.13%	41.32%	A, D	207	42	294	1643	69.81%	83.13%
E, D	207	42	294	1643	83.13%	41.32%	E, D	207	42	294	1643	69.81%	83.13%
G, D	207	42	294	1643	83.13%	41.32%	G, D	207	42	294	1643	69.81%	83.13%
B, C	184	65	3	1934	73.9%	98.4%	B, C	184	65	3	1934	64.19%	73.9%
B, A	154	95	3	1934	61.85%	98.09%	B, A	154	95	3	1934	50.0%	61.85%
B, F	152	97	3	1934	61.04%	98.06%	B, F	152	97	3	1934	49.11%	61.04%
B, G	152	97	3	1934	61.04%	98.06%	B, G	152	97	3	1934	49.11%	61.04%
B, E	152	97	3	1934	61.04%	98.06%	B, E	152	97	3	1934	49.11%	61.04%
C, E	138	111	109	1828	55.42%	55.87%	C, E	138	111	109	1828	41.51%	55.42%
C, F	119	130	0	1937	47.79%	100.0%	C, F	119	130	0	1937	35.32%	47.79%
A, E	110	139	109	1828	44.18%	50.23%	A, E	110	139	109	1828	30.6%	44.18%
F, E	109	140	109	1828	43.78%	50.0%	F, E	109	140	109	1828	30.24%	43.78%
G, E	106	143	109	1828	42.57%	49.3%	G, E	106	143	109	1828	29.15%	42.57%
A, F	92	157	0	1937	36.95%	100.0%	A, F	92	157	0	1937	25.3%	36.95%
F, G	87	162	0	1937	34.94%	100.0%	F, G	87	162	0	1937	23.57%	34.94%
C, A	41	208	263	1674	16.47%	13.49%	C, A	41	208	263	1674	8.47%	16.47%
C, G	32	217	263	1674	12.85%	10.85%	C, G	32	217	263	1674	6.38%	12.85%
A, G	10	239	10	1927	4.02%	50.0%	A, G	10	239	10	1927	2.08%	4.02%
Cross-Site Request Forgery													
G, D	275	3	80	2	98.92%	77.46%	B, E	202	76	0	82	62.73%	72.66%
B, E	202	76	0	82	72.66%	100.0%	C, E	202	76	0	82	62.73%	72.66%
C, E	202	76	0	82	72.66%	100.0%	A, E	202	76	0	82	62.73%	72.66%
A, E	202	76	0	82	72.66%	100.0%	F, E	202	76	0	82	62.73%	72.66%
F, E	202	76	0	82	72.66%	100.0%	G, E	202	76	0	82	62.73%	72.66%
G, E	202	76	0	82	72.66%	100.0%	E, D	202	76	0	82	62.73%	72.66%
E, D	202	76	0	82	72.66%	100.0%	F, D	275	3	80	2	50.13%	98.92%
B, C	9	269	0	82	3.24%	100.0%	G, D	275	3	80	2	50.13%	98.92%
B, A	9	269	0	82	3.24%	100.0%	B, C	10	268	2	80	1.82%	3.6%
B, F	9	269	0	82	3.24%	100.0%	C, F	10	268	2	80	1.82%	3.6%
B, G	9	269	0	82	3.24%	100.0%	C, A	10	268	2	80	1.82%	3.6%
B, D	9	269	0	82	3.24%	100.0%	C, G	10	268	2	80	1.82%	3.6%
F, D	4	274	0	82	1.44%	100.0%	C, D	10	268	2	80	1.82%	3.6%
C, F	4	274	0	82	1.44%	100.0%	B, A	9	269	0	82	1.67%	3.24%
A, F	4	274	0	82	1.44%	100.0%	B, F	9	269	0	82	1.67%	3.24%
F, G	4	274	0	82	1.44%	100.0%	B, G	9	269	0	82	1.67%	3.24%
C, A	10	268	2	80	3.6%	83.33%	B, D	9	269	0	82	1.67%	3.24%
C, G	10	268	2	80	3.6%	83.33%	A, F	8	270	5	77	1.39%	2.88%
C, D	10	268	2	80	3.6%	83.33%	A, G	8	270	5	77	1.39%	2.88%

A, G	8	270	5	77	2.88%	61.54%	A, D	8	270	5	77	1.39%	2.88%
A, D	8	270	5	77	2.88%	61.54%	F, G	4	274	0	82	0.73%	1.44%
Insufficient Session Expiration													
B, F	17	0	0	30	100.0%	100.0%	B, F	17	0	0	30	100.0%	100.0%
C, F	17	0	0	30	100.0%	100.0%	C, F	17	0	0	30	100.0%	100.0%
A, F	17	0	0	30	100.0%	100.0%	A, F	17	0	0	30	100.0%	100.0%
F, G	17	0	0	30	100.0%	100.0%	F, G	17	0	0	30	100.0%	100.0%
F, E	17	0	0	30	100.0%	100.0%	F, E	17	0	0	30	100.0%	100.0%
F, D	17	0	0	30	100.0%	100.0%	F, D	17	0	0	30	100.0%	100.0%
B, C	0	17	0	30	0.0%	0.00%	B, C	0	17	0	30	0.0%	0.0%
B, A	0	17	0	30	0.0%	0.00%	B, A	0	17	0	30	0.0%	0.0%
B, G	0	17	0	30	0.0%	0.00%	B, G	0	17	0	30	0.0%	0.0%
B, E	0	17	0	30	0.0%	0.00%	B, E	0	17	0	30	0.0%	0.0%
B, D	0	17	0	30	0.0%	0.00%	B, D	0	17	0	30	0.0%	0.0%
C, A	0	17	0	30	0.0%	0.00%	C, A	0	17	0	30	0.0%	0.0%
C, G	0	17	0	30	0.0%	0.00%	C, G	0	17	0	30	0.0%	0.0%
C, E	0	17	0	30	0.0%	0.00%	C, E	0	17	0	30	0.0%	0.0%
C, D	0	17	0	30	0.0%	0.00%	C, D	0	17	0	30	0.0%	0.0%
A, G	0	17	0	30	0.0%	0.00%	A, G	0	17	0	30	0.0%	0.0%
A, E	0	17	0	30	0.0%	0.00%	A, E	0	17	0	30	0.0%	0.0%
A, D	0	17	0	30	0.0%	0.00%	A, D	0	17	0	30	0.0%	0.0%
G, E	0	17	0	30	0.0%	0.00%	G, E	0	17	0	30	0.0%	0.0%
G, D	0	17	0	30	0.0%	0.00%	G, D	0	17	0	30	0.0%	0.0%
E, D	0	17	0	30	0.0%	0.00%	E, D	0	17	0	30	0.0%	0.0%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.2: Ranking of combinations of 2 SAST tools regarding their performance in category A1: Broken Access Control - Business and Heightened Critical Scenarios

A1: Broken Access Control													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Path Traversal													
B, C	378	23	112	1498	84.85%	94.26%	C, F	365	36	1	1609	98.77%	99.73%
B, D	371	30	112	1498	83.94%	92.52%	F, D	359	42	1	1609	98.59%	99.72%
C, E	368	33	123	1487	82.51%	91.77%	A, F	189	212	1	1609	93.92%	99.47%
E, D	359	42	123	1487	81.31%	89.53%	F, G	13	388	1	1609	86.71%	92.86%
B, E	340	61	112	1498	79.72%	84.79%	B, C	378	23	112	1498	87.82%	77.14%
B, A	308	93	112	1498	75.03%	76.81%	B, D	371	30	112	1498	87.42%	76.81%
B, F	308	93	112	1498	75.03%	76.81%	B, E	340	61	112	1498	85.65%	75.22%
B, G	308	93	112	1498	75.03%	76.81%	C, E	368	33	123	1487	86.39%	74.95%
A, E	289	112	123	1487	71.09%	72.07%	E, D	359	42	123	1487	85.87%	74.48%
F, E	275	126	123	1487	68.84%	68.58%	B, A	308	93	112	1498	83.74%	73.33%
G, E	275	126	123	1487	68.84%	68.58%	B, F	308	93	112	1498	83.74%	73.33%
F, D	375	26	782	828	48.14%	93.52%	B, G	308	93	112	1498	83.74%	73.33%
A, D	375	26	782	828	48.14%	93.52%	A, E	289	112	123	1487	81.57%	70.15%
G, D	375	26	782	828	48.14%	93.52%	F, E	275	126	123	1487	80.64%	69.1%
C, D	366	35	732	878	48.83%	91.27%	G, E	275	126	123	1487	80.64%	69.1%
C, A	364	37	732	878	48.63%	90.77%	C, A	378	23	228	1382	80.37%	62.38%
C, F	355	46	732	878	47.72%	88.53%	A, D	363	38	228	1382	79.37%	61.42%
C, G	355	46	732	878	47.72%	88.53%	A, G	193	208	228	1382	66.38%	45.84%
A, F	193	208	228	1382	46.96%	48.13%	C, D	392	9	782	828	66.16%	33.39%
A, G	193	208	228	1382	46.96%	48.13%	C, G	355	46	732	878	63.84%	32.66%
F, G	13	388	1	1609	6.27%	3.24%	G, D	375	26	782	828	64.68%	32.41%
Bypassing Authorization													
F, D	196	53	0	1937	88.09%	78.71%	F, D	196	53	0	1937	98.67%	100.0%
B, D	196	53	3	1934	87.5%	78.71%	B, F	152	97	0	1937	97.62%	100.0%
B, C	184	65	3	1934	84.4%	73.9%	C, F	119	130	0	1937	96.86%	100.0%
B, A	154	95	3	1934	75.86%	61.85%	F, E	109	140	0	1937	96.63%	100.0%
B, F	152	97	3	1934	75.25%	61.04%	A, F	92	157	0	1937	96.25%	100.0%
B, G	152	97	3	1934	75.25%	61.04%	F, G	87	162	0	1937	96.14%	100.0%
B, E	152	97	3	1934	75.25%	61.04%	B, D	196	53	3	1934	97.91%	98.49%
E, D	196	53	109	1828	70.76%	78.71%	B, C	184	65	3	1934	97.57%	98.4%
C, D	239	10	294	1643	61.13%	95.98%	B, A	154	95	3	1934	96.7%	98.09%
C, F	119	130	0	1937	64.67%	47.79%	B, G	152	97	3	1934	96.64%	98.06%
F, E	109	140	0	1937	60.89%	43.78%	B, E	152	97	3	1934	96.64%	98.06%
A, D	207	42	294	1643	55.2%	83.13%	A, D	197	52	10	1927	96.27%	95.17%

G, D	207	42	294	1643	55.2%	83.13%	C, A	42	207	10	1927	85.53%	80.77%
C, E	138	111	109	1828	55.65%	55.42%	E, D	196	53	109	1828	80.72%	64.26%
A, F	92	157	0	1937	53.96%	36.95%	C, E	138	111	109	1828	75.07%	55.87%
F, G	87	162	0	1937	51.79%	34.94%	A, E	110	139	109	1828	71.58%	50.23%
A, E	110	139	109	1828	47.01%	44.18%	G, E	106	143	109	1828	71.02%	49.3%
G, E	106	143	109	1828	45.69%	42.57%	C, D	239	10	294	1643	72.12%	44.84%
C, A	41	208	263	1674	14.83%	16.47%	A, G	10	239	10	1927	69.48%	50.0%
C, G	32	217	263	1674	11.76%	12.85%	G, D	207	42	294	1643	69.41%	41.32%
A, G	10	239	10	1927	7.43%	4.02%	C, G	32	217	263	1674	49.69%	10.85%
Cross-Site Request Forgery													
F, D	275	3	80	2	86.89%	98.92%	B, E	202	76	0	82	75.95%	100.0%
G, D	275	3	80	2	86.89%	98.92%	C, E	202	76	0	82	75.95%	100.0%
B, E	202	76	0	82	84.17%	72.66%	A, E	202	76	0	82	75.95%	100.0%
C, E	202	76	0	82	84.17%	72.66%	F, E	202	76	0	82	75.95%	100.0%
A, E	202	76	0	82	84.17%	72.66%	G, E	202	76	0	82	75.95%	100.0%
F, E	202	76	0	82	84.17%	72.66%	E, D	202	76	0	82	75.95%	100.0%
G, E	202	76	0	82	84.17%	72.66%	B, C	9	269	0	82	61.68%	100.0%
E, D	202	76	0	82	84.17%	72.66%	B, A	9	269	0	82	61.68%	100.0%
B, C	10	268	2	80	6.9%	3.6%	B, F	9	269	0	82	61.68%	100.0%
C, F	10	268	2	80	6.9%	3.6%	B, G	9	269	0	82	61.68%	100.0%
C, A	10	268	2	80	6.9%	3.6%	B, D	9	269	0	82	61.68%	100.0%
C, G	10	268	2	80	6.9%	3.6%	F, D	4	274	0	82	61.52%	100.0%
C, D	10	268	2	80	6.9%	3.6%	C, F	4	274	0	82	61.52%	100.0%
B, A	9	269	0	82	6.27%	3.24%	A, F	4	274	0	82	61.52%	100.0%
B, F	9	269	0	82	6.27%	3.24%	F, G	4	274	0	82	61.52%	100.0%
B, G	9	269	0	82	6.27%	3.24%	G, D	275	3	80	2	58.73%	77.46%
B, D	9	269	0	82	6.27%	3.24%	C, A	10	268	2	80	53.16%	83.33%
A, F	8	270	5	77	5.5%	2.88%	C, G	10	268	2	80	53.16%	83.33%
A, G	8	270	5	77	5.5%	2.88%	C, D	10	268	2	80	53.16%	83.33%
A, D	8	270	5	77	5.5%	2.88%	A, G	8	270	5	77	41.86%	61.54%
F, G	4	274	0	82	2.84%	1.44%	A, D	8	270	5	77	41.86%	61.54%
Insufficient Session Expiration													
B, F	17	0	0	30	100.0%	100.0%	B, F	17	0	0	30	100.0%	100.0%
C, F	17	0	0	30	100.0%	100.0%	C, F	17	0	0	30	100.0%	100.0%
A, F	17	0	0	30	100.0%	100.0%	A, F	17	0	0	30	100.0%	100.0%
F, G	17	0	0	30	100.0%	100.0%	F, G	17	0	0	30	100.0%	100.0%
F, E	17	0	0	30	100.0%	100.0%	F, E	17	0	0	30	100.0%	100.0%
F, D	17	0	0	30	100.0%	100.0%	F, D	17	0	0	30	100.0%	100.0%
B, C	0	17	0	30	0.0%	0.0%	B, C	0	17	0	30	0.00%	0.00%
B, A	0	17	0	30	0.0%	0.0%	B, A	0	17	0	30	0.00%	0.00%
B, G	0	17	0	30	0.0%	0.0%	B, G	0	17	0	30	0.00%	0.00%
B, E	0	17	0	30	0.0%	0.0%	B, E	0	17	0	30	0.00%	0.00%
B, D	0	17	0	30	0.0%	0.0%	B, D	0	17	0	30	0.00%	0.00%
C, A	0	17	0	30	0.0%	0.0%	C, A	0	17	0	30	0.00%	0.00%
C, G	0	17	0	30	0.0%	0.0%	C, G	0	17	0	30	0.00%	0.00%
C, E	0	17	0	30	0.0%	0.0%	C, E	0	17	0	30	0.00%	0.00%
C, D	0	17	0	30	0.0%	0.0%	C, D	0	17	0	30	0.00%	0.00%
A, G	0	17	0	30	0.0%	0.0%	A, G	0	17	0	30	0.00%	0.00%
A, E	0	17	0	30	0.0%	0.0%	A, E	0	17	0	30	0.00%	0.00%
A, D	0	17	0	30	0.0%	0.0%	A, D	0	17	0	30	0.00%	0.00%
G, E	0	17	0	30	0.0%	0.0%	G, E	0	17	0	30	0.00%	0.00%
G, D	0	17	0	30	0.0%	0.0%	G, D	0	17	0	30	0.00%	0.00%
E, D	0	17	0	30	0.0%	0.0%	E, D	0	17	0	30	0.00%	0.00%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.3: Ranking of combinations of 2 SAST tools regarding their performance in category A1: Broken Access Control - Best and Minimum Effort Scenarios

Results obtained in A2: Cryptographic Failures

A2: Cryptographic Failures													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Use of Old/Insecure algorithms													
C, G	206	22	122	552	90.35%	62.8%	G, E	206	22	122	552	77.81%	90.35%
A, G	206	22	122	552	90.35%	62.8%	B, G	206	22	122	552	77.81%	90.35%

G, E	206	22	122	552	90.35%	62.8%	G, D	206	22	122	552	77.81%	90.35%
B, G	206	22	122	552	90.35%	62.8%	B, D	184	44	71	603	68.66%	80.7%
G, D	206	22	122	552	90.35%	62.8%	F, D	184	44	71	603	68.66%	80.7%
C, D	184	44	71	603	80.7%	72.16%	C, G	168	60	0	674	63.99%	73.68%
E, D	184	44	71	603	80.7%	72.16%	C, D	168	60	0	674	63.99%	73.68%
B, D	184	44	71	603	80.7%	72.16%	C, F	168	60	0	674	63.99%	73.68%
F, D	184	44	71	603	80.7%	72.16%	B, C	168	60	0	674	63.99%	73.68%
F, G	173	55	122	552	75.88%	58.64%	E, D	167	61	40	634	61.27%	73.25%
C, F	168	60	0	674	73.68%	100.0%	F, E	167	61	40	634	61.27%	73.25%
B, A	165	63	0	674	72.37%	100.0%	B, E	167	61	40	634	61.27%	73.25%
C, A	165	63	0	674	72.37%	100.0%	A, G	165	63	0	674	62.37%	72.37%
A, F	165	63	0	674	72.37%	100.0%	B, A	165	63	0	674	62.37%	72.37%
A, E	165	63	0	674	72.37%	100.0%	C, A	165	63	0	674	62.37%	72.37%
A, D	165	63	0	674	72.37%	100.0%	A, F	165	63	0	674	62.37%	72.37%
F, E	167	61	40	634	73.25%	80.68%	A, E	165	63	0	674	62.37%	72.37%
B, C	165	63	70	604	72.37%	70.21%	A, D	165	63	0	674	62.37%	72.37%
B, E	165	63	70	604	72.37%	70.21%	F, G	173	55	122	552	59.86%	75.88%
B, F	165	63	70	604	72.37%	70.21%	B, F	165	63	70	604	58.61%	72.37%
C, E	152	76	0	674	66.67%	100.0%	C, E	152	76	0	674	55.56%	66.67%
Deprecated Hash Functions													
B, G	277	99	13	214	73.67%	95.52%	B, G	277	99	13	214	61.86%	73.67%
C, G	277	99	13	214	73.67%	95.52%	C, G	277	99	13	214	61.86%	73.67%
G, E	277	99	13	214	73.67%	95.52%	G, E	277	99	13	214	61.86%	73.67%
F, G	277	99	13	214	73.67%	95.52%	F, G	277	99	13	214	61.86%	73.67%
A, G	277	99	13	214	73.67%	95.52%	A, G	277	99	13	214	61.86%	73.67%
G, D	277	99	13	214	73.67%	95.52%	G, D	277	99	13	214	61.86%	73.67%
A, D	199	177	14	213	52.93%	93.43%	A, D	199	177	14	213	38.84%	52.93%
B, A	185	191	0	227	49.2%	100.0%	B, C	185	191	0	227	36.71%	49.2%
B, D	185	191	0	227	49.2%	100.0%	B, E	185	191	0	227	36.71%	49.2%
B, C	182	194	2	225	48.4%	98.91%	B, F	185	191	0	227	36.71%	49.2%
C, F	182	194	2	225	48.4%	98.91%	B, A	185	191	0	227	36.71%	49.2%
C, E	182	194	2	225	48.4%	98.91%	B, D	185	191	0	227	36.71%	49.2%
C, A	182	194	2	225	48.4%	98.91%	C, F	182	194	2	225	35.7%	48.4%
C, D	182	194	2	225	48.4%	98.91%	C, E	182	194	2	225	35.7%	48.4%
B, E	180	196	2	225	47.87%	98.9%	C, A	182	194	2	225	35.7%	48.4%
F, E	180	196	2	225	47.87%	98.9%	C, D	182	194	2	225	35.7%	48.4%
A, E	180	196	2	225	47.87%	98.9%	F, E	180	196	2	225	35.18%	47.87%
E, D	180	196	2	225	47.87%	98.9%	A, E	180	196	2	225	35.18%	47.87%
B, F	175	201	2	225	46.54%	98.87%	E, D	180	196	2	225	35.18%	47.87%
A, F	175	201	2	225	46.54%	98.87%	A, F	175	201	2	225	33.9%	46.54%
F, D	175	201	2	225	46.54%	98.87%	F, D	175	201	2	225	33.9%	46.54%
Use of Weak PRNG													
C, F	296	11	52	307	96.42%	85.06%	C, F	296	11	52	307	87.71%	96.42%
C, D	296	11	52	307	96.42%	85.06%	C, D	296	11	52	307	87.71%	96.42%
C, A	296	11	52	307	96.42%	85.06%	C, A	296	11	52	307	87.71%	96.42%
B, C	296	11	52	307	96.42%	85.06%	B, C	296	11	52	307	87.71%	96.42%
C, G	296	11	52	307	96.42%	85.06%	C, G	296	11	52	307	87.71%	96.42%
C, E	296	11	52	307	96.42%	85.06%	C, E	296	11	52	307	87.71%	96.42%
B, D	286	21	5	354	93.16%	98.28%	B, D	286	21	5	354	89.32%	93.16%
A, D	286	21	5	354	93.16%	98.28%	A, D	286	21	5	354	89.32%	93.16%
F, D	286	21	5	354	93.16%	98.28%	F, D	286	21	5	354	89.32%	93.16%
G, D	286	21	5	354	93.16%	98.28%	G, D	286	21	5	354	89.32%	93.16%
E, D	286	21	5	354	93.16%	98.28%	E, D	286	21	5	354	89.32%	93.16%
F, G	254	53	0	359	82.74%	100.0%	F, G	254	53	0	359	75.59%	82.74%
A, G	244	63	0	359	79.48%	100.0%	A, G	244	63	0	359	71.32%	79.48%
B, G	241	66	0	359	78.5%	100.0%	B, G	241	66	0	359	70.06%	78.5%
B, F	237	70	0	359	77.2%	100.0%	B, F	237	70	0	359	68.4%	77.2%
A, F	237	70	0	359	77.2%	100.0%	A, F	237	70	0	359	68.4%	77.2%
F, E	237	70	0	359	77.2%	100.0%	F, E	237	70	0	359	68.4%	77.2%
B, A	227	80	0	359	73.94%	100.0%	B, A	227	80	0	359	64.31%	73.94%
A, E	227	80	0	359	73.94%	100.0%	A, E	227	80	0	359	64.31%	73.94%
B, E	224	83	0	359	72.96%	100.0%	B, E	224	83	0	359	63.1%	72.96%
G, E	226	81	55	304	73.62%	80.43%	G, E	226	81	55	304	58.27%	73.62%
Seeds Hard Coded in PRNG													
B, F	17	0	0	30	100.0%	100.0%	B, F	17	0	0	30	100.0%	100.0%
B, G	17	0	0	30	100.0%	100.0%	B, G	17	0	0	30	100.0%	100.0%
C, F	17	0	0	30	100.0%	100.0%	C, F	17	0	0	30	100.0%	100.0%
C, G	17	0	0	30	100.0%	100.0%	C, G	17	0	0	30	100.0%	100.0%
A, F	17	0	0	30	100.0%	100.0%	A, F	17	0	0	30	100.0%	100.0%

A, G	17	0	0	30	100.0%	100.0%	A, G	17	0	0	30	100.0%	100.0%
F, G	17	0	0	30	100.0%	100.0%	F, G	17	0	0	30	100.0%	100.0%
F, E	17	0	0	30	100.0%	100.0%	F, E	17	0	0	30	100.0%	100.0%
F, D	17	0	0	30	100.0%	100.0%	F, D	17	0	0	30	100.0%	100.0%
G, E	17	0	0	30	100.0%	100.0%	G, E	17	0	0	30	100.0%	100.0%
G, D	17	0	0	30	100.0%	100.0%	G, D	17	0	0	30	100.0%	100.0%
B, C	0	17	0	30	0.0%	0.00%	B, C	0	17	0	30	0.0%	0.0%
B, A	0	17	0	30	0.0%	0.00%	B, A	0	17	0	30	0.0%	0.0%
B, E	0	17	0	30	0.0%	0.00%	B, E	0	17	0	30	0.0%	0.0%
B, D	0	17	0	30	0.0%	0.00%	B, D	0	17	0	30	0.0%	0.0%
C, A	0	17	0	30	0.0%	0.00%	C, A	0	17	0	30	0.0%	0.0%
C, E	0	17	0	30	0.0%	0.00%	C, E	0	17	0	30	0.0%	0.0%
C, D	0	17	0	30	0.0%	0.00%	C, D	0	17	0	30	0.0%	0.0%
A, E	0	17	0	30	0.0%	0.00%	A, E	0	17	0	30	0.0%	0.0%
A, D	0	17	0	30	0.0%	0.00%	A, D	0	17	0	30	0.0%	0.0%
E, D	0	17	0	30	0.0%	0.00%	E, D	0	17	0	30	0.0%	0.0%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.4: Ranking of combinations of 2 SAST tools regarding their performance in category A2: Cryptographic Failures - Business and Heightened Critical Scenarios

A2: Cryptographic Failures													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Use of Old/Insecure algorithms													
C, G	168	60	0	674	84.85%	73.68%	C, G	168	60	0	674	95.91%	100.0%
C, D	168	60	0	674	84.85%	73.68%	C, D	168	60	0	674	95.91%	100.0%
C, F	168	60	0	674	84.85%	73.68%	C, F	168	60	0	674	95.91%	100.0%
B, C	168	60	0	674	84.85%	73.68%	B, C	168	60	0	674	95.91%	100.0%
A, G	165	63	0	674	83.97%	72.37%	A, G	165	63	0	674	95.73%	100.0%
B, A	165	63	0	674	83.97%	72.37%	B, A	165	63	0	674	95.73%	100.0%
C, A	165	63	0	674	83.97%	72.37%	C, A	165	63	0	674	95.73%	100.0%
A, F	165	63	0	674	83.97%	72.37%	A, F	165	63	0	674	95.73%	100.0%
A, E	165	63	0	674	83.97%	72.37%	A, E	165	63	0	674	95.73%	100.0%
A, D	165	63	0	674	83.97%	72.37%	A, D	165	63	0	674	95.73%	100.0%
C, E	152	76	0	674	80.0%	66.67%	C, E	152	76	0	674	94.93%	100.0%
B, D	184	44	71	603	76.19%	80.7%	G, E	167	61	40	634	85.95%	80.68%
F, D	184	44	71	603	76.19%	80.7%	E, D	167	61	40	634	85.95%	80.68%
G, E	167	61	40	634	76.78%	73.25%	F, E	167	61	40	634	85.95%	80.68%
E, D	167	61	40	634	76.78%	73.25%	B, E	167	61	40	634	85.95%	80.68%
F, E	167	61	40	634	76.78%	73.25%	B, D	184	44	71	603	82.68%	72.16%
B, E	167	61	40	634	76.78%	73.25%	F, D	184	44	71	603	82.68%	72.16%
B, G	206	22	122	552	74.1%	90.35%	B, F	165	63	70	604	80.38%	70.21%
G, D	206	22	122	552	74.1%	90.35%	B, G	206	22	122	552	79.49%	62.8%
B, F	165	63	70	604	71.27%	72.37%	G, D	206	22	122	552	79.49%	62.8%
F, G	173	55	122	552	66.16%	75.88%	F, G	173	55	122	552	74.79%	58.64%
Deprecated Hash Functions													
B, G	277	99	13	214	83.18%	73.67%	B, G	185	191	0	227	77.15%	100.0%
C, G	277	99	13	214	83.18%	73.67%	C, G	182	194	2	225	76.31%	98.91%
G, E	277	99	13	214	83.18%	73.67%	B, C	182	194	2	225	76.31%	98.91%
F, G	277	99	13	214	83.18%	73.67%	C, F	182	194	2	225	76.31%	98.91%
A, G	277	99	13	214	83.18%	73.67%	C, E	182	194	2	225	76.31%	98.91%
G, D	277	99	13	214	83.18%	73.67%	G, E	180	196	2	225	76.17%	98.9%
A, D	199	177	14	213	67.57%	52.93%	B, E	180	196	2	225	76.17%	98.9%
B, C	185	191	0	227	65.95%	49.2%	F, E	180	196	2	225	76.17%	98.9%
B, E	185	191	0	227	65.95%	49.2%	F, G	175	201	2	225	75.84%	98.87%
B, F	185	191	0	227	65.95%	49.2%	B, F	175	201	2	225	75.84%	98.87%
B, A	185	191	0	227	65.95%	49.2%	A, G	144	232	0	227	74.73%	100.0%
B, D	185	191	0	227	65.95%	49.2%	B, A	144	232	0	227	74.73%	100.0%
C, F	182	194	2	225	65.0%	48.4%	C, A	144	232	0	227	74.73%	100.0%
C, E	182	194	2	225	65.0%	48.4%	A, E	144	232	0	227	74.73%	100.0%
C, A	182	194	2	225	65.0%	48.4%	A, F	144	232	0	227	74.73%	100.0%
C, D	182	194	2	225	65.0%	48.4%	G, D	199	177	14	213	74.02%	93.43%
F, E	180	196	2	225	64.52%	47.87%	A, D	199	177	14	213	74.02%	93.43%
A, E	180	196	2	225	64.52%	47.87%	B, D	199	177	14	213	74.02%	93.43%
E, D	180	196	2	225	64.52%	47.87%	C, D	199	177	14	213	74.02%	93.43%
A, F	175	201	2	225	63.29%	46.54%	E, D	199	177	14	213	74.02%	93.43%

F, D	175	201	2	225	63.29%	46.54%	F, D	199	177	14	213	74.02%	93.43%
Use of Weak PRNG													
B, D	286	21	5	354	95.65%	93.16%	C, F	271	36	0	359	95.44%	100.0%
A, D	286	21	5	354	95.65%	93.16%	B, D	286	21	5	354	96.34%	98.28%
F, D	286	21	5	354	95.65%	93.16%	A, D	286	21	5	354	96.34%	98.28%
G, D	286	21	5	354	95.65%	93.16%	F, D	286	21	5	354	96.34%	98.28%
E, D	286	21	5	354	95.65%	93.16%	G, D	286	21	5	354	96.34%	98.28%
C, F	296	11	52	307	90.38%	96.42%	E, D	286	21	5	354	96.34%	98.28%
C, D	296	11	52	307	90.38%	96.42%	C, D	286	21	5	354	96.34%	98.28%
C, A	296	11	52	307	90.38%	96.42%	C, A	261	46	0	359	94.32%	100.0%
B, C	296	11	52	307	90.38%	96.42%	B, C	258	49	0	359	94.0%	100.0%
C, G	296	11	52	307	90.38%	96.42%	F, G	254	53	0	359	93.57%	100.0%
C, E	296	11	52	307	90.38%	96.42%	A, G	244	63	0	359	92.54%	100.0%
F, G	254	53	0	359	90.55%	82.74%	B, G	241	66	0	359	92.24%	100.0%
A, G	244	63	0	359	88.57%	79.48%	B, F	237	70	0	359	91.84%	100.0%
B, G	241	66	0	359	87.96%	78.5%	A, F	237	70	0	359	91.84%	100.0%
B, F	237	70	0	359	87.13%	77.2%	F, E	237	70	0	359	91.84%	100.0%
A, F	237	70	0	359	87.13%	77.2%	B, A	227	80	0	359	90.89%	100.0%
F, E	237	70	0	359	87.13%	77.2%	A, E	227	80	0	359	90.89%	100.0%
B, A	227	80	0	359	85.02%	73.94%	B, E	224	83	0	359	90.61%	100.0%
A, E	227	80	0	359	85.02%	73.94%	C, G	296	11	52	307	90.8%	85.06%
B, E	224	83	0	359	84.37%	72.96%	C, E	296	11	52	307	90.8%	85.06%
G, E	226	81	55	304	76.87%	73.62%	G, E	226	81	55	304	79.69%	80.43%
Seeds Hard Coded in PRNG													
B, F	17	0	0	30	100.0%	100.0%	B, F	17	0	0	30	100.0%	100.0%
B, G	17	0	0	30	100.0%	100.0%	B, G	17	0	0	30	100.0%	100.0%
C, F	17	0	0	30	100.0%	100.0%	C, F	17	0	0	30	100.0%	100.0%
C, G	17	0	0	30	100.0%	100.0%	C, G	17	0	0	30	100.0%	100.0%
A, F	17	0	0	30	100.0%	100.0%	A, F	17	0	0	30	100.0%	100.0%
A, G	17	0	0	30	100.0%	100.0%	A, G	17	0	0	30	100.0%	100.0%
F, G	17	0	0	30	100.0%	100.0%	F, G	17	0	0	30	100.0%	100.0%
F, E	17	0	0	30	100.0%	100.0%	F, E	17	0	0	30	100.0%	100.0%
F, D	17	0	0	30	100.0%	100.0%	F, D	17	0	0	30	100.0%	100.0%
G, E	17	0	0	30	100.0%	100.0%	G, E	17	0	0	30	100.0%	100.0%
G, D	17	0	0	30	100.0%	100.0%	G, D	17	0	0	30	100.0%	100.0%
B, C	0	17	0	30	0.0%	0.0%	B, C	0	17	0	30	0.00%	0.00%
B, A	0	17	0	30	0.0%	0.0%	B, A	0	17	0	30	0.00%	0.00%
B, E	0	17	0	30	0.0%	0.0%	B, E	0	17	0	30	0.00%	0.00%
B, D	0	17	0	30	0.0%	0.0%	B, D	0	17	0	30	0.00%	0.00%
C, A	0	17	0	30	0.0%	0.0%	C, A	0	17	0	30	0.00%	0.00%
C, E	0	17	0	30	0.0%	0.0%	C, E	0	17	0	30	0.00%	0.00%
C, D	0	17	0	30	0.0%	0.0%	C, D	0	17	0	30	0.00%	0.00%
A, E	0	17	0	30	0.0%	0.0%	A, E	0	17	0	30	0.00%	0.00%
A, D	0	17	0	30	0.0%	0.0%	A, D	0	17	0	30	0.00%	0.00%
E, D	0	17	0	30	0.0%	0.0%	E, D	0	17	0	30	0.00%	0.00%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.5: Ranking of combinations of 2 SAST tools regarding their performance in category A2: Cryptographic Failures - Best and Minimum Effort Scenarios

Results obtained in A3: Injection

A3: Injection													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Cross-Site Scripting													
A, E	498	115	965	1315	81.24%	34.04%	B, F	475	138	167	2113	65.93%	77.49%
C, E	498	115	965	1315	81.24%	34.04%	B, C	460	153	167	2113	62.93%	75.04%
F, E	498	115	965	1315	81.24%	34.04%	B, A	446	167	167	2113	60.18%	72.76%
B, E	497	116	965	1315	81.08%	33.99%	A, E	498	115	965	1315	56.43%	81.24%
E, D	497	116	965	1315	81.08%	33.99%	C, E	498	115	965	1315	56.43%	81.24%
G, E	496	117	965	1315	80.91%	33.95%	F, E	498	115	965	1315	56.43%	81.24%
B, F	475	138	167	2113	77.49%	73.99%	B, E	497	116	965	1315	56.25%	81.08%
B, C	460	153	167	2113	75.04%	73.37%	E, D	497	116	965	1315	56.25%	81.08%
B, A	446	167	167	2113	72.76%	72.76%	G, E	496	117	965	1315	56.07%	80.91%
B, D	444	169	167	2113	72.43%	72.67%	B, D	444	169	167	2113	59.79%	72.43%

B, G	432	181	167	2113	70.47%	72.12%	B, G	432	181	167	2113	57.49%	70.47%
C, F	419	194	203	2077	68.35%	67.36%	C, F	419	194	203	2077	54.49%	68.35%
A, D	426	187	832	1448	69.49%	33.86%	A, D	426	187	832	1448	46.21%	69.49%
C, D	387	226	203	2077	63.13%	65.59%	C, D	387	226	203	2077	48.68%	63.13%
G, D	395	218	832	1448	64.44%	32.19%	G, D	395	218	832	1448	41.22%	64.44%
C, A	365	248	203	2077	59.54%	64.26%	C, A	365	248	203	2077	44.85%	59.54%
C, G	360	253	203	2077	58.73%	63.94%	C, G	360	253	203	2077	43.99%	58.73%
F, D	352	261	576	1704	57.42%	37.93%	F, D	352	261	576	1704	37.94%	57.42%
A, F	347	266	576	1704	56.61%	37.59%	A, F	347	266	576	1704	37.17%	56.61%
F, G	347	266	576	1704	56.61%	37.59%	F, G	347	266	576	1704	37.17%	56.61%
A, G	147	466	67	2213	23.98%	68.69%	A, G	147	466	67	2213	14.51%	23.98%
SQL Injection													
B, D	615	0	537	1356	100.0%	53.39%	B, D	615	0	537	1356	85.82%	100.0%
F, D	615	0	537	1356	100.0%	53.39%	F, D	615	0	537	1356	85.82%	100.0%
C, D	615	0	537	1356	100.0%	53.39%	C, D	615	0	537	1356	85.82%	100.0%
E, D	615	0	537	1356	100.0%	53.39%	G, D	615	0	537	1356	85.82%	100.0%
G, D	615	0	537	1356	100.0%	53.39%	A, D	615	0	537	1356	85.82%	100.0%
A, D	615	0	537	1356	100.0%	53.39%	B, G	555	60	126	1767	82.84%	90.24%
B, C	549	66	281	1612	89.27%	66.14%	F, G	545	70	128	1765	80.58%	88.62%
C, F	549	66	281	1612	89.27%	66.14%	A, G	552	63	420	1473	75.2%	89.76%
C, G	549	66	281	1612	89.27%	66.14%	B, C	549	66	281	1612	77.85%	89.27%
G, E	543	72	329	1564	88.29%	62.27%	C, F	549	66	281	1612	77.85%	89.27%
C, E	539	76	329	1564	87.64%	62.1%	C, G	549	66	281	1612	77.85%	89.27%
B, E	537	78	329	1564	87.32%	62.01%	E, D	544	71	329	1564	75.66%	88.46%
F, E	526	89	329	1564	85.53%	61.52%	G, E	543	72	329	1564	75.45%	88.29%
A, G	552	63	420	1473	89.76%	56.79%	C, A	544	71	420	1473	73.54%	88.46%
C, A	544	71	420	1473	88.46%	56.43%	B, A	541	74	420	1473	72.92%	87.97%
B, A	541	74	420	1473	87.97%	56.3%	C, E	539	76	329	1564	74.61%	87.64%
A, F	530	85	420	1473	86.18%	55.79%	B, E	537	78	329	1564	74.19%	87.32%
B, G	535	80	679	1214	86.99%	44.07%	A, F	530	85	420	1473	70.66%	86.18%
F, G	535	80	679	1214	86.99%	44.07%	F, E	526	89	329	1564	71.91%	85.53%
A, E	518	97	329	1564	84.23%	61.16%	A, E	518	97	329	1564	70.27%	84.23%
B, F	463	152	126	1767	75.28%	78.61%	B, F	463	152	126	1767	63.48%	75.28%
HTTP Response Splitting													
B, D	391	4	299	1108	98.99%	56.67%	B, D	391	4	299	1108	87.97%	98.99%
E, D	372	23	299	1108	94.18%	55.44%	E, D	372	23	299	1108	81.43%	94.18%
C, D	372	23	299	1108	94.18%	55.44%	C, D	372	23	299	1108	81.43%	94.18%
A, D	372	23	299	1108	94.18%	55.44%	A, D	372	23	299	1108	81.43%	94.18%
F, D	372	23	299	1108	94.18%	55.44%	F, D	372	23	299	1108	81.43%	94.18%
G, D	372	23	299	1108	94.18%	55.44%	G, D	372	23	299	1108	81.43%	94.18%
B, E	315	80	6	1401	79.75%	98.13%	B, E	315	80	6	1401	71.5%	79.75%
B, C	266	129	6	1401	67.34%	97.79%	B, C	266	129	6	1401	56.2%	67.34%
C, E	265	130	42	1365	67.09%	86.32%	C, E	265	130	42	1365	55.05%	67.09%
B, A	253	142	6	1401	64.05%	97.68%	B, A	253	142	6	1401	52.4%	64.05%
B, F	253	142	6	1401	64.05%	97.68%	B, F	253	142	6	1401	52.4%	64.05%
B, G	253	142	6	1401	64.05%	97.68%	B, G	253	142	6	1401	52.4%	64.05%
A, E	171	224	42	1365	43.29%	80.28%	A, E	171	224	42	1365	30.37%	43.29%
F, E	171	224	42	1365	43.29%	80.28%	F, E	171	224	42	1365	30.37%	43.29%
G, E	171	224	42	1365	43.29%	80.28%	G, E	171	224	42	1365	30.37%	43.29%
C, A	139	256	233	1174	35.19%	37.37%	C, A	139	256	233	1174	20.87%	35.19%
C, F	139	256	233	1174	35.19%	37.37%	C, F	139	256	233	1174	20.87%	35.19%
C, G	139	256	233	1174	35.19%	37.37%	C, G	139	256	233	1174	20.87%	35.19%
A, F	0	395	0	1407	0.0%	0.00%	A, F	0	395	0	1407	0.0%	0.0%
A, G	0	395	0	1407	0.0%	0.00%	A, G	0	395	0	1407	0.0%	0.0%
F, G	0	395	0	1407	0.0%	0.00%	F, G	0	395	0	1407	0.0%	0.0%
LDAP Injection													
G, D	293	0	292	173	100.0%	50.09%	G, D	292	1	7	458	98.74%	99.66%
E, D	293	0	292	173	100.0%	50.09%	F, G	292	1	7	458	98.74%	99.66%
B, D	293	0	292	173	100.0%	50.09%	B, D	292	1	13	452	98.1%	99.66%
B, G	291	2	7	458	99.32%	97.65%	B, A	292	1	13	452	98.1%	99.66%
G, E	288	5	7	458	98.29%	97.63%	B, F	292	1	13	452	98.1%	99.66%
C, G	292	1	80	385	99.66%	78.49%	B, G	291	2	7	458	98.23%	99.32%
C, E	292	1	80	385	99.66%	78.49%	A, G	291	2	7	458	98.23%	99.32%
B, C	292	1	80	385	99.66%	78.49%	G, E	288	5	7	458	96.71%	98.29%
C, A	292	1	80	385	99.66%	78.49%	C, G	292	1	80	385	90.92%	99.66%
C, F	292	1	80	385	99.66%	78.49%	C, E	292	1	80	385	90.92%	99.66%
C, D	292	1	80	385	99.66%	78.49%	B, C	292	1	80	385	90.92%	99.66%
A, E	292	1	256	209	99.66%	53.28%	C, A	292	1	80	385	90.92%	99.66%
B, A	292	1	256	209	99.66%	53.28%	C, F	292	1	80	385	90.92%	99.66%

A, D	292	1	256	209	99.66%	53.28%	C, D	292	1	80	385	90.92%	99.66%
A, G	291	2	256	209	99.32%	53.2%	A, E	292	1	256	209	72.06%	99.66%
F, G	292	1	279	186	99.66%	51.14%	E, D	293	0	292	173	68.6%	100.0%
F, E	292	1	279	186	99.66%	51.14%	A, D	293	0	292	173	68.6%	100.0%
B, F	292	1	279	186	99.66%	51.14%	F, E	292	1	279	186	69.59%	99.66%
A, F	292	1	279	186	99.66%	51.14%	A, F	292	1	279	186	69.59%	99.66%
F, D	292	1	279	186	99.66%	51.14%	F, D	292	1	279	186	69.59%	99.66%
B, E	225	68	13	452	76.79%	94.54%	B, E	225	68	13	452	66.81%	76.79%
OS Command Injection													
G, D	387	0	391	178	100.0%	49.74%	B, G	383	4	45	524	94.54%	98.97%
B, D	387	0	391	178	100.0%	49.74%	B, D	383	4	45	524	94.54%	98.97%
F, D	387	0	391	178	100.0%	49.74%	B, C	383	4	45	524	94.54%	98.97%
A, D	387	0	391	178	100.0%	49.74%	A, G	369	18	5	564	92.71%	95.35%
E, D	387	0	391	178	100.0%	49.74%	F, G	367	20	5	564	91.96%	94.83%
C, D	387	0	391	178	100.0%	49.74%	G, E	383	4	125	444	87.58%	98.97%
A, G	369	18	5	564	95.35%	98.66%	B, E	317	70	45	524	71.27%	81.91%
B, G	383	4	45	524	98.97%	89.49%	G, D	387	0	391	178	65.64%	100.0%
G, E	383	4	125	444	98.97%	75.39%	F, D	387	0	391	178	65.64%	100.0%
C, G	384	3	396	173	99.22%	49.23%	A, D	387	0	391	178	65.64%	100.0%
B, C	384	3	396	173	99.22%	49.23%	E, D	387	0	391	178	65.64%	100.0%
C, F	384	3	396	173	99.22%	49.23%	C, G	384	3	396	173	64.31%	99.22%
C, A	384	3	396	173	99.22%	49.23%	C, F	384	3	396	173	64.31%	99.22%
C, E	384	3	396	173	99.22%	49.23%	C, A	384	3	396	173	64.31%	99.22%
F, G	367	20	5	564	94.83%	98.66%	C, E	384	3	396	173	64.31%	99.22%
B, E	317	70	45	524	81.91%	87.57%	C, D	384	3	396	173	64.31%	99.22%
B, A	295	92	45	524	76.23%	86.76%	B, A	295	92	45	524	64.15%	76.23%
B, F	295	92	45	524	76.23%	86.76%	B, F	295	92	45	524	64.15%	76.23%
F, E	273	114	125	444	70.54%	68.59%	F, E	273	114	125	444	52.4%	70.54%
A, E	273	114	125	444	70.54%	68.59%	A, E	273	114	125	444	52.4%	70.54%
A, F	222	165	67	502	57.36%	76.82%	A, F	222	165	67	502	41.76%	57.36%
XPath Injection													
B, D	280	0	282	591	100.0%	49.82%	B, C	278	2	36	837	96.88%	99.29%
G, D	280	0	282	591	100.0%	49.82%	C, A	278	2	36	837	96.88%	99.29%
F, D	280	0	282	591	100.0%	49.82%	C, F	278	2	36	837	96.88%	99.29%
E, D	280	0	282	591	100.0%	49.82%	C, G	278	2	36	837	96.88%	99.29%
A, D	280	0	282	591	100.0%	49.82%	C, E	278	2	36	837	96.88%	99.29%
B, C	278	2	36	837	99.29%	88.54%	C, D	278	2	36	837	96.88%	99.29%
C, A	278	2	36	837	99.29%	88.54%	B, D	280	0	282	591	83.85%	100.0%
C, F	278	2	36	837	99.29%	88.54%	G, D	280	0	282	591	83.85%	100.0%
C, G	278	2	36	837	99.29%	88.54%	F, D	280	0	282	591	83.85%	100.0%
C, E	278	2	36	837	99.29%	88.54%	E, D	280	0	282	591	83.85%	100.0%
C, D	278	2	36	837	99.29%	88.54%	A, D	280	0	282	591	83.85%	100.0%
B, E	179	101	169	704	63.93%	51.44%	B, E	179	101	169	704	46.21%	63.93%
A, E	179	101	169	704	63.93%	51.44%	A, E	179	101	169	704	46.21%	63.93%
F, E	179	101	169	704	63.93%	51.44%	F, E	179	101	169	704	46.21%	63.93%
G, E	179	101	169	704	63.93%	51.44%	G, E	179	101	169	704	46.21%	63.93%
A, F	123	157	120	753	43.93%	50.62%	A, F	123	157	120	753	28.59%	43.93%
B, F	120	160	120	753	42.86%	50.0%	B, F	120	160	120	753	27.67%	42.86%
F, G	120	160	120	753	42.86%	50.0%	F, G	120	160	120	753	27.67%	42.86%
B, A	69	211	67	806	24.64%	50.74%	B, A	69	211	67	806	14.41%	24.64%
A, G	69	211	67	806	24.64%	50.74%	A, G	69	211	67	806	14.41%	24.64%
B, G	16	264	7	866	5.71%	69.57%	B, G	16	264	7	866	3.0%	5.71%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.6: Ranking of combinations of 2 SAST tools regarding their performance in category A3: Injection - Business and Heightened Critical Scenarios

A3: Injection													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Cross-Site Scripting													
B, E	524	89	167	2113	80.37%	85.48%	A, E	501	112	67	2213	91.69%	88.2%
B, F	475	138	167	2113	75.7%	77.49%	A, F	391	222	67	2213	88.13%	85.37%
C, E	487	126	203	2077	74.75%	79.45%	C, A	379	234	67	2213	87.71%	84.98%
B, C	460	153	167	2113	74.19%	75.04%	A, D	352	261	67	2213	86.73%	84.01%
B, A	446	167	167	2113	72.76%	72.76%	B, E	524	89	167	2113	85.9%	75.83%
B, D	444	169	167	2113	72.55%	72.43%	B, F	475	138	167	2113	83.93%	73.99%

B, G	432	181	167	2113	71.29%	70.47%	B, C	460	153	167	2113	83.31%	73.37%
C, F	419	194	203	2077	67.85%	68.35%	B, A	446	167	167	2113	82.72%	72.76%
A, D	352	261	67	2213	68.22%	57.42%	B, D	444	169	167	2113	82.63%	72.67%
C, D	387	226	203	2077	64.34%	63.13%	B, G	432	181	167	2113	82.12%	72.12%
C, A	365	248	203	2077	61.81%	59.54%	C, E	487	126	203	2077	82.43%	70.58%
C, G	360	253	203	2077	61.22%	58.73%	A, G	147	466	67	2213	75.65%	68.69%
A, E	498	115	965	1315	47.98%	81.24%	C, F	419	194	203	2077	79.41%	67.36%
F, E	498	115	965	1315	47.98%	81.24%	C, D	387	226	203	2077	77.89%	65.59%
E, D	497	116	965	1315	47.9%	81.08%	C, G	360	253	203	2077	76.54%	63.94%
G, E	496	117	965	1315	47.83%	80.91%	F, E	457	156	576	1704	67.93%	44.24%
F, D	352	261	576	1704	45.68%	57.42%	F, D	352	261	576	1704	62.32%	37.93%
A, F	347	266	576	1704	45.18%	56.61%	F, G	347	266	576	1704	62.05%	37.59%
F, G	347	266	576	1704	45.18%	56.61%	E, D	497	116	965	1315	62.94%	33.99%
G, D	395	218	832	1448	42.93%	64.44%	G, E	496	117	965	1315	62.89%	33.95%
A, G	147	466	67	2213	35.55%	23.98%	G, D	395	218	832	1448	59.55%	32.19%
SQL Injection													
B, D	555	60	126	1767	85.65%	90.24%	B, D	555	60	126	1767	89.11%	81.5%
B, G	555	60	126	1767	85.65%	90.24%	B, G	555	60	126	1767	89.11%	81.5%
B, C	555	60	126	1767	85.65%	90.24%	B, C	555	60	126	1767	89.11%	81.5%
B, E	548	67	126	1767	85.03%	89.11%	B, E	548	67	126	1767	88.83%	81.31%
F, D	545	70	128	1765	84.63%	88.62%	B, A	542	73	126	1767	88.59%	81.14%
F, G	545	70	128	1765	84.63%	88.62%	F, D	545	70	128	1765	88.58%	80.98%
C, F	545	70	128	1765	84.63%	88.62%	F, G	545	70	128	1765	88.58%	80.98%
B, A	542	73	126	1767	84.49%	88.13%	C, F	545	70	128	1765	88.58%	80.98%
F, E	527	88	128	1765	82.99%	85.69%	F, E	527	88	128	1765	87.85%	80.46%
A, F	521	94	128	1765	82.44%	84.72%	A, F	521	94	128	1765	87.61%	80.28%
C, D	549	66	281	1612	75.99%	89.27%	B, F	463	152	126	1767	85.34%	78.61%
C, G	549	66	281	1612	75.99%	89.27%	C, D	549	66	281	1612	81.11%	66.14%
C, E	544	71	281	1612	75.56%	88.46%	C, G	549	66	281	1612	81.11%	66.14%
C, A	539	76	281	1612	75.12%	87.64%	C, E	544	71	281	1612	80.86%	65.94%
B, F	463	152	126	1767	76.91%	75.28%	C, A	539	76	281	1612	80.61%	65.73%
E, D	544	71	329	1564	73.12%	88.46%	E, D	544	71	329	1564	78.99%	62.31%
G, E	543	72	329	1564	73.03%	88.29%	G, E	543	72	329	1564	78.93%	62.27%
A, E	518	97	329	1564	70.86%	84.23%	A, E	518	97	329	1564	77.66%	61.16%
G, D	615	0	537	1356	69.61%	100.0%	A, D	554	61	420	1473	76.45%	56.88%
A, D	554	61	420	1473	69.73%	90.08%	A, G	552	63	420	1473	76.34%	56.79%
A, G	552	63	420	1473	69.57%	89.76%	G, D	615	0	537	1356	76.69%	53.39%
HTTP Response Splitting													
B, D	391	4	6	1401	98.74%	98.99%	B, D	391	4	6	1401	99.1%	98.49%
E, D	371	24	42	1365	91.83%	93.92%	B, E	315	80	6	1401	96.36%	98.13%
B, E	315	80	6	1401	87.99%	79.75%	B, C	266	129	6	1401	94.68%	97.79%
B, C	266	129	6	1401	79.76%	67.34%	B, A	253	142	6	1401	94.24%	97.68%
C, E	265	130	42	1365	75.5%	67.09%	B, F	253	142	6	1401	94.24%	97.68%
B, A	253	142	6	1401	77.37%	64.05%	B, G	253	142	6	1401	94.24%	97.68%
B, F	253	142	6	1401	77.37%	64.05%	E, D	371	24	42	1365	94.05%	89.83%
B, G	253	142	6	1401	77.37%	64.05%	C, E	265	130	42	1365	88.81%	86.32%
C, D	372	23	299	1108	69.79%	94.18%	A, E	171	224	42	1365	83.09%	80.28%
A, D	372	23	299	1108	69.79%	94.18%	F, E	171	224	42	1365	83.09%	80.28%
F, D	372	23	299	1108	69.79%	94.18%	G, E	171	224	42	1365	83.09%	80.28%
G, D	372	23	299	1108	69.79%	94.18%	C, D	372	23	299	1108	76.7%	55.44%
A, E	171	224	42	1365	56.25%	43.29%	A, D	372	23	299	1108	76.7%	55.44%
F, E	171	224	42	1365	56.25%	43.29%	F, D	372	23	299	1108	76.7%	55.44%
G, E	171	224	42	1365	56.25%	43.29%	G, D	372	23	299	1108	76.7%	55.44%
C, A	139	256	233	1174	36.25%	35.19%	C, A	139	256	233	1174	59.73%	37.37%
C, F	139	256	233	1174	36.25%	35.19%	C, F	139	256	233	1174	59.73%	37.37%
C, G	139	256	233	1174	36.25%	35.19%	C, G	139	256	233	1174	59.73%	37.37%
A, F	0	395	0	1407	0.0%	0.0%	A, F	0	395	0	1407	0.00%	0.00%
A, G	0	395	0	1407	0.0%	0.0%	A, G	0	395	0	1407	0.00%	0.00%
F, G	0	395	0	1407	0.0%	0.0%	F, G	0	395	0	1407	0.00%	0.00%
LDAP Injection													
A, E	293	0	8	457	98.65%	100.0%	G, D	292	1	7	458	98.72%	97.66%
F, E	293	0	8	457	98.65%	100.0%	F, G	292	1	7	458	98.72%	97.66%
E, D	293	0	8	457	98.65%	100.0%	C, G	292	1	7	458	98.72%	97.66%
G, D	292	1	7	458	98.65%	99.66%	B, G	291	2	7	458	98.61%	97.65%
F, G	292	1	7	458	98.65%	99.66%	A, G	291	2	7	458	98.61%	97.65%
C, G	292	1	7	458	98.65%	99.66%	G, E	288	5	7	458	98.27%	97.63%
B, D	292	1	13	452	97.66%	99.66%	A, E	293	0	8	457	98.67%	97.34%
B, A	292	1	13	452	97.66%	99.66%	F, E	293	0	8	457	98.67%	97.34%
B, F	292	1	13	452	97.66%	99.66%	E, D	293	0	8	457	98.67%	97.34%

B, G	291	2	7	458	98.48%	99.32%	C, E	293	0	8	457	98.67%	97.34%
A, G	291	2	7	458	98.48%	99.32%	B, D	292	1	13	452	97.76%	95.74%
G, E	288	5	7	458	97.96%	98.29%	B, A	292	1	13	452	97.76%	95.74%
C, E	292	1	80	385	87.82%	99.66%	B, F	292	1	13	452	97.76%	95.74%
B, C	292	1	80	385	87.82%	99.66%	B, C	292	1	13	452	97.76%	95.74%
C, A	292	1	80	385	87.82%	99.66%	B, E	226	67	8	457	91.9%	96.58%
C, F	292	1	80	385	87.82%	99.66%	C, A	292	1	80	385	89.12%	78.49%
C, D	292	1	80	385	87.82%	99.66%	C, F	292	1	80	385	89.12%	78.49%
B, E	225	68	13	452	84.75%	76.79%	C, D	292	1	80	385	89.12%	78.49%
A, D	293	0	292	173	66.74%	100.0%	A, D	292	1	256	209	76.4%	53.28%
A, F	292	1	279	186	67.59%	99.66%	A, F	292	1	279	186	75.3%	51.14%
F, D	292	1	279	186	67.59%	99.66%	F, D	292	1	279	186	75.3%	51.14%
OS Command Injection													
G, E	378	9	5	564	98.18%	97.67%	G, E	378	9	5	564	98.56%	98.69%
G, D	378	9	5	564	98.18%	97.67%	G, D	378	9	5	564	98.56%	98.69%
C, G	378	9	5	564	98.18%	97.67%	C, G	378	9	5	564	98.56%	98.69%
A, G	369	18	5	564	96.98%	95.35%	B, G	378	9	5	564	98.56%	98.69%
F, G	367	20	5	564	96.71%	94.83%	A, G	369	18	5	564	97.79%	98.66%
B, G	383	4	45	524	93.99%	98.97%	F, G	367	20	5	564	97.62%	98.66%
B, D	383	4	45	524	93.99%	98.97%	B, D	383	4	45	524	94.36%	89.49%
B, C	383	4	45	524	93.99%	98.97%	B, C	383	4	45	524	94.36%	89.49%
F, D	378	9	67	502	90.87%	97.67%	F, D	378	9	67	502	91.59%	84.94%
C, F	378	9	67	502	90.87%	97.67%	C, F	378	9	67	502	91.59%	84.94%
E, D	383	4	125	444	85.59%	98.97%	B, E	317	70	45	524	87.89%	87.57%
C, E	383	4	125	444	85.59%	98.97%	B, A	295	92	45	524	85.91%	86.76%
B, E	317	70	45	524	84.65%	81.91%	B, F	295	92	45	524	85.91%	86.76%
B, A	295	92	45	524	81.16%	76.23%	E, D	383	4	125	444	87.25%	75.39%
B, F	295	92	45	524	81.16%	76.23%	C, E	383	4	125	444	87.25%	75.39%
A, D	387	0	391	178	66.44%	100.0%	A, D	387	0	131	438	87.36%	74.71%
C, A	384	3	396	173	65.81%	99.22%	C, A	387	0	131	438	87.36%	74.71%
C, D	384	3	396	173	65.81%	99.22%	F, E	268	119	67	502	80.42%	80.0%
F, E	273	114	125	444	69.55%	70.54%	A, F	222	165	67	502	76.04%	76.82%
A, E	273	114	125	444	69.55%	70.54%	A, E	273	114	125	444	74.08%	68.59%
A, F	222	165	67	502	65.68%	57.36%	C, D	387	0	391	178	74.87%	49.74%
XPath Injection													
B, C	278	2	36	837	93.6%	99.29%	B, D	279	1	7	866	98.72%	97.55%
C, A	278	2	36	837	93.6%	99.29%	G, D	278	2	20	853	96.53%	93.29%
C, F	278	2	36	837	93.6%	99.29%	B, E	180	100	7	866	92.95%	96.26%
C, G	278	2	36	837	93.6%	99.29%	B, C	278	2	36	837	94.15%	88.54%
C, E	278	2	36	837	93.6%	99.29%	C, A	278	2	36	837	94.15%	88.54%
C, D	278	2	36	837	93.6%	99.29%	C, F	278	2	36	837	94.15%	88.54%
F, D	278	2	120	753	82.01%	99.29%	C, G	278	2	36	837	94.15%	88.54%
E, D	278	2	169	704	76.48%	99.29%	C, E	278	2	36	837	94.15%	88.54%
B, D	280	0	282	591	66.51%	100.0%	C, D	278	2	36	837	94.15%	88.54%
G, D	280	0	282	591	66.51%	100.0%	B, F	121	159	7	866	89.51%	94.53%
A, D	280	0	282	591	66.51%	100.0%	B, A	70	210	7	866	85.7%	90.91%
B, E	179	101	169	704	57.01%	63.93%	F, G	120	160	20	853	84.96%	85.71%
A, E	179	101	169	704	57.01%	63.93%	F, D	278	2	120	753	84.79%	69.85%
F, E	179	101	169	704	57.01%	63.93%	E, D	278	2	169	704	80.95%	62.19%
G, E	179	101	169	704	57.01%	63.93%	A, G	69	211	20	853	78.85%	77.53%
A, F	123	157	120	753	47.04%	43.93%	A, D	280	0	282	591	74.91%	49.82%
B, F	120	160	120	753	46.15%	42.86%	B, G	16	264	7	866	73.1%	69.57%
F, G	120	160	120	753	46.15%	42.86%	A, E	179	101	169	704	69.45%	51.44%
B, A	69	211	67	806	33.17%	24.64%	F, E	179	101	169	704	69.45%	51.44%
A, G	69	211	67	806	33.17%	24.64%	G, E	179	101	169	704	69.45%	51.44%
B, G	16	264	7	866	10.56%	5.71%	A, F	123	157	120	753	66.68%	50.62%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.7: Ranking of combinations of 2 SAST tools regarding their performance in category A3: Injection - Best and Minimum Effort Scenarios

Results obtained in A4: Insecure Design

A4: Insecure Design													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall

Method Tampering													
B, E	137	12	0	48	91.95%	100.0%	B, E	137	12	0	48	88.24%	91.95%
C, E	137	12	0	48	91.95%	100.0%	C, E	137	12	0	48	88.24%	91.95%
A, E	137	12	0	48	91.95%	100.0%	A, E	137	12	0	48	88.24%	91.95%
F, E	137	12	0	48	91.95%	100.0%	F, E	137	12	0	48	88.24%	91.95%
G, E	137	12	0	48	91.95%	100.0%	G, E	137	12	0	48	88.24%	91.95%
E, D	137	12	0	48	91.95%	100.0%	E, D	137	12	0	48	88.24%	91.95%
B, D	137	12	45	3	91.95%	75.27%	B, D	137	12	45	3	45.14%	91.95%
C, D	137	12	45	3	91.95%	75.27%	C, D	137	12	45	3	45.14%	91.95%
F, D	137	12	45	3	91.95%	75.27%	F, D	137	12	45	3	45.14%	91.95%
G, D	137	12	45	3	91.95%	75.27%	G, D	137	12	45	3	45.14%	91.95%
B, A	1	148	0	48	0.67%	100.0%	B, A	1	148	0	48	0.34%	0.67%
C, A	1	148	0	48	0.67%	100.0%	C, A	1	148	0	48	0.34%	0.67%
A, F	1	148	0	48	0.67%	100.0%	A, F	1	148	0	48	0.34%	0.67%
A, G	1	148	0	48	0.67%	100.0%	A, G	1	148	0	48	0.34%	0.67%
A, D	1	148	0	48	0.67%	100.0%	A, D	1	148	0	48	0.34%	0.67%
B, C	0	149	0	48	0.0%	0.00%	B, C	0	149	0	48	0.0%	0.0%
B, F	0	149	0	48	0.0%	0.00%	B, F	0	149	0	48	0.0%	0.0%
B, G	0	149	0	48	0.0%	0.00%	B, G	0	149	0	48	0.0%	0.0%
C, F	0	149	0	48	0.0%	0.00%	C, F	0	149	0	48	0.0%	0.0%
C, G	0	149	0	48	0.0%	0.00%	C, G	0	149	0	48	0.0%	0.0%
F, G	0	149	0	48	0.0%	0.00%	F, G	0	149	0	48	0.0%	0.0%
Improper Error Handling													
C, E	403	297	730	1902	57.57%	35.57%	C, E	403	297	730	1902	37.37%	57.57%
C, G	401	299	730	1902	57.29%	35.46%	C, G	401	299	730	1902	37.11%	57.29%
C, A	401	299	730	1902	57.29%	35.46%	C, A	401	299	730	1902	37.11%	57.29%
B, C	401	299	730	1902	57.29%	35.46%	B, C	401	299	730	1902	37.11%	57.29%
C, F	401	299	730	1902	57.29%	35.46%	C, F	401	299	730	1902	37.11%	57.29%
C, D	401	299	730	1902	57.29%	35.46%	C, D	401	299	730	1902	37.11%	57.29%
B, D	125	575	32	2600	17.86%	79.62%	B, D	125	575	32	2600	10.41%	17.86%
F, D	125	575	32	2600	17.86%	79.62%	F, D	125	575	32	2600	10.41%	17.86%
G, E	81	619	0	2632	11.57%	100.0%	G, E	81	619	0	2632	6.46%	11.57%
B, G	61	639	0	2632	8.71%	100.0%	B, G	61	639	0	2632	4.74%	8.71%
A, G	61	639	0	2632	8.71%	100.0%	A, G	61	639	0	2632	4.74%	8.71%
F, G	61	639	0	2632	8.71%	100.0%	F, G	61	639	0	2632	4.74%	8.71%
G, D	61	639	0	2632	8.71%	100.0%	G, D	61	639	0	2632	4.74%	8.71%
A, E	24	676	0	2632	3.43%	100.0%	A, E	21	679	18	2614	1.53%	3.0%
B, E	21	679	18	2614	3.0%	53.85%	B, E	21	679	18	2614	1.53%	3.0%
F, E	21	679	18	2614	3.0%	53.85%	F, E	21	679	18	2614	1.53%	3.0%
E, D	21	679	18	2614	3.0%	53.85%	E, D	21	679	18	2614	1.53%	3.0%
B, A	4	696	0	2632	0.57%	100.0%	B, A	4	696	0	2632	0.29%	0.57%
A, F	4	696	0	2632	0.57%	100.0%	A, F	4	696	0	2632	0.29%	0.57%
A, D	4	696	0	2632	0.57%	100.0%	A, D	4	696	0	2632	0.29%	0.57%
B, F	0	700	0	2632	0.0%	0.00%	B, F	0	700	0	2632	0.0%	0.0%
Trust Boundary Violation													
C, D	83	0	53	501	100.0%	61.03%	B, F	83	0	30	524	97.29%	100.0%
B, F	83	0	30	524	100.0%	73.45%	C, F	83	0	30	524	97.29%	100.0%
B, D	83	0	53	501	100.0%	61.03%	A, F	83	0	30	524	97.29%	100.0%
A, D	83	0	53	501	100.0%	61.03%	F, G	83	0	30	524	97.29%	100.0%
C, F	83	0	30	524	100.0%	73.45%	F, E	83	0	30	524	97.29%	100.0%
A, F	83	0	30	524	100.0%	73.45%	F, D	83	0	30	524	97.29%	100.0%
F, G	83	0	30	524	100.0%	73.45%	C, D	83	0	53	501	95.22%	100.0%
F, E	83	0	30	524	100.0%	73.45%	B, D	83	0	53	501	95.22%	100.0%
F, D	83	0	30	524	100.0%	73.45%	A, D	83	0	53	501	95.22%	100.0%
G, D	83	0	53	501	100.0%	61.03%	G, D	83	0	53	501	95.22%	100.0%
E, D	83	0	53	501	100.0%	61.03%	E, D	83	0	53	501	95.22%	100.0%
B, A	82	1	24	530	98.8%	77.36%	B, A	82	1	24	530	96.06%	98.8%
B, E	82	1	24	530	98.8%	77.36%	B, E	82	1	24	530	96.06%	98.8%
B, C	76	7	24	530	91.57%	76.0%	B, C	76	7	24	530	85.72%	91.57%
B, G	76	7	24	530	91.57%	76.0%	B, G	76	7	24	530	85.72%	91.57%
C, E	75	8	522	32	90.36%	12.56%	C, A	73	10	26	528	80.59%	87.95%
C, A	73	10	26	528	87.95%	73.74%	A, E	72	11	26	528	78.96%	86.75%
A, E	72	11	522	32	86.75%	12.12%	A, G	69	14	26	528	74.17%	83.13%
G, E	72	11	522	32	86.75%	12.12%	C, E	75	8	522	32	43.44%	90.36%
A, G	69	14	26	528	83.13%	72.63%	G, E	72	11	522	32	40.13%	86.75%
C, G	31	52	12	542	37.35%	72.09%	C, G	31	52	12	542	25.25%	37.35%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.8: Ranking of combinations of 2 SAST tools regarding their performance in category A4: Insecure Design - Business and Heightened Critical Scenarios

A4: Insecure Design													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Method Tampering													
B, E	137	12	0	48	95.8%	91.95%	B, E	137	12	0	48	90.0%	100.0%
C, E	137	12	0	48	95.8%	91.95%	C, E	137	12	0	48	90.0%	100.0%
A, E	137	12	0	48	95.8%	91.95%	A, E	137	12	0	48	90.0%	100.0%
F, E	137	12	0	48	95.8%	91.95%	F, E	137	12	0	48	90.0%	100.0%
G, E	137	12	0	48	95.8%	91.95%	G, E	137	12	0	48	90.0%	100.0%
E, D	137	12	0	48	95.8%	91.95%	E, D	137	12	0	48	90.0%	100.0%
B, D	137	12	45	3	82.78%	91.95%	B, A	1	148	0	48	62.24%	100.0%
C, D	137	12	45	3	82.78%	91.95%	C, A	1	148	0	48	62.24%	100.0%
F, D	137	12	45	3	82.78%	91.95%	A, F	1	148	0	48	62.24%	100.0%
G, D	137	12	45	3	82.78%	91.95%	A, G	1	148	0	48	62.24%	100.0%
B, A	1	148	0	48	1.33%	0.67%	A, D	1	148	0	48	62.24%	100.0%
C, A	1	148	0	48	1.33%	0.67%	B, D	137	12	45	3	47.64%	75.27%
A, F	1	148	0	48	1.33%	0.67%	C, D	137	12	45	3	47.64%	75.27%
A, G	1	148	0	48	1.33%	0.67%	F, D	137	12	45	3	47.64%	75.27%
A, D	1	148	0	48	1.33%	0.67%	G, D	137	12	45	3	47.64%	75.27%
B, C	0	149	0	48	0.0%	0.0%	B, C	0	149	0	48	0.00%	0.00%
B, F	0	149	0	48	0.0%	0.0%	B, F	0	149	0	48	0.00%	0.00%
B, G	0	149	0	48	0.0%	0.0%	B, G	0	149	0	48	0.00%	0.00%
C, F	0	149	0	48	0.0%	0.0%	C, F	0	149	0	48	0.00%	0.00%
C, G	0	149	0	48	0.0%	0.0%	C, G	0	149	0	48	0.00%	0.00%
F, G	0	149	0	48	0.0%	0.0%	F, G	0	149	0	48	0.00%	0.00%
Improper Error Handling													
C, E	403	297	730	1902	43.97%	57.57%	C, G	112	588	0	2632	90.87%	100.0%
C, G	401	299	730	1902	43.8%	57.29%	G, E	81	619	0	2632	90.48%	100.0%
C, A	401	299	730	1902	43.8%	57.29%	B, G	61	639	0	2632	90.23%	100.0%
B, C	401	299	730	1902	43.8%	57.29%	A, G	61	639	0	2632	90.23%	100.0%
C, F	401	299	730	1902	43.8%	57.29%	F, G	61	639	0	2632	90.23%	100.0%
C, D	401	299	730	1902	43.8%	57.29%	G, D	61	639	0	2632	90.23%	100.0%
B, D	125	575	32	2600	29.17%	17.86%	C, A	55	645	0	2632	90.16%	100.0%
F, D	125	575	32	2600	29.17%	17.86%	A, E	24	676	0	2632	89.78%	100.0%
G, E	81	619	0	2632	20.74%	11.57%	B, A	4	696	0	2632	89.54%	100.0%
B, G	61	639	0	2632	16.03%	8.71%	A, F	4	696	0	2632	89.54%	100.0%
A, G	61	639	0	2632	16.03%	8.71%	A, D	4	696	0	2632	89.54%	100.0%
F, G	61	639	0	2632	16.03%	8.71%	B, D	125	575	32	2600	80.75%	79.62%
G, D	61	639	0	2632	16.03%	8.71%	F, D	125	575	32	2600	80.75%	79.62%
A, E	21	679	18	2614	5.68%	3.0%	C, E	54	646	18	2614	77.59%	75.0%
B, E	21	679	18	2614	5.68%	3.0%	B, E	21	679	18	2614	66.61%	53.85%
F, E	21	679	18	2614	5.68%	3.0%	F, E	21	679	18	2614	66.61%	53.85%
E, D	21	679	18	2614	5.68%	3.0%	E, D	21	679	18	2614	66.61%	53.85%
B, A	4	696	0	2632	1.14%	0.57%	B, C	401	299	730	1902	60.94%	35.46%
A, F	4	696	0	2632	1.14%	0.57%	C, F	401	299	730	1902	60.94%	35.46%
A, D	4	696	0	2632	1.14%	0.57%	C, D	401	299	730	1902	60.94%	35.46%
B, F	0	700	0	2632	0.0%	0.0%	B, F	0	700	0	2632	0.00%	0.00%
Trust Boundary Violation													
B, A	82	1	24	530	86.77%	98.8%	C, D	83	0	12	542	93.68%	87.37%
B, E	82	1	24	530	86.77%	98.8%	C, E	75	8	12	542	92.38%	86.21%
C, E	75	8	12	542	88.24%	90.36%	B, F	83	0	24	530	88.79%	77.57%
B, F	83	0	30	524	84.69%	100.0%	B, D	83	0	24	530	88.79%	77.57%
C, F	83	0	30	524	84.69%	100.0%	B, A	82	1	24	530	88.59%	77.36%
A, F	83	0	30	524	84.69%	100.0%	B, E	82	1	24	530	88.59%	77.36%
F, G	83	0	30	524	84.69%	100.0%	A, D	83	0	26	528	88.07%	76.15%
F, E	83	0	30	524	84.69%	100.0%	B, C	76	7	24	530	87.35%	76.0%
F, D	83	0	30	524	84.69%	100.0%	B, G	76	7	24	530	87.35%	76.0%
B, C	76	7	24	530	83.06%	91.57%	C, A	73	10	26	528	85.94%	73.74%
B, G	76	7	24	530	83.06%	91.57%	A, E	72	11	26	528	85.71%	73.47%
C, A	73	10	26	528	80.22%	87.95%	C, F	83	0	30	524	86.73%	73.45%
C, D	83	0	53	501	75.8%	100.0%	A, F	83	0	30	524	86.73%	73.45%
B, D	83	0	53	501	75.8%	100.0%	F, G	83	0	30	524	86.73%	73.45%
A, D	83	0	53	501	75.8%	100.0%	F, E	83	0	30	524	86.73%	73.45%

G, D	83	0	53	501	75.8%	100.0%	F, D	83	0	30	524	86.73%	73.45%
E, D	83	0	53	501	75.8%	100.0%	A, G	69	14	26	528	85.02%	72.63%
A, E	72	11	26	528	79.56%	86.75%	C, G	31	52	12	542	81.67%	72.09%
A, G	69	14	26	528	77.53%	83.13%	G, D	83	0	53	501	80.51%	61.03%
C, G	31	52	12	542	49.21%	37.35%	E, D	83	0	53	501	80.51%	61.03%
G, E	72	11	522	32	21.27%	86.75%	G, E	72	11	522	32	43.27%	12.12%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.9: Ranking of combinations of 2 SAST tools regarding their performance in category A4: Insecure Design - Best and Minimum Effort Scenarios

Results obtained in A5: Security Misconfiguration

A5: Security Misconfiguration													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Insecure Use of Hard Coded Constants													
B, F	59	3	0	57	95.16%	100.0%	B, F	59	3	0	57	92.86%	95.16%
B, E	50	12	0	57	80.65%	100.0%	B, E	50	12	0	57	72.84%	80.65%
B, C	45	17	0	57	72.58%	100.0%	B, C	45	17	0	57	62.63%	72.58%
B, A	45	17	0	57	72.58%	100.0%	B, A	45	17	0	57	62.63%	72.58%
B, G	45	17	0	57	72.58%	100.0%	B, G	45	17	0	57	62.63%	72.58%
B, D	45	17	0	57	72.58%	100.0%	B, D	45	17	0	57	62.63%	72.58%
F, E	41	21	0	57	66.13%	100.0%	F, E	41	21	0	57	54.93%	66.13%
F, D	41	21	0	57	66.13%	100.0%	F, D	41	21	0	57	54.93%	66.13%
A, F	40	22	0	57	64.52%	100.0%	A, F	40	22	0	57	53.07%	64.52%
F, G	40	22	0	57	64.52%	100.0%	F, G	40	22	0	57	53.07%	64.52%
C, F	40	22	0	57	64.52%	100.0%	C, F	40	22	0	57	53.07%	64.52%
C, E	31	31	0	57	50.0%	100.0%	C, E	31	31	0	57	37.5%	50.0%
A, E	31	31	0	57	50.0%	100.0%	A, E	31	31	0	57	37.5%	50.0%
G, E	31	31	0	57	50.0%	100.0%	G, E	31	31	0	57	37.5%	50.0%
E, D	31	31	0	57	50.0%	100.0%	E, D	31	31	0	57	37.5%	50.0%
C, D	26	36	3	54	41.94%	89.66%	C, D	26	36	3	54	28.66%	41.94%
A, D	26	36	3	54	41.94%	89.66%	A, D	26	36	3	54	28.66%	41.94%
G, D	26	36	3	54	41.94%	89.66%	G, D	26	36	3	54	28.66%	41.94%
A, G	7	55	0	57	11.29%	100.0%	A, G	7	55	0	57	6.28%	11.29%
C, A	6	56	0	57	9.68%	100.0%	C, A	6	56	0	57	5.31%	9.68%
C, G	4	58	0	57	6.45%	100.0%	C, G	5	57	0	57	4.36%	8.06%
XML External Entities													
B, C	5	5	3	22	50.0%	62.5%	B, C	5	5	3	22	34.5%	50.0%
B, A	5	5	3	22	50.0%	62.5%	B, A	5	5	3	22	34.5%	50.0%
B, F	5	5	3	22	50.0%	62.5%	B, F	5	5	3	22	34.5%	50.0%
B, G	5	5	3	22	50.0%	62.5%	B, G	5	5	3	22	34.5%	50.0%
B, E	5	5	3	22	50.0%	62.5%	B, E	5	5	3	22	34.5%	50.0%
B, D	5	5	3	22	50.0%	62.5%	B, D	5	5	3	22	34.5%	50.0%
C, D	5	5	3	22	50.0%	62.5%	C, D	5	5	3	22	34.5%	50.0%
F, D	5	5	3	22	50.0%	62.5%	F, D	5	5	3	22	34.5%	50.0%
G, D	5	5	3	22	50.0%	62.5%	G, D	5	5	3	22	34.5%	50.0%
E, D	5	5	3	22	50.0%	62.5%	E, D	5	5	3	22	34.5%	50.0%
C, F	1	9	1	24	10.0%	50.0%	A, D	2	8	12	13	7.2%	20.0%
F, G	1	9	1	24	10.0%	50.0%	A, F	2	8	12	13	7.2%	20.0%
F, E	1	9	1	24	10.0%	50.0%	C, A	2	8	12	13	7.2%	20.0%
A, D	2	8	12	13	20.0%	14.29%	A, G	2	8	12	13	7.2%	20.0%
A, F	2	8	12	13	20.0%	14.29%	A, E	2	8	12	13	7.2%	20.0%
C, A	2	8	12	13	20.0%	14.29%	C, F	1	9	1	24	5.3%	10.0%
A, G	2	8	12	13	20.0%	14.29%	F, G	1	9	1	24	5.3%	10.0%
A, E	2	8	12	13	20.0%	14.29%	F, E	1	9	1	24	5.3%	10.0%
C, E	1	9	9	16	10.0%	10.0%	C, E	1	9	9	16	3.7%	10.0%
G, E	1	9	9	16	10.0%	10.0%	G, E	1	9	9	16	3.7%	10.0%
C, G	0	10	17	8	0.0%	0.0%	C, G	0	10	17	8	0.0%	0.0%
Bad Programming of Cookies													
B, A	1044	621	160	2059	62.7%	86.71%	B, A	1044	621	160	2059	48.75%	62.7%
A, D	1044	621	160	2059	62.7%	86.71%	A, D	1044	621	160	2059	48.75%	62.7%
A, G	894	771	160	2059	53.69%	84.82%	A, G	894	771	160	2059	39.33%	53.69%
A, E	894	771	160	2059	53.69%	84.82%	A, E	894	771	160	2059	39.33%	53.69%

C, A	832	833	160	2059	49.97%	83.87%	C, A	832	833	160	2059	35.67%	49.97%
F, G	716	949	82	2137	43.0%	89.72%	F, G	716	949	82	2137	29.95%	43.0%
F, E	716	949	82	2137	43.0%	89.72%	F, E	716	949	82	2137	29.95%	43.0%
C, F	671	994	82	2137	40.3%	89.11%	C, F	671	994	82	2137	27.53%	40.3%
B, F	563	1102	82	2137	33.81%	87.29%	B, F	563	1102	82	2137	22.0%	33.81%
F, D	562	1103	82	2137	33.75%	87.27%	F, D	562	1103	82	2137	21.95%	33.75%
A, F	537	1128	160	2059	32.25%	77.04%	A, F	537	1128	160	2059	20.16%	32.25%
G, D	273	1392	111	2108	16.4%	71.09%	G, D	273	1392	111	2108	9.13%	16.4%
E, D	273	1392	111	2108	16.4%	71.09%	E, D	273	1392	111	2108	9.13%	16.4%
B, G	230	1435	84	2135	13.81%	73.25%	B, G	230	1435	84	2135	7.6%	13.81%
B, E	230	1435	84	2135	13.81%	73.25%	B, E	230	1435	84	2135	7.6%	13.81%
B, C	168	1497	84	2135	10.09%	66.67%	C, D	212	1453	111	2108	6.86%	12.73%
C, D	212	1453	111	2108	12.73%	65.63%	B, C	168	1497	84	2135	5.36%	10.09%
C, G	125	1540	202	2017	7.51%	38.23%	C, G	125	1540	202	2017	3.69%	7.51%
C, E	125	1540	202	2017	7.51%	38.23%	C, E	125	1540	202	2017	3.69%	7.51%
B, D	60	1605	84	2135	3.6%	41.67%	B, D	60	1605	84	2135	1.8%	3.6%
G, E	1	1664	36	2183	0.06%	2.7%	G, E	1	1664	36	2183	0.03%	0.06%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.10: Ranking of combinations of 2 SAST tools regarding their performance in category A5: Security Misconfiguration - Business and Heightened Critical Scenarios

A5: Security Misconfiguration													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Insecure Use of Hard Coded Constants													
B, F	59	3	0	57	97.52%	95.16%	B, F	59	3	0	57	97.5%	100.0%
B, E	50	12	0	57	89.29%	80.65%	B, E	50	12	0	57	91.3%	100.0%
B, C	45	17	0	57	84.11%	72.58%	B, C	45	17	0	57	88.51%	100.0%
B, A	45	17	0	57	84.11%	72.58%	B, A	45	17	0	57	88.51%	100.0%
B, G	45	17	0	57	84.11%	72.58%	B, G	45	17	0	57	88.51%	100.0%
B, D	45	17	0	57	84.11%	72.58%	B, D	45	17	0	57	88.51%	100.0%
F, E	41	21	0	57	79.61%	66.13%	F, E	41	21	0	57	86.54%	100.0%
F, D	41	21	0	57	79.61%	66.13%	A, F	40	22	0	57	86.08%	100.0%
A, F	40	22	0	57	78.43%	64.52%	F, G	40	22	0	57	86.08%	100.0%
F, G	40	22	0	57	78.43%	64.52%	C, F	39	23	0	57	85.62%	100.0%
C, F	40	22	0	57	78.43%	64.52%	C, E	31	31	0	57	82.39%	100.0%
C, E	31	31	0	57	66.67%	50.0%	A, E	31	31	0	57	82.39%	100.0%
A, E	31	31	0	57	66.67%	50.0%	G, E	31	31	0	57	82.39%	100.0%
G, E	31	31	0	57	66.67%	50.0%	E, D	31	31	0	57	82.39%	100.0%
E, D	31	31	0	57	66.67%	50.0%	F, D	45	17	3	54	84.9%	93.75%
C, D	26	36	3	54	57.14%	41.94%	A, G	7	55	0	57	75.45%	100.0%
A, D	26	36	3	54	57.14%	41.94%	C, A	6	56	0	57	75.22%	100.0%
G, D	26	36	3	54	57.14%	41.94%	C, G	4	58	0	57	74.78%	100.0%
A, G	7	55	0	57	20.29%	11.29%	C, D	26	36	3	54	74.83%	89.66%
C, A	6	56	0	57	17.65%	9.68%	A, D	26	36	3	54	74.83%	89.66%
C, G	5	57	0	57	14.93%	8.06%	G, D	26	36	3	54	74.83%	89.66%
XML External Entities													
B, C	5	5	3	22	55.56%	50.0%	B, C	5	5	3	22	71.99%	62.5%
B, A	5	5	3	22	55.56%	50.0%	B, A	5	5	3	22	71.99%	62.5%
B, F	5	5	3	22	55.56%	50.0%	B, F	5	5	3	22	71.99%	62.5%
B, G	5	5	3	22	55.56%	50.0%	B, G	5	5	3	22	71.99%	62.5%
B, E	5	5	3	22	55.56%	50.0%	B, E	5	5	3	22	71.99%	62.5%
B, D	5	5	3	22	55.56%	50.0%	B, D	5	5	3	22	71.99%	62.5%
C, D	5	5	3	22	55.56%	50.0%	C, D	5	5	3	22	71.99%	62.5%
F, D	5	5	3	22	55.56%	50.0%	F, D	5	5	3	22	71.99%	62.5%
G, D	5	5	3	22	55.56%	50.0%	G, D	5	5	3	22	71.99%	62.5%
E, D	5	5	3	22	55.56%	50.0%	E, D	5	5	3	22	71.99%	62.5%
A, D	2	8	12	13	16.67%	20.0%	A, D	5	5	3	22	71.99%	62.5%
A, F	2	8	12	13	16.67%	20.0%	A, F	1	9	1	24	61.36%	50.0%
C, A	2	8	12	13	16.67%	20.0%	C, F	1	9	1	24	61.36%	50.0%
A, G	2	8	12	13	16.67%	20.0%	F, G	1	9	1	24	61.36%	50.0%
A, E	2	8	12	13	16.67%	20.0%	F, E	1	9	1	24	61.36%	50.0%
C, F	1	9	1	24	16.67%	10.0%	C, A	2	8	12	13	38.1%	14.29%
F, G	1	9	1	24	16.67%	10.0%	A, G	2	8	12	13	38.1%	14.29%
F, E	1	9	1	24	16.67%	10.0%	A, E	2	8	12	13	38.1%	14.29%
C, E	1	9	9	16	10.0%	10.0%	C, E	1	9	9	16	37.0%	10.0%

G, E	1	9	9	16	10.0%	10.0%	G, E	1	9	9	16	37.0%	10.0%
C, G	0	10	17	8	0.0%	0.0%	C, G	0	10	5	20	33.33%	0.0%
Bad Programming of Cookies													
B, A	1044	621	160	2059	72.78%	62.7%	B, A	1044	621	160	2059	81.77%	86.71%
A, D	1044	621	160	2059	72.78%	62.7%	A, D	1044	621	160	2059	81.77%	86.71%
A, G	894	771	160	2059	65.76%	53.69%	F, G	716	949	82	2137	79.49%	89.72%
A, E	894	771	160	2059	65.76%	53.69%	F, E	716	949	82	2137	79.49%	89.72%
C, A	832	833	160	2059	62.63%	49.97%	C, F	671	994	82	2137	78.68%	89.11%
F, G	716	949	82	2137	58.14%	43.0%	B, F	563	1102	82	2137	76.63%	87.29%
F, E	716	949	82	2137	58.14%	43.0%	F, D	562	1103	82	2137	76.61%	87.27%
C, F	671	994	82	2137	55.5%	40.3%	A, F	546	1119	82	2137	76.29%	86.94%
B, F	563	1102	82	2137	48.74%	33.81%	A, G	894	771	160	2059	78.79%	84.82%
F, D	562	1103	82	2137	48.68%	33.75%	A, E	894	771	160	2059	78.79%	84.82%
A, F	537	1128	160	2059	45.47%	32.25%	C, A	832	833	160	2059	77.53%	83.87%
G, D	273	1392	111	2108	26.65%	16.4%	B, G	230	1435	84	2135	66.53%	73.25%
E, D	273	1392	111	2108	26.65%	16.4%	B, E	230	1435	84	2135	66.53%	73.25%
B, G	230	1435	84	2135	23.24%	13.81%	G, D	273	1392	111	2108	65.66%	71.09%
B, E	230	1435	84	2135	23.24%	13.81%	E, D	273	1392	111	2108	65.66%	71.09%
C, D	212	1453	111	2108	21.33%	12.73%	B, C	168	1497	84	2135	62.72%	66.67%
B, C	168	1497	84	2135	17.53%	10.09%	C, D	212	1453	111	2108	62.42%	65.63%
C, G	125	1540	202	2017	12.55%	7.51%	B, D	60	1605	84	2135	49.38%	41.67%
C, E	125	1540	202	2017	12.55%	7.51%	C, G	125	1540	202	2017	47.47%	38.23%
B, D	60	1605	84	2135	6.63%	3.6%	C, E	125	1540	202	2017	47.47%	38.23%
G, E	1	1664	36	2183	0.12%	0.06%	G, E	1	1664	36	2183	29.72%	2.7%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.11: Ranking of combinations of 2 SAST tools regarding their performance in category A5: Security Misconfiguration - Best and Minimum Effort Scenarios

Results obtained in A6: Vulnerable and Outdated Components

A6: Vulnerable and Outdated Components													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Vulnerable Third-Party Components													
C, E	229	59	0	491	79.51%	100.0%	C, E	229	59	0	491	71.37%	79.51%
B, E	195	93	0	491	67.71%	100.0%	B, E	195	93	0	491	56.78%	67.71%
A, E	195	93	0	491	67.71%	100.0%	A, E	195	93	0	491	56.78%	67.71%
F, E	195	93	0	491	67.71%	100.0%	F, E	195	93	0	491	56.78%	67.71%
G, E	195	93	0	491	67.71%	100.0%	G, E	195	93	0	491	56.78%	67.71%
E, D	195	93	0	491	67.71%	100.0%	E, D	195	93	0	491	56.78%	67.71%
C, D	37	251	176	315	12.85%	17.37%	C, D	37	251	176	315	4.95%	12.85%
C, A	37	251	176	315	12.85%	17.37%	C, A	37	251	176	315	4.95%	12.85%
B, C	37	251	176	315	12.85%	17.37%	B, C	37	251	176	315	4.95%	12.85%
C, F	37	251	176	315	12.85%	17.37%	C, F	37	251	176	315	4.95%	12.85%
C, G	37	251	176	315	12.85%	17.37%	C, G	37	251	176	315	4.95%	12.85%
A, G	5	283	0	491	1.74%	100.0%	A, G	10	278	2	489	1.79%	3.47%
B, A	5	283	0	491	1.74%	100.0%	B, G	10	278	2	489	1.79%	3.47%
A, F	5	283	0	491	1.74%	100.0%	F, G	10	278	2	489	1.79%	3.47%
A, D	5	283	0	491	1.74%	100.0%	G, D	10	278	2	489	1.79%	3.47%
B, F	2	286	0	491	0.69%	100.0%	B, A	5	283	0	491	0.88%	1.74%
B, G	1	287	0	491	0.35%	100.0%	A, F	5	283	0	491	0.88%	1.74%
F, G	1	287	0	491	0.35%	100.0%	A, D	5	283	0	491	0.88%	1.74%
B, D	1	287	0	491	0.35%	100.0%	B, F	2	286	0	491	0.35%	0.69%
F, D	1	287	0	491	0.35%	100.0%	B, D	1	287	0	491	0.17%	0.35%
G, D	10	278	2	489	3.47%	83.33%	F, D	1	287	0	491	0.17%	0.35%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.12: Ranking of combinations of 2 SAST tools regarding their performance in category A6: Vulnerable and Outdated Components - Business and Heightened Critical Scenarios

A6: Vulnerable and Outdated Components													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Vulnerable Third-Party Components													
C, E	229	59	0	491	88.59%	79.51%	C, D	247	41	2	489	95.73%	99.2%
B, E	195	93	0	491	80.75%	67.71%	C, E	229	59	0	491	94.64%	100.0%
A, E	195	93	0	491	80.75%	67.71%	B, E	195	93	0	491	92.04%	100.0%
F, E	195	93	0	491	80.75%	67.71%	A, E	195	93	0	491	92.04%	100.0%
G, E	195	93	0	491	80.75%	67.71%	F, E	195	93	0	491	92.04%	100.0%
E, D	195	93	0	491	80.75%	67.71%	G, E	195	93	0	491	92.04%	100.0%
C, D	37	251	176	315	14.77%	12.85%	E, D	195	93	0	491	92.04%	100.0%
C, A	37	251	176	315	14.77%	12.85%	C, A	39	249	0	491	83.18%	100.0%
B, C	37	251	176	315	14.77%	12.85%	B, C	35	253	0	491	83.0%	100.0%
C, F	37	251	176	315	14.77%	12.85%	C, F	35	253	0	491	83.0%	100.0%
C, G	37	251	176	315	14.77%	12.85%	A, G	5	283	0	491	81.72%	100.0%
A, G	10	278	2	489	6.67%	3.47%	B, A	5	283	0	491	81.72%	100.0%
B, G	10	278	2	489	6.67%	3.47%	A, F	5	283	0	491	81.72%	100.0%
F, G	10	278	2	489	6.67%	3.47%	A, D	5	283	0	491	81.72%	100.0%
G, D	10	278	2	489	6.67%	3.47%	B, F	2	286	0	491	81.6%	100.0%
B, A	5	283	0	491	3.41%	1.74%	B, G	1	287	0	491	81.56%	100.0%
A, F	5	283	0	491	3.41%	1.74%	F, G	1	287	0	491	81.56%	100.0%
A, D	5	283	0	491	3.41%	1.74%	B, D	1	287	0	491	81.56%	100.0%
B, F	2	286	0	491	1.38%	0.69%	F, D	1	287	0	491	81.56%	100.0%
B, D	1	287	0	491	0.69%	0.35%	C, G	44	244	2	489	81.18%	95.65%
F, D	1	287	0	491	0.69%	0.35%	G, D	10	278	2	489	73.54%	83.33%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.13: Ranking of combinations of 2 SAST tools regarding their performance in category A6: Vulnerable and Outdated Components - Best and Minimum Effort Scenarios

Results obtained in A7: Identification and Authentication Failures

A7: Identification and Authentication Failures													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Bypassing Authentication													
B, D	2	1	0	0	66.67%	100.0%	B, D	2	1	0	0	0.00%	66.67%
C, D	2	1	0	0	66.67%	100.0%	C, D	2	1	0	0	0.00%	66.67%
A, D	2	1	0	0	66.67%	100.0%	A, D	2	1	0	0	0.00%	66.67%
F, D	2	1	0	0	66.67%	100.0%	F, D	2	1	0	0	0.00%	66.67%
G, D	2	1	0	0	66.67%	100.0%	G, D	2	1	0	0	0.00%	66.67%
E, D	2	1	0	0	66.67%	100.0%	E, D	2	1	0	0	0.00%	66.67%
B, C	0	3	0	0	0.0%	0.00%	B, C	0	3	0	0	0.00%	0.0%
B, A	0	3	0	0	0.0%	0.00%	B, A	0	3	0	0	0.00%	0.0%
B, F	0	3	0	0	0.0%	0.00%	B, F	0	3	0	0	0.00%	0.0%
B, G	0	3	0	0	0.0%	0.00%	B, G	0	3	0	0	0.00%	0.0%
B, E	0	3	0	0	0.0%	0.00%	B, E	0	3	0	0	0.00%	0.0%
C, A	0	3	0	0	0.0%	0.00%	C, A	0	3	0	0	0.00%	0.0%
C, F	0	3	0	0	0.0%	0.00%	C, F	0	3	0	0	0.00%	0.0%
C, G	0	3	0	0	0.0%	0.00%	C, G	0	3	0	0	0.00%	0.0%
C, E	0	3	0	0	0.0%	0.00%	C, E	0	3	0	0	0.00%	0.0%
A, F	0	3	0	0	0.0%	0.00%	A, F	0	3	0	0	0.00%	0.0%
A, G	0	3	0	0	0.0%	0.00%	A, G	0	3	0	0	0.00%	0.0%
A, E	0	3	0	0	0.0%	0.00%	A, E	0	3	0	0	0.00%	0.0%
F, G	0	3	0	0	0.0%	0.00%	F, G	0	3	0	0	0.00%	0.0%
F, E	0	3	0	0	0.0%	0.00%	F, E	0	3	0	0	0.00%	0.0%
G, E	0	3	0	0	0.0%	0.00%	G, E	0	3	0	0	0.00%	0.0%
Hard Coded Passwords													
B, A	116	28	37	201	80.56%	75.82%	B, A	116	28	37	201	66.46%	80.56%
B, E	116	28	37	201	80.56%	75.82%	B, E	116	28	37	201	66.46%	80.56%
B, F	106	38	3	235	73.61%	97.25%	B, F	106	38	3	235	63.43%	73.61%
F, E	106	38	3	235	73.61%	97.25%	F, E	106	38	3	235	63.43%	73.61%
F, D	105	39	3	235	72.92%	97.22%	F, D	105	39	3	235	62.58%	72.92%

A, F	104	40	3	235	72.22%	97.2%	A, F	104	40	3	235	61.74%	72.22%
C, F	103	41	3	235	71.53%	97.17%	C, F	103	41	3	235	60.89%	71.53%
F, G	102	42	3	235	70.83%	97.14%	F, G	102	42	3	235	60.06%	70.83%
B, C	103	41	37	201	71.53%	73.57%	B, C	103	41	37	201	55.79%	71.53%
B, D	102	42	37	201	70.83%	73.38%	B, D	102	42	37	201	55.0%	70.83%
B, G	102	42	37	201	70.83%	73.38%	B, G	102	42	37	201	55.0%	70.83%
E, D	97	47	73	165	67.36%	57.06%	E, D	97	47	73	165	46.04%	67.36%
A, D	80	64	2	236	55.56%	97.56%	A, D	80	64	2	236	42.98%	55.56%
C, E	81	63	73	165	56.25%	52.6%	C, E	81	63	73	165	35.32%	56.25%
A, E	80	64	73	165	55.56%	52.29%	C, D	66	78	2	236	33.23%	45.83%
G, E	80	64	73	165	55.56%	52.29%	A, E	80	64	73	165	34.69%	55.56%
C, D	66	78	2	236	45.83%	97.06%	G, E	80	64	73	165	34.69%	55.56%
G, D	61	83	2	236	42.36%	96.83%	G, D	61	83	2	236	29.97%	42.36%
C, A	57	87	36	202	39.58%	61.29%	C, A	57	87	36	202	24.63%	39.58%
A, G	36	108	36	202	25.0%	50.0%	A, G	36	108	36	202	13.73%	25.0%
C, G	28	116	34	204	19.44%	45.16%	C, G	28	116	34	204	10.22%	19.44%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.14: Ranking of combinations of 2 SAST tools regarding their performance in category A7: Identification and Authentication Failures - Business and Heightened Critical Scenarios

A7: Identification and Authentication Failures													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Bypassing Authentication													
B, D	2	1	0	0	80.0%	66.67%	B, D	2	1	0	0	50.0%	100.0%
C, D	2	1	0	0	80.0%	66.67%	C, D	2	1	0	0	50.0%	100.0%
A, D	2	1	0	0	80.0%	66.67%	A, D	2	1	0	0	50.0%	100.0%
F, D	2	1	0	0	80.0%	66.67%	F, D	2	1	0	0	50.0%	100.0%
G, D	2	1	0	0	80.0%	66.67%	G, D	2	1	0	0	50.0%	100.0%
E, D	2	1	0	0	80.0%	66.67%	E, D	2	1	0	0	50.0%	100.0%
B, C	0	3	0	0	0.0%	0.0%	B, C	0	3	0	0	0.00%	0.00%
B, A	0	3	0	0	0.0%	0.0%	B, A	0	3	0	0	0.00%	0.00%
B, F	0	3	0	0	0.0%	0.0%	B, F	0	3	0	0	0.00%	0.00%
B, G	0	3	0	0	0.0%	0.0%	B, G	0	3	0	0	0.00%	0.00%
B, E	0	3	0	0	0.0%	0.0%	B, E	0	3	0	0	0.00%	0.00%
C, A	0	3	0	0	0.0%	0.0%	C, A	0	3	0	0	0.00%	0.00%
C, F	0	3	0	0	0.0%	0.0%	C, F	0	3	0	0	0.00%	0.00%
C, G	0	3	0	0	0.0%	0.0%	C, G	0	3	0	0	0.00%	0.00%
C, E	0	3	0	0	0.0%	0.0%	C, E	0	3	0	0	0.00%	0.00%
A, F	0	3	0	0	0.0%	0.0%	A, F	0	3	0	0	0.00%	0.00%
A, G	0	3	0	0	0.0%	0.0%	A, G	0	3	0	0	0.00%	0.00%
A, E	0	3	0	0	0.0%	0.0%	A, E	0	3	0	0	0.00%	0.00%
F, G	0	3	0	0	0.0%	0.0%	F, G	0	3	0	0	0.00%	0.00%
F, E	0	3	0	0	0.0%	0.0%	F, E	0	3	0	0	0.00%	0.00%
G, E	0	3	0	0	0.0%	0.0%	G, E	0	3	0	0	0.00%	0.00%
Hard Coded Passwords													
B, F	106	38	3	235	83.79%	73.61%	F, D	110	34	2	236	92.81%	98.21%
F, E	106	38	3	235	83.79%	73.61%	B, F	106	38	3	235	91.66%	97.25%
F, D	105	39	3	235	83.33%	72.92%	F, E	106	38	3	235	91.66%	97.25%
A, F	104	40	3	235	82.87%	72.22%	A, F	104	40	3	235	91.33%	97.2%
C, F	103	41	3	235	82.4%	71.53%	C, F	103	41	3	235	91.16%	97.17%
F, G	102	42	3	235	81.93%	70.83%	F, G	102	42	3	235	90.99%	97.14%
B, A	116	28	37	201	78.11%	80.56%	E, D	92	52	2	236	89.91%	97.87%
B, E	116	28	37	201	78.11%	80.56%	B, D	83	61	2	236	88.55%	97.65%
B, C	103	41	37	201	72.54%	71.53%	A, D	80	64	2	236	88.11%	97.56%
E, D	92	52	2	236	77.31%	63.89%	C, D	66	78	2	236	86.11%	97.06%
B, D	102	42	37	201	72.08%	70.83%	G, D	61	83	2	236	85.4%	96.83%
B, G	102	42	37	201	72.08%	70.83%	B, A	116	28	37	201	81.79%	75.82%
A, D	80	64	2	236	70.8%	55.56%	B, E	116	28	37	201	81.79%	75.82%
C, D	66	78	2	236	62.26%	45.83%	B, C	103	41	37	201	78.31%	73.57%
G, D	61	83	2	236	58.94%	42.36%	B, G	102	42	37	201	78.05%	73.38%
C, E	81	63	73	165	54.36%	56.25%	A, E	70	74	36	202	69.61%	66.04%
A, E	80	64	73	165	53.87%	55.56%	C, A	57	87	36	202	65.59%	61.29%
G, E	80	64	73	165	53.87%	55.56%	C, E	81	63	73	165	62.48%	52.6%
C, A	57	87	36	202	48.1%	39.58%	G, E	80	64	73	165	62.17%	52.29%

A, G	36	108	36	202	33.33%	25.0%	A, G	36	108	36	202	57.58%	50.0%
C, G	28	116	34	204	27.18%	19.44%	C, G	28	116	34	204	54.46%	45.16%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.15: Ranking of combinations of 2 SAST tools regarding their performance in category A7: Identification and Authentication Failures - Best and Minimum Effort Scenarios

Results obtained in A8: Software and Data Integrity Failures

A8: Software and Data Integrity Failures													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Insecure Deserialization													
B, D	6	1	26	5	85.71%	18.75%	B, D	6	1	26	5	43.65%	85.71%
C, D	5	2	26	5	71.43%	16.13%	C, D	5	2	26	5	31.27%	71.43%
G, D	5	2	26	5	71.43%	16.13%	G, D	5	2	26	5	31.27%	71.43%
E, D	5	2	26	5	71.43%	16.13%	E, D	5	2	26	5	31.27%	71.43%
B, F	3	4	3	28	42.86%	50.0%	A, D	5	2	26	5	31.27%	71.43%
B, A	3	4	26	5	42.86%	10.34%	B, F	3	4	3	28	28.54%	42.86%
C, F	3	4	3	28	42.86%	50.0%	C, F	3	4	3	28	28.54%	42.86%
A, F	3	4	3	28	42.86%	50.0%	A, F	3	4	3	28	28.54%	42.86%
F, G	3	4	3	28	42.86%	50.0%	F, G	3	4	3	28	28.54%	42.86%
F, E	3	4	3	28	42.86%	50.0%	F, E	3	4	3	28	28.54%	42.86%
A, E	3	4	26	5	42.86%	10.34%	F, D	3	4	3	28	28.54%	42.86%
F, D	3	4	3	28	42.86%	50.0%	B, A	2	5	0	31	18.37%	28.57%
A, D	3	4	26	5	42.86%	10.34%	B, C	2	5	0	31	18.37%	28.57%
C, A	3	4	26	5	42.86%	10.34%	B, G	2	5	0	31	18.37%	28.57%
A, G	3	4	26	5	42.86%	10.34%	B, E	2	5	0	31	18.37%	28.57%
B, C	2	5	0	31	28.57%	100.0%	A, E	3	4	26	5	12.64%	42.86%
B, G	2	5	0	31	28.57%	100.0%	C, A	3	4	26	5	12.64%	42.86%
B, E	2	5	0	31	28.57%	100.0%	A, G	3	4	26	5	12.64%	42.86%
C, E	1	6	2	29	14.29%	33.33%	C, E	1	6	2	29	7.7%	14.29%
G, E	1	6	2	29	14.29%	33.33%	G, E	1	6	2	29	7.7%	14.29%
C, G	0	7	0	31	0.0%	0.00%	C, G	0	7	0	31	0.0%	0.0%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.16: Ranking of combinations of 2 SAST tools regarding their performance in category A8: Software and Data Integrity Failures - Business and Heightened Critical Scenarios

A8: Software and Data Integrity Failures													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Insecure Deserialization													
B, D	6	1	26	5	30.77%	85.71%	B, F	2	5	0	31	93.06%	100.0%
C, D	5	2	26	5	26.32%	71.43%	B, A	2	5	0	31	93.06%	100.0%
G, D	5	2	26	5	26.32%	71.43%	B, C	2	5	0	31	93.06%	100.0%
E, D	5	2	26	5	26.32%	71.43%	B, G	2	5	0	31	93.06%	100.0%
A, D	5	2	26	5	26.32%	71.43%	B, E	2	5	0	31	93.06%	100.0%
B, F	3	4	3	28	46.15%	42.86%	C, F	3	4	3	28	68.75%	50.0%
C, F	3	4	3	28	46.15%	42.86%	A, F	3	4	3	28	68.75%	50.0%
A, F	3	4	3	28	46.15%	42.86%	F, G	3	4	3	28	68.75%	50.0%
F, G	3	4	3	28	46.15%	42.86%	F, E	3	4	3	28	68.75%	50.0%
F, E	3	4	3	28	46.15%	42.86%	A, E	1	6	2	29	58.1%	33.33%
F, D	3	4	3	28	46.15%	42.86%	C, E	1	6	2	29	58.1%	33.33%
C, A	3	4	26	5	16.67%	42.86%	G, E	1	6	2	29	58.1%	33.33%
A, G	3	4	26	5	16.67%	42.86%	B, D	6	1	26	5	51.04%	18.75%
B, A	2	5	0	31	44.44%	28.57%	F, D	5	2	26	5	43.78%	16.13%
B, C	2	5	0	31	44.44%	28.57%	C, D	5	2	26	5	43.78%	16.13%
B, G	2	5	0	31	44.44%	28.57%	G, D	5	2	26	5	43.78%	16.13%
B, E	2	5	0	31	44.44%	28.57%	E, D	5	2	26	5	43.78%	16.13%

A, E	1	6	2	29	20.0%	14.29%	A, D	5	2	26	5	43.78%	16.13%
C, E	1	6	2	29	20.0%	14.29%	C, A	0	7	0	31	0.00%	0.00%
G, E	1	6	2	29	20.0%	14.29%	A, G	0	7	0	31	0.00%	0.00%
C, G	0	7	0	31	0.0%	0.0%	C, G	0	7	0	31	0.00%	0.00%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.17: Ranking of combinations of 2 SAST tools regarding their performance in category A8: Software and Data Integrity Failures - Best and Minimum Effort Scenarios

Results obtained in A9: Security Logging and Monitoring Failures

A9: Security Logging and Monitoring Failures													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Improper Output Neutralization for Logs													
C, A	379	358	245	566	51.42%	60.74%	C, A	379	358	245	566	31.17%	51.42%
C, E	379	358	245	566	51.42%	60.74%	C, E	379	358	245	566	31.17%	51.42%
B, C	362	375	245	566	49.12%	59.64%	B, C	362	375	245	566	29.2%	49.12%
C, D	345	392	245	566	46.81%	58.47%	C, D	345	392	245	566	27.29%	46.81%
C, F	345	392	245	566	46.81%	58.47%	C, F	345	392	245	566	27.29%	46.81%
C, G	345	392	245	566	46.81%	58.47%	C, G	345	392	245	566	27.29%	46.81%
B, A	180	557	1	810	24.42%	99.45%	B, A	180	557	1	810	15.18%	24.42%
A, F	180	557	1	810	24.42%	99.45%	A, F	180	557	1	810	15.18%	24.42%
A, G	180	557	1	810	24.42%	99.45%	A, G	180	557	1	810	15.18%	24.42%
A, E	180	557	1	810	24.42%	99.45%	A, E	180	557	1	810	15.18%	24.42%
A, D	180	557	1	810	24.42%	99.45%	A, D	180	557	1	810	15.18%	24.42%
B, E	133	604	5	806	18.05%	96.38%	G, D	143	594	61	750	10.85%	19.4%
F, E	133	604	5	806	18.05%	96.38%	B, E	133	604	5	806	10.6%	18.05%
G, E	133	604	5	806	18.05%	96.38%	F, E	133	604	5	806	10.6%	18.05%
E, D	133	604	5	806	18.05%	96.38%	G, E	133	604	5	806	10.6%	18.05%
B, F	130	607	12	799	17.64%	91.55%	E, D	133	604	5	806	10.6%	18.05%
B, G	130	607	12	799	17.64%	91.55%	B, F	130	607	12	799	10.24%	17.64%
B, D	130	607	12	799	17.64%	91.55%	B, G	130	607	12	799	10.24%	17.64%
G, D	143	594	61	750	19.4%	70.1%	B, D	130	607	12	799	10.24%	17.64%
F, D	143	594	61	750	19.4%	70.1%	F, D	18	719	121	690	1.07%	2.44%
F, G	18	719	121	690	2.44%	12.95%	F, G	18	719	121	690	1.07%	2.44%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.18: Ranking of combinations of 2 SAST tools regarding their performance in category A9: Security Logging and Monitoring Failures - Business and Heightened Critical Scenarios

A9: Security Logging and Monitoring Failures													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Improper Output Neutralization for Logs													
C, A	379	358	245	566	55.69%	51.42%	C, A	180	557	1	810	79.35%	99.45%
C, E	379	358	245	566	55.69%	51.42%	B, A	180	557	1	810	79.35%	99.45%
B, C	362	375	245	566	53.87%	49.12%	A, F	180	557	1	810	79.35%	99.45%
C, D	345	392	245	566	52.0%	46.81%	A, G	180	557	1	810	79.35%	99.45%
C, F	345	392	245	566	52.0%	46.81%	A, E	180	557	1	810	79.35%	99.45%
C, G	345	392	245	566	52.0%	46.81%	A, D	180	557	1	810	79.35%	99.45%
B, A	180	557	1	810	39.22%	24.42%	C, E	133	604	5	806	76.77%	96.38%
A, F	180	557	1	810	39.22%	24.42%	B, E	133	604	5	806	76.77%	96.38%
A, G	180	557	1	810	39.22%	24.42%	F, E	133	604	5	806	76.77%	96.38%
A, E	180	557	1	810	39.22%	24.42%	G, E	133	604	5	806	76.77%	96.38%
A, D	180	557	1	810	39.22%	24.42%	E, D	133	604	5	806	76.77%	96.38%
G, D	143	594	61	750	30.39%	19.4%	B, C	130	607	12	799	74.19%	91.55%
B, E	133	604	5	806	30.4%	18.05%	B, F	130	607	12	799	74.19%	91.55%
F, E	133	604	5	806	30.4%	18.05%	B, G	130	607	12	799	74.19%	91.55%
G, E	133	604	5	806	30.4%	18.05%	B, D	130	607	12	799	74.19%	91.55%

E, D	133	604	5	806	30.4%	18.05%	C, D	143	594	61	750	62.95%	70.1%
B, F	130	607	12	799	29.58%	17.64%	G, D	143	594	61	750	62.95%	70.1%
B, G	130	607	12	799	29.58%	17.64%	F, D	143	594	61	750	62.95%	70.1%
B, D	130	607	12	799	29.58%	17.64%	C, F	345	392	245	566	58.78%	58.47%
F, D	18	719	121	690	4.11%	2.44%	C, G	345	392	245	566	58.78%	58.47%
F, G	18	719	121	690	4.11%	2.44%	F, G	18	719	121	690	30.96%	12.95%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.19: Ranking of combinations of 2 SAST tools regarding their performance in category A9: Security Logging and Monitoring Failures - Best and Minimum Effort Scenarios

Results obtained in A10: Server-Side Request Forgery

A10: Server-Side Request Forgery													
Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
Server-Side Request Forgery													
C, D	14	3	29	1	82.35%	32.56%	C, D	14	3	29	1	35.28%	82.35%
G, D	14	3	29	1	82.35%	32.56%	G, D	14	3	29	1	35.28%	82.35%
A, F	6	11	11	19	35.29%	35.29%	A, F	6	11	11	19	17.4%	35.29%
A, E	6	11	11	19	35.29%	35.29%	A, E	6	11	11	19	17.4%	35.29%
B, A	6	11	11	19	35.29%	35.29%	B, A	6	11	11	19	17.4%	35.29%
C, A	6	11	11	19	35.29%	35.29%	C, A	6	11	11	19	17.4%	35.29%
A, G	6	11	11	19	35.29%	35.29%	A, G	6	11	11	19	17.4%	35.29%
A, D	6	11	11	19	35.29%	35.29%	A, D	6	11	11	19	17.4%	35.29%
B, F	5	12	7	23	29.41%	41.67%	B, F	5	12	7	23	15.6%	29.41%
B, C	5	12	7	23	29.41%	41.67%	B, C	5	12	7	23	15.6%	29.41%
B, G	5	12	7	23	29.41%	41.67%	B, G	5	12	7	23	15.6%	29.41%
B, E	5	12	7	23	29.41%	41.67%	B, E	5	12	7	23	15.6%	29.41%
B, D	5	12	7	23	29.41%	41.67%	B, D	5	12	7	23	15.6%	29.41%
F, E	2	15	1	29	11.76%	66.67%	F, E	2	15	1	29	6.38%	11.76%
C, E	2	15	1	29	11.76%	66.67%	C, E	2	15	1	29	6.38%	11.76%
G, E	2	15	1	29	11.76%	66.67%	G, E	2	15	1	29	6.38%	11.76%
E, D	2	15	1	29	11.76%	66.67%	E, D	2	15	1	29	6.38%	11.76%
C, F	1	16	0	30	5.88%	100.0%	C, F	1	16	0	30	3.11%	5.88%
F, G	1	16	0	30	5.88%	100.0%	F, G	1	16	0	30	3.11%	5.88%
F, D	1	16	0	30	5.88%	100.0%	F, D	1	16	0	30	3.11%	5.88%
C, G	0	17	0	30	0.0%	0.00%	C, G	0	17	0	30	0.0%	0.0%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.20: Ranking of combinations of 2 SAST tools regarding their performance in category A10: Server-Side Request Forgery - Business and Heightened Critical Scenarios

A10: Server-Side Request Forgery													
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
Server-Side Request Forgery													
C, D	14	3	29	1	46.67%	82.35%	A, F	1	16	0	30	82.61%	100.0%
G, D	14	3	29	1	46.67%	82.35%	B, F	1	16	0	30	82.61%	100.0%
A, F	6	11	11	19	35.29%	35.29%	F, E	1	16	0	30	82.61%	100.0%
A, E	6	11	11	19	35.29%	35.29%	C, F	1	16	0	30	82.61%	100.0%
B, A	6	11	11	19	35.29%	35.29%	F, G	1	16	0	30	82.61%	100.0%
C, A	6	11	11	19	35.29%	35.29%	F, D	1	16	0	30	82.61%	100.0%
A, G	6	11	11	19	35.29%	35.29%	A, E	2	15	1	29	66.29%	66.67%
A, D	6	11	11	19	35.29%	35.29%	C, E	2	15	1	29	66.29%	66.67%
B, F	5	12	7	23	34.48%	29.41%	G, E	2	15	1	29	66.29%	66.67%
B, C	5	12	7	23	34.48%	29.41%	E, D	2	15	1	29	66.29%	66.67%
B, G	5	12	7	23	34.48%	29.41%	B, A	5	12	7	23	53.69%	41.67%
B, E	5	12	7	23	34.48%	29.41%	B, C	5	12	7	23	53.69%	41.67%
B, D	5	12	7	23	34.48%	29.41%	B, G	5	12	7	23	53.69%	41.67%

F, E	2	15	1	29	20.0%	11.76%	B, E	5	12	7	23	53.69%	41.67%
C, E	2	15	1	29	20.0%	11.76%	B, D	5	12	7	23	53.69%	41.67%
G, E	2	15	1	29	20.0%	11.76%	C, A	6	11	11	19	49.31%	35.29%
E, D	2	15	1	29	20.0%	11.76%	A, G	6	11	11	19	49.31%	35.29%
C, F	1	16	0	30	11.11%	5.88%	A, D	6	11	11	19	49.31%	35.29%
F, G	1	16	0	30	11.11%	5.88%	C, D	14	3	29	1	28.78%	32.56%
F, D	1	16	0	30	11.11%	5.88%	G, D	14	3	29	1	28.78%	32.56%
C, G	0	17	0	30	0.0%	0.0%	C, G	0	17	0	30	0.00%	0.00%
A - Semgrep | B - Snyk | C - Fortify | D - Spotbugs | E - Kiuwan | F - Synospys | G - Horusec													

Table 5.21: Ranking of combinations of 2 SAST tools regarding their performance in category A10: Server-Side Request Forgery - Best and Minimum Effort Scenarios

Chapter 6

Agreement for all pairs of SAST Tools

To better understand the results obtained and the conclusions drawn from the combinations, the concordance of the SAST tools' outputs was calculated. This is because the level of overlap between the issues detected by the combinations of two directly impacts the number of TPs they can achieve and, at the same time, the number of FPs generated. Therefore, for each combination of two, the number of issues detected in common was counted and divided by the lowest number of issues identified between the tools. This process was carried out separately for TPs and FPs, and the agreement rate obtained is shown in table 6.1.

Combinations of tools	TP Agreement Rate (%)	FP Agreement Rate (%)
Semgrep, Kiuwan	54.83%	34.65%
Snyk, Semgrep	56.69%	30.11%
Synopsys, Kiuwan	59.07%	42.15%
Fortify, Semgrep	53.17%	42.13%
Fortify, Synopsys	62.20%	16.48%
Snyk, Fortify	68.20%	26.33%
Fortify, Kiuwan	65.09%	21.53%
Semgrep, SpotBugs	61.29%	94.91%
Snyk, Synopsys	69.76%	39.59%
Kiuwan, SpotBugs	69.82%	90.46%
Snyk, Kiuwan	79.02%	29.14%
Semgrep, Synopsys	69.99%	43.21%
Horusec, Kiuwan	56.12%	7.86%
Synopsys, SpotBugs	76.63%	89.90%
Fortify, SpotBugs	76.04%	31.25%
Fortify, Horusec	77.89%	12.45%
Snyk, SpotBugs	83.41%	57.80%
Semgrep, Horusec	67.50%	10.42%
Synopsys, Horusec	66.80%	12.63%
Horusec, SpotBugs	78.76%	46.58%
Snyk, Horusec	97.50%	17.62%

Table 6.1: TP and FP agreement rate for each combination of 2