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

João Silva

Performance Results Tables for thesis "Evaluation of Dynamic Analysis Tools in detecting OWASP Top 10 Vulnerabilities"

September 6, 2024

Contents

1. Introduction

This document is used to present the results commented in thesis "Evaluation of Dynamic Analysis tools in detecting the Open Worldwide Application Security Project (OWASP) Top 10 vulnerabilities", chapter "Benchmark Results". The following information is present here:

- Results achieved by the tools in each application
- Results achieved by combinations of 2 and 3 tools without weights
- Results achieved by combinations of 2 tools with weights

2. Performance Results of all DAST Tools for each Application

This chapter provides a better ideia of how well the Dynamic Application Security Testing (DAST) tools worked in each application, demonstrating the True Positive (TP)s, False Positive (FP)s, True Negative (TN)s and False Negative (FN)s obtained. The conclusions about this chapter will be in section X of the mentioned thesis.

Results obtained in OWASP Benchmark

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	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
	Path Traversal	133	135	14	0	133	4	145	0	133	4	145	0	133	6	143
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Untrusted/Invalid TLS Certificate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	126	125	0	68	58	0	125	11	115	0	125	21	105	0	125
	SQL Injection	272	232	172	158	114	39	365	0	272	15	389	67	205	5	399
	LDAP Injection	27	32	5	0	27	0	37	0	27	5	32	0	27	0	37
	Cross-Site Scripting	246	209	476	190	56	178	507	74	172	476	209	5	241	0	685
	XPath Injection	15	20	0	0	15	0	20	0	15	0	20	0	15	0	20
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Bad Security Design of Form Fields	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	FPFP	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	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	FPFP	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	FPFP	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 2.1: DAST tools output in relation to OWASP Benchmark - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	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
	Path Traversal	133	135	14	0	133	0	149	33	100	26	123	90	43	91	58
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Untrusted/Invalid TLS Certificate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	126	125	0	0	126	0	125	20	106	19	106	78	48	80	45
	SQL Injection	272	232	172	114	158	0	404	74	198	73	331	194	78	235	169
	LDAP Injection	27	32	5	17	10	5	32	0	27	0	37	3	24	3	34
	Cross-Site Scripting	246	209	476	70	176	0	685	70	176	55	630	114	132	135	550
	XPath Injection	15	20	0	0	15	0	20	2	13	2	18	7	8	13	7
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Bad Security Design of Form Fields	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	FPFP	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	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	FPFP	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	FPFP	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 2.2: DAST tools output in relation to OWASP Benchmark - Part2

Results obtained in WAVSEP Benchmark

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	60	9	7	40	20	4	12	29	31	7	9	8	52	2	14
	Path Traversal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Remote File Inclusion	108	6	402	44	64	0	408	59	49	3	405	0	108	0	408
	Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Untrusted/Invalid TLS Certificate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	128	0	0	31	97	0	0	4	124	0	0	0	128	0	0
	SQL Injection	161	10	7	0	161	0	17	0	161	3	14	0	161	7	10
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	117	7	751	74	43	166	592	89	28	483	275	110	7	33	725
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Bad Security Design of Form Fields	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	12	0	0	0	12	0	0	0	12	0	0	0	12	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	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	FPFP	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	817	8	115	117	700	31	92	350	467	66	57	118	699	0	123

Table 2.3: DAST tools output in relation to WAVSEP Benchmark - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	60	9	7	0	60	0	16	60	0	9	7	60	0	9	7
	Path Traversal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Remote File Inclusion	108	6	402	36	72	339	69	0	108	64	344	0	108	0	408
	Cross-Site Request Forgery	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Untrusted/Invalid TLS Certificate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	128	0	0	0	128	0	0	0	128	0	0	77	51	0	0
	SQL Injection	161	10	7	0	161	0	17	93	68	0	17	25	136	10	7
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	117	7	751	104	13	143	615	4	113	191	567	113	4	153	605
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Bad Security Design of Form Fields	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	12	0	0	0	12	0	0	5	7	0	0	0	12	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	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	FPFP	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	817	8	115	448	369	76	47	109	708	0	123	9	808	8	115

Table 2.4: DAST tools output in relation to WAVSEP Benchmark - Part2

Results obtained in WebGoat

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	16	5	0	0	16	0	5	0	16	0	5	0	16	0	5
	Path Traversal	4	12	48	2	2	49	11	0	4	0	60	0	4	0	60
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	79	100	0	79	0	37	63	24	55	15	85	0	79	0	100
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	17	9	49	1	16	48	10	0	17	0	58	0	17	0	58
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	6	5	12	0	6	4	13	0	6	4	13	0	6	0	17
	XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	HTTP Response Splitting	3	2	0	0	3	0	2	0	3	0	2	0	3	0	2
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	16	3	10	0	16	1	12	0	16	0	13	0	16	0	13
	Bad Security Design of Form Fields	80	54	0	0	80	0	54	0	80	0	54	1	79	0	54
	Method Tampering	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A5	Security Misconfiguration	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0
	Bad Programming of Cookies	18	2	0	4	14	0	2	1	17	0	2	1	17	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	5	1	1	2	3	2	0	0	5	0	2	0	5	0	2
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	2	3	0	0	2	0	3	0	2	0	3	0	2	0	3
	Brute Force Attacks	7	2	0	0	7	0	2	0	7	0	2	0	7	0	2
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	3	2	0	0	3	0	2	2	1	1	1	0	3	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	13	0	0	0	13	0	0	0	13	0	0	0	13	0	0
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0

Table 2.5: DAST tools output in relation to WebGoat - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	16	5	0	0	16	0	5	1	15	0	5	2	14	0	5
	Path Traversal	4	12	48	0	4	0	60	0	4	2	58	3	1	2	58
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	79	100	0	3	76	0	100	32	47	12	88	79	0	49	51
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	17	9	49	1	16	0	58	2	15	3	55	4	13	2	56
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	6	5	12	0	6	0	17	3	3	4	13	1	5	2	15
	XPath Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	HTTP Response Splitting	3	2	0	0	3	0	2	0	3	0	2	0	3	0	2
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	16	3	10	1	15	7	6	1	15	2	11	4	12	1	12
	Bad Security Design of Form Fields	80	54	0	0	80	3	51	0	80	0	54	0	80	0	54
	Method Tampering	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A5	Security Misconfiguration	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0
	Bad Programming of Cookies	18	2	0	3	15	0	2	3	15	0	2	3	15	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	5	1	1	0	5	0	2	0	5	0	2	2	3	1	1
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	2	3	0	0	2	0	3	0	2	0	3	0	2	0	3
	Brute Force Attacks	7	2	0	3	4	1	1	2	5	1	1	0	7	0	2
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	3	2	0	0	3	0	2	0	3	0	2	0	3	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	13	0	0	2	11	0	0	2	11	0	0	0	13	0	0
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	2	0	0	0	2	0	0	1	1	0	0	2	0	0	0

Table 2.6: DAST tools output in relation to the WebGoat - Part2

Results obtained in Juice Shop

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	25	10	0	0	25	0	10	0	25	0	10	0	25	0	10
	Path Traversal	5	5	0	0	5	0	5	0	5	0	5	0	5	0	5
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	21	8	0	1	20	0	8	0	21	0	8	0	21	0	8
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	1	0	1	0	1	1	0	0	1	0	1	0	1	0	1
	SQL Injection	2	1	11	2	0	11	1	0	2	0	12	0	2	0	12
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	6	3	13	1	5	10	6	0	6	0	16	0	6	0	16
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	6	1	1	1	5	0	2	1	5	0	2	0	6	0	2
	Bad Security Design of Form Fields	4	24	0	0	4	0	24	0	4	0	24	0	4	0	24
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	1	5	0	0	1	0	5	0	1	0	5	0	1	0	5
	Bad Programming of Cookies	11	1	0	2	9	0	1	2	9	0	1	0	11	0	1
	Insecure Use of Hard Coded Constants	13	0	0	0	13	0	0	0	13	0	0	0	13	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	3	0	0	1	2	0	0	1	2	0	0	0	3	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	2	1	0	0	2	0	1	0	2	0	1	0	2	0	1
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	1	2	0	1	0	0	2	1	0	0	2	0	1	0	2
	Insecure Deserialization	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
A9	Security Logging and Monitoring Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2

Table 2.7: DAST tools output in relation to Juice Shop - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	25	10	0	0	25	0	10	1	24	1	9	3	22	2	8
	Path Traversal	5	5	0	0	5	0	5	0	5	0	5	1	4	0	5
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	21	8	0	0	21	0	8	0	21	2	6	3	18	1	7
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	1	0	1	0	1	0	1	0	1	0	1	1	0	0	1
	SQL Injection	2	1	11	0	2	0	12	0	2	0	12	2	0	5	7
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	6	3	13	0	6	0	16	1	5	0	16	0	6	3	13
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	6	1	1	0	6	0	2	1	5	0	2	0	6	1	1
	Bad Security Design of Form Fields	4	24	0	0	4	0	24	0	4	0	24	0	4	0	24
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	XML External Entities	1	5	0	0	1	0	5	0	1	0	5	0	1	0	5
	Bad Programming of Cookies	11	1	0	0	11	0	1	0	11	0	1	3	8	0	1
	Insecure Use of Hard Coded Constants	13	0	0	0	13	0	0	0	13	0	0	0	13	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	2	1	0	0	2	0	1	0	2	0	1	0	2	0	1
	Brute Force Attacks	2	0	0	0	2	0	0	1	1	0	0	0	2	0	0
	Session Fixation	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
	Insecure Deserialization	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
A9	Security Logging and Monitoring Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	1	2	0	0	1	0	2	1	0	0	2	0	1	0	2

Table 2.8: DAST tools output in relation to Juice Shop - Part2

Results obtained in Mutillidae II

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	20	0	14	1	19	0	14	1	19	14	0	0	20	0	14
	Path Traversal	6	0	0	3	3	0	0	3	3	0	0	1	5	0	0
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	55	2	0	55	0	2	0	42	13	0	2	0	55	0	2
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	4	0	0	0	4	0	0	3	1	0	0	0	4	0	0
	SQL Injection	17	0	21	6	11	15	6	4	13	4	17	2	15	0	21
	LDAP Injection	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
	Cross-Site Scripting	45	5	36	23	22	27	14	22	23	9	32	1	44	0	41
	XPath Injection	3	0	2	0	3	0	2	0	3	2	0	0	3	0	2
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	37	4	71	12	25	66	9	0	37	0	75	0	37	0	75
	Bad Security Design of Form Fields	21	15	0	0	21	0	15	0	21	0	15	0	21	0	15
	Method Tampering	74	1	2	23	51	3	0	6	68	0	3	0	74	0	3
A5	Security Misconfiguration	P	N	FPFP	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	13	3	0	8	5	0	3	3	10	0	3	2	11	0	3
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	4	0	0	2	2	0	0	2	2	0	0	0	4	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	3	3	0	2	1	3	0	0	3	0	3	0	3	0	3
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	4	0	0	2	2	0	0	2	2	0	0	0	4	0	0

Table 2.9: DAST tools output in relation to Mutillidae II - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	20	0	14	1	19	0	14	0	20	0	14	0	20	7	7
	Path Traversal	6	0	0	0	6	0	0	0	6	0	0	2	4	0	0
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	55	2	0	0	55	1	1	21	34	0	2	55	0	2	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	4	0	0	0	4	0	0	1	3	0	0	2	2	0	0
	SQL Injection	17	0	21	7	10	3	18	4	13	0	21	7	10	7	14
	LDAP Injection	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
	Cross-Site Scripting	45	5	36	0	45	0	41	2	43	1	40	25	20	3	38
	XPath Injection	3	0	2	0	3	0	2	0	3	0	2	0	3	0	2
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	37	4	71	26	11	7	68	6	31	0	75	14	23	33	42
	Bad Security Design of Form Fields	21	15	0	0	21	6	9	0	21	0	15	0	21	0	15
	Method Tampering	74	1	2	0	74	0	3	0	74	0	3	30	44	0	3
A5	Security Misconfiguration	P	N	FPFP	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	13	3	0	1	12	0	3	2	11	0	3	8	5	0	3
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	1	0	0	1	0	0	0	0	1	0	0	1	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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	1	0	0	0
	Brute Force Attacks	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	3	3	0	0	3	0	3	0	3	1	2	3	0	2	1
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0

Table 2.10: DAST tools output in relation to Mutillidae II - Part2

Results obtained in Altoro Mutual

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	3	2	0	1	2	0	2	0	3	0	2	1	2	0	2
	Path Traversal	1	0	3	0	1	3	0	0	1	0	3	1	0	0	3
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	7	23	0	7	0	23	0	4	3	10	13	0	7	0	23
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	5	9	3	3	2	1	11	2	3	1	11	0	5	0	12
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	5	4	51	5	0	51	4	2	3	3	52	2	3	2	53
	XPath Injection	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	5	0	7	0	5	1	6	0	5	0	7	0	5	0	7
	Bad Security Design of Form Fields	10	7	0	0	10	0	7	0	10	0	7	1	9	0	7
	Method Tampering	3	0	0	2	1	0	0	0	3	0	0	0	3	0	0
A5	Security Misconfiguration	P	N	FPFP	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	7	1	0	3	4	0	1	0	7	0	1	0	7	0	1
	Insecure Use of Hard Coded Constants	11	0	0	0	11	0	0	0	11	0	0	0	11	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	2	0	0	0	2	0	0	1	1	0	0	0	2	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	1	1	0	1	0	0	1	0	1	0	1	0	1	0	1
A10	Server-Side Request Forgery	P	N	FPFP	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 2.11: DAST tools output in relation to Altoro Mutual - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	3	2	0	0	3	0	2	2	1	0	2	2	1	0	2
	Path Traversal	1	0	3	1	0	0	3	0	1	0	3	1	0	0	3
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	7	23	0	3	4	0	23	2	5	19	4	7	0	23	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	5	9	3	1	4	0	12	2	3	3	9	3	2	6	6
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	5	4	51	1	4	0	55	1	4	2	53	4	1	19	36
	XPath Injection	1	1	0	0	1	0	1	1	0	1	0	0	1	0	1
	HTTP Response Splitting	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	Insecure Design	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	5	0	7	1	4	6	1	0	5	2	5	2	3	0	7
	Bad Security Design of Form Fields	10	7	0	0	10	1	6	0	10	0	7	0	10	0	7
	Method Tampering	3	0	0	0	3	0	0	1	2	0	0	2	1	0	0
A5	Security Misconfiguration	P	N	FPFP	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	7	1	0	0	7	0	1	1	6	0	1	3	4	0	1
	Insecure Use of Hard Coded Constants	11	0	0	0	11	0	0	0	11	0	0	0	11	0	0
A6	Vulnerable and Outdated Components	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	0	2	0	0	0	2	0	0	2	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	1	1	0	0	1	0	1	0	1	0	1	1	0	0	1
A10	Server-Side Request Forgery	P	N	FPFP	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 2.12: DAST tools output in relation to Altoro Mutual - Part2

Results obtained in BWapp

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	5	0	3	2	3	1	2	1	4	1	2	1	4	0	3
	Path Traversal	4	0	0	1	3	0	0	2	2	0	0	1	3	0	0
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	92	0	0	92	0	0	0	67	25	0	0	0	92	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	3	0	0	0	3	0	0	1	2	0	0	1	2	0	0
	SQL Injection	15	1	6	0	15	0	7	0	15	0	7	5	10	6	1
	LDAP Injection	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
	Cross-Site Scripting	15	1	52	8	7	45	8	7	8	4	49	3	12	4	49
	XPath Injection	3	0	0	0	3	0	0	1	2	0	0	2	1	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	4	0	45	1	3	12	33	0	4	0	45	1	3	0	45
	Bad Security Design of Form Fields	26	44	0	0	26	0	44	0	26	0	44	0	26	2	42
	Method Tampering	8	0	1	4	4	0	1	0	8	1	0	0	8	0	1
A5	Security Misconfiguration	P	N	FPFP	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	17	3	0	7	10	0	3	1	16	0	3	4	13	0	3
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	7	0	0	1	6	0	0	1	6	0	0	0	7	0	0
	Brute Force Attacks	3	2	0	0	3	0	2	0	3	0	2	0	3	0	2
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	5	0	0	3	2	0	0	3	2	0	0	0	5	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	13	1	0	10	3	1	0	5	8	0	1	8	5	0	1
A10	Server-Side Request Forgery	P	N	FPFP	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 2.13: DAST tools output in relation to the BWapp - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	5	0	3	0	5	1	2	1	4	0	3	2	3	1	2
	Path Traversal	4	0	0	1	3	0	0	1	3	0	0	1	3	0	0
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	92	0	0	32	60	0	0	42	50	0	0	92	0	0	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	3	0	0	0	3	0	0	0	3	0	0	1	2	0	0
	SQL Injection	15	1	6	0	15	0	7	4	11	0	7	2	13	0	7
	LDAP Injection	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
	Cross-Site Scripting	15	1	52	2	13	0	53	2	13	0	53	9	6	16	37
	XPath Injection	3	0	0	0	3	0	0	1	2	0	0	0	3	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	4	0	45	4	0	36	9	0	4	0	45	2	2	4	41
	Bad Security Design of Form Fields	26	44	0	0	26	4	40	0	26	0	44	0	26	0	44
	Method Tampering	8	0	1	0	8	0	1	0	8	0	1	2	6	0	1
A5	Security Misconfiguration	P	N	FPFP	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	17	3	0	1	16	0	3	2	15	0	3	5	12	0	3
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	7	0	0	0	7	0	0	0	7	0	0	0	7	0	0
	Brute Force Attacks	3	2	0	3	0	2	0	1	2	1	1	0	3	0	2
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	5	0	0	0	5	0	0	0	5	0	0	0	5	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	13	1	0	6	7	0	1	3	10	0	1	10	3	1	0
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0

Table 2.14: DAST tools output in relation to BWapp - Part2

Results obtained in Piwigo

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
	Path Traversal	0	2	12	0	0	12	2	0	0	1	13	0	0	0	14
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	6	34	0	6	0	25	9	6	0	15	19	0	6	0	34
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	10	92	17	0	10	13	96	0	10	3	106	0	10	1	108
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	7	19	56	0	7	18	57	0	7	21	54	0	7	13	62
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	6	11	0	4	2	11	0	0	6	0	11	0	6	0	11
	Bad Security Design of Form Fields	12	41	1	0	12	0	42	0	12	0	42	0	12	0	42
	Method Tampering	4	0	5	3	1	5	0	0	4	0	5	0	4	0	5
A5	Security Misconfiguration	P	N	FPFP	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	30	2	0	1	29	0	2	0	30	0	2	1	29	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	2	0	0	0	0	2	0	0	1	1	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	8	0	0	0	8	0	0	4	4	0	0	0	8	0	0
	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	FPFP	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	FPFP	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 2.15: DAST tools output in relation to Piwigo - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
	Path Traversal	0	2	12	0	0	0	14	0	0	0	14	0	0	2	12
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	6	34	0	6	0	0	34	4	2	10	24	6	0	29	5
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	10	92	17	0	10	2	107	1	9	11	98	4	6	3	106
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	7	19	56	0	7	6	69	0	7	1	74	3	4	13	62
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	6	11	0	4	2	1	10	0	6	0	11	6	0	11	0
	Bad Security Design of Form Fields	12	41	1	0	12	2	40	0	12	0	42	0	12	0	42
	Method Tampering	4	0	5	0	4	0	5	0	4	0	5	2	2	0	5
A5	Security Misconfiguration	P	N	FPFP	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	30	2	0	0	30	0	2	2	28	0	2	3	27	0	2
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	0	2	0	0	0	2	0	0	2	0	0	0
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	2	0	0	0	2	0	0	1	1	0	0	0	2	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	8	0	0	0	8	0	0	0	8	0	0	0	8	0	0
	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	FPFP	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	FPFP	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 2.16: DAST tools output in relation to Piwigo - Part2

Results obtained in Shopizer

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	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
	Path Traversal	0	0	4	0	0	4	0	0	0	0	4	0	0	0	4
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	26	6	0	0	26	0	6	13	13	2	4	0	26	0	6
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	0	2	0	0	2	0	0	0	0	2	0	0	0	2
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	0	1	0	0	0	0	1	0	0	0	1	0	0	0	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	1	2	0	0	2	1	0	0	0	3	0	0	0	3
	Bad Security Design of Form Fields	97	92	0	0	97	0	92	0	97	0	92	0	97	0	92
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	4	0	0	1	3	0	0	0	4	0	0	0	4	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	18	1	0	0	2	17	0	0	0	19	0	0	0	19
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
	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	FPFP	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	FPFP	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 2.17: DAST tools output in relation to Shopizer - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	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
	Path Traversal	0	0	4	0	0	0	4	0	0	1	3	0	0	1	3
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	26	6	0	1	25	0	6	17	9	5	1	26	0	6	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	0	2	0	0	0	2	0	0	0	2	0	0	2	0
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	0	1	0	0	0	0	1	0	0	0	1	0	0	0	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	1	2	0	0	0	3	0	0	0	3	0	0	0	3
	Bad Security Design of Form Fields	97	92	0	0	97	0	92	0	97	0	92	0	97	0	92
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	4	0	0	0	4	0	0	0	4	0	0	2	2	0	0
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	18	1	0	0	0	19	0	0	0	19	0	0	2	17
A7	Identification and Authentication Failures	P	N	FPFP	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
	Brute Force Attacks	4	0	0	0	4	0	0	1	3	0	0	0	4	0	0
	Session Fixation	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
	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	FPFP	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	FPFP	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 2.18: DAST tools output in relation to Shopizer - Part2

Results obtained in PhpBB

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	3	0	0	0	0	3	0	0	0	3	0	0	0	3
	Path Traversal	0	2	3	0	0	0	5	0	0	3	2	0	0	0	5
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	20	7	0	20	0	7	0	3	17	0	7	0	20	0	7
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	0	57	0	0	46	11	0	0	15	42	0	0	0	57
	LDAP Injection	0	0	4	0	0	0	4	0	0	4	0	0	0	0	4
	Cross-Site Scripting	0	4	38	0	0	0	42	0	0	37	5	0	0	0	42
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	3	0	0	0	3	0	0	0	3	0	0	0	3
	Bad Security Design of Form Fields	7	22	0	0	7	0	22	0	7	0	22	0	7	1	21
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	6	6	0	3	3	0	6	0	6	0	6	0	6	0	6
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1
	Brute Force Attacks	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2
	Session Fixation	0	1	0	0	0	0	1	0	0	0	1	0	0	1	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	3	0	0	2	1	0	0	2	1	0	0	0	3	0	0
	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	FPFP	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1

Table 2.19: DAST tools output in relation to PhpBB - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	3	0	0	0	0	3	0	0	0	3	0	0	1	2
	Path Traversal	0	2	3	0	0	0	5	0	0	0	5	0	0	0	5
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	20	7	0	3	17	0	7	9	11	2	5	20	0	7	0
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	0	57	0	0	0	57	0	0	0	57	0	0	9	48
	LDAP Injection	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
	Cross-Site Scripting	0	4	38	0	0	0	42	0	0	5	37	0	0	3	39
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	3	0	0	0	3	0	0	0	3	0	0	3	0
	Bad Security Design of Form Fields	7	22	0	0	7	1	21	0	7	0	22	0	7	0	22
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	6	6	0	0	6	0	6	2	4	0	6	3	3	0	6
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	0	1	0	0	0	0	1	0	0	0	1	0	0	1	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
	Brute Force Attacks	0	2	0	0	0	2	0	0	0	0	2	0	0	0	2
	Session Fixation	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	3	0	0	1	2	0	0	0	3	0	0	0	3	0	0
	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	FPFP	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1

Table 2.20: DAST tools output in relation to PhpBB - Part2

Results obtained in WordPress

Vulnerability					Tools											
ID	Name	Total			OWASP ZAP				BurpSuite				Iron Wasp			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	5	9	0	0	0	14	0	0	9	5	0	0	0	14
	Path Traversal	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	0	40	0	0	0	25	15	0	0	13	27	0	0	0	40
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	2	23	0	0	19	6	0	0	1	24	0	0	3	22
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	1	14	42	0	1	0	56	0	1	42	14	0	1	0	56
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	12	0	0	2	10	0	0	0	12	0	0	0	12
	Bad Security Design of Form Fields	10	14	2	0	10	0	16	0	10	0	16	1	9	0	16
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	13	7	0	5	8	0	7	0	13	0	7	0	13	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1
	Brute Force Attacks	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	5	0	0	1	4	0	0	2	3	0	0	0	5	0	0
	Insecure Deserialization	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2
A9	Security Logging and Monitoring Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	0	8	0	0	0	0	8	0	0	0	8	0	0	0	8
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2

Table 2.21: DAST tools output in relation to WordPress - Part1

Vulnerability					Tools											
ID	Name	Total			Acunetix				Wapiti				OWASP ZAP Plugins			
A1	Broken Access Control	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authorization	0	5	9	0	0	0	14	0	0	0	14	0	0	0	14
	Path Traversal	1	2	0	0	1	0	2	0	1	0	2	0	1	0	2
	Remote File Inclusion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Request Forgery	0	40	0	0	0	8	32	0	0	3	37	0	0	25	15
A2	Cryptographic Failure	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Transmission of Information in Cleartext	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0
	Untrusted/Invalid TLS Certificate	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1
A3	Injection	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	OS Command Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	SQL Injection	0	2	23	0	0	0	25	0	0	0	25	0	0	4	21
	LDAP Injection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Cross-Site Scripting	1	14	42	0	1	0	56	0	1	0	56	0	1	7	49
	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Exposed Improper Error Handling	0	0	12	0	0	8	4	0	0	0	12	0	0	2	10
	Bad Security Design of Form Fields	10	14	2	0	10	3	13	0	10	0	16	0	10	0	16
	Method Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	Security Misconfiguration	P	N	FPFP	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	13	7	0	0	13	0	7	3	10	0	7	0	13	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	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure/Vulnerable Third-Party Software	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0
A7	Identification and Authentication Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Bypassing Authentication	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
	Brute Force Attacks	2	0	0	0	2	0	0	1	1	0	0	0	2	0	0
	Session Fixation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	Software and Data Integrity Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Insecure Scope of Cookies	5	0	0	0	5	0	0	0	5	0	0	0	5	0	0
	Insecure Deserialization	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2
A9	Security Logging and Monitoring Failures	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Improper Output Neutralization for Logs	0	8	0	0	0	0	8	0	0	0	8	0	0	0	8
A10	Server-Side Request Forgery	P	N	FPFP	TP	FN	FP	TN	TP	FN	FP	TN	TP	FN	FP	TN
	Server-Side Request Forgery	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2

Table 2.22: DAST tools output in relation to WordPress - Part2

3. Performance Results for all Combinations of 2 and 3 DAST Tools without Weights

This chapter provides the rankings obtained for combinations 2 and 3 DAST tools regarding each of the scenarios without using weights. This ranking will follow the methodology proposed in section X of the mentioned thesis, mainly disjunction of the tools results.

Results obtained in Combinations of 2 Tools

Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
C, F	1890	1623	1714	2657	53.8%	52.44%	C, F	1890	1623	1714	2657	30.82%	53.8%
B, F	1779	1734	2198	2173	50.64%	44.73%	B, F	1779	1734	2198	2173	25.41%	50.64%
E, F	1591	1922	1447	2924	45.29%	52.37%	A, F	1692	1821	1697	2674	26.33%	48.16%
A, C	1649	1864	1606	2765	46.94%	50.66%	A, C	1649	1864	1606	2765	25.86%	46.94%
A, F	1692	1821	1697	2674	48.16%	49.93%	E, F	1591	1922	1447	2924	25.4%	45.29%
A, B	1584	1929	2126	2245	45.09%	42.7%	A, B	1584	1929	2126	2245	21.74%	45.09%
D, F	1450	2063	1142	3229	41.28%	55.94%	A, E	1548	1965	1462	2909	24.37%	44.06%
C, E	1421	2092	1172	3199	40.45%	54.8%	D, F	1450	2063	1142	3229	23.76%	41.28%
A, E	1548	1965	1462	2909	44.06%	51.43%	C, E	1421	2092	1172	3199	22.98%	40.45%
A, D	1318	2195	1110	3261	37.52%	54.28%	A, D	1318	2195	1110	3261	21.03%	37.52%
B, E	1362	2151	1734	2637	38.77%	43.99%	B, E	1362	2151	1734	2637	19.21%	38.77%
B, C	1338	2175	1822	2549	38.09%	42.34%	B, C	1338	2175	1822	2549	18.36%	38.09%
D, C	1062	2451	753	3618	30.23%	58.51%	B, D	1088	2425	1360	3011	15.46%	30.97%
B, D	1088	2425	1360	3011	30.97%	44.44%	D, C	1062	2451	753	3618	17.08%	30.23%
D, E	1015	2498	617	3754	28.89%	62.19%	D, E	1015	2498	617	3754	16.58%	28.89%
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
C, F	1890	1623	1714	2657	53.11%	53.8%	D, E	1015	2498	617	3754	61.12%	62.19%
B, F	1779	1734	2198	2173	47.5%	50.64%	D, C	1062	2451	753	3618	59.06%	58.51%
A, F	1692	1821	1697	2674	49.03%	48.16%	D, F	1450	2063	1142	3229	58.48%	55.94%
A, C	1649	1864	1606	2765	48.73%	46.94%	C, E	1421	2092	1172	3199	57.63%	54.8%
E, F	1591	1922	1447	2924	48.57%	45.29%	A, D	1318	2195	1110	3261	57.03%	54.28%
A, E	1548	1965	1462	2909	47.46%	44.06%	C, F	1890	1623	1714	2657	57.26%	52.44%
D, F	1450	2063	1142	3229	47.5%	41.28%	E, F	1591	1922	1447	2924	56.35%	52.37%
C, E	1421	2092	1172	3199	46.54%	40.45%	A, E	1548	1965	1462	2909	55.56%	51.43%
A, B	1584	1929	2126	2245	43.86%	45.09%	A, C	1649	1864	1606	2765	55.2%	50.66%
B, E	1362	2151	1734	2637	41.22%	38.77%	A, F	1692	1821	1697	2674	54.71%	49.93%
B, C	1338	2175	1822	2549	40.1%	38.09%	B, F	1779	1734	2198	2173	50.18%	44.73%
A, D	1318	2195	1110	3261	44.37%	37.52%	B, D	1088	2425	1360	3011	49.92%	44.44%
B, D	1088	2425	1360	3011	36.5%	30.97%	B, E	1362	2151	1734	2637	49.53%	43.99%
D, C	1062	2451	753	3618	39.86%	30.23%	A, B	1584	1929	2126	2245	48.24%	42.7%
D, E	1015	2498	617	3754	39.46%	28.89%	B, C	1338	2175	1822	2549	48.15%	42.34%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Acunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 3.1: Ranking of Combination of 2 Tools by scenario

Results obtained in Combinations of 3 Tools

Business Critical					Metric	Tiebreaker	Heightened Critical					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	Recall	Precison	Comb.	TP	FN	FP	TN	Rec.*Infor.	Recall
C, E, F	2116	1397	2066	2305	60.23%	50.6%	A, C, F	2132	1381	2270	2101	33.0%	60.69%
A, C, F	2132	1381	2270	2101	60.69%	48.43%	C, E, F	2116	1397	2066	2305	34.02%	60.23%
D, C, F	1983	1530	1790	2581	56.45%	52.56%	D, C, F	1983	1530	1790	2581	32.6%	56.45%
A, C, E	1963	1550	2031	2340	55.88%	49.15%	A, C, E	1963	1550	2031	2340	30.57%	55.88%
A, E, F	1935	1578	2025	2346	55.08%	48.86%	B, C, F	2059	1454	2721	1650	28.24%	58.61%
B, E, F	2014	1499	2509	1862	57.33%	44.53%	A, B, F	2032	1481	2712	1659	27.71%	57.84%
B, C, F	2059	1454	2721	1650	58.61%	43.08%	B, E, F	2014	1499	2509	1862	28.64%	57.33%
A, B, F	2032	1481	2712	1659	57.84%	42.83%	A, E, F	1935	1578	2025	2346	29.95%	55.08%
A, D, F	1803	1710	1771	2600	51.32%	50.45%	B, D, F	1889	1624	2256	2115	27.47%	53.77%
B, D, F	1889	1624	2256	2115	53.77%	45.57%	A, B, E	1870	1643	2512	1859	25.49%	53.23%
A, B, E	1870	1643	2512	1859	53.23%	42.67%	A, D, F	1803	1710	1771	2600	28.44%	51.32%
A, B, C	1799	1714	2626	1745	51.21%	40.66%	D, E, F	1754	1759	1526	2845	28.71%	49.93%
D, E, F	1754	1759	1526	2845	49.93%	53.48%	A, D, C	1721	1792	1683	2688	27.06%	48.99%
A, D, E	1689	1824	1539	2832	48.08%	52.32%	A, D, E	1689	1824	1539	2832	27.13%	48.08%
A, D, C	1721	1792	1683	2688	48.99%	50.56%	D, C, E	1536	1977	1251	3120	25.16%	43.72%
B, C, E	1745	1768	2254	2117	49.67%	43.64%	A, B, C	1799	1714	2626	1745	23.33%	51.21%
A, B, D	1676	1837	2187	2184	47.71%	43.39%	B, C, E	1745	1768	2254	2117	24.37%	49.67%
D, C, E	1536	1977	1251	3120	43.72%	55.11%	A, B, D	1676	1837	2187	2184	23.3%	47.71%
B, D, E	1553	1960	1795	2576	44.21%	46.39%	B, D, E	1553	1960	1795	2576	22.8%	44.21%
B, D, C	1448	2065	1884	2487	41.22%	43.46%	B, D, C	1448	2065	1884	2487	20.22%	41.22%
Best Effort					Metric	Tiebreaker	Minimum Effort					Metric	Tiebreaker
Comb.	TP	FN	FP	TN	F-measure	Recall	Comb.	TP	FN	FP	TN	Markedness	Precision
A, C, F	2132	1381	2270	2101	53.87%	60.69%	D, C, E	1536	1977	1251	3120	58.16%	55.11%
C, E, F	2116	1397	2066	2305	55.0%	60.23%	D, E, F	1754	1759	1526	2845	57.63%	53.48%
B, E, F	2014	1499	2509	1862	50.12%	57.33%	D, C, F	1983	1530	1790	2581	57.67%	52.56%
D, C, F	1983	1530	1790	2581	54.43%	56.45%	A, D, E	1689	1824	1539	2832	56.57%	52.32%
A, C, E	1963	1550	2031	2340	52.3%	55.88%	C, E, F	2116	1397	2066	2305	56.43%	50.6%
A, E, F	1935	1578	2025	2346	51.79%	55.08%	A, D, C	1721	1792	1683	2688	55.28%	50.56%
A, D, F	1803	1710	1771	2600	50.88%	51.32%	A, D, F	1803	1710	1771	2600	55.39%	50.45%
D, E, F	1754	1759	1526	2845	51.64%	49.93%	A, C, E	1963	1550	2031	2340	54.65%	49.15%
A, D, E	1689	1824	1539	2832	50.11%	48.08%	A, E, F	1935	1578	2025	2346	54.32%	48.86%
B, C, F	2059	1454	2721	1650	49.66%	58.61%	A, C, F	2132	1381	2270	2101	54.39%	48.43%
A, B, F	2032	1481	2712	1659	49.22%	57.84%	B, D, E	1553	1960	1795	2576	51.59%	46.39%
B, D, F	1889	1624	2256	2115	49.33%	53.77%	B, D, F	1889	1624	2256	2115	51.07%	45.57%
A, B, E	1870	1643	2512	1859	47.37%	53.23%	B, E, F	2014	1499	2509	1862	49.96%	44.53%
A, B, C	1799	1714	2626	1745	45.33%	51.21%	B, C, E	1745	1768	2254	2117	49.06%	43.64%
B, C, E	1745	1768	2254	2117	46.46%	49.67%	B, D, C	1448	2065	1884	2487	49.05%	43.46%
A, D, C	1721	1792	1683	2688	49.76%	48.99%	A, B, D	1676	1837	2187	2184	48.85%	43.39%
A, B, D	1676	1837	2187	2184	45.44%	47.71%	B, C, F	2059	1454	2721	1650	48.12%	43.08%
B, D, E	1553	1960	1795	2576	45.27%	44.21%	A, B, F	2032	1481	2712	1659	47.83%	42.83%
D, C, E	1536	1977	1251	3120	48.76%	43.72%	A, B, E	1870	1643	2512	1859	47.88%	42.67%
B, D, C	1448	2065	1884	2487	42.31%	41.22%	A, B, C	1799	1714	2626	1745	45.55%	40.66%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Acunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 3.2: Ranking of Combination of 3 Tools by scenario

4. Performance Results for all Combinations of 2 DAST Tools with Weights

This chapter provides the rankings obtained for combinations 2 DAST tools regarding each of the scenarios per vulnerability using weights. This ranking will follow the methodology proposed in section X of the mentioned thesis, mainly following the weights approach. Here will provided too the tables with weights used.

Weights used for each tool regarding all vulnerabilities and scenarios

Vulnerability	Bypassing Authorization				Vulnerability	Path Traversal			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1429	0.1429	0.1429	0.1529	OWASP ZAP	0.1279	0.1429	0.1429	0.1279
Burp Suite	0.1379	0.1379	0.1379	0.1279	Burp Suite	0.1379	0.1379	0.1379	0.1379
Iron Wasp	0.1329	0.1329	0.1329	0.1379	Iron Wasp	0.1329	0.1329	0.1329	0.1329
Acunetix	0.1279	0.1279	0.1279	0.1329	Acunetix	0.1429	0.1279	0.1279	0.1529
Wapiti	0.1529	0.1479	0.1479	0.1479	Wapiti	0.1479	0.1479	0.1479	0.1429
OZ Plugins	0.1479	0.1529	0.1529	0.1429	OZ Plugins	0.1529	0.1529	0.1529	0.1479
Vulnerability	Remote File Inclusion				Vulnerability	Cross-Site Request Forgery			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1479	0.1479	0.1479	0.1529	OWASP ZAP	0.1479	0.1479	0.1479	0.1479
Burp Suite	0.1529	0.1529	0.1529	0.1479	Burp Suite	0.1429	0.1429	0.1429	0.1379
Iron Wasp	0.1329	0.1329	0.1329	0.1404	Iron Wasp	0.1279	0.1279	0.1279	0.1279
Acunetix	0.1429	0.1429	0.1429	0.1279	Acunetix	0.1329	0.1329	0.1329	0.1429
Wapiti	0.1329	0.1329	0.1329	0.1329	Wapiti	0.1379	0.1379	0.1379	0.1329
OZ Plugins	0.1329	0.1329	0.1329	0.1404	OZ Plugins	0.1529	0.1529	0.1529	0.1529
Vulnerability	Transmission of Information in Cleartext				Vulnerability	Untrusted/Invalid TLS certificate			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1304	0.1304	0.1304	0.1304	OWASP ZAP	0.1354	0.1354	0.1354	0.1354
Burp Suite	0.1529	0.1529	0.1529	0.1454	Burp Suite	0.1504	0.1504	0.1504	0.1504
Iron Wasp	0.1479	0.1479	0.1479	0.1454	Iron Wasp	0.1354	0.1354	0.1354	0.1354
Acunetix	0.1404	0.1404	0.1404	0.1454	Acunetix	0.1354	0.1354	0.1354	0.1354
Wapiti	0.1404	0.1404	0.1404	0.1454	Wapiti	0.1504	0.1504	0.1504	0.1504
OZ Plugins	0.1304	0.1304	0.1304	0.1304	OZ Plugins	0.1354	0.1354	0.1354	0.1354
Vulnerability	Command Injection				Vulnerability	SQL Injection			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1479	0.1479	0.1479	0.1529	OWASP ZAP	0.1429	0.1429	0.1429	0.1379
Burp Suite	0.1379	0.1329	0.1329	0.1429	Burp Suite	0.1279	0.1279	0.1279	0.1279
Iron Wasp	0.1429	0.1429	0.1429	0.1479	Iron Wasp	0.1329	0.1329	0.1329	0.1479
Acunetix	0.1279	0.1279	0.1279	0.1279	Acunetix	0.1379	0.1379	0.1379	0.1529
Wapiti	0.1529	0.1479	0.1479	0.1479	Wapiti	0.1479	0.1479	0.1479	0.1429
OZ Plugins	0.1529	0.1529	0.1529	0.1379	OZ Plugins	0.1529	0.1529	0.1529	0.1329
Vulnerability	LDAP Injection				Vulnerability	Cross-Site Scripting			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1354	0.1354	0.1354	0.1379	OWASP ZAP	0.1529	0.1529	0.1479	0.1379
Burp Suite	0.1354	0.1354	0.1354	0.1279	Burp Suite	0.1429	0.1379	0.1329	0.1279
Iron Wasp	0.1354	0.1354	0.1354	0.1379	Iron Wasp	0.1329	0.1329	0.1379	0.1529
Acunetix	0.1529	0.1529	0.1529	0.1529	Acunetix	0.1379	0.1429	0.1429	0.1479
Wapiti	0.1354	0.1354	0.1354	0.1379	Wapiti	0.1279	0.1279	0.1279	0.1329
OZ Plugins	0.1479	0.1479	0.1479	0.1479	OZ Plugins	0.1479	0.1479	0.1529	0.1429
Vulnerability	XPath Injection				Vulnerability	HTTP Response Splitting			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1304	0.1304	0.1304	0.1304	OWASP ZAP	0.1404	0.1404	0.1404	0.1404
Burp Suite	0.1379	0.1379	0.1379	0.1429	Burp Suite	0.1404	0.1404	0.1404	0.1404
Iron Wasp	0.1429	0.1429	0.1429	0.1529	Iron Wasp	0.1404	0.1404	0.1404	0.1404
Acunetix	0.1304	0.1304	0.1304	0.1304	Acunetix	0.1404	0.1404	0.1404	0.1404
Wapiti	0.1479	0.1479	0.1479	0.1479	Wapiti	0.1404	0.1404	0.1404	0.1404
OZ Plugins	0.1529	0.1529	0.1529	0.1379	OZ Plugins	0.1404	0.1404	0.1404	0.1404
Vulnerability	Exposed Improper Error Handling				Vulnerability	Bad Security Design of Form Fields			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1429	0.1429	0.1429	0.1279	OWASP ZAP	0.1379	0.1379	0.1379	0.1404
Burp Suite	0.1304	0.1304	0.1304	0.1504	Burp Suite	0.1379	0.1379	0.1379	0.1404
Iron Wasp	0.1304	0.1304	0.1304	0.1504	Iron Wasp	0.1529	0.1529	0.1529	0.1529
Acunetix	0.1529	0.1529	0.1529	0.1379	Acunetix	0.1379	0.1379	0.1379	0.1279
Wapiti	0.1379	0.1379	0.1379	0.1429	Wapiti	0.1379	0.1379	0.1379	0.1404
OZ Plugins	0.1479	0.1479	0.1479	0.1329	OZ Plugins	0.1379	0.1379	0.1379	0.1404
Vulnerability	Method Tampering				Vulnerability	XML External Entities			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1479	0.1479	0.1479	0.1379	OWASP ZAP	0.1379	0.1379	0.1379	0.1379
Burp Suite	0.1379	0.1379	0.1379	0.1279	Burp Suite	0.1379	0.1379	0.1379	0.1379
Iron Wasp	0.1304	0.1304	0.1304	0.1304	Iron Wasp	0.1379	0.1379	0.1379	0.1379
Acunetix	0.1304	0.1304	0.1304	0.1304	Acunetix	0.1379	0.1379	0.1379	0.1379
Wapiti	0.1379	0.1379	0.1379	0.1479	Wapiti	0.1529	0.1529	0.1529	0.1529
OZ Plugins	0.1529	0.1529	0.1529	0.1529	OZ Plugins	0.1379	0.1379	0.1379	0.1379
Vulnerability	Bad Programming of Cookies				Vulnerability	Ins. Use of Hard Coded Constants			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1304	0.1304	0.1304	0.1304	OWASP ZAP	0.1404	0.1404	0.1404	0.1404

Burp Suite	0.1379	0.1379	0.1379	0.1429	Burp Suite	0.1404	0.1404	0.1404	0.1404
Iron Wasp	0.1429	0.1429	0.1429	0.1529	Iron Wasp	0.1404	0.1404	0.1404	0.1404
Acunetix	0.1304	0.1304	0.1304	0.1304	Acunetix	0.1404	0.1404	0.1404	0.1404
Wapiti	0.1479	0.1479	0.1479	0.1479	Wapiti	0.1404	0.1404	0.1404	0.1404
OZ Plugins	0.1529	0.1529	0.1529	0.1379	OZ Plugins	0.1404	0.1404	0.1404	0.1404
Vulnerability	Insecure/Vulnerable Third-Party Software				Vulnerability	Bypassing Authentication			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1529	0.1529	0.1529	0.1379	OWASP ZAP	0.1454	0.1454	0.1454	0.1454
Burp Suite	0.1404	0.1404	0.1404	0.1504	Burp Suite	0.1454	0.1454	0.1454	0.1454
Iron Wasp	0.1329	0.1329	0.1329	0.1379	Iron Wasp	0.1329	0.1329	0.1329	0.1329
Acunetix	0.1404	0.1404	0.1404	0.1504	Acunetix	0.1329	0.1329	0.1329	0.1329
Wapiti	0.1479	0.1479	0.1479	0.1429	Wapiti	0.1329	0.1329	0.1329	0.1329
OZ Plugins	0.1329	0.1329	0.1329	0.1404	OZ Plugins	0.1529	0.1529	0.1529	0.1529
Vulnerability	Brute Force Attacks				Vulnerability	Session Fixation			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1479	0.1479	0.1479	0.1379	OWASP ZAP	0.1379	0.1379	0.1379	0.1379
Burp Suite	0.1379	0.1379	0.1379	0.1279	Burp Suite	0.1379	0.1379	0.1379	0.1379
Iron Wasp	0.1304	0.1304	0.1304	0.1504	Iron Wasp	0.1529	0.1529	0.1529	0.1529
Acunetix	0.1304	0.1304	0.1304	0.1304	Acunetix	0.1379	0.1379	0.1379	0.1379
Wapiti	0.1479	0.1529	0.1479	0.1529	Wapiti	0.1379	0.1379	0.1379	0.1379
OZ Plugins	0.1529	0.1529	0.1529	0.1529	OZ Plugins	0.1379	0.1379	0.1379	0.1379
Vulnerability	Insecure Scope of Cookies				Vulnerability	Insecure Deserialization			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1304	0.1304	0.1304	0.1304	OWASP ZAP	0.1404	0.1404	0.1404	0.1404
Burp Suite	0.1379	0.1379	0.1379	0.1429	Burp Suite	0.1404	0.1404	0.1404	0.1404
Iron Wasp	0.1429	0.1429	0.1429	0.1529	Iron Wasp	0.1404	0.1404	0.1404	0.1404
Acunetix	0.1304	0.1304	0.1304	0.1304	Acunetix	0.1404	0.1404	0.1404	0.1404
Wapiti	0.1479	0.1479	0.1479	0.1479	Wapiti	0.1404	0.1404	0.1404	0.1404
OZ Plugins	0.1529	0.1529	0.1529	0.1379	OZ Plugins	0.1404	0.1404	0.1404	0.1404
Vulnerability	Improper Output Neutralization for Logs				Vulnerability	Server-Side Request Forgery			
Tool	1	2	3	4	Tool	1	2	3	4
OWASP ZAP	0.1479	0.1479	0.1479	0.1279	OWASP ZAP	0.1329	0.1429	0.1379	0.1329
Burp Suite	0.1329	0.1329	0.1329	0.1429	Burp Suite	0.1479	0.1479	0.1479	0.1379
Iron Wasp	0.1404	0.1404	0.1404	0.1504	Iron Wasp	0.1429	0.1379	0.1429	0.1529
Acunetix	0.1404	0.1404	0.1404	0.1504	Acunetix	0.1529	0.1529	0.1529	0.1429
Wapiti	0.1279	0.1279	0.1279	0.1379	Wapiti	0.1379	0.1329	0.1329	0.1479
OZ Plugins	0.1529	0.1529	0.1529	0.1329	OZ Plugins	0.1279	0.1279	0.1279	0.1279
1 - Business Critical | 2 - Heightened Critical | 3 - Best Effort | 4 - Minimum Effort									

Table 4.1: 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
Bypassing Authorization													
A, E	65	64	10	25	50.39%	86.67%	A, F	69	60	12	23	31.88%	53.49%
B, E	65	64	10	25	50.39%	86.67%	B, F	69	60	12	23	31.88%	53.49%
C, E	65	64	10	25	50.39%	86.67%	C, F	69	60	12	23	31.88%	53.49%
D, E	65	64	10	25	50.39%	86.67%	D, F	69	60	12	23	31.88%	53.49%
E, F	65	64	10	25	50.39%	86.67%	E, F	69	60	12	23	31.88%	53.49%
A, F	69	60	12	23	53.49%	85.19%	A, E	65	64	10	25	30.69%	50.39%
B, F	69	60	12	23	53.49%	85.19%	B, E	65	64	10	25	30.69%	50.39%
C, F	69	60	12	23	53.49%	85.19%	C, E	65	64	10	25	30.69%	50.39%
D, F	69	60	12	23	53.49%	85.19%	D, E	65	64	10	25	30.69%	50.39%
A, B	44	85	1	34	34.11%	97.78%	A, B	44	85	1	34	22.38%	34.11%
A, C	44	85	1	34	34.11%	97.78%	A, C	44	85	1	34	22.38%	34.11%
A, D	44	85	1	34	34.11%	97.78%	A, D	44	85	1	34	22.38%	34.11%
B, C	31	98	0	35	24.03%	100.0%	B, C	31	98	0	35	14.9%	24.03%
B, D	31	98	0	35	24.03%	100.0%	B, D	31	98	0	35	14.9%	24.03%
C, D	10	119	1	34	7.75%	90.91%	C, D	10	119	1	34	4.07%	7.75%
Path Traversal													
A, F	98	56	95	63	63.64%	50.78%	A, F	98	56	95	63	32.93%	63.64%
B, F	98	56	95	63	63.64%	50.78%	B, F	98	56	95	63	32.93%	63.64%
C, F	98	56	95	63	63.64%	50.78%	C, F	98	56	95	63	32.93%	63.64%
D, F	98	56	95	63	63.64%	50.78%	D, F	98	56	95	63	32.93%	63.64%
E, F	98	56	95	63	63.64%	50.78%	E, F	98	56	95	63	32.93%	63.64%
A, E	34	120	28	130	22.08%	54.84%	A, E	34	120	28	130	11.52%	22.08%
B, E	34	120	28	130	22.08%	54.84%	B, E	34	120	28	130	11.52%	22.08%
C, E	34	120	28	130	22.08%	54.84%	C, E	34	120	28	130	11.52%	22.08%
D, E	34	120	28	130	22.08%	54.84%	D, E	34	120	28	130	11.52%	22.08%
A, B	5	149	0	158	3.25%	100.0%	A, B	6	148	2	156	2.0%	3.9%
B, C	5	149	0	158	3.25%	100.0%	A, C	6	148	2	156	2.0%	3.9%
A, C	3	151	0	158	1.95%	100.0%	A, D	6	148	2	156	2.0%	3.9%
A, D	2	152	0	158	1.3%	100.0%	B, C	5	149	0	158	1.68%	3.25%
B, D	2	152	0	158	1.3%	100.0%	B, D	5	149	0	158	1.68%	3.25%
C, D	2	152	0	158	1.3%	100.0%	C, D	3	151	0	158	0.99%	1.95%
Remote File Inclusion													
A, B	59	49	2	4	54.63%	96.72%	A, B	59	49	2	4	33.13%	54.63%
B, C	59	49	2	4	54.63%	96.72%	B, C	59	49	2	4	33.13%	54.63%
B, D	59	49	2	4	54.63%	96.72%	B, D	59	49	2	4	33.13%	54.63%
B, E	59	49	2	4	54.63%	96.72%	B, E	59	49	2	4	33.13%	54.63%
B, F	59	49	2	4	54.63%	96.72%	B, F	59	49	2	4	33.13%	54.63%
A, C	44	64	0	6	40.74%	100.0%	A, C	44	64	0	6	28.67%	40.74%
A, D	44	64	0	6	40.74%	100.0%	A, D	44	64	0	6	28.67%	40.74%
A, E	44	64	0	6	40.74%	100.0%	A, E	44	64	0	6	28.67%	40.74%
A, F	44	64	0	6	40.74%	100.0%	A, F	44	64	0	6	28.67%	40.74%
C, D	36	72	1	5	33.33%	97.3%	C, D	36	72	1	5	19.44%	33.33%
D, E	36	72	1	5	33.33%	97.3%	D, E	36	72	1	5	19.44%	33.33%
D, F	36	72	1	5	33.33%	97.3%	D, F	36	72	1	5	19.44%	33.33%
C, E	0	108	0	6	0.0%	0.0%	C, E	0	108	0	6	0.0%	0.0%
C, F	0	108	0	6	0.0%	0.0%	C, F	0	108	0	6	0.0%	0.0%
E, F	0	108	0	6	0.0%	0.0%	E, F	0	108	0	6	0.0%	0.0%
Cross-Site Request Forgery													
A, F	288	18	142	78	94.12%	66.98%	A, F	288	18	142	78	60.98%	94.12%
B, F	288	18	142	78	94.12%	66.98%	B, F	288	18	142	78	60.98%	94.12%
C, F	288	18	142	78	94.12%	66.98%	C, F	288	18	142	78	60.98%	94.12%
D, F	288	18	142	78	94.12%	66.98%	D, F	288	18	142	78	60.98%	94.12%
E, F	288	18	142	78	94.12%	66.98%	E, F	288	18	142	78	60.98%	94.12%
A, B	260	46	119	101	84.97%	68.6%	A, B	260	46	119	101	55.6%	84.97%
A, C	260	46	119	101	84.97%	68.6%	A, C	260	46	119	101	55.6%	84.97%
A, D	260	46	119	101	84.97%	68.6%	A, D	260	46	119	101	55.6%	84.97%
A, E	260	46	119	101	84.97%	68.6%	A, E	260	46	119	101	55.6%	84.97%
B, D	159	147	55	165	51.96%	74.3%	B, C	159	147	55	165	32.98%	51.96%
B, C	159	147	55	165	51.96%	74.3%	B, D	159	147	55	165	32.98%	51.96%
B, E	159	147	55	165	51.96%	74.3%	B, E	159	147	55	165	32.98%	51.96%
C, E	127	179	53	167	41.5%	70.56%	C, E	127	179	53	167	24.36%	41.5%
D, E	127	179	53	167	41.5%	70.56%	D, E	127	179	53	167	24.36%	41.5%
C, D	48	258	9	211	15.69%	84.21%	C, D	48	258	9	211	8.75%	15.69%

A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins

Table 4.2: 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
Bypassing Authorization													
A, F	69	60	12	23	65.71%	53.49%	B, D	1	128	0	35	60.74%	100.0%
B, F	69	60	12	23	65.71%	53.49%	A, B	44	85	1	34	63.17%	97.78%
C, F	69	60	12	23	65.71%	53.49%	A, C	44	85	1	34	63.17%	97.78%
D, F	69	60	12	23	65.71%	53.49%	A, D	44	85	1	34	63.17%	97.78%
E, F	69	60	12	23	65.71%	53.49%	A, E	44	85	1	34	63.17%	97.78%
A, E	65	64	10	25	63.73%	50.39%	A, F	44	85	1	34	63.17%	97.78%
B, E	65	64	10	25	63.73%	50.39%	B, C	10	119	1	34	56.57%	90.91%
C, E	65	64	10	25	63.73%	50.39%	C, D	10	119	1	34	56.57%	90.91%
D, E	65	64	10	25	63.73%	50.39%	B, E	65	64	10	25	57.38%	86.67%
A, B	44	85	1	34	50.57%	34.11%	C, E	65	64	10	25	57.38%	86.67%
A, C	44	85	1	34	50.57%	34.11%	D, E	65	64	10	25	57.38%	86.67%
A, D	44	85	1	34	50.57%	34.11%	E, F	65	64	10	25	57.38%	86.67%
B, C	31	98	0	35	38.75%	24.03%	B, F	69	60	12	23	56.45%	85.19%
B, D	31	98	0	35	38.75%	24.03%	C, F	69	60	12	23	56.45%	85.19%
C, D	10	119	1	34	14.29%	7.75%	D, F	69	60	12	23	56.45%	85.19%
Path Traversal													
A, F	98	56	95	63	56.48%	63.64%	A, B	5	149	0	158	75.73%	100.0%
B, F	98	56	95	63	56.48%	63.64%	B, C	5	149	0	158	75.73%	100.0%
C, F	98	56	95	63	56.48%	63.64%	A, C	3	151	0	158	75.57%	100.0%
D, F	98	56	95	63	56.48%	63.64%	A, D	2	152	0	158	75.48%	100.0%
E, F	98	56	95	63	56.48%	63.64%	B, D	2	152	0	158	75.48%	100.0%
A, E	34	120	28	130	31.48%	22.08%	C, D	2	152	0	158	75.48%	100.0%
B, E	34	120	28	130	31.48%	22.08%	D, E	2	152	0	158	75.48%	100.0%
C, E	34	120	28	130	31.48%	22.08%	D, F	2	152	0	158	75.48%	100.0%
D, E	34	120	28	130	31.48%	22.08%	A, E	34	120	28	130	53.42%	54.84%
A, B	6	148	2	156	7.41%	3.9%	B, E	34	120	28	130	53.42%	54.84%
A, C	6	148	2	156	7.41%	3.9%	C, E	34	120	28	130	53.42%	54.84%
A, D	6	148	2	156	7.41%	3.9%	A, F	98	56	95	63	51.86%	50.78%
B, C	5	149	0	158	6.29%	3.25%	B, F	98	56	95	63	51.86%	50.78%
B, D	5	149	0	158	6.29%	3.25%	C, F	98	56	95	63	51.86%	50.78%
C, D	3	151	0	158	3.82%	1.95%	E, F	98	56	95	63	51.86%	50.78%
Remote File Inclusion													
A, B	59	49	2	4	69.82%	54.63%	A, B	44	64	0	6	54.29%	100.0%
B, C	59	49	2	4	69.82%	54.63%	A, C	44	64	0	6	54.29%	100.0%
B, D	59	49	2	4	69.82%	54.63%	A, D	44	64	0	6	54.29%	100.0%
B, E	59	49	2	4	69.82%	54.63%	A, E	44	64	0	6	54.29%	100.0%
B, F	59	49	2	4	69.82%	54.63%	A, F	44	64	0	6	54.29%	100.0%
A, C	44	64	0	6	57.89%	40.74%	B, C	59	49	2	4	52.13%	96.72%
A, D	44	64	0	6	57.89%	40.74%	B, D	59	49	2	4	52.13%	96.72%
A, E	44	64	0	6	57.89%	40.74%	B, E	59	49	2	4	52.13%	96.72%
A, F	44	64	0	6	57.89%	40.74%	B, F	59	49	2	4	52.13%	96.72%
C, D	36	72	1	5	49.66%	33.33%	C, D	0	108	0	6	2.63%	0.0%
D, E	36	72	1	5	49.66%	33.33%	C, E	0	108	0	6	2.63%	0.0%
D, F	36	72	1	5	49.66%	33.33%	C, F	0	108	0	6	2.63%	0.0%
C, E	0	108	0	6	0.0%	0.0%	D, E	0	108	0	6	2.63%	0.0%
C, F	0	108	0	6	0.0%	0.0%	D, F	0	108	0	6	2.63%	0.0%
E, F	0	108	0	6	0.0%	0.0%	E, F	0	108	0	6	2.63%	0.0%
Cross-Site Request Forgery													
A, F	288	18	142	78	78.26%	94.12%	A, F	288	18	142	78	74.11%	66.98%
B, F	288	18	142	78	78.26%	94.12%	B, F	288	18	142	78	74.11%	66.98%
C, F	288	18	142	78	78.26%	94.12%	C, F	288	18	142	78	74.11%	66.98%
D, F	288	18	142	78	78.26%	94.12%	D, F	288	18	142	78	74.11%	66.98%
E, F	288	18	142	78	78.26%	94.12%	E, F	288	18	142	78	74.11%	66.98%
A, B	260	46	119	101	75.91%	84.97%	A, B	260	46	119	101	68.65%	68.6%
A, C	260	46	119	101	75.91%	84.97%	A, C	260	46	119	101	68.65%	68.6%
A, D	260	46	119	101	75.91%	84.97%	A, D	260	46	119	101	68.65%	68.6%
A, E	260	46	119	101	75.91%	84.97%	A, E	260	46	119	101	68.65%	68.6%

B, C	159	147	55	165	61.15%	51.96%	B, D	48	258	9	211	64.6%	84.21%
B, D	159	147	55	165	61.15%	51.96%	C, D	48	258	9	211	64.6%	84.21%
B, E	159	147	55	165	61.15%	51.96%	D, E	48	258	9	211	64.6%	84.21%
C, E	127	179	53	167	52.26%	41.5%	B, C	159	147	55	165	63.59%	74.3%
D, E	127	179	53	167	52.26%	41.5%	B, E	159	147	55	165	63.59%	74.3%
C, D	48	258	9	211	26.45%	15.69%	C, E	127	179	53	167	59.41%	70.56%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.3: 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
Transmission of Information in Cleartext													
D, E	9	0	0	0	100.0%	100.0%	D, E	9	0	0	0	100.0%	100.0%
A, B	8	1	0	0	88.89%	100.0%	A, B	8	1	0	0	88.89%	88.89%
B, C	8	1	0	0	88.89%	100.0%	B, C	8	1	0	0	88.89%	88.89%
B, D	8	1	0	0	88.89%	100.0%	B, D	8	1	0	0	88.89%	88.89%
B, E	8	1	0	0	88.89%	100.0%	B, E	8	1	0	0	88.89%	88.89%
B, F	8	1	0	0	88.89%	100.0%	B, F	8	1	0	0	88.89%	88.89%
A, C	7	2	0	0	77.78%	100.0%	A, C	7	2	0	0	77.78%	77.78%
C, D	7	2	0	0	77.78%	100.0%	C, D	7	2	0	0	77.78%	77.78%
C, E	7	2	0	0	77.78%	100.0%	C, E	7	2	0	0	77.78%	77.78%
C, F	7	2	0	0	77.78%	100.0%	C, F	7	2	0	0	77.78%	77.78%
A, D	6	3	0	0	66.67%	100.0%	A, D	6	3	0	0	66.67%	66.67%
A, E	6	3	0	0	66.67%	100.0%	A, E	6	3	0	0	66.67%	66.67%
D, F	6	3	0	0	66.67%	100.0%	D, F	6	3	0	0	66.67%	66.67%
E, F	6	3	0	0	66.67%	100.0%	E, F	6	3	0	0	66.67%	66.67%
A, F	0	9	0	0	0.0%	0.0%	A, F	0	9	0	0	0.0%	0.0%
Untrusted/Invalid TLS certificate													
A, B	1	1	0	7	50.0%	100.0%	A, B	1	1	0	7	37.5%	50.0%
A, E	1	1	0	7	50.0%	100.0%	A, E	1	1	0	7	37.5%	50.0%
B, C	1	1	0	7	50.0%	100.0%	B, C	1	1	0	7	37.5%	50.0%
B, D	1	1	0	7	50.0%	100.0%	B, D	1	1	0	7	37.5%	50.0%
B, E	1	1	0	7	50.0%	100.0%	B, E	1	1	0	7	37.5%	50.0%
B, F	1	1	0	7	50.0%	100.0%	B, F	1	1	0	7	37.5%	50.0%
C, E	1	1	0	7	50.0%	100.0%	C, E	1	1	0	7	37.5%	50.0%
D, E	1	1	0	7	50.0%	100.0%	D, E	1	1	0	7	37.5%	50.0%
E, F	1	1	0	7	50.0%	100.0%	E, F	1	1	0	7	37.5%	50.0%
A, C	0	2	0	7	0.0%	0.0%	A, C	0	2	0	7	0.0%	0.0%
A, D	0	2	0	7	0.0%	0.0%	A, D	0	2	0	7	0.0%	0.0%
A, F	0	2	0	7	0.0%	0.0%	A, F	0	2	0	7	0.0%	0.0%
C, D	0	2	0	7	0.0%	0.0%	C, D	0	2	0	7	0.0%	0.0%
C, F	0	2	0	7	0.0%	0.0%	C, F	0	2	0	7	0.0%	0.0%
D, F	0	2	0	7	0.0%	0.0%	D, F	0	2	0	7	0.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.4: 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
Transmission of Information in Cleartext													
D, E	9	0	0	0	100.0%	100.0%	D, E	9	0	0	0	100.0%	100.0%
A, B	8	1	0	0	94.12%	88.89%	A, B	8	1	0	0	50.0%	100.0%
B, C	8	1	0	0	94.12%	88.89%	A, C	7	2	0	0	50.0%	100.0%
B, D	8	1	0	0	94.12%	88.89%	A, D	6	3	0	0	50.0%	100.0%
B, E	8	1	0	0	94.12%	88.89%	A, E	6	3	0	0	50.0%	100.0%
B, F	8	1	0	0	94.12%	88.89%	B, E	8	1	0	0	50.0%	100.0%

A, C	7	2	0	0	87.5%	77.78%	B, F	8	1	0	0	50.0%	100.0%
C, D	7	2	0	0	87.5%	77.78%	C, D	7	2	0	0	50.0%	100.0%
C, E	7	2	0	0	87.5%	77.78%	C, F	7	2	0	0	50.0%	100.0%
C, F	7	2	0	0	87.5%	77.78%	D, F	6	3	0	0	50.0%	100.0%
A, D	6	3	0	0	80.0%	66.67%	E, F	6	3	0	0	50.0%	100.0%
A, E	6	3	0	0	80.0%	66.67%	B, C	9	0	0	0	50.0%	100.0%
D, F	6	3	0	0	80.0%	66.67%	B, D	9	0	0	0	50.0%	100.0%
E, F	6	3	0	0	80.0%	66.67%	C, E	9	0	0	0	50.0%	100.0%
A, F	0	9	0	0	0.0%	0.0%	A, F	0	9	0	0	0.0%	0.0%
Untrusted/Invalid TLS certificate													
A, B	1	1	0	7	66.67%	50.0%	A, B	1	1	0	7	93.75%	100.0%
A, E	1	1	0	7	66.67%	50.0%	A, E	1	1	0	7	93.75%	100.0%
B, C	1	1	0	7	66.67%	50.0%	B, C	1	1	0	7	93.75%	100.0%
B, D	1	1	0	7	66.67%	50.0%	B, D	1	1	0	7	93.75%	100.0%
B, E	1	1	0	7	66.67%	50.0%	B, E	1	1	0	7	93.75%	100.0%
B, F	1	1	0	7	66.67%	50.0%	B, F	1	1	0	7	93.75%	100.0%
C, E	1	1	0	7	66.67%	50.0%	C, E	1	1	0	7	93.75%	100.0%
D, E	1	1	0	7	66.67%	50.0%	D, E	1	1	0	7	93.75%	100.0%
E, F	1	1	0	7	66.67%	50.0%	E, F	1	1	0	7	93.75%	100.0%
A, C	0	2	0	7	0.0%	0.0%	A, C	0	2	0	7	38.89%	0.0%
A, D	0	2	0	7	0.0%	0.0%	A, D	0	2	0	7	38.89%	0.0%
A, F	0	2	0	7	0.0%	0.0%	A, F	0	2	0	7	38.89%	0.0%
C, D	0	2	0	7	0.0%	0.0%	C, D	0	2	0	7	38.89%	0.0%
C, F	0	2	0	7	0.0%	0.0%	C, F	0	2	0	7	38.89%	0.0%
D, F	0	2	0	7	0.0%	0.0%	D, F	0	2	0	7	38.89%	0.0%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.5: 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
Command Injection													
A, F	159	103	80	45	60.69%	66.53%	A, F	159	103	80	45	29.34%	60.69%
B, F	159	103	80	45	60.69%	66.53%	B, F	159	103	80	45	29.34%	60.69%
C, F	159	103	80	45	60.69%	66.53%	C, F	159	103	80	45	29.34%	60.69%
D, F	159	103	80	45	60.69%	66.53%	D, F	159	103	80	45	29.34%	60.69%
E, F	159	103	80	45	60.69%	66.53%	E, F	159	103	80	45	29.34%	60.69%
A, B	99	163	0	125	37.79%	100.0%	A, B	99	163	0	125	26.03%	37.79%
A, C	99	163	0	125	37.79%	100.0%	A, C	99	163	0	125	26.03%	37.79%
A, D	99	163	0	125	37.79%	100.0%	A, D	99	163	0	125	26.03%	37.79%
A, E	99	163	0	125	37.79%	100.0%	A, E	99	163	0	125	26.03%	37.79%
B, C	22	240	0	125	8.4%	100.0%	B, C	22	240	0	125	4.55%	8.4%
C, D	22	240	0	125	8.4%	100.0%	C, D	22	240	0	125	4.55%	8.4%
C, E	22	240	0	125	8.4%	100.0%	C, E	22	240	0	125	4.55%	8.4%
B, D	19	243	0	125	7.25%	100.0%	B, E	21	241	19	106	3.72%	8.02%
B, E	19	243	0	125	7.25%	100.0%	D, E	21	241	19	106	3.72%	8.02%
D, E	21	241	19	106	8.02%	52.5%	B, D	19	243	0	125	3.89%	7.25%
SQL Injection													
A, F	241	258	157	199	48.3%	60.55%	A, F	241	258	157	199	25.16%	48.3%
B, F	241	258	157	199	48.3%	60.55%	B, F	241	258	157	199	25.16%	48.3%
C, F	241	258	157	199	48.3%	60.55%	C, F	241	258	157	199	25.16%	48.3%
D, F	241	258	157	199	48.3%	60.55%	D, F	241	258	157	199	25.16%	48.3%
E, F	241	258	157	199	48.3%	60.55%	E, F	241	258	157	199	25.16%	48.3%
A, E	180	319	54	302	36.07%	76.92%	A, E	180	319	54	302	21.81%	36.07%
B, E	180	319	54	302	36.07%	76.92%	B, E	180	319	54	302	21.81%	36.07%
C, E	180	319	54	302	36.07%	76.92%	C, E	180	319	54	302	21.81%	36.07%
D, E	180	319	54	302	36.07%	76.92%	D, E	180	319	54	302	21.81%	36.07%
A, B	170	329	9	347	34.07%	94.97%	A, B	170	329	9	347	22.41%	34.07%
A, C	170	329	9	347	34.07%	94.97%	A, C	170	329	9	347	22.41%	34.07%
A, D	170	329	9	347	34.07%	94.97%	A, D	170	329	9	347	22.41%	34.07%
B, D	123	376	0	356	24.65%	100.0%	B, D	123	376	0	356	15.36%	24.65%
C, D	123	376	0	356	24.65%	100.0%	C, D	123	376	0	356	15.36%	24.65%

B, C	74	425	5	351	14.83%	93.67%	B, C	74	425	5	351	8.41%	14.83%
LDAP Injection													
A, D	17	12	5	27	58.62%	77.27%	A, D	17	12	5	27	41.91%	58.62%
B, D	17	12	5	27	58.62%	77.27%	B, D	17	12	5	27	41.91%	58.62%
C, D	17	12	5	27	58.62%	77.27%	C, D	17	12	5	27	41.91%	58.62%
D, E	17	12	5	27	58.62%	77.27%	D, E	17	12	5	27	41.91%	58.62%
D, F	17	12	5	27	58.62%	77.27%	D, F	17	12	5	27	41.91%	58.62%
A, F	3	26	3	29	10.34%	50.0%	A, F	3	26	3	29	5.22%	10.34%
B, F	3	26	3	29	10.34%	50.0%	B, F	3	26	3	29	5.22%	10.34%
C, F	3	26	3	29	10.34%	50.0%	C, F	3	26	3	29	5.22%	10.34%
E, F	3	26	3	29	10.34%	50.0%	E, F	3	26	3	29	5.22%	10.34%
A, B	0	29	0	32	0.0%	0.0%	A, B	0	29	0	32	0.0%	0.0%
A, C	0	29	0	32	0.0%	0.0%	A, C	0	29	0	32	0.0%	0.0%
A, E	0	29	0	32	0.0%	0.0%	A, E	0	29	0	32	0.0%	0.0%
B, C	0	29	0	32	0.0%	0.0%	B, C	0	29	0	32	0.0%	0.0%
B, E	0	29	0	32	0.0%	0.0%	B, E	0	29	0	32	0.0%	0.0%
C, E	0	29	0	32	0.0%	0.0%	C, E	0	29	0	32	0.0%	0.0%
Cross-Site Scripting													
A, B	301	147	179	93	67.19%	62.71%	A, B	301	147	179	93	34.06%	67.19%
A, C	301	147	179	93	67.19%	62.71%	A, C	301	147	179	93	34.06%	67.19%
A, D	301	147	179	93	67.19%	62.71%	A, D	301	147	179	93	34.06%	67.19%
A, E	301	147	179	93	67.19%	62.71%	A, E	301	147	179	93	34.06%	67.19%
A, F	301	147	179	93	67.19%	62.71%	A, F	301	147	179	93	34.06%	67.19%
B, F	269	179	121	151	60.04%	68.97%	B, F	269	179	121	151	34.69%	60.04%
C, F	269	179	121	151	60.04%	68.97%	C, F	269	179	121	151	34.69%	60.04%
D, F	269	179	121	151	60.04%	68.97%	D, F	269	179	121	151	34.69%	60.04%
E, F	269	179	121	151	60.04%	68.97%	E, F	269	179	121	151	34.69%	60.04%
B, C	194	254	44	228	43.3%	81.51%	B, C	194	254	44	228	27.53%	43.3%
B, D	194	254	44	228	43.3%	81.51%	B, E	194	254	44	228	27.53%	43.3%
B, E	194	254	44	228	43.3%	81.51%	B, D	177	271	0	272	27.56%	39.51%
C, D	177	271	0	272	39.51%	100.0%	C, D	177	271	0	272	27.56%	39.51%
D, E	177	271	0	272	39.51%	100.0%	D, E	177	271	0	272	27.56%	39.51%
C, E	121	327	2	270	27.01%	98.37%	C, E	121	327	2	270	17.05%	27.01%
XPath Injection													
A, F	7	15	13	8	31.82%	35.0%	A, F	7	15	13	8	11.12%	31.82%
B, F	7	15	13	8	31.82%	35.0%	B, F	7	15	13	8	11.12%	31.82%
C, F	7	15	13	8	31.82%	35.0%	C, F	7	15	13	8	11.12%	31.82%
D, F	7	15	13	8	31.82%	35.0%	D, F	7	15	13	8	11.12%	31.82%
E, F	7	15	13	8	31.82%	35.0%	E, F	7	15	13	8	11.12%	31.82%
A, E	4	18	3	18	18.18%	57.14%	A, E	4	18	3	18	9.45%	18.18%
B, E	4	18	3	18	18.18%	57.14%	B, E	4	18	3	18	9.45%	18.18%
C, E	4	18	3	18	18.18%	57.14%	C, E	4	18	3	18	9.45%	18.18%
D, E	4	18	3	18	18.18%	57.14%	D, E	4	18	3	18	9.45%	18.18%
A, C	2	20	0	21	9.09%	100.0%	A, C	2	20	0	21	4.96%	9.09%
B, C	2	20	0	21	9.09%	100.0%	B, C	2	20	0	21	4.96%	9.09%
C, D	2	20	0	21	9.09%	100.0%	C, D	2	20	0	21	4.96%	9.09%
A, B	1	21	0	21	4.55%	100.0%	A, B	1	21	0	21	2.38%	4.55%
B, D	1	21	0	21	4.55%	100.0%	B, D	1	21	0	21	2.38%	4.55%
A, D	0	22	0	21	0.0%	0.0%	A, D	0	22	0	21	0.0%	0.0%
HTTP Response Splitting													
A, B	0	3	0	2	0.0%	0.0%	A, B	0	3	0	2	0.0%	0.0%
A, C	0	3	0	2	0.0%	0.0%	A, C	0	3	0	2	0.0%	0.0%
A, D	0	3	0	2	0.0%	0.0%	A, D	0	3	0	2	0.0%	0.0%
A, E	0	3	0	2	0.0%	0.0%	A, E	0	3	0	2	0.0%	0.0%
A, F	0	3	0	2	0.0%	0.0%	A, F	0	3	0	2	0.0%	0.0%
B, C	0	3	0	2	0.0%	0.0%	B, C	0	3	0	2	0.0%	0.0%
B, D	0	3	0	2	0.0%	0.0%	B, D	0	3	0	2	0.0%	0.0%
B, E	0	3	0	2	0.0%	0.0%	B, E	0	3	0	2	0.0%	0.0%
B, F	0	3	0	2	0.0%	0.0%	B, F	0	3	0	2	0.0%	0.0%
C, D	0	3	0	2	0.0%	0.0%	C, D	0	3	0	2	0.0%	0.0%
C, E	0	3	0	2	0.0%	0.0%	C, E	0	3	0	2	0.0%	0.0%
C, F	0	3	0	2	0.0%	0.0%	C, F	0	3	0	2	0.0%	0.0%
D, E	0	3	0	2	0.0%	0.0%	D, E	0	3	0	2	0.0%	0.0%
D, F	0	3	0	2	0.0%	0.0%	D, F	0	3	0	2	0.0%	0.0%
E, F	0	3	0	2	0.0%	0.0%	E, F	0	3	0	2	0.0%	0.0%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.6: 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
Command Injection													
A, F	159	103	80	45	63.47%	60.69%	A, B	99	163	0	125	71.7%	100.0%
B, F	159	103	80	45	63.47%	60.69%	A, C	99	163	0	125	71.7%	100.0%
C, F	159	103	80	45	63.47%	60.69%	A, D	99	163	0	125	71.7%	100.0%
D, F	159	103	80	45	63.47%	60.69%	A, E	99	163	0	125	71.7%	100.0%
E, F	159	103	80	45	63.47%	60.69%	A, F	99	163	0	125	71.7%	100.0%
A, B	99	163	0	125	54.85%	37.79%	B, C	22	240	0	125	67.12%	100.0%
A, C	99	163	0	125	54.85%	37.79%	C, D	22	240	0	125	67.12%	100.0%
A, D	99	163	0	125	54.85%	37.79%	C, E	22	240	0	125	67.12%	100.0%
A, E	99	163	0	125	54.85%	37.79%	C, F	22	240	0	125	67.12%	100.0%
B, C	22	240	0	125	15.49%	8.4%	B, D	19	243	0	125	66.98%	100.0%
C, D	22	240	0	125	15.49%	8.4%	B, E	19	243	0	125	66.98%	100.0%
C, E	22	240	0	125	15.49%	8.4%	B, F	19	243	0	125	66.98%	100.0%
B, E	21	241	19	106	13.91%	8.02%	D, F	159	103	80	45	48.47%	66.53%
D, E	21	241	19	106	13.91%	8.02%	E, F	159	103	80	45	48.47%	66.53%
B, D	19	243	0	125	13.52%	7.25%	D, E	21	241	19	106	41.52%	52.5%
SQL Injection													
A, F	241	258	157	199	53.73%	48.3%	A, D	123	376	0	356	74.32%	100.0%
B, F	241	258	157	199	53.73%	48.3%	B, D	123	376	0	356	74.32%	100.0%
C, F	241	258	157	199	53.73%	48.3%	C, D	123	376	0	356	74.32%	100.0%
D, F	241	258	157	199	53.73%	48.3%	D, E	123	376	0	356	74.32%	100.0%
E, F	241	258	157	199	53.73%	48.3%	D, F	123	376	0	356	74.32%	100.0%
A, B	170	329	9	347	50.15%	34.07%	A, B	170	329	9	347	73.15%	94.97%
A, C	170	329	9	347	50.15%	34.07%	A, F	170	329	9	347	73.15%	94.97%
A, D	170	329	9	347	50.15%	34.07%	A, C	74	425	5	351	69.45%	93.67%
A, E	180	319	54	302	49.11%	36.07%	B, C	74	425	5	351	69.45%	93.67%
B, E	180	319	54	302	49.11%	36.07%	C, E	74	425	5	351	69.45%	93.67%
C, E	180	319	54	302	49.11%	36.07%	C, F	74	425	5	351	69.45%	93.67%
D, E	180	319	54	302	49.11%	36.07%	A, E	180	319	54	302	62.78%	76.92%
B, D	123	376	0	356	39.55%	24.65%	B, E	180	319	54	302	62.78%	76.92%
C, D	123	376	0	356	39.55%	24.65%	E, F	180	319	54	302	62.78%	76.92%
B, C	74	425	5	351	25.61%	14.83%	B, F	241	258	157	199	52.05%	60.55%
LDAP Injection													
A, D	17	12	5	27	66.67%	58.62%	A, D	17	12	5	27	73.25%	77.27%
B, D	17	12	5	27	66.67%	58.62%	B, D	17	12	5	27	73.25%	77.27%
C, D	17	12	5	27	66.67%	58.62%	C, D	17	12	5	27	73.25%	77.27%
D, E	17	12	5	27	66.67%	58.62%	D, E	17	12	5	27	73.25%	77.27%
D, F	17	12	5	27	66.67%	58.62%	D, F	17	12	5	27	73.25%	77.27%
A, F	3	26	3	29	17.14%	10.34%	A, F	3	26	3	29	51.36%	50.0%
B, F	3	26	3	29	17.14%	10.34%	B, F	3	26	3	29	51.36%	50.0%
C, F	3	26	3	29	17.14%	10.34%	C, F	3	26	3	29	51.36%	50.0%
E, F	3	26	3	29	17.14%	10.34%	E, F	3	26	3	29	51.36%	50.0%
A, B	0	29	0	32	0.0%	0.0%	A, B	0	29	0	32	26.23%	0.0%
A, C	0	29	0	32	0.0%	0.0%	A, C	0	29	0	32	26.23%	0.0%
A, E	0	29	0	32	0.0%	0.0%	A, E	0	29	0	32	26.23%	0.0%
B, C	0	29	0	32	0.0%	0.0%	B, C	0	29	0	32	26.23%	0.0%
B, E	0	29	0	32	0.0%	0.0%	B, E	0	29	0	32	26.23%	0.0%
C, E	0	29	0	32	0.0%	0.0%	C, E	0	29	0	32	26.23%	0.0%
Cross-Site Scripting													
A, B	301	147	179	93	64.87%	67.19%	A, D	177	271	0	272	75.05%	100.0%
A, C	301	147	179	93	64.87%	67.19%	B, D	177	271	0	272	75.05%	100.0%
A, D	301	147	179	93	64.87%	67.19%	D, E	177	271	0	272	75.05%	100.0%
A, E	301	147	179	93	64.87%	67.19%	D, F	177	271	0	272	75.05%	100.0%
A, F	269	179	121	151	64.2%	60.04%	A, C	121	327	2	270	71.8%	98.37%
B, F	269	179	121	151	64.2%	60.04%	B, C	121	327	2	270	71.8%	98.37%
C, F	269	179	121	151	64.2%	60.04%	C, D	121	327	2	270	71.8%	98.37%
D, F	269	179	121	151	64.2%	60.04%	C, E	121	327	2	270	71.8%	98.37%
E, F	269	179	121	151	64.2%	60.04%	C, F	121	327	2	270	71.8%	98.37%
B, E	194	254	44	228	56.56%	43.3%	A, F	269	179	121	151	57.37%	68.97%
B, D	177	271	0	272	56.64%	39.51%	B, F	269	179	121	151	57.37%	68.97%
C, D	177	271	0	272	56.64%	39.51%	E, F	269	179	121	151	57.37%	68.97%
D, E	177	271	0	272	56.64%	39.51%	B, E	83	365	45	227	51.59%	64.84%
B, C	121	327	2	270	42.38%	27.01%	A, B	301	147	179	93	50.73%	62.71%
C, E	121	327	2	270	42.38%	27.01%	A, E	301	147	179	93	50.73%	62.71%
XPath Injection													
A, F	7	15	13	8	33.33%	31.82%	A, C	2	20	0	21	75.61%	100.0%

B, F	7	15	13	8	33.33%	31.82%	B, C	2	20	0	21	75.61%	100.0%
C, F	7	15	13	8	33.33%	31.82%	C, D	2	20	0	21	75.61%	100.0%
D, F	7	15	13	8	33.33%	31.82%	C, E	2	20	0	21	75.61%	100.0%
E, F	7	15	13	8	33.33%	31.82%	C, F	2	20	0	21	75.61%	100.0%
A, E	4	18	3	18	27.59%	18.18%	A, B	1	21	0	21	75.0%	100.0%
B, E	4	18	3	18	27.59%	18.18%	B, D	1	21	0	21	75.0%	100.0%
C, E	4	18	3	18	27.59%	18.18%	B, F	1	21	0	21	75.0%	100.0%
D, E	4	18	3	18	27.59%	18.18%	A, E	4	18	3	18	53.57%	57.14%
A, C	2	20	0	21	16.67%	9.09%	B, E	4	18	3	18	53.57%	57.14%
B, C	2	20	0	21	16.67%	9.09%	D, E	4	18	3	18	53.57%	57.14%
C, D	2	20	0	21	16.67%	9.09%	E, F	4	18	3	18	53.57%	57.14%
A, B	1	21	0	21	8.7%	4.55%	A, F	7	15	13	8	34.89%	35.0%
B, D	1	21	0	21	8.7%	4.55%	D, F	7	15	13	8	34.89%	35.0%
A, D	0	22	0	21	0.0%	0.0%	A, D	0	22	0	21	24.42%	0.0%
HTTP Response Splitting													
A, B	0	3	0	2	0.0%	0.0%	A, B	0	3	0	2	20.0%	0.0%
A, C	0	3	0	2	0.0%	0.0%	A, C	0	3	0	2	20.0%	0.0%
A, D	0	3	0	2	0.0%	0.0%	A, D	0	3	0	2	20.0%	0.0%
A, E	0	3	0	2	0.0%	0.0%	A, E	0	3	0	2	20.0%	0.0%
A, F	0	3	0	2	0.0%	0.0%	A, F	0	3	0	2	20.0%	0.0%
B, C	0	3	0	2	0.0%	0.0%	B, C	0	3	0	2	20.0%	0.0%
B, D	0	3	0	2	0.0%	0.0%	B, D	0	3	0	2	20.0%	0.0%
B, E	0	3	0	2	0.0%	0.0%	B, E	0	3	0	2	20.0%	0.0%
B, F	0	3	0	2	0.0%	0.0%	B, F	0	3	0	2	20.0%	0.0%
C, D	0	3	0	2	0.0%	0.0%	C, D	0	3	0	2	20.0%	0.0%
C, E	0	3	0	2	0.0%	0.0%	C, E	0	3	0	2	20.0%	0.0%
C, F	0	3	0	2	0.0%	0.0%	C, F	0	3	0	2	20.0%	0.0%
D, E	0	3	0	2	0.0%	0.0%	D, E	0	3	0	2	20.0%	0.0%
D, F	0	3	0	2	0.0%	0.0%	D, F	0	3	0	2	20.0%	0.0%
E, F	0	3	0	2	0.0%	0.0%	E, F	0	3	0	2	20.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.7: 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
Exposed Improper Error Handling													
A, D	36	38	2	18	48.65%	94.74%	A, D	36	38	2	18	33.73%	48.65%
B, D	36	38	2	18	48.65%	94.74%	B, D	36	38	2	18	33.73%	48.65%
C, D	36	38	2	18	48.65%	94.74%	C, D	36	38	2	18	33.73%	48.65%
D, E	36	38	2	18	48.65%	94.74%	D, E	36	38	2	18	33.73%	48.65%
D, F	36	38	2	18	48.65%	94.74%	D, F	36	38	2	18	33.73%	48.65%
A, F	28	46	12	8	37.84%	70.0%	A, F	28	46	12	8	14.73%	37.84%
B, F	28	46	12	8	37.84%	70.0%	B, F	28	46	12	8	14.73%	37.84%
C, F	28	46	12	8	37.84%	70.0%	C, F	28	46	12	8	14.73%	37.84%
E, F	28	46	12	8	37.84%	70.0%	E, F	28	46	12	8	14.73%	37.84%
A, B	18	56	12	8	24.32%	60.0%	A, B	18	56	12	8	7.82%	24.32%
A, C	18	56	12	8	24.32%	60.0%	A, C	18	56	12	8	7.82%	24.32%
A, E	18	56	12	8	24.32%	60.0%	A, E	18	56	12	8	7.82%	24.32%
B, E	8	66	0	20	10.81%	100.0%	B, E	8	66	0	20	5.99%	10.81%
C, E	8	66	0	20	10.81%	100.0%	C, E	8	66	0	20	5.99%	10.81%
B, C	2	72	0	20	2.7%	100.0%	B, C	2	72	0	20	1.39%	2.7%
Bad Security Design of Form Fields													
A, C	3	264	3	310	1.12%	50.0%	A, C	3	264	3	310	0.56%	1.12%
B, C	3	264	3	310	1.12%	50.0%	B, C	3	264	3	310	0.56%	1.12%
C, D	3	264	3	310	1.12%	50.0%	C, D	3	264	3	310	0.56%	1.12%
C, E	3	264	3	310	1.12%	50.0%	C, E	3	264	3	310	0.56%	1.12%
C, F	3	264	3	310	1.12%	50.0%	C, F	3	264	3	310	0.56%	1.12%
A, B	0	267	0	313	0.0%	0.0%	A, B	0	267	0	313	0.0%	0.0%
A, D	0	267	17	296	0.0%	0.0%	A, D	0	267	17	296	0.0%	0.0%
A, E	0	267	0	313	0.0%	0.0%	A, E	0	267	0	313	0.0%	0.0%
A, F	0	267	0	313	0.0%	0.0%	A, F	0	267	0	313	0.0%	0.0%

B, D	0	267	17	296	0.0%	0.0%	B, D	0	267	17	296	0.0%	0.0%
B, E	0	267	0	313	0.0%	0.0%	B, E	0	267	0	313	0.0%	0.0%
B, F	0	267	0	313	0.0%	0.0%	B, F	0	267	0	313	0.0%	0.0%
D, E	0	267	17	296	0.0%	0.0%	D, E	0	267	17	296	0.0%	0.0%
D, F	0	267	17	296	0.0%	0.0%	D, F	0	267	17	296	0.0%	0.0%
E, F	0	267	0	313	0.0%	0.0%	E, F	0	267	0	313	0.0%	0.0%
Method Tampering													
A, F	36	54	0	1	40.0%	100.0%	A, F	36	54	0	1	28.0%	40.0%
B, F	36	54	0	1	40.0%	100.0%	B, F	36	54	0	1	28.0%	40.0%
C, F	36	54	0	1	40.0%	100.0%	C, F	36	54	0	1	28.0%	40.0%
D, F	36	54	0	1	40.0%	100.0%	D, F	36	54	0	1	28.0%	40.0%
E, F	36	54	0	1	40.0%	100.0%	E, F	36	54	0	1	28.0%	40.0%
A, B	32	58	1	0	35.56%	96.97%	A, B	32	58	1	0	6.32%	35.56%
A, C	32	58	1	0	35.56%	96.97%	A, C	32	58	1	0	6.32%	35.56%
A, D	32	58	1	0	35.56%	96.97%	A, D	32	58	1	0	6.32%	35.56%
A, E	32	58	1	0	35.56%	96.97%	A, E	32	58	1	0	6.32%	35.56%
B, C	6	84	0	1	6.67%	100.0%	B, C	6	84	0	1	3.56%	6.67%
B, D	6	84	0	1	6.67%	100.0%	B, D	6	84	0	1	3.56%	6.67%
B, E	6	84	0	1	6.67%	100.0%	B, E	6	84	0	1	3.56%	6.67%
C, E	1	89	0	1	1.11%	100.0%	C, E	1	89	0	1	0.56%	1.11%
D, E	1	89	0	1	1.11%	100.0%	D, E	1	89	0	1	0.56%	1.11%
C, D	0	90	0	1	0.0%	0.0%	C, D	0	90	0	1	0.0%	0.0%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.8: 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
Exposed Improper Error Handling													
A, D	36	38	2	18	64.29%	48.65%	A, E	8	66	0	20	61.63%	100.0%
B, D	36	38	2	18	64.29%	48.65%	D, E	8	66	0	20	61.63%	100.0%
C, D	36	38	2	18	64.29%	48.65%	E, F	8	66	0	20	61.63%	100.0%
D, E	36	38	2	18	64.29%	48.65%	B, C	2	72	0	20	60.87%	100.0%
D, F	36	38	2	18	64.29%	48.65%	A, B	1	73	0	20	60.75%	100.0%
A, F	28	46	12	8	49.12%	37.84%	A, C	1	73	0	20	60.75%	100.0%
B, F	28	46	12	8	49.12%	37.84%	B, D	1	73	0	20	60.75%	100.0%
C, F	28	46	12	8	49.12%	37.84%	B, E	1	73	0	20	60.75%	100.0%
E, F	28	46	12	8	49.12%	37.84%	B, F	1	73	0	20	60.75%	100.0%
A, B	18	56	12	8	34.62%	24.32%	C, D	1	73	0	20	60.75%	100.0%
A, C	18	56	12	8	34.62%	24.32%	C, E	1	73	0	20	60.75%	100.0%
A, E	18	56	12	8	34.62%	24.32%	C, F	1	73	0	20	60.75%	100.0%
B, E	8	66	0	20	19.51%	10.81%	A, D	36	38	2	18	63.44%	94.74%
C, E	8	66	0	20	19.51%	10.81%	D, F	36	38	2	18	63.44%	94.74%
B, C	2	72	0	20	5.26%	2.7%	A, F	28	46	12	8	42.41%	70.0%
Bad Security Design of Form Fields													
A, C	3	264	3	310	2.2%	1.12%	A, C	3	264	3	310	52.0%	50.0%
B, C	3	264	3	310	2.2%	1.12%	B, C	3	264	3	310	52.0%	50.0%
C, D	3	264	3	310	2.2%	1.12%	C, D	3	264	3	310	52.0%	50.0%
C, E	3	264	3	310	2.2%	1.12%	C, E	3	264	3	310	52.0%	50.0%
C, F	3	264	3	310	2.2%	1.12%	C, F	3	264	3	310	52.0%	50.0%
A, B	0	267	0	313	0.0%	0.0%	A, B	0	267	0	313	26.98%	0.0%
A, D	0	267	17	296	0.0%	0.0%	A, D	0	267	0	313	26.98%	0.0%
A, E	0	267	0	313	0.0%	0.0%	A, E	0	267	0	313	26.98%	0.0%
A, F	0	267	0	313	0.0%	0.0%	A, F	0	267	0	313	26.98%	0.0%
B, D	0	267	17	296	0.0%	0.0%	B, D	0	267	0	313	26.98%	0.0%
B, E	0	267	0	313	0.0%	0.0%	B, E	0	267	0	313	26.98%	0.0%
B, F	0	267	0	313	0.0%	0.0%	B, F	0	267	0	313	26.98%	0.0%
D, E	0	267	17	296	0.0%	0.0%	D, E	0	267	0	313	26.98%	0.0%
D, F	0	267	17	296	0.0%	0.0%	D, F	0	267	0	313	26.98%	0.0%
E, F	0	267	0	313	0.0%	0.0%	E, F	0	267	0	313	26.98%	0.0%
Method Tampering													
A, F	36	54	0	1	57.14%	40.0%	A, F	36	54	0	1	50.91%	100.0%
B, F	36	54	0	1	57.14%	40.0%	B, F	36	54	0	1	50.91%	100.0%
C, F	36	54	0	1	57.14%	40.0%	C, F	36	54	0	1	50.91%	100.0%
D, F	36	54	0	1	57.14%	40.0%	D, F	36	54	0	1	50.91%	100.0%

E, F	36	54	0	1	57.14%	40.0%	E, F	36	54	0	1	50.91%	100.0%
A, B	32	58	1	0	52.03%	35.56%	A, B	6	84	0	1	50.59%	100.0%
A, C	32	58	1	0	52.03%	35.56%	B, C	6	84	0	1	50.59%	100.0%
A, D	32	58	1	0	52.03%	35.56%	B, D	6	84	0	1	50.59%	100.0%
A, E	32	58	1	0	52.03%	35.56%	A, E	1	89	0	1	50.56%	100.0%
B, C	6	84	0	1	12.5%	6.67%	B, E	1	89	0	1	50.56%	100.0%
B, D	6	84	0	1	12.5%	6.67%	C, E	1	89	0	1	50.56%	100.0%
B, E	6	84	0	1	12.5%	6.67%	D, E	1	89	0	1	50.56%	100.0%
C, E	1	89	0	1	2.2%	1.11%	A, C	32	58	1	0	48.48%	96.97%
D, E	1	89	0	1	2.2%	1.11%	A, D	32	58	1	0	48.48%	96.97%
C, D	0	90	0	1	0.0%	0.0%	C, D	0	90	0	1	0.55%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.9: 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
XML External Entities													
A, E	5	13	0	5	27.78%	100.0%	A, E	5	13	0	5	17.75%	27.78%
B, E	5	13	0	5	27.78%	100.0%	B, E	5	13	0	5	17.75%	27.78%
C, E	5	13	0	5	27.78%	100.0%	C, E	5	13	0	5	17.75%	27.78%
D, E	5	13	0	5	27.78%	100.0%	D, E	5	13	0	5	17.75%	27.78%
E, F	5	13	0	5	27.78%	100.0%	E, F	5	13	0	5	17.75%	27.78%
A, B	0	18	0	5	0.0%	0.0%	A, B	0	18	0	5	0.0%	0.0%
A, C	0	18	0	5	0.0%	0.0%	A, C	0	18	0	5	0.0%	0.0%
A, D	0	18	0	5	0.0%	0.0%	A, D	0	18	0	5	0.0%	0.0%
A, F	0	18	0	5	0.0%	0.0%	A, F	0	18	0	5	0.0%	0.0%
B, C	0	18	0	5	0.0%	0.0%	B, C	0	18	0	5	0.0%	0.0%
B, D	0	18	0	5	0.0%	0.0%	B, D	0	18	0	5	0.0%	0.0%
B, F	0	18	0	5	0.0%	0.0%	B, F	0	18	0	5	0.0%	0.0%
C, D	0	18	0	5	0.0%	0.0%	C, D	0	18	0	5	0.0%	0.0%
C, F	0	18	0	5	0.0%	0.0%	C, F	0	18	0	5	0.0%	0.0%
D, F	0	18	0	5	0.0%	0.0%	D, F	0	18	0	5	0.0%	0.0%
Bad Programming of Cookies													
A, B	34	85	0	25	28.57%	100.0%	A, B	34	85	0	25	18.37%	28.57%
A, C	34	85	0	25	28.57%	100.0%	A, C	34	85	0	25	18.37%	28.57%
A, D	34	85	0	25	28.57%	100.0%	A, D	34	85	0	25	18.37%	28.57%
A, E	34	85	0	25	28.57%	100.0%	A, E	34	85	0	25	18.37%	28.57%
A, F	34	85	0	25	28.57%	100.0%	A, F	34	85	0	25	18.37%	28.57%
B, F	30	89	0	25	25.21%	100.0%	B, F	30	89	0	25	15.78%	25.21%
C, F	30	89	0	25	25.21%	100.0%	C, F	30	89	0	25	15.78%	25.21%
D, F	30	89	0	25	25.21%	100.0%	D, F	30	89	0	25	15.78%	25.21%
E, F	30	89	0	25	25.21%	100.0%	E, F	30	89	0	25	15.78%	25.21%
B, E	15	104	0	25	12.61%	100.0%	B, E	15	104	0	25	7.1%	12.61%
C, E	15	104	0	25	12.61%	100.0%	C, E	15	104	0	25	7.1%	12.61%
D, E	15	104	0	25	12.61%	100.0%	D, E	15	104	0	25	7.1%	12.61%
B, C	8	111	0	25	6.72%	100.0%	B, C	8	111	0	25	3.59%	6.72%
C, D	8	111	0	25	6.72%	100.0%	C, D	8	111	0	25	3.59%	6.72%
B, D	7	112	0	25	5.88%	100.0%	B, D	7	112	0	25	3.11%	5.88%
Insecure Use of Hard Coded Constants													
A, B	0	24	0	0	0.0%	0.0%	A, B	0	24	0	0	0.0%	0.0%
A, C	0	24	0	0	0.0%	0.0%	A, C	0	24	0	0	0.0%	0.0%
A, D	0	24	0	0	0.0%	0.0%	A, D	0	24	0	0	0.0%	0.0%
A, E	0	24	0	0	0.0%	0.0%	A, E	0	24	0	0	0.0%	0.0%
A, F	0	24	0	0	0.0%	0.0%	A, F	0	24	0	0	0.0%	0.0%
B, C	0	24	0	0	0.0%	0.0%	B, C	0	24	0	0	0.0%	0.0%
B, D	0	24	0	0	0.0%	0.0%	B, D	0	24	0	0	0.0%	0.0%
B, E	0	24	0	0	0.0%	0.0%	B, E	0	24	0	0	0.0%	0.0%
B, F	0	24	0	0	0.0%	0.0%	B, F	0	24	0	0	0.0%	0.0%
C, D	0	24	0	0	0.0%	0.0%	C, D	0	24	0	0	0.0%	0.0%
C, E	0	24	0	0	0.0%	0.0%	C, E	0	24	0	0	0.0%	0.0%
C, F	0	24	0	0	0.0%	0.0%	C, F	0	24	0	0	0.0%	0.0%

D, E	0	24	0	0	0.0%	0.0%	D, E	0	24	0	0	0.0%	0.0%
D, F	0	24	0	0	0.0%	0.0%	D, F	0	24	0	0	0.0%	0.0%
E, F	0	24	0	0	0.0%	0.0%	E, F	0	24	0	0	0.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.10: 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
XML External Entities													
A, E	5	13	0	5	43.48%	27.78%	A, E	5	13	0	5	63.89%	100.0%
B, E	5	13	0	5	43.48%	27.78%	B, E	5	13	0	5	63.89%	100.0%
C, E	5	13	0	5	43.48%	27.78%	C, E	5	13	0	5	63.89%	100.0%
D, E	5	13	0	5	43.48%	27.78%	D, E	5	13	0	5	63.89%	100.0%
E, F	5	13	0	5	43.48%	27.78%	E, F	5	13	0	5	63.89%	100.0%
A, B	0	18	0	5	0.0%	0.0%	A, B	0	18	0	5	10.87%	0.0%
A, C	0	18	0	5	0.0%	0.0%	A, C	0	18	0	5	10.87%	0.0%
A, D	0	18	0	5	0.0%	0.0%	A, D	0	18	0	5	10.87%	0.0%
A, F	0	18	0	5	0.0%	0.0%	A, F	0	18	0	5	10.87%	0.0%
B, C	0	18	0	5	0.0%	0.0%	B, C	0	18	0	5	10.87%	0.0%
B, D	0	18	0	5	0.0%	0.0%	B, D	0	18	0	5	10.87%	0.0%
B, F	0	18	0	5	0.0%	0.0%	B, F	0	18	0	5	10.87%	0.0%
C, D	0	18	0	5	0.0%	0.0%	C, D	0	18	0	5	10.87%	0.0%
C, F	0	18	0	5	0.0%	0.0%	C, F	0	18	0	5	10.87%	0.0%
D, F	0	18	0	5	0.0%	0.0%	D, F	0	18	0	5	10.87%	0.0%
Bad Programming of Cookies													
A, B	34	85	0	25	44.44%	28.57%	A, B	34	85	0	25	61.36%	100.0%
A, C	34	85	0	25	44.44%	28.57%	A, C	34	85	0	25	61.36%	100.0%
A, D	34	85	0	25	44.44%	28.57%	A, D	34	85	0	25	61.36%	100.0%
A, E	34	85	0	25	44.44%	28.57%	A, E	34	85	0	25	61.36%	100.0%
A, F	34	85	0	25	44.44%	28.57%	A, F	34	85	0	25	61.36%	100.0%
B, F	30	89	0	25	40.27%	25.21%	B, F	30	89	0	25	60.96%	100.0%
C, F	30	89	0	25	40.27%	25.21%	C, F	30	89	0	25	60.96%	100.0%
D, F	30	89	0	25	40.27%	25.21%	D, F	30	89	0	25	60.96%	100.0%
E, F	30	89	0	25	40.27%	25.21%	E, F	30	89	0	25	60.96%	100.0%
B, E	15	104	0	25	22.39%	12.61%	B, E	15	104	0	25	59.69%	100.0%
C, E	15	104	0	25	22.39%	12.61%	C, E	15	104	0	25	59.69%	100.0%
D, E	15	104	0	25	22.39%	12.61%	D, E	15	104	0	25	59.69%	100.0%
B, C	8	111	0	25	12.6%	6.72%	B, C	8	111	0	25	59.19%	100.0%
C, D	8	111	0	25	12.6%	6.72%	C, D	8	111	0	25	59.19%	100.0%
B, D	7	112	0	25	11.11%	5.88%	B, D	7	112	0	25	59.12%	100.0%
Insecure Use of Hard Coded Constants													
A, B	0	24	0	0	0.0%	0.0%	A, B	0	24	0	0	0.0%	0.0%
A, C	0	24	0	0	0.0%	0.0%	A, C	0	24	0	0	0.0%	0.0%
A, D	0	24	0	0	0.0%	0.0%	A, D	0	24	0	0	0.0%	0.0%
A, E	0	24	0	0	0.0%	0.0%	A, E	0	24	0	0	0.0%	0.0%
A, F	0	24	0	0	0.0%	0.0%	A, F	0	24	0	0	0.0%	0.0%
B, C	0	24	0	0	0.0%	0.0%	B, C	0	24	0	0	0.0%	0.0%
B, D	0	24	0	0	0.0%	0.0%	B, D	0	24	0	0	0.0%	0.0%
B, E	0	24	0	0	0.0%	0.0%	B, E	0	24	0	0	0.0%	0.0%
B, F	0	24	0	0	0.0%	0.0%	B, F	0	24	0	0	0.0%	0.0%
C, D	0	24	0	0	0.0%	0.0%	C, D	0	24	0	0	0.0%	0.0%
C, E	0	24	0	0	0.0%	0.0%	C, E	0	24	0	0	0.0%	0.0%
C, F	0	24	0	0	0.0%	0.0%	C, F	0	24	0	0	0.0%	0.0%
D, E	0	24	0	0	0.0%	0.0%	D, E	0	24	0	0	0.0%	0.0%
D, F	0	24	0	0	0.0%	0.0%	D, F	0	24	0	0	0.0%	0.0%
E, F	0	24	0	0	0.0%	0.0%	E, F	0	24	0	0	0.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.11: 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
Insecure/Vulnerable Third-Party Software													
A, B	9	7	2	18	56.25%	81.82%	A, B	9	7	2	18	41.13%	56.25%
A, C	9	7	2	18	56.25%	81.82%	A, C	9	7	2	18	41.13%	56.25%
A, D	9	7	2	18	56.25%	81.82%	A, D	9	7	2	18	41.13%	56.25%
A, E	9	7	2	18	56.25%	81.82%	A, E	9	7	2	18	41.13%	56.25%
A, F	9	7	2	18	56.25%	81.82%	A, F	9	7	2	18	41.13%	56.25%
B, F	7	9	4	16	43.75%	63.64%	B, F	7	9	4	16	27.07%	43.75%
C, F	7	9	4	16	43.75%	63.64%	C, F	7	9	4	16	27.07%	43.75%
D, F	7	9	4	16	43.75%	63.64%	D, F	7	9	4	16	27.07%	43.75%
E, F	7	9	4	16	43.75%	63.64%	E, F	7	9	4	16	27.07%	43.75%
B, D	3	13	0	20	18.75%	100.0%	B, D	3	13	0	20	11.13%	18.75%
B, C	2	14	0	20	12.5%	100.0%	B, C	2	14	0	20	7.03%	12.5%
B, E	2	14	0	20	12.5%	100.0%	B, E	2	14	0	20	7.03%	12.5%
C, D	2	14	0	20	12.5%	100.0%	C, D	2	14	0	20	7.03%	12.5%
D, E	2	14	0	20	12.5%	100.0%	D, E	2	14	0	20	7.03%	12.5%
C, E	1	15	0	20	6.25%	100.0%	C, E	1	15	0	20	3.32%	6.25%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.12: 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
Insecure/Vulnerable Third-Party Software													
A, B	9	7	2	18	66.67%	56.25%	B, D	3	13	0	20	80.3%	100.0%
A, C	9	7	2	18	66.67%	56.25%	A, B	2	14	0	20	79.41%	100.0%
A, D	9	7	2	18	66.67%	56.25%	A, D	2	14	0	20	79.41%	100.0%
A, E	9	7	2	18	66.67%	56.25%	B, C	2	14	0	20	79.41%	100.0%
A, F	9	7	2	18	66.67%	56.25%	B, E	2	14	0	20	79.41%	100.0%
B, F	7	9	4	16	51.85%	43.75%	B, F	2	14	0	20	79.41%	100.0%
C, F	7	9	4	16	51.85%	43.75%	C, D	2	14	0	20	79.41%	100.0%
D, F	7	9	4	16	51.85%	43.75%	D, E	2	14	0	20	79.41%	100.0%
E, F	7	9	4	16	51.85%	43.75%	D, F	2	14	0	20	79.41%	100.0%
B, D	3	13	0	20	31.58%	18.75%	A, C	1	15	0	20	78.57%	100.0%
B, C	2	14	0	20	22.22%	12.5%	C, E	1	15	0	20	78.57%	100.0%
B, E	2	14	0	20	22.22%	12.5%	C, F	1	15	0	20	78.57%	100.0%
C, D	2	14	0	20	22.22%	12.5%	A, E	9	7	2	18	76.91%	81.82%
D, E	2	14	0	20	22.22%	12.5%	A, F	9	7	2	18	76.91%	81.82%
C, E	1	15	0	20	11.76%	6.25%	E, F	7	9	4	16	63.82%	63.64%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.13: 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													
A, F	1	11	0	5	8.33%	100.0%	A, F	1	11	0	5	4.51%	8.33%
B, C	1	11	0	5	8.33%	100.0%	B, C	1	11	0	5	4.51%	8.33%
B, D	1	11	0	5	8.33%	100.0%	B, D	1	11	0	5	4.51%	8.33%

B, E	1	11	0	5	8.33%	100.0%	B, E	1	11	0	5	4.51%	8.33%
B, F	1	11	0	5	8.33%	100.0%	B, F	1	11	0	5	4.51%	8.33%
C, F	1	11	0	5	8.33%	100.0%	C, F	1	11	0	5	4.51%	8.33%
D, F	1	11	0	5	8.33%	100.0%	D, F	1	11	0	5	4.51%	8.33%
E, F	1	11	0	5	8.33%	100.0%	E, F	1	11	0	5	4.51%	8.33%
A, B	1	11	1	4	8.33%	50.0%	A, B	1	11	1	4	3.68%	8.33%
A, C	1	11	1	4	8.33%	50.0%	A, C	1	11	1	4	3.68%	8.33%
A, D	1	11	1	4	8.33%	50.0%	A, D	1	11	1	4	3.68%	8.33%
A, E	1	11	1	4	8.33%	50.0%	A, E	1	11	1	4	3.68%	8.33%
C, D	0	12	0	5	0.0%	0.0%	C, D	0	12	0	5	0.0%	0.0%
C, E	0	12	0	5	0.0%	0.0%	C, E	0	12	0	5	0.0%	0.0%
D, E	0	12	0	5	0.0%	0.0%	D, E	0	12	0	5	0.0%	0.0%
Brute Force Attacks													
A, D	8	16	5	1	33.33%	61.54%	A, E	7	17	2	4	13.98%	29.17%
B, D	8	16	5	1	33.33%	61.54%	B, E	7	17	2	4	13.98%	29.17%
C, D	8	16	5	1	33.33%	61.54%	C, E	7	17	2	4	13.98%	29.17%
D, E	8	16	5	1	33.33%	61.54%	D, E	7	17	2	4	13.98%	29.17%
D, F	8	16	5	1	33.33%	61.54%	E, F	7	17	2	4	13.98%	29.17%
A, E	7	17	2	4	29.17%	77.78%	A, D	8	16	5	1	8.33%	33.33%
B, E	7	17	2	4	29.17%	77.78%	B, D	8	16	5	1	8.33%	33.33%
C, E	7	17	2	4	29.17%	77.78%	C, D	8	16	5	1	8.33%	33.33%
E, F	7	17	2	4	29.17%	77.78%	D, F	8	16	5	1	8.33%	33.33%
A, B	0	24	0	6	0.0%	0.0%	A, B	0	24	0	6	0.0%	0.0%
A, C	0	24	0	6	0.0%	0.0%	A, C	0	24	0	6	0.0%	0.0%
A, F	0	24	0	6	0.0%	0.0%	A, F	0	24	0	6	0.0%	0.0%
B, C	0	24	0	6	0.0%	0.0%	B, C	0	24	0	6	0.0%	0.0%
B, F	0	24	0	6	0.0%	0.0%	B, F	0	24	0	6	0.0%	0.0%
C, F	0	24	0	6	0.0%	0.0%	C, F	0	24	0	6	0.0%	0.0%
Session Fixation													
A, C	4	2	1	1	66.67%	80.0%	A, C	4	2	1	1	38.89%	66.67%
B, C	4	2	1	1	66.67%	80.0%	B, C	4	2	1	1	38.89%	66.67%
C, D	4	2	1	1	66.67%	80.0%	C, D	4	2	1	1	38.89%	66.67%
C, E	4	2	1	1	66.67%	80.0%	C, E	4	2	1	1	38.89%	66.67%
C, F	4	2	1	1	66.67%	80.0%	C, F	4	2	1	1	38.89%	66.67%
A, B	0	6	0	2	0.0%	0.0%	A, B	0	6	0	2	0.0%	0.0%
A, D	0	6	0	2	0.0%	0.0%	A, D	0	6	0	2	0.0%	0.0%
A, E	0	6	0	2	0.0%	0.0%	A, E	0	6	0	2	0.0%	0.0%
A, F	0	6	0	2	0.0%	0.0%	A, F	0	6	0	2	0.0%	0.0%
B, D	0	6	0	2	0.0%	0.0%	B, D	0	6	0	2	0.0%	0.0%
B, E	0	6	0	2	0.0%	0.0%	B, E	0	6	0	2	0.0%	0.0%
B, F	0	6	0	2	0.0%	0.0%	B, F	0	6	0	2	0.0%	0.0%
D, E	0	6	0	2	0.0%	0.0%	D, E	0	6	0	2	0.0%	0.0%
D, F	0	6	0	2	0.0%	0.0%	D, F	0	6	0	2	0.0%	0.0%
E, F	0	6	0	2	0.0%	0.0%	E, F	0	6	0	2	0.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.14: 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													
A, F	1	11	0	5	15.38%	8.33%	A, F	1	11	0	5	65.62%	100.0%
B, C	1	11	0	5	15.38%	8.33%	B, C	1	11	0	5	65.62%	100.0%
B, D	1	11	0	5	15.38%	8.33%	B, D	1	11	0	5	65.62%	100.0%
B, E	1	11	0	5	15.38%	8.33%	B, E	1	11	0	5	65.62%	100.0%
B, F	1	11	0	5	15.38%	8.33%	B, F	1	11	0	5	65.62%	100.0%
C, F	1	11	0	5	15.38%	8.33%	C, F	1	11	0	5	65.62%	100.0%
D, F	1	11	0	5	15.38%	8.33%	D, F	1	11	0	5	65.62%	100.0%
E, F	1	11	0	5	15.38%	8.33%	E, F	1	11	0	5	65.62%	100.0%
A, B	1	11	1	4	14.29%	8.33%	A, B	1	11	1	4	38.33%	50.0%
A, C	1	11	1	4	14.29%	8.33%	A, C	1	11	1	4	38.33%	50.0%
A, D	1	11	1	4	14.29%	8.33%	A, D	1	11	1	4	38.33%	50.0%
A, E	1	11	1	4	14.29%	8.33%	A, E	1	11	1	4	38.33%	50.0%
C, D	0	12	0	5	0.0%	0.0%	C, D	0	12	0	5	14.71%	0.0%

C, E	0	12	0	5	0.0%	0.0%	C, E	0	12	0	5	14.71%	0.0%
D, E	0	12	0	5	0.0%	0.0%	D, E	0	12	0	5	14.71%	0.0%
Brute Force Attacks													
A, D	8	16	5	1	43.24%	33.33%	A, E	7	17	2	4	48.41%	77.78%
B, D	8	16	5	1	43.24%	33.33%	B, E	7	17	2	4	48.41%	77.78%
C, D	8	16	5	1	43.24%	33.33%	C, E	7	17	2	4	48.41%	77.78%
D, E	8	16	5	1	43.24%	33.33%	D, E	7	17	2	4	48.41%	77.78%
D, F	8	16	5	1	43.24%	33.33%	E, F	7	17	2	4	48.41%	77.78%
A, E	7	17	2	4	42.42%	29.17%	A, D	8	16	5	1	33.71%	61.54%
B, E	7	17	2	4	42.42%	29.17%	B, D	8	16	5	1	33.71%	61.54%
C, E	7	17	2	4	42.42%	29.17%	C, D	8	16	5	1	33.71%	61.54%
E, F	7	17	2	4	42.42%	29.17%	D, F	8	16	5	1	33.71%	61.54%
A, B	0	24	0	6	0.0%	0.0%	A, B	0	24	0	6	20.0%	0.0%
A, C	0	24	0	6	0.0%	0.0%	A, C	0	24	0	6	20.0%	0.0%
A, F	0	24	0	6	0.0%	0.0%	A, F	0	24	0	6	20.0%	0.0%
B, C	0	24	0	6	0.0%	0.0%	B, C	0	24	0	6	20.0%	0.0%
B, F	0	24	0	6	0.0%	0.0%	B, F	0	24	0	6	20.0%	0.0%
C, F	0	24	0	6	0.0%	0.0%	C, F	0	24	0	6	20.0%	0.0%
Session Fixation													
A, C	4	2	1	1	72.73%	66.67%	A, C	4	2	1	1	56.67%	80.0%
B, C	4	2	1	1	72.73%	66.67%	B, C	4	2	1	1	56.67%	80.0%
C, D	4	2	1	1	72.73%	66.67%	C, D	4	2	1	1	56.67%	80.0%
C, E	4	2	1	1	72.73%	66.67%	C, E	4	2	1	1	56.67%	80.0%
C, F	4	2	1	1	72.73%	66.67%	C, F	4	2	1	1	56.67%	80.0%
A, B	0	6	0	2	0.0%	0.0%	A, B	0	6	0	2	25.0%	0.0%
A, D	0	6	0	2	0.0%	0.0%	A, D	0	6	0	2	25.0%	0.0%
A, E	0	6	0	2	0.0%	0.0%	A, E	0	6	0	2	25.0%	0.0%
A, F	0	6	0	2	0.0%	0.0%	A, F	0	6	0	2	25.0%	0.0%
B, D	0	6	0	2	0.0%	0.0%	B, D	0	6	0	2	25.0%	0.0%
B, E	0	6	0	2	0.0%	0.0%	B, E	0	6	0	2	25.0%	0.0%
B, F	0	6	0	2	0.0%	0.0%	B, F	0	6	0	2	25.0%	0.0%
D, E	0	6	0	2	0.0%	0.0%	D, E	0	6	0	2	25.0%	0.0%
D, F	0	6	0	2	0.0%	0.0%	D, F	0	6	0	2	25.0%	0.0%
E, F	0	6	0	2	0.0%	0.0%	E, F	0	6	0	2	25.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.15: 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 Scope of Cookies													
A, B	17	15	1	3	53.12%	94.44%	A, B	17	15	1	3	34.03%	53.12%
B, C	17	15	1	3	53.12%	94.44%	B, C	17	15	1	3	34.03%	53.12%
B, D	17	15	1	3	53.12%	94.44%	B, D	17	15	1	3	34.03%	53.12%
B, E	17	15	1	3	53.12%	94.44%	B, E	17	15	1	3	34.03%	53.12%
B, F	17	15	1	3	53.12%	94.44%	B, F	17	15	1	3	34.03%	53.12%
A, C	10	22	0	4	31.25%	100.0%	A, C	10	22	0	4	20.51%	31.25%
A, D	10	22	0	4	31.25%	100.0%	A, D	10	22	0	4	20.51%	31.25%
A, E	10	22	0	4	31.25%	100.0%	A, E	10	22	0	4	20.51%	31.25%
A, F	10	22	0	4	31.25%	100.0%	A, F	10	22	0	4	20.51%	31.25%
C, D	1	31	0	4	3.12%	100.0%	C, D	1	31	0	4	1.61%	3.12%
D, E	1	31	0	4	3.12%	100.0%	D, E	1	31	0	4	1.61%	3.12%
D, F	1	31	0	4	3.12%	100.0%	D, F	1	31	0	4	1.61%	3.12%
C, E	0	32	0	4	0.0%	0.0%	C, E	0	32	0	4	0.0%	0.0%
C, F	0	32	0	4	0.0%	0.0%	C, F	0	32	0	4	0.0%	0.0%
E, F	0	32	0	4	0.0%	0.0%	E, F	0	32	0	4	0.0%	0.0%
Insecure Deserialization													
A, B	0	2	0	4	0.0%	0.0%	A, B	0	2	0	4	0.0%	0.0%
A, C	0	2	0	4	0.0%	0.0%	A, C	0	2	0	4	0.0%	0.0%

A, D	0	2	0	4	0.0%	0.0%	A, D	0	2	0	4	0.0%	0.0%
A, E	0	2	0	4	0.0%	0.0%	A, E	0	2	0	4	0.0%	0.0%
A, F	0	2	0	4	0.0%	0.0%	A, F	0	2	0	4	0.0%	0.0%
B, C	0	2	0	4	0.0%	0.0%	B, C	0	2	0	4	0.0%	0.0%
B, D	0	2	0	4	0.0%	0.0%	B, D	0	2	0	4	0.0%	0.0%
B, E	0	2	0	4	0.0%	0.0%	B, E	0	2	0	4	0.0%	0.0%
B, F	0	2	0	4	0.0%	0.0%	B, F	0	2	0	4	0.0%	0.0%
C, D	0	2	0	4	0.0%	0.0%	C, D	0	2	0	4	0.0%	0.0%
C, E	0	2	0	4	0.0%	0.0%	C, E	0	2	0	4	0.0%	0.0%
C, F	0	2	0	4	0.0%	0.0%	C, F	0	2	0	4	0.0%	0.0%
D, E	0	2	0	4	0.0%	0.0%	D, E	0	2	0	4	0.0%	0.0%
D, F	0	2	0	4	0.0%	0.0%	D, F	0	2	0	4	0.0%	0.0%
E, F	0	2	0	4	0.0%	0.0%	E, F	0	2	0	4	0.0%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.16: 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 Scope of Cookies													
A, B	17	15	1	3	68.0%	53.12%	A, B	10	22	0	4	57.69%	100.0%
B, C	17	15	1	3	68.0%	53.12%	A, C	10	22	0	4	57.69%	100.0%
B, D	17	15	1	3	68.0%	53.12%	A, D	10	22	0	4	57.69%	100.0%
B, E	17	15	1	3	68.0%	53.12%	A, E	10	22	0	4	57.69%	100.0%
B, F	17	15	1	3	68.0%	53.12%	A, F	10	22	0	4	57.69%	100.0%
A, C	10	22	0	4	47.62%	31.25%	B, D	1	31	0	4	55.71%	100.0%
A, D	10	22	0	4	47.62%	31.25%	C, D	1	31	0	4	55.71%	100.0%
A, E	10	22	0	4	47.62%	31.25%	D, E	1	31	0	4	55.71%	100.0%
A, F	10	22	0	4	47.62%	31.25%	D, F	1	31	0	4	55.71%	100.0%
C, D	1	31	0	4	6.06%	3.12%	B, C	17	15	1	3	55.56%	94.44%
D, E	1	31	0	4	6.06%	3.12%	B, E	17	15	1	3	55.56%	94.44%
D, F	1	31	0	4	6.06%	3.12%	B, F	17	15	1	3	55.56%	94.44%
C, E	0	32	0	4	0.0%	0.0%	C, E	0	32	0	4	5.56%	0.0%
C, F	0	32	0	4	0.0%	0.0%	C, F	0	32	0	4	5.56%	0.0%
E, F	0	32	0	4	0.0%	0.0%	E, F	0	32	0	4	5.56%	0.0%
Insecure Deserialization													
A, B	0	2	0	4	0.0%	0.0%	A, B	0	2	0	4	33.33%	0.0%
A, C	0	2	0	4	0.0%	0.0%	A, C	0	2	0	4	33.33%	0.0%
A, D	0	2	0	4	0.0%	0.0%	A, D	0	2	0	4	33.33%	0.0%
A, E	0	2	0	4	0.0%	0.0%	A, E	0	2	0	4	33.33%	0.0%
A, F	0	2	0	4	0.0%	0.0%	A, F	0	2	0	4	33.33%	0.0%
B, C	0	2	0	4	0.0%	0.0%	B, C	0	2	0	4	33.33%	0.0%
B, D	0	2	0	4	0.0%	0.0%	B, D	0	2	0	4	33.33%	0.0%
B, E	0	2	0	4	0.0%	0.0%	B, E	0	2	0	4	33.33%	0.0%
B, F	0	2	0	4	0.0%	0.0%	B, F	0	2	0	4	33.33%	0.0%
C, D	0	2	0	4	0.0%	0.0%	C, D	0	2	0	4	33.33%	0.0%
C, E	0	2	0	4	0.0%	0.0%	C, E	0	2	0	4	33.33%	0.0%
C, F	0	2	0	4	0.0%	0.0%	C, F	0	2	0	4	33.33%	0.0%
D, E	0	2	0	4	0.0%	0.0%	D, E	0	2	0	4	33.33%	0.0%
D, F	0	2	0	4	0.0%	0.0%	D, F	0	2	0	4	33.33%	0.0%
E, F	0	2	0	4	0.0%	0.0%	E, F	0	2	0	4	33.33%	0.0%
A - OWASP ZAP ǀ B - Burp Suite ǀ C - Iron Wasp ǀ D - Accunetix ǀ E - Wapiti ǀ F - OWASP ZAP + Plugins													

Table 4.17: 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													
A, F	14	18	3	10	43.75%	82.35%	A, F	14	18	3	10	26.4%	43.75%
B, F	14	18	3	10	43.75%	82.35%	B, F	14	18	3	10	26.4%	43.75%
C, F	14	18	3	10	43.75%	82.35%	C, F	14	18	3	10	26.4%	43.75%
D, F	14	18	3	10	43.75%	82.35%	D, F	14	18	3	10	26.4%	43.75%
E, F	14	18	3	10	43.75%	82.35%	E, F	14	18	3	10	26.4%	43.75%
A, B	13	19	4	9	40.62%	76.47%	C, D	12	20	0	13	25.78%	37.5%
A, C	13	19	4	9	40.62%	76.47%	A, B	13	19	4	9	22.31%	40.62%
A, D	13	19	4	9	40.62%	76.47%	A, C	13	19	4	9	22.31%	40.62%
A, E	13	19	4	9	40.62%	76.47%	A, D	13	19	4	9	22.31%	40.62%
C, D	12	20	0	13	37.5%	100.0%	A, E	13	19	4	9	22.31%	40.62%
B, C	8	24	0	13	25.0%	100.0%	B, C	8	24	0	13	15.62%	25.0%
B, D	8	24	0	13	25.0%	100.0%	B, D	8	24	0	13	15.62%	25.0%
C, E	8	24	0	13	25.0%	100.0%	C, E	8	24	0	13	15.62%	25.0%
D, E	8	24	0	13	25.0%	100.0%	D, E	8	24	0	13	15.62%	25.0%
B, E	5	27	0	13	15.62%	100.0%	B, E	5	27	0	13	9.03%	15.62%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.18: 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													
A, F	14	18	3	10	57.14%	43.75%	C, D	12	20	0	13	69.7%	100.0%
B, F	14	18	3	10	57.14%	43.75%	A, C	8	24	0	13	67.57%	100.0%
C, F	14	18	3	10	57.14%	43.75%	A, D	8	24	0	13	67.57%	100.0%
D, F	14	18	3	10	57.14%	43.75%	B, C	8	24	0	13	67.57%	100.0%
E, F	14	18	3	10	57.14%	43.75%	B, D	8	24	0	13	67.57%	100.0%
A, B	13	19	4	9	53.06%	40.62%	C, E	8	24	0	13	67.57%	100.0%
A, C	13	19	4	9	53.06%	40.62%	C, F	8	24	0	13	67.57%	100.0%
A, D	13	19	4	9	53.06%	40.62%	D, E	8	24	0	13	67.57%	100.0%
A, E	13	19	4	9	53.06%	40.62%	D, F	8	24	0	13	67.57%	100.0%
C, D	12	20	0	13	54.55%	37.5%	A, B	5	27	0	13	66.25%	100.0%
B, C	8	24	0	13	40.0%	25.0%	B, E	5	27	0	13	66.25%	100.0%
B, D	8	24	0	13	40.0%	25.0%	B, F	5	27	0	13	66.25%	100.0%
C, E	8	24	0	13	40.0%	25.0%	A, E	5	27	1	12	57.05%	83.33%
D, E	8	24	0	13	40.0%	25.0%	E, F	5	27	1	12	57.05%	83.33%
B, E	5	27	0	13	27.03%	15.62%	A, F	14	18	3	10	59.03%	82.35%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.19: 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													
A, D	448	378	1	12	54.24%	99.78%	A, D	448	378	1	12	39.74%	54.24%
B, D	448	378	1	12	54.24%	99.78%	B, D	448	378	1	12	39.74%	54.24%
C, D	448	378	1	12	54.24%	99.78%	C, D	448	378	1	12	39.74%	54.24%
D, E	448	378	1	12	54.24%	99.78%	D, E	448	378	1	12	39.74%	54.24%
D, F	448	378	1	12	54.24%	99.78%	D, F	448	378	1	12	39.74%	54.24%
A, B	352	474	2	11	42.62%	99.44%	A, B	352	474	2	11	27.11%	42.62%
B, C	352	474	2	11	42.62%	99.44%	B, C	352	474	2	11	27.11%	42.62%

B, E	352	474	2	11	42.62%	99.44%	B, E	352	474	2	11	27.11%	42.62%
B, F	352	474	2	11	42.62%	99.44%	B, F	352	474	2	11	27.11%	42.62%
A, C	118	708	0	13	14.29%	100.0%	A, C	121	705	1	12	7.83%	14.65%
C, E	118	708	0	13	14.29%	100.0%	A, E	121	705	1	12	7.83%	14.65%
C, F	118	708	0	13	14.29%	100.0%	A, F	121	705	1	12	7.83%	14.65%
A, E	112	714	0	13	13.56%	100.0%	C, E	118	708	0	13	8.16%	14.29%
E, F	112	714	0	13	13.56%	100.0%	C, F	118	708	0	13	8.16%	14.29%
A, F	121	705	1	12	14.65%	99.18%	E, F	112	714	0	13	7.7%	13.56%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.20: 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													
A, D	448	378	1	12	70.27%	54.24%	A, C	118	708	0	13	50.9%	100.0%
B, D	448	378	1	12	70.27%	54.24%	B, C	118	708	0	13	50.9%	100.0%
C, D	448	378	1	12	70.27%	54.24%	C, D	118	708	0	13	50.9%	100.0%
D, E	448	378	1	12	70.27%	54.24%	C, E	118	708	0	13	50.9%	100.0%
D, F	448	378	1	12	70.27%	54.24%	C, F	118	708	0	13	50.9%	100.0%
A, B	352	474	2	11	59.66%	42.62%	A, E	112	714	0	13	50.89%	100.0%
B, C	352	474	2	11	59.66%	42.62%	B, E	112	714	0	13	50.89%	100.0%
B, E	352	474	2	11	59.66%	42.62%	D, E	112	714	0	13	50.89%	100.0%
B, F	352	474	2	11	59.66%	42.62%	E, F	112	714	0	13	50.89%	100.0%
A, E	121	705	1	12	25.53%	14.65%	A, D	448	378	1	12	51.43%	99.78%
A, F	121	705	1	12	25.53%	14.65%	B, D	448	378	1	12	51.43%	99.78%
A, C	118	708	0	13	25.0%	14.29%	D, F	448	378	1	12	51.43%	99.78%
C, E	118	708	0	13	25.0%	14.29%	A, B	352	474	2	11	50.85%	99.44%
C, F	118	708	0	13	25.0%	14.29%	B, F	352	474	2	11	50.85%	99.44%
E, F	112	714	0	13	23.88%	13.56%	A, F	121	705	1	12	50.43%	99.18%
A - OWASP ZAP | B - Burp Suite | C - Iron Wasp | D - Accunetix | E - Wapiti | F - OWASP ZAP + Plugins													

Table 4.21: Ranking of combinations of 2 SAST tools regarding their performance in category A10: Server-Side Request Forgery - Best and Minimum Effort Scenarios

5. Conclusão

Conclusão da sebenta, onde se resume as observações feitas.