

# Static Code Analysis Tools Pilot Procedure

Document Part of SSEF (Software Security Engineering Framework) – A Coffee & Security Initiative



## Static Code Analysis Evaluation Criteria Matrix

				Vendors (Rate 0,4,7,10)					
Number	Support Item	Category / Family	Weight	<Tool Name> Score					
	Vulnerability Detection			Tester 1	Tester 2	Debasis	Developers	Total	
			10						
1	SQL Injection	Input Validation	9.59	7	7	10	10	10	440.0
2	XSS (Cross Site Scripting)	Input Validation		7	7	10			418.0
3	HTTP Response Splitting	Input Validation	9	77	74	77	107	77	342.0
4	Command Injection (Semantic & Dataflow)	Input Validation	7						288.0
5	Denial-of-Service (DoS) Log	Input Validation		77	77	77	47	107	245.0
6	Forging	Input Validation	7.65						245.0
7	Missing XML Validation Path	Input Validation		77	74	77	107	1010	266.5
8	Manipulation	Input Validation	7.85						245.0
9	Resource Injection	Input Validation	7.5	7	7	7	77	77	297.5
10	Setting Manipulation	Input Validation	6.5	7	4	7			240.0
11	Unsafe JNI	Input Validation	6.5	7	7	7	10	7	247.0
12	Unsafe Reflection	Input Validation		7	4	7	10	7	227.5
13	Access Control: Database	Security Features		7	7	7	7	7	262.5
			7.56						
14	Insecure Randomness	Security Features	9	77	7	7	1010	1010	246.0
15	Password Management: Storing Plain-Text	Security Features	9		10	10			423.0
16	Password Management: Hardcoded Password	Security Features	9	7	1010	10	1010	10	423.0
17	Password Management: Password in Redirect	Security Features	8	7		10		7	396.0
18	Password Management: Weak Cryptography	Security Features	5.833333333	77	107	107	7	74	328.0
19	Privacy Violation	Security Features					7		186.7
20	Code Correctness: Call to Thread.run()	API Abuse	5	7	4	7	10	10	190.0
21	EJB Bad Practices: Use of Sockets	API Abuse	5.5	7	4	7	10	10	209.0
22	J2EE Bad Practices: getConnection()	API Abuse	6	7	4	7	10	10	228.0
23	J2EE Bad Practices: Sockets	API Abuse	5.5	7	4	7	10	7	192.5
24	Missing Check against Null	API Abuse	7	7	7	7	7	10	266.0
25	Missing Check for Null Parameter, controlflow	API Abuse	7	7	7	7	7	7	245.0
26	Code Correctness: Call to System.gc()	API Abuse	4	7	7	7	10	10	164.0
27	Code Correctness: Erroneous finalize() Method	API Abuse	4	7	4	7	10	4	128.0
28	EJB Bad Practices: Use of AWT/Swing	API Abuse	3.333333333	7	4	7	10	4	106.7
29	EJB Bad Practices: Use of Class Loader	API Abuse	2.666666667	7	4	7	10	4	85.3
30	EJB Bad Practices: Use of java.io	API Abuse	5	7	4	7	10	4	160.0
31	EJB Bad Practices: Use of Synchronization Primitives	API Abuse	3.333333333	7	4	7	10	4	106.7
32	Object Model Violation: Erroneous clone() Method	API Abuse	4	7	4	7	10	4	128.0
33	Object Model Violation: Just One of equals() and hashCode() Defined	API Abuse	4	7	4	7	10	7	140.0
34	J2EE Bad Practices: System.exit()	Time and State	6	7	4	7	10	7	210.0
35	J2EE Bad Practices: Threads	Time and State	5.5	7	7	7	10	7	209.0
36	Race Condition: Singleton Member Field, structural	Time and State	6.5	7	7	7	10	7	247.0
37	Session Fixation	Time and State	7	7	7	7	4	7	224.0
38	Code Correctness: Double-Checked Locking	Time and State	4.333333333	7	7	7	7	7	151.7
39	J2EE Bad Practices: Non-Serializable Object Stored in Session	Time and State	5	7	7	7	10	10	205.0
40	Race Condition: Static Database Connection	Time and State	5	7	7	7	10	7	190.0
41	Poor Error Handling: Empty Catch	Errors	6	7	7	7	10	10	246.0
42	Poor Error Handling: Program Catches NullPointerException	Errors	6	7	7	7	10	10	246.0
43	Poor Error Handling: Overly Broad Catch	Errors	6	7	7	7	10	7	228.0
44	Poor Error Handling: Overly Broad Throws	Errors	6	7	7	7	10	7	228.0
45	Poor Error Handling: Return Inside Finally	Errors	6.5	7	7	7	10	7	247.0
46	Code Correctness: Erroneous String Compare	Code Quality	5.5	7	4	7	10	7	192.5
47	Dead Code: Unused Field	Code Quality	4	7	4	7	10	7	140.0
48	Dead Code: Unused Method	Code Quality	4	7	4	7	10	7	140.0
49	Null Dereference	Code Quality	6	7	4	7	10	10	228.0
50	Unreleased Resource	Code Quality	6.5	7	4	7	10	10	247.0
51	Code Correctness: Class Does Not Implement Cloneable	Code Quality	1.333333333	7	4	7	10	4	42.7
52	Code Correctness: Misspelled Method Name	Code Quality	5.5	7	4	7	10	7	192.5
53	Code Correctness: null Argument to equals()	Code Quality	5	7	4	7	10	7	175.0
54	Dead Code: Expression is Always False	Code Quality	5.5	7	4	7	10	7	192.5
55	Dead Code: Expression is Always True	Code Quality	5.5	7	4	7	10	7	192.5
56	Obsolete	Code Quality	5	7	4	7	10	4	160.0
57	Poor Style: Confusing Naming (Class and Member)	Code Quality	3.833333333	7	4	7	10	4	122.7

58	Poor Style: Confusing Naming (Class and Method)	Code Quality	3.833333333	7	4	7	10	4	122.7
59	Poor Style: Empty Synchronized Block	Code Quality	2.666666667	7	4	7	10	7	93.3
60	Poor Style: Identifier Contains Dollar Symbol (\$)	Code Quality	4	7	4	7	10	10	152.0
61	J2EE Bad Practices: Leftover Debug Code	Encapsulation	5.5	7	7	7	10	7	209.0
62	Poor Logging Practice: Multiple Loggers	Encapsulation	2	7	4	7	10	7	70.0
63	System Information Leak	Encapsulation	7	7	7	7	10	7	266.0
64	System Information Leak: HTML Comment in JSP	Encapsulation	7	7	7	7	10	7	266.0
65	System Information Leak: Missing Catch Block	Encapsulation	7	7	7	7	10	7	266.0
66	Trust Boundary Violation	Encapsulation	7	7	4	7	4	7	203.0
67	Unsafe Mobile Code: Access Violation	Encapsulation	6.5	7	4	7	7	7	208.0
68	Unsafe Mobile Code: Inner Class	Encapsulation	5.8	7	4	7	7	7	185.6
69	Poor Logging Practice: Logger Not Declared Static Final	Encapsulation	5.2	7	7	7	10	10	213.2
70	Poor Logging Practice: Use of System Output Stream	Encapsulation	5.8	7	7	7	10	7	220.4
71	Unsafe Mobile Code: Public finalize() Method	Encapsulation	5.8	7	7	7	10	10	237.8
72	Unsafe Mobile Code: Unsafe Array Declaration	Encapsulation	5.8	7	7	7	10	7	220.4
73	Unsafe Mobile Code: Unsafe Public Field	Encapsulation	5.8	7	7	7	10	4	203.0
74	J2EE Misconfiguration: Insufficient Session-ID Length	Environment	5.5	7	7	7	10	10	225.5
75	J2EE Misconfiguration: Missing Error Handling (Missing 404)	Environment	5.5	7	7	7	10	4	192.5
76	J2EE Misconfiguration: Missing Error Handling (Missing 500)	Environment	5.5	7	7	7	10	7	209.0
77	J2EE Misconfiguration: Weak Access Permissions	Environment	7.5	7	10	7	4	10	285.0
78	Password Management: Empty Password in Configuration File	Environment	8.5	7	7	7	10	7	323.0
79	Password Management: Password in Configuration File	Environment	8.5	7	7	7	10	7	323.0
80	J2EE Misconfiguration: Missing Error Handling (Missing Throwable)	Environment	6.5	7	7	7	10	7	247.0
81	J2EE Misconfiguration: Unsafe Bean Declaration	Environment	4	7	4	7	10	4	128.0
	<b>FEATURES</b>		9						
82	<b>IDE Supported</b> (Plug-in Support for atleast RAD 6.0, Eclipse 3.2 and WAS)	Platform		7	10	10	10	10	423.0
83	<b>Reporting</b> (Report generation in different standard file formats)	Framework	9	7	10	10	10	10	423.0
84	<b>Reporting</b> (Options to compare results to track vulnerability trend)	Framework	8	7	10	10	10	10	376.0
85	<b>Reporting</b> (Options to generated both summarised and comprehensive)	Framework	8.5	7	7	10	10	10	374.0
86	<b>Customizable Vulnerability Scanning Rules</b> (Options to customise vulnerability scanning rules as per need)	Framework	10	7	10	10	10	10	470.0
87	Integration into Configuration Management System	Platform	5.166666667	7	4	4	4	0	98.2
88	Integration Trouble Tracking	Platform	3.666666667	7	4	4	0	0	55.0
89	Custom report forms that easily integrate	Framework	6	7	7	4	0	0	108.0
90	Ease of Use for developers and Managers	Framework	9	7	7	7	7	10	342.0
91	Traceability of security defects through lifecycle	Lifecycle	7.5	7	10	7	7	10	307.5
92	Collaboration notification of found security defects	Framework	7	7	7	7	7	7	245.0
93	Policy Integration to scan for know policy checks (SOX, ISO17799)	Framework	5.5	7	7	7	10	7	209.0
	<b>Language Support</b>		9.5						
94	.Net Support	Languages		7	4	7	7	7	304.0
95	Java Support	Languages	9.5	7	4	7	10	10	361.0
			9						
96	C and C++ Support	Languages		7	4	7	7	7	288.0
97	C# Support	Languages	9	7	4	7	7	7	288.0
			7.5						
98	Structured Database languages	Languages		7	4	4	4	7	195.0
	<b>Others</b>								
99	Vulnerability v/s False Positive ratio		7.5	7	7	7	7	7	262.5
100	Frequency of Security Rules updates		6.5	7	7	7	10	10	266.5
101	Effectiveness of suggested remediation		8.5	7	4	7	7	10	297.5
102	Clarity of notes or description of Vulnerabilities Detected		10	7	4	10	10	10	410.0
103	Central Dashboard for vulnerability tracking and trend analysis		8.5	7	7	10	10	10	374.0
104	Ease of configuration (IDE Config + Database Config + time taken)		9	7	7	7	7	4	288.0
	<b>SUPPORT</b>								
105	Global Presence		5	7	4	4	7	7	145.0
106	Packaged Service Offering		3	7	4	7	7	10	105.0
107	Ability to Bring In-House		7	7	4	4	7	7	203.0

108	Product Deployment Capability		8.5	7	4	7	7	4	246.5
	<b>PRICING</b>								
109	Total Cost of Ownership		8	7	4	7	7	7	256.0
110	Modular Pricing		7	7	4	7	7	7	224.0
111	Maintenance Costs		8	7	4	7	7	7	256.0
112	Training Costs		8	7	4	7	7	7	256.0
	<b>COMPANY</b>								
113	Customer References from Fortune 500 Companies		5	7	4	7	10	7	175.0
114	Multi-Regional Experience with Installation and Support		6	7	4	7	7	7	192.0
115	Technically Certified and Experienced Personnel		9	7	4	10	10	10	369.0
116	Past Performance (Personal dealings with the company)		7	7	4	10	10	10	287.0
	<b>Score without weighting</b>			<b>812</b>	<b>671</b>	<b>839</b>	<b>1011</b>	<b>857</b>	
	<b>TOTAL Composite SCORE with Weighting</b>								<b>27321.9</b>

When selecting Scoring values, please use the rating methodology of (0,4,7,10).

0 = Not included in response or Does not perform 4

= Below expectation or supports with conditions

7 = Meets minimum requirements

10 = Excellent or performs above expectations

Number	Support Item Vulnerability Detection	Evaluators					Average
		Debasish Mohanty	Evaluator 1	Evaluator 2	Evaluator 3	Evaluator 4	
1	SQL Injection	10	10	10	10	10	10
2	XSS (Cross Site Scripting)	10	10	10	7	10	9.5
3	HTTP Response Splitting	10	10	10	7	7	9
4	Command Injection (Semantic & Dataflow)	10	7	7	10	10	9
5	Denial-of-Service (DoS)	7	7	7	7	7	7
6	Log Forging	7	7	7	7	7	7
7	Missing XML Validation	7	7	4	7	7	6.5
8	Path Manipulation	7	7	7	7	7	7
9	Resource Injection	10	7	7	7	10	8.5
10	Setting Manipulation	7	7	7	7	7	7.5
11	Unsafe JNI	4	7	7	7	7	6.5
12	Unsafe Reflection	4	7	7	7	7	6.5
13	Access Control: Database	4	4	7	10	10	7.5
14	Insecure Randomness	7	4	4	7	7	6
15	Password Management: Storing Plain-Text	10	10	10	7	7	9
16	Password Management: Hardcoded Password	10	10	10	7	7	9
17	Password Management: Password in Redirect	10	10	10	7	7	9
18	Password Management: Weak Cryptography	7	10	7	7	7	8
19	Privacy Violation	4	7	4	10	10	6.83333
20	Code Correctness: Call to Thread.run()	4	7	7	4	4	5
21	EJB Bad Practices: Use of Sockets	4	7	7	4	4	5.5
22	J2EE Bad Practices: getURLConnection()	4	10	7	4	4	6
23	J2EE Bad Practices: Sockets	4	7	7	4	4	5.5
24	Missing Check against Null	7	10	7	4	4	7
25	Missing Check for Null Parameter, controlflow	7	10	7	4	4	7
26	Code Correctness: Call to System.gc()	4	4	4	4	4	4
27	Code Correctness: Erroneous finalize() Method	4	4	4	4	4	4
28	EJB Bad Practices: Use of AWT/Swing	4	0	4	4	4	3.33333
29	EJB Bad Practices: Use of Class Loader	4	0	0	4	4	2.66667
30	EJB Bad Practices: Use of java.io	4	7	4	4	4	5
31	EJB Bad Practices: Use of Synchronization Primitives	0	4	4	4	4	3.33333
32	Object Model Violation: Erroneous clone() Method	4	4	4	4	4	4
33	Object Model Violation: Just One of equals() and hashCode() Defined	4	4	4	4	4	4
34	J2EE Bad Practices: System.exit()	7	7	7	4	4	6
35	J2EE Bad Practices: Threads	4	7	7	4	4	5.5
36	Race Condition: Singleton Member Field, structural	7	7	7	4	4	6.5
37	Session Fixation	7	10	7	4	4	7
38	Code Correctness: Double-Checked Locking	0	7	7	4	4	4.33333
39	J2EE Bad Practices: Non-Serializable Object Stored in Session	4	7	4	4	4	5
40	Race Condition: Static Database Connection	4	7	4	4	4	5
41	Poor Error Handling: Empty Catch	4	4	7	7	7	6
42	Poor Error Handling: Program Catches NullPointerException	4	4	7	7	7	6
43	Poor Error Handling: Overly Broad Catch	4	4	7	7	7	6
44	Poor Error Handling: Overly Broad Throws	4	4	7	7	7	6
45	Poor Error Handling: Return Inside Finally	4	7	7	7	7	6.5
46	Code Correctness: Erroneous String Compare	4	7	4	4	4	5.5
47	Dead Code: Unused Field	4	4	4	4	4	4
48	Dead Code: Unused Method	4	4	4	4	4	4
49	Null Dereference	7	7	7	4	4	6
50	Unreleased Resource	4	10	7	4	4	6.5
51	Code Correctness: Class Does Not Implement Cloneable	0	0	0	4	4	1.33333
52	Code Correctness: Misspelled Method Name	4	7	7	4	4	5.5
53	Code Correctness: null Argument to equals()	4	7	7	4	4	5
54	Dead Code: Expression is Always False	4	7	7	4	4	5.5
55	Dead Code: Expression is Always True	4	7	7	4	4	5.5
56	Obscure	4	7	7	4	4	5
57	Poor Style: Confusing Naming (Class and Member)	4	4	7	4	4	3.83333
58	Poor Style: Confusing Naming (Class and Method)	4	4	7	4	4	3.83333
59	Poor Style: Empty Synchronized Block	0	4	4	4	4	2.66667
60	Poor Style: Identifier Contains Dollar Symbol (\$)	4	4	4	4	4	4
61	J2EE Bad Practices: Leftover Debug Code	7	4	7	4	4	5.5
62	Poor Logging Practice: Multiple Loggers	0	0	0	4	4	2
63	System Information Leak	7	7	7	7	7	7
64	System Information Leak: HTML Comment in JSP	7	7	7	7	7	7
65	System Information Leak: Missing Catch Block	7	7	7	7	7	7
66	Trust Boundary Violation	7	7	7	7	7	7
67	Unsafe Mobile Code: Access Violation	7	7	7	4	7	6.5
68	Unsafe Mobile Code: Inner Class	7	7	7	4	4	5.8
69	Poor Logging Practice: Logger Not Declared Static Final	4	4	4	7	7	5.2
70	Poor Logging Practice: Use of System Output Stream	4	4	7	7	7	5.8
71	Unsafe Mobile Code: Public finalize() Method	7	7	7	4	4	5.8
72	Unsafe Mobile Code: Unsafe Array Declaration	7	7	7	4	4	5.8
73	Unsafe Mobile Code: Unsafe Public Field	7	7	7	4	4	5.8
74	J2EE Misconfiguration: Insufficient Session-ID Length	4	7	7	4	4	5.5
75	J2EE Misconfiguration: Missing Error Handling (Missing 404)	7	7	7	4	4	5.5
76	J2EE Misconfiguration: Missing Error Handling (Missing 500)	7	7	7	4	4	5.5
77	J2EE Misconfiguration: Weak Access Permissions	7	7	7	7	7	7.5
78	Password Management: Empty Password in Configuration File	10	10	10	4	7	8.5
79	Password Management: Password in Configuration File	10	10	10	4	7	8.5
80	J2EE Misconfiguration: Missing Error Handling (Missing Throwables)	4	7	7	7	7	6.5
81	J2EE Misconfiguration: Unsafe Bean Declaration	4	4	4	4	4	4
<b>FEATURES</b>							
82	<b>IDE Supported</b> (Plug-in Support for atleast RAD 6.0, Eclipse 3.2 and WAS)	10	10	10	7	7	9
83	<b>Reporting</b> (Report generation in different standard file formats)	10	10	10	7	7	9
84	<b>Reporting</b> (Options to compare results to track vulnerability trends)	7	10	10	7	10	8
85	<b>Reporting</b> (Options to generate both summarised and comprehensive reports)	7	10	10	7	10	8.5
86	<b>Customizable Vulnerability Scanning Rules</b> (Options to customise vulnerability scanning rules as per need)	10	10	10	10	10	10
87	Integration into Configuration Management System	0	7	7	10	7	5.16667
88	Integration Trouble Tracking	0	4	4	7	7	3.66667
89	Custom report forms that easily integrate	4	4	4	10	10	4
90	Ease of Use for developers and Managers	10	7	10	7	10	9
91	Traceability of security defects through lifecycle	7	10	10	7	7	7.5
92	Collaboration notification of found security defects	7	7	10	7	7	7
93	Policy Integration to scan for know policy checks (SOX, ISO17799)	4	7	4	7	7	5.5
<b>Language Support</b>							
94	.Net Support	10	10	10	7	10	9.5
95	Java Support	10	10	10	7	10	9.5
96	C and C++ Support	10	7	10	7	10	9
97	C# Support	10	7	10	7	10	9
98	Structured Database languages	7	7	7	7	10	7.5
<b>Others</b>							
99	Vulnerability v/s False Positive ratio	7	7	7	7	10	7.5

100	Frequency of Security Rules updates	4	7	7	7	7	7	6.5
101	Effectiveness of suggested remediation	10	10	10	7	7	7	8.5
102	Clarity of notes or description of Vulnerabilities Detected	10	10	10	10	10	10	10
103	Central Dashboard for vulnerability tracking and trend analysis	7	10	7	10	10	7	8.5
104	Ease of configuration (IDE Config + Database Config + time taken)	10	7	10	7	10	10	9
<b>SUPPORT</b>								
105	Global Presence	4	4	4	7	7	4	5
106	Packaged Service Offering	0	0	0	7	7	4	3
107	Ability to Bring In-House	7	7	7	7	7	7	7
108	Product Deployment Capability	10	10	10	7	7	7	8.5
<b>PRICING</b>								
109	Total Cost of Ownership	7	10	10	7	7	7	8
110	Modular Pricing	7	7	7	7	7	7	7
111	Maintenance Costs	7	10	10	7	7	7	8
112	Training Costs	7	10	10	7	7	7	8
<b>COMPANY</b>								
113	Customer References from Fortune 500 Companies	4	7	7	4	4	4	5
114	Multi-Regional Experience with Installation and Support	7	7	7	4	7	4	6
115	Technically Certified and Experienced Personnel	10	10	10	4	10	10	9
116	Past Performance (Personal dealings with the company)	7	7	10	4	7	7	7

When selecting weighting values, please use the Six

- 0 = Not important
- 4 = low importance
- 7 = moderate important
- 10 = Critical Success Factor

<b>EVALUATION ITEMS</b>	
	<b>Product Name</b>
<b>Vulnerability Detection</b>	<b>17842.23333</b>
<b>FEATURES</b>	<b>3430.666667</b>
<b>Language Support</b>	<b>1436</b>
<b>Others</b>	<b>1898.5</b>
<b>SUPPORT</b>	<b>699.5</b>
<b>PRICING</b>	<b>992</b>
<b>COMPANY</b>	<b>1023.0</b>
<b>Summary Totals</b>	<b>27321.9</b>