WebCruiser Web Vulnerability Scanner Test Report

V3.4.0 Made by Janusec (http://www.janusec.com)

1. Test Report

1.1. SQL Injection Test Report

Input Vector	Test Cases	Cases Count	Report	Pass Rate
GET Input Vector	Erroneous 500 Responses	19	19	100%
	Erroneous 200 Responses	19	19	100%
	200 Responses With Differentiation	19	19	100%
	Identical 200 Responses	8	8	100%
POST Input Vector	Erroneous 500 Responses	19	19	100%
	Erroneous 200 Responses	19	19	100%
	200 Responses With Differentiation	19	19	100%
	Identical 200 Responses	8	8	100%
GET Input Vector – Experimental	Insert / Delete / Other	1	1	100%
POST Input Vector - Experimental	Insert / Delete / Other	1	1	100%

1.2. XSS Test Report

Input Vector	Test Cases	Cases Count	Report	Pass Rate
GET Input Vector	ReflectedXSS	32	32	100%
POST Input Vector	ReflectedXSS	32	32	100%
Cookie Input Vector - Experimental	ReflectedXSS	1	1	100%
GET Input Vector - Experimental	ReflectedXSS	11	11	100%
POST Input Vector - Experimental	ReflectedXSS	11	11	100%
GET Input Vector - Experimental	DomXSS	4	4	100%

1.3. LFI Test Report

Input Vector	Test Cases	Cases Count	Report	Pass Rate
Get Input Vector	Erroneous HTTP 500 Responses	68	68	100%
	Erroneous HTTP 404 Responses	68	68	100%
	Erroneous HTTP 200 Responses	68	68	100%
	HTTP 302 Redirect Responses	68	68	100%
	HTTP 200 Responses With Differentiation	68	68	100%
	HTTP 200 Responses with Default File on Error	68	68	100%
POST Input Vector	Erroneous HTTP 500 Responses	68	68	100%
	Erroneous HTTP 404 Responses	68	68	100%
	Erroneous HTTP 200 Responses	68	68	100%
	HTTP 302 Redirect Responses	68	68	100%
	HTTP 200 Responses With Differentiation	68	68	100%
	HTTP 200 Responses with Default File on Error	68	68	100%

1.4. RFI Test Report

Input Vector	Test Cases	Cases Count	Report	Pass Rate
Get Input Vector	Erroneous HTTP 500 Responses	9	9	100%
	Erroneous HTTP 404 Responses	9	9	100%
	Erroneous HTTP 200 Responses	9	9	100%
	HTTP 302 Redirect Responses	9	9	100%
	HTTP 200 Responses With Differentiation	9	9	100%
	HTTP 200 Responses with	9	9	100%

	Default File on Error			
POST Input Vector	Erroneous HTTP 500 Responses	9	9	100%
	Erroneous HTTP 404 Responses	9	9	100%
	Erroneous HTTP 200 Responses	9	9	100%
	HTTP 302 Redirect Responses	9	9	100%
	HTTP 200 Responses With Differentiation	9	9	100%
	HTTP 200 Responses with Default File on Error	9	9	100%

1.5. Redirect Test Report

Input Vector	Test Cases	Cases Count	Report	Pass Rate
Get Input Vector	HTTP 302 Redirect Responses	15	15	100%
	HTTP 200 Responses With Javascript Redirect	15	15	100%
POST Input Vector	HTTP 302 Redirect Responses	15	15	100%
	HTTP 200 Responses With Javascript Redirect	15	15	100%

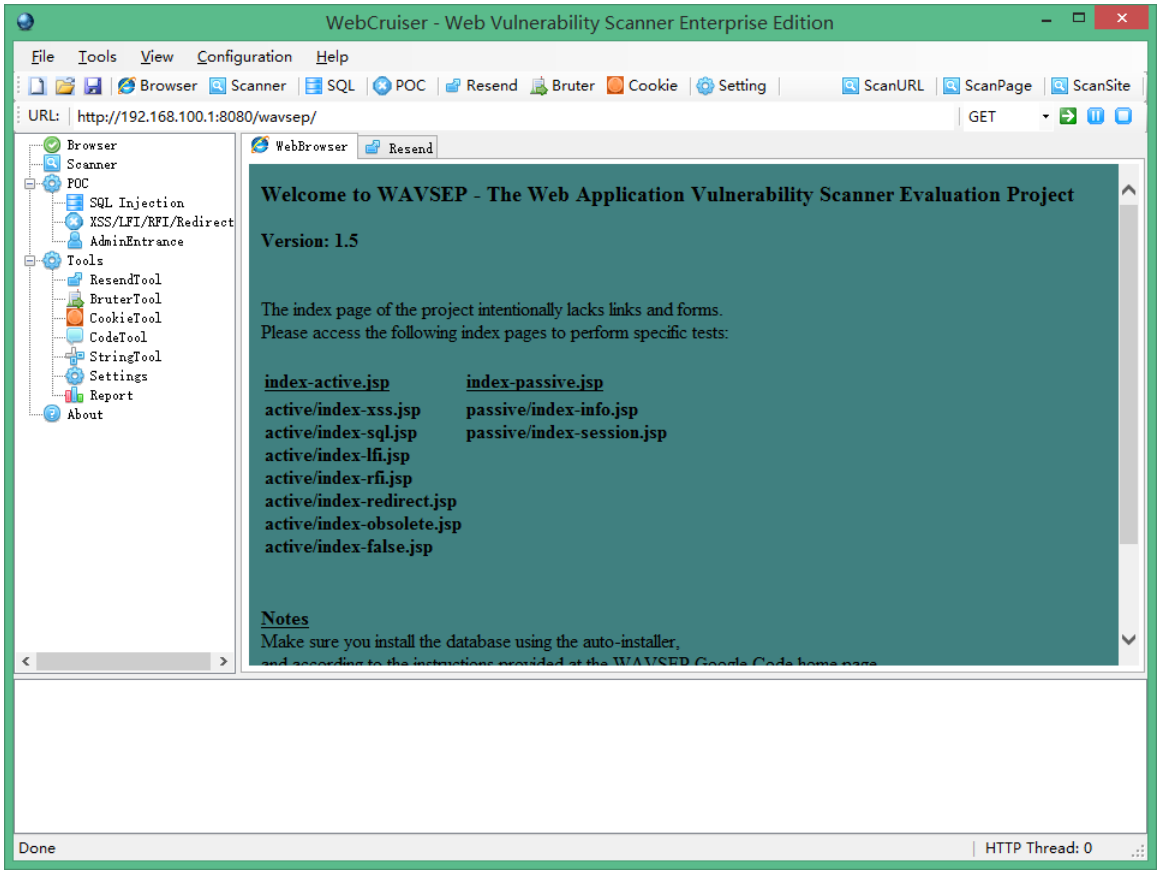
1.6. False Positive Test Report

False Vuln	Test Cases	Cases Count	Report	Pass Rate
SQL Injection	False Positive	10	0	100%
XSS	False Positive	7	0	100%
LFI	False Positive	8	0	100%
RFI	False Positive	6	0	100%
Redirect	False Positive	9	0	100%
Backup	False Positive	4	0	100%

2. Test Environment

2.1. Product and Test Cases

WAVSEP (Web Application Vulnerability Scanner Evaluation Project) v1.5
WAVSEP Environment: Windows8.1 + XAMPP (Tomcat + MySQL)
WebCruiser Web Vulnerability Scanner Enterprise Edition V3.4.0



2.2. Test Scope

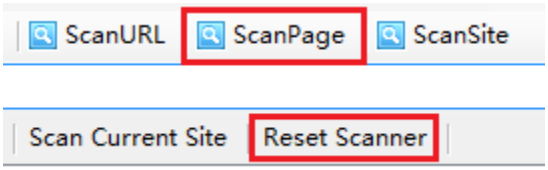
This test report includes the following vulnerabilities:

- ✧ SQL Injection
- ✧ Cross-site Scripting(XSS)
- ✧ LFI(Local File Inclusion)
- ✧ RFI(Remote File Inclusion)
- ✧ Redirect
- ✧ Obsolete Backup

Other test cases are not included.

2.3. Test Method

In order to get the test results quickly, we use a new feature of WebCruiser Web Vulnerability Scanner, which is “Scan Page”, which means it will scan all links in a page once a time. This function requires that the links locate under the same or sub directory, links under other directories will be skipped.
When start a new page scan, click “Reset Scanner” to clear previous result, and navigate to new page, and then click “ScanPage”



2.4. SQL Injection Test Details

2.4.1. Get Input Vector

Erroneous 500 Responses (19 cases)

	Vulnerability
GET-500Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithErrors.jsp?msgid=1	URL SQL INJECTION
GET-500Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithErrors.jsp?msgid=1	URL SQL INJECTION
GET-500Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithErrors.jsp?minBalanace=99999999	URL SQL INJECTION
GET-500Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithErrors.jsp?minBalanace=10000	URL SQL INJECTION
GET-500Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithErrors.jsp?minBalanace=10000	URL SQL INJECTION
GET-500Error/Case17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithErrors.jsp?msgId=99999999	URL SQL INJECTION
GET-500Error/Case17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithErrors.jsp?msgId=1	URL SQL INJECTION
GET-500Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithErrors.jsp?transactionId=99999999	URL SQL INJECTION
GET-500Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithErrors.jsp?transactionId=132	URL SQL INJECTION
GET-500Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithErrors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-500Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithErrors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-500Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithErrors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-500Error/Case14-InjectionInUpdate-Date-CommandInjection-WithErrors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-500Error/Case14-InjectionInUpdate-Date-CommandInjection-WithErrors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-500Error/Case13-InjectionInCalc-Date-BooleanExploit-WithErrors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-500Error/Case13-InjectionInCalc-Date-BooleanExploit-WithErrors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-500Error/Case12-InjectionInSearch-Date-UnionExploit-WithErrors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-500Error/Case12-InjectionInSearch-Date-UnionExploit-WithErrors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-500Error/Case11-InjectionInView-Date-PermissionBypass-WithErrors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-500Error/Case11-InjectionInView-Date-PermissionBypass-WithErrors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-500Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithErrors.jsp?orderby=1	URL SQL INJECTION
GET-500Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithErrors.jsp?orderby=1	URL SQL INJECTION
GET-500Error/Case09-InjectionInUpdate-Numeric-CommandInjection-WithErrors.jsp?msgid=1	URL SQL INJECTION
GET-500Error/Case09-InjectionInUpdate-Numeric-CommandInjection-WithErrors.jsp?msgid=1	URL SQL INJECTION
GET-500Error/Case08-InjectionInCalc-Numeric-BooleanExploit-WithErrors.jsp?minBalanace=99999999	URL SQL INJECTION
GET-500Error/Case08-InjectionInCalc-Numeric-BooleanExploit-WithErrors.jsp?minBalanace=10000	URL SQL INJECTION
GET-500Error/Case08-InjectionInCalc-Numeric-BooleanExploit-WithErrors.jsp?minBalanace=10000	URL SQL INJECTION
GET-500Error/Case07-InjectionInSearch-Numeric-UnionExploit-WithErrors.jsp?msgId=99999999	URL SQL INJECTION
GET-500Error/Case07-InjectionInSearch-Numeric-UnionExploit-WithErrors.jsp?msgId=1	URL SQL INJECTION
GET-500Error/Case06-InjectionInView-Numeric-PermissionBypass-WithErrors.jsp?transactionId=99999999	URL SQL INJECTION
GET-500Error/Case06-InjectionInView-Numeric-PermissionBypass-WithErrors.jsp?transactionId=132	URL SQL INJECTION
GET-500Error/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithErrors.jsp?orderby=msgid	URL SQL INJECTION
GET-500Error/Case04-InjectionInUpdate-String-CommandInjection-WithErrors.jsp?msg=textvalue	URL SQL INJECTION
GET-500Error/Case03-InjectionInCalc-String-BooleanExploit-WithErrors.jsp?username=textvalue	URL SQL INJECTION
GET-500Error/Case03-InjectionInCalc-String-BooleanExploit-WithErrors.jsp?username=99999999	URL SQL INJECTION
GET-500Error/Case02-InjectionInSearch-String-UnionExploit-WithErrors.jsp?msg=	URL SQL INJECTION
GET-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?username=textvalue&password=textvalue2	URL SQL INJECTION
GET-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?username=textvalue&password=textvalue2	URL SQL INJECTION
GET-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?username=textvalue&password=99999999	URL SQL INJECTION
GET-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?password=textvalue2&username=textvalue	URL SQL INJECTION
GET-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?password=textvalue2&username=textvalue	URL SQL INJECTION

Erroneous 200 Responses (19 cases)

		Vulnerability
GET-200Error/Cas	19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-With200Errors.jsp?msgid=1	URL SQL INJECTION
GET-200Error/Cas	19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-With200Errors.jsp?msgid=1	URL SQL INJECTION
GET-200Error/Cas	18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-With200Errors.jsp?minBalanace=99999999	URL SQL INJECTION
GET-200Error/Cas	18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-With200Errors.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Error/Cas	18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-With200Errors.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Error/Cas	17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-With200Errors.jsp?msgId=99999999	URL SQL INJECTION
GET-200Error/Cas	17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-With200Errors.jsp?msgId=1	URL SQL INJECTION
GET-200Error/Cas	16-InjectionInView-NumericWithoutQuotes-PermissionBypass-With200Errors.jsp?transactionId=999...	URL SQL INJECTION
GET-200Error/Cas	16-InjectionInView-NumericWithoutQuotes-PermissionBypass-With200Errors.jsp?transactionId=132	URL SQL INJECTION
GET-200Error/Cas	15-InjectionInSearch-DateWithoutQuotes-UnionExploit-With200Errors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Error/Cas	15-InjectionInSearch-DateWithoutQuotes-UnionExploit-With200Errors.jsp?transactionDate=2010-0...	URL SQL INJECTION
GET-200Error/Cas	15-InjectionInSearch-DateWithoutQuotes-UnionExploit-With200Errors.jsp?transactionDate=2010-0...	URL SQL INJECTION
GET-200Error/Cas	14-InjectionInUpdate-Date-CommandInjection-With200Errors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-200Error/Cas	14-InjectionInUpdate-Date-CommandInjection-With200Errors.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-200Error/Cas	13-InjectionInCalc-Date-BooleanExploit-With200Errors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Error/Cas	13-InjectionInCalc-Date-BooleanExploit-With200Errors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-200Error/Cas	12-InjectionInSearch-Date-UnionExploit-With200Errors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Error/Cas	12-InjectionInSearch-Date-UnionExploit-With200Errors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-200Error/Cas	11-InjectionInView-Date-PermissionBypass-With200Errors.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Error/Cas	11-InjectionInView-Date-PermissionBypass-With200Errors.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-200Error/Cas	10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-With200Errors.jsp?orderby=1	URL SQL INJECTION
GET-200Error/Cas	10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-With200Errors.jsp?orderby=1	URL SQL INJECTION
GET-200Error/Cas	09-InjectionInUpdate-Numeric-CommandInjection-With200Errors.jsp?msgid=1	URL SQL INJECTION
GET-200Error/Cas	09-InjectionInUpdate-Numeric-CommandInjection-With200Errors.jsp?msgid=1	URL SQL INJECTION
GET-200Error/Cas	08-InjectionInCalc-Numeric-BooleanExploit-With200Errors.jsp?minBalanace=99999999	URL SQL INJECTION
GET-200Error/Cas	08-InjectionInCalc-Numeric-BooleanExploit-With200Errors.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Error/Cas	08-InjectionInCalc-Numeric-BooleanExploit-With200Errors.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Error/Cas	07-InjectionInSearch-Numeric-UnionExploit-With200Errors.jsp?msgId=99999999	URL SQL INJECTION
GET-200Error/Cas	07-InjectionInSearch-Numeric-UnionExploit-With200Errors.jsp?msgId=1	URL SQL INJECTION
GET-200Error/Cas	06-InjectionInView-Numeric-PermissionBypass-With200Errors.jsp?transactionId=99999999	URL SQL INJECTION
GET-200Error/Cas	06-InjectionInView-Numeric-PermissionBypass-With200Errors.jsp?transactionId=132	URL SQL INJECTION
GET-200Error/Cas	05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-With200Errors.jsp?orderby=msgid	URL SQL INJECTION
GET-200Error/Cas	05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-With200Errors.jsp?orderby=msgid	URL SQL INJECTION
GET-200Error/Cas	04-InjectionInUpdate-String-CommandInjection-With200Errors.jsp?msg=textvalue	URL SQL INJECTION
GET-200Error/Cas	03-InjectionInCalc-String-BooleanExploit-With200Errors.jsp?username=textvalue	URL SQL INJECTION
GET-200Error/Cas	03-InjectionInCalc-String-BooleanExploit-With200Errors.jsp?username=99999999	URL SQL INJECTION
GET-200Error/Cas	02-InjectionInSearch-String-UnionExploit-With200Errors.jsp?msg=textvalue	URL SQL INJECTION
GET-200Error/Cas	02-InjectionInSearch-String-UnionExploit-With200Errors.jsp?msg=	URL SQL INJECTION
GET-200Error/Cas	01-InjectionInLogin-String-LoginBypass-With200Errors.jsp?username=textvalue&password=textvalue2	URL SQL INJECTION
GET-200Error/Cas	01-InjectionInLogin-String-LoginBypass-With200Errors.jsp?username=textvalue&password=textvalue2	URL SQL INJECTION
GET-200Error/Cas	01-InjectionInLogin-String-LoginBypass-With200Errors.jsp?username=textvalue&password=99999999	URL SQL INJECTION
GET-200Error/Cas	01-InjectionInLogin-String-LoginBypass-With200Errors.jsp?password=textvalue2&username=textvalue	URL SQL INJECTION
GET-200Error/Cas	01-InjectionInLogin-String-LoginBypass-With200Errors.jsp?password=textvalue2&username=textvalue	URL SQL INJECTION

200 Responses With Differentiation (19 cases)

	Vulnerability
GET-200Valid/Cas 19 InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithDifferent200Responses.jsp?msg...	URL SQL INJECTION
GET-200Valid/Cas 19 InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithDifferent200Responses.jsp?msg...	URL SQL INJECTION
GET-200Valid/Cas 18 InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithDifferent200Responses.jsp?minBala...	URL SQL INJECTION
GET-200Valid/Cas 18 InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithDifferent200Responses.jsp?minBala...	URL SQL INJECTION
GET-200Valid/Cas 18 InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithDifferent200Responses.jsp?minBala...	URL SQL INJECTION
GET-200Valid/Cas 17 InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithDifferent200Responses.jsp?msgId=9...	URL SQL INJECTION
GET-200Valid/Cas 17 InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithDifferent200Responses.jsp?msgId=1	URL SQL INJECTION
GET-200Valid/Cas 16 InjectionInView-NumericWithoutQuotes-PermissionBypass-WithDifferent200Responses.jsp?trans...	URL SQL INJECTION
GET-200Valid/Cas 16 InjectionInView-NumericWithoutQuotes-PermissionBypass-WithDifferent200Responses.jsp?trans...	URL SQL INJECTION
GET-200Valid/Cas 15 InjectionInSearch-DateWithoutQuotes-UnionExploit-WithDifferent200Responses.jsp?transactio...	URL SQL INJECTION
GET-200Valid/Cas 15 InjectionInSearch-DateWithoutQuotes-UnionExploit-WithDifferent200Responses.jsp?transactio...	URL SQL INJECTION
GET-200Valid/Cas 15 InjectionInSearch-DateWithoutQuotes-UnionExploit-WithDifferent200Responses.jsp?transactio...	URL SQL INJECTION
GET-200Valid/Cas 14 InjectionInUpdate-Date-CommandInjection-WithDifferent200Responses.jsp?transactionDate=201...	URL SQL INJECTION
GET-200Valid/Cas 14 InjectionInUpdate-Date-CommandInjection-WithDifferent200Responses.jsp?transactionDate=201...	URL SQL INJECTION
GET-200Valid/Cas 13 InjectionInCalc-Date-BooleanExploit-WithDifferent200Responses.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Valid/Cas 13 InjectionInCalc-Date-BooleanExploit-WithDifferent200Responses.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-200Valid/Cas 12 InjectionInSearch-Date-UnionExploit-WithDifferent200Responses.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Valid/Cas 12 InjectionInSearch-Date-UnionExploit-WithDifferent200Responses.jsp?transactionDate=2010-01-01	URL SQL INJECTION
GET-200Valid/Cas 11 InjectionInView-Date-PermissionBypass-WithDifferent200Responses.jsp?transactionDate=99999999	URL SQL INJECTION
GET-200Valid/Cas 11 InjectionInView-Date-PermissionBypass-WithDifferent200Responses.jsp?transactionDate=2010-...	URL SQL INJECTION
GET-200Valid/Cas 10 InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithDifferent200Responses.j...	URL SQL INJECTION
GET-200Valid/Cas 10 InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithDifferent200Responses.j...	URL SQL INJECTION
GET-200Valid/Cas 09 InjectionInUpdate-Numeric-CommandInjection-WithDifferent200Responses.jsp?msgid=1	URL SQL INJECTION
GET-200Valid/Cas 09 InjectionInUpdate-Numeric-CommandInjection-WithDifferent200Responses.jsp?msgid=1	URL SQL INJECTION
GET-200Valid/Cas 08 InjectionInCalc-Numeric-BooleanExploit-WithDifferent200Responses.jsp?minBalanace=99999999	URL SQL INJECTION
GET-200Valid/Cas 08 InjectionInCalc-Numeric-BooleanExploit-WithDifferent200Responses.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Valid/Cas 08 InjectionInCalc-Numeric-BooleanExploit-WithDifferent200Responses.jsp?minBalanace=10000	URL SQL INJECTION
GET-200Valid/Cas 07 InjectionInSearch-Numeric-UnionExploit-WithDifferent200Responses.jsp?msgId=99999999	URL SQL INJECTION
GET-200Valid/Cas 07 InjectionInSearch-Numeric-UnionExploit-WithDifferent200Responses.jsp?msgId=1	URL SQL INJECTION
GET-200Valid/Cas 06 InjectionInView-Numeric-PermissionBypass-WithDifferent200Responses.jsp?transactionId=9999...	URL SQL INJECTION
GET-200Valid/Cas 06 InjectionInView-Numeric-PermissionBypass-WithDifferent200Responses.jsp?transactionId=132	URL SQL INJECTION
GET-200Valid/Cas 05 InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithDifferent200Responses.js...	URL SQL INJECTION
GET-200Valid/Cas 05 InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithDifferent200Responses.js...	URL SQL INJECTION
GET-200Valid/Cas 04 InjectionInUpdate-String-CommandInjection-WithDifferent200Responses.jsp?msg=textvalue	URL SQL INJECTION
GET-200Valid/Cas 03 InjectionInCalc-String-BooleanExploit-WithDifferent200Responses.jsp?username=textvalue	URL SQL INJECTION
GET-200Valid/Cas 03 InjectionInCalc-String-BooleanExploit-WithDifferent200Responses.jsp?username=99999999	URL SQL INJECTION
GET-200Valid/Cas 02 InjectionInSearch-String-UnionExploit-WithDifferent200Responses.jsp?msg=textvalue	URL SQL INJECTION
GET-200Valid/Cas 02 InjectionInSearch-String-UnionExploit-WithDifferent200Responses.jsp?msg=	URL SQL INJECTION
GET-200Valid/Cas 01 InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp?username=textvalue&pass...	URL SQL INJECTION
GET-200Valid/Cas 01 InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp?username=textvalue&pass...	URL SQL INJECTION
GET-200Valid/Cas 01 InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp?username=textvalue&pass...	URL SQL INJECTION
GET-200Valid/Cas 01 InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp?password=textvalue2&use...	URL SQL INJECTION
GET-200Valid/Cas 01 InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp?password=textvalue2&use...	URL SQL INJECTION

Identical 200 Responses (8 cases)

	Vulnerability
GET-200Identical/Cas 08 InjectionInUpdate-DateWithoutQuotes-TimeDelayExploit-200Identical.jsp?transactionDate...	URL SQL INJECTION
GET-200Identical/Cas 07 InjectionInUpdate-NumericWithoutQuotes-TimeDelayExploit-200Identical.jsp?transactionI...	URL SQL INJECTION
GET-200Identical/Cas 06 InjectionInUpdate-Date-TimeDelayExploit-200Identical.jsp?transactionDate=2010-02-02	URL SQL INJECTION
GET-200Identical/Cas 05 InjectionInUpdate-String-TimeDelayExploit-200Identical.jsp?description=empty	URL SQL INJECTION
GET-200Identical/Cas 04 InjectionInUpdate-Numeric-TimeDelayExploit-200Identical.jsp?transactionId=895	URL SQL INJECTION
GET-200Identical/Cas 03 InjectionInView-Date-Blind-200ValidResponseWithDefaultOnException.jsp?transactionDate...	URL SQL INJECTION
GET-200Identical/Cas 03 InjectionInView-Date-Blind-200ValidResponseWithDefaultOnException.jsp?transactionDate...	URL SQL INJECTION
GET-200Identical/Cas 02 InjectionInView-String-Blind-200ValidResponseWithDefaultOnException.jsp?username=user1	URL SQL INJECTION
GET-200Identical/Cas 02 InjectionInView-String-Blind-200ValidResponseWithDefaultOnException.jsp?username=user1	URL SQL INJECTION
GET-200Identical/Cas 02 InjectionInView-String-Blind-200ValidResponseWithDefaultOnException.jsp?username=9999...	URL SQL INJECTION
GET-200Identical/Cas 01 InjectionInView-Numeric-Blind-200ValidResponseWithDefaultOnException.jsp?transactionI...	URL SQL INJECTION
GET-200Identical/Cas 01 InjectionInView-Numeric-Blind-200ValidResponseWithDefaultOnException.jsp?transactionI...	URL SQL INJECTION

2.4.2. Post Input Vector

Erroneous 500 Responses (19 cases)

	Vulnerability
↳POST-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp^password=5508194&username=...	POST SQL INJECTION
↳POST-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp^password=5508194&username=...	POST SQL INJECTION
↳POST-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp^username=8960148&password=...	POST SQL INJECTION
↳POST-500Error/Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp^username=8960148&password=...	POST SQL INJECTION
↳POST-500Error/Case02-InjectionInSearch-String-UnionExploit-WithErrors.jsp^msg=	POST SQL INJECTION
↳POST-500Error/Case02-InjectionInSearch-String-UnionExploit-WithErrors.jsp^msg=9768931	POST SQL INJECTION
↳POST-500Error/Case03-InjectionInCalc-String-BooleanExploit-WithErrors.jsp^username=4370344	POST SQL INJECTION
↳POST-500Error/Case04-InjectionInUpdate-String-CommandInjection-WithErrors.jsp^msg=3477097	POST SQL INJECTION
↳POST-500Error/Case04-InjectionInUpdate-String-CommandInjection-WithErrors.jsp^msg=3477097	POST SQL INJECTION
↳POST-500Error/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithErrors.jsp^o...	POST SQL INJECTION
↳POST-500Error/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithErrors.jsp^o...	POST SQL INJECTION
↳POST-500Error/Case06-InjectionInView-Numeric-PermissionBypass-WithErrors.jsp^transactionId=1	POST SQL INJECTION
↳POST-500Error/Case06-InjectionInView-Numeric-PermissionBypass-WithErrors.jsp^transactionId=1	POST SQL INJECTION
↳POST-500Error/Case07-InjectionInSearch-Numeric-UnionExploit-WithErrors.jsp^msgId=1	POST SQL INJECTION
↳POST-500Error/Case08-InjectionInCalc-Numeric-BooleanExploit-WithErrors.jsp^minBalanace=10000	POST SQL INJECTION
↳POST-500Error/Case08-InjectionInCalc-Numeric-BooleanExploit-WithErrors.jsp^minBalanace=10000	POST SQL INJECTION
↳POST-500Error/Case09-InjectionInUpdate-Numeric-CommandInjection-WithErrors.jsp^msgid=1	POST SQL INJECTION
↳POST-500Error/Case09-InjectionInUpdate-Numeric-CommandInjection-WithErrors.jsp^msgid=1	POST SQL INJECTION
↳POST-500Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithErrors.jsp^...	POST SQL INJECTION
↳POST-500Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithErrors.jsp^...	POST SQL INJECTION
↳POST-500Error/Case11-InjectionInView-Date-PermissionBypass-WithErrors.jsp^transactionDate=2010-01-01	POST SQL INJECTION
↳POST-500Error/Case12-InjectionInSearch-Date-UnionExploit-WithErrors.jsp^transactionDate=2010-01-01	POST SQL INJECTION
↳POST-500Error/Case13-InjectionInCalc-Date-BooleanExploit-WithErrors.jsp^transactionDate=2010-01-01	POST SQL INJECTION
↳POST-500Error/Case14-InjectionInUpdate-Date-CommandInjection-WithErrors.jsp^transactionDate=2010-0...	POST SQL INJECTION
↳POST-500Error/Case14-InjectionInUpdate-Date-CommandInjection-WithErrors.jsp^transactionDate=2010-0...	POST SQL INJECTION
↳POST-500Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithErrors.jsp^transactionDa...	POST SQL INJECTION
↳POST-500Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithErrors.jsp^transactionDa...	POST SQL INJECTION
↳POST-500Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithErrors.jsp^transact...	POST SQL INJECTION
↳POST-500Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithErrors.jsp^transact...	POST SQL INJECTION
↳POST-500Error/Case17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithErrors.jsp^msgId=1	POST SQL INJECTION
↳POST-500Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithErrors.jsp^minBalanac...	POST SQL INJECTION
↳POST-500Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithErrors.jsp^minBalanac...	POST SQL INJECTION
↳POST-500Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithErrors.jsp^msgid=1	POST SQL INJECTION
↳POST-500Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithErrors.jsp^msgid=1	POST SQL INJECTION

Erroneous 200 Responses (19 cases)

	Vulnerability
POST-200Error/Case01-InjectionInLogin-String-LoginBypass-With200Errors.jsp^password=2568487&userna...	POST SQL INJECTION
POST-200Error/Case01-InjectionInLogin-String-LoginBypass-With200Errors.jsp^password=2568487&userna...	POST SQL INJECTION
POST-200Error/Case01-InjectionInLogin-String-LoginBypass-With200Errors.jsp^username=1724348&passwo...	POST SQL INJECTION
POST-200Error/Case01-InjectionInLogin-String-LoginBypass-With200Errors.jsp^username=1724348&passwo...	POST SQL INJECTION
POST-200Error/Case02-InjectionInSearch-String-UnionExploit-With200Errors.jsp^msg=	POST SQL INJECTION
POST-200Error/Case02-InjectionInSearch-String-UnionExploit-With200Errors.jsp^msg=4404914	POST SQL INJECTION
POST-200Error/Case03-InjectionInCalc-String-BooleanExploit-With200Errors.jsp^username=2602002	POST SQL INJECTION
POST-200Error/Case04-InjectionInUpdate-String-CommandInjection-With200Errors.jsp^msg=7232700	POST SQL INJECTION
POST-200Error/Case04-InjectionInUpdate-String-CommandInjection-With200Errors.jsp^msg=7232700	POST SQL INJECTION
POST-200Error/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-With200Errors.js...	POST SQL INJECTION
POST-200Error/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-With200Errors.js...	POST SQL INJECTION
POST-200Error/Case06-InjectionInView-Numeric-PermissionBypass-With200Errors.jsp^transactionId=1	POST SQL INJECTION
POST-200Error/Case06-InjectionInView-Numeric-PermissionBypass-With200Errors.jsp^transactionId=1	POST SQL INJECTION
POST-200Error/Case07-InjectionInSearch-Numeric-UnionExploit-With200Errors.jsp^msgId=1	POST SQL INJECTION
POST-200Error/Case08-InjectionInCalc-Numeric-BooleanExploit-With200Errors.jsp^minBalanace=10000	POST SQL INJECTION
POST-200Error/Case08-InjectionInCalc-Numeric-BooleanExploit-With200Errors.jsp^minBalanace=10000	POST SQL INJECTION
POST-200Error/Case09-InjectionInUpdate-Numeric-CommandInjection-With200Errors.jsp^msgid=1	POST SQL INJECTION
POST-200Error/Case09-InjectionInUpdate-Numeric-CommandInjection-With200Errors.jsp^msgid=1	POST SQL INJECTION
POST-200Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-With200Errors.j...	POST SQL INJECTION
POST-200Error/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-With200Errors.j...	POST SQL INJECTION
POST-200Error/Case11-InjectionInView-Date-PermissionBypass-With200Errors.jsp^transactionDate=2010-...	POST SQL INJECTION
POST-200Error/Case12-InjectionInSearch-Date-UnionExploit-With200Errors.jsp^transactionDate=2010-01-01	POST SQL INJECTION
POST-200Error/Case13-InjectionInCalc-Date-BooleanExploit-With200Errors.jsp^transactionDate=2010-01-01	POST SQL INJECTION
POST-200Error/Case14-InjectionInUpdate-Date-CommandInjection-With200Errors.jsp^transactionDate=201...	POST SQL INJECTION
POST-200Error/Case14-InjectionInUpdate-Date-CommandInjection-With200Errors.jsp^transactionDate=201...	POST SQL INJECTION
POST-200Error/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-With200Errors.jsp^transactio...	POST SQL INJECTION
POST-200Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-With200Errors.jsp^trans...	POST SQL INJECTION
POST-200Error/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-With200Errors.jsp^trans...	POST SQL INJECTION
POST-200Error/Case17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-With200Errors.jsp^msgId=1	POST SQL INJECTION
POST-200Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-With200Errors.jsp^minBala...	POST SQL INJECTION
POST-200Error/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-With200Errors.jsp^minBala...	POST SQL INJECTION
POST-200Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-With200Errors.jsp^msg...	POST SQL INJECTION
POST-200Error/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-With200Errors.jsp^msg...	POST SQL INJECTION

200 Responses With Differentiation (19 cases)

	Vulnerability
POST-200Valid/Case01-InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp^password=84...	POST SQL INJECTION
POST-200Valid/Case01-InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp^password=84...	POST SQL INJECTION
POST-200Valid/Case01-InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp^username=62...	POST SQL INJECTION
POST-200Valid/Case01-InjectionInLogin-String-LoginBypass-WithDifferent200Responses.jsp^username=62...	POST SQL INJECTION
POST-200Valid/Case02-InjectionInSearch-String-UnionExploit-WithDifferent200Responses.jsp^msg=	POST SQL INJECTION
POST-200Valid/Case02-InjectionInSearch-String-UnionExploit-WithDifferent200Responses.jsp^msg=9770237	POST SQL INJECTION
POST-200Valid/Case03-InjectionInCalc-String-BooleanExploit-WithDifferent200Responses.jsp^username=...	POST SQL INJECTION
POST-200Valid/Case04-InjectionInUpdate-String-CommandInjection-WithDifferent200Responses.jsp^msg=5...	POST SQL INJECTION
POST-200Valid/Case04-InjectionInUpdate-String-CommandInjection-WithDifferent200Responses.jsp^msg=5...	POST SQL INJECTION
POST-200Valid/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithDifferent200...	POST SQL INJECTION
POST-200Valid/Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithDifferent200...	POST SQL INJECTION
POST-200Valid/Case06-InjectionInView-Numeric-PermissionBypass-WithDifferent200Responses.jsp^transa...	POST SQL INJECTION
POST-200Valid/Case06-InjectionInView-Numeric-PermissionBypass-WithDifferent200Responses.jsp^transa...	POST SQL INJECTION
POST-200Valid/Case07-InjectionInSearch-Numeric-UnionExploit-WithDifferent200Responses.jsp^msgId=1	POST SQL INJECTION
POST-200Valid/Case08-InjectionInCalc-Numeric-BooleanExploit-WithDifferent200Responses.jsp^minBalan...	POST SQL INJECTION
POST-200Valid/Case08-InjectionInCalc-Numeric-BooleanExploit-WithDifferent200Responses.jsp^minBalan...	POST SQL INJECTION
POST-200Valid/Case09-InjectionInUpdate-Numeric-CommandInjection-WithDifferent200Responses.jsp^msgid=1	POST SQL INJECTION
POST-200Valid/Case09-InjectionInUpdate-Numeric-CommandInjection-WithDifferent200Responses.jsp^msgid=1	POST SQL INJECTION
POST-200Valid/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithDifferent20...	POST SQL INJECTION
POST-200Valid/Case10-InjectionInSearchOrderBy-Numeric-BinaryDeliberateRuntimeError-WithDifferent20...	POST SQL INJECTION
POST-200Valid/Case11-InjectionInView-Date-PermissionBypass-WithDifferent200Responses.jsp^transacti...	POST SQL INJECTION
POST-200Valid/Case12-InjectionInSearch-Date-UnionExploit-WithDifferent200Responses.jsp^transaction...	POST SQL INJECTION
POST-200Valid/Case13-InjectionInCalc-Date-BooleanExploit-WithDifferent200Responses.jsp^transaction...	POST SQL INJECTION
POST-200Valid/Case14-InjectionInUpdate-Date-CommandInjection-WithDifferent200Responses.jsp^transac...	POST SQL INJECTION
POST-200Valid/Case14-InjectionInUpdate-Date-CommandInjection-WithDifferent200Responses.jsp^transac...	POST SQL INJECTION
POST-200Valid/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithDifferent200Responses.js...	POST SQL INJECTION
POST-200Valid/Case15-InjectionInSearch-DateWithoutQuotes-UnionExploit-WithDifferent200Responses.js...	POST SQL INJECTION
POST-200Valid/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithDifferent200Respons...	POST SQL INJECTION
POST-200Valid/Case16-InjectionInView-NumericWithoutQuotes-PermissionBypass-WithDifferent200Respons...	POST SQL INJECTION
POST-200Valid/Case17-InjectionInSearch-NumericWithoutQuotes-UnionExploit-WithDifferent200Responses...	POST SQL INJECTION
POST-200Valid/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithDifferent200Responses...	POST SQL INJECTION
POST-200Valid/Case18-InjectionInCalc-NumericWithoutQuotes-BooleanExploit-WithDifferent200Responses...	POST SQL INJECTION
POST-200Valid/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithDifferent200Respo...	POST SQL INJECTION
POST-200Valid/Case19-InjectionInUpdate-NumericWithoutQuotes-CommandInjection-WithDifferent200Respo...	POST SQL INJECTION

Identical 200 Responses (xx cases)

	Vulnerability
POST-200Identical/Case01-InjectionInView-Numeric-Blind-200ValidResponseWithDefaultOnException.jsp^...	POST SQL INJECTION
POST-200Identical/Case02-InjectionInView-String-Blind-200ValidResponseWithDefaultOnException.jsp^u...	POST SQL INJECTION
POST-200Identical/Case02-InjectionInView-String-Blind-200ValidResponseWithDefaultOnException.jsp^u...	POST SQL INJECTION
POST-200Identical/Case03-InjectionInView-Date-Blind-200ValidResponseWithDefaultOnException.jsp^tra...	POST SQL INJECTION
POST-200Identical/Case04-InjectionInUpdate-Numeric-TimeDelayExploit-200Identical.jsp^transactionId...	POST SQL INJECTION
POST-200Identical/Case05-InjectionInUpdate-String-TimeDelayExploit-200Identical.jsp^description=empty	POST SQL INJECTION
POST-200Identical/Case06-InjectionInUpdate-Date-TimeDelayExploit-200Identical.jsp^transactionDate=...	POST SQL INJECTION
POST-200Identical/Case07-InjectionInUpdate-NumericWithoutQuotes-TimeDelayExploit-200Identical.jsp^...	POST SQL INJECTION
POST-200Identical/Case08-InjectionInUpdate-DateWithoutQuotes-TimeDelayExploit-200Identical.jsp^tra...	POST SQL INJECTION

2.4.3. GET Input Vector – Experimental

Experimental 1 case

	Vulnerability
GET-200Error-Experimental/Case01-InjectionInInsertValues-String-BinaryDeliberateRunt...	URL SQL INJECTION
GET-200Error-Experimental/Case01-InjectionInInsertValues-String-BinaryDeliberateRunt...	URL SQL INJECTION

2.4.4. POST Input Vector – Experimental

Experimental 1 case

	Vulnerability
-POST-200Error-Experimental/Case01-InjectionInInsertValues-String-BinaryDeli...	POST SQL INJECTION
-POST-200Error-Experimental/Case01-InjectionInInsertValues-String-BinaryDeli...	POST SQL INJECTION

2.5. XSS Test Details

2.5.1. Get Input Vector

	Vulnerability
RXSS-Detection-Evaluation-GET/Case01-Tag2HtmlPageScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case02-Tag2TagScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case03-Tag2TagStructure.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case04-Tag2HtmlComment.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case05-Tag2Frameset.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case06-Event2TagScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case07-Event2DoubleQuotePropertyScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case08-Event2SingleQuotePropertyScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case09-SrcProperty2TagStructure.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case10-Js2DoubleQuoteJsEventScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case11-Js2SingleQuoteJsEventScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case12-Js2JsEventScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case13-Vbs2DoubleQuoteVbsEventScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case14-Vbs2SingleQuoteVbsEventScope.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case15-Vbs2VbsEventScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case16-Js2ScriptSupportingProperty.jsp?userinput=dummy.html	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case17-Js2PropertyJsScopeDoubleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case18-Js2PropertyJsScopeSingleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case19-Js2PropertyJsScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case20-Vbs2PropertyVbsScopeDoubleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case21-Vbs2PropertyVbsScope.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case22-Js2ScriptTagDoubleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case23-Js2ScriptTagSingleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case24-Js2ScriptTag.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case25-Vbs2ScriptTagDoubleQuoteDelimiter.jsp?userinput=david	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case26-Vbs2ScriptTag.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case27-Js2ScriptTagOLCommentScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case28-Js2ScriptTagMLCommentScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case29-Vbs2ScriptTagOLCommentScope.jsp?userinput=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case30-Tag2HtmlPageScopeMultipleVulnerabilities.jsp?userinput=1234&userinput2=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case30-Tag2HtmlPageScopeMultipleVulnerabilities.jsp?userinput=1234&userinput2=1234	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case31-Tag2HtmlPageScopeDuringException.jsp?userinput=textvalue	ReflectedXSS-GET
RXSS-Detection-Evaluation-GET/Case32-Tag2HtmlPageScopeValidViewstateRequired.jsp?userinput=textvalue&__VIEWSTATE=%2F...	ReflectedXSS-GET

2.5.2. POST Input Vector

	Vulnerability
/RXSS-Detection-Evaluation-POST/Case01-Tag2HtmlPageScope.jsp^userinput=7031589	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case02-Tag2TagScope.jsp^userinput=4795125	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case03-Tag2TagStructure.jsp^userinput=5302795	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case04-Tag2HtmlComment.jsp^userinput=5730901	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case05-Tag2Frameset.jsp^userinput=6393602	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case06-Event2TagScope.jsp^userinput=6932910	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case07-Event2DoubleQuotePropertyScope.jsp^userinput=4561956	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case08-Event2SingleQuotePropertyScope.jsp^userinput=6619670	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case09-SrcProperty2TagStructure.jsp^userinput=4344575	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case10-Js2DoubleQuoteJsEventScope.jsp^userinput=6638847	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case11-Js2SingleQuoteJsEventScope.jsp^userinput=6345682	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case12-Js2JsEventScope.jsp^userinput=1612529	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case13-Vbs2DoubleQuoteVbsEventScope.jsp^userinput=2255295	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case14-Vbs2SingleQuoteVbsEventScope.jsp^userinput=8402616	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case15-Vbs2VbsEventScope.jsp^userinput=8330887	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case16-Js2ScriptSupportingProperty.jsp^userinput=4970293	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case17-Js2PropertyJsScopeDoubleQuoteDelimiter.jsp^userinput=5465240	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case18-Js2PropertyJsScopeSingleQuoteDelimiter.jsp^userinput=4911249	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case19-Js2PropertyJsScope.jsp^userinput=6213872	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case20-Vbs2PropertyVbsScopeDoubleQuoteDelimiter.jsp^userinput=1044026	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case21-Vbs2PropertyVbsScope.jsp^userinput=4434459	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case22-Js2ScriptTagDoubleQuoteDelimiter.jsp^userinput=7795458	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case23-Js2ScriptTagSingleQuoteDelimiter.jsp^userinput=6385048	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case24-Js2ScriptTag.jsp^userinput=1013530	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case25-Vbs2ScriptTagDoubleQuoteDelimiter.jsp^userinput=6259433	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case26-Vbs2ScriptTag.jsp^userinput=1860312	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case27-Js2ScriptTagOLCommentScope.jsp^userinput=8557180	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case28-Js2ScriptTagMLCommentScope.jsp^userinput=5548096	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case29-Vbs2ScriptTagOLCommentScope.jsp^userinput=8515158	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case30-Tag2HtmlPageScopeMultipleVulnerabilities.jsp^userinput=4207661&userinput2=6900178	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case30-Tag2HtmlPageScopeMultipleVulnerabilities.jsp^userinput=4207661&userinput2=6900178	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case31-Tag2HtmlPageScopeDuringException.jsp^userinput=5549896	ReflectedXSS-POST
/RXSS-Detection-Evaluation-POST/Case32-Tag2HtmlPageScopeValidViewstateRequired.jsp^userinput=6001445&__VIEWSTATE=/wEP...	ReflectedXSS-POST

2.5.3. Cookie Input Vector – Experimental

	Vulnerability
/Reflected-XSS/RXSS-Detection-Evaluation-COOKIE-Experimental/Case01-Tag2HtmlPageScope.jsp?userinput=textvalue	ReflectedXSS-Cookie

2.5.4. GET Input Vector – Experimental

	Vulnerability
-Detection-Evaluation-GET-Experimental/Case01-Tag2HtmlPageScope-StripScriptTag.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case02-Tag2HtmlPageScope-SecretVectorPOST.jsp?userinput=textvalue	ReflectedXSS-POST
-Detection-Evaluation-GET-Experimental/Case03-Tag2HtmlPageScope-ConstantAntiCSRFToken.jsp?anticsrf=0.022520676250725402&user...	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case04-Tag2HtmlPageScope-ChangingAntiCSRFToken.jsp?userinput=3817070&newAnticsrfToken...	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case05-ScriptlessInjectionInFormTagActionAttribute.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case06-ScriptlessInjectionInBaseTagHrefAttribute.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case07-ScriptlessInjectionInScriptTagSrcAttribute.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case08-InjectionInToCssSelector.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case09-InjectionInToCssSelectorAttributeName.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case10-InjectionInToCssProperty.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case11-InjectionInToCssPropertyValue.jsp?userinput=textvalue	ReflectedXSS-GET

2.5.5. POST Input Vector – Experimental

	Vulnerability
-Detection-Evaluation-POST-Experimental/Case01-Tag2HtmlPageScope-StripScriptTag.jsp^userinput=7513034	ReflectedXSS-POST
-Detection-Evaluation-POST-Experimental/Case02-Tag2HtmlPageScope-SecretVectorGET.jsp^userinput=7746895	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case03-Tag2HtmlPageScope-ConstantAntiCSRFToken.jsp^userinput=7034445&anticsrf=0.0225...	ReflectedXSS-POST
-Detection-Evaluation-POST-Experimental/Case04-Tag2HtmlPageScope-ChangingAntiCSRFToken.jsp^userinput=2932712&newAnticsrfToke...	ReflectedXSS-POST
-Detection-Evaluation-POST-Experimental/Case05-ScriptlessInjectionInFormTagActionAttribute.jsp?userinput=5667955	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case06-ScriptlessInjectionInBaseTagHrefAttribute.jsp?userinput=1266850	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case07-ScriptlessInjectionInScriptTagSrcAttribute.jsp?userinput=8799289	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case08-InjectionInToCssSelector.jsp?userinput=3361876	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case09-InjectionInToCssSelectorAttributeName.jsp?userinput=7887917	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case10-InjectionInToCssProperty.jsp?userinput=9439815	ReflectedXSS-GET
-Detection-Evaluation-POST-Experimental/Case11-InjectionInToCssPropertyValue.jsp?userinput=6397818	ReflectedXSS-GET

2.5.6. DomXSS GET Input Vector – Experimental

	Vulnerability
-Detection-Evaluation-GET-Experimental/Case01-InjectionDirectlyInToDomXssSinkEval.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case02-InjectionDirectlyInToDomXssSinkLocation.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case03-InjectionInToVariableBeingAssignedToDomXssSinkEval.jsp?userinput=textvalue	ReflectedXSS-GET
-Detection-Evaluation-GET-Experimental/Case04-InjectionInToVariableBeingAssignedToDomXssSinkLocation.jsp?userinput=textvalue	ReflectedXSS-GET

2.6. Other Test Details

Test details not list here, test report please refer to the chapter 1: test report.

http://www.janusec.com

Feb 24, 2015