Hewlett Packard Enterprise

HPE Security Fortify Audit Workbench

OWASP Top 10 2013

Benchmark

FORTIFY

Table of Contents

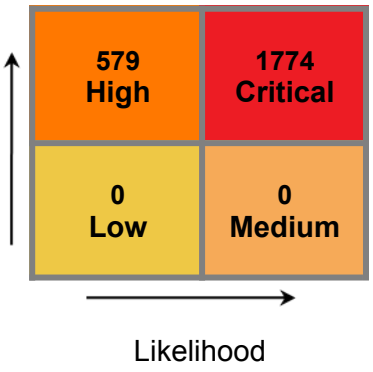
Executive Summary
Project Description
Issue Breakdown
Issue Details
- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

Description of Key Terminology

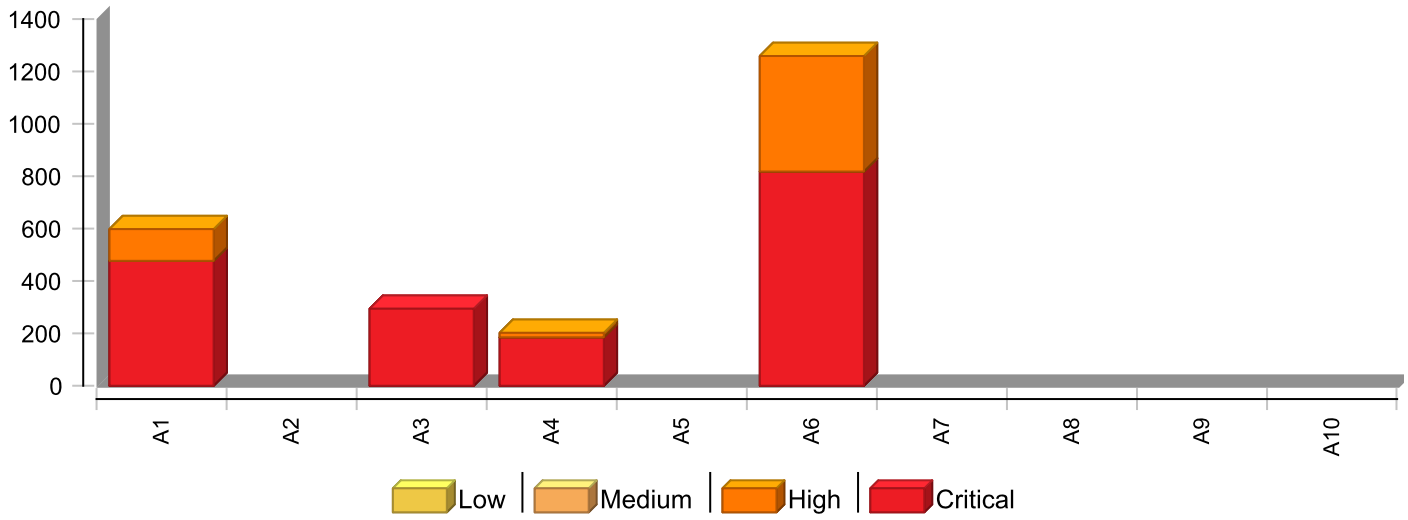
Executive Summary

Project Name:	Benchmark
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
SecurityScope:	Results Not Present
Other:	Results Not Present

Issues by Priority



Issues by OWASP Top 10 2013 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the HPE Security Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	May 6, 2019, 12:26 PM	**Engine Version:**	17.10.0156
Host Name:	WIN-4TID9RMQRU6	**Certification:**	VALID
Number of Files:	11,109	**Lines of Code:**	178,986

Issue BreakDown

The following table summarizes the number of issues identified across the different OWASP Top 10 2013 categories and broken down by Fortify Priority Order.

	Fortify Priority				Total Issues
	Critical	High	Medium	Low	
A1 Injection	477	121	0	0	598
A2 Broken Authentication and Session Management	0	0	0	0	0
A3 Cross-Site Scripting (XSS)	294	0	0	0	294
A4 Insecure Direct Object References	185	17	0	0	202
A5 Security Misconfiguration	0	0	0	0	0
A6 Sensitive Data Exposure	818	441	0	0	1259
A7 Missing Function Level Access Control	0	0	0	0	0
A8 Cross-Site Request Forgery (CSRF)	0	0	0	0	0
A9 Using Components with Known Vulnerabilities	0	0	0	0	0
A10 Unvalidated Redirects and Forwards	0	0	0	0	0

NOTE:
1. Reported issues in the above table may violate more than one OWASP Top 10 2013 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by OWASP Top 10 2013, Fortify Priority Order, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00006.java:63	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00006.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00006.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00007.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00007.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00007.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00015.java:67	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00015.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00015.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00017.java:62	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00017.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00017.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00077.java:90	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00077.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00077.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00090.java:74	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00090.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00090.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00091.java:66	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00091.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00091.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00092.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00092.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00092.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00093.java:79	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00093.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00093.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00158.java:71	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00158.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00158.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00172.java:65	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00172.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00172.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00173.java:64	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00173.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00173.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00176.java:63	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00176.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00176.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00177.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00177.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00177.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00294.java:73	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00294.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00294.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00295.java:73	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00295.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00295.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00302.java:70	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00302.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00302.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00304.java:88	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00304.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00304.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00306.java:68	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00306.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00306.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00307.java:75	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00307.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00307.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00308.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00308.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00308.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00310.java:84	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00310.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00310.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00311.java:78	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00311.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00311.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00396.java:70	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00396.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00396.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00406.java:77	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00406.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00406.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00407.java:83	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00407.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00407.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00408.java:79	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00408.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00408.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00409.java:92	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00409.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00409.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00412.java:64	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00412.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00412.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00480.java:75	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00480.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00480.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00481.java:73	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00481.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00481.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00494.java:86	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00494.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00494.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00495.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00495.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00495.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00497.java:81	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00497.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00497.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00499.java:65	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00499.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00499.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00500.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00500.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00500.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00558.java:86	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00558.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00558.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00570.java:81	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00570.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00570.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00571.java:77	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00571.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00571.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00572.java:80	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00572.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00572.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00573.java:70	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00573.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00573.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00574.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00574.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00574.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00575.java:84	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00575.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00575.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00658.java:66	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00659.java:80	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00731.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00731.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00731.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00738.java:82	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00738.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00738.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00739.java:82	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00739.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00739.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00740.java:65	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00740.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00740.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00741.java:73	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00741.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00741.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00743.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00743.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00743.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00814.java:84	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00814.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00814.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00815.java:78	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00815.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00815.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00816.java:83	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00816.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00816.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00823.java:81	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00823.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00823.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00824.java:92	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00824.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00824.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00826.java:80	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00826.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00826.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00827.java:78	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00827.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00827.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00968.java:69	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00968.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00968.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00970.java:69	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00970.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00970.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00979.java:80	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00979.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00979.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00980.java:64	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00980.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00980.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00981.java:80	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00981.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00981.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00983.java:63	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00983.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00983.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01064.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01064.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01064.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01065.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01065.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01065.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01067.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01067.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01067.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01068.java:61	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01068.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01068.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01182.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01182.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01182.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01189.java:74	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01189.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01189.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01190.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01190.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01190.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01192.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01192.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01192.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01193.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01193.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01193.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01194.java:63	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01194.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01194.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01269.java:62	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01269.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01269.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01270.java:60	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01270.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01270.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01285.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01285.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01285.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01286.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01286.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01286.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01288.java:55	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01288.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01288.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01289.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01289.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01289.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01290.java:54	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01290.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01290.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01353.java:67	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01353.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01353.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01360.java:62	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01360.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01360.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01361.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01361.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01361.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01362.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01362.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01362.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01364.java:59	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01364.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01364.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01365.java:63	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01365.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01365.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01440.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01440.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01440.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01442.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01442.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01442.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01443.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01443.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01443.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01444.java:68	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01444.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01444.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01517.java:61	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01526.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01527.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01528.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01529.java:70	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01530.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01531.java:56	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01532.java:59	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01600.java:65	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01600.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01600.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01601.java:63	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01601.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01601.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01606.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01606.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01606.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01607.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01607.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01607.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01609.java:61	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01609.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01609.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01672.java:76	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01672.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01672.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01673.java:74	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01673.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01673.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01685.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01685.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01685.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01686.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01686.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01686.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01687.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01687.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01687.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01688.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01688.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01688.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01689.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01689.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01689.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01690.java:68	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01690.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01690.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01691.java:68	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01691.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01691.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01693.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01693.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01693.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01850.java:69	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01850.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01850.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01851.java:69	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01851.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01851.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01852.java:69	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01852.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01852.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01864.java:67	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01864.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01864.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01865.java:67	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01865.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01865.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01928.java:65	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01928.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01928.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01929.java:63	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01929.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01929.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01936.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01936.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01936.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01937.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01937.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01937.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01938.java:74	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01938.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01938.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01939.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01939.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01939.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01942.java:61	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01942.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01942.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01944.java:61	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01944.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01944.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02058.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02058.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02058.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02059.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02059.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02059.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02067.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02067.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02067.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02068.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02068.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02068.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02069.java:63	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02069.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02069.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02070.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02070.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02070.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02137.java:62	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02137.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02137.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02146.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02146.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02146.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02147.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02147.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02147.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02149.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02149.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02149.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02150.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02150.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02150.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02151.java:71	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02151.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02151.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02154.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02154.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02154.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02155.java:52	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02155.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02155.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02156.java:52	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02156.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02156.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02243.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02243.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02243.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02249.java:62	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02249.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02249.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02250.java:62	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02250.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02250.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02251.java:74	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02251.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02251.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02252.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02252.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02252.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02253.java:76	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02253.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02253.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02334.java:76	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02334.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02334.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02335.java:76	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02335.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02335.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02340.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02340.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02340.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02341.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02341.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02341.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02342.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02342.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02342.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02344.java:66	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02344.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02344.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02411.java:63	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02413.java:63	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02414.java:61	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02431.java:56	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02432.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02496.java:65	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02496.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02496.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02511.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02511.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02511.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02512.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02512.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02512.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02513.java:58	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02513.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02513.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02516.java:55	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02516.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02516.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02518.java:55	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02518.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02518.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02610.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02610.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02610.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02613.java:66	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02613.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02613.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00012.java:65	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00012.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00012.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00021.java:59	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00021.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00021.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00044.java:62	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00044.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00044.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00138.java:71	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00138.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00138.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00530.java:95	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00530.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00530.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00630.java:82	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00694.java:63	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00694.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00694.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00695.java:68	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00695.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00695.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00959.java:69	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00959.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00959.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01023.java:61	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01023.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01023.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01024.java:61	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01024.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01024.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01154.java:63	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01154.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01154.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01243.java:60	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01243.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01243.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01402.java:72	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01402.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01402.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01490.java:59	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01492.java:59	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01501.java:61	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01832.java:67	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01832.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01832.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01902.java:61	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01902.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01902.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01903.java:61	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01903.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01903.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02025.java:63	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02025.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02025.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02036.java:65	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02036.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02036.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02037.java:65	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02037.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02037.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02104.java:58	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02104.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02104.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02114.java:60	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02114.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02114.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02116.java:60	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02116.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02116.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02196.java:63	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02196.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02196.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02208.java:65	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02208.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02208.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02305.java:74	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02305.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02305.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02376.java:59	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02384.java:61	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02571.java:74	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02571.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02571.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02572.java:74	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02572.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02572.java:43	SCA

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00008.java:53	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00008.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00008.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00018.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00018.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00018.java:46	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00024.java:53	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00024.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00024.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00027.java:53	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00027.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00027.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00034.java:58	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00034.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00034.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00037.java:67	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00037.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00037.java:47	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00043.java:54	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00100.java:68	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00100.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00100.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00101.java:73	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00101.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00101.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00105.java:69	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00105.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00105.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00106.java:73	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00106.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00106.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00108.java:82	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00108.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00108.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00111.java:73	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00111.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00111.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00112.java:64	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00112.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00112.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00114.java:69	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00114.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00114.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00115.java:68	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00115.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00115.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00190.java:67	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00190.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00190.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00191.java:76	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00191.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00191.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00192.java:76	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00192.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00192.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00193.java:63	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00193.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00193.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00203.java:63	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00203.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00203.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00204.java:58	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00204.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00204.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00205.java:67	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00205.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00205.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00328.java:65	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00328.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00328.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00329.java:65	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00329.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00329.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00333.java:65	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00333.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00333.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00335.java:65	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00335.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00335.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00342.java:69	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00342.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00342.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00343.java:65	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00343.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00343.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00344.java:65	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00344.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00344.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00428.java:64	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00428.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00428.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00429.java:60	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00429.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00429.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00430.java:60	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00430.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00430.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00435.java:59	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00435.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00435.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00436.java:60	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00436.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00436.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00437.java:60	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00437.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00437.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00438.java:60	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00438.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00438.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00439.java:54	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00439.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00439.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00441.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00441.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00441.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00510.java:78	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00510.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00510.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00512.java:59	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00512.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00512.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00514.java:65	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00514.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00514.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00515.java:69	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00515.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00515.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00516.java:78	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00516.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00516.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00517.java:65	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00517.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00517.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00518.java:60	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00518.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00518.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00589.java:78	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00589.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00589.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00590.java:74	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00590.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00590.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00591.java:69	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00591.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00591.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00593.java:87	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00593.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00593.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00594.java:73	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00594.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00594.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00595.java:74	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00595.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00595.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00601.java:74	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00601.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00601.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00602.java:78	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00602.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00602.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00603.java:69	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00603.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00603.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00605.java:74	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00605.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00605.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00606.java:74	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00606.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00606.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00672.java:61	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00673.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00675.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00676.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00681.java:55	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00682.java:74	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00760.java:62	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00760.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00760.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00761.java:76	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00761.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00761.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00762.java:63	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00762.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00762.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00763.java:76	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00763.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00763.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00770.java:67	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00770.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00770.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00771.java:62	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00771.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00771.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00772.java:76	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00772.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00772.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00773.java:67	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00773.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00773.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00774.java:76	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00774.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00774.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00838.java:87	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00838.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00838.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00839.java:74	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00839.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00839.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00847.java:78	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00847.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00847.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00848.java:68	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00848.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00848.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00849.java:78	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00849.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00849.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00850.java:78	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00850.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00850.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00851.java:74	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00851.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00851.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00997.java:61	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00997.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00997.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00998.java:61	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00998.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00998.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00999.java:61	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00999.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00999.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01001.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01001.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01001.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01002.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01002.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01002.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01003.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01003.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01003.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01004.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01004.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01004.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01011.java:61	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01011.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01011.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01012.java:61	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01012.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01012.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01083.java:55	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01083.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01083.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01084.java:55	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01084.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01084.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01090.java:55	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01090.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01090.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01091.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01091.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01091.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01092.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01092.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01092.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01093.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01093.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01093.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01094.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01094.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01094.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01095.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01095.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01095.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01096.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01096.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01096.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01097.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01097.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01097.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01098.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01098.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01098.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01208.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01208.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01208.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01209.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01209.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01209.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01210.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01210.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01210.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01211.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01211.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01211.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01212.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01212.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01212.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01213.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01213.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01213.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01216.java:57	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01216.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01216.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01218.java:57	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01218.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01218.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01220.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01220.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01220.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01222.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01222.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01222.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01303.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01303.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01303.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01304.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01304.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01304.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01305.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01305.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01305.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01307.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01307.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01307.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01310.java:52	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01310.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01310.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01311.java:52	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01311.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01311.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01312.java:52	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01312.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01312.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01313.java:52	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01313.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01313.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01314.java:52	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01314.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01314.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01315.java:52	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01315.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01315.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01379.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01379.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01379.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01380.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01380.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01380.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01381.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01381.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01381.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01382.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01382.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01382.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01383.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01383.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01383.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01384.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01384.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01384.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01385.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01385.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01385.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01391.java:57	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01391.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01391.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01392.java:57	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01392.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01392.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01394.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01394.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01394.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01395.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01395.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01395.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01396.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01396.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01396.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01459.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01459.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01459.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01460.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01460.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01460.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01462.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01462.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01462.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01463.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01463.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01463.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01464.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01464.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01464.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01473.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01473.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01473.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01475.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01475.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01475.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01476.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01476.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01476.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01477.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01477.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01477.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01552.java:53	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01557.java:53	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01558.java:53	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01559.java:53	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01560.java:53	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01620.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01620.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01620.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01621.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01621.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01621.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01622.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01622.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01622.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01623.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01623.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01623.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01626.java:55	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01626.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01626.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01627.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01627.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01627.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01628.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01628.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01628.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01629.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01629.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01629.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01631.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01631.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01631.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01712.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01712.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01712.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01714.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01714.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01714.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01715.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01715.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01715.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01716.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01716.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01716.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01717.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01717.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01717.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01718.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01718.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01718.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01719.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01719.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01719.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01728.java:66	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01728.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01728.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01729.java:66	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01729.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01729.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01730.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01730.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01730.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01731.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01731.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01731.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01732.java:66	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01732.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01732.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01733.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01733.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01733.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01877.java:61	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01877.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01877.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01878.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01878.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01878.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01879.java:61	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01879.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01879.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01885.java:61	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01885.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01885.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01887.java:61	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01887.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01887.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01888.java:61	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01888.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01888.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01889.java:61	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01889.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01889.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01890.java:61	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01890.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01890.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01891.java:61	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01891.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01891.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01969.java:55	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01969.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01969.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01970.java:55	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01970.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01970.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01971.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01971.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01971.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01972.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01972.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01972.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01973.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01973.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01973.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02087.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02087.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02087.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02088.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02088.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02088.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02089.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02089.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02089.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02092.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02092.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02092.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02093.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02093.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02093.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02094.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02094.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02094.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02098.java:57	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02098.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02098.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02169.java:52	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02169.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02169.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02172.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02172.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02172.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02173.java:52	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02173.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02173.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02185.java:52	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02185.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02185.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02186.java:52	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02186.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02186.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02187.java:52	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02187.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02187.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02264.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02264.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02264.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02265.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02265.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02265.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02266.java:57	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02266.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02266.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02267.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02267.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02267.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02269.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02269.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02269.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02270.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02270.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02270.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02271.java:57	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02271.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02271.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02283.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02283.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02283.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02284.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02284.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02284.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02285.java:57	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02285.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02285.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02287.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02287.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02287.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02288.java:57	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02288.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02288.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02353.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02353.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02353.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02354.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02354.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02354.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02355.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02355.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02355.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02364.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02364.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02364.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02365.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02365.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02365.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02366.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02366.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02366.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02368.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02368.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02368.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02369.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02369.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02369.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02449.java:53	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02450.java:53	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02454.java:53	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02455.java:53	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02456.java:53	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02528.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02528.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02528.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02530.java:55	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02530.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02530.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02531.java:55	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02531.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02531.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02533.java:55	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02533.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02533.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02534.java:55	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02534.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02534.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02541.java:55	**Sink:** java.sql.Statement.addBatch() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02541.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02541.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02542.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02542.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02542.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02543.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02543.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02543.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02544.java:55	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02544.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02544.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02545.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02545.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02545.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02546.java:55	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02546.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02546.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02625.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02625.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02625.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02626.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02626.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02626.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02628.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02628.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02628.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02629.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02629.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02629.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02630.java:66	**Sink:** java.sql.Connection.prepareCall() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02630.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02630.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02631.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02631.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02631.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02632.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02632.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02632.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02634.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02634.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02634.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02635.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02635.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02635.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02636.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02636.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02636.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02637.java:66	**Sink:** java.sql.Connection.prepareStatement() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02637.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02637.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02649.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02649.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02649.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02650.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02650.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02650.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02651.java:66	**Sink:** java.sql.Statement.execute() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02651.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02651.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02653.java:66	**Sink:** java.sql.Statement.executeQuery() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02653.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02653.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02654.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02654.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02654.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02655.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02655.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02655.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

SQL Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02656.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02656.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02656.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02657.java:66	**Sink:** java.sql.Statement.executeUpdate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02657.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02657.java:43	SCA

XPath Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00117.java:76	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00117.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00117.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00118.java:75	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00118.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00118.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00442.java:66	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00442.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00442.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00520.java:71	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00520.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00520.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XPath Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00683.java:68	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01013.java:68	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01013.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01013.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01014.java:67	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01014.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01014.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01223.java:64	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01223.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01223.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01224.java:63	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01224.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01224.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01225.java:63	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01225.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01225.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01316.java:58	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01316.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01316.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XPath Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01397.java:63	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01397.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01397.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01478.java:73	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01478.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01478.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01479.java:73	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01479.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01479.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01561.java:60	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01562.java:60	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01632.java:62	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01632.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01632.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01734.java:73	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01734.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01734.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XPath Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01735.java:73	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01735.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01735.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01736.java:72	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01736.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01736.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01892.java:68	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01892.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01892.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01893.java:68	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01893.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01893.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01894.java:67	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01894.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01894.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01974.java:62	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01974.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01974.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02100.java:64	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02100.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02100.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XPath Injection	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02189.java:59	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02189.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02189.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02370.java:73	**Sink:** javax.xml.xpath.XPath.compile() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02370.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02370.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02457.java:59	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

Command Injection	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00159.java:66	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00159.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00159.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00174.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00174.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00174.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00568.java:88	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00568.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00568.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00576.java:75	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00576.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00576.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00825.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00825.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00825.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01191.java:60	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01191.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01191.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01441.java:83	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01441.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01441.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01674.java:74	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01674.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01674.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02244.java:65	**Sink:** java.lang.ProcessBuilder.ProcessBuilder() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02244.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02244.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02333.java:76	**Sink:** java.lang.ProcessBuilder.command() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02333.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02333.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Command Injection	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02343.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02343.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02343.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02429.java:70	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02433.java:72	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02515.java:57	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02515.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02515.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02517.java:55	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02517.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02517.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02611.java:85	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02611.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02611.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02612.java:69	**Sink:** java.lang.Runtime.exec() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02612.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02612.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00016.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00016.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00016.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00087.java:75	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00087.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00087.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00088.java:71	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00088.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00088.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00089.java:77	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00089.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00089.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00169.java:75	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00169.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00169.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00170.java:79	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00170.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00170.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00241.java:82	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00241.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00241.java:45	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00242.java:86	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00242.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00242.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00300.java:71	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00300.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00300.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00348.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getInputStream() **from** org.owasp.benchmark.testcode.BenchmarkTest00348.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00348.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00403.java:68	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00403.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00403.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00404.java:66	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00404.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00404.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00405.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00405.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00405.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00491.java:71	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00491.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00491.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00565.java:76	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00565.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00565.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00566.java:77	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00566.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00566.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00655.java:67	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00736.java:71	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00736.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00736.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00820.java:76	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00820.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00820.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00821.java:77	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00821.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00821.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00977.java:69	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00977.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00977.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01061.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01061.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01061.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01062.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01062.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01062.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01134.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01134.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01134.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01185.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01185.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01185.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01186.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01186.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01186.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01187.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01187.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01187.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01280.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01280.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01280.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01281.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01281.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01281.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01282.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01282.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01282.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01283.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01283.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01283.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01359.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01359.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01359.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01436.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01436.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01436.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01521.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01522.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01523.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01524.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01604.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01604.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01604.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01605.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01605.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01605.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01682.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01682.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01682.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01683.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01683.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01683.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01684.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01684.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01684.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01861.java:69	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01861.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01861.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01862.java:69	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01862.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01862.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01863.java:69	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01863.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01863.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01935.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01935.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01935.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02005.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02005.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02005.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02006.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02006.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02006.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02064.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02064.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02064.java:44	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02065.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02065.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02065.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02066.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02066.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02066.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02142.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02142.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02142.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02143.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02143.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02143.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02144.java:60	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02144.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02144.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02247.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02247.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02247.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02248.java:65	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02248.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02248.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Header Manipulation: Cookies		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02339.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02339.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02339.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02427.java:61	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02507.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02507.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02507.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02508.java:63	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02508.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02508.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02607.java:74	**Sink:** javax.servlet.http.Cookie.Cookie() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02607.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02607.java:43	SCA

LDAP Injection		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00947.java:67	**Sink:** javax.naming.directory.DirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00947.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00947.java:43	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

LDAP Injection		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01242.java:60	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01242.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01242.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02306.java:74	**Sink:** javax.naming.directory.InitialDirContext.search() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02306.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02306.java:45	SCA

XML Entity Expansion Injection		High
Package: org.owasp.benchmark.score		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:1312	**Sink:** docBuilder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** getXMLDocument() **Source:**	SCA
Package: org.owasp.benchmark.score.parsers		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/parsers/XanitizerReader.java:140	**Sink:** factory.setFeature(...) : External entity resolution allowed **Enclosing Method:** parse() **Source:**	SCA
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00116.java:69	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XML Entity Expansion Injection	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00117.java:69	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00118.java:69	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00207.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00442.java:60	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00520.java:65	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00607.java:69	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00683.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00852.java:74	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00941.java:58	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XML Entity Expansion Injection		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01013.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01014.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01223.java:57	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01224.java:57	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01225.java:57	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01316.java:52	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01397.java:57	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01478.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01479.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XML Entity Expansion Injection	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01561.java:53	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01562.java:53	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01632.java:55	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01633.java:55	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01734.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01735.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01736.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01821.java:52	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01892.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XML Entity Expansion Injection		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01893.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01894.java:61	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01974.java:55	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02100.java:57	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02189.java:52	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02370.java:66	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02457.java:53	**Sink:** builder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** doPost() **Source:**	SCA
Package: org.owasp.benchmark.tools		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/tools/BenchmarkCrawler.java:83	**Sink:** docBuilder.parse(...) : XML document parsed allowing external entity resolution **Enclosing Method:** parseHttpFile() **Source:**	SCA

A1 Injection

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

XML Entity Expansion Injection		High
Package: org.owasp.benchmark.tools		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/tools/NoisyCricket.java:72	**Sink:** transformerFactory.newTransformer() : XML document parsed allowing external entity resolution **Enclosing Method:** main() **Source:**	SCA

XPath Injection		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00607.java:75	**Sink:** javax.xml.xpath.XPath.evaluate() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00607.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00607.java:45	SCA

A2 Broken Authentication and Session Management

Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.

No Issues

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00013.java:53	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00013.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00013.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00014.java:53	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00014.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00014.java:46	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00030.java:55	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00030.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00030.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00036.java:66	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00036.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00036.java:47	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00041.java:53	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00047.java:64	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00047.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00047.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00048.java:63	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00048.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00048.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00049.java:63	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00049.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00049.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00144.java:62	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00144.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00144.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00145.java:57	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00145.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00145.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00146.java:56	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00146.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00146.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00147.java:61	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00147.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00147.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00148.java:58	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00148.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00148.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00149.java:53	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00149.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00149.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00150.java:58	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00150.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00150.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00151.java:62	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00151.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00151.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00152.java:70	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00152.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00152.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00153.java:56	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00153.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00153.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00154.java:70	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00154.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00154.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00155.java:52	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00155.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00155.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00156.java:61	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00156.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00156.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00157.java:57	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00157.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00157.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00276.java:61	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00276.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00276.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00279.java:65	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00279.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00279.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00280.java:74	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00280.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00280.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00281.java:62	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00281.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00281.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00284.java:55	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00284.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00284.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00287.java:58	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00287.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00287.java:44	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00290.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00290.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00290.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00291.java:58	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00291.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00291.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00292.java:61	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00292.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00292.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00301.java:60	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00301.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00301.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00362.java:57	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.testcode.BenchmarkTes t00362.doPost() **In** Desktop/Benchmark/Benchmark-1 .2beta/src/main/java/org/owasp/benchmark/testcode /BenchmarkTest00362.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00375.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.testcode.BenchmarkTes t00375.doPost() **In** Desktop/Benchmark/Benchmark-1 .2beta/src/main/java/org/owasp/benchmark/testcode /BenchmarkTest00375.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00376.java:57	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.testcode.BenchmarkTes t00376.doPost() **In** Desktop/Benchmark/Benchmark-1 .2beta/src/main/java/org/owasp/benchmark/testcode /BenchmarkTest00376.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00377.java:61	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00377.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00377.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00378.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00378.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00378.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00380.java:69	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00380.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00380.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00382.java:61	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00382.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00382.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00384.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00384.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00384.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00387.java:56	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00387.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00387.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00388.java:51	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00388.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00388.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00392.java:57	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00392.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00392.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00393.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00393.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00393.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00394.java:63	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00394.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00394.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00395.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00395.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00395.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00457.java:72	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00457.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00457.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00458.java:81	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00458.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00458.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00467.java:61	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00467.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00467.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00469.java:62	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00469.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00469.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00472.java:62	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00472.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00472.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00475.java:61	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00475.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00475.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00476.java:61	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00476.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00476.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00477.java:56	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00477.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00477.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00492.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test00492.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest00492.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00542.java:84	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00542.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00542.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00543.java:75	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00543.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00543.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00544.java:74	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00544.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00544.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00546.java:74	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00546.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00546.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00547.java:66	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00547.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00547.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00549.java:70	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00549.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00549.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00550.java:74	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00550.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00550.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00551.java:64	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00551.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00551.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00552.java:69	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00552.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00552.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00553.java:83	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00553.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00553.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00554.java:70	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00554.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00554.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00555.java:70	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00555.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00555.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00556.java:83	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00556.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00556.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00557.java:68	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00557.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00557.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00626.java:68	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00642.java:61	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00643.java:52	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00644.java:52	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00645.java:53	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00646.java:61	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00651.java:60	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00656.java:57	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00711.java:66	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00711.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00711.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00712.java:62	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00712.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00712.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00715.java:54	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00715.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00715.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00719.java:55	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00719.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00719.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00720.java:73	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00720.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00720.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00721.java:64	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00721.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00721.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00723.java:60	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00723.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00723.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00724.java:72	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00724.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00724.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00727.java:56	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00727.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00727.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00728.java:59	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00728.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00728.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00729.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest00729.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest00729.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00799.java:77	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00799.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00799.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00800.java:84	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00800.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00800.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00801.java:65	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00801.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00801.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00803.java:64	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00803.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00803.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00804.java:65	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00804.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00804.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00806.java:75	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00806.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00806.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00807.java:66	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00807.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00807.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00808.java:75	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00808.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00808.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00809.java:71	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00809.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00809.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00810.java:65	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest00810.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00810.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00811.java:83	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00811.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00811.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00812.java:70	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00812.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00812.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00813.java:73	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00813.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00813.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00822.java:70	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00822.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00822.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01033.java:58	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01033.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01033.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01046.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01046.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01046.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01047.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01047.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01047.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01049.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01049.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01049.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01050.java:49	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01050.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01050.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01051.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01051.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01051.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01052.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01052.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01052.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01053.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01053.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01053.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01055.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01055.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01055.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01056.java:52	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01056.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01056.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01057.java:49	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01057.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01057.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01171.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01171.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01171.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01172.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01172.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01172.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01173.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01173.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01173.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01174.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01174.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01174.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01176.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01176.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01176.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01177.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01177.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01177.java:44	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01178.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01178.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01178.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01179.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01179.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01179.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01180.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01180.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01180.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01252.java:49	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01252.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01252.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01253.java:49	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01253.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01253.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01256.java:48	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01256.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01256.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01257.java:48	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01257.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01257.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01259.java:49	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01259.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01259.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01260.java:49	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01260.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01260.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01262.java:48	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01262.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01262.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01263.java:48	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01263.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01263.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01265.java:51	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01265.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01265.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01266.java:51	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01266.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01266.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01267.java:48	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01267.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01267.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01284.java:48	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01284.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01284.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01330.java:60	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01330.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01330.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01335.java:56	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01335.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01335.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01336.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01336.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01336.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01337.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01337.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01337.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01338.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01338.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01338.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01343.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01343.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01343.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01344.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01344.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01344.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01345.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01345.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01345.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01346.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01346.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01346.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01349.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01349.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01349.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01350.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test01350.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest01350.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01417.java:65	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01417.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01417.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01419.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01419.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01419.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01421.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01421.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01421.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01423.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01423.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01423.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01424.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01424.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01424.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01425.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01425.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01425.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01426.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01426.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01426.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01427.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01427.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01427.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01428.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01428.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01428.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01429.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01429.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01429.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01437.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest01437.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest01437.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01497.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01505.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01506.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01507.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01508.java:49	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01509.java:49	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01510.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01511.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01512.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01513.java:49	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01525.java:49	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01583.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01583.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01583.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01584.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01584.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01584.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01587.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01587.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01587.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01588.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01588.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01588.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01589.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01589.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01589.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01590.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01590.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01590.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01592.java:51	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01592.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01592.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01593.java:51	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01593.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01593.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01594.java:51	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01594.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01594.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01596.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01596.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01596.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01597.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01597.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01597.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01657.java:65	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01657.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01657.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01658.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01658.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01658.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01660.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01660.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01660.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01665.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01665.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01665.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01666.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01666.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01666.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01667.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01667.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01667.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01670.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01670.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01670.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01840.java:64	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01840.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01840.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01906.java:58	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01906.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01906.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01907.java:58	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01907.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01907.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01914.java:52	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01914.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01914.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01915.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01915.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01915.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01916.java:49	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01916.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01916.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01918.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01918.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01918.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01919.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01919.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01919.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01920.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01920.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01920.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01921.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01921.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01921.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01922.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01922.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01922.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01923.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01923.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01923.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01925.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01925.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01925.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01926.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01926.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01926.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02045.java:56	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02045.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02045.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02046.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02046.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02046.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02047.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02047.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02047.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02050.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02050.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02050.java:44	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02051.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02051.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02051.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02053.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02053.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02053.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02054.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02054.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02054.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02055.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02055.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02055.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02056.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02056.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02056.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02057.java:56	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest02057.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest02057.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02110.java:55	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.testcode.BenchmarkTes t02110.doPost() **In** Desktop/Benchmark/Benchmark-1 .2beta/src/main/java/org/owasp/benchmark/testcode /BenchmarkTest02110.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02122.java:51	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02122.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02122.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02123.java:49	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02123.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02123.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02124.java:48	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02124.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02124.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02127.java:48	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02127.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02127.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02128.java:48	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02128.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02128.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02129.java:49	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02129.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02129.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02130.java:49	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02130.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02130.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02131.java:49	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02131.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02131.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02133.java:48	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02133.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02133.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02134.java:48	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02134.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02134.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02136.java:51	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02136.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02136.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02221.java:56	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02221.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02221.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02222.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02222.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02222.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02223.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02223.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02223.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02224.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02224.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02224.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02225.java:54	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02225.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02225.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02226.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02226.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02226.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02227.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02227.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02227.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02228.java:53	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02228.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02228.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02230.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02230.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02230.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02232.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02232.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02232.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02233.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02233.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02233.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02234.java:54	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02234.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02234.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02235.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02235.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02235.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02236.java:53	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02236.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02236.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02239.java:53	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02239.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02239.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02240.java:53	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02240.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02240.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02241.java:53	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Map() **from** org.owasp.benchmark.testcode.Benchmark Test02241.doPost() **In** Desktop/Benchmark/Benchmar k-1.2beta/src/main/java/org/owasp/benchmark/testc ode/BenchmarkTest02241.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02314.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02314.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02314.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02315.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02315.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02315.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02316.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02316.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02316.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02317.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02317.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02317.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02319.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02319.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02319.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02322.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02322.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02322.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02323.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02323.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02323.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02324.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02324.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02324.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02325.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02325.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02325.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02327.java:65	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02327.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02327.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02328.java:65	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02328.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02328.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02329.java:65	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02329.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02329.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02330.java:65	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02330.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02330.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02332.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest02332.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest02332.java:45	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02395.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02397.java:50	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02399.java:49	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02400.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02402.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02404.java:50	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02405.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02406.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02407.java:49	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02409.java:52	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02410.java:52	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02480.java:51	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02480.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02480.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02481.java:51	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02481.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02481.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02482.java:51	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02482.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02482.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02483.java:51	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02483.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02483.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02485.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02485.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02485.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02486.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02486.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02486.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02487.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02487.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02487.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02489.java:52	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02489.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02489.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02493.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02493.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02493.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02494.java:51	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02494.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02494.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02495.java:54	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02495.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02495.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02509.java:51	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02509.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02509.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02578.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02578.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02578.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02579.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02579.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02579.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02580.java:63	**Sink:** java.io.PrintWriter.format() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02580.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02580.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02582.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02582.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02582.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02583.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02583.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02583.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02584.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02584.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02584.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02585.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02585.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02585.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02586.java:62	**Sink:** java.io.PrintWriter.print() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02586.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02586.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02589.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02589.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02589.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02591.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02591.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02591.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02592.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02592.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02592.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02593.java:63	**Sink:** java.io.PrintWriter.printf() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02593.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02593.java:43	SCA

A3 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Cross-Site Scripting: Reflected		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02594.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02594.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02594.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02595.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02595.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02595.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02597.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02597.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02597.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02598.java:62	**Sink:** java.io.PrintWriter.println() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02598.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02598.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02599.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02599.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02599.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02600.java:65	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02600.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02600.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02608.java:62	**Sink:** java.io.PrintWriter.write() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02608.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02608.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.score		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:958	**Sink:** java.io.File.File() **Enclosing Method:** produceResultsFile() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:958	**Sink:** java.io.File.File() **Enclosing Method:** produceResultsFile() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.parsers.ContrastReader.parse() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/parsers/ContrastReader.java:48	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:1026	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** generateVulnerabilityScorecards() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:1106	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** generateVulnerabilityScorecards() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:215	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:139	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:215	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:136	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:221	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:139	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.score		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:221	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:136	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:229	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:139	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:229	**Sink:** java.io.File.File() **Enclosing Method:** resultsFileName() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.WriteFiles.getLine() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/WriteTime.java:136	SCA
Package: org.owasp.benchmark.score.report		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:75	**Sink:** java.io.File.File() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:75	**Sink:** java.io.File.File() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.parsers.ContrastReader.parse() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/parsers/ContrastReader.java:48	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:81	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:81	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.parsers.ContrastReader.parse() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/parsers/ContrastReader.java:48	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.score.report		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:82	**Sink:** java.io.File.File() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.parsers.ContrastReader.parse() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/parsers/ContrastReader.java:48	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/Report.java:82	**Sink:** java.io.File.File() **Enclosing Method:** Report() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/report/ScatterVulns.java:385	**Sink:** java.io.File.File() **Enclosing Method:** generateComparisonChart() **Source:** java.io.BufferedReader.readLine() **from** org.owasp.benchmark.score.BenchmarkScore.readExpectedResults() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/score/BenchmarkScore.java:876	SCA
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00001.java:63	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00001.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00001.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00002.java:64	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00002.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00002.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00011.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00011.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00011.java:46	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00028.java:60	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00028.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00028.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00040.java:50	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00045.java:65	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00045.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00045.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00062.java:69	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00062.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00062.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00063.java:70	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00063.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00063.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00064.java:71	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00064.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00064.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00131.java:72	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00131.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00131.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00132.java:77	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00132.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00132.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00133.java:64	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00133.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00133.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00134.java:76	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00134.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00134.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00135.java:85	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00135.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00135.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00136.java:78	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest00136.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00136.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00215.java:64	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00215.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00215.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00216.java:70	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00216.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00216.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00218.java:94	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get HeaderNames() **from** org.owasp.benchmark.testcode.B enchmarkTest00218.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00218.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00219.java:75	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get HeaderNames() **from** org.owasp.benchmark.testcode.B enchmarkTest00219.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00219.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00221.java:76	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get HeaderNames() **from** org.owasp.benchmark.testcode.B enchmarkTest00221.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00221.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00222.java:89	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get HeaderNames() **from** org.owasp.benchmark.testcode.B enchmarkTest00222.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest00222.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00262.java:74	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00262.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00262.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00263.java:79	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00263.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00263.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00264.java:66	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Headers() **from** org.owasp.benchmark.testcode.Bench markTest00264.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest00264.java:44	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00265.java:71	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest00265.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00265.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00359.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00359.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00359.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00361.java:74	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00361.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00361.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00362.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00362.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00362.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00363.java:63	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00363.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00363.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00364.java:66	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00364.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00364.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00366.java:73	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest00366.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00366.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00454.java:66	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00454.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00454.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00456.java:65	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00456.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00456.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00457.java:71	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00457.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00457.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00458.java:80	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest00458.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00458.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00525.java:74	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00525.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00525.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00526.java:64	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00526.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00526.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00528.java:80	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00528.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00528.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00529.java:69	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Names() **from** org.owasp.benchmark.testcode.Benchma rkTest00529.doPost() **In** Desktop/Benchmark/Benchm ark-1.2beta/src/main/java/org/owasp/benchmark/tes tcode/BenchmarkTest00529.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00619.java:61	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00620.java:61	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00622.java:70	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00625.java:63	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00626.java:67	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00629.java:61	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter () **from** org.owasp.benchmark.helpers.SeparateClass Request.getTheParameter() **In** Desktop/Benchmark/B enchmark-1.2beta/src/main/java/org/owasp/benchmar k/helpers/SeparateClassRequest.java:33	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00696.java:72	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00696.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00696.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00699.java:72	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00699.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00699.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00783.java:74	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00783.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00783.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00784.java:88	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00784.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00784.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00785.java:75	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00785.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00785.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00949.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00949.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00949.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00950.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00950.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00950.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00951.java:68	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00951.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00951.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00952.java:68	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00952.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00952.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00953.java:70	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00953.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00953.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00955.java:70	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00955.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00955.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00956.java:70	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00956.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00956.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00957.java:61	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest00957.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00957.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01027.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01027.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01027.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01028.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01028.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01028.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01030.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01030.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01030.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01031.java:56	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01031.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01031.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01032.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01032.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01032.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01035.java:57	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01035.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01035.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01110.java:73	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01110.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01110.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01111.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01111.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01111.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01112.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01112.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01112.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01116.java:75	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01116.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01116.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01155.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01155.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01155.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01156.java:64	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01156.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01156.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01157.java:64	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01157.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01157.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01158.java:58	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01158.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01158.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01160.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01160.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01160.java:44	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01161.java:59	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest01161.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01161.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01231.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01231.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01231.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01233.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01233.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01233.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01235.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01235.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01235.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01237.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01237.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01237.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01238.java:54	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01238.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01238.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01239.java:61	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01239.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01239.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01240.java:54	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01240.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01240.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01329.java:64	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01329.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01329.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01330.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01330.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01330.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01331.java:59	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest01331.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01331.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01405.java:67	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01405.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01405.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01406.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01406.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01406.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01407.java:75	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01407.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01407.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01494.java:49	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01495.java:60	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01496.java:54	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01497.java:55	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01499.java:55	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01500.java:53	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01570.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01570.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01570.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01571.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01571.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01571.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01573.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest01573.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest01573.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01643.java:73	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01643.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01643.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01644.java:67	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01644.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01644.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01645.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01645.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01645.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01647.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest01647.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest01647.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01833.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get Cookies() **from** org.owasp.benchmark.testcode.Bench markTest01833.doPost() **In** Desktop/Benchmark/Benc hmark-1.2beta/src/main/java/org/owasp/benchmark/t estcode/BenchmarkTest01833.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01834.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01834.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01834.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01835.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01835.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01835.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01836.java:68	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01836.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01836.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01837.java:68	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01837.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01837.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01838.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01838.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01838.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01839.java:63	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01839.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01839.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01840.java:63	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getCookies() **from** org.owasp.benchmark.testcode.BenchmarkTest01840.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01840.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01904.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01904.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01904.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01906.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01906.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01906.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01907.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01907.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01907.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01908.java:55	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01908.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01908.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01983.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01983.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01983.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01987.java:73	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01987.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01987.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01989.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01989.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01989.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01990.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaderNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01990.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01990.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02026.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02026.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02026.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02027.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02027.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02027.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02028.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02028.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02028.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02031.java:58	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02031.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02031.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02032.java:58	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02032.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02032.java:44	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02033.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02033.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02033.java:44	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02034.java:66	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02034.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02034.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02035.java:57	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeaders() **from** org.owasp.benchmark.testcode.BenchmarkTest02035.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02035.java:44	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02105.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02105.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02105.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02107.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02107.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02107.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02110.java:54	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02110.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02110.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02111.java:61	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02111.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02111.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02112.java:54	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02112.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02112.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02113.java:52	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest02113.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02113.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02197.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02197.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02197.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02198.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02198.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02198.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02199.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02199.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02199.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02200.java:53	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02200.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02200.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02201.java:58	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02201.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02201.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02202.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02202.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02202.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02204.java:66	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02204.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02204.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02205.java:59	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02205.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02205.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02206.java:57	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02206.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02206.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02207.java:57	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterMap() **from** org.owasp.benchmark.testcode.BenchmarkTest02207.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02207.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02301.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02301.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02301.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02303.java:67	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02303.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02303.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02304.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02304.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02304.java:45	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02377.java:49	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02379.java:60	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02382.java:55	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02383.java:55	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02462.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02462.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02462.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02463.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02463.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02463.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02464.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest02464.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02464.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02465.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02465.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02465.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02466.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02466.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02466.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02468.java:64	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02468.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02468.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02470.java:57	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02470.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02470.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02471.java:55	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter Values() **from** org.owasp.benchmark.testcode.Benchm arkTest02471.doPost() **In** Desktop/Benchmark/Bench mark-1.2beta/src/main/java/org/owasp/benchmark/te stcode/BenchmarkTest02471.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02554.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02554.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02554.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02556.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.get QueryString() **from** org.owasp.benchmark.testcode.B enchmarkTest02556.doPost() **In** Desktop/Benchmark/ Benchmark-1.2beta/src/main/java/org/owasp/benchma rk/testcode/BenchmarkTest02556.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		Critical
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02557.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02557.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02557.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02558.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02558.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02558.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02560.java:67	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02560.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02560.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02561.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02561.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02561.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02562.java:67	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02562.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02562.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02564.java:68	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02564.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02564.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02566.java:75	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02566.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02566.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation	Critical
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02567.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02567.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02567.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02568.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02568.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02568.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02569.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02569.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02569.java:43	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02570.java:66	**Sink:** java.nio.file.Paths.get() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02570.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02570.java:43	SCA

Path Manipulation	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00527.java:65	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest00527.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00527.java:45	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00624.java:58	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00698.java:54	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest00698.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00698.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00788.java:71	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest00788.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00788.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01025.java:51	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01025.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01025.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01029.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01029.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01029.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01033.java:57	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getHeader() **from** org.owasp.benchmark.testcode.BenchmarkTest01033.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01033.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01232.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01232.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01232.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01234.java:48	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01234.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01234.java:43	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01236.java:59	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.testcode.BenchmarkTest01236.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01236.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01403.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01403.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01403.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01408.java:68	**Sink:** java.io.FileOutputStream.FileOutputStream() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest01408.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01408.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01572.java:56	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterValues() **from** org.owasp.benchmark.testcode.BenchmarkTest01572.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01572.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01642.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest01642.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest01642.java:43	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02302.java:62	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameterNames() **from** org.owasp.benchmark.testcode.BenchmarkTest02302.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02302.java:45	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02378.java:60	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.ServletRequest.getParameter() **from** org.owasp.benchmark.helpers.SeparateClassRequest.getTheParameter() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/SeparateClassRequest.java:33	SCA

A4 Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Path Manipulation		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02559.java:73	**Sink:** java.io.File.File() **Enclosing Method:** doPost() **Source:** javax.servlet.http.HttpServletRequest.getQueryString() **from** org.owasp.benchmark.testcode.BenchmarkTest02559.doPost() **In** Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest02559.java:43	SCA

A5 Security Misconfiguration

Having a strong server configuration standard is critical to a secure web application. Servers have many configuration options that affect security and many are not secure out of the box.

No Issues

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00021.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00022.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00026.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00027.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00031.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00032.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00041.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00042.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00046.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00047.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00048.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00049.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00050.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00348.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00352.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00353.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00357.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00358.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00362.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00363.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00367.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00368.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00372.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00373.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00377.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00378.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00382.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00383.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00387.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00388.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00392.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00393.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00397.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00398.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00402.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00403.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00407.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00408.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00412.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00413.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00417.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00418.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00422.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00423.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00427.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00428.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00432.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00433.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00437.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00438.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00442.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00443.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00447.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00448.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00452.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00453.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00457.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00458.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00462.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00463.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00467.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00468.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00472.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00473.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00477.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00478.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00482.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00483.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00487.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00488.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00492.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00493.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00497.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00498.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00502.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00503.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00507.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00508.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00512.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00513.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00517.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00518.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00609.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00610.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00614.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00615.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00619.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00620.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00624.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00625.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00629.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00630.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00634.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00635.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00639.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00640.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00644.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00645.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00649.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00650.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00654.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00655.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00659.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00660.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00664.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00665.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00669.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00670.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00674.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00675.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00679.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00680.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00684.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00685.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00689.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00690.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00694.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00695.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00699.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00700.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00704.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00705.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00709.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00710.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00714.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00715.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00719.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00720.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00724.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00725.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00729.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00730.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00734.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00735.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00739.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00740.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00744.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00745.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00749.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00750.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00754.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00755.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00759.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00760.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00764.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00765.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00769.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00770.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00774.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00775.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00776.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00777.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00778.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00779.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00780.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00781.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00782.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00783.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00784.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00785.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00786.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00787.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00788.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00789.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00790.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00791.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00792.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00793.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00794.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00795.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00796.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00797.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00798.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00799.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00800.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00801.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00802.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00803.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00804.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00805.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00806.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00807.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00808.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00809.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00810.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00811.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00812.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00813.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00814.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00815.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00816.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00817.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00818.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00819.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00820.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00821.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00822.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00823.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00824.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00825.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00826.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00827.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00828.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00829.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00830.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00831.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00832.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00833.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00834.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00835.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00836.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00837.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00838.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00839.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00840.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00841.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00842.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00843.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00844.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest00845.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00846.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00847.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00848.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00849.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00850.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00851.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00852.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00853.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00857.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00858.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00862.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00863.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00867.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00868.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00872.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00873.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00877.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00878.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00882.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00883.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00887.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00888.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00892.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00893.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00897.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00898.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00902.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00903.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00907.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00908.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00912.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00913.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00917.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00918.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00922.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00923.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00927.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00928.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00932.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00933.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00937.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest00938.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01228.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01229.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01233.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01234.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01238.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01239.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01243.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01244.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01248.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01249.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01253.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01254.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01258.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01259.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01263.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01264.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01268.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01269.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01273.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01274.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01278.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01279.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01283.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01284.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01288.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01289.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01293.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01294.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01298.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01299.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01303.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01304.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01308.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01309.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01313.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01314.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01318.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01319.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01323.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01324.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01328.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01329.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01333.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01334.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01338.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01339.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01343.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01344.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01348.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01349.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01353.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01354.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01358.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01359.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01363.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01364.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01368.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01369.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01373.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01374.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01378.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01379.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01383.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01384.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01388.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01389.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01393.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01394.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01481.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01482.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01486.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01487.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01491.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01492.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01496.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01497.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01501.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01502.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01506.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01507.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01511.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01512.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01516.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01517.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01521.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01522.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01526.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01527.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01531.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01532.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01536.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01537.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01541.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01542.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01546.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01547.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01551.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01552.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01556.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01557.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01561.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01562.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01566.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01567.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01571.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01572.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01576.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01577.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01581.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01582.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01586.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01587.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01591.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01592.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01596.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01597.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01601.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01602.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01606.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01607.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01611.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01612.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01616.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01617.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01621.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01622.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01626.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01627.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01631.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01632.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01634.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01635.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01636.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01637.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01638.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01639.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01640.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01641.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01642.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01643.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01644.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01645.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01646.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01647.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01648.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01649.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01650.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01651.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01652.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01653.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01654.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01655.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01656.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01657.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01658.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01659.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01660.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01661.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01662.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01663.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01664.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01665.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01666.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01667.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01668.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01669.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01670.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01671.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01672.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01673.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01674.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01675.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01676.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01677.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01678.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01679.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01680.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01681.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01682.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01683.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01684.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01685.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01686.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01687.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01688.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01689.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01690.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01691.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01692.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01693.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01694.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01695.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01696.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01697.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01698.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01699.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01700.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01701.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01702.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01703.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01704.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01705.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01706.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01707.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01708.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01709.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01710.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01711.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01712.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01713.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01714.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01715.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01716.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01717.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01718.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01719.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01720.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest01721.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01722.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01723.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01724.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01725.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01726.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01727.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01728.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01729.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01730.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01731.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01732.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01733.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01734.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01735.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01736.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01737.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01741.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01742.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01746.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01747.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01751.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01752.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01756.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01757.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01761.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01762.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01766.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01767.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01771.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01772.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01776.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01777.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01781.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01782.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01786.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01787.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01791.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01792.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01796.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01797.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01801.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01802.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01806.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01807.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01811.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01812.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01816.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01817.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest01821.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02103.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02104.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02108.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02109.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02113.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02114.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02118.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02119.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02123.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02124.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02128.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02129.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02133.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02134.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02138.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02139.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02143.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02144.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02148.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02149.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02153.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02154.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02158.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02159.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02163.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02164.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02168.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02169.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02173.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02174.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02178.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02179.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02183.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02184.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02188.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02189.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02193.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02194.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02198.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02199.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02203.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02204.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02208.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02209.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02213.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02214.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02218.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02219.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02223.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02224.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02228.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02229.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02233.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02234.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02238.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02239.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02243.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02244.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02248.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02249.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02253.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02254.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02258.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02259.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02263.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02264.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02268.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02269.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02273.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02274.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02278.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02279.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02283.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02284.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02288.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02372.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02373.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02377.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02378.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02382.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02383.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02387.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02388.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02392.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02393.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02397.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02398.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02402.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02403.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02407.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02408.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02412.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02413.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02417.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02418.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02422.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02423.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02427.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02428.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02432.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02433.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02437.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02438.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02442.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02443.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02447.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02448.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02452.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02453.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02457.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02458.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02462.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02463.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02467.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02468.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02472.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02473.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02477.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02478.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02482.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02483.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02487.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02488.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02492.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02493.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02497.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02498.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02502.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02503.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02507.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02508.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02512.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02513.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02517.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02518.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02522.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02523.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02527.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02528.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02532.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02533.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02537.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02538.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02542.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02543.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02547.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02548.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02549.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02550.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02551.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02552.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02553.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02554.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02555.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02556.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02557.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02558.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02559.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02560.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02561.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02562.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02563.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02564.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02565.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02566.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02567.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02568.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02569.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02570.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02571.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02572.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02573.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02574.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02575.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02576.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02577.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02578.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02579.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02580.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02581.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02582.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02583.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02584.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02585.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02586.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02587.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02588.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02589.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02590.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02591.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02592.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02593.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02594.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02595.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02596.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02597.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02598.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02599.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02600.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02601.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02602.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02603.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02604.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02605.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02606.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02607.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02608.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02609.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02610.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02611.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02612.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02613.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02614.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02615.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02616.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02617.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02618.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02619.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02620.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02621.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02622.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password		Critical
Package: .src.main.webapp		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02623.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02624.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02625.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02626.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02627.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02628.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02629.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02630.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02631.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ webapp/ BenchmarkTest02632.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02633.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02634.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02635.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02636.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02637.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02638.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02639.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02640.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02641.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02642.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02643.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02644.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02645.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02646.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02647.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02648.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02649.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02650.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02651.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02652.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02653.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02654.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02655.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02656.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02657.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02658.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02662.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02663.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02667.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02668.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02672.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02673.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02677.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02678.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02682.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02683.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02687.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02688.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02692.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02693.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02697.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02698.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02702.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02703.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02707.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02708.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02712.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02713.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02717.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02718.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Privacy Violation: Password	Critical
Package: .src.main.webapp	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02722.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02723.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02727.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02728.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02732.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02733.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02737.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/webapp/BenchmarkTest02738.html:16	**Sink:** null **Enclosing Method:** () **Source:**	SCA

Password Management: Empty Password	High
Package: org.owasp.benchmark.helpers	

Location	Analysis Info	Analyzer
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/helpers/DatabaseHelper.java:137	**Sink:** getConnection() **Enclosing Method:** getSqlConnection() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00005.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00005.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00019.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00020.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00020.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00035.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00050.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00050.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00053.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00053.java:77	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00055.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00055.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00056.java:78	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00056.java:80	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00057.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00057.java:77	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00058.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00119.java:75	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00119.java:78	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00120.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00120.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00123.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00123.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00124.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00124.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00125.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00125.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00126.java:67	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00208.java:79	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00208.java:81	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00209.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00210.java:76	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00210.java:79	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00211.java:78	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00212.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00254.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00254.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00256.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00256.java:76	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00257.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00257.java:67	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00258.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00258.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00259.java:59	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00260.java:59	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00345.java:53	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00350.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00351.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00352.java:67	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00353.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00354.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00355.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00356.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00444.java:59	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00445.java:77	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00445.java:80	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00446.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00446.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00447.java:78	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00448.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00449.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00521.java:79	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00521.java:82	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00522.java:79	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00522.java:81	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00523.java:82	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00608.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00608.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00609.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00609.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00610.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00610.java:77	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00611.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00611.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00613.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00614.java:70	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00614.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00615.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00615.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00616.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00617.java:59	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00684.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00684.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00685.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00685.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00688.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00688.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00689.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00690.java:76	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00691.java:72	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00691.java:75	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00692.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00692.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00693.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00693.java:68	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00779.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00779.java:75	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00780.java:87	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00781.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00781.java:76	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00782.java:87	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00853.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00853.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00855.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00855.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00856.java:72	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00856.java:75	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00857.java:78	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00857.java:81	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00858.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00859.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00943.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00944.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00945.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00946.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01015.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01015.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01016.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01016.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01017.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01017.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01018.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01018.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01019.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01020.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01099.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01099.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01100.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01101.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01102.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01102.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01103.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01103.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01104.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01105.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01106.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01107.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01148.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01148.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01149.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01149.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01150.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01150.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01151.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01152.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01228.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01228.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01229.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01229.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01230.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01317.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01317.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01318.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01318.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01320.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01320.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01321.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01322.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01322.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01323.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01323.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01324.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01325.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01398.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01398.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01399.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01400.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01480.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01480.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01483.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01483.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01484.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01484.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01485.java:53	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01486.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01486.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01487.java:53	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01488.java:53	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01489.java:56	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01565.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01565.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01566.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01634.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01634.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01637.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01637.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01638.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01638.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01639.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01639.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01640.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01641.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01738.java:52	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01739.java:52	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01740.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01741.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01742.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01822.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01822.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01823.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01823.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01828.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01829.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01830.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01895.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01895.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01896.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01897.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01897.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01898.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01898.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01899.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01900.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01978.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01978.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01979.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01980.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01981.java:69	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02017.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02017.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02018.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02018.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02019.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02019.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02020.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02020.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02021.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02022.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02023.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02101.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02101.java:59	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02102.java:52	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02192.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02192.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02193.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02193.java:64	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02194.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02194.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02195.java:62	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02195.java:65	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02290.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02290.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02291.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02291.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02292.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02292.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02293.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02293.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02294.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02294.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02295.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02295.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02372.java:53	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02373.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02373.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02374.java:58	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02374.java:61	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02375.java:56	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02458.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02458.java:63	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02461.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02548.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02548.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02549.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02549.java:73	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02550.java:71	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02550.java:74	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02551.java:66	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02658.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02658.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02660.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02660.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02661.java:57	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02661.java:60	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02662.java:52	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02663.java:55	**Sink:** getInstance() **Enclosing Method:** doPost() **Source:**	SCA

Weak Encryption: Insecure Initial Value	High
Package: org.owasp.benchmark.testcode	

Location	Analysis Info	Analyzer
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00005.java:62	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00020.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00050.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00053.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00054.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00055.java:71	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00056.java:81	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00057.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00059.java:76	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00119.java:79	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00120.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00121.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00122.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00123.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00124.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00125.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00127.java:79	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00128.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00129.java:69	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/Benchmark-1.2beta/src/main/java/org/owasp/benchmark/testcode/BenchmarkTest00130.java:88	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00208.java:82	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00210.java:80	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00213.java:90	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00214.java:80	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00254.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00255.java:73	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00256.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00257.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00258.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00357.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00358.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00443.java:76	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00445.java:81	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00446.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00450.java:84	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00451.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00521.java:83	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00522.java:82	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00524.java:93	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00608.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00609.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00610.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00611.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00612.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00614.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00615.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00618.java:73	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00684.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00685.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00686.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00687.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00688.java:69	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00691.java:76	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00692.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00693.java:69	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00775.java:89	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00776.java:83	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00777.java:85	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00778.java:85	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00779.java:76	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00781.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00853.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00854.java:71	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00855.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00856.java:76	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00857.java:82	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest00942.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01015.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01016.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01017.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01018.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01021.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01022.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01099.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01102.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01103.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01108.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01147.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01148.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01149.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01150.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01153.java:69	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01226.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01227.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01228.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01229.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01317.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01318.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01319.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01320.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01322.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01323.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01398.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01401.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01480.java:62	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01481.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01482.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01483.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01484.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01486.java:62	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01563.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01564.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01565.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01567.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01634.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01635.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01636.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01637.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01638.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01639.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01737.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01822.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01823.java:70	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01824.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01825.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01826.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01827.java:72	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01895.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01897.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01898.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01901.java:67	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01975.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01976.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01977.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01978.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest01982.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02017.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02018.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02019.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02020.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02024.java:69	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02101.java:60	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02103.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02190.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02191.java:68	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02192.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02193.java:65	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02194.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02195.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02289.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02290.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02291.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02292.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02293.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02294.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02295.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02296.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02297.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02298.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02371.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02373.java:62	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02374.java:62	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02458.java:64	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02459.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02460.java:66	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Weak Encryption: Insecure Initial Value		High
Package: org.owasp.benchmark.testcode		
Location	**Analysis Info**	**Analyzer**
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02547.java:77	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02548.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02549.java:74	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02550.java:75	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02552.java:78	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02658.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02659.java:63	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02660.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA
Desktop/Benchmark/ Benchmark-1.2beta/src/main/ java/org/owasp/benchmark/ testcode/ BenchmarkTest02661.java:61	**Sink:** IvParameterSpec() **Enclosing Method:** doPost() **Source:**	SCA

A6 Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

A7 Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed.

No Issues

A8 Cross-Site Request Forgery (CSRF)

CSRF attacks force an authenticated victim's browser to send an unauthenticated request to a vulnerable web application, which then performs unauthorized action on behalf of the attacker. CSRF can be as powerful as the web application that it targets.

No Issues

A9 Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

No Issues

A10 Unvalidated Redirects and Forwards

Redirects allow web applications to direct users to different pages within the same application or to external sites. Attackers can utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. Open redirects are often abused as part of phishing scams to harvest sensitive end-user data.

No Issues

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.