

Web Application Report

This report includes important security information about your Web Application.

Security Report

This report was created by IBM Rational AppScan 8.5.0.1
21/08/2012 14:49:51 PM

Report Information

Web Application Report

Scan Name: demo.testfire.net

Scanned Host(s)

Host	Operating System	Web Server	Application Server
demo.testfire.net	Win32	IIS, IIS6	ASP.NET

Content

This report contains the following sections:

- Executive Summary

Executive Summary

Test Policy

- Default

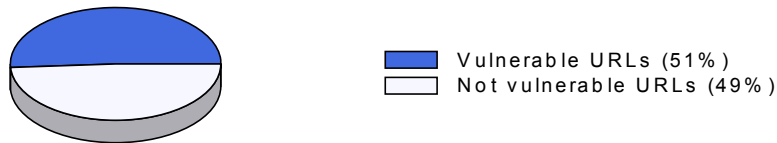
Security Risks

Following are the security risks that appeared most often in the application. To explore which issues included these risks, please refer to the 'Detailed Security Issues' section in this report.

- It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
- It is possible to view, modify or delete database entries and tables
- It is possible to gather sensitive debugging information
- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Vulnerable URLs

51% of the URLs had test results that included security issues.



Scanned URLs

115 URLs were scanned by AppScan.

Security Issue Possible Causes

Following are the most common causes for the security issues found in the application. The causes below are those that repeated in the maximal number of issues. To explore which issues included these causes, please refer to the 'Detailed Security Issues' section in this report.

- Sanitation of hazardous characters was not performed correctly on user input
- No validation was done in order to make sure that user input matches the data type expected
- Proper bounds checking were not performed on incoming parameter values
- Insecure web application programming or configuration
- Insufficient authentication method was used by the application

URLs with the Most Security Issues (number issues)

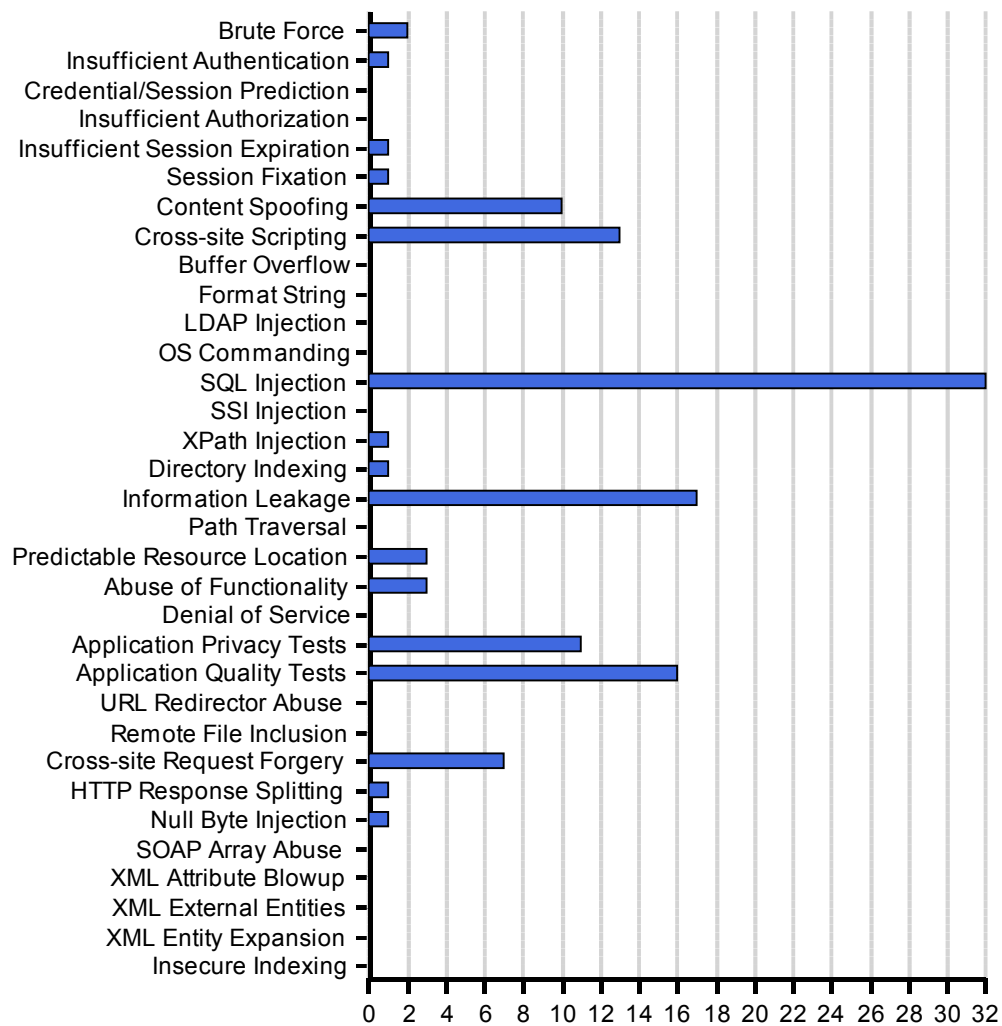
- <http://demo.testfire.net/bank/login.aspx> (22)
- <http://demo.testfire.net/bank/transfer.aspx> (16)
- <http://demo.testfire.net/bank/transaction.aspx> (12)
- <http://demo.testfire.net/bank/ws.aspx> (9)
- <http://demo.testfire.net/bank/customize.aspx> (8)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
http://demo.testfire.net/	38	23	37	25	123
Total	38	23	37	25	123

Security Issue Distribution per Threat Class

The following is a list of the security issues, distributed by Threat Class.



Security Issue Cause Distribution

94% Application-related Security Issues (116 out of a total of 123 issues).

Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.

6% Infrastructure and Platform Security Issues (7 out of a total 123 issues).

Infrastructure and Platform Security Issues can usually be fixed by system and network administrators as these security issues result from misconfiguration of, or defects in 3rd party products.