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
1/18/2013 5:50:18 PM

Report Information

Web Application Report

Scan Name: ncias-d704-v-examplerest_20130118

Scanned Host(s)

Host	Operating System	Web Server	Application Server
ncias-d704-v.nci.nih.gov:29080		Apache	Apache AXIS

Content

This report contains the following sections:

- Executive Summary

Executive Summary

Test Policy

- Default

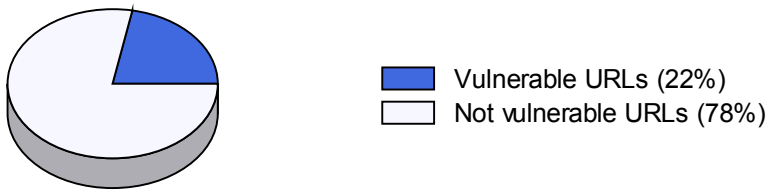
Security Risks

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 retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
- It is possible to gather sensitive debugging information
- 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
- The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
- It is possible to upload, modify or delete web pages, scripts and files on the web server

Vulnerable URLs

22% of the URLs had test results that included security issues.



Scanned URLs

2310 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.

- Debugging information was left by the programmer in web pages
- Latest patches or hotfixes for 3rd. party products were not installed
- Temporary files were left in production environment

- 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

URLs with the Most Security Issues (number issues)

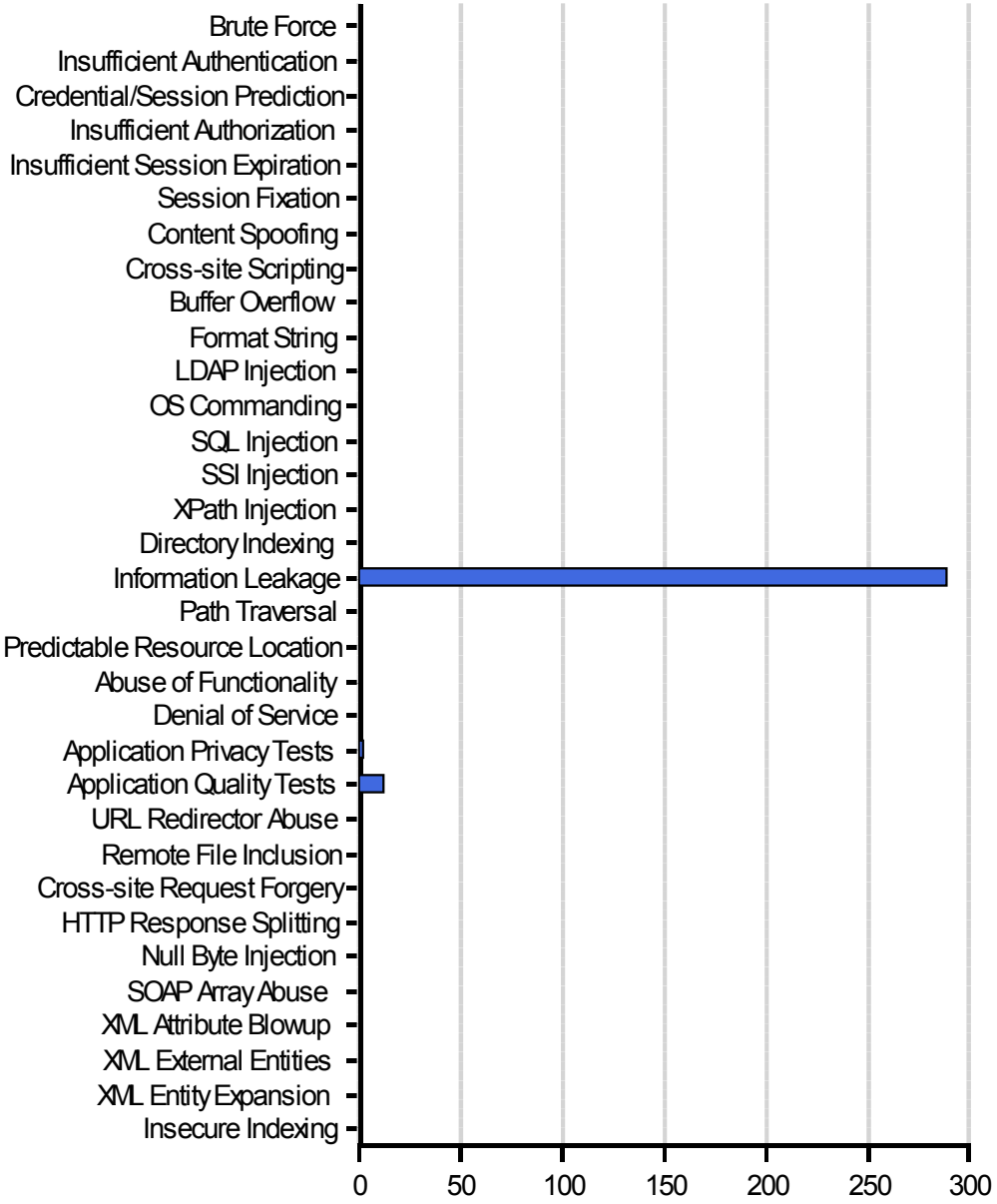
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Result.action (5)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (2)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action (2)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/ (1)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (1)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
http://ncias-d704-v.nci.nih.gov:29080/	0	1	290	14	305
Total	**0**	**1**	**290**	**14**	**305**

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

99% Application-related Security Issues (304 out of a total of 305 issues).
Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.
1% Infrastructure and Platform Security Issues (1 out of a total 305 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.