

Web Application Report

This report includes important security information about your Web Application.

Security Report

This report was created by IBM Rational AppScan 8.0.0.3
4/10/2012 10:14:57 AM

Report Information

Web Application Report

Scan Name: csm-uptlogin_040512-2

Scanned Host(s)

Host	Operating System	Web Server	Application Server
ncias-d704-v.nci.nih.gov:29543		Apache	Apache AXIS

Content

This report contains the following sections:

- Executive Summary

Executive Summary

Test Policy

- Default

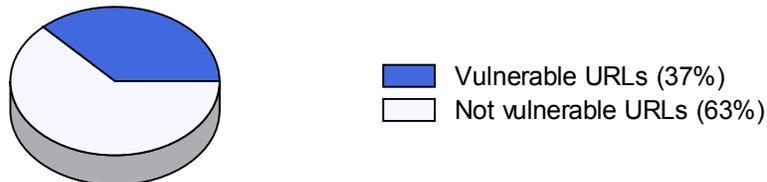
Security Risks

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 gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to gather sensitive debugging information
- It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
- It is possible to prevent the web application from serving other users (denial of service)

Vulnerable URLs

37% of the URLs had test results that included security issues.



Scanned URLs

38 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.

- Sensitive information might have been cached by your browser
- Insecure web application programming or configuration
- 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

- Query parameters were passed over SSL, and may contain sensitive information

URLs with the Most Security Issues (number issues)

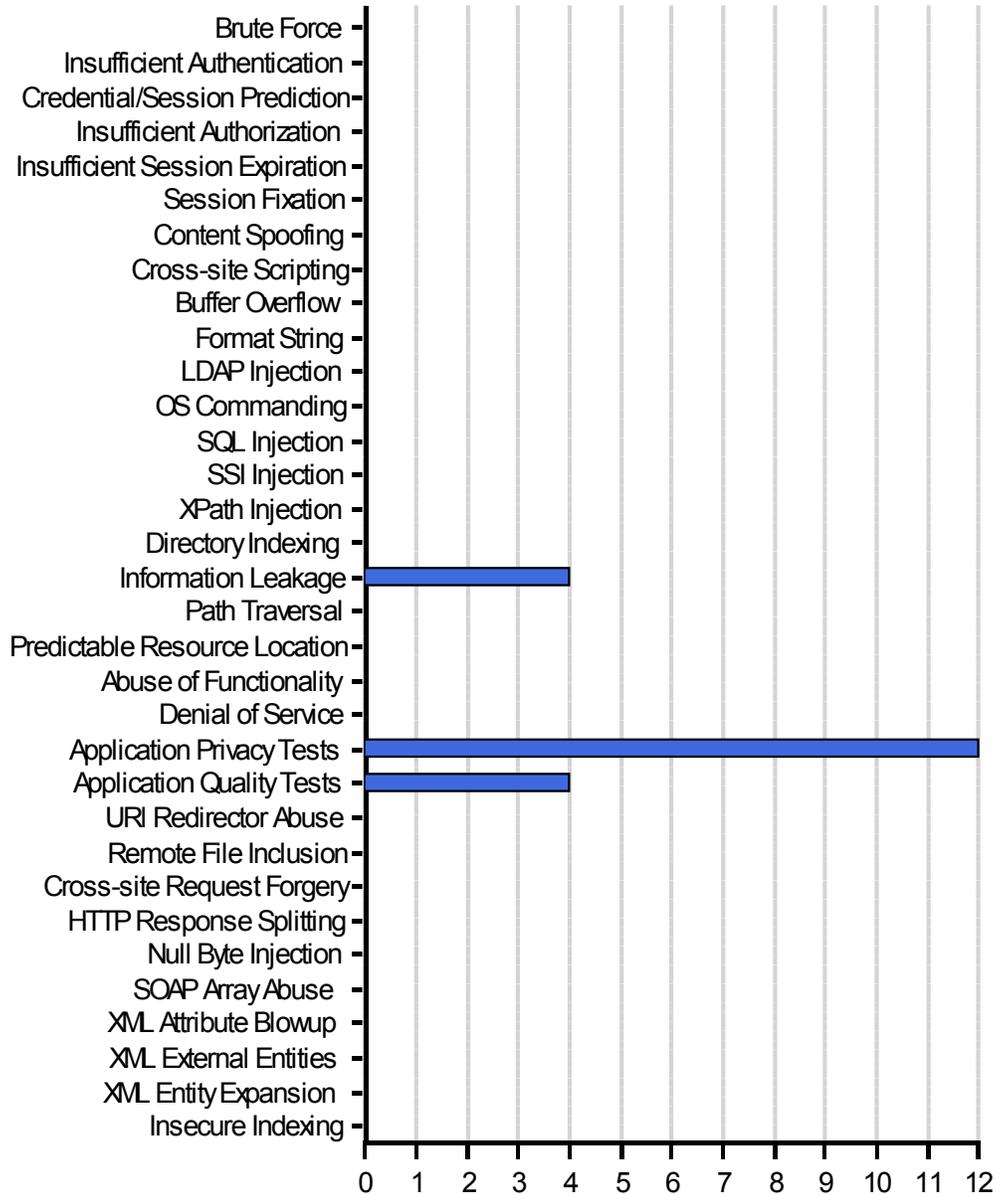
- <https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do> (3)
- <https://ncias-d704-v.nci.nih.gov:29543/uptlogin/> (2)
- <https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterApplicationSupport.do> (2)
- <https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterContactUs.do> (2)
- <https://ncias-d704-v.nci.nih.gov:29543/upt423/images/appLogo.gif;jsessionid=C785E2BDBEB2EA995525BE2A53106E58> (2)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://ncias-d704-v.nci.nih.gov:29543/	0	0	12	8	20
Total	0	0	12	8	20

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

100% Application-related Security Issues (20 out of a total of 20 issues).

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

0% Infrastructure and Platform Security Issues (0 out of a total 20 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.