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
1/3/2013 8:13:51 AM

Report Information

Web Application Report

Scan Name: upt-stage_20121214

Scanned Host(s)

Host	Operating System	Web Server	Application Server
upt-stage.nci.nih.gov:443	Unix/Linux	Apache	

Content

This report contains the following sections:

- Executive Summary

Executive Summary

Test Policy

- Default

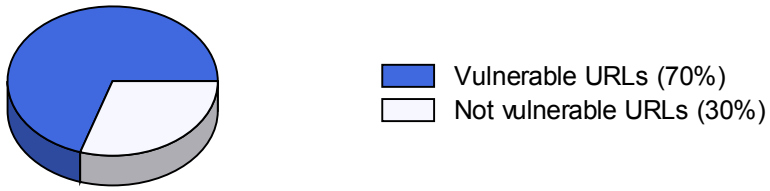
Security Risks

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 information about the site's file system structure, which may help the attacker to map the web site
- 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 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 is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Vulnerable URLs

70% of the URLs had test results that included security issues.



Scanned URLs

74 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.

- The web server or application server are configured in an insecure way
- 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
- Sensitive information might have been cached by your browser

URLs with the Most Security Issues (number issues)

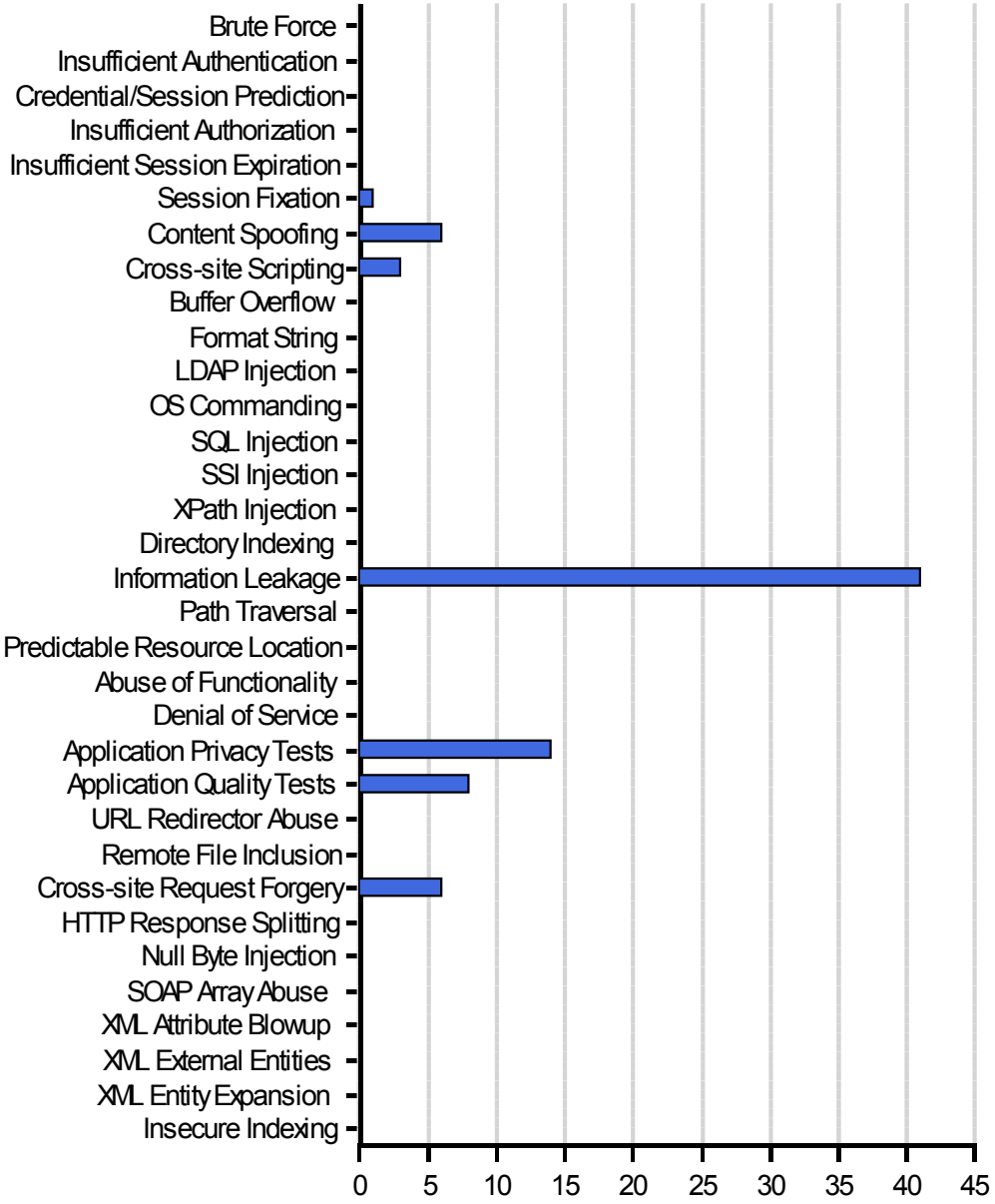
- https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do (7)
- https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do (7)
- https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do (5)
- https://upt-stage.nci.nih.gov/uptlogin/Login.do (4)
- https://upt-stage.nci.nih.gov/upt42/AdminHome.do;jsessionid=DFE10D66B4862F58DDDED3E0616E03C8 (2)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://upt-stage.nci.nih.gov/	3	13	51	12	79
Total	**3**	**13**	**51**	**12**	**79**

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

53% Application-related Security Issues (42 out of a total of 79 issues).
Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.
47% Infrastructure and Platform Security Issues (37 out of a total 79 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.