Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 8.6.0.1, Rules: 1529
Scan started: 2/13/2013 5:31:01 PM

Table of Contents

Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

Low severity issues:	51
Informational severity issues:	9
Total security issues included in the report:	60
Total security issues discovered in the scan:	60

General Information

Scan file name:	upt50-qa.nci.nih.gov_20130213
Scan started:	2/13/2013 5:31:01 PM
Test policy:	Default
Host	upt50-qa.nci.nih.gov
Operating system:	Unknown
Web server:	Apache
Application server:	Any
Host	upt50-qa.nci.nih.gov
Operating system:	Unknown
Web server:	Apache
Application server:	JavaAppServer

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
JavaScript execution:	Enabled
In-session detection:	Enabled
In-session pattern:	

Tracked or session ID cookies:	`__utma`
	`__utmz`
	`JSESSIONID`

Tracked or session ID parameters:	

Login sequence:	`http://upt50-qa.nci.nih.gov/upt50/`
	`https://upt50-qa.nci.nih.gov/upt50/`
	`https://upt50-qa.nci.nih.gov/upt50/scripts/script.js`
	`https://upt50-qa.nci.nih.gov/upt50/Login.do`
	`https://upt50-qa.nci.nih.gov/upt50/scripts/script.js`

Executive Summary

Issue Types 6

TOC

	Issue Type	Number of Issues
L	Cacheable SSL Page Found	12
L	Email Address Pattern Found in Parameter Value	2
L	Hidden Directory Detected	37
I	Application Error	4
I	Email Address Pattern Found	3
I	HTML Comments Sensitive Information Disclosure	2

Vulnerable URLs 51

TOC

	URL	Number of Issues
	Root	0
L	https://upt50-qa.nci.nih.gov/upt50/AppUserLogin.do	4
L	https://upt50-qa.nci.nih.gov/upt50/ApplicationDBOperation.do	1
L	https://upt50-qa.nci.nih.gov/upt50/FooterAccessibility.do	1
L	https://upt50-qa.nci.nih.gov/upt50/FooterApplicationSupport.do	2
L	https://upt50-qa.nci.nih.gov/upt50/FooterContactUs.do	2
L	https://upt50-qa.nci.nih.gov/upt50/FooterDisclaimer.do	1
L	https://upt50-qa.nci.nih.gov/upt50/FooterPrivacy.do	1
L	https://upt50-qa.nci.nih.gov/upt50/Home.do	1
L	https://upt50-qa.nci.nih.gov/upt50/Login.do	5
L	https://upt50-qa.nci.nih.gov/upt50/PrivilegeDBOperation.do	1
L	https://upt50-qa.nci.nih.gov/upt50/RoleDBOperation.do	1
L	https://upt50-qa.nci.nih.gov/upt50/UserDBOperation.do	2
L	https://upt50-qa.nci.nih.gov/cgi-bin/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/.cobalt/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/calendar/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/carello/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/cgi-bin/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/cgi/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/csfaq/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/cssearch/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/cutecast/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/dasp/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/dbman/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/dcforum/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/ews/	1

L	https://upt50-qa.nci.nih.gov/cgi-bin/excite/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/gbook/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/guestbook/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/gw5/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/hamweather/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/hwadmin5340/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/iisadmin/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/ikonboard/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/logs	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/mwf/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/news/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/openwebmail/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/pollit/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/powerup/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/rwcgi60/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/samples/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/search/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/ssi/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/suche/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/sws/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/templates/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/tools/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/w3-msql/	1
L	https://upt50-qa.nci.nih.gov/cgi-bin/www-sql/	1
I	https://upt50-qa.nci.nih.gov/upt50/	1

Fix Recommendations 5

TOC

	Remediation Task	Number of Issues
L	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	37
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	12
L	Remove e-mail addresses from the website	5
L	Remove sensitive information from HTML comments	2
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	4

Security Risks 3

TOC

	Risk	Number of Issues
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	19
L	It is possible to retrieve information about the site's file system structure, which may help	37

	the attacker to map the web site		
I	It is possible to gather sensitive debugging information	4	

Causes 6

TOC

	Cause	Number of Issues
L	Sensitive information might have been cached by your browser	12
L	Insecure web application programming or configuration	5
L	The web server or application server are configured in an insecure way	37
I	Proper bounds checking were not performed on incoming parameter values	4
I	No validation was done in order to make sure that user input matches the data type expected	4
I	Debugging information was left by the programmer in web pages	2

WASC Threat Classification

TOC

Threat	Number of Issues
Application Privacy Tests	12
Application Quality Tests	4
Information Leakage	44