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: 1556
Scan started: 3/22/2013 11:11:17 AM

Table of Contents

Introduction

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

Low severity issues:	24
Informational severity issues:	7
Total security issues included in the report:	31
Total security issues discovered in the scan:	31

General Information

Scan file name:	upt50-stage.nci.nih.gov_20130322
Scan started:	3/22/2013 11:11:17 AM
Test policy:	Default
Host	upt50-stage.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:	`>LOG OUT<`

Tracked or session ID cookies:	`__utma`
	`__utmz`
	`__qca`
	`ncbi_sid`
	`newuser`
	`JSESSIONID`

Tracked or session ID parameters:	

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

Executive Summary

Issue Types 6

TOC

	Issue Type	Number of Issues
L	Cacheable SSL Page Found	8
L	Email Address Pattern Found in Parameter Value	1
L	Hidden Directory Detected	15
I	Application Error	3
I	Email Address Pattern Found	2
I	HTML Comments Sensitive Information Disclosure	2

Vulnerable URLs 25

TOC

	URL	Number of Issues
	Root	0
L	https://upt50-stage.nci.nih.gov/upt50/AppUserLogin.do	2
L	https://upt50-stage.nci.nih.gov/upt50/FooterAccessibility.do	1
L	https://upt50-stage.nci.nih.gov/upt50/FooterApplicationSupport.do	2
L	https://upt50-stage.nci.nih.gov/upt50/FooterContactUs.do	2
L	https://upt50-stage.nci.nih.gov/upt50/FooterDisclaimer.do	1
L	https://upt50-stage.nci.nih.gov/upt50/FooterPrivacy.do	1
L	https://upt50-stage.nci.nih.gov/upt50/Home.do	1
L	https://upt50-stage.nci.nih.gov/upt50/Login.do	5
L	https://upt50-stage.nci.nih.gov/cgi-bin/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/.cobalt/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/dbman/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/dcforum/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/ews/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/excite/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/gbook/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/guestbook/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/gw5/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/hamweather/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/hwadmin5340/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/iisadmin/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/ikonboard/	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/logs	1
L	https://upt50-stage.nci.nih.gov/cgi-bin/mwf/	1
I	https://upt50-stage.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	15
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	8
L	Remove e-mail addresses from the website	3
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	3

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	13
L	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	15
I	It is possible to gather sensitive debugging information	3

Causes 6

TOC

	Cause	Number of Issues
L	Sensitive information might have been cached by your browser	8
L	Insecure web application programming or configuration	3
L	The web server or application server are configured in an insecure way	15
I	Proper bounds checking were not performed on incoming parameter values	3
I	No validation was done in order to make sure that user input matches the data type expected	3
I	Debugging information was left by the programmer in web pages	2

WASC Threat Classification

TOC

Threat	Number of Issues
Application Privacy Tests	8
Application Quality Tests	3
Information Leakage	20