

Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.1.1, Rules: 1809
Scan started: 1/19/2015 6:11:52 PM

Table of Contents

Introduction

- General Information
- Login Settings

Executive Summary

- Issue Types
- Vulnerable URLs
- Fix Recommendations
- Security Risks
- Causes
- WASC Threat Classification

Introduction

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

High severity issues:	60
Medium severity issues:	55
Low severity issues:	104
Informational severity issues:	9
Total security issues included in the report:	228
Total security issues discovered in the scan:	228

General Information

Scan file name:	rap.pmaktif.com - Admin Console
Scan started:	1/19/2015 6:11:52 PM
Test policy:	Default
Host	rap.pmaktif.com
Operating system:	Win32
Web server:	IIS
Application server:	Any
Host	rap.pmaktif.com
Operating system:	Win32
Web server:	IIS
Application server:	Any

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
JavaScript execution:	Disabled
In-session detection:	Enabled
In-session pattern:	AdminLogout.aspx'
Tracked or session ID cookies:	ASP.NET_SessionId
Tracked or session ID parameters:	
Login sequence:	https://rap.pmaktif.com/admin https://rap.pmaktif.com/admin/ https://rap.pmaktif.com/admin/default.aspx https://rap.pmaktif.com/admin/Main.aspx

Executive Summary

Issue Types 18

[TOC](#)






















Issue Type		Number of Issues	
H	Blind SQL Injection	55	
H	Cross-Site Scripting	5	
M	Cross-Site Request Forgery	33	
M	Inadequate Account Lockout	4	
M	Missing Secure Attribute in Encrypted Session (SSL) Cookie	10	
M	Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)	2	
M	Session Identifier Not Updated	5	
M	Weak SSL Cipher Suites are Supported	1	
L	Autocomplete HTML Attribute Not Disabled for Password Field	6	
L	Cacheable SSL Page Found	41	
L	Direct Access to Administration Pages	1	
L	Microsoft ASP.NET Debugging Enabled	2	
L	Microsoft IIS Missing Host Header Information Leakage	1	
L	Missing Cross-Frame Scripting Defence	34	
L	Query Parameter in SSL Request	15	
L	Unencrypted __VIEWSTATE Parameter	4	
I	Client-Side (JavaScript) Cookie References	3	
I	Email Address Pattern Found	6	

Vulnerable URLs 59

[TOC](#)











URL		Number of Issues	
H	https://rap.pmaktif.com/ChangePasswordOthers.aspx	3	
H	https://rap.pmaktif.com/Login.aspx	8	
H	https://rap.pmaktif.com/admin/DepartmentList.aspx	4	
H	https://rap.pmaktif.com/admin/EventFormatList.aspx	8	

H	https://rap.pmaktif.com/admin/EventList.aspx	4	
H	https://rap.pmaktif.com/admin/FirmList.aspx	12	
H	https://rap.pmaktif.com/admin/OrderManagementOrderReturnConfirmation.aspx	4	
H	https://rap.pmaktif.com/admin/OrderManagementReportsOrderList.aspx	10	
H	https://rap.pmaktif.com/admin/ProductManagementCategories.aspx	4	
H	https://rap.pmaktif.com/admin/ProductManagementProducts.aspx	15	
H	https://rap.pmaktif.com/admin/ReportManagementAccountTransaction.aspx	4	
H	https://rap.pmaktif.com/admin/ReportsOrderAndProduct.aspx	24	
H	https://rap.pmaktif.com/admin/UserAdd.aspx	5	
H	https://rap.pmaktif.com/admin/UserManagementUserList.aspx	5	
M	https://rap.pmaktif.com/admin/AdminLogout.aspx	3	
M	https://rap.pmaktif.com/admin/Default.aspx	6	
M	https://rap.pmaktif.com/admin/EventFormatAdd.aspx	3	
M	https://rap.pmaktif.com/admin/EventFormatEdit.aspx	3	
M	https://rap.pmaktif.com/admin/EventMailLogs.aspx	3	
M	https://rap.pmaktif.com/admin/EventTypeEdit.aspx	3	
M	https://rap.pmaktif.com/admin/EventTypeList.aspx	3	
M	https://rap.pmaktif.com/admin/FirmAdd.aspx	3	
M	https://rap.pmaktif.com/admin/OrderManagementOrderReject.aspx	3	
M	https://rap.pmaktif.com/admin/ReportManagementDepartmentGiftBudget.aspx	3	
M	https://rap.pmaktif.com/admin/ReportManagementLogUserPages.aspx	3	
M	https://rap.pmaktif.com/admin/ReportManagementRetailersHqProduct.aspx	3	
M	https://rap.pmaktif.com/admin/ReportManagementRetailersHqRetailer.aspx	3	
M	https://rap.pmaktif.com/admin/UserManagementBudgetMovements.aspx	2	
M	https://rap.pmaktif.com/admin/UserManagementDepartmentBudgetImport.aspx	3	
M	https://rap.pmaktif.com/admin/UserManagementDepartments.aspx	3	
M	https://rap.pmaktif.com/admin/UserManagementEditDepartment.aspx	3	
M	https://rap.pmaktif.com/admin/UserManagementRetailerList.aspx	3	
M	https://rap.pmaktif.com/admin/UserManagementTransferBudget.aspx	3	
M	https://rap.pmaktif.com/admin/default.aspx	5	
M	https://rap.pmaktif.com/login.aspx	8	
M	https://rap.pmaktif.com/admin/	3	
M	https://rap.pmaktif.com/admin/Main.aspx	7	
M	http://rap.pmaktif.com/admin/	1	

M	https://rap.pmaktif.com/admin	3	
L	https://rap.pmaktif.com/ApplicationList.aspx	2	
L	https://rap.pmaktif.com/EventSelection.aspx	1	
L	https://rap.pmaktif.com/ForgetPassword.aspx	2	
L	https://rap.pmaktif.com/admin/Error.aspx	3	
L	https://rap.pmaktif.com/admin/EventDetail.aspx	1	
L	https://rap.pmaktif.com/admin/EventTypeAdd.aspx	2	
L	https://rap.pmaktif.com/admin/FirmEdit.aspx	2	
L	https://rap.pmaktif.com/admin/NoAuth.aspx	2	
L	https://rap.pmaktif.com/	2	
L	http://rap.pmaktif.com/	1	
L	https://rap.pmaktif.com/Error.aspx	1	
L	https://rap.pmaktif.com/WebResource.axd	2	
L	https://rap.pmaktif.com/admin/ProductManagementProductEdit.aspx	1	
L	https://rap.pmaktif.com/admin/ScriptResource.axd	2	
L	https://rap.pmaktif.com/admin/UserDetail.aspx	1	
L	https://rap.pmaktif.com/admin/UserManagementContactTermRelStat usTransaction.aspx	1	
L	https://rap.pmaktif.com/admin/WebResource.axd	2	
I	https://rap.pmaktif.com/admin/JS/xtree.js	1	
I	https://rap.pmaktif.com/admin/Js/jquery-ui-personalized-1.6rc6.js	1	
I	https://rap.pmaktif.com/admin/Js/jquery.cookie.js	2	

Fix Recommendations 16

TOC

Remediation Task		Number of Issues	
H	Review possible solutions for hazardous character injection	60	
M	Add the 'Secure' attribute to all sensitive cookies	10	
M	Change session identifier values after login	5	
M	Decline malicious requests	67	
M	Enforce account lockout after several failed login attempts	4	
M	Implement TLS_FALLBACK_SCSV. Additionally, either disable SSLv3 altogether, or disable all cipher suites that operate in CBC mode over SSLv3.	2	
M	Use a different signature algorithm for the certificate	1	
L	Always use SSL and POST (body) parameters when sending sensitive information.	15	
L	Apply configuration changes according to Q218180	1	
L	Apply proper authorization to administration scripts	1	
L	Correctly set the "autocomplete" attribute to "off"	6	

L	Disable Debugging on Microsoft ASP.NET	2	
L	Modify your Web.Config file to encrypt the VIEWSTATE parameter	4	
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	41	
L	Remove business and security logic from the client side	3	
L	Remove e-mail addresses from the website	6	

Security Risks 9




TOC

Risk		Number of Issues	
H	It is possible to view, modify or delete database entries and tables	55	
H	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	44	
M	It might be possible to escalate user privileges and gain administrative permissions over the web application	5	
M	It may be possible to steal user and session information (cookies) that was sent during an encrypted session	10	
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	90	
L	It may be possible to bypass the web application's authentication mechanism	6	
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	34	
L	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	15	
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	3	

Causes 8








TOC

Cause		Number of Issues	
H	Sanitation of hazardous characters was not performed correctly on user input	60	
M	Insufficient authentication method was used by the application	33	
M	Insecure web application programming or configuration	61	
M	The web application sends non-secure cookies over SSL	10	
M	The web server or application server are configured in an insecure way	5	

L	Sensitive information might have been cached by your browser	41	
L	Query parameters were passed over SSL, and may contain sensitive information	15	
I	Cookies are created at the client side	3	

WASC Threat Classification

[TOC](#)

Threat	Number of Issues	
Brute Force	4	
Cross-site Request Forgery	33	
Cross-site Scripting	5	
Information Leakage	124	
Predictable Resource Location	1	
Server Misconfiguration	1	
Session Fixation	5	
SQL Injection	55	