Web Application Report

This report includes important security information about your Web Application.

The Sarbanes-Oxley Act of 2002 Compliance Report

This report was created by IBM Rational AppScan 7.7
6/27/2008 12:52:27 PM

The Sarbanes-Oxley Act of 2002

Web Application Report

This report was created by IBM Rational AppScan 7.7

Scanned Web Application: http://local/altoro
Scan Name: testfire

Content

This report contains the following sections:

IMPORTANT INFORMATION ABOUT THIS REPORT

This Compliance Scan Results Report is based on the results of an automated Web Application Security scan, performed by AppScan.

An AppScan scan attempts to uncover security-related issues in web applications, testing both the http frameworks (e.g. web servers) and the code of the application itself (e.g. dynamic pages). The testing is performed over HTTP, and is limited only to those issues that are specified for testing and identified in an automated fashion via the HTTP channel. The scan is also limited to those specific issues included in an automatic and/or manual explore performed during the scan. The security-related issues detected are compared to selected regulatory or industry standard requirements to produce this report. There may be areas of compliance risk associated with such regulation or standard that are not specified for testing by AppScan. This report will not detect any compliance-related issues in areas of compliance risk that are not tested by AppScan. The report identifies areas where there may be a compliance risk, but the exact impact of each uncovered issue type depends on the individual application, environment, and the subject regulation or standard. Regulations and standards are subject to change, and the scans performed by AppScan may not reflect all such changes. It is the user’s responsibility to interpret the results in this report for determination of impact, actual compliance violations, and appropriate remedial measures, if any.
Section references to regulations are provided for reference purposes only. The issues reported are general compliance-related risks and are not to be interpreted as excerpts from any regulation.

The information provided does not constitute legal advice. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Description

Summary

The Sarbanes-Oxley Act (officially titled the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX and Sarbox), signed into law on 30 July 2002 by President Bush, is considered the most significant change to federal securities laws in the United States since the New Deal. It came in the wake of a series of corporate financial scandals, including those affecting Enron, Arthur Andersen, and WorldCom. The law is named after sponsors Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OH). It was approved by the House by a vote of 423-3 and by the Senate 99-0.

The act was designed to review dated legislative audit requirements. The goal of the act was to protect investors by improving the accuracy and reliability of corporate disclosures. The act covers issues such as establishing a public company accounting oversight board, auditor independence, corporate responsibility and enhanced financial disclosure.

Provisions

The Sarbanes-Oxley Act's major provisions include:

-Certification of financial reports by CEOs and CFOs
-Ban on personal loans to any Executive Officer and Director
-Accelerated reporting of trades by insiders
-Prohibition on insider trades during pension fund blackout periods
-Public reporting of CEO and CFO compensation and profits
-Additional disclosure
-Auditor independence, including outright bans on certain types of work and pre-certification by the company's Audit Committee of all other non-audit work
-Criminal and civil penalties for securities violations
-US companies are now obliged to have an internal audit function, which will need to be certified by external auditors.
-Significantly longer jail sentences and larger fines for corporate executives who knowingly and willfully misstate financial statements.
-Prohibition on audit firms providing extra "value-added" services to their clients including actuarial services, legal and extra services (such as consulting) unrelated to their audit work.
-A requirement that publicly traded companies furnish independent annual audit reports on the existence and condition (i.e., reliability) of internal controls as they relate to financial reporting.

Internal Controls

One key element of the Act is to require a report of the internal controls a company has in place to ensure compliance with the Act itself. Section 404 mandates that CEOs and CFOs must file Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. The SEC published the final form of its rules and guidelines on the content of these reports in June of 2003.

Section 404 requires management to document and assess the effectiveness of their internal controls over financial reporting. Additionally, the Public Company Accounting Oversight Board (PCAOB) ([1] (http://www.pcaobus.org/)) has issued guidelines on how management should render their opinion. The main point of these guidelines is that management should use an internal control framework such as COSO (which describes how to assess the control environment, determine control objectives, perform risk assessments, and identify controls and monitor compliance). Companies have almost uniformly elected COSO as the standard when choosing an internal control framework.

Information Technology and SOX 404

The PCAOB suggests considering the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework in management/auditor assessment of controls. Auditors have also looked to the IT Governance Institute's "COBIT": Control Objectives of Information and Related Technology for more appropriate standards of measure. This framework focuses on IT processes while keeping in mind the big picture of COSO's "control activities" and "information and communication". However, certain aspects of COBIT are outside the boundaries of Sarbanes-Oxley regulation.

Definition of Internal Control Over Financial Reporting

Internal control is defined by the COSO as a process-effected by an entity's board of directors, management, and other personnel-designed to provide reasonable assurance of the achievement of objectives in the following categories: effectiveness and efficiency of operations, compliance with applicable laws and regulations, and reliability of financial reporting.

The SEC rules implementing section 404(a) of the Act focus on those objectives related to the reliability of a company's external financial reporting. This subset of internal control is commonly referred to as internal control over financial reporting.

Internal control over financial reporting is defined in Standard No. 2 as a process designed by or under the supervision of the company's principal executive and financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP). It also includes policies and procedures that pertain to maintenance of accounting records, authorization of receipts and disbursements, and safeguarding of assets.

For purposes of an audit of internal control over financial reporting, "internal control over financial reporting" includes controls over the safeguarding of assets and controls related to the prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets that could have a material effect on the financial statements. These safeguarding controls are a subset of the broader segment of internal control.

IT Controls, IT Audit and SOX

In today's business environment, the financial reporting processes of most organizations are driven by Information Technology (IT) systems. Few companies manage their data manually and most companies have moved to electronic management of data, documents, and key operational processes. Therefore, it is apparent that IT plays a vital role in internal control. As PCAOB Auditing Standard 2 states:

The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting.

Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.

IBM and Section 404

The security and exchange commission explains that the Statement on Auditing Standards No. 55, revised the term 'Internal Control'. Under the new definition, the safeguarding of assets became a subset of the 'control procedures' component required under the section. SAS 55 states that control procedures may generally be categorized as procedures that include, among other things, "adequate safeguards over access to and use of assets and records, such as secured facilities and authorization for access to computer programs and data files".

Covered Entities

Companies listed in U.S stock exchange, external auditors of companies listed in the U.S stock exchange (registered public accounting firms).

Effective Date

July, 2002

Compliance Required By

Accelerated filers - Generally, U.S based companies with aggregate market value of the voting and non-voting common equity held by non-affiliates of the issuer of $75 million or more - November 2004.

Non-accelerated filers and foreign private issuers - (Generally, but not limited to U.S based companies with aggregate market value of the voting and non-voting common equity held by non-affiliates of the issuer less than $75 million, and foreign companies that are listed in the U.S exchange - July 2006.

Regulators/Auditors

The Security and Exchange Commission

For more information on securing web applications, please visit www.watchfire.com.

(*) DISCLAIMER IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Compliance Scan Results

62 unique issues detected across 1 sections of the regulation:

	Section	No. of Issues
1.	Each annual report supplied by the company in accordance with the Securities Exchange act of 1934, should contain an internal control report, which shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. (Title IV, Sec.404)	62

Unique Compliance-related Issues Detected

62 unique issues detected across 1 sections of the regulation:

ID	URL	Parameter/Cookie	Test Name	Sections
1	http://local/altoro/		Application Test Script Detected	1
2	http://local/altoro/bank/login.aspx		Database Error Pattern Found	1
3	http://local/altoro/subscribe.aspx		Database Error Pattern Found	1
4	http://local/altoro/bank/transaction.aspx	after	Database Error Pattern Found	1
5	http://local/altoro/bank/transaction.aspx	before	Database Error Pattern Found	1
6	http://local/altoro/bank/transfer.aspx	creditAccount	Database Error Pattern Found	1
7	http://local/altoro/bank/transfer.aspx	debitAccount	Database Error Pattern Found	1
8	http://local/altoro/bank/account.aspx	listAccounts	Database Error Pattern Found	1
9	http://local/altoro/bank/login.aspx	passw	Database Error Pattern Found	1
10	http://local/altoro/subscribe.aspx	txtEmail	Database Error Pattern Found	1
11	http://local/altoro/bank/login.aspx	uid	Database Error Pattern Found	1
12	http://local/altoro/bank/login.aspx	passw	Inadequate Account Lockout	1
13	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Button1	Blind SQL Injection	1
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	Blind SQL Injection	1
15	http://local/altoro/bank/transaction.aspx	before	Blind SQL Injection	1
16	http://local/altoro/subscribe.aspx	btnSubmit	Blind SQL Injection	1
17	http://local/altoro/comment.aspx	comments	Blind SQL Injection	1
18	http://local/altoro/comment.aspx	email_addr	Blind SQL Injection	1
19	http://local/altoro/bank/login.aspx	passw	Blind SQL Injection	1
20	http://local/altoro/comment.aspx	subject	Blind SQL Injection	1
21	http://local/altoro/comment.aspx	submit	Blind SQL Injection	1
22	http://local/altoro/bank/transfer.aspx	transfer	Blind SQL Injection	1
23	http://local/altoro/subscribe.aspx	txtEmail	Blind SQL Injection	1
24	http://local/altoro/bank/login.aspx	uid	Blind SQL Injection	1
25	http://local/altoro/search.aspx		Cross-Site Scripting	1
26	http://local/altoro/bank/transfer.aspx	creditAccount	Cross-Site Scripting	1
27	http://local/altoro/bank/transfer.aspx	debitAccount	Cross-Site Scripting	1

ID	URL	Parameter/Cookie	Test Name	Sections
28	http://local/altoro/bank/customize.aspx	lang	Cross-Site Scripting	1
29	http://local/altoro/cgi.exe	m	Cross-Site Scripting	1
30	http://local/altoro/comment.aspx	name	Cross-Site Scripting	1
31	http://local/altoro/subscribe.aspx	txtEmail	Cross-Site Scripting	1
32	http://local/altoro/search.aspx	txtSearch	Cross-Site Scripting	1
33	http://local/altoro/bank/login.aspx	uid	Cross-Site Scripting	1
34	http://local/altoro/bank/login.aspx		Predictable Login Credentials	1
35	http://local/altoro/cgi.exe	m	Format String Remote Command Execution	1
36	http://local/altoro/bank/customize.aspx	lang	HTTP Response Splitting	1
37	http://local/altoro/comment.aspx	name	Link Injection (facilitates Cross-Site Request Forgery)	1
38	http://local/altoro/search.aspx	txtSearch	Link Injection (facilitates Cross-Site Request Forgery)	1
39	http://local/altoro/bank/login.aspx		Unencrypted Login Request	1
40	http://local/altoro/default.aspx	content	Poison Null Byte Files Retrieval	1
41	http://local/altoro/bank/transaction.aspx	after	SQL Injection	1
42	http://local/altoro/bank/transaction.aspx	before	SQL Injection	1
43	http://local/altoro/bank/transfer.aspx	creditAccount	SQL Injection	1
44	http://local/altoro/bank/transfer.aspx	debitAccount	SQL Injection	1
45	http://local/altoro/bank/account.aspx	listAccounts	SQL Injection	1
46	http://local/altoro/bank/login.aspx	passw	SQL Injection	1
47	http://local/altoro/subscribe.aspx	txtEmail	SQL Injection	1
48	http://local/altoro/bank/login.aspx	uid	SQL Injection	1
49	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	Application Error	1
50	http://local/altoro/bank/transaction.aspx	after	Application Error	1
51	http://local/altoro/bank/transaction.aspx	before	Application Error	1
52	http://local/altoro/comment.aspx	cfile	Application Error	1
53	http://local/altoro/bank/transfer.aspx	creditAccount	Application Error	1
54	http://local/altoro/bank/transfer.aspx	debitAccount	Application Error	1
55	http://local/altoro/bank/account.aspx	listAccounts	Application Error	1
56	http://local/altoro/bank/login.aspx	passw	Application Error	1
57	http://local/altoro/bank/transfer.aspx	transferAmount	Application Error	1

ID	URL	Parameter/Cookie	Test Name	Sections
58	http://local/altoro/subscribe.aspx	txtEmail	Application Error	1
59	http://local/altoro/bank/login.aspx	uid	Application Error	1
60	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	XPath Injection	1
61	http://local/altoro/bank/login.aspx	passw	Login Page SQL Injection	1
62	http://local/altoro/bank/login.aspx	uid	Login Page SQL Injection	1

Compliance-Related Issues and Section References

1) **Each annual report supplied by the company in accordance with the Securities Exchange act of 1934, should contain an internal control report, which shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.**

(Title IV, Sec.404)

62 Issues

Application Test Script Detected

Security Risks

- It is possible to download temporary script files, which may expose the application logic and other sensitive information such as usernames and passwords

Causes:

- Temporary files were left in production environment

Remediation Tasks:

Remove test scripts from the server

Issues:

Issue ID	URL	Parameter/Cookie
1	http://local/altoro/	

Database Error Pattern Found

Security Risks

- It is possible to view, modify or delete database entries and tables

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/bank/login.aspx	
3	http://local/altoro/subscribe.aspx	
4	http://local/altoro/bank/transaction.aspx	after

5	http://local/altoro/bank/transaction.aspx	before
6	http://local/altoro/bank/transfer.aspx	creditAccount
7	http://local/altoro/bank/transfer.aspx	debitAccount
8	http://local/altoro/bank/account.aspx	listAccounts
9	http://local/altoro/bank/login.aspx	passw
10	http://local/altoro/subscribe.aspx	txtEmail
11	http://local/altoro/bank/login.aspx	uid

Inadequate Account Lockout

Security Risks

- It may be possible to escalate user privileges and gain administrative permissions over the web application

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Enforce account lockout after several failed login attempts

Issues:

Issue ID	URL	Parameter/Cookie
12	http://local/altoro/bank/login.aspx	passw

Blind SQL Injection

Security Risks

- It is possible to view, modify or delete database entries and tables

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
13	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te

15	http://local/altoro/bank/transaction.aspx	before
16	http://local/altoro/subscribe.aspx	btnSubmit
17	http://local/altoro/comment.aspx	comments
18	http://local/altoro/comment.aspx	email_addr
19	http://local/altoro/bank/login.aspx	passw
20	http://local/altoro/comment.aspx	subject
21	http://local/altoro/comment.aspx	submit
22	http://local/altoro/bank/transfer.aspx	transfer
23	http://local/altoro/subscribe.aspx	txtEmail
24	http://local/altoro/bank/login.aspx	uid

Cross-Site Scripting

Security Risks

- It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
25	http://local/altoro/search.aspx	
26	http://local/altoro/bank/transfer.aspx	creditAccount
27	http://local/altoro/bank/transfer.aspx	debitAccount
28	http://local/altoro/bank/customize.aspx	lang
29	http://local/altoro/cgi.exe	m
30	http://local/altoro/comment.aspx	name
31	http://local/altoro/subscribe.aspx	txtEmail
32	http://local/altoro/search.aspx	txtSearch
33	http://local/altoro/bank/login.aspx	uid

Predictable Login Credentials

Security Risks

- It may be possible to escalate user privileges and gain administrative permissions over the web application

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Change the login credentials to a stronger combination

Issues:

Issue ID	URL	Parameter/Cookie
34	http://local/altoro/bank/login.aspx	

Format String Remote Command Execution

Security Risks

- It is possible to execute remote commands on the web server. This usually means complete compromise of the server and its contents

Causes:

- User input is used directly as a formatting string input for C/C++/Perl's sprintf and similar functions

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
35	http://local/altoro/cgi.exe	m

HTTP Response Splitting

Security Risks

- It is possible to deface the site content through web-cache poisoning
- It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
36	http://local/altoro/bank/customize.aspx	lang

Link Injection (facilitates Cross-Site Request Forgery)

Security Risks

- 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 steal or manipulate customer session and cookies, which may 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 upload, modify or delete web pages, scripts and files on the web server

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
37	http://local/altoro/comment.aspx	name
38	http://local/altoro/search.aspx	txtSearch

Unencrypted Login Request

Security Risks

- It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Remediation Tasks:

Encrypt all login requests

Issues:

Issue ID	URL	Parameter/Cookie
39	http://local/altoro/bank/login.aspx	

Poison Null Byte Files Retrieval

Security Risks

- It is possible to view the contents of any file (e.g. databases, user information or configuration files) on the web server (under the permission restrictions of the web server user)

Causes:

- Sanitation of hazardous characters was not performed correctly on user input
- User input is not checked for the '..' (dot dot) string

Remediation Tasks:

Ensure that accessed files reside in the virtual path and have certain extensions; remove special characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
40	http://local/altoro/default.aspx	content

SQL Injection

Security Risks

- It is possible to view, modify or delete database entries and tables

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
41	http://local/altoro/bank/transaction.aspx	after
42	http://local/altoro/bank/transaction.aspx	before
43	http://local/altoro/bank/transfer.aspx	creditAccount
44	http://local/altoro/bank/transfer.aspx	debitAccount
45	http://local/altoro/bank/account.aspx	listAccounts
46	http://local/altoro/bank/login.aspx	passw
47	http://local/altoro/subscribe.aspx	txtEmail
48	http://local/altoro/bank/login.aspx	uid

Application Error

Security Risks

- It is possible to gather sensitive debugging information

Causes:

- Proper bounds checking were not performed on incoming parameter values
- No validation was done in order to make sure that user input matches the data type expected

Remediation Tasks:

Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Issues:

Issue ID	URL	Parameter/Cookie
49	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
50	http://local/altoro/bank/transaction.aspx	after
51	http://local/altoro/bank/transaction.aspx	before

52	http://local/altoro/comment.aspx	cfile
53	http://local/altoro/bank/transfer.aspx	creditAccount
54	http://local/altoro/bank/transfer.aspx	debitAccount
55	http://local/altoro/bank/account.aspx	listAccounts
56	http://local/altoro/bank/login.aspx	passw
57	http://local/altoro/bank/transfer.aspx	transferAmount
58	http://local/altoro/subscribe.aspx	txtEmail
59	http://local/altoro/bank/login.aspx	uid

XPath Injection

Security Risks

- It is possible to access information stored in a sensitive data resource

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
60	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te

Login Page SQL Injection

Security Risks

- It may be possible to bypass the web application's authentication mechanism

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Remediation Tasks:

Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
61	http://local/altoro/bank/login.aspx	passw
62	http://local/altoro/bank/login.aspx	uid