Web Application Report

This report includes important security information about your Web Application.

Visa's Payment Application Best Practices Report

This report was created by IBM Rational AppScan 7.7
6/27/2008 12:51:16 PM

© Copyright IBM Corp. 2000, 2008. All Rights Reserved.

Visa's Payment Application Best Practices

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 Payment Card Industry Data Security Standard (PCI DSS) prohibits the storage of the full contents of any magnetic-stripe, CVV2 or PIN block data beyond transaction authorization. To help ensure merchants and agents meet PCI DSS requirements, Visa has developed the Payment Application Best Practices (PABP). Members are encouraged to work closely with their merchants and agents to ensure they use secure payment applications that have been validated against the PABP.

Under the PCI DSS, merchants and agents are prohibited from storing the full contents of any magnetic-stripe, CVV2 or PIN block data beyond transaction authorization. All entities that use payment applications should limit data retention to the minimum needed for business purposes and verify that their applications do not store prohibited data. Certain payment applications inadvertently store prohibited data and were not developed using secure coding procedures. To address such vulnerabilities, Visa developed a set of best practices for payment applications.

The requirements for the PABP are derived from the Payment Card Industry Data Security Standard (PCI DSS) and the PCI DSS Security Audit Procedures. Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Payment applications, when implemented according to the PABP Implementation Guide, and when implemented into a PCI DSS compliant environment, should facilitate and support customers' PCI DSS compliance.

Covered Entities

The PABP applies to software vendors who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement. The PABP does not apply to payment software developed by merchants and agents if used only in-house (not sold to a third party), since this in-house developed payment software would be covered as part of the merchant's or agent's normal PCI DSS compliance.

All validated payment application products must be general releases and not beta versions.

For more information on Visa's Payment Application Best Practices (PABP), please visit:

http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

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

Copyright: The PABP information contained in this report is proprietary and confidential to Visa U.S.A. Inc. and its members.(C) 2007 Visa U.S.A. Inc.

(*) DISCLAIMER The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. 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

71 unique issues detected across 21 sections of the regulation:

	Section	No. of Issues
1.	Securely delete any log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems. (Requirement 1.1.6)	18
2.	Application must require unique usernames and complex passwords for all administrative access and for all access to cardholder data. (Requirement 3.1)	52
3.	Access to PCs, servers, and databases with payment applications must require a unique username and complex password. (Requirement 3.2)	52
4.	Encrypt application passwords. (Requirement 3.3)	13
5.	Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. (Requirement 5.1)	71
6.	Unvalidated input. (Requirement 5.1.1)	46
7.	Broken access control. (Requirement 5.1.2)	5
8.	Broken authentication and session management. (Requirement 5.1.3)	15
9.	Cross-site scripting (XSS) attacks. (Requirement 5.1.4)	9
10.	Buffer overflows. (Requirement 5.1.5)	-
11.	Injection flaws. (Requirement 5.1.6)	32
12.	Improper error handling. (Requirement 5.1.7)	12

Section	No. of Issues
13. Insecure storage. (Requirement 5.1.8)	2
14. Insecure configuration management. (Requirement 5.1.9)	10
15. Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle. (Requirement 5.2)	3
16. Removal of test data and accounts before production systems become active. (Requirement 5.2.5)	13
17. Removal of custom application accounts, usernames, and passwords before applications are released to customers. (Requirement 5.2.6)	21
18. Review of custom code prior to release to customers, to identify any potential coding vulnerability. (Requirement 5.2.7)	71
19. If vendors, resellers/integrators, or customers can access customers' applications remotely, the remote access software must be implemented securely. (Requirement 11.3)	10
20. Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks. (Requirement 12.1)	1
21. Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. (Requirement 13.1)	1

Unique Compliance-related Issues Detected

71 unique issues detected across 21 sections of the regulation:

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

ID	URL	Parameter/Cookie	Test Name	Sections
26	http://local/altoro/search.aspx		Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
27	http://local/altoro/bank/transfer.aspx	creditAccount	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
28	http://local/altoro/bank/transfer.aspx	debitAccount	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
29	http://local/altoro/bank/customize.aspx	lang	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
30	http://local/altoro/cgi.exe	m	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
31	http://local/altoro/comment.aspx	name	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
32	http://local/altoro/subscribe.aspx	txtEmail	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
33	http://local/altoro/search.aspx	txtSearch	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
34	http://local/altoro/bank/login.aspx	uid	Cross-Site Scripting	2, 3, 4, 5, 6, 8, 9, 18, 19
35	http://local/altoro/bank/login.aspx		Predictable Login Credentials	2, 3, 5, 7, 14, 18
36	http://local/altoro/cgi.exe	m	Format String Remote Command Execution	5, 11, 18, 19
37	http://local/altoro/bank/customize.aspx	lang	HTTP Response Splitting	2, 3, 4, 5, 6, 8, 18
38	http://local/altoro/comment.aspx	name	Link Injection (facilitates Cross-Site Request Forgery)	2, 3, 4, 5, 6, 8, 18
39	http://local/altoro/search.aspx	txtSearch	Link Injection (facilitates Cross-Site Request Forgery)	2, 3, 4, 5, 6, 8, 18
40	http://local/altoro/bank/login.aspx		Unencrypted Login Request	1, 4, 5, 8, 13, 17, 18, 20, 21
41	http://local/altoro/default.aspx	content	Poison Null Byte Files Retrieval	5, 6, 7, 17, 18
42	http://local/altoro/bank/login.aspx		HTML Comments Sensitive Information Disclosure	1, 2, 3, 5, 15, 16, 17, 18
43	http://local/altoro/bank/account.aspx		HTML Comments Sensitive Information Disclosure	1, 2, 3, 5, 15, 16, 17, 18
44	http://local/altoro/bank/transaction.aspx	after	SQL Injection	2, 3, 5, 6, 11, 18
45	http://local/altoro/bank/transaction.aspx	before	SQL Injection	2, 3, 5, 6, 11, 18
46	http://local/altoro/bank/transfer.aspx	creditAccount	SQL Injection	2, 3, 5, 6, 11, 18
47	http://local/altoro/bank/transfer.aspx	debitAccount	SQL Injection	2, 3, 5, 6, 11, 18
48	http://local/altoro/bank/account.aspx	listAccounts	SQL Injection	2, 3, 5, 6, 11, 18
49	http://local/altoro/bank/login.aspx	passw	SQL Injection	2, 3, 5, 6, 11, 18
50	http://local/altoro/subscribe.aspx	txtEmail	SQL Injection	2, 3, 5, 6, 11, 18
51	http://local/altoro/bank/login.aspx	uid	SQL Injection	2, 3, 5, 6, 11, 18
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	Application Error	1, 5, 12, 16, 17, 18
53	http://local/altoro/bank/transaction.aspx	after	Application Error	1, 5, 12, 16, 17, 18
54	http://local/altoro/bank/transaction.aspx	before	Application Error	1, 5, 12, 16, 17, 18

ID	URL	Parameter/Cookie	Test Name	Sections
55	http://local/altoro/comment.aspx	cfile	Application Error	1, 5, 12, 16, 17, 18
56	http://local/altoro/bank/transfer.aspx	creditAccount	Application Error	1, 5, 12, 16, 17, 18
57	http://local/altoro/bank/transfer.aspx	debitAccount	Application Error	1, 5, 12, 16, 17, 18
58	http://local/altoro/bank/account.aspx	listAccounts	Application Error	1, 5, 12, 16, 17, 18
59	http://local/altoro/bank/login.aspx	passw	Application Error	1, 5, 12, 16, 17, 18
60	http://local/altoro/bank/transfer.aspx	transferAmount	Application Error	1, 5, 12, 16, 17, 18
61	http://local/altoro/subscribe.aspx	txtEmail	Application Error	1, 5, 12, 16, 17, 18
62	http://local/altoro/bank/login.aspx	uid	Application Error	1, 5, 12, 16, 17, 18
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE	Unencrypted __VIEWSTATE Parameter	1, 2, 3, 5, 14, 17, 18
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE	Unencrypted __VIEWSTATE Parameter	1, 2, 3, 5, 14, 17, 18
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE	Unencrypted __VIEWSTATE Parameter	1, 2, 3, 5, 14, 17, 18
66	http://local/altoro/bank/transaction.aspx	__VIEWSTATE	Unsigned __VIEWSTATE Parameter	5, 14, 18
67	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE	Unsigned __VIEWSTATE Parameter	5, 14, 18
68	http://local/altoro/bank/customize.aspx	__VIEWSTATE	Unsigned __VIEWSTATE Parameter	5, 14, 18
69	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	XPath Injection	2, 3, 5, 6, 11, 17, 18
70	http://local/altoro/bank/login.aspx	passw	Login Page SQL Injection	2, 3, 5, 6, 7, 8, 18
71	http://local/altoro/bank/login.aspx	uid	Login Page SQL Injection	2, 3, 5, 6, 7, 8, 18

Compliance-Related Issues and Section References

1) **Securely delete any log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems.**

(Requirement 1.1.6)

18 Issues

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
40	http://local/altoro/bank/login.aspx	

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before
55	http://local/altoro/comment.aspx	cfile
56	http://local/altoro/bank/transfer.aspx	creditAccount
57	http://local/altoro/bank/transfer.aspx	debitAccount
58	http://local/altoro/bank/account.aspx	listAccounts

59	http://local/altoro/bank/login.aspx	passw
60	http://local/altoro/bank/transfer.aspx	transferAmount
61	http://local/altoro/subscribe.aspx	txtEmail
62	http://local/altoro/bank/login.aspx	uid

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

2) Application must require unique usernames and complex passwords for all administrative access and for all access to cardholder data.

(Requirement 3.1)

52 Issues

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
3	http://local/altoro/bank/login.aspx	
4	http://local/altoro/subscribe.aspx	
5	http://local/altoro/bank/transaction.aspx	after
6	http://local/altoro/bank/transaction.aspx	before
7	http://local/altoro/bank/transfer.aspx	creditAccount
8	http://local/altoro/bank/transfer.aspx	debitAccount
9	http://local/altoro/bank/account.aspx	listAccounts
10	http://local/altoro/bank/login.aspx	passw
11	http://local/altoro/subscribe.aspx	txtEmail
12	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
13	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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments
19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name
32	http://local/altoro/subscribe.aspx	txtEmail
33	http://local/altoro/search.aspx	txtSearch
34	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
35	http://local/altoro/bank/login.aspx	

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
37	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
38	http://local/altoro/comment.aspx	name
39	http://local/altoro/search.aspx	txtSearch

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	http://local/altoro/bank/login.aspx	uid

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

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
69	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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

3) Access to PCs, servers, and databases with payment applications must require a unique username and complex password.

(Requirement 3.2)

52 Issues

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
3	http://local/altoro/bank/login.aspx	
4	http://local/altoro/subscribe.aspx	
5	http://local/altoro/bank/transaction.aspx	after
6	http://local/altoro/bank/transaction.aspx	before
7	http://local/altoro/bank/transfer.aspx	creditAccount
8	http://local/altoro/bank/transfer.aspx	debitAccount

9	http://local/altoro/bank/account.aspx	listAccounts
10	http://local/altoro/bank/login.aspx	passw
11	http://local/altoro/subscribe.aspx	txtEmail
12	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
13	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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments

19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name
32	http://local/altoro/subscribe.aspx	txtEmail
33	http://local/altoro/search.aspx	txtSearch
34	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
35	http://local/altoro/bank/login.aspx	

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
37	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
38	http://local/altoro/comment.aspx	name
39	http://local/altoro/search.aspx	txtSearch

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	http://local/altoro/bank/login.aspx	uid

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

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
69	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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

4) Encrypt application passwords.

(Requirement 3.3)

13 Issues

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

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
37	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
38	http://local/altoro/comment.aspx	name
39	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
40	http://local/altoro/bank/login.aspx	

5) Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities.

(Requirement 5.1)

71 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/	

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
3	http://local/altoro/bank/login.aspx	
4	http://local/altoro/subscribe.aspx	
5	http://local/altoro/bank/transaction.aspx	after
6	http://local/altoro/bank/transaction.aspx	before
7	http://local/altoro/bank/transfer.aspx	creditAccount
8	http://local/altoro/bank/transfer.aspx	debitAccount
9	http://local/altoro/bank/account.aspx	listAccounts
10	http://local/altoro/bank/login.aspx	passw
11	http://local/altoro/subscribe.aspx	txtEmail
12	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
13	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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments
19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name
32	http://local/altoro/subscribe.aspx	txtEmail
33	http://local/altoro/search.aspx	txtSearch
34	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
35	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
36	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
37	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
38	http://local/altoro/comment.aspx	name
39	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
40	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
41	http://local/altoro/default.aspx	content

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before

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

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

Unsigned __VIEWSTATE Parameter

Security Risks

- It may be possible to undermine application logic

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify the property of each ASP.NET page to sign the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
66	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
67	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
68	http://local/altoro/bank/customize.aspx	__VIEWSTATE

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
69	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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

6) Unvalidated input.

(Requirement 5.1.1)

46 Issues

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

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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments
19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name
32	http://local/altoro/subscribe.aspx	txtEmail

33	http://local/altoro/search.aspx	txtSearch
34	http://local/altoro/bank/login.aspx	uid

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
37	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
38	http://local/altoro/comment.aspx	name
39	http://local/altoro/search.aspx	txtSearch

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
41	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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	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
69	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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

7) Broken access control.

(Requirement 5.1.2)

5 Issues

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
13	http://local/altoro/bank/login.aspx	passw

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
35	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
41	http://local/altoro/default.aspx	content

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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

8) Broken authentication and session management.

(Requirement 5.1.3)

15 Issues

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

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
37	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
38	http://local/altoro/comment.aspx	name
39	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
40	http://local/altoro/bank/login.aspx	

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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

9) Cross-site scripting (XSS) attacks.

(Requirement 5.1.4)

9 Issues

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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name

32	http://local/altoro/subscribe.aspx	txtEmail
33	http://local/altoro/search.aspx	txtSearch
34	http://local/altoro/bank/login.aspx	uid

10) Buffer overflows.

(Requirement 5.1.5)

No issues.

11) Injection flaws.

(Requirement 5.1.6)

32 Issues

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

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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments
19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	http://local/altoro/bank/login.aspx	uid

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
36	http://local/altoro/cgi.exe	m

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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	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
69	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te

12) Improper error handling.

(Requirement 5.1.7)

12 Issues

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before
55	http://local/altoro/comment.aspx	cfile
56	http://local/altoro/bank/transfer.aspx	creditAccount
57	http://local/altoro/bank/transfer.aspx	debitAccount
58	http://local/altoro/bank/account.aspx	listAccounts
59	http://local/altoro/bank/login.aspx	passw
60	http://local/altoro/bank/transfer.aspx	transferAmount
61	http://local/altoro/subscribe.aspx	txtEmail
62	http://local/altoro/bank/login.aspx	uid

13) Insecure storage.

(Requirement 5.1.8)

2 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/	

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
40	http://local/altoro/bank/login.aspx	

14) Insecure configuration management.

(Requirement 5.1.9)

10 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/	

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
13	http://local/altoro/bank/login.aspx	passw

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
35	http://local/altoro/bank/login.aspx	

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

Unsigned __VIEWSTATE Parameter

Security Risks

- It may be possible to undermine application logic

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify the property of each ASP.NET page to sign the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
66	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
67	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
68	http://local/altoro/bank/customize.aspx	__VIEWSTATE

15) Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.

(Requirement 5.2)

3 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/	

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

16) Removal of test data and accounts before production systems become active.

(Requirement 5.2.5)

13 Issues

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before
55	http://local/altoro/comment.aspx	cfile
56	http://local/altoro/bank/transfer.aspx	creditAccount
57	http://local/altoro/bank/transfer.aspx	debitAccount
58	http://local/altoro/bank/account.aspx	listAccounts
59	http://local/altoro/bank/login.aspx	passw
60	http://local/altoro/bank/transfer.aspx	transferAmount
61	http://local/altoro/subscribe.aspx	txtEmail
62	http://local/altoro/bank/login.aspx	uid

17) Removal of custom application accounts, usernames, and passwords before applications are released to customers.

(Requirement 5.2.6)

21 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/	

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
40	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
41	http://local/altoro/default.aspx	content

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before
55	http://local/altoro/comment.aspx	cfile
56	http://local/altoro/bank/transfer.aspx	creditAccount
57	http://local/altoro/bank/transfer.aspx	debitAccount
58	http://local/altoro/bank/account.aspx	listAccounts
59	http://local/altoro/bank/login.aspx	passw
60	http://local/altoro/bank/transfer.aspx	transferAmount

61	http://local/altoro/subscribe.aspx	txtEmail
62	http://local/altoro/bank/login.aspx	uid

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

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
69	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te

18) Review of custom code prior to release to customers, to identify any potential coding vulnerability.

(Requirement 5.2.7)

71 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/	

Possible Server Path Disclosure Pattern Found

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which may help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Upgrade to the latest version of ATutor

Issues:

Issue ID	URL	Parameter/Cookie
2	http://local/altoro/feedback.aspx	

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
3	http://local/altoro/bank/login.aspx	
4	http://local/altoro/subscribe.aspx	
5	http://local/altoro/bank/transaction.aspx	after
6	http://local/altoro/bank/transaction.aspx	before
7	http://local/altoro/bank/transfer.aspx	creditAccount
8	http://local/altoro/bank/transfer.aspx	debitAccount
9	http://local/altoro/bank/account.aspx	listAccounts
10	http://local/altoro/bank/login.aspx	passw
11	http://local/altoro/subscribe.aspx	txtEmail
12	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
13	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
14	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:But
15	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
16	http://local/altoro/bank/transaction.aspx	before
17	http://local/altoro/subscribe.aspx	btnSubmit
18	http://local/altoro/comment.aspx	comments
19	http://local/altoro/comment.aspx	email_addr
20	http://local/altoro/bank/login.aspx	passw
21	http://local/altoro/comment.aspx	subject
22	http://local/altoro/comment.aspx	submit
23	http://local/altoro/bank/transfer.aspx	transfer
24	http://local/altoro/subscribe.aspx	txtEmail
25	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
26	http://local/altoro/search.aspx	
27	http://local/altoro/bank/transfer.aspx	creditAccount
28	http://local/altoro/bank/transfer.aspx	debitAccount
29	http://local/altoro/bank/customize.aspx	lang
30	http://local/altoro/cgi.exe	m
31	http://local/altoro/comment.aspx	name
32	http://local/altoro/subscribe.aspx	txtEmail
33	http://local/altoro/search.aspx	txtSearch
34	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
35	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
36	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
37	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
38	http://local/altoro/comment.aspx	name
39	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
40	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
41	http://local/altoro/default.aspx	content

HTML Comments Sensitive Information Disclosure

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Debugging information was left by the programmer in web pages

Remediation Tasks:

Remove sensitive information from HTML comments

Issues:

Issue ID	URL	Parameter/Cookie
42	http://local/altoro/bank/login.aspx	
43	http://local/altoro/bank/account.aspx	

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
44	http://local/altoro/bank/transaction.aspx	after
45	http://local/altoro/bank/transaction.aspx	before
46	http://local/altoro/bank/transfer.aspx	creditAccount
47	http://local/altoro/bank/transfer.aspx	debitAccount
48	http://local/altoro/bank/account.aspx	listAccounts
49	http://local/altoro/bank/login.aspx	passw
50	http://local/altoro/subscribe.aspx	txtEmail
51	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
52	http://local/altoro/bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:Te
53	http://local/altoro/bank/transaction.aspx	after
54	http://local/altoro/bank/transaction.aspx	before

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

Unencrypted __VIEWSTATE Parameter

Security Risks

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify your Web.Config file to encrypt the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
63	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
64	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
65	http://local/altoro/bank/customize.aspx	__VIEWSTATE

Unsigned __VIEWSTATE Parameter

Security Risks

- It may be possible to undermine application logic

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Modify the property of each ASP.NET page to sign the VIEWSTATE parameter

Issues:

Issue ID	URL	Parameter/Cookie
66	http://local/altoro/bank/transaction.aspx	__VIEWSTATE
67	http://local/altoro/bank/queryxpath.aspx	__VIEWSTATE
68	http://local/altoro/bank/customize.aspx	__VIEWSTATE

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
69	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
70	http://local/altoro/bank/login.aspx	passw
71	http://local/altoro/bank/login.aspx	uid

19) If vendors, resellers/integrators, or customers can access customers' applications remotely, the remote access software must be implemented securely.

(Requirement 11.3)

10 Issues

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

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
36	http://local/altoro/cgi.exe	m

20) Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks.

(Requirement 12.1)

1 Issues

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
40	http://local/altoro/bank/login.aspx	

21) Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

(Requirement 13.1)

1 Issues

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
40	http://local/altoro/bank/login.aspx	