AppScan on Cloud

Security Report

Scan Name: SAST 2024-02-28 AltoroJ.irx

Technology: SAST

Report Name: Demo Scan

Report created at: Wednesday, February 28, 2024

Notes: Sample report for demo application.

Summary of security issues

High severity issues:	73
Medium severity issues:	21
Low severity issues:	11
Total security issues:	**105**

Scan Information

Scan started: Wednesday, February 28, 2024 5:43:14 AM (UTC)

Table of Contents

- Common API Call: Reflected Cross Site Scripting: Insecure Use of InnerHTML or OuterHTML
- Common API Call: Improper Handling of Exceptional Conditions: java.lang.Throwable.printStackTrace():void
- Common API Call: SQL Injection: java.sql.Statement.executeQuery(java.lang.String):java.sql.ResultSet
- Common API Call: Inappropriate Encoding for Output Context: java.io.PrintWriter.print(java.lang.Object):void
- Common API Call: Inappropriate Encoding for Output Context: java.io.PrintWriter.write(java.lang.String):void
- Common API Call: Validation Required: javax.servlet.http.HttpSession.setAttribute(java.lang.String;java.lang.Object):void
- Common API Call: Validation Required: javax.servlet.ServletRequest.setAttribute(java.lang.String;java.lang.Object):void
- Common API Call: Open Redirect: Allowing untrusted site by passing user controlled input
- Common API Call: Open Redirect: javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String):void
- Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(java.lang.String;java.lang.String):java.lang.String
- Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(java.lang.String;java.lang.String;com.ibm.security.appscan.altoromutual.model.Account[];int):com.ibm.security.appscan.altoromutual.model.Transaction[]
- Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(java.lang.String;java.lang.String):boolean
- Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
- Common Fix Point: Inappropriate Encoding for Output Context: com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(java.lang.String;javax.servlet.http.HttpServletRequest):javax.ws.rs.core.Response
- Common Fix Point: Validation Required: com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword(java.lang.String;java.lang.String):java.lang.String
- Common Fix Point:Cross-Site Scripting: com.ibm.security.appscan.altoromutual.model.Transaction.<init>(int;long;java.util.Date;java.lang.String;double):void
- Common Fix Point:Cross-Site Scripting: com.ibm.security.appscan.altoromutual.model.User.getAccounts():com.ibm.security.appscan.altoromutual.model.Account[]
- Common Fix Point:Cross-Site Scripting: java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder
- Common Fix Point:Cross-Site Scripting: java.util.ArrayList.add(java.lang.Object):boolean
- Common Fix Point:Cross-Site Scripting: javax.servlet.jsp.JspWriter.print(java.lang.String):void
- Common Fix Point:Command Injection: java.lang.Runtime.exec(java.lang.String[]):java.lang.Process
- Common Fix Point:SQL Injection: java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder
- Common Fix Point:SQL Injection: java.lang.StringBuilder.toString():java.lang.String
- Common Fix Point:Inappropriate Encoding for Output Context: com.ibm.security.appscan.altoromutual.model.Transaction.<init>(int;long;java.util.Date;java.lang.String;double):void
- Common Fix Point:Validation Required: javax.servlet.ServletRequest.setAttribute(java.lang.String;java.lang.Object):void
- Common Fix Point:Open Redirect: java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder

How to Fix

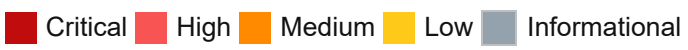
- Authentication.Entity - java.sql.DriverManager.getConnection(String):Connection
- Command Injection
- Cross-Site Scripting
- Improper Handling of Exceptional Conditions - java.lang.Throwable.printStackTrace():void
- Inappropriate Encoding for Output Context
- Open Redirect - Allowing untrusted site by passing user controlled input
- Open Redirect
- Reflected Cross Site Scripting - Insecure Use of Document.Write
- Reflected Cross Site Scripting - Insecure Use of InnerHTML or OuterHTML
- SQL Injection
- Validation Required

Summary

Total security issues: **105**

Issue Types: **9**

	Number of Issues
Command Injection	2
Cross-Site Scripting	34
Inappropriate Encoding for Output Context	16
Open Redirect	6
Reflected Cross Site Scripting	8
SQL Injection	19
Validation Required	7
Authentication.Entity	2
Improper Handling of Exceptional Conditions	11



Issues - By Fix Groups:

M	Common API Call: Authentication.Entity: java.sql.DriverManager.getConnection(java.lang.String):java.sql...

Fix Group ID:	7a116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	java.sql.DriverManager.getConnection(java.lang.String):java.sql.Connection
How to Fix:	Authentication.Entity

Issue 1 of 2

Issue ID:	68126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	7a116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():Connection:119
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():java.sql.Connection
Line	119
Source File	com\ibm\security\appscan\altoromutual\util\DBUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	255
API:	java.sql.DriverManager.getConnection(String):Connection
Caller:	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():Connection:119

Issue 1 of 2 - Details

Call

```
getConnection("jdbc:derby:altoro")
```

Issue 2 of 2

Issue ID:	6b126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	7a116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():Connection:127
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():java.sql.Connection
Line	127
Source File	com\ibm\security\appscan\altoromutual\util\DBUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	255
API:	java.sql.DriverManager.getConnection(String):Connection
Caller:	com.ibm.security.appscan.altoromutual.util.DBUtil.getConnection():Connection:127

Issue 2 of 2 - Details

Call

```
getConnection("jdbc:derby:altoro;create=true")
```

M Common API Call: Cross-Site Scripting: javax.servlet.jsp.JspWriter.print(java.lang.Object):void

Fix Group ID:	77116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.jsp.JspWriter.print(java.lang.Object):void
How to Fix:	Cross-Site Scripting

Issue 1 of 2

Issue ID:	d9116e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	77116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(Object):void org.apache.jsp.bank.transfer_jsp:101
Calling Method	org.apache.jsp.bank.transfer_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	101
Source File	org.apache.jsp.bank.transfer_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getAttribute(String):Object *via* org.apache.jsp.bank.transfer_jsp:101
Sink:	javax.servlet.jsp.JspWriter.print(Object):void *via* org.apache.jsp.bank.transfer_jsp:101

Issue 1 of 2 - Details

Trace

org.apache.jsp.bank.transfer_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.transfer_jsp:101
request.**getAttribute**("message")

org.apache.jsp.bank.transfer_jsp:101
Temp#17@0.print(**Temp#18@0**)

Issue 2 of 2

Issue ID:	cf126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	77116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(Object):void org.apache.jsp.subscribe_jsp:40
Calling Method	org.apache.jsp.subscribe_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	40
Source File	org.apache.jsp.subscribe_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getAttribute(String):Object *via* org.apache.jsp.subscribe_jsp:40
Sink:	javax.servlet.jsp.JspWriter.print(Object):void *via* org.apache.jsp.subscribe_jsp:40

Issue 2 of 2 - Details

Trace

org.apache.jsp.subscribe_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.subscribe_jsp:40
request.**getAttribute**("message_subscribe")

org.apache.jsp.subscribe_jsp:40
Temp#9@0.print(**Temp#10@0**)

H Common API Call: Cross-Site Scripting: javax.servlet.jsp.JspWriter.print(java.lang.String):void

Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.jsp.JspWriter.print(java.lang.String):void
How to Fix:	Cross-Site Scripting

Issue 1 of 14

Issue ID:	b5116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.customize_jsp:44
Calling Method	org.apache.jsp.bank.customize_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	44
Source File	org.apache.jsp.bank.customize_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.customize_jsp:44
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.customize_jsp:44

Issue 1 of 14 - Details

Trace

org.apache.jsp.bank.customize_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.customize_jsp:44
request.**getParameter**("lang")

org.apache.jsp.bank.customize_jsp:44
Temp#9@0.print(**Temp#10@0**)

Issue 2 of 14

Issue ID:	8e116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.admin_jsp:61
Calling Method	org.apache.jsp.admin.admin_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	61
Source File	org.apache.jsp.admin.admin_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.admin.admin_jsp:58
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.admin_jsp:61

Issue 2 of 14 - Details

Trace

org.apache.jsp.admin.admin_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.admin.admin_jsp:58
error = request.getSession().**getAttribute**("message")

org.apache.jsp.admin.admin_jsp:61
out.print(**error**)

Issue 3 of 14

Issue ID:	c1116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.queryxpath_jsp:36
Calling Method	org.apache.jsp.bank.queryxpath_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	36
Source File	org.apache.jsp.bank.queryxpath_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.queryxpath_jsp:36
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.queryxpath_jsp:36

Issue 3 of 14 - Details

Trace

org.apache.jsp.bank.queryxpath_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.queryxpath_jsp:36
request.**getParameter**("query")

org.apache.jsp.bank.queryxpath_jsp:36
Temp#13@0.print(**Temp#14@0**)

Issue 4 of 14

Issue ID:	9d116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.login_jsp:47
Calling Method	org.apache.jsp.admin.login_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	47
Source File	org.apache.jsp.admin.login_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getAttribute(String):Object *via* org.apache.jsp.admin.login_jsp:43
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.login_jsp:47

Issue 4 of 14 - Details

Trace

org.apache.jsp.admin.login_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.admin.login_jsp:43
error = request.**getAttribute**("loginError")

org.apache.jsp.admin.login_jsp:47
out.print(**error**)

Issue 5 of 14

Issue ID:	c7116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.transaction_jsp:126
Calling Method	org.apache.jsp.bank.transaction_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	126
Source File	org.apache.jsp.bank.transaction_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.transaction_jsp:126
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.transaction_jsp:126

Issue 5 of 14 - Details

Trace

org.apache.jsp.bank.transaction_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.transaction_jsp:126
request.**getParameter**("startDate")

org.apache.jsp.bank.transaction_jsp:126
Temp#19@0.print(**Temp#20@0**)

Issue 6 of 14

Issue ID:	ca116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.transaction_jsp:128
Calling Method	org.apache.jsp.bank.transaction_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	128
Source File	org.apache.jsp.bank.transaction_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.transaction_jsp:128
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.transaction_jsp:128

Issue 6 of 14 - Details

Trace

org.apache.jsp.bank.transaction_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.transaction_jsp:128
request.**getParameter**("endDate")

org.apache.jsp.bank.transaction_jsp:128
Temp#21@0.print(**Temp#22@0**)

Issue 7 of 14

Issue ID:	b4126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.feedback_jsp:59
Calling Method	org.apache.jsp.feedback_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	59
Source File	org.apache.jsp.feedback_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.feedback_jsp:33
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.feedback_jsp:59

Issue 7 of 14 - Details

Trace

org.apache.jsp.feedback_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.feedback_jsp:33
user = request.getSession().**getAttribute**("user")

org.apache.jsp.feedback_jsp:59
user.getLastName()

org.apache.jsp.feedback_jsp:59
Temp#19@0 = Temp#19@0.append(**Temp#20@0**)

org.apache.jsp.feedback_jsp:59
Temp#19@0.append(Temp#20@0).toString()

org.apache.jsp.feedback_jsp:59
Temp#18@0.print(**Temp#19@0.append(Temp#20@0).toString()**)

Issue 8 of 14

Issue ID:	b7126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.feedbacksuccess_jsp:42
Calling Method	org.apache.jsp.feedbacksuccess_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	42
Source File	org.apache.jsp.feedbacksuccess_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getAttribute(String):Object *via* org.apache.jsp.feedbacksuccess_jsp:42
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.feedbacksuccess_jsp:42

Issue 8 of 14 - Details

Trace

org.apache.jsp.feedbacksuccess_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.feedbacksuccess_jsp:42
request.**getAttribute**("message_feedback")

org.apache.jsp.feedbacksuccess_jsp:42
new StringBuilder().append(**request.getAttribute("message_feedback")**)

org.apache.jsp.feedbacksuccess_jsp:42
new StringBuilder().append(request.getAttribute("message_feedback")).toString()

org.apache.jsp.feedbacksuccess_jsp:42
Temp#14@0.print(**Temp#15@0**)

Issue 9 of 14

Issue ID:	ba126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.feedbacksuccess_jsp:46
Calling Method	org.apache.jsp.feedbacksuccess_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	46
Source File	org.apache.jsp.feedbacksuccess_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.feedbacksuccess_jsp:43
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.feedbacksuccess_jsp:46

Issue 9 of 14 - Details

Trace

org.apache.jsp.feedbacksuccess_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.feedbacksuccess_jsp:43
email = request.**getParameter**("email_addr")

org.apache.jsp.feedbacksuccess_jsp:46
email.toLowerCase()

org.apache.jsp.feedbacksuccess_jsp:46
sanitzieHtmlWithRegex(**email.toLowerCase()**)

org.apache.jsp.feedbacksuccess_jsp:46
out.print(**sanitzieHtmlWithRegex(email.toLowerCase())**)

Issue 10 of 14

Issue ID:	d2126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.util.serverStatusCheckService_jsp:4
Calling Method	org.apache.jsp.util.serverStatusCheckService_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	4
Source File	org.apache.jsp.util.serverStatusCheckService_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.util.serverStatusCheckService_jsp:4
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.util.serverStatusCheckService_jsp:4

Issue 10 of 14 - Details

Trace

org.apache.jsp.util.serverStatusCheckService_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.util.serverStatusCheckService_jsp:4
request.**getParameter**("HostName")

org.apache.jsp.util.serverStatusCheckService_jsp:4
out.print(**request.getParameter("HostName")**)

Issue 11 of 14

Issue ID:	bd126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.feedbacksuccess_jsp:48
Calling Method	org.apache.jsp.feedbacksuccess_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	48
Source File	org.apache.jsp.feedbacksuccess_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.feedbacksuccess_jsp:43
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.feedbacksuccess_jsp:48

Issue 11 of 14 - Details

Trace

org.apache.jsp.feedbacksuccess_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.feedbacksuccess_jsp:43
email = request.**getParameter**("email_addr")

org.apache.jsp.feedbacksuccess_jsp:48
email.toLowerCase()

org.apache.jsp.feedbacksuccess_jsp:48
sanitzieHtmlWithRegex(**email.toLowerCase()**)

org.apache.jsp.feedbacksuccess_jsp:48
out.print(**sanitzieHtmlWithRegex(email.toLowerCase())**)

Issue 12 of 14

Issue ID:	c6126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.index_jsp:91
Calling Method	org.apache.jsp.index_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	91
Source File	org.apache.jsp.index_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.io.BufferedReader.readLine():String *via* org.apache.jsp.index_jsp:86
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.index_jsp:91

Issue 12 of 14 - Details

Trace

org.apache.jsp.index_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.index_jsp:86
line = br.**readLine**()

org.apache.jsp.index_jsp:87
new StringBuilder().append(**line**)

org.apache.jsp.index_jsp:87
Temp@503#119=**new StringBuilder().append(line)**.append("
")

org.apache.jsp.index_jsp:87
text=**new StringBuilder().append(line).append("
")**.toString()

org.apache.jsp.index_jsp:91
out.print(**text**)

Issue 13 of 14

Issue ID:	c9126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.login_jsp:40
Calling Method	org.apache.jsp.login_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	40
Source File	org.apache.jsp.login_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.login_jsp:36
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.login_jsp:40

Issue 13 of 14 - Details

Trace

org.apache.jsp.login_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.login_jsp:36
error = request.getSession(1).**getAttribute**("loginError")

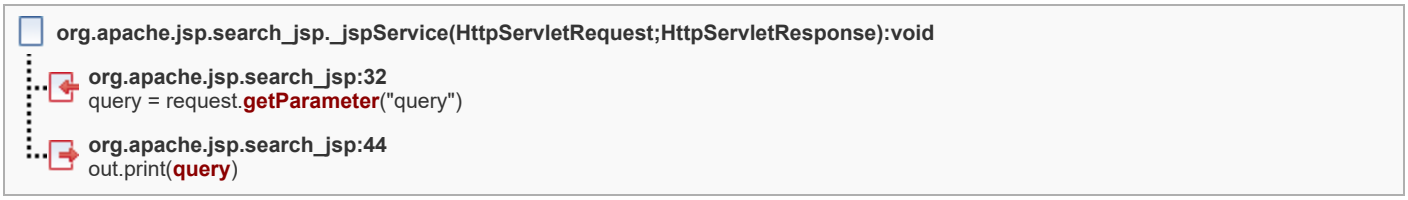
org.apache.jsp.login_jsp:40
out.print(**error**)

Issue 14 of 14

Issue ID:	cc126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	78116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.search_jsp:44
Calling Method	org.apache.jsp.search_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	44
Source File	org.apache.jsp.search_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.search_jsp:32
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.search_jsp:44

Issue 14 of 14 - Details

Trace



H Common API Call: Cross-Site Scripting: javax.servlet.jsp.JspWriter.println(java.lang.String):void

Fix Group ID:	8d116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.jsp.JspWriter.println(java.lang.String):void
How to Fix:	Cross-Site Scripting

Issue 1 of 4

Issue ID:	be116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.main_jsp:51
Calling Method	org.apache.jsp.bank.main_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	51
Source File	org.apache.jsp.bank.main_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.main_jsp:33
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.main_jsp:51

Issue 1 of 4 - Details

Trace

org.apache.jsp.bank.main_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.main_jsp:33
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.main_jsp:50
user.getAccounts()

org.apache.jsp.bank.main_jsp:51
account.getAccountName()

org.apache.jsp.bank.main_jsp:51
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.main_jsp:51
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>")

org.apache.jsp.bank.main_jsp:51
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>").StringBuild

org.apache.jsp.bank.main_jsp:51
out.println(new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).StringBuilder

Issue 2 of 4

Issue ID:	c4116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.queryxpath_jsp:47
Calling Method	org.apache.jsp.bank.queryxpath_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	47
Source File	org.apache.jsp.bank.queryxpath_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.queryxpath_jsp:41
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.queryxpath_jsp:47

Issue 2 of 4 - Details

Trace

org.apache.jsp.bank.queryxpath_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.queryxpath_jsp:41
request.**getParameter**("query")

org.apache.jsp.bank.queryxpath_jsp:41
results = searchArticles(**request.getParameter("query")**, request.getSession().getServletContext().getRealPath("/pr/Docs.xml"))

org.apache.jsp.bank.queryxpath_jsp:47
valueOf(**result**)

org.apache.jsp.bank.queryxpath_jsp:47
new StringBuilder(**valueOf(result)**)

org.apache.jsp.bank.queryxpath_jsp:47
new StringBuilder().append("
")

org.apache.jsp.bank.queryxpath_jsp:47
**new StringBuilder().append("
")**.toString()

org.apache.jsp.bank.queryxpath_jsp:47
out.println(**new StringBuilder().append("
").toString()**)

Issue 3 of 4

Issue ID:	d3116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.transfer_jsp:70
Calling Method	org.apache.jsp.bank.transfer_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	70
Source File	org.apache.jsp.bank.transfer_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.transfer_jsp:32
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.transfer_jsp:70

Issue 3 of 4 - Details

Trace

org.apache.jsp.bank.transfer_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.transfer_jsp:32
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.transfer_jsp:69
user.getAccounts()

org.apache.jsp.bank.transfer_jsp:70
account.getAccountName()

org.apache.jsp.bank.transfer_jsp:70
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.transfer_jsp:70
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>")

org.apache.jsp.bank.transfer_jsp:70
new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>").StringBuild

org.apache.jsp.bank.transfer_jsp:70
out.println(new StringBuilder().append(account.getAccountId()).append("\" >").append(account.getAccountId()).append(" ").append(account.getAccountName()).StringBuilder

Issue 4 of 4

Issue ID:	d6116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.transfer_jsp:82
Calling Method	org.apache.jsp.bank.transfer_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	82
Source File	org.apache.jsp.bank.transfer_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.transfer_jsp:32
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.transfer_jsp:82

Issue 4 of 4 - Details

Trace

org.apache.jsp.bank.transfer_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.transfer_jsp:32
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.transfer_jsp:81
user.getAccounts()

org.apache.jsp.bank.transfer_jsp:82
account.getAccountName()

org.apache.jsp.bank.transfer_jsp:82
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.transfer_jsp:82
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>")

org.apache.jsp.bank.transfer_jsp:82
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>").StringBuilde

org.apache.jsp.bank.transfer_jsp:82
out.println(new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).

H Common API Call: Reflected Cross Site Scripting: Insecure Use of Document.Write

Fix Group ID:	74116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	Insecure Use of Document.Write
How to Fix:	Insecure Use of Document.Write

Issue 1 of 1

Issue ID:	e2116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	74116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:50
Line	50
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/disclaimer.htm
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of Document.Write
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:50

Issue 1 of 1 - Details

Call

```
.write(encodeURI(sDst)
```

H Common API Call: Reflected Cross Site Scripting: Insecure Use of InnerHTML or OuterHTML

Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	Insecure Use of InnerHTML or OuterHTML
How to Fix:	Insecure Use of Document.Write

Issue 1 of 7

Issue ID:	e5116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:46
Line	46
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:46

Issue 1 of 7 - Details

Call

```
.innerHTML=jsonFetchHostName
```

Issue 2 of 7

Issue ID:	e8116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:48
Line	48
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:48

Issue 2 of 7 - Details

Call

```
.innerHTML=jsonFetchHostStatus
```

Issue 3 of 7

Issue ID:	eb116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:53
Line	53
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:53

Issue 3 of 7 - Details

Call

```
.innerHTML=sLastHostName
```

Issue 4 of 7

Issue ID:	ee116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:60
Line	60
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:60

Issue 4 of 7 - Details

Call

```
.innerHTML=sLastHostName
```

Issue 5 of 7

Issue ID:	f1116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:67
Line	67
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:67

Issue 5 of 7 - Details

Call

```
.innerHTML=sLastHostName
```

Issue 6 of 7

Issue ID:	f4116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:74
Line	74
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/serverStatusCheck.html
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\serverStatusCheck.html:74

Issue 6 of 7 - Details

Call

```
.innerHTML=sLastHostName
```

Issue 7 of 7

Issue ID:	f7116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	87116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\util\swfobject.js:4
Line	4
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/util/swfobject.js
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
API:	Insecure Use of InnerHTML or OuterHTML
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\util\swfobject.js:4

Issue 7 of 7 - Details

Call

```
.innerHTML=ab
```

L Common API Call: Improper Handling of Exceptional Conditions: java.lang.Throwable.printStackTrace():void

Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	java.lang.Throwable.printStackTrace():void
How to Fix:	Improper Handling of Exceptional Conditions

Issue 1 of 11

Issue ID:	ab126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.ServletUtil.searchArticles(String;String):String[]:132
Calling Method	com.ibm.security.appscan.altoromutual.util.ServletUtil.searchArticles(java.lang.String;java.lang.String):java.lang.String[]
Line	132
Source File	com\ibm\security\appscan\altoromutual\util\ServletUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.ServletUtil.searchArticles(String;String):String[]:132

Issue 1 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 2 of 11

Issue ID:	3b126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.model.User.getAccounts():Account[]:80
Calling Method	com.ibm.security.appscan.altoromutual.model.User.getAccounts():com.ibm.security.appscan.altoromutual.model.Account[]
Line	80
Source File	com\ibm\security\appscan\altoromutual\model\User.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.model.User.getAccounts():Account[]:80

Issue 2 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 3 of 11

Issue ID:	62126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.DBUtil():void:80
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.<init>():void
Line	80
Source File	com\ibm\security\appscan\altoromutual\util\DBUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.DBUtil():void:80

Issue 3 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 4 of 11

Issue ID:	65126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.DBUtil():void:94
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.<init>():void
Line	94
Source File	com\ibm\security\appscan\altoromutual\util\DBUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.DBUtil():void:94

Issue 4 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 5 of 11

Issue ID:	6e126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUsernames():String[]:442
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUsernames():java.lang.String[]
Line	442
Source File	com\ibm\security\appscan\altoromutual\util\DBUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUsernames():String[]:442

Issue 5 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 6 of 11

Issue ID:	ae126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.ServletUtil.establishSession(String;HttpSession):Cookie:345
Calling Method	com.ibm.security.appscan.altoromutual.util.ServletUtil.establishSession(java.lang.String;javax.servlet.http.HttpSession):javax.servlet.http.Cookie
Line	345
Source File	com\ibm\security\appscan\altoromutual\util\ServletUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.ServletUtil.establishSession(String;HttpSession):Cookie:345

Issue 6 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 7 of 11

Issue ID:	50126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.servlet.LoginServlet.doPost(HttpServletRequest;HttpServletResponse):void: 99
Calling Method	com.ibm.security.appscan.altoromutual.servlet.LoginServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	99
Source File	com\ibm\security\appscan\altoromutual\servlet\LoginServlet.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.servlet.LoginServlet.doPost(HttpServletRequest;HttpServletResponse):void: 99

Issue 7 of 11 - Details

Call

```
ex.printStackTrace()
```

Issue 8 of 11

Issue ID:	b1126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.util.ServletUtil.isLoggedin(HttpServletRequest):boolean:358
Calling Method	com.ibm.security.appscan.altoromutual.util.ServletUtil.isLoggedin(javax.servlet.http.HttpServletRequest):boolean
Line	358
Source File	com\ibm\security\appscan\altoromutual\util\ServletUtil.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.util.ServletUtil.isLoggedin(HttpServletRequest):boolean:358

Issue 8 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 9 of 11

Issue ID:	fa116e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.Log4AltoroJ():void:35
Calling Method	com.ibm.security.appscan.Log4AltoroJ.<init>():void
Line	35
Source File	com\ibm\security\appscan\Log4AltoroJ.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.Log4AltoroJ():void:35

Issue 9 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 10 of 11

Issue ID:	fd116e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.api.AccountAPI.getAccountBalance(String;HttpServletRequest):Response:120
Calling Method	com.ibm.security.appscan.altoromutual.api.AccountAPI.getAccountBalance(java.lang.String;javax.servlet.http.HttpServletRequest):javax.ws.rs.core.Response
Line	120
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.api.AccountAPI.getAccountBalance(String;HttpServletRequest):Response:120

Issue 10 of 11 - Details

Call

```
e.printStackTrace()
```

Issue 11 of 11

Issue ID:	1b126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Low
Status	Open
Fix Group ID:	88116e59-fcd5-ee11-9f02-14cb65725114
Location	com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(String;HttpServletRequest):Response:41
Calling Method	com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(java.lang.String;javax.servlet.http.HttpServletRequest):javax.ws.rs.core.Response
Line	41
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	497
API:	java.lang.Throwable.printStackTrace():void
Caller:	com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(String;HttpServletRequest):Response:41

Issue 11 of 11 - Details

Call

```
e.printStackTrace()
```

H	Common API Call: SQL Injection: java.sql.Statement.executeQuery(java.lang.String):java.sql.Resu...

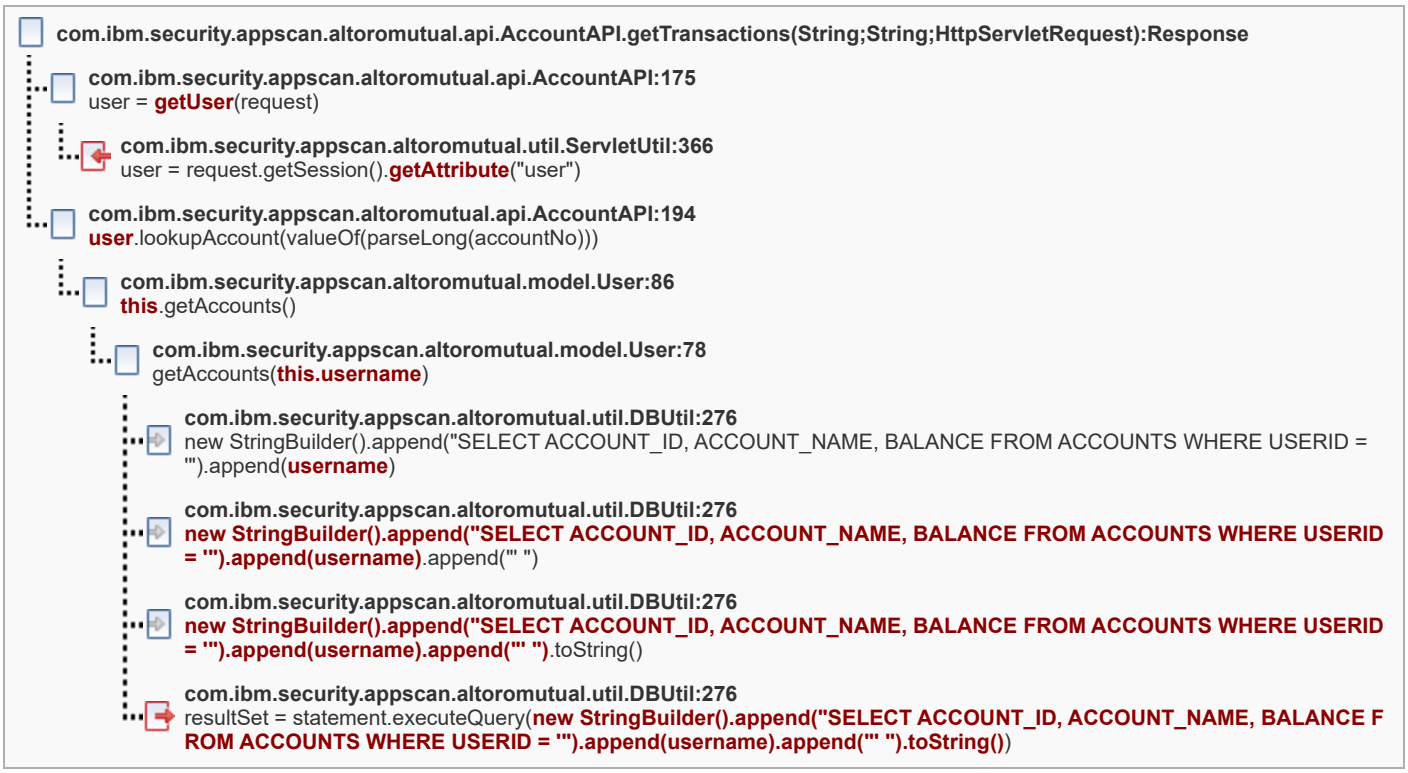
Fix Group ID:	72116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	java.sql.Statement.executeQuery(java.lang.String):java.sql.ResultSet
How to Fix:	SQL Injection

Issue 1 of 1

Issue ID:	7d126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	72116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:276
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getAccounts(java.lang.String):com.ibm.security.appscan.altoromutual.model.Account[]
Line	276
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* com.ibm.security.appscan.altoromutual.util.ServletUtil:366
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:276

Issue 1 of 1 - Details

Trace



M Common API Call: Inappropriate Encoding for Output Context: java.io.PrintWriter.print(java.lang.Object):void

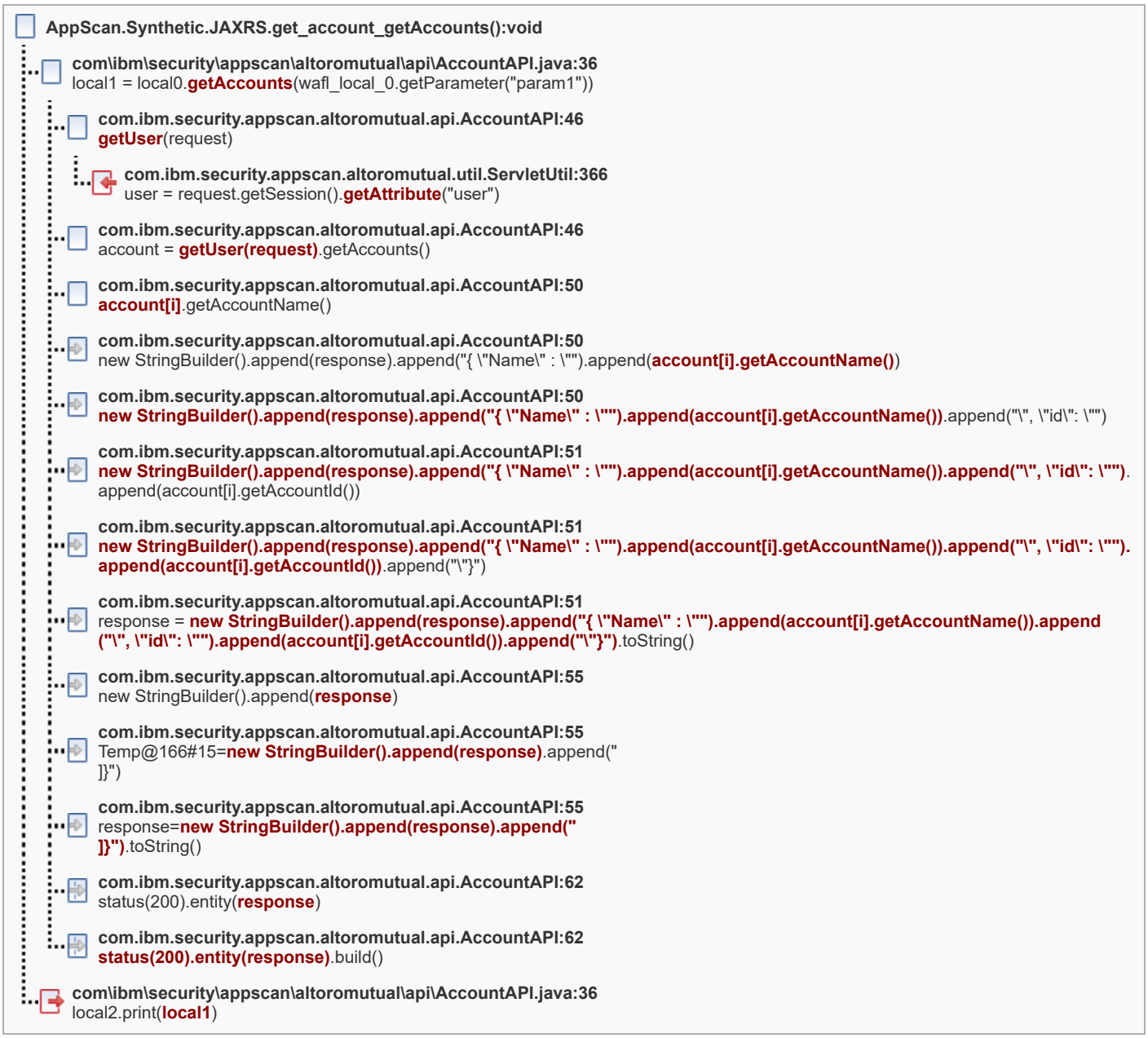
Fix Group ID:	89116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	java.io.PrintWriter.print(java.lang.Object):void
How to Fix:	Inappropriate Encoding for Output Context

Issue 1 of 1

Issue ID:	00126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	89116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:36
Calling Method	AppScan.Synthetic.JAXRS.get_account_getAccounts():void
Line	36
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* com.ibm.security.appscan.altoromutual.util.ServletUtil: 366
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:36

Issue 1 of 1 - Details

Trace



H Common API Call: Inappropriate Encoding for Output Context: java.io.PrintWriter.write(java.lang.String):void

Fix Group ID:	81116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	java.io.PrintWriter.write(java.lang.String):void
How to Fix:	Inappropriate Encoding for Output Context

Issue 1 of 1

Issue ID:	59126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	81116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.write(String):void com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:102
Calling Method	com.ibm.security.appscan.altoromutual.servlet.SurveyServlet.doGet(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	102
Source File	com.ibm.security.appscan.altoromutual.servlet.SurveyServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:82
Sink:	java.io.PrintWriter.write(String):void *via* com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:102

Issue 1 of 1 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet.doGet(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:82
request.**getParameter**("txtEmail")

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:82
new StringBuilder().append("<h1>Thanks</h1><div width=\"99%\"> Thanks for your entry. We will contact you shortly at:

").append(**request.getParameter("txtEmail")**)

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:82
**new StringBuilder().append("<h1>Thanks</h1><div width=\"99%\"> Thanks for your entry. We will contact you shortly at:

 ").append(request.getParameter("txtEmail"))**.append(" ")

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:82
content = **new StringBuilder().append("<h1>Thanks</h1><div width=\"99%\"> Thanks for your entry. We will contact you shortly at:

 ").append(request.getParameter("txtEmail")).append(" ")**.toString()

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:102
response.getWriter().write(**content**)

H Common API Call: Validation Required: javax.servlet.http.HttpSession.setAttribute(java.lang.String;ja...

Fix Group ID:	8c116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.http.HttpSession.setAttribute(java.lang.String;java.lang.Object):void
How to Fix:	Validation Required

Issue 1 of 1

Issue ID:	56126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8c116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpSession.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:99
Calling Method	com.ibm.security.appscan.altoromutual.servlet.SurveyServlet.doGet(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	99
Source File	com.ibm.security.appscan.altoromutual.servlet.SurveyServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:47
Sink:	javax.servlet.http.HttpSession.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:99

Issue 1 of 1 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet.doGet(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:47
step = request.**getParameter**("step")

com.ibm.security.appscan.altoromutual.servlet.SurveyServlet:99
request.getSession().setAttribute("surveyStep", **step**)

H Common API Call: Validation Required: javax.servlet.ServletRequest.setAttribute(java.lang.String;java...

Fix Group ID:	75116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.ServletRequest.setAttribute(java.lang.String;java.lang.Object):void
How to Fix:	Validation Required

Issue 1 of 2

Issue ID:	4d126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	75116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.ServletRequest.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:52
Calling Method	com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	52
Source File	com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:50
Sink:	javax.servlet.ServletRequest.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:52

Issue 1 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:50
name = request.**getParameter**("name")

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:52
request.setAttribute("message_feedback", **name**)

Issue 2 of 2

Issue ID:	53126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	75116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.ServletRequest.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50
Calling Method	com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	50
Source File	com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:43
Sink:	javax.servlet.ServletRequest.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50

Issue 2 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet.doPost(HttpServletRequest;HttpServletResponse):void

- **com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:43**
  email = request.**getParameter**("txtEmail")
- **com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50**
  new StringBuilder().append("Thank you. Your **email** ").append(**email**)
- **com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50**
  new StringBuilder().append("Thank you. Your email ").append(email).append(" has been accepted.")
- **com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50**
  new StringBuilder().append("Thank you. Your email ").append(email).append(" has been accepted.").toString()
- **com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet:50**
  request.setAttribute("message_subscribe", **new StringBuilder().append("Thank you. Your email ").append(email).append(" has been accepted.").toString()**)

M Common API Call: Open Redirect: Allowing untrusted site by passing user controlled input

Fix Group ID:	80116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	Allowing untrusted site by passing user controlled input
How to Fix:	Open Redirect

Issue 1 of 2

Issue ID:	dc116e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	80116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:19
Line	19
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/disclaimer.htm
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
API:	Allowing untrusted site by passing user controlled input
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:19

Issue 1 of 2 - Details

Call

```
window.location.href = sDst;
```

Issue 2 of 2

Issue ID:	df116e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	80116e59-fcd5-ee11-9f02-14cb65725114
Location	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:35
Line	35
Source File	build/_oJ-3.1.1_1/stage/1/Java/analyze/disclaimer.htm
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
API:	Allowing untrusted site by passing user controlled input
Caller:	build_oJ-3.1.1_1\stage\1\Java\analyze\disclaimer.htm:35

Issue 2 of 2 - Details

Call

```
window.location.href = "http" + sDst.substring(4);
```

H Common API Call: Open Redirect: javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.S...

Fix Group ID:	79116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
API:	javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String):void
How to Fix:	Open Redirect

Issue 1 of 1

Issue ID:	b2116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	79116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpServletResponse.sendRedirect(String):void org.apache.jsp.bank.customize_jsp:35
Calling Method	org.apache.jsp.bank.customize_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	35
Source File	org.apache.jsp.bank.customize_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.customize_jsp:32
Sink:	javax.servlet.http.HttpServletResponse.sendRedirect(String):void *via* org.apache.jsp.bank.customize_jsp:35

Issue 1 of 1 - Details

Trace

org.apache.jsp.bank.customize_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.customize_jsp:32
content = request.**getParameter**("content")

org.apache.jsp.bank.customize_jsp:35
response.sendRedirect(**content**)

H Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(ja...

Fix Group ID:	7b116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(java.lang.String;java.lang.String):java.lang.String
How to Fix:	SQL Injection

Issue 1 of 2

Issue ID:	86126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7b116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:471
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(java.lang.String;java.lang.String):java.lang.String
Line	471
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:44
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:471

Issue 1 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:44
username = request.**getParameter**("username")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:49
error = addAccount(**username**, acctType)

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(**username**)

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','")

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType)

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)")

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:471
statement.execute(**new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)").toString()**)

Issue 2 of 2

Issue ID:	89126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7b116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:471
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(java.lang.String;java.lang.String):java.lang.String
Line	471
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:45
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:471

Issue 2 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:45
acctType = request.**getParameter**("accttypes")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:49
error = addAccount(username, **acctType**)

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(**acctType**)

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)")

com.ibm.security.appscan.altoromutual.util.DBUtil:471
new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:471
statement.execute(**new StringBuilder().append("INSERT INTO ACCOUNTS (USERID,ACCOUNT_NAME,BALANCE) VALUES ('").append(username).append("','").append(acctType).append("', 0)").toString()**)

H Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactio...

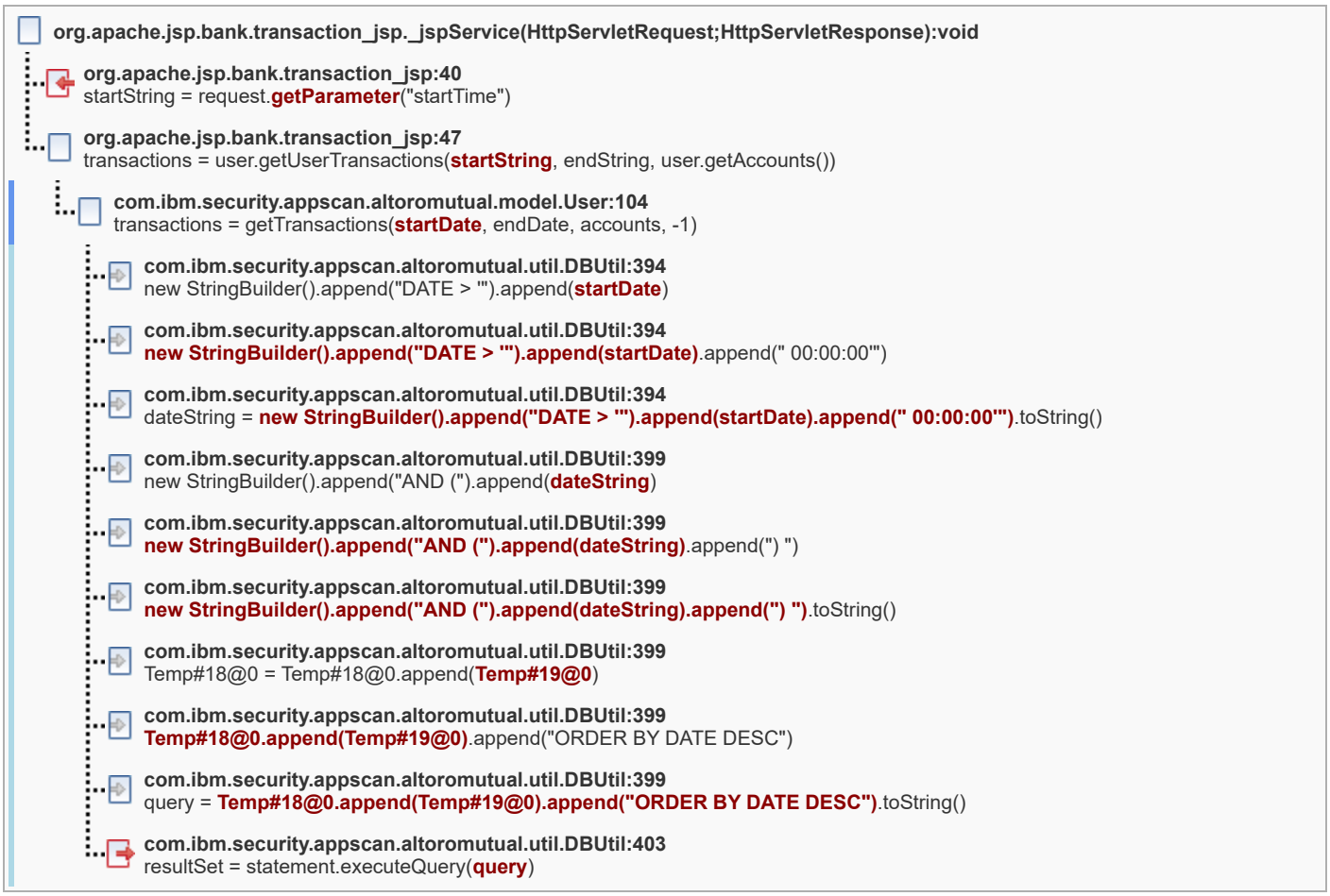
Fix Group ID:	8b116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(java.lang.String;java.lang.String;com.ibm.security.appscan.altoromutual.model.Account[];int):com.ibm.security.appscan.altoromutual.model.Transaction[]
How to Fix:	SQL Injection

Issue 1 of 2

Issue ID:	83126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8b116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:403
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(java.lang.String;java.lang.String;com.ibm.security.appscan.altoromutual.model.Account[];int):com.ibm.security.appscan.altoromutual.model.Transaction[]
Line	403
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.transaction_jsp:40
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403

Issue 1 of 2 - Details

Trace

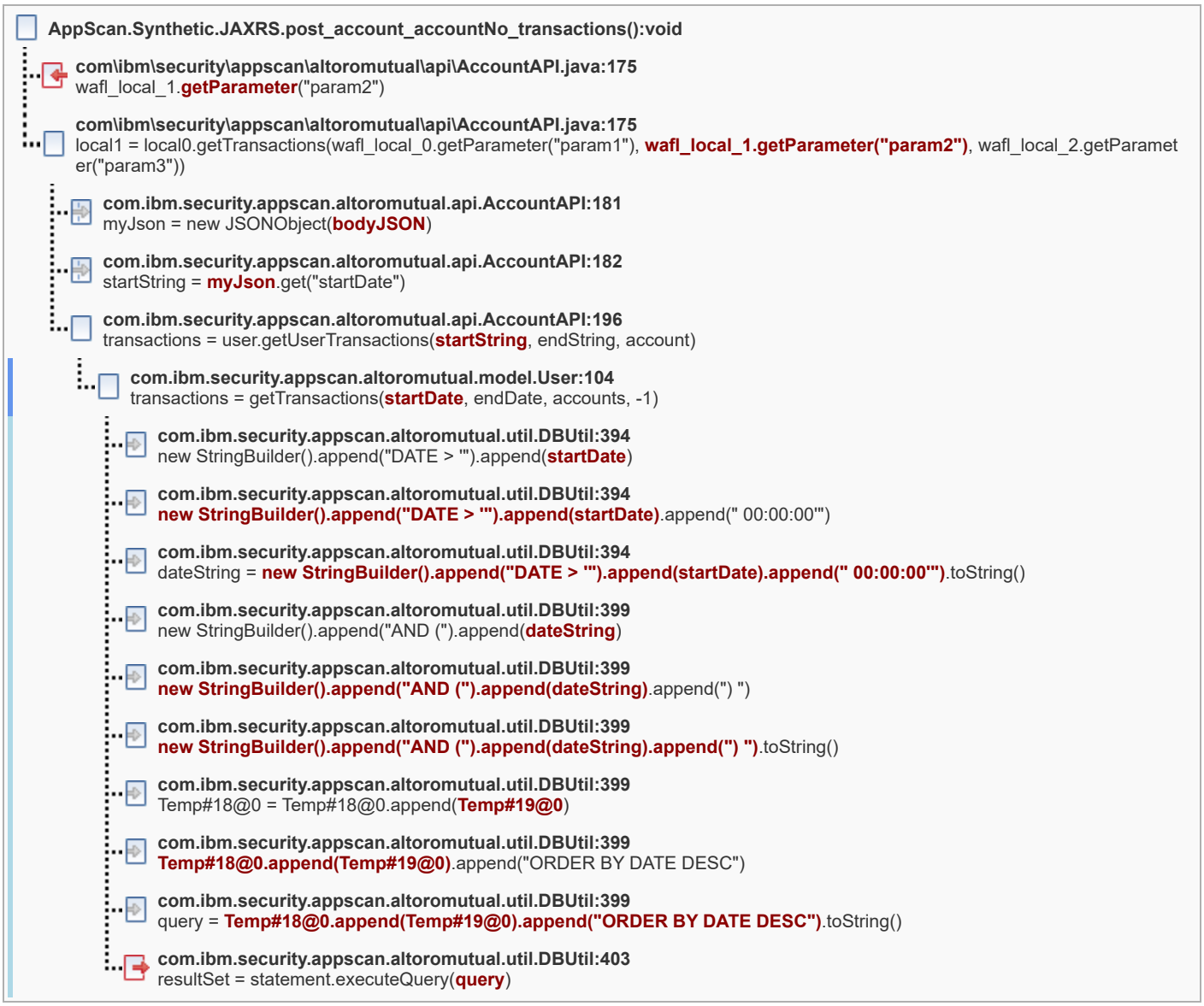


Issue 2 of 2

Issue ID:	80126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8b116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:403
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(java.lang.String;java.lang.String;com.ibm.security.appscan.altoromutual.model.Account[];int):com.ibm.security.appscan.altoromutual.model.Transaction[]
Line	403
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403

Issue 2 of 2 - Details

Trace



H Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(j...

Fix Group ID:	7f116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(java.lang.String;java.lang.String):boolean
How to Fix:	SQL Injection

Issue 1 of 2

Issue ID:	71126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:219
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(java.lang.String;java.lang.String):boolean
Line	219
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.LoginServlet:79
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:219

Issue 1 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.LoginServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:79
password = request.**getParameter**("passw")

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:80
password.trim()

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:80
password = **password.trim()**.toLowerCase()

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:82
isValidUser(username, **password**)

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD ='").append(**password**)

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'")

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:219
resultSet = statement.executeQuery(**new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'").toString()**)

Issue 2 of 2

Issue ID:	74126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:219
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(java.lang.String;java.lang.String):boolean
Line	219
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.LoginServlet:75
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:219

Issue 2 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.LoginServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:75
username = request.**getParameter**("uid")

com.ibm.security.appscan.altoromutual.servlet.LoginServlet:82
isValidUser(**username**, password)

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(**user**)

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='")

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password)

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'")

com.ibm.security.appscan.altoromutual.util.DBUtil:219
new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:219
resultSet = statement.executeQuery(**new StringBuilder().append("SELECT COUNT(*)FROM PEOPLE WHERE USER_ID = '").append(user).append("' AND PASSWORD='").append(password).append("'").toString()**)

H Common Fix Point: SQL Injection: com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback...

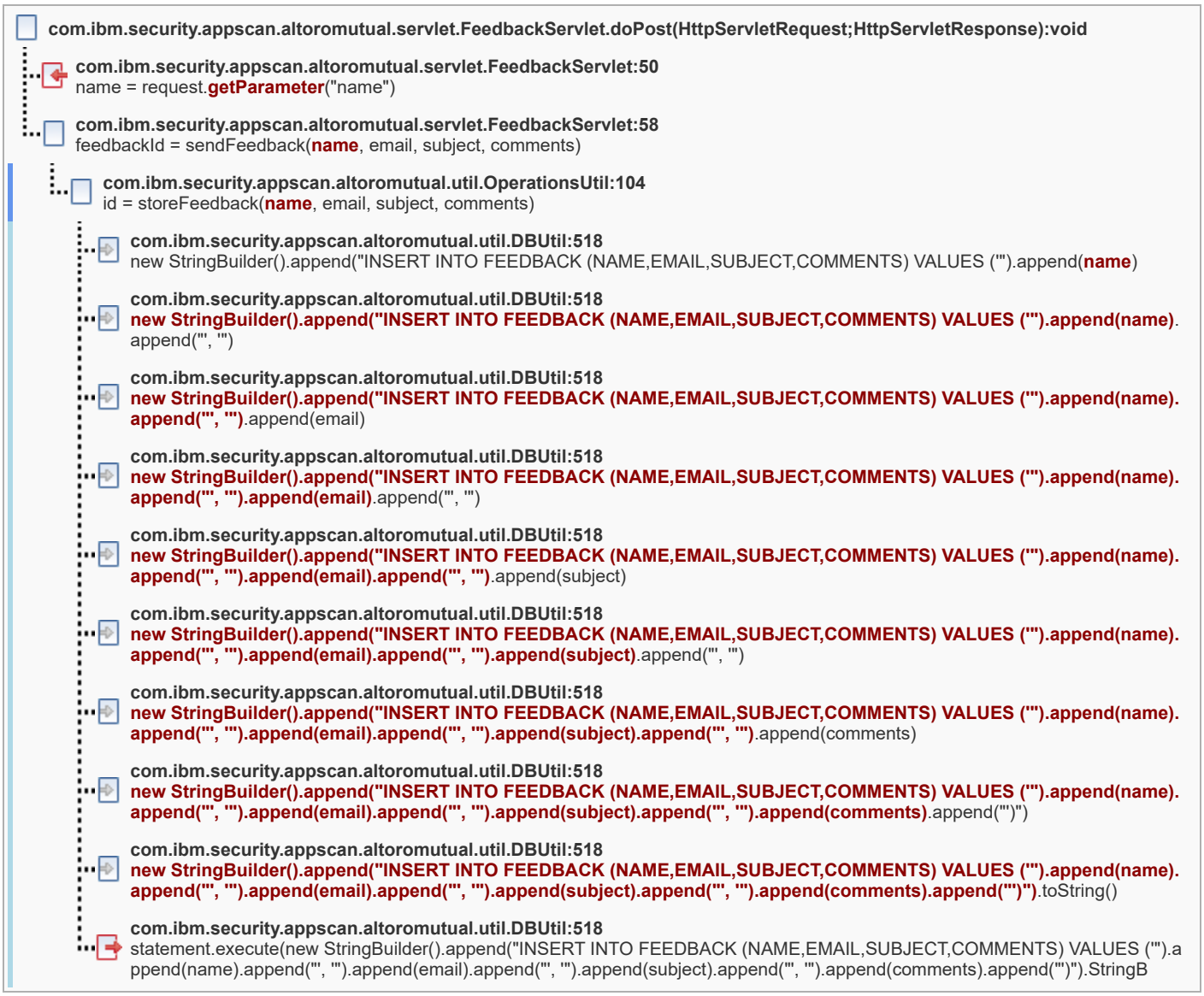
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
How to Fix:	SQL Injection

Issue 1 of 5

Issue ID:	9b126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String;int):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:518
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
Line	518
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:50
Sink:	java.sql.Statement.execute(String;int):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:518

Issue 1 of 5 - Details

Trace


com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(HttpServletRequest;HttpServletResponse):void
com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:50
name = request.getParameter("name")
com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:58
feedbackId = sendFeedback(name, email, subject, comments)
com.ibm.security.appscan.altoromutual.util.OperationsUtil:104
id = storeFeedback(name, email, subject, comments)
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name)
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '")
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email)
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '")
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject)
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '")
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments)
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')")
com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").toString()
com.ibm.security.appscan.altoromutual.util.DBUtil:518
statement.execute(new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").StringB

Issue 2 of 5

Issue ID:	9f126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String;int):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:518
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
Line	518
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:54
Sink:	java.sql.Statement.execute(String;int):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:518

Issue 2 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:54
subject = request.**getParameter**("subject")

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:58
feedbackId = sendFeedback(name, email, **subject**, comments)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:101
subject = escapeSql(**subject**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:104
id = storeFeedback(name, email, **subject**, comments)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(**subject**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:518
statement.execute(new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").StringB

Issue 3 of 5

Issue ID:	a2126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String;int):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:518
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
Line	518
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com\ibm\security\appscan\altoromutual\api\FeedbackAPI.java:24
Sink:	java.sql.Statement.execute(String;int):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:518

Issue 3 of 5 - Details

Trace

AppScan.Synthetic.JAXRS.post_feedback_submit():void

com\ibm\security\appscan\altoromutual\api\FeedbackAPI.java:24
wafl_local_0.**getParameter**("param1")

com\ibm\security\appscan\altoromutual\api\FeedbackAPI.java:24
local1 = local0.sendFeedback(**wafl_local_0.getParameter("param1")**, wafl_local_1.getParameter("param2"))

com.ibm.security.appscan.altoromutual.api.FeedbackAPI:29
myJson = new JSONObject(**bodyJSON**)

com.ibm.security.appscan.altoromutual.api.FeedbackAPI:44
comments = **myJson**.get("message")

com.ibm.security.appscan.altoromutual.api.FeedbackAPI:51
feedbackId = sendFeedback(name, email, subject, **comments**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:102
comments = escapeSql(**comments**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:104
id = storeFeedback(name, email, subject, **comments**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(**comments**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:518
statement.execute(new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").StringB

Issue 4 of 5

Issue ID:	a5126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String;int):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:518
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
Line	518
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:55
Sink:	java.sql.Statement.execute(String;int):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:518

Issue 4 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:55
comments = request.**getParameter**("comments")

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:58
feedbackId = sendFeedback(name, email, subject, **comments**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:102
comments = escapeSql(**comments**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:104
id = storeFeedback(name, email, subject, **comments**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(**comments**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:518
statement.execute(new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").StringB

Issue 5 of 5

Issue ID:	a8126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	6f116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String;int):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:518
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.storeFeedback(java.lang.String;java.lang.String;java.lang.String;java.lang.String):long
Line	518
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:53
Sink:	java.sql.Statement.execute(String;int):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:518

Issue 5 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:53
email = request.**getParameter**("email_addr")

com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet:58
feedbackId = sendFeedback(name, **email**, subject, comments)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:100
email = escapeSql(**email**)

com.ibm.security.appscan.altoromutual.util.OperationsUtil:104
id = storeFeedback(name, **email**, subject, comments)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(**email**)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments)

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')")

com.ibm.security.appscan.altoromutual.util.DBUtil:518
new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").toString()

com.ibm.security.appscan.altoromutual.util.DBUtil:518
statement.execute(new StringBuilder().append("INSERT INTO FEEDBACK (NAME,EMAIL,SUBJECT,COMMENTS) VALUES ('").append(name).append("', '").append(email).append("', '").append(subject).append("', '").append(comments).append("')").StringB

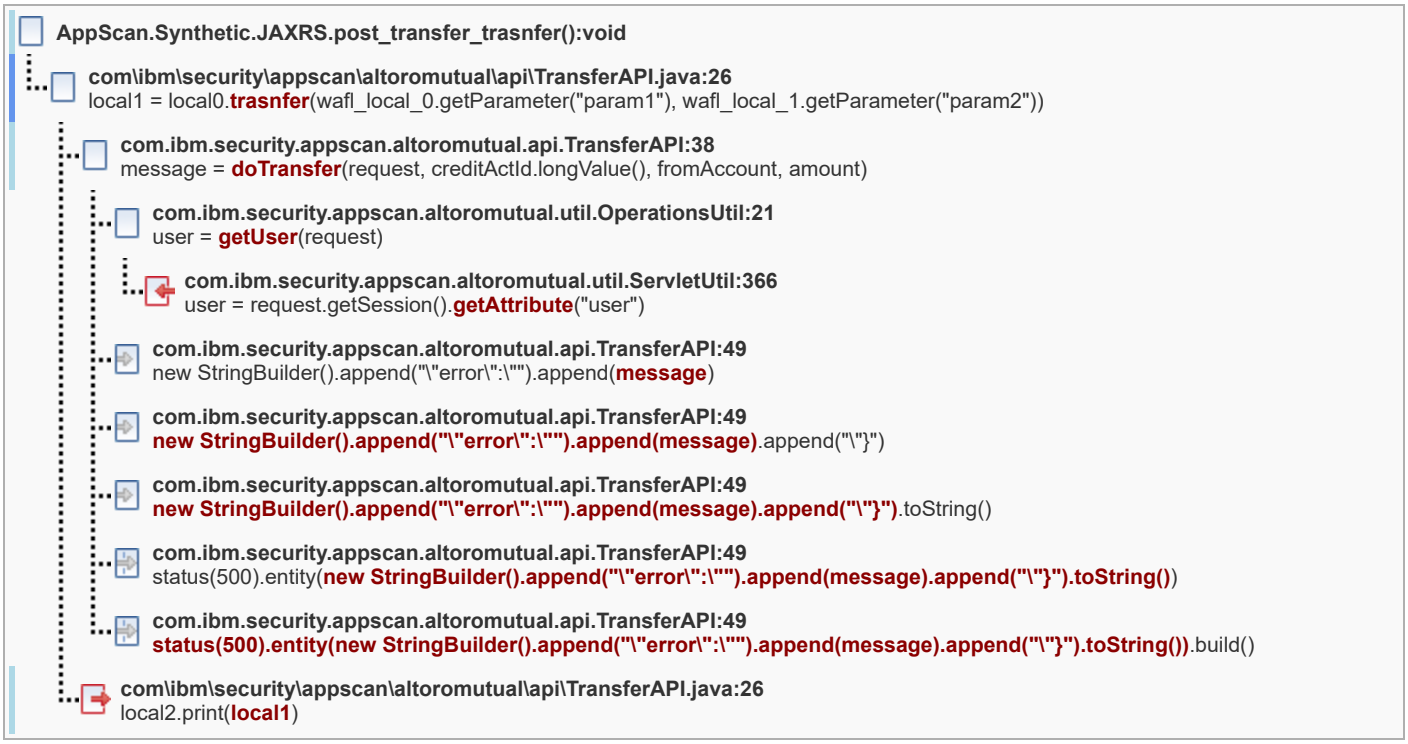
M	Common Fix Point: Inappropriate Encoding for Output Context: com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(...
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.api.TransferAPI.trasnfer(java.lang.String;javax.servlet.http.HttpServletRequest):javax.ws.rs.core.Response
How to Fix:	Inappropriate Encoding for Output Context

Issue 1 of 6

Issue ID:	35126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* com.ibm.security.appscan.altoromutual.util.ServletUtil:366
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 1 of 6 - Details

Trace

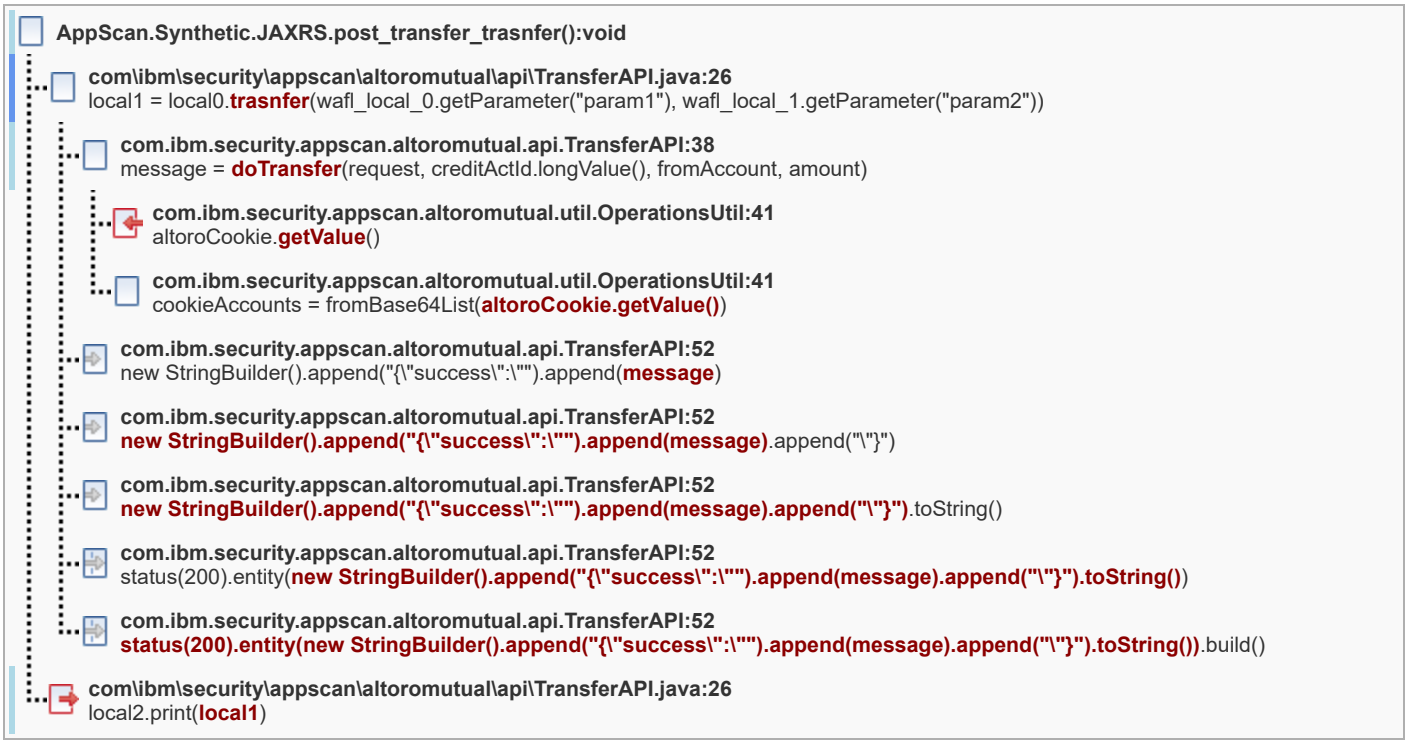


Issue 2 of 6

Issue ID:	38126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.Cookie.getValue():String *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:41
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 2 of 6 - Details

Trace

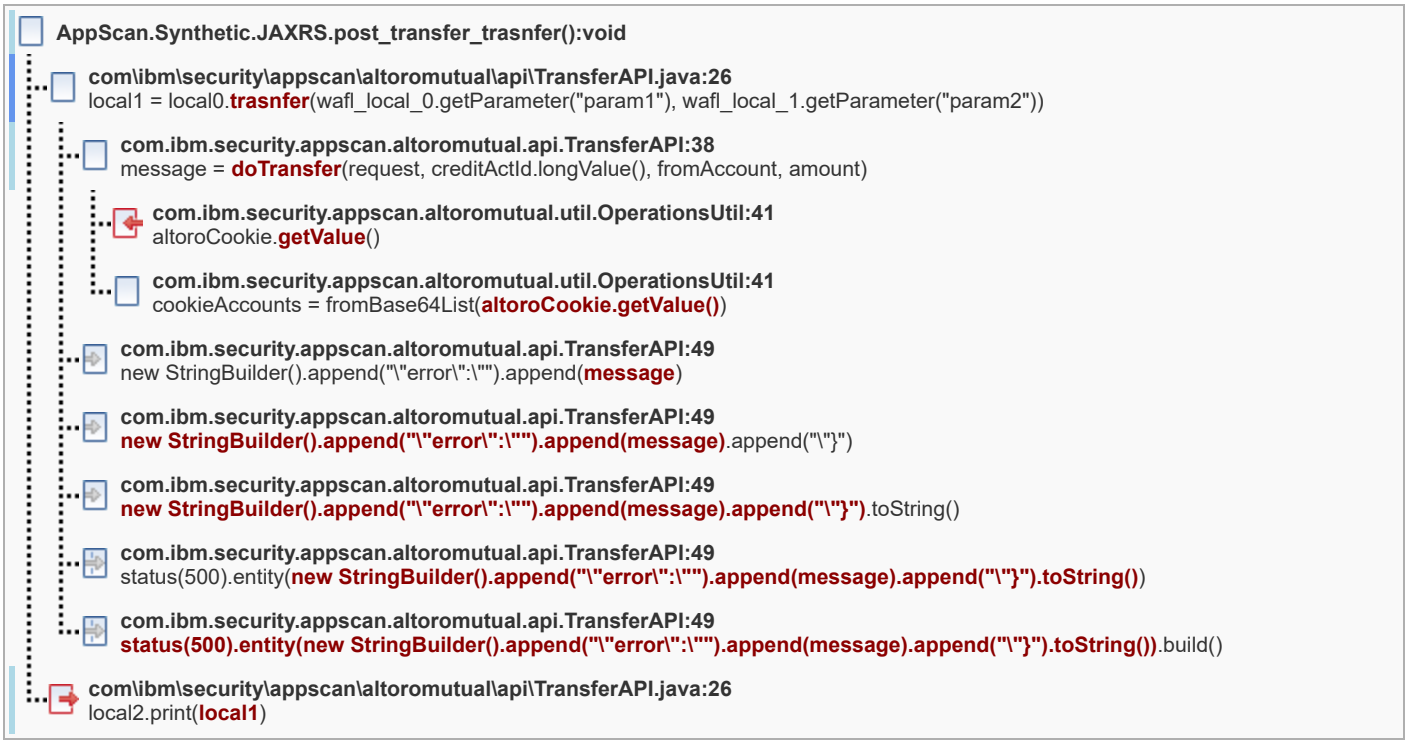


Issue 3 of 6

Issue ID:	1e126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.Cookie.getValue():String *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:41
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 3 of 6 - Details

Trace

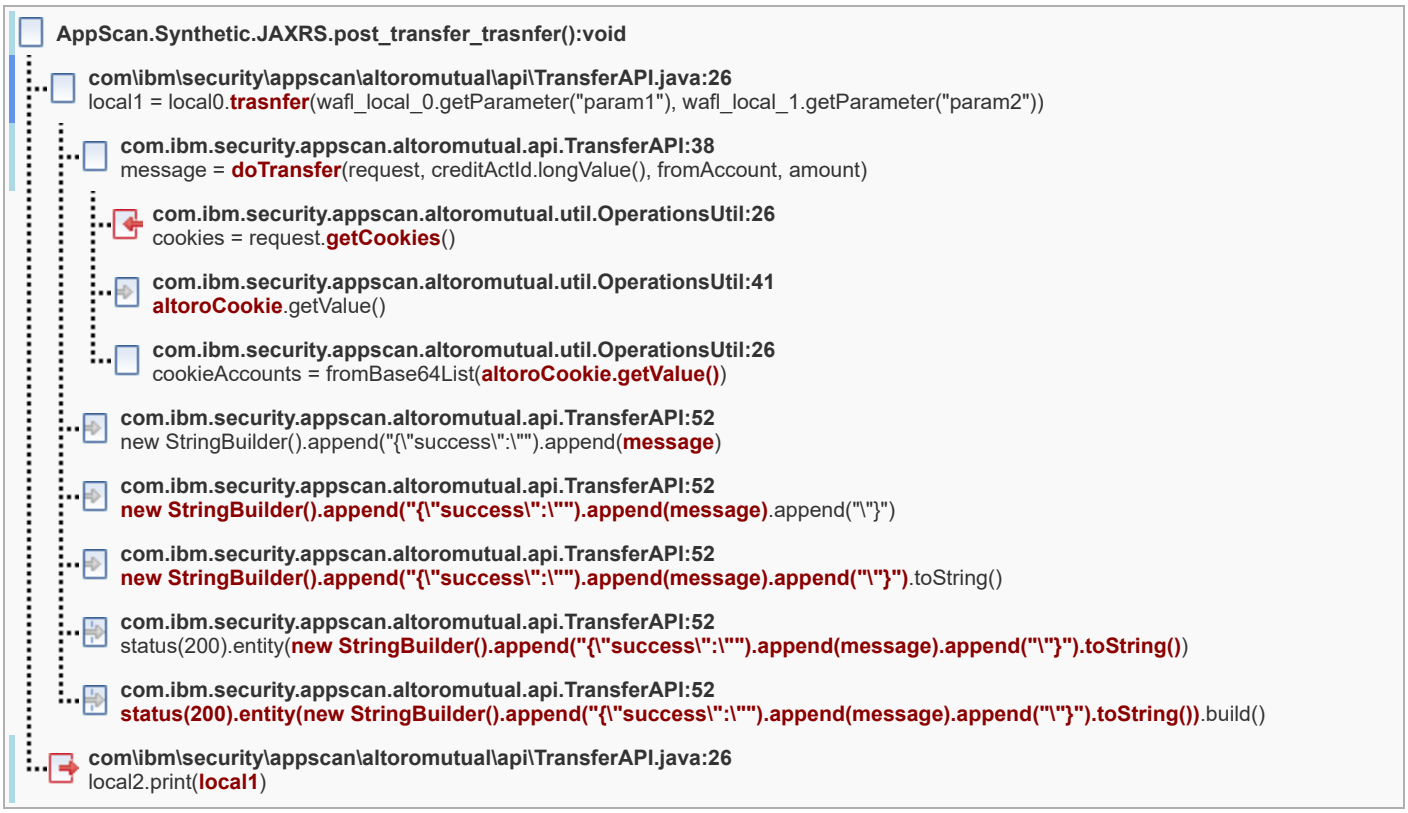


Issue 4 of 6

Issue ID:	21126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.HttpServletRequest.getCookies():Cookie[] *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:26
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 4 of 6 - Details

Trace

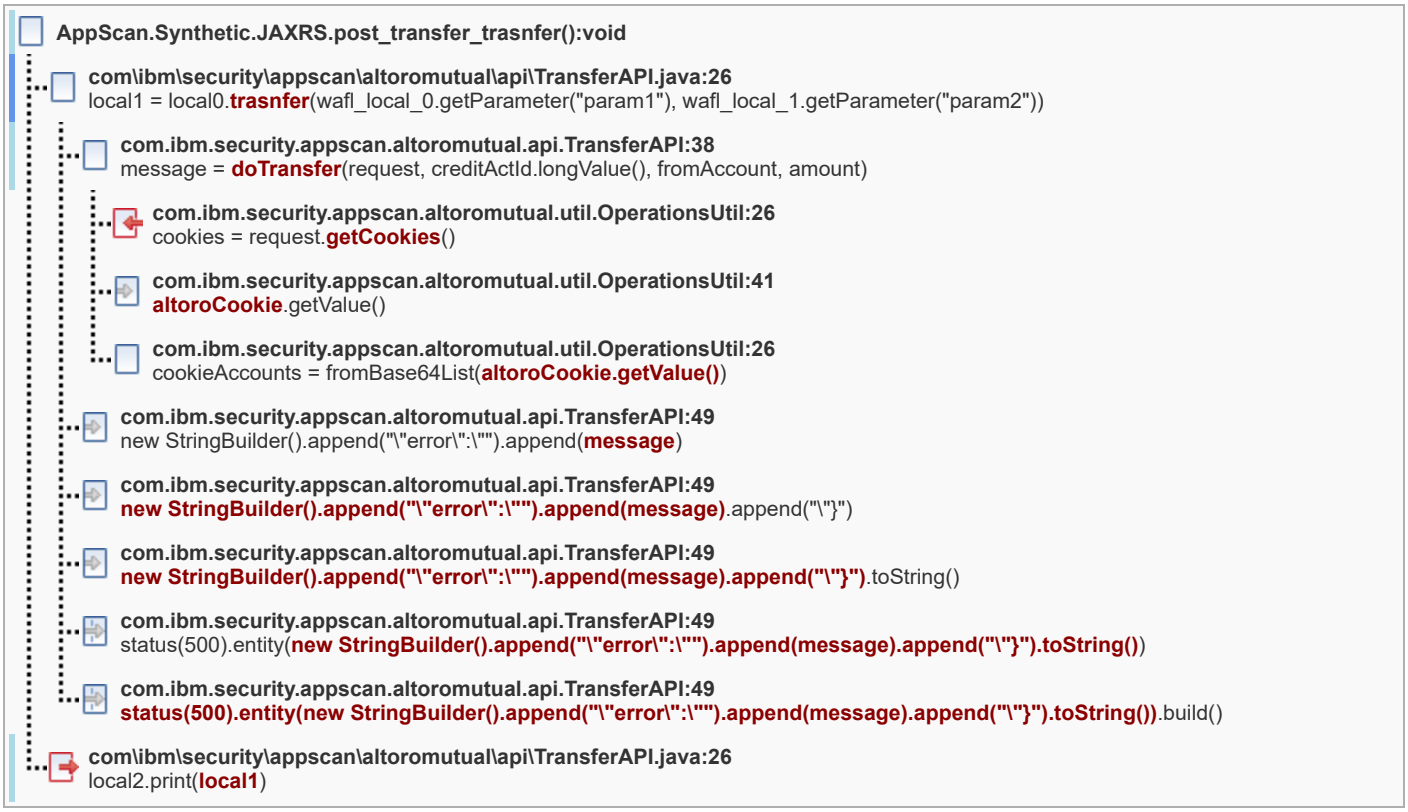


Issue 5 of 6

Issue ID:	2f126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.HttpServletRequest.getCookies():Cookie[] *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:26
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 5 of 6 - Details

Trace

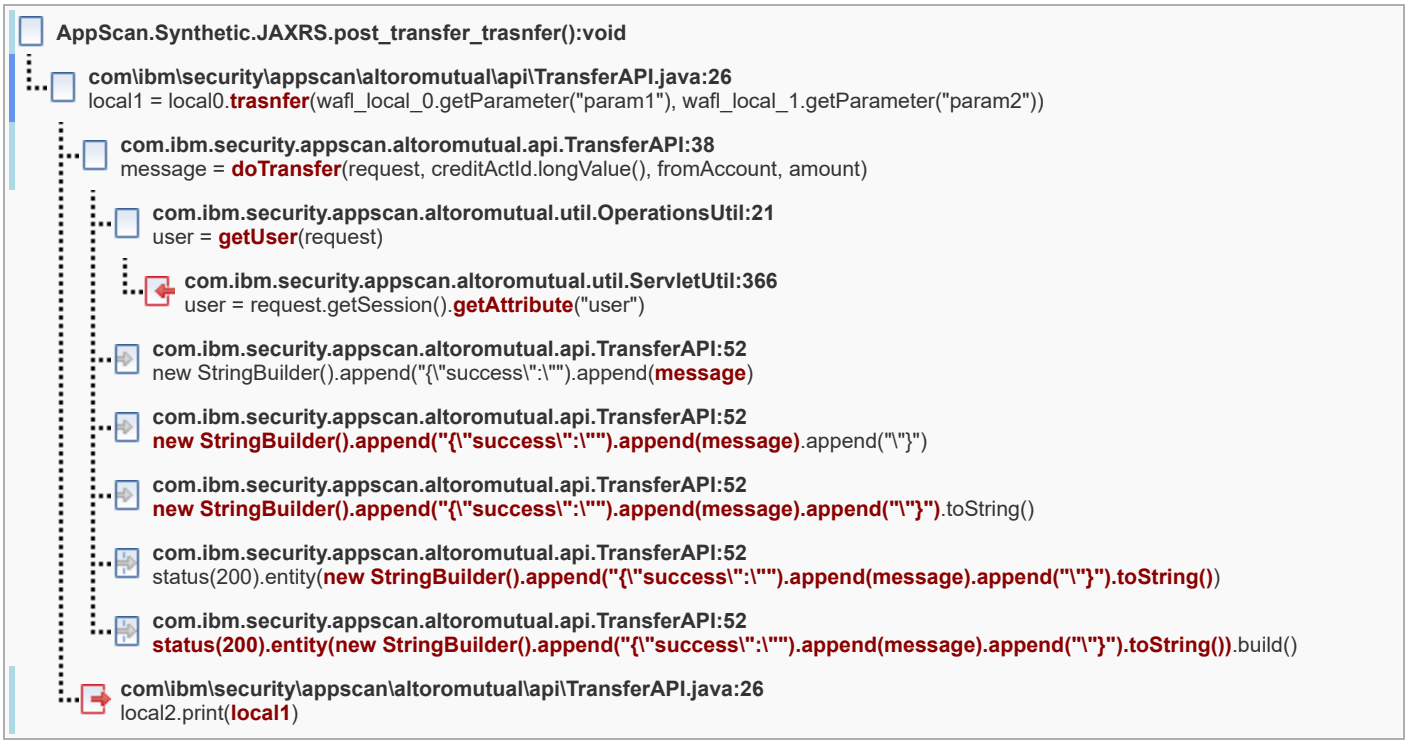


Issue 6 of 6

Issue ID:	32126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	76116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26
Calling Method	AppScan.Synthetic.JAXRS.post_transfer_trasnfer():void
Line	26
Source File	com\ibm\security\appscan\altoromutual\api\TransferAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* com.ibm.security.appscan.altoromutual.util.ServletUtil:366
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\TransferAPI.java:26

Issue 6 of 6 - Details

Trace



H Common Fix Point: Validation Required: com.ibm.security.appscan.altoromutual.util.DBUtil.changePasswor...

Fix Group ID:	83116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword(java.lang.String;java.lang.String):java.lang.String
How to Fix:	Validation Required

Issue 1 of 2

Issue ID:	47126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	83116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpSession.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118
Calling Method	com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	118
Source File	com.ibm.security.appscan.altoromutual.servlet.AdminServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:91
Sink:	javax.servlet.http.HttpSession.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118

Issue 1 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:91
password1 = request.**getParameter**("password1")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:103
error = changePassword(username, **password1**)

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:114
new StringBuilder().append("Error: ").append(**message**)

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:114
message = **new StringBuilder().append("Error: ").append(message)**.toString()

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118
request.getSession().setAttribute("**message**", **message**)

Issue 2 of 2

Issue ID:	4a126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	83116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpSession.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118
Calling Method	com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	118
Source File	com.ibm.security.appscan.altoromutual.servlet.AdminServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:90
Sink:	javax.servlet.http.HttpSession.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118

Issue 2 of 2 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:90
username = request.**getParameter**("username")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:103
error = changePassword(**username**, password1)

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:114
new StringBuilder().append("Error: ").append(**message**)

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:114
message = **new StringBuilder().append("Error: ").append(message)**.toString()

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:118
request.getSession().setAttribute("**message**", **message**)

H Common Fix Point:Cross-Site Scripting: com.ibm.security.appscan.altoromutual.model.Transaction.<init>(...

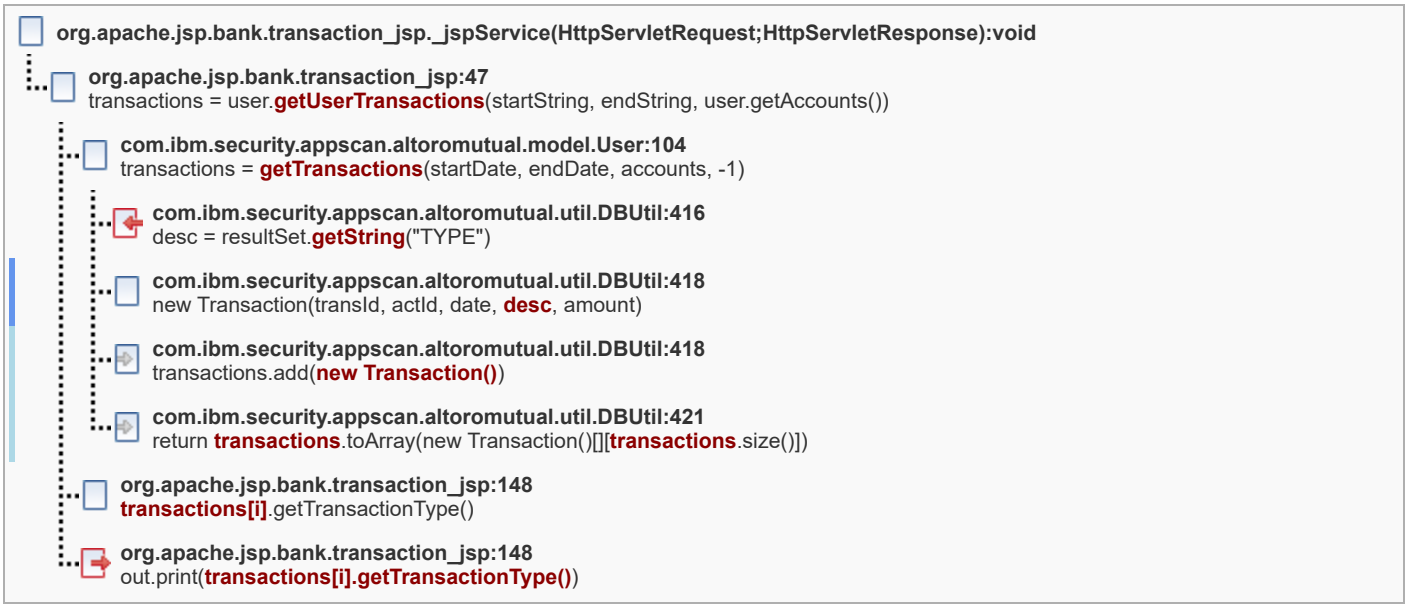
Fix Group ID:	71116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.model.Transaction.<init>(int;long;java.util.Date;java.lang.String;double):void
How to Fix:	Cross-Site Scripting

Issue 1 of 4

Issue ID:	cd116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	71116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.transaction_jsp:148
Calling Method	org.apache.jsp.bank.transaction_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	148
Source File	org.apache.jsp.bank.transaction_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.transaction_jsp:148

Issue 1 of 4 - Details

Trace

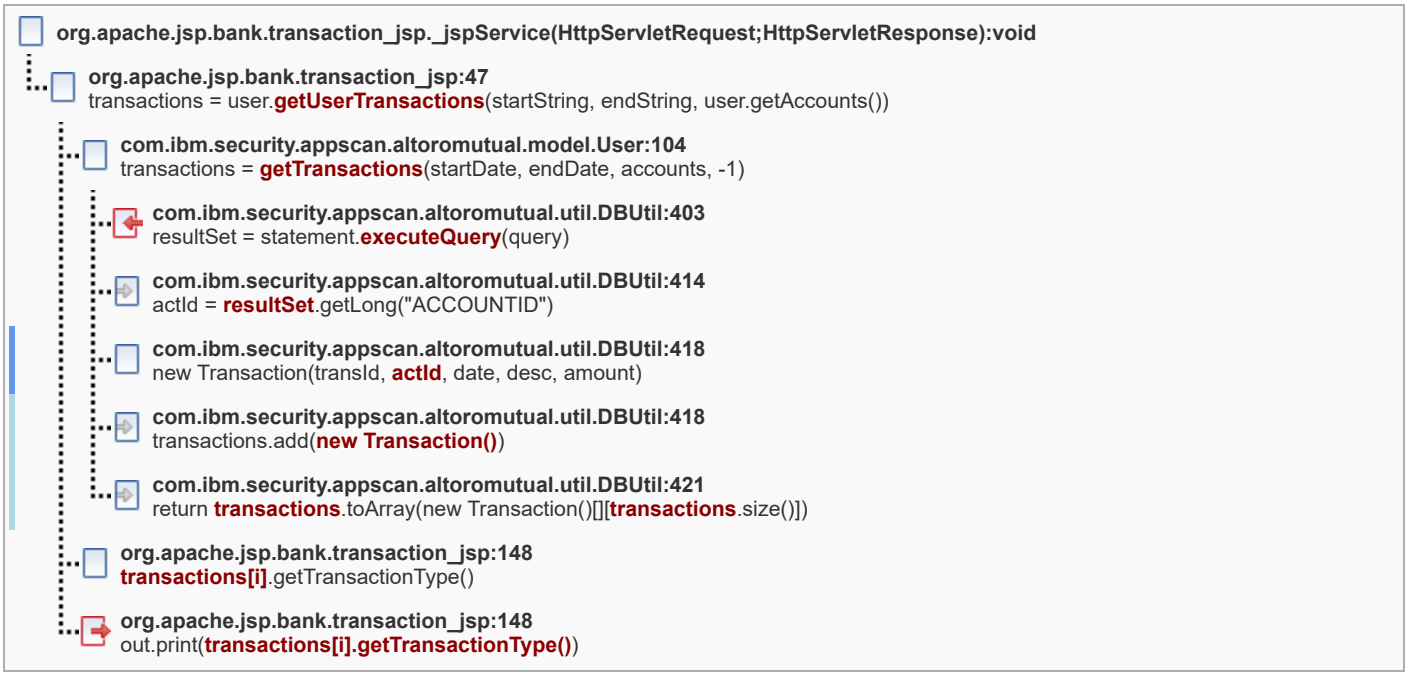


Issue 2 of 4

Issue ID:	d0116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	71116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.transaction_jsp:148
Calling Method	org.apache.jsp.bank.transaction_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	148
Source File	org.apache.jsp.bank.transaction_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.transaction_jsp:148

Issue 2 of 4 - Details

Trace

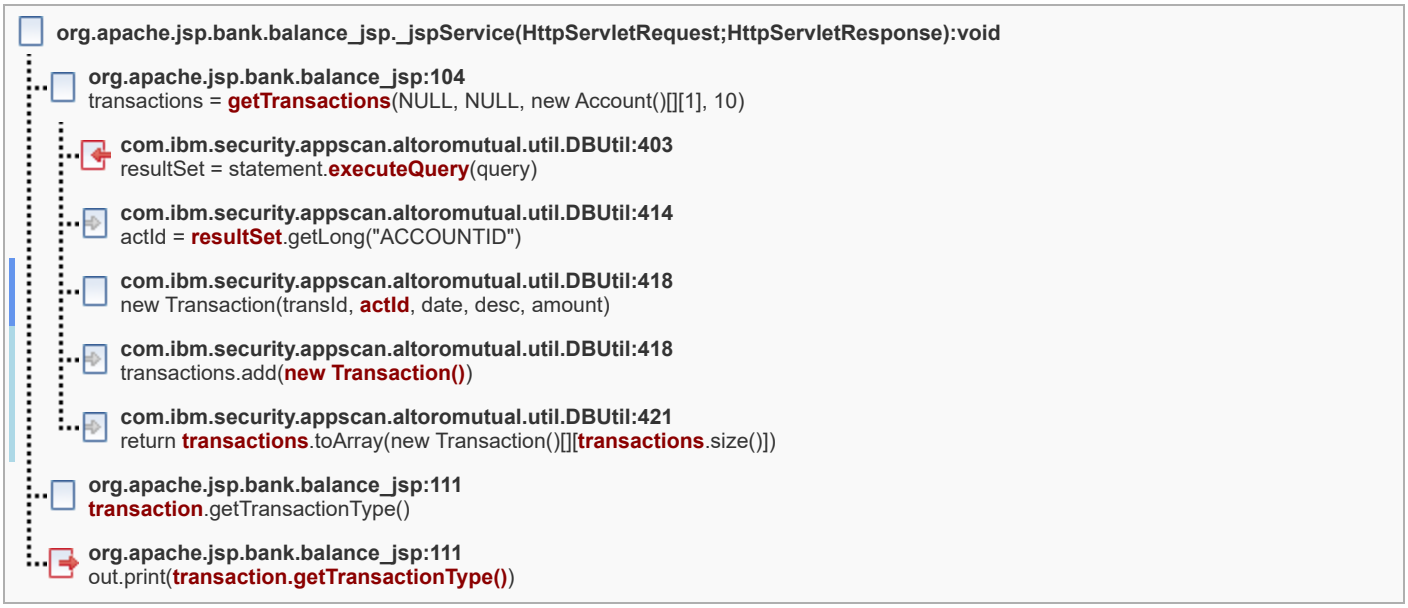


Issue 3 of 4

Issue ID:	ac116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	71116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.balance_jsp:111
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	111
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.balance_jsp:111

Issue 3 of 4 - Details

Trace

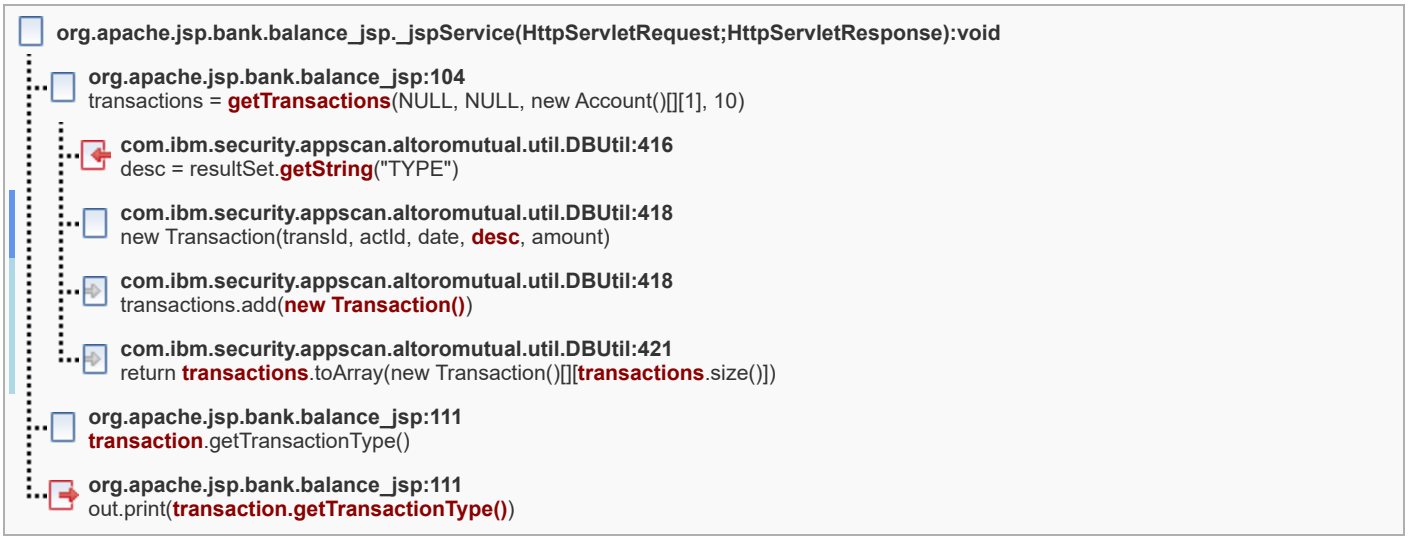


Issue 4 of 4

Issue ID:	af116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	71116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.balance_jsp:111
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	111
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.balance_jsp:111

Issue 4 of 4 - Details

Trace



H Common Fix Point:Cross-Site Scripting: com.ibm.security.appscan.altoromutual.model.User.getAccounts():...

Fix Group ID:	7d116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.model.User.getAccounts():com.ibm.security.appscan.altoromutual.model.Account[]
How to Fix:	Cross-Site Scripting

Issue 1 of 2

Issue ID:	a6116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.balance_jsp:72
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	72
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.balance_jsp:38
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.balance_jsp:72

Issue 1 of 2 - Details

Trace

org.apache.jsp.bank.balance_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.balance_jsp:38
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.balance_jsp:43
balance = **user**.getAccounts()

org.apache.jsp.bank.balance_jsp:48
accounts.add(0, **account**)

org.apache.jsp.bank.balance_jsp:71
accounts.iterator()

org.apache.jsp.bank.balance_jsp:71
account = **Temp#28@0**.next()

org.apache.jsp.bank.balance_jsp:72
account.getAccountName()

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>")

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>").StringBuilde

org.apache.jsp.bank.balance_jsp:72
out.println(new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).

Issue 2 of 2

Issue ID:	a9116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7d116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.println(String):void org.apache.jsp.bank.balance_jsp:72
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	72
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.balance_jsp:38
Sink:	javax.servlet.jsp.JspWriter.println(String):void *via* org.apache.jsp.bank.balance_jsp:72

Issue 2 of 2 - Details

Trace

org.apache.jsp.bank.balance_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.balance_jsp:38
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.balance_jsp:43
balance = **user**.getAccounts()

org.apache.jsp.bank.balance_jsp:46
accounts.add(**account**)

org.apache.jsp.bank.balance_jsp:71
accounts.iterator()

org.apache.jsp.bank.balance_jsp:71
account = **Temp#28@0**.next()

org.apache.jsp.bank.balance_jsp:72
account.getAccountName()

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>")

org.apache.jsp.bank.balance_jsp:72
new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).append("</option>").StringBuilde

org.apache.jsp.bank.balance_jsp:72
out.println(new StringBuilder().append(account.getAccountId()).append("\">").append(account.getAccountId()).append(" ").append(account.getAccountName()).

H Common Fix Point:Cross-Site Scripting: java.lang.StringBuilder.append(java.lang.String):java.lang.Stri...

Fix Group ID:	7c116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder
How to Fix:	Cross-Site Scripting

Issue 1 of 2

Issue ID:	b8116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7c116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.main_jsp:36
Calling Method	org.apache.jsp.bank.main_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	36
Source File	org.apache.jsp.bank.main_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.main_jsp:33
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.main_jsp:36

Issue 1 of 2 - Details

Trace

org.apache.jsp.bank.main_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.main_jsp:33
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.main_jsp:36
user.getFirstName()

org.apache.jsp.bank.main_jsp:36
valueOf(**user.getFirstName()**)

org.apache.jsp.bank.main_jsp:36
new StringBuilder(**valueOf(user.getFirstName())**)

org.apache.jsp.bank.main_jsp:36
new StringBuilder().append(" ")

org.apache.jsp.bank.main_jsp:36
new StringBuilder().append(" ").append(user.getLastName())

org.apache.jsp.bank.main_jsp:36
new StringBuilder().append(" ").append(user.getLastName()).toString()

org.apache.jsp.bank.main_jsp:36
out.print(**new StringBuilder().append(" ").append(user.getLastName()).toString()**)

Issue 2 of 2

Issue ID:	bb116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7c116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.main_jsp:36
Calling Method	org.apache.jsp.bank.main_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	36
Source File	org.apache.jsp.bank.main_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.main_jsp:33
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.main_jsp:36

Issue 2 of 2 - Details

Trace

org.apache.jsp.bank.main_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.main_jsp:33
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.main_jsp:36
user.getLastName()

org.apache.jsp.bank.main_jsp:36
new StringBuilder().append(" ").append(**user.getLastName()**)

org.apache.jsp.bank.main_jsp:36
new StringBuilder().append(" ").append(user.getLastName()).toString()

org.apache.jsp.bank.main_jsp:36
out.print(**new StringBuilder().append(" ").append(user.getLastName()).toString()**)

H Common Fix Point:Cross-Site Scripting: java.util.ArrayList.add(java.lang.Object):boolean

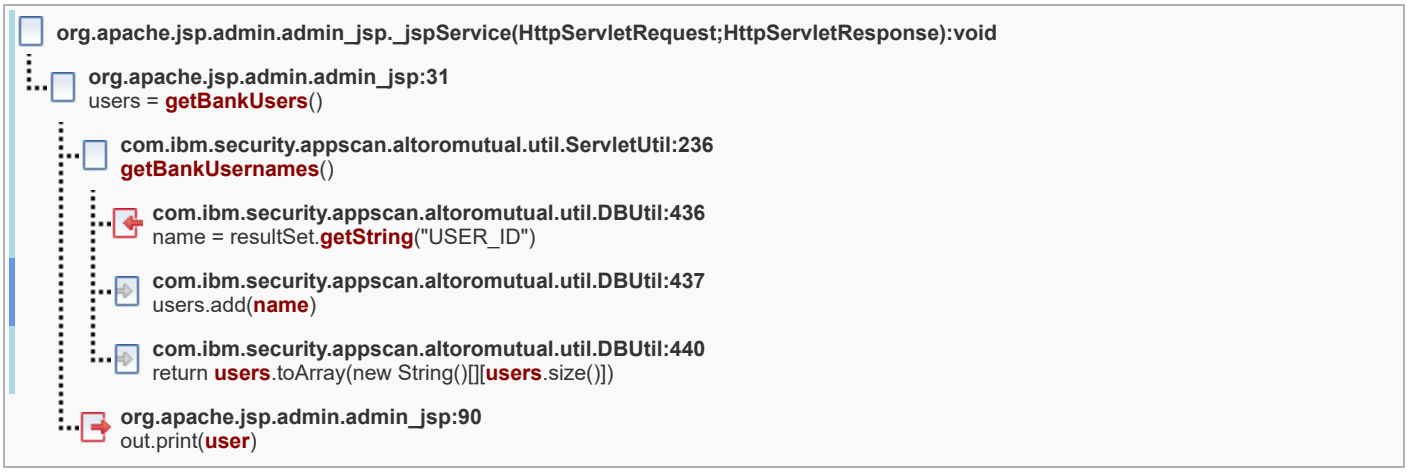
Fix Group ID:	85116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.util.ArrayList.add(java.lang.Object):boolean
How to Fix:	Cross-Site Scripting

Issue 1 of 4

Issue ID:	91116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	85116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.admin_jsp:90
Calling Method	org.apache.jsp.admin.admin_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	90
Source File	org.apache.jsp.admin.admin_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:436
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.admin_jsp:90

Issue 1 of 4 - Details

Trace

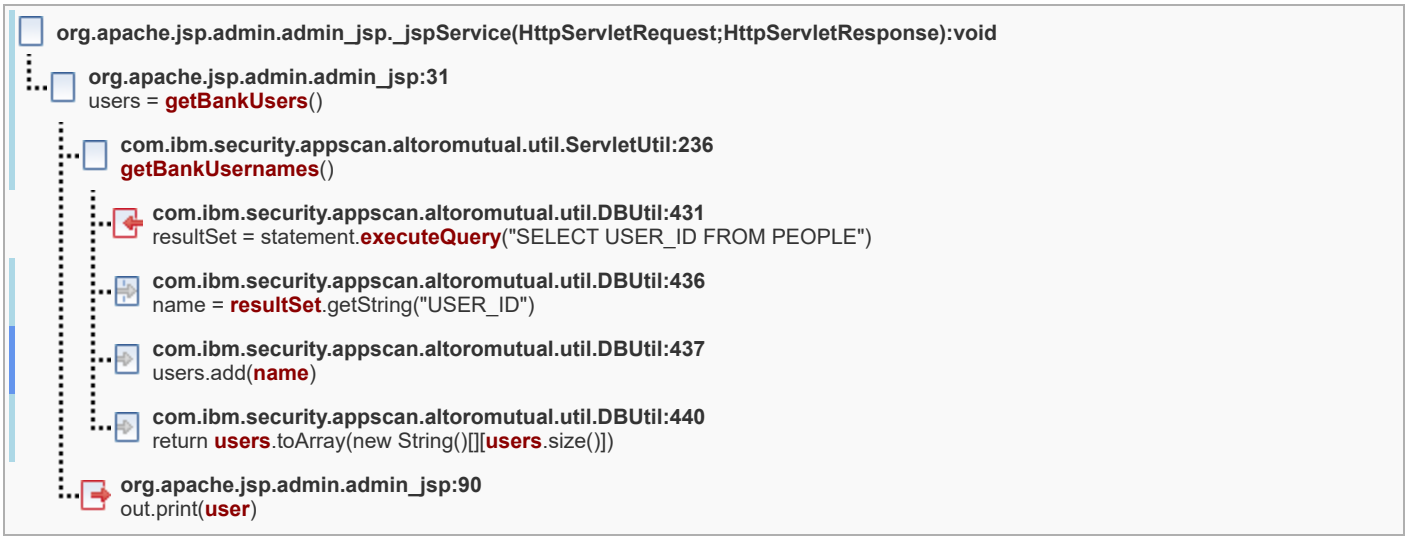


Issue 2 of 4

Issue ID:	94116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	85116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.admin_jsp:90
Calling Method	org.apache.jsp.admin.admin_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	90
Source File	org.apache.jsp.admin.admin_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:431
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.admin_jsp:90

Issue 2 of 4 - Details

Trace

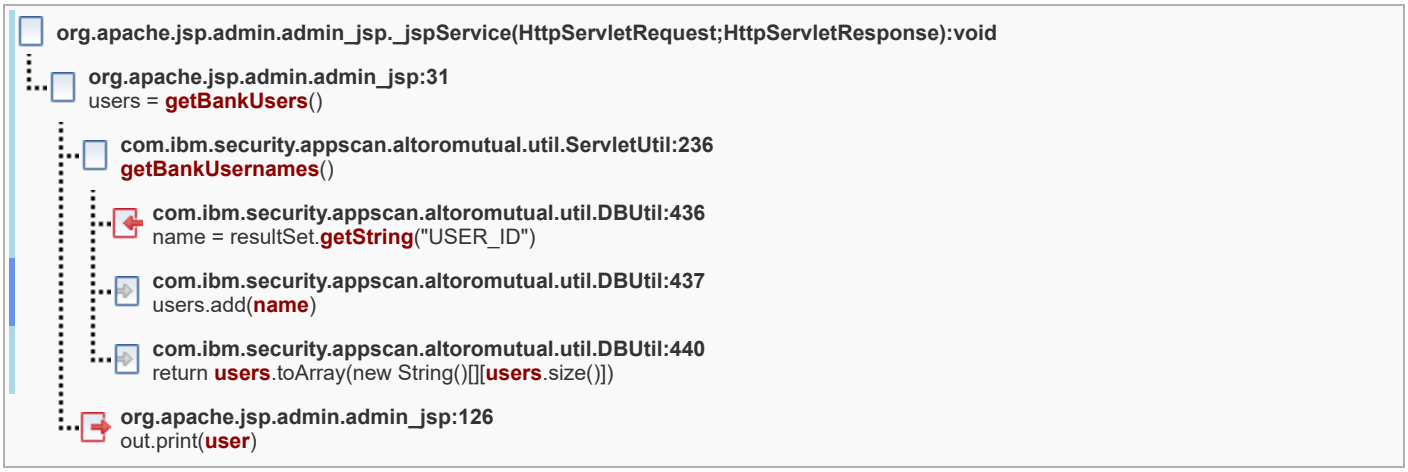


Issue 3 of 4

Issue ID:	97116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	85116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.admin_jsp:126
Calling Method	org.apache.jsp.admin.admin_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	126
Source File	org.apache.jsp.admin.admin_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:436
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.admin_jsp:126

Issue 3 of 4 - Details

Trace

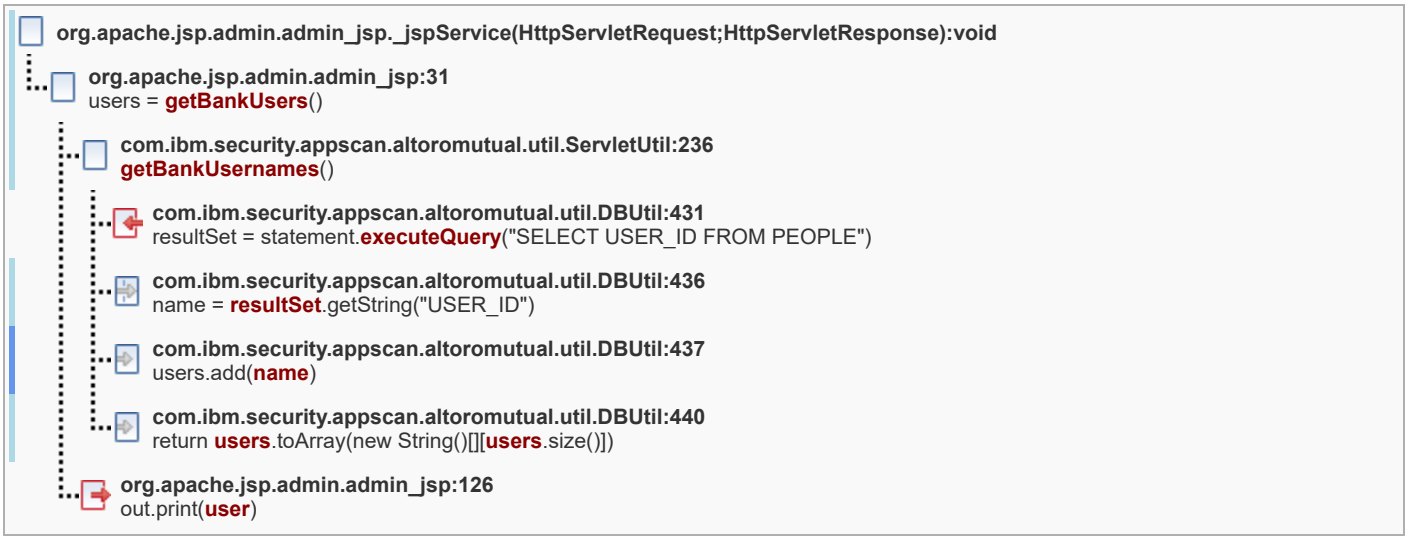


Issue 4 of 4

Issue ID:	9a116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	85116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.admin.admin_jsp:126
Calling Method	org.apache.jsp.admin.admin_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	126
Source File	org.apache.jsp.admin.admin_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:431
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.admin.admin_jsp:126

Issue 4 of 4 - Details

Trace



H Common Fix Point:Cross-Site Scripting: javax.servlet.jsp.JspWriter.print(java.lang.String):void

Fix Group ID:	8a116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	javax.servlet.jsp.JspWriter.print(java.lang.String):void
How to Fix:	Cross-Site Scripting

Issue 1 of 2

Issue ID:	a0116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8a116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.balance_jsp:57
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	57
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* org.apache.jsp.bank.balance_jsp:38
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.balance_jsp:57

Issue 1 of 2 - Details

Trace

org.apache.jsp.bank.balance_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.balance_jsp:38
user = request.getSession().**getAttribute**("user")

org.apache.jsp.bank.balance_jsp:43
balance = **user**.getAccounts()

org.apache.jsp.bank.balance_jsp:49
account.getAccountName()

org.apache.jsp.bank.balance_jsp:49
new StringBuilder().append(" ").append(**account.getAccountName()**)

org.apache.jsp.bank.balance_jsp:49
accountName = **new StringBuilder().append(" ").append(account.getAccountName())**.toString()

org.apache.jsp.bank.balance_jsp:57
out.print(**accountName**)

Issue 2 of 2

Issue ID:	a3116e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	8a116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.jsp.JspWriter.print(String):void org.apache.jsp.bank.balance_jsp:57
Calling Method	org.apache.jsp.bank.balance_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	57
Source File	org.apache.jsp.bank.balance_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	79
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.bank.balance_jsp:40
Sink:	javax.servlet.jsp.JspWriter.print(String):void *via* org.apache.jsp.bank.balance_jsp:57

Issue 2 of 2 - Details

Trace

org.apache.jsp.bank.balance_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.bank.balance_jsp:40
paramName = request.**getParameter**("acctId")

org.apache.jsp.bank.balance_jsp:57
out.print(**accountName**)

H Common Fix Point:Command Injection: java.lang.Runtime.exec(java.lang.String[]):java.lang.Process

Fix Group ID:	70116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.lang.Runtime.exec(java.lang.String[]):java.lang.Process
How to Fix:	Command Injection

Issue 1 of 2

Issue ID:	c0126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	70116e59-fcd5-ee11-9f02-14cb65725114
Location	java.lang.Runtime.exec(String[]):Process org.apache.jsp.index_jsp:65
Calling Method	org.apache.jsp.index_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	65
Source File	org.apache.jsp.index_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	78
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.index_jsp:38
Sink:	java.lang.Runtime.exec(String[]):Process *via* org.apache.jsp.index_jsp:65

Issue 1 of 2 - Details

Trace

org.apache.jsp.index_jsp._jspService(HttpServletRequest;HttpServletResponse):void

org.apache.jsp.index_jsp:38
content = request.**getParameter**("content")

org.apache.jsp.index_jsp:62
new StringBuilder().append(path).append("/").append(**content**)

org.apache.jsp.index_jsp:62
command = **new StringBuilder().append(path).append("/").append(content)**.toString()

org.apache.jsp.index_jsp:65
proc = getRuntime().exec(**new String()[][3]**)

Issue 2 of 2

Issue ID:	c3126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	70116e59-fcd5-ee11-9f02-14cb65725114
Location	java.lang.Runtime.exec(String[]):Process org.apache.jsp.index_jsp:65
Calling Method	org.apache.jsp.index_jsp._jspService(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	65
Source File	org.apache.jsp.index_jsp
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	78
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* org.apache.jsp.index_jsp:38
Sink:	java.lang.Runtime.exec(String[]):Process *via* org.apache.jsp.index_jsp:65

Issue 2 of 2 - Details

Trace

H	Common Fix Point:SQL Injection: java.lang.StringBuilder.append(java.lang.String):java.lang.Stri...

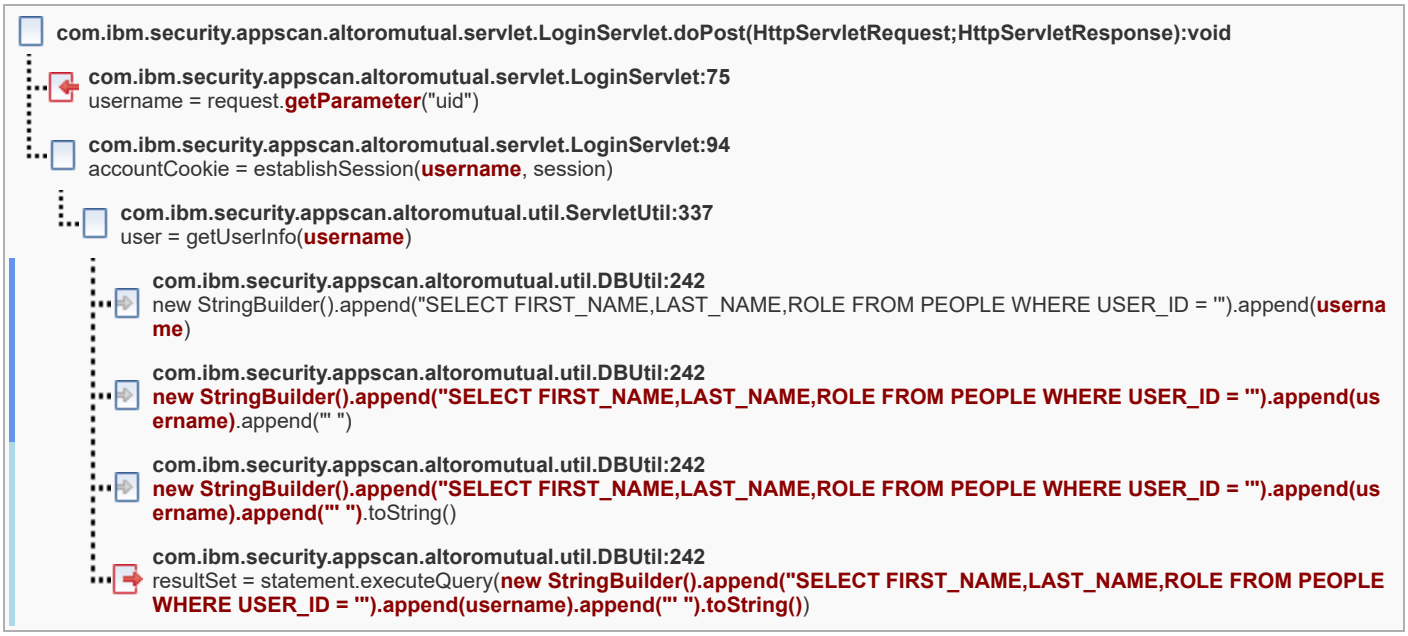
Fix Group ID:	7e116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder
How to Fix:	SQL Injection

Issue 1 of 2

Issue ID:	77126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7e116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:242
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getUserInfo(java.lang.String):com.ibm.security.appscan.altoromutual.model.User
Line	242
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.LoginServlet:75
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:242

Issue 1 of 2 - Details

Trace

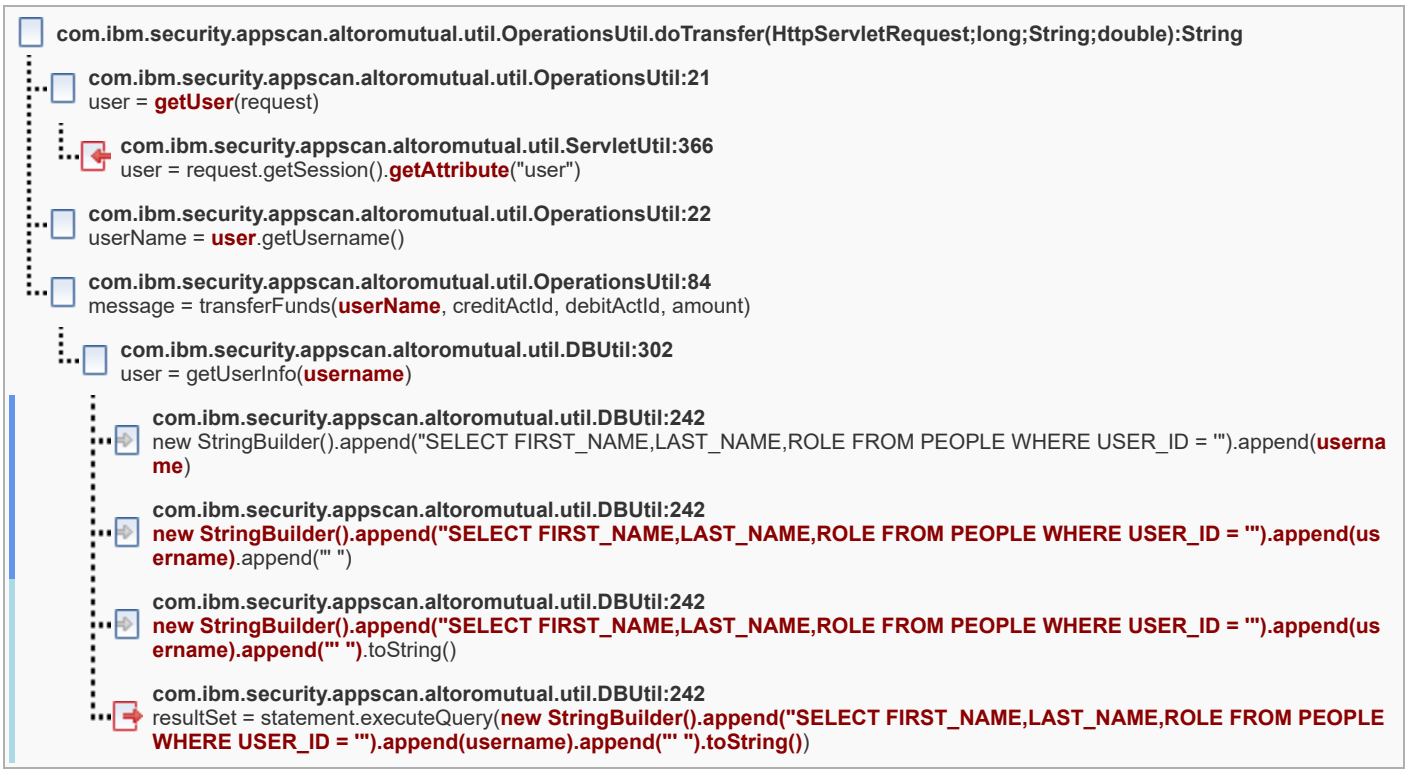


Issue 2 of 2

Issue ID:	7a126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	7e116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.executeQuery(String):ResultSet com.ibm.security.appscan.altoromutual.util.DBUtil:242
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.getUserInfo(java.lang.String):com.ibm.security.appscan.altoromutual.model.User
Line	242
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.http.HttpSession.getAttribute(String):Object *via* com.ibm.security.appscan.altoromutual.util.ServletUtil:366
Sink:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:242

Issue 2 of 2 - Details

Trace



H	Common Fix Point:SQL Injection: java.lang.StringBuilder.toString():java.lang.String
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.lang.StringBuilder.toString():java.lang.String
How to Fix:	SQL Injection

Issue 1 of 5

Issue ID:	8c126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:494
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String):java.lang.String
Line	494
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:58
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:494

Issue 1 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:58
lastname = request.**getParameter**("lastname")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:80
error = addUser(username, password1, firstname, **lastname**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(**lastname**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')").toStri

com.ibm.security.appscan.altoromutual.util.DBUtil:494
statement.execute(new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','

Issue 2 of 5

Issue ID:	8f126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:494
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String):java.lang.String
Line	494
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:60
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:494

Issue 2 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:60
password1 = request.**getParameter**("password1")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:80
error = addUser(username, **password1**, firstname, lastname)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(**password**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')").toStri

com.ibm.security.appscan.altoromutual.util.DBUtil:494
statement.execute(new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','

Issue 3 of 5

Issue ID:	92126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:494
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String):java.lang.String
Line	494
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:57
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:494

Issue 3 of 5 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:57
firstname = request.**getParameter**("firstname")

com.ibm.security.appscan.altoromutual.servlet.AdminServlet:80
error = addUser(username, password1, **firstname**, lastname)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(**firstname**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')").toStri

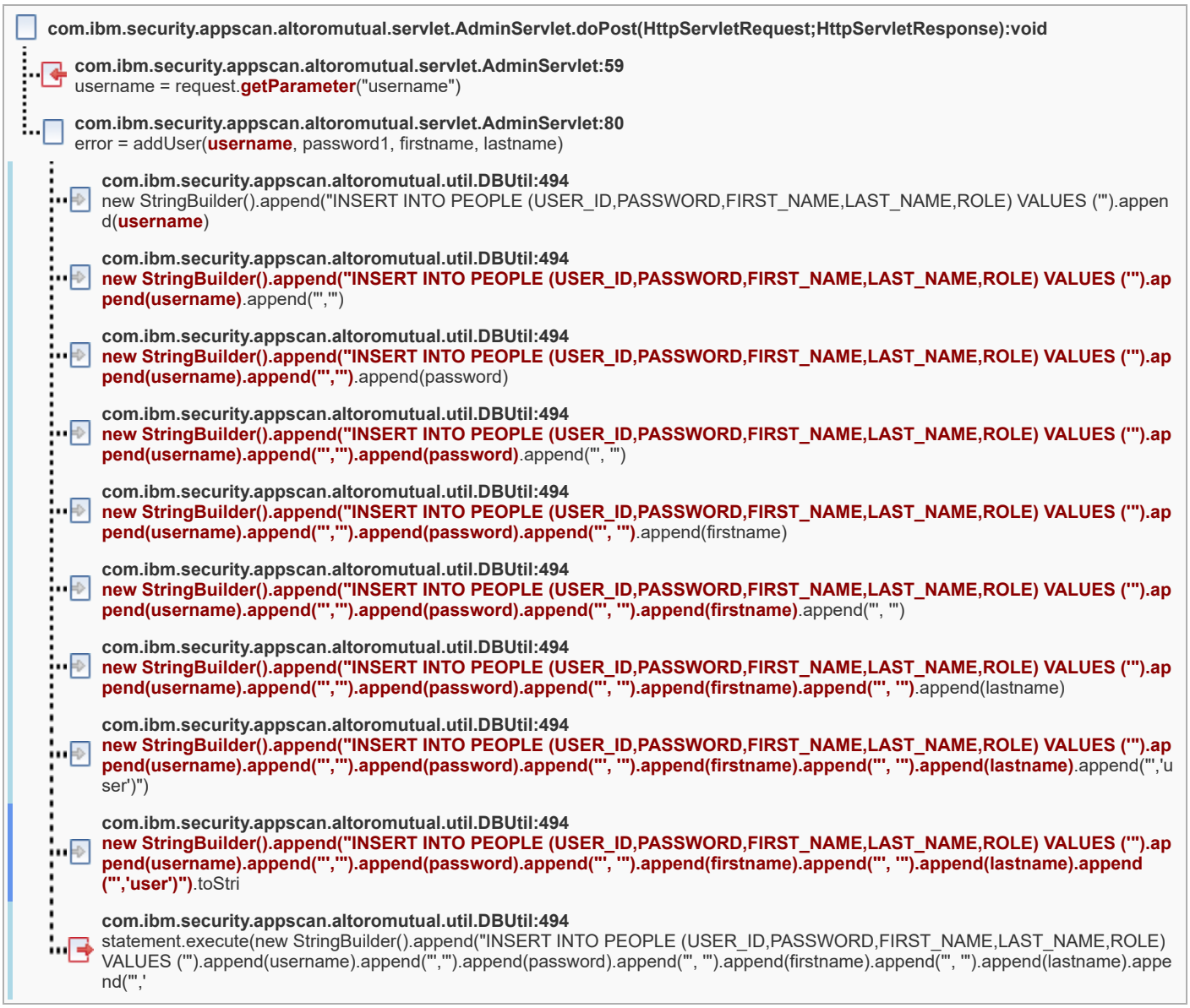
com.ibm.security.appscan.altoromutual.util.DBUtil:494
statement.execute(new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','

Issue 4 of 5

Issue ID:	95126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:494
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String):java.lang.String
Line	494
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AdminServlet:59
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:494

Issue 4 of 5 - Details

Trace


com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost(HttpServletRequest;HttpServletResponse):void
com.ibm.security.appscan.altoromutual.servlet.AdminServlet:59
username = request.getParameter("username")
com.ibm.security.appscan.altoromutual.servlet.AdminServlet:80
error = addUser(username, password1, firstname, lastname)
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username)
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','")
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password)
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '")
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname)
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '")
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname)
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append('user')")
com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')").toStri
com.ibm.security.appscan.altoromutual.util.DBUtil:494
statement.execute(new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','

Issue 5 of 5

Issue ID:	98126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	84116e59-fcd5-ee11-9f02-14cb65725114
Location	java.sql.Statement.execute(String):boolean com.ibm.security.appscan.altoromutual.util.DBUtil:494
Calling Method	com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String):java.lang.String
Line	494
Source File	com.ibm.security.appscan.altoromutual.util.DBUtil
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	89
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com\ibm\security\appscan\altoromutual\api\AdminAPI.java:69
Sink:	java.sql.Statement.execute(String):boolean *via* com.ibm.security.appscan.altoromutual.util.DBUtil:494

Issue 5 of 5 - Details

Trace

AppScan.Synthetic.JAXRS.post_admin_addUser():void

com\ibm\security\appscan\altoromutual\api\AdminAPI.java:69
wafl_local_0.**getParameter**("param1")

com\ibm\security\appscan\altoromutual\api\AdminAPI.java:69
local1 = local0.addUser(**wafl_local_0.getParameter("param1")**, wafl_local_1.getParameter("param2"))

com.ibm.security.appscan.altoromutual.api.AdminAPI:88
bodyJson = new JSONObject(**bodyJSON**)

com.ibm.security.appscan.altoromutual.api.AdminAPI:91
bodyJson.get("lastname")

com.ibm.security.appscan.altoromutual.api.AdminAPI:91
lastname = **bodyJson.get("lastname")**.toString()

com.ibm.security.appscan.altoromutual.api.AdminAPI:116
error = addUser(username, password1, firstname, **lastname**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(**lastname**)

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')")

com.ibm.security.appscan.altoromutual.util.DBUtil:494
new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','user')").toStri

com.ibm.security.appscan.altoromutual.util.DBUtil:494
statement.execute(new StringBuilder().append("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('").append(username).append("','").append(password).append("', '").append(firstname).append("', '").append(lastname).append("','

M Common Fix Point:Inappropriate Encoding for Output Context: com.ibm.security.appscan.altoromutual.model.Transaction.<init>(...

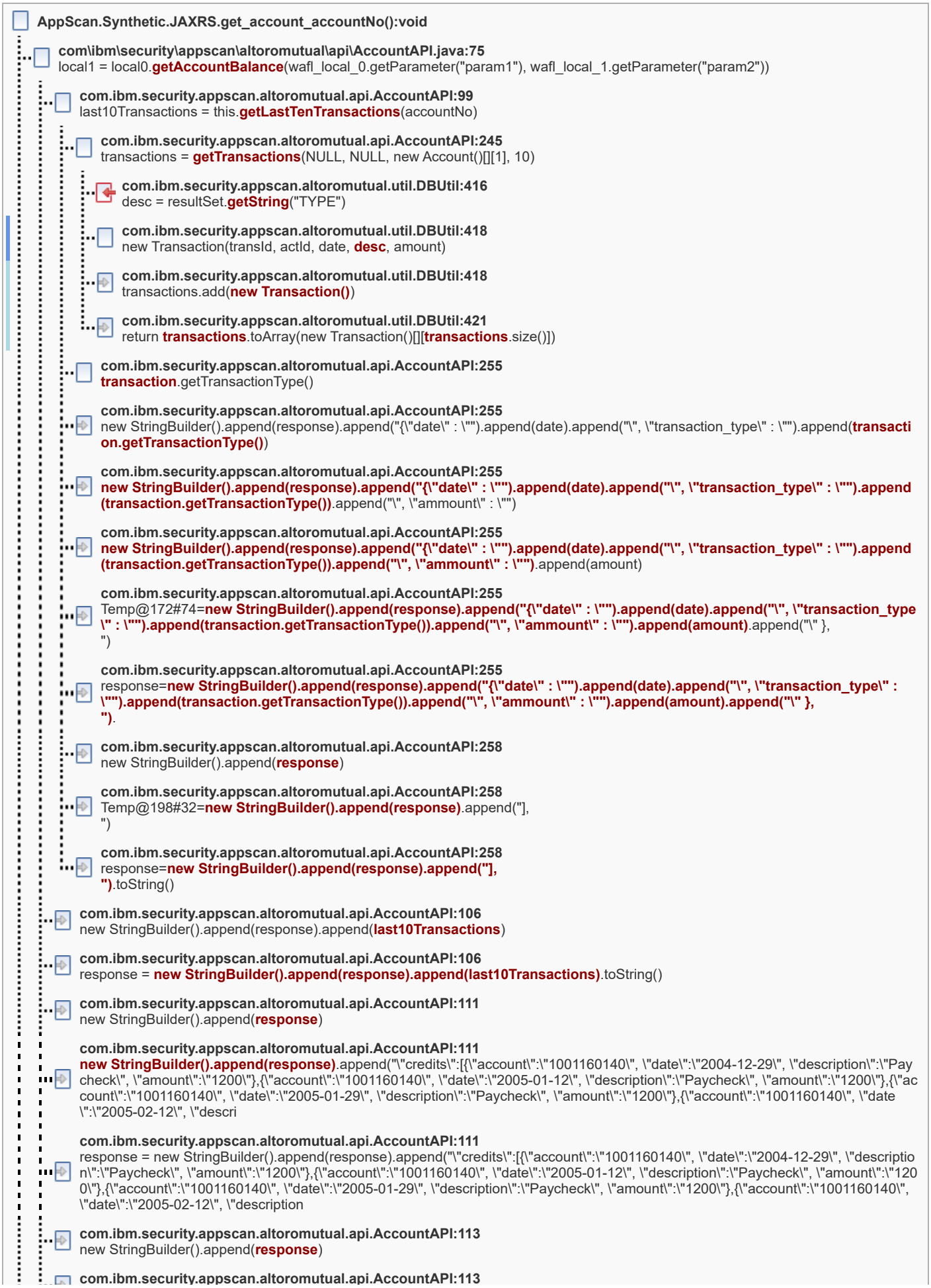
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	com.ibm.security.appscan.altoromutual.model.Transaction.<init>(int;long;java.util.Date;java.lang.String;double):void
How to Fix:	Inappropriate Encoding for Output Context

Issue 1 of 8

Issue ID:	03126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo():void
Line	75
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75

Issue 1 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
local1 = local0.getAccountBalance(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:99
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:416
desc = resultSet.getString("TYPE")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"descri
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
response = new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"description
com.ibm.security.appscan.altoromutual.api.AccountAPI:113
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:113

new StringBuilder().append(response).append("25\"},{\"account\":\"1001160140\", \"date\":\"2005-01-28\",

com.ibm.security.appscan.altoromutual.api.AccountAPI:113
response = new StringBuilder().append(response).append("25\"},{\"account\":\"1001160140\", \"date\":\"2005-01-28\", \"des

com.ibm.security.appscan.altoromutual.api.AccountAPI:115
myJson = new JSONObject(**response**)

com.ibm.security.appscan.altoromutual.api.AccountAPI:117
myJson.toString()

com.ibm.security.appscan.altoromutual.api.AccountAPI:117
status(200).entity(**myJson.toString()**)

com.ibm.security.appscan.altoromutual.api.AccountAPI:117
status(200).entity(myJson.toString()).build()

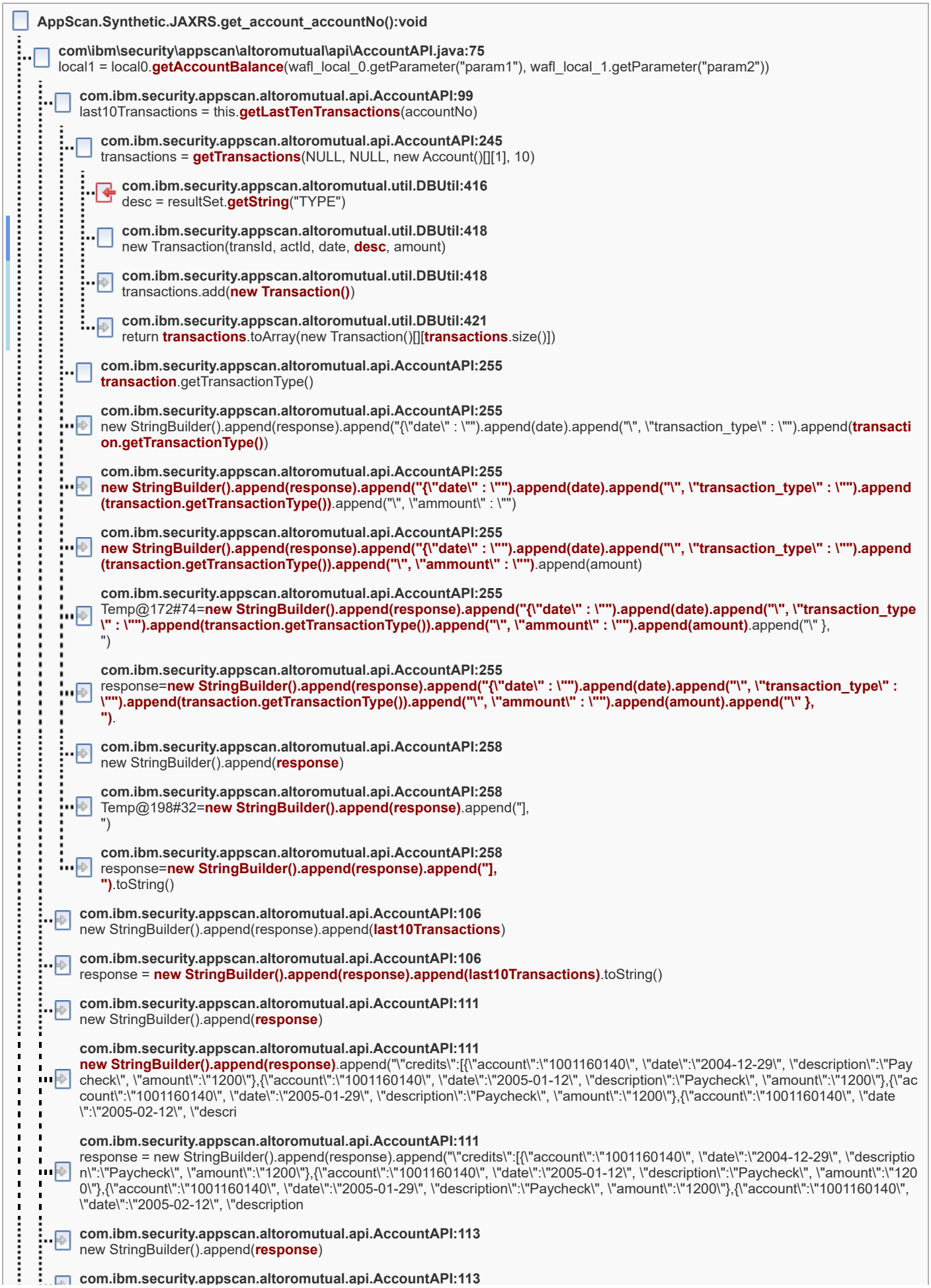
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
local2.print(**local1**)

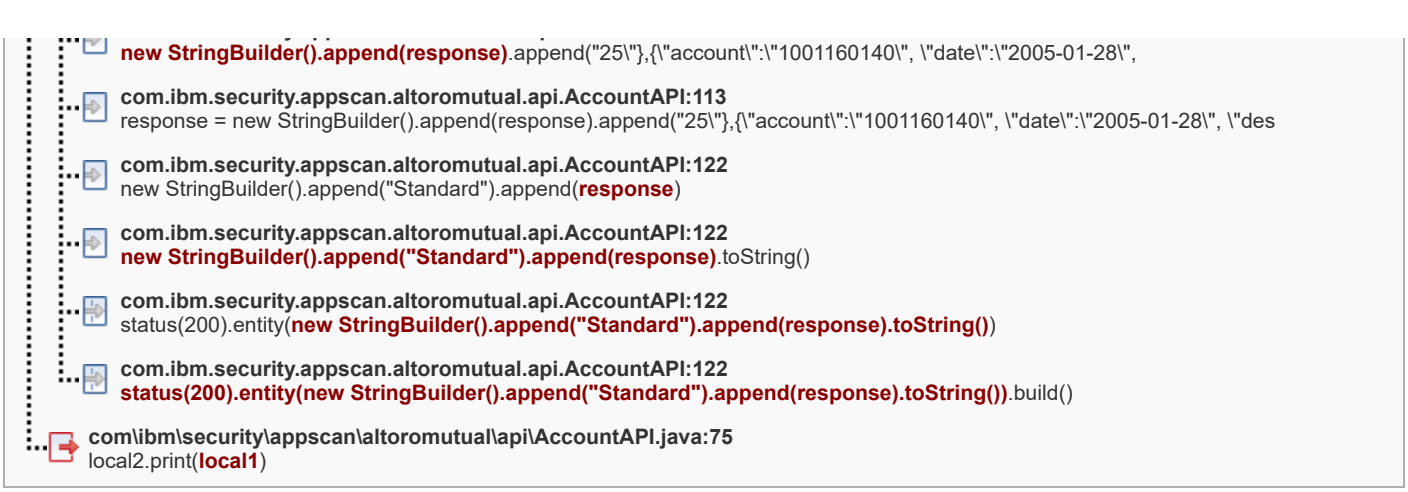
Issue 2 of 8

Issue ID:	06126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo():void
Line	75
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75

Issue 2 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
local1 = local0.getAccountBalance(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:99
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:416
desc = resultSet.getString("TYPE")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"descri
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
response = new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"description
com.ibm.security.appscan.altoromutual.api.AccountAPI:113
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:113

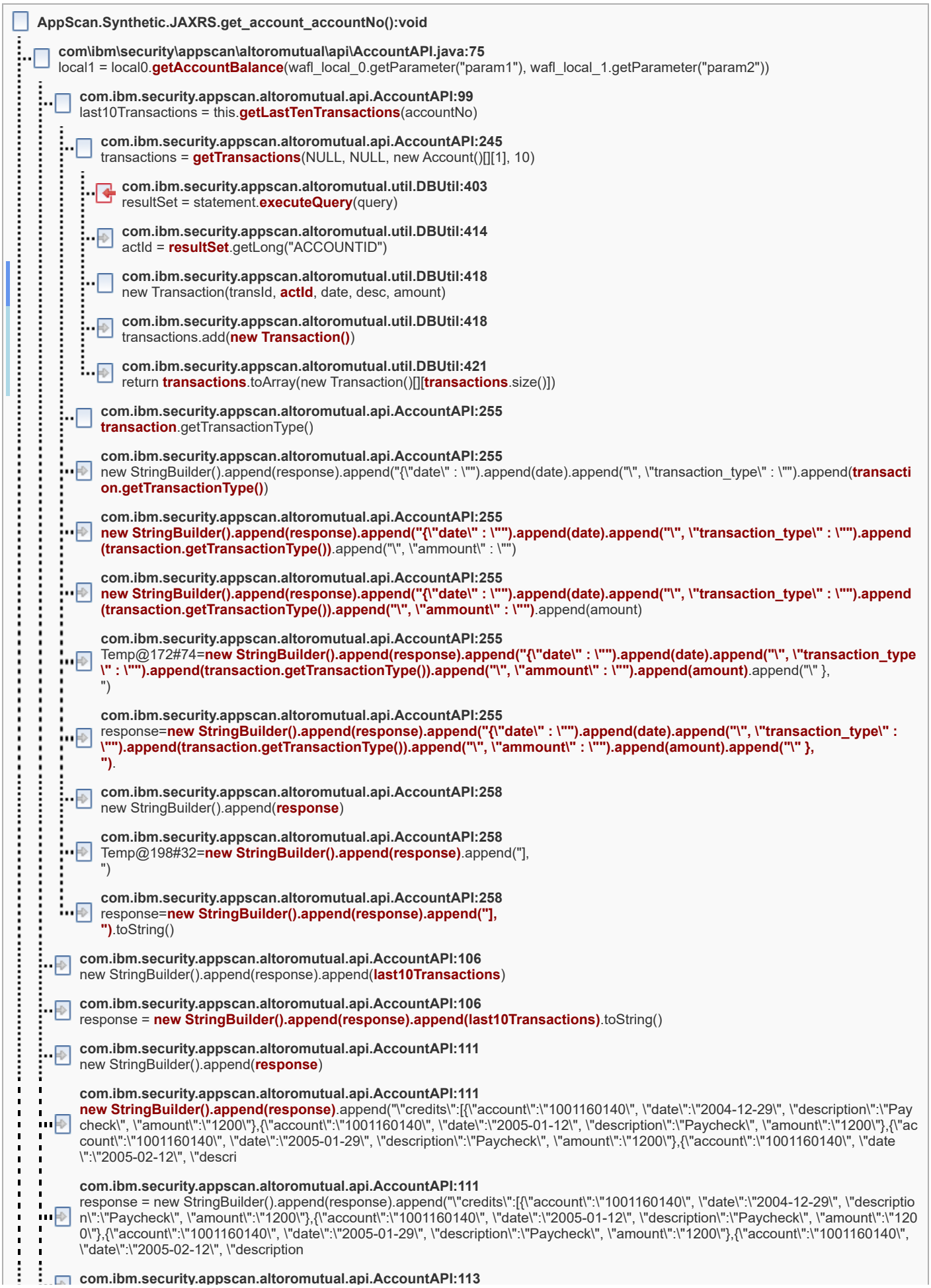


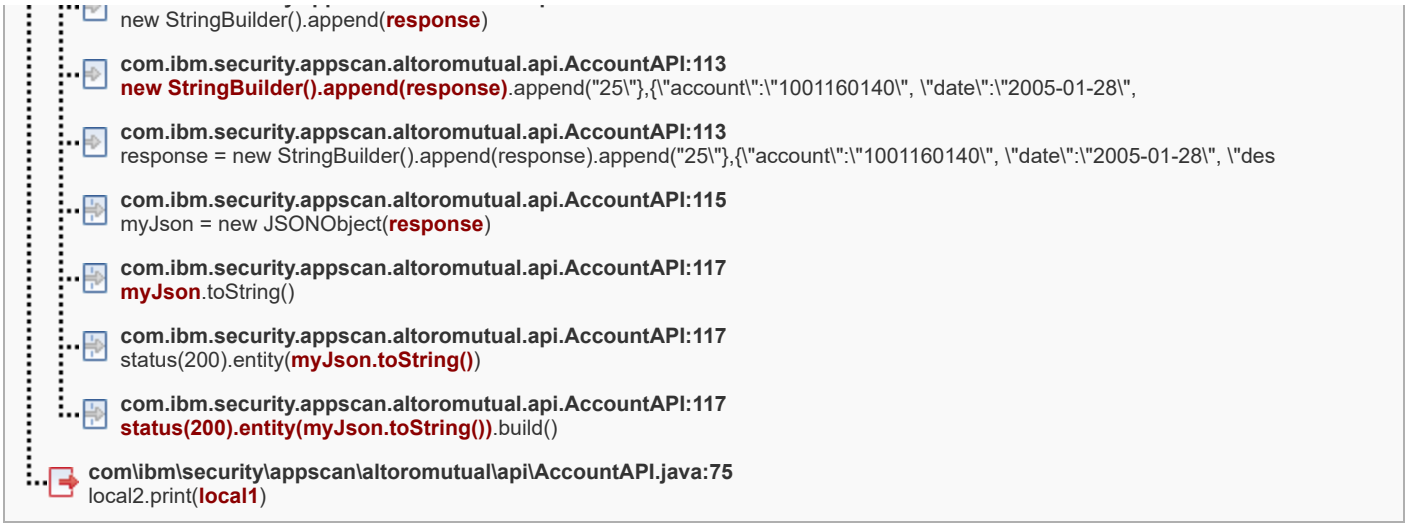
Issue 3 of 8

Issue ID:	09126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo():void
Line	75
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75

Issue 3 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
local1 = local0.getAccountBalance(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:99
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:403
resultSet = statement.executeQuery(query)
com.ibm.security.appscan.altoromutual.util.DBUtil:414
actId = resultSet.getLong("ACCOUNTID")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"descri
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
response = new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"description
com.ibm.security.appscan.altoromutual.api.AccountAPI:113

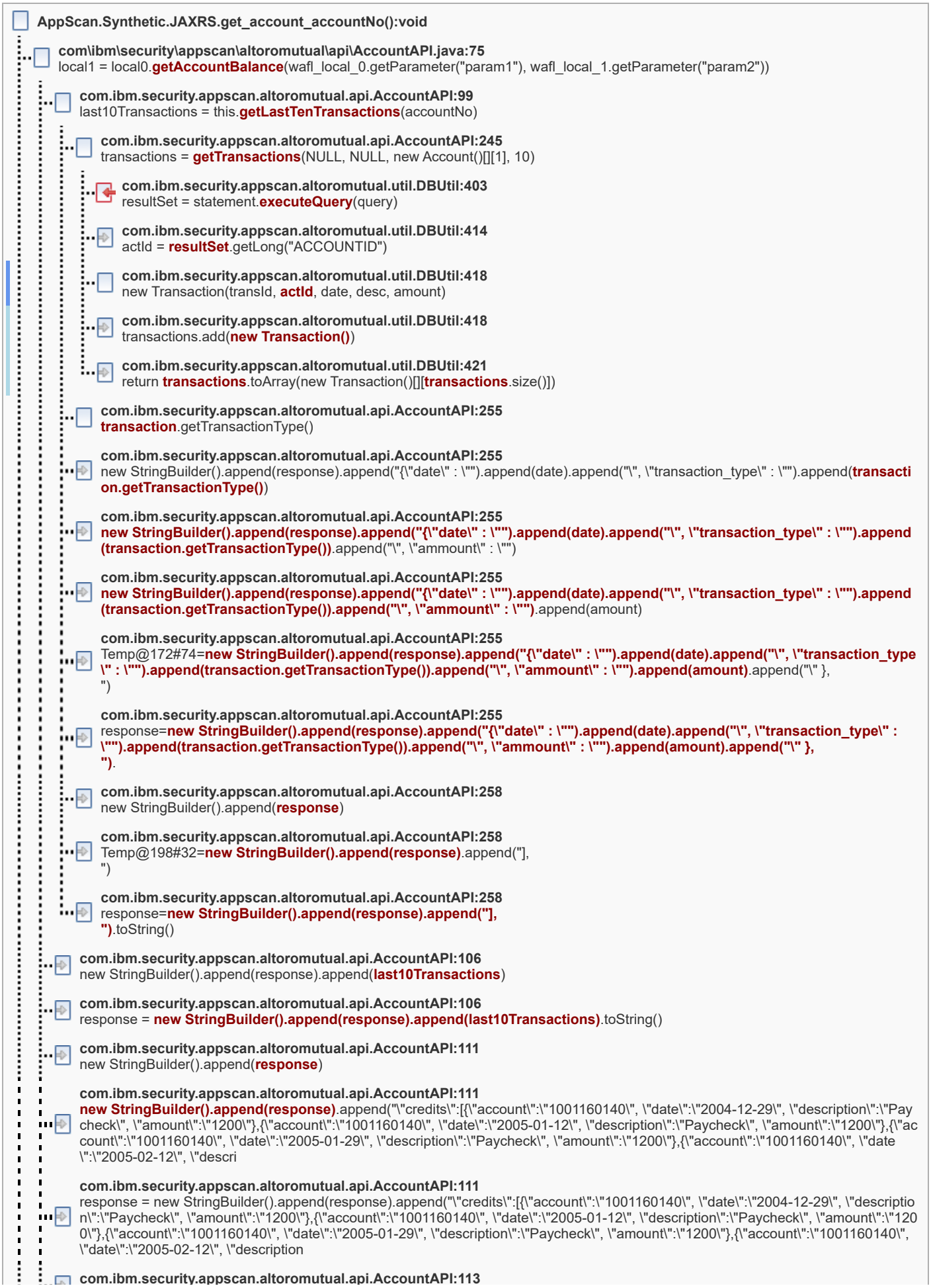


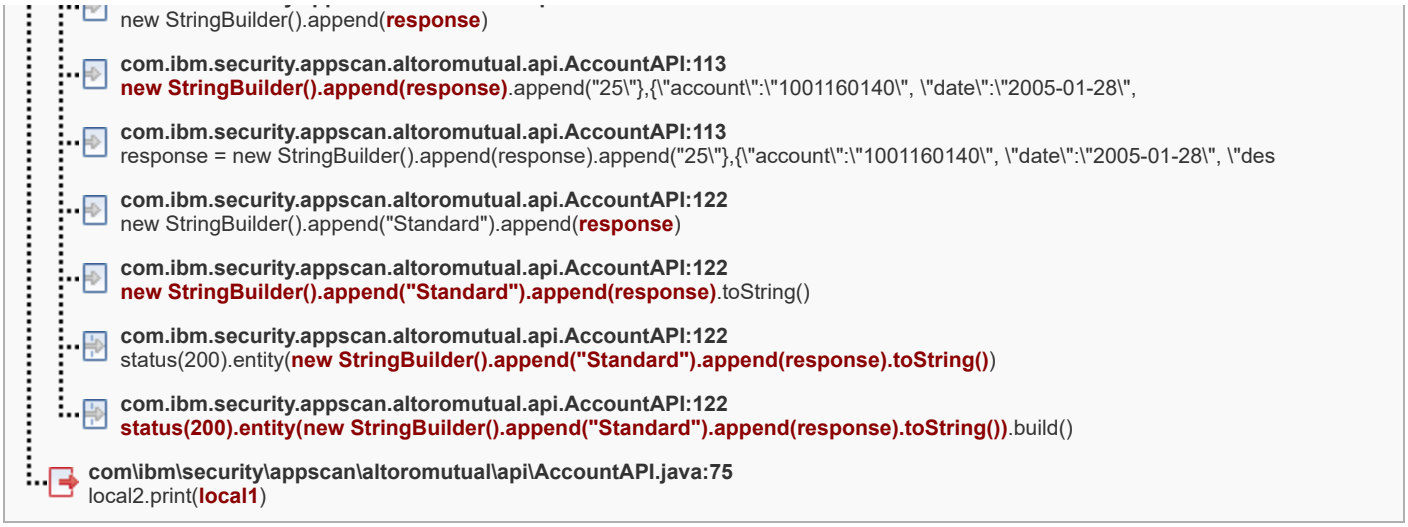
Issue 4 of 8

Issue ID:	0c126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo():void
Line	75
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75

Issue 4 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:75
local1 = local0.getAccountBalance(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:99
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:403
resultSet = statement.executeQuery(query)
com.ibm.security.appscan.altoromutual.util.DBUtil:414
actId = resultSet.getLong("ACCOUNTID")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:106
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"descri
com.ibm.security.appscan.altoromutual.api.AccountAPI:111
response = new StringBuilder().append(response).append("\"credits\":[{\"account\":\"1001160140\", \"date\":\"2004-12-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-12\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-01-29\", \"description\":\"Paycheck\", \"amount\":\"1200\"},{\"account\":\"1001160140\", \"date\":\"2005-02-12\", \"description
com.ibm.security.appscan.altoromutual.api.AccountAPI:113

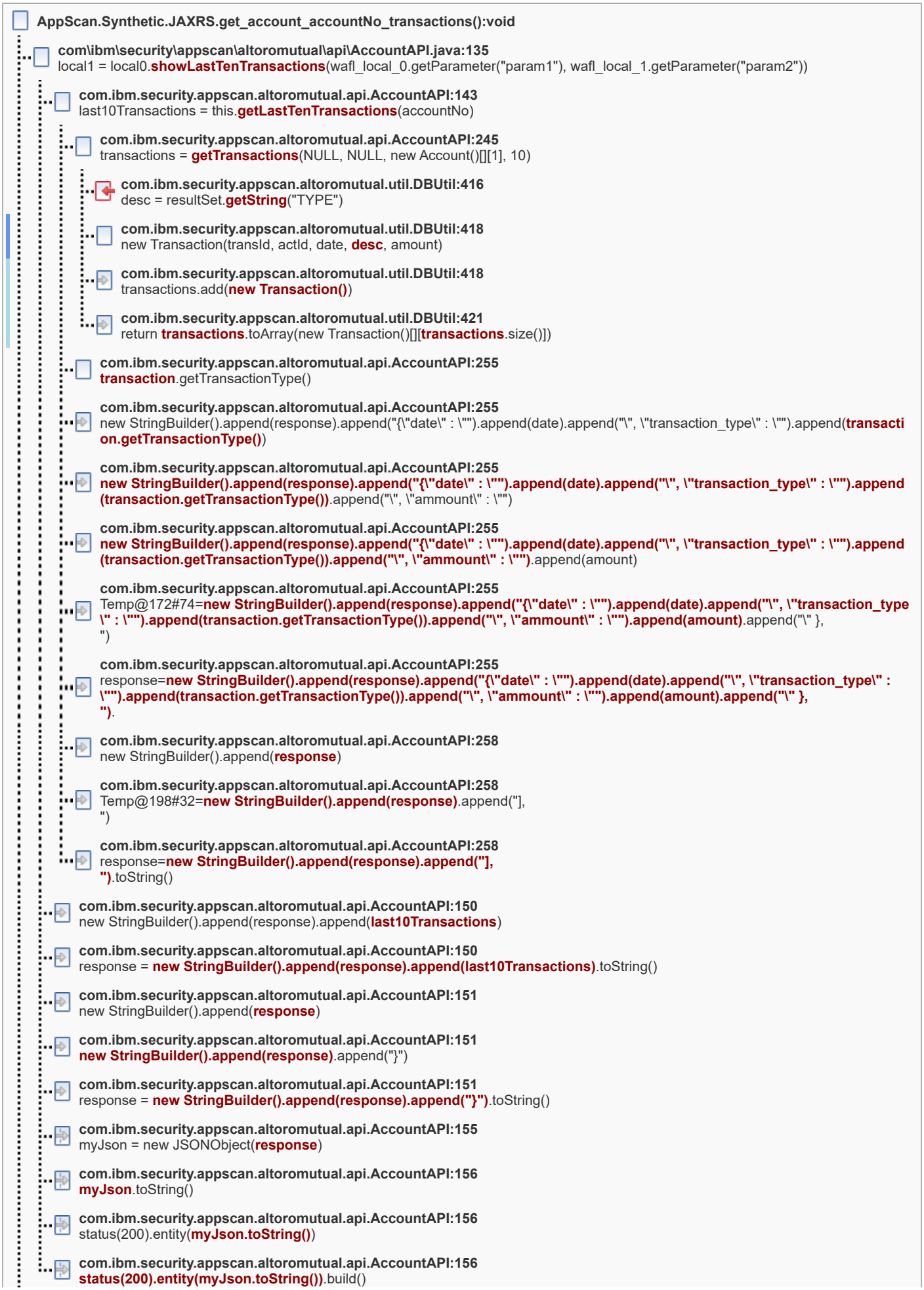


Issue 5 of 8

Issue ID:	0f126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo_transactions():void
Line	135
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135

Issue 5 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo_transactions():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
local1 = local0.showLastTenTransactions(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:143
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:416
desc = resultSet.getString("TYPE")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:150
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:150
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
new StringBuilder().append(response).append("}")
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
response = new StringBuilder().append(response).append("}").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:155
myJson = new JSONObject(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:156
myJson.toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:156
status(200).entity(myJson.toString())
com.ibm.security.appscan.altoromutual.api.AccountAPI:156
status(200).entity(myJson.toString()).build()

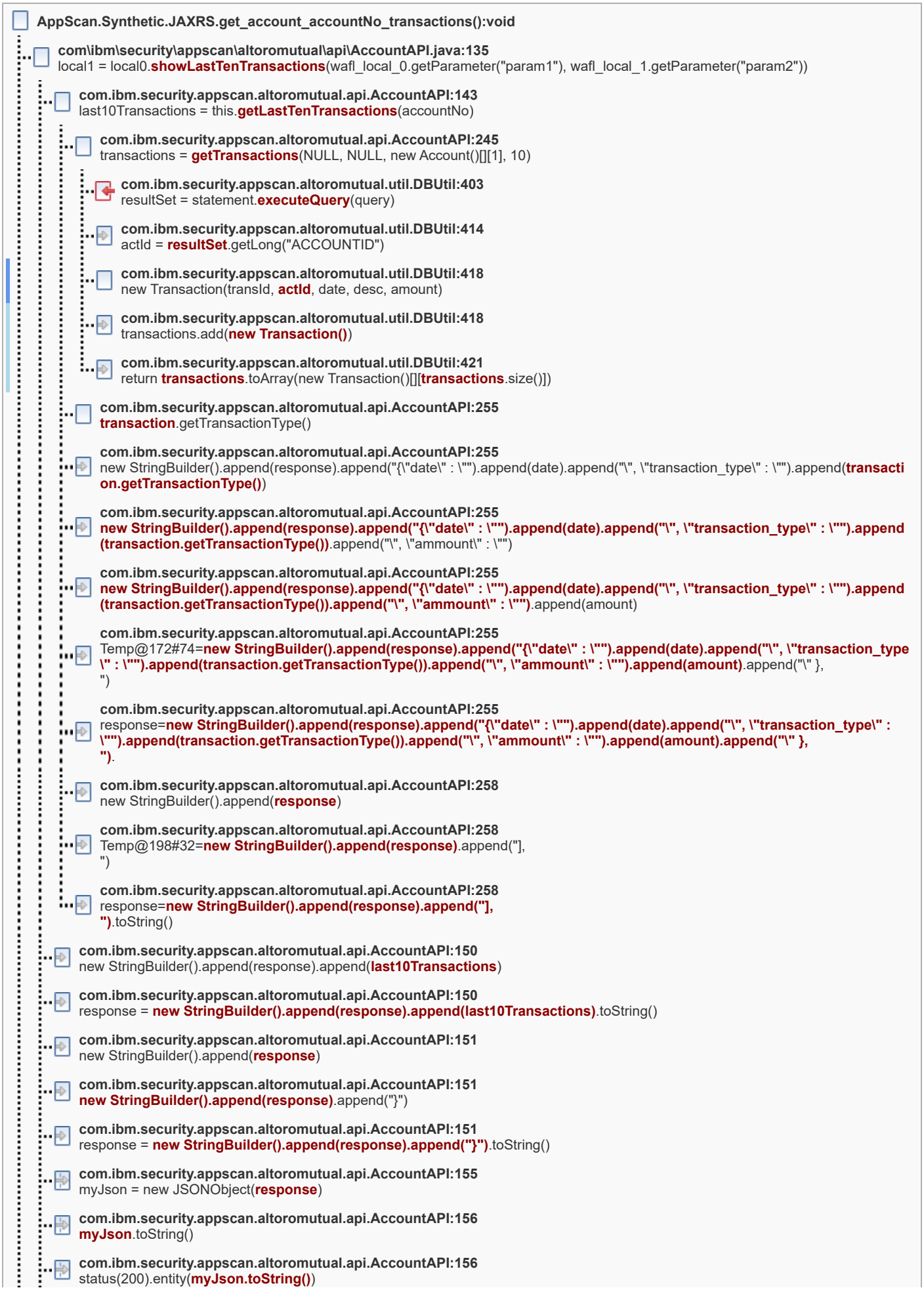
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
local2.print(**local1**)

Issue 6 of 8

Issue ID:	12126e59-fcd5-ee11-9f02-14cb65725114
Severity:	**Medium**
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
Calling Method	AppScan.Synthetic.JAXRS.get_account_accountNo_transactions():void
Line	135
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135

Issue 6 of 8 - Details

Trace


AppScan.Synthetic.JAXRS.get_account_accountNo_transactions():void
com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
local1 = local0.showLastTenTransactions(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"))
com.ibm.security.appscan.altoromutual.api.AccountAPI:143
last10Transactions = this.getLastTenTransactions(accountNo)
com.ibm.security.appscan.altoromutual.api.AccountAPI:245
transactions = getTransactions(NULL, NULL, new Account()[][1], 10)
com.ibm.security.appscan.altoromutual.util.DBUtil:403
resultSet = statement.executeQuery(query)
com.ibm.security.appscan.altoromutual.util.DBUtil:414
actId = resultSet.getLong("ACCOUNTID")
com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, desc, amount)
com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(new Transaction())
com.ibm.security.appscan.altoromutual.util.DBUtil:421
return transactions.toArray(new Transaction()[][transactions.size()])
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
transaction.getTransactionType()
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType())
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount)
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
Temp@172#74=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:255
response=new StringBuilder().append(response).append("{\"date\" : \"").append(date).append("\", \"transaction_type\" : \"").append(transaction.getTransactionType()).append("\", \"ammount\" : \"").append(amount).append("\" },
").
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
Temp@198#32=new StringBuilder().append(response).append("],
")
com.ibm.security.appscan.altoromutual.api.AccountAPI:258
response=new StringBuilder().append(response).append("],
").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:150
new StringBuilder().append(response).append(last10Transactions)
com.ibm.security.appscan.altoromutual.api.AccountAPI:150
response = new StringBuilder().append(response).append(last10Transactions).toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
new StringBuilder().append(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
new StringBuilder().append(response).append("}")
com.ibm.security.appscan.altoromutual.api.AccountAPI:151
response = new StringBuilder().append(response).append("}").toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:155
myJson = new JSONObject(response)
com.ibm.security.appscan.altoromutual.api.AccountAPI:156
myJson.toString()
com.ibm.security.appscan.altoromutual.api.AccountAPI:156
status(200).entity(myJson.toString())

com.ibm.security.appscan.altoromutual.api.AccountAPI:156
status(200).entity(myJson.toString()).build()

com\ibm\security\appscan\altoromutual\api\AccountAPI.java:135
local2.print(**local1**)

Issue 7 of 8

Issue ID:	15126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
Calling Method	AppScan.Synthetic.JAXRS.post_account_accountNo_transactions():void
Line	175
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.ResultSet.getString(String):String *via* com.ibm.security.appscan.altoromutual.util.DBUtil:416
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175

Issue 7 of 8 - Details

Trace

AppScan.Synthetic.JAXRS.post_account_accountNo_transactions():void

com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
local1 = local0.**getTransactions**(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"), wafl_local_2.getParameter("param3"))

com.ibm.security.appscan.altoromutual.api.AccountAPI:196
transactions = user.**getUserTransactions**(startString, endString, account)

com.ibm.security.appscan.altoromutual.model.User:104
transactions = **getTransactions**(startDate, endDate, accounts, -1)

com.ibm.security.appscan.altoromutual.util.DBUtil:416
desc = resultSet.**getString**("TYPE")

com.ibm.security.appscan.altoromutual.util.DBUtil:418
new Transaction(transId, actId, date, **desc**, amount)

com.ibm.security.appscan.altoromutual.util.DBUtil:418
transactions.add(**new Transaction()**)

com.ibm.security.appscan.altoromutual.util.DBUtil:421
return **transactions**.toArray(new Transaction()[][**transactions**.size()])

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
transactions[i].getTransactionType()

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append(date).append("\",\"account\":\"").append(transactions[i].g

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append(date).append("\",\"account\":\"").append(transactions[i].g

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append(date).append("\",\"account\":\"").append(transactions[i].g

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append(date).append("\",\"account\":\"").append(transactions[i].g

com.ibm.security.appscan.altoromutual.api.AccountAPI:223
response = new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append(date).append("\",\"account\":\"").append(transactions[i].getA

com.ibm.security.appscan.altoromutual.api.AccountAPI:227
new StringBuilder().append(**response**)

com.ibm.security.appscan.altoromutual.api.AccountAPI:227
new StringBuilder().append(response).append("]}")

com.ibm.security.appscan.altoromutual.api.AccountAPI:227
response = **new StringBuilder().append(response).append("]}")**.toString()

com.ibm.security.appscan.altoromutual.api.AccountAPI:230
myJson = new JSONObject(**response**)

com.ibm.security.appscan.altoromutual.api.AccountAPI:235
myJson.toString()

com.ibm.security.appscan.altoromutual.api.AccountAPI:235
status(200).entity(**myJson.toString()**)

com.ibm.security.appscan.altoromutual.api.AccountAPI:235
status(200).entity(myJson.toString()).build()

com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
local2.print(**local1**)

Issue 8 of 8

Issue ID:	18126e59-fcd5-ee11-9f02-14cb65725114
Severity:	Medium
Status	Open
Fix Group ID:	86116e59-fcd5-ee11-9f02-14cb65725114
Location	java.io.PrintWriter.print(Object):void com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
Calling Method	AppScan.Synthetic.JAXRS.post_account_accountNo_transactions():void
Line	175
Source File	com\ibm\security\appscan\altoromutual\api\AccountAPI.java
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	116
Source:	java.sql.Statement.executeQuery(String):ResultSet *via* com.ibm.security.appscan.altoromutual.util.DBUtil:403
Sink:	java.io.PrintWriter.print(Object):void *via* com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175

Issue 8 of 8 - Details

Trace

```
AppScan.Synthetic.JAXRS.post_account_accountNo_transactions():void

  com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
  local1 = local0.getTransactions(wafl_local_0.getParameter("param1"), wafl_local_1.getParameter("param2"), wafl_local_2.getParameter
  ("param3"))

    com.ibm.security.appscan.altoromutual.api.AccountAPI:196
    transactions = user.getUserTransactions(startString, endString, account)

      com.ibm.security.appscan.altoromutual.model.User:104
      transactions = getTransactions(startDate, endDate, accounts, -1)

        com.ibm.security.appscan.altoromutual.util.DBUtil:403
        resultSet = statement.executeQuery(query)

        com.ibm.security.appscan.altoromutual.util.DBUtil:414
        actId = resultSet.getLong("ACCOUNTID")

        com.ibm.security.appscan.altoromutual.util.DBUtil:418
        new Transaction(transId, actId, date, desc, amount)

        com.ibm.security.appscan.altoromutual.util.DBUtil:418
        transactions.add(new Transaction())

        com.ibm.security.appscan.altoromutual.util.DBUtil:421
        return transactions.toArray(new Transaction()[][transactions.size()])

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      transactions[i].getTransactionType()

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append
      (date).append("\",\"account\":\"").append(transactions[i].g

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append
      (date).append("\",\"account\":\"").append(transactions[i].g

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append
      (date).append("\",\"account\":\"").append(transactions[i].g

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date\":\"").append
      (date).append("\",\"account\":\"").append(transactions[i].g

      com.ibm.security.appscan.altoromutual.api.AccountAPI:223
      response = new StringBuilder().append(response).append("{\"id\":\"").append(transactions[i].getTransactionId()).append("\",\"date
      \":\"").append(date).append("\",\"account\":\"").append(transactions[i].getA

      com.ibm.security.appscan.altoromutual.api.AccountAPI:227
      new StringBuilder().append(response)

      com.ibm.security.appscan.altoromutual.api.AccountAPI:227
      new StringBuilder().append(response).append("]}")

      com.ibm.security.appscan.altoromutual.api.AccountAPI:227
      response = new StringBuilder().append(response).append("]}").toString()

      com.ibm.security.appscan.altoromutual.api.AccountAPI:230
      myJson = new JSONObject(response)

      com.ibm.security.appscan.altoromutual.api.AccountAPI:235
      myJson.toString()

      com.ibm.security.appscan.altoromutual.api.AccountAPI:235
      status(200).entity(myJson.toString())

      com.ibm.security.appscan.altoromutual.api.AccountAPI:235
      status(200).entity(myJson.toString()).build()

    com\ibm\security\appscan\altoromutual\api\AccountAPI.java:175
    local2.print(local1)
```

H Common Fix Point:Validation Required: javax.servlet.ServletRequest.setAttribute(java.lang.String;java...

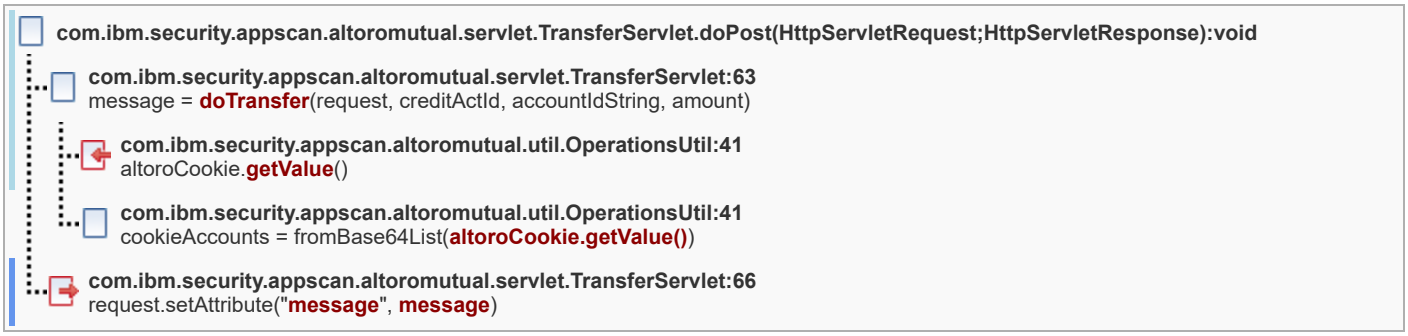
Fix Group ID:	82116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	javax.servlet.ServletRequest.setAttribute(java.lang.String;java.lang.Object):void
How to Fix:	Validation Required

Issue 1 of 2

Issue ID:	5c126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	82116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.ServletRequest.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.TransferServlet:66
Calling Method	com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	66
Source File	com.ibm.security.appscan.altoromutual.servlet.TransferServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.http.Cookie.getValue():String *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:41
Sink:	javax.servlet.ServletRequest.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.TransferServlet:66

Issue 1 of 2 - Details

Trace

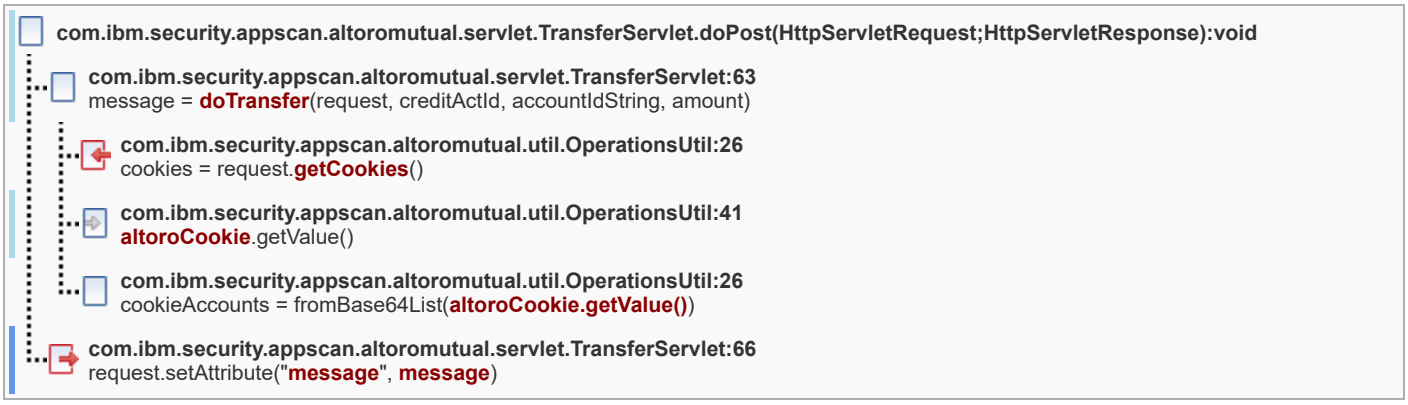


Issue 2 of 2

Issue ID:	5f126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	82116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.ServletRequest.setAttribute(String;Object):void com.ibm.security.appscan.altoromutual.servlet.TransferServlet:66
Calling Method	com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	66
Source File	com.ibm.security.appscan.altoromutual.servlet.TransferServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	20
Source:	javax.servlet.http.HttpServletRequest.getCookies():Cookie[] *via* com.ibm.security.appscan.altoromutual.util.OperationsUtil:26
Sink:	javax.servlet.ServletRequest.setAttribute(String;Object):void *via* com.ibm.security.appscan.altoromutual.servlet.TransferServlet:66

Issue 2 of 2 - Details

Trace



H Common Fix Point:Open Redirect: java.lang.StringBuilder.append(java.lang.String):java.lang.Stri...

Fix Group ID:	73116e59-fcd5-ee11-9f02-14cb65725114
Status:	Open
Date:	2024-02-28 05:43:51Z
Location of fix:	java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder
How to Fix:	Open Redirect

Issue 1 of 3

Issue ID:	3e126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	73116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpServletResponse.sendRedirect(String):void com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
Calling Method	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	53
Source File	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
Source:	javax.servlet.http.HttpServlet.doGet(HttpServletRequest;HttpServletResponse):void *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:65
Sink:	javax.servlet.http.HttpServletResponse.sendRedirect(String):void *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53

Issue 1 of 3 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:65
this.doGet(**request**, response)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
request.getContextPath()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(**request.getContextPath()**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp")

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
response.sendRedirect(**new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()**)

Issue 2 of 3

Issue ID:	41126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	73116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpServletResponse.sendRedirect(String):void com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
Calling Method	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	53
Source File	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:51
Sink:	javax.servlet.http.HttpServletResponse.sendRedirect(String):void *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53

Issue 2 of 3 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:51
accountName = request.**getParameter**("listAccounts")

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
new StringBuilder().append("/bank/balance.jsp?acctId=").append(**accountName**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
new StringBuilder().append("/bank/balance.jsp?acctId=").append(accountName).toString()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
dispatcher = request.getRequestDispatcher(**new StringBuilder().append("/bank/balance.jsp?acctId=").append(accountName).toString()**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:63
this.doPost(**request**, response)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
request.getContextPath()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(**request.getContextPath()**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp")

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
response.sendRedirect(**new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()**)

Issue 3 of 3

Issue ID:	44126e59-fcd5-ee11-9f02-14cb65725114
Severity:	High
Status	Open
Fix Group ID:	73116e59-fcd5-ee11-9f02-14cb65725114
Location	javax.servlet.http.HttpServletResponse.sendRedirect(String):void com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
Calling Method	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(javax.servlet.http.HttpServletRequest;javax.servlet.http.HttpServletResponse):void
Line	53
Source File	com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet
Date Created	Wednesday, February 28, 2024
Last Updated	Wednesday, February 28, 2024
CWE:	601
Source:	javax.servlet.ServletRequest.getParameter(String):String *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:51
Sink:	javax.servlet.http.HttpServletResponse.sendRedirect(String):void *via* com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53

Issue 3 of 3 - Details

Trace

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(HttpServletRequest;HttpServletResponse):void

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:51
accountName = request.**getParameter**("listAccounts")

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
new StringBuilder().append("/bank/balance.jsp?acctId=").append(**accountName**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
new StringBuilder().append("/bank/balance.jsp?acctId=").append(accountName).toString()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:57
dispatcher = request.getRequestDispatcher(**new StringBuilder().append("/bank/balance.jsp?acctId=").append(accountName).toString()**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
request.getContextPath()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(**request.getContextPath()**)

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp")

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()

com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet:53
response.sendRedirect(**new StringBuilder().append(request.getContextPath()).append("/bank/main.jsp").toString()**)

How to Fix

M Authentication.Entity - java.sql.DriverManager.getConnection(String):Connection

Cause

Authentication.Entity refers to cases in which an application insecurely performs authentication. For example, if username and password information are stored in the source code in clear text, an attacker who gains access to the source code will learn the credentials needed to compromise the database.

Fix recommendation

Never store passwords in clear text. If the password must be remembered in memory for a short time to perform authentication null out the value as soon as possible to mitigate reading memory blocks to determine the password. In some languages String objects are kept alive throughout the run of the program. In those instances prefer using a char[] array instead of a String ibject and set every byte to '0' after the password is used for login.

H Command Injection

Cause

The software constructs a system command using untrusted data, such as user input. However, the application fails to neutralize elements that could modify the intended OS command, leading to execution of arbitrary OS commands.

Risk

Command injection allows attackers to execute unexpected, dangerous commands directly on the operating system. This may result in the attacker being able to remotely run arbitrary commands on the server.

This can often result in complete compromise of the server and its contents.

This weakness can lead to a vulnerability in cases where the attacker does not have direct access to the operating system, such as in web applications. Alternatively, if the weakness occurs in a privileged program, it could allow the attacker to specify commands that would not normally be accessible, or to call alternative commands with privileges that the attacker does not have. The problem is exacerbated if the compromised process does not follow the principle of least privilege, because the attacker-controlled commands may run with special system privileges that increases the damage.

Fix recommendation

Use secure APIs for executing commands. Avoid calling OS commands directly, and use library calls rather than external processes to create the desired functionality.

Sanitize user input and perform Input Validation. The best way to do this is to use an allowlist. An allowlist is an accepted list of values that the application will accept. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules.

Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment.

CWE

78

External references

- OWASP Command Injection Defense Cheat Sheet

Go to Table of Contents

H Cross-Site Scripting

Cause

Cross-site scripting (XSS) vulnerabilities arise when an attacker sends malicious code to the victim's browser, mostly using JavaScript. A vulnerable web application might embed untrusted data in the output, without filtering or encoding it. In this way, an attacker can inject a malicious script to the application, and the script will be returned in the response. This will then run on the victim's browser.
In particular, sanitization of hazardous characters was not performed correctly on user input or untrusted data.

Risk

XSS attacks can expose the user's session cookie, allowing the attacker to hijack the user's session and gain access to the user's account, which could lead to impersonation of users.

An attacker could modify and view the users' records and perform transactions as those users. The attacker may be able to perform privileged operations on behalf of the user, or gain access to any sensitive data belonging to the user. This would be especially dangerous if the user has administrator permissions.

The attacker could even run a malicious script on the victim's browser which would redirect the user to other pages or sites, modify content presentation, or even make it possible to run malicious software or a crypto miner.

Exploit example

The following example shows a script that returns a parameter value in the response.
The parameter value is sent to the script using a GET request, and then returned in the response embedded in the HTML.

```
GET /index.aspx?name=JSmith HTTP/1.1
```

```
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

An attacker might leverage the attack like this. In this case, the JavaScript code will be executed by the browser.

```
GET /index.aspx?name=>'"><script>alert('XSS')</script> HTTP/1.1
```

```
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >'"><script>alert('XSS')</script>
</HTML>
```

Fix recommendation

Fully encode all dynamic data from an untrusted source that is inserted into the webpage, to ensure it is treated as literal text and not as a script that could be executed or markup that could be rendered.

Consider the context in which your data will be used, and contextually encode the data as close as possible to the actual output: e.g. HTML encoding for HTML content; HTML Attribute encoding for data output to attribute values; JavaScript encoding for dynamically generated JavaScript. For example, when HTML encoding non-alphanumeric characters into HTML entities, `<` and `>` would become `<` and `>`.

As an extra defensive measure, validate all external input on the server, regardless of source. Carefully check each input parameter against a rigorous positive specification (allowlist) defining data type; size; range; format; and acceptable values. Regular expressions or framework controls may be useful in some cases, though this is not a replacement for output encoding.

Output encoding and data validation must be done on all untrusted data, wherever it comes from: e.g. form fields, URL parameters, web service arguments, cookies, any data from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files and filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

For every web page that is returned by the server, explicitly set the `Content-Type` HTTP response header. This header value should define a specific character encoding (charset), such as `ISO-8859-1` or `UTF-8`. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page, which would allow a potential attacker to bypass XSS protections.

Additionally, set the `httpOnly` flag on the session cookie, to prevent any XSS exploits from stealing a user's cookie.

Prefer using a framework or standard library that prevents this vulnerability by automatically encoding all dynamic output based on context, or at least that provides constructs that make it easier to avoid.

For every web page that is returned by the server, explicitly set the `Content-Security-Policy` HTTP response header, In order to make it significantly more difficult for the attacker to actually exploit the XSS attack.

CWE

79

External references

- Cross-site Scripting (XSS)
- OWASP XSS Cheat Sheet

L Improper Handling of Exceptional Conditions - java.lang.Throwable.printStackTrace():void

Cause

An attacker can cause errors to occur by submitting unusual requests to the web application. The response to these errors can reveal detailed system information, deny service, cause security mechanisms to fail, or crash the server. An attacker can use error messages that reveal technologies, operating systems, and product versions to tune the attack against known vulnerabilities in these technologies. The application uses diagnostic methods that provide significant implementation details such as stack traces as part of its error handling mechanism.
Production applications should never use methods that generate internal details such as stack traces and error messages unless that information is directly committed to a log that is not viewable by the end user. All error message text should be HTML entity encoded before being written to the log file to protect against potential cross-site scripting attacks against the viewer of the logs.

Fix recommendation

Rather than providing full details including stack traces to the user of your application, log the full details privately, and display a generic message to the user. The following example shows a caught exception being logged to a log file and a simple error message displayed to the user.

try{ //something here} catch (Exception e) { // full details in log file Utils.logExceptions("Some note here", e); // rethrow with generic message throw new Exception("Generic user message");}bad

H Inappropriate Encoding for Output Context

Cause

The application uses a method that sends data to an external system and that external system is capable of executing code embedded in the data it receives. If the sent data contains malicious scripts, this can lead to malicious scripting attacks and unexpected behavior on the external system. Therefore, it is important to encode the output data appropriately to prevent it from subsequently being interpreted as script code. Although not a common practice, sometimes it may be necessary to encode received data to prevent malicious scripts from getting into the application in the first place.
Typical vulnerable external systems include scripting-enabled clients such as web browsers and database servers. Thus, this finding is primarily applicable to web applications. If content created from unvalidated user input generates dynamic web pages or is stored in data sources, an attacker can introduce malicious scripts, such as JavaScript, into data that other users may later view in a web browser. When viewed, these scripts will be interpreted by the browser and run with the viewing user's security context for communicating with the originating web site. Thus, the attacker's code runs with the same privileges granted to legitimate code sent by the web site.
For example, in a message board application, an attacker can put the following malicious script onto the message board:

```
This is my message <script>alert(document.cookie)</script>
```

When viewed by another user, the victim's browser interprets the code between the <script> tags, resulting in a cross-site scripting attack. In this case, the victim's session cookie appears to the victim in a popup window. In a real attack scenario, a malicious script can send the cookie to the attacker's web site, and then use it for a session hijacking attack.

Non web-based applications can also stage malicious scripting attacks. For example, any application that generates log messages could attack system or security administrators through web-based log viewers. Also, an application that generates email alert messages can attack web-based or other JavaScript-enabled mail clients.

Fix recommendation

To defend against this kind of attack, the application should encode certain special characters that may be meaningful to other systems, especially for data that will be sent to other systems. For example, it may be useful to apply HTML entity encoding to all data that will be sent to an HTML browser, which may include web pages and log files. HTML entity encoding translates all non-alphanumeric characters into a special character sequence that HTML enabled viewers will not interpret. For example, < and > become < and > respectively. Likewise, if the contents of a free text field are to be stored in a database, one alternative to filtering out special SQL characters (like ' or -) is simply base64 encoding the text before sending it to the database.

Encoded with HTML entity encoding, the above message will become:

This is my message <script>alert(document.cookie)</script>bad

When viewed by a browser, the whole message will be interpreted as pure text.

External references

- Escaping special characters

Go to Table of Contents

M Open Redirect - Allowing untrusted site by passing user controlled input

Cause

The web application redirects users to an external site based on untrusted data.
In particular, the submitted request was found to include a URL as a parameter. The web application uses this value to redirect the user's browser to the specified URL.
An attacker can modify this URL value to an arbitrary address. The attacker would then cause the victim to submit the altered request, thus being redirected to a site of the attacker's choosing.

Risk

This vulnerability can allow an attacker to take advantage of the trust the user holds for the application, causing them to trust an arbitrary site under control of the attacker as well. This would often be leveraged through the use of phishing techniques.

Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

An attacker may successfully launch a phishing scam and steal user credentials or other sensitive information such as credit card number, social security number, and more.

It can also be possible to redirect the user to install malware that could infect the user's computer.

Exploit example

The following example shows a URL redirection to untrusted site.
The redir parameter is used to redirect the user to a different page automatically.

```
GET /MyPage.php?redir=/AnotherPage.php HTTP/1.1
```

An attacker might trick the GET parameter used to redirect the user to an external site

```
GET /MyPage.php?redir=https://www.malware.com HTTP/1.1
```

Fix recommendation

Avoid redirecting requests based on untrusted data if possible.

If relying on user input cannot be avoided, the URL should first be validated before redirection. Data that a user can modify must be treated as untrusted data.

A unique token, linked to the current user session, should be sent along with the redirect field value. This unique token should then be verified by the server before the actual redirect takes place. This ensures that attackers would have a harder time using the redirect field to propagate their malicious activities, since they cannot guess the user's session token.

Sanitize input by comparing to a predefined list of trusted URLs, based on an allow-list.

Force all redirects to first go through a page notifying users that they are about to leave your site, with the destination clearly displayed, and have them click a link to confirm.

CWE

601

External references

- Unvalidated Redirects and Forwards Cheat Sheet

Go to Table of Contents

H Open Redirect

Cause

The web application redirects users to an external site based on untrusted data.
In particular, the submitted request was found to include a URL as a parameter. The web application uses this value to redirect the user's browser to the specified URL.
An attacker can modify this URL value to an arbitrary address. The attacker would then cause the victim to submit the altered request, thus being redirected to a site of the attacker's choosing.

Risk

This vulnerability can allow an attacker to take advantage of the trust the user holds for the application, causing them to trust an arbitrary site under control of the attacker as well. This would often be leveraged through the use of phishing techniques.

Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

An attacker may successfully launch a phishing scam and steal user credentials or other sensitive information such as credit card number, social security number, and more.

It can also be possible to redirect the user to install malware that could infect the user's computer.

Exploit example

The following example shows a URL redirection to untrusted site.
The redir parameter is used to redirect the user to a different page automatically.

```
GET /MyPage.php?redir=/AnotherPage.php HTTP/1.1
```

An attacker might trick the GET parameter used to redirect the user to an external site

```
GET /MyPage.php?redir=https://www.malware.com HTTP/1.1
```

Fix recommendation

Avoid redirecting requests based on untrusted data if possible.

If relying on user input cannot be avoided, the URL should first be validated before redirection. Data that a user can modify must be treated as untrusted data.

A unique token, linked to the current user session, should be sent along with the redirect field value. This unique token should then be verified by the server before the actual redirect takes place. This ensures that attackers would have a harder time using the redirect field to propagate their malicious activities, since they cannot guess the user's session token.

Sanitize input by comparing to a predefined list of trusted URLs, based on an allow-list.

Force all redirects to first go through a page notifying users that they are about to leave your site, with the destination clearly displayed, and have them click a link to confirm.

CWE

601

External references

- Unvalidated Redirects and Forwards Cheat Sheet

Go to Table of Contents

H Reflected Cross Site Scripting - Insecure Use of Document.Write

Cause

Content being passed into the `document.write()` or the `document.writeln()` method could be carrying tainted data. Since this data is further used to display the HyperText Markup Language (HTML) inside a page, take steps to validate it.
The Document Object Model (DOM) as defined by the World Wide Web Consortium (W3C) provides two methods for controlling output being written to the document: `document.write()` and `document.writeln()`.
Content inputted to `document.write()` or the `document.writeln()` method should not be trusted without further validation. Using such content without validation can lead to a variety of Cross Site Scripting and HTML Injection attacks.

```
<script language="javascript">
…
  var inText = <%request.getParameter("text_type")%>;
```

```
  document.write("The text inputted is: " + inText);
...
</script>
```

Fix recommendation

In the cases where these methods carry input originating from an external location, further validation on the input is recommended.

Validation of such content when it is exposed to the user should be performed in the same manner as server-side input validation. Input validation should not be solely performed by client-side JavaScript components exposed to the user. Validation implemented in this manner can be bypassed by means of manipulating the browser and/or the submitted request. Use Server-Side validation or a combination of Client-Side and Server-Side validation.

Furthermore, any unnecessary content should not be passed to these methods.

<script language="javascript">… var inText = <%request.getEncodedParameter("text_type")%>; document.write("The text inputted is: " + inText);…</script>bad

External references

- document.writeln
- Cross-site Scripting (XSS)
- OWASP XSS Cheat Sheet

Go to Table of Contents

H Reflected Cross Site Scripting - Insecure Use of InnerHTML or OuterHTML

Cause

Content being passed into the `InnerHTML()` or `OuterHTML()` methods should be checked for tainted data. Since this data is further used to insert text, HyperText Markup Language (HTML), and/or script inside of a page, steps should be taken towards validating this data.
Content inputted to the `InnerHTML()` or `OuterHTML()` methods should not be trusted without further validation. Using such content without validation can lead to a variety of Cross Site Scripting and HTML Injection attacks.

```
<script language="javascript">
...
  var par = <%request.getParameter("param1")%>;
  document.getElementById('div1').innerHtml = par;
...
</script>
```

Fix recommendation

It is recommended that all `InnerHTML()` or `OuterHTML()` methods be replaced with `InnerText()` or `OuterText()` methods. These methods simply write the data as plain text to the browser without rendering HTML or script.

If the `InnerHTML()` or `OuterHTML()` methods are necessary, further validation on the input is recommended.

Validation of such content when it is exposed to the user should be performed in the same manner as server-side input validation. Input validation should not be solely performed by client-side JavaScript components exposed to the user. Validation implemented in this manner can be bypassed by means of manipulating the browser and/or the submitted request. Use Server-Side validation or a

combination of Client-Side and Server-Side validation.

Furthermore, any unnecessary content should not be passed to these methods.

<script language="javascript">... var par = <%request.getEncodedParameter("param1")%>; document.getElementById('div1').innerText = par;...</script>bad

Additionally, you can add JavaScript that performs whitelist validation on the input data:

<script language="javascript">... var par = document.URL; if (inText.match(/^[a-zA-Z0-9]$/)) // Only allow alpha-numeric data { document.getElementById('div1').innerText = par; }...</script>bad

External references

- element.innerHTML
- Cross-site Scripting (XSS)
- OWASP XSS Cheat Sheet

Go to Table of Contents

H SQL Injection

Cause

Sanitization of hazardous characters was not performed correctly on user input.
Dynamically generating queries that include unvalidated user input can lead to SQL injection attacks. An attacker can insert SQL commands or modifiers in the user input that can cause the query to behave in an unsafe manner.
Without sufficient validation and encapsulation of user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
SQL payloads can enter the system through any untrusted data, including user input, data previously stored in the database, files, 3rd party APIs, and more.

Risk

Potential consequences include the loss of:

Confidentiality - Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.

Authentication - If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.

Authorization - If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability.

Integrity - Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.

Fix recommendation

Use stored procedures with parameters to prevent injection of SQL commands in data, or at least parameterized database calls that do not allow the injection of code. Do not include any dynamic SQL execution in the stored procedures.

An even better solution is to use an ORM (object-relational mapping) framework such as Hibernate or EntityFramework, if you have one available on your platform.

Ensure that all user input is validated and filtered on the server side, not just to disallow bad characters such as a single quote (') and double quotes ("), but rather to only allow safe characters. Narrowly define the set of safe characters based on the expected value of the parameter in the request.

Use escaping functions on all user input.

Configure the application identity for the least database privileges that are required to accomplish the necessary tasks. Harden the database server to disable any unneeded functionality, such as shell commands.

CWE

89

External references

- OWASP - SQL Injection Prevention Cheat Sheet

Go to Table of Contents

H Validation Required

Cause

Input validation is necessary to ensure the integrity of the dynamic data of the application. Validation is useful to protect against cross-site scripting, SQL and command injection, and corrupt application data fields. Even if there are no directly vulnerable uses of a piece of data inside one application, data that is being passed to other applications should be validated to ensure that those applications are not given bad data. Validation, especially for size and metacharacters that might cause string expansion, is even more important when dealing with fixed size, overflowable buffers.
You should validate input from untrusted sources before using it. The untrusted data sources can be HTTP requests or other network traffic, file systems, databases, and any external systems that provide data to the application. In the case of HTTP requests, validate all parts of the request, including headers, form fields, cookies, and URL components that transfer information from the browser to the server side application.
Attackers use unvalidated parameters to target the application's security mechanisms such as authentication and authorization or business logic, and as the primary vector for exercising many other kinds of error, including buffer overflows. If the unvalidated parameters are stored in log files, used in dynamically generated database queries or shell commands, and/or stored in database tables, attackers may also target the server operating system, a database, back-end processing systems, or even log viewing tools.
For example, if the application looks up products from the database using an unvalidated productID from HTTP request. This productID can be manipulated using readily available tools to submit SQL injection attacks to the backend database.

```
final String productID = request.getParameter( "productID" );
final String sql = "Select * from Product Where productID = '" + productID + "'";
final Statement statement = connection.createStatement();
final boolean rsReturned = statement.execute(sql);
```

```
char productID[28];
fscanf(fd, "%28s", productID);
char sql[71] = "Select * from Product Where productID = '";
strncat(sql, productID, 28);
strncat(sql, "'", 1);
SQLPrepare(handle, sql, 71);
SQLRETURN ret = SQLExecute(handle);
```

Note that using dynamically generated SQL queries is another bad practice. Refer to vulnerability type SQL Injection for more detail.

```
// This class would simply associate parameter names with a data type, plus bounds for
```

```
// numeric data or a regular expression for text.
Validator validator = Validator.getInstance( this.getServletContext );
Boolean valid = false;
try
{
    validator.validate( request );
    valid = true;
}
catch ( ValidationException e )
{
    request.getSession().invalidate();
    out.println("Invalid HTTP request");
    out.close();
}
if ( valid )
{
    final String productId = request.getParameter( "productID" );
    final String sql = "Select * from Product where productID= ?");
    final PreparedStatement ps = con.prepareStatement(sql);
    ps.setString(1,productID);
    ps.execute();
}
```

```
char productID[28];
fscanf(fd, "%.28s", productID);
regex_t * productIDValidator;
regcomp(productIDValidator, "[^a-z]*", REG_EXTENDED);
int matchCount;
regmatch_t * matches;
regexec(productIDValidator, productID, matches, matchCount, 0);
if(0 == matches)
{
    char sql[70] = "Select * from Product Where productID = '?'";
    int sqlLen = 70;
    SQLPrepare(handle, sql, 70);
    SQLBindParameter(handle, 1, SQL_PARAM_INPUT, SQL_C_CHAR, SQL_CHAR, 28, 0, productID, *sqlLen)
    SQLRETURN ret = SQLExecute(handle);
}
else
{
    HandleBadProductID();
}
```

In this instance, a regular expression constrained input to a known set of characters, through a whitelist (rejecting inputs containing anything not in that set), and of a known and limited length. Using a whitelist instead of a blacklist is important, because it can be difficult to anticipate which characters (especially when Unicode is involved) may cause problems, while it is normally easy to determine which characters are legal in a given input field.

Fix recommendation

The primary recommendation is to validate each input value against a detailed specification of the expectation for that value. This specification should detail characteristics like the character set allowed, length, whether to allow null, minimum value, maximum value, enumerated values, or a specific regular expression. For example, make sure all email fields have the same format. Also, limit name fields and other text fields to an appropriate character set, no special characters, and with expected minimum and maximum sizes. A input pattern violation can be evidence of an attack and should be logged and responded to appropriately.

There are several possible approaches to input validation in an application. The recommendation is to implement the features in a single component that is invoked in a central location. If this is not possible, then enforce a strong policy for the use of a common set of input validation functions.