AppScan Source Findings Report

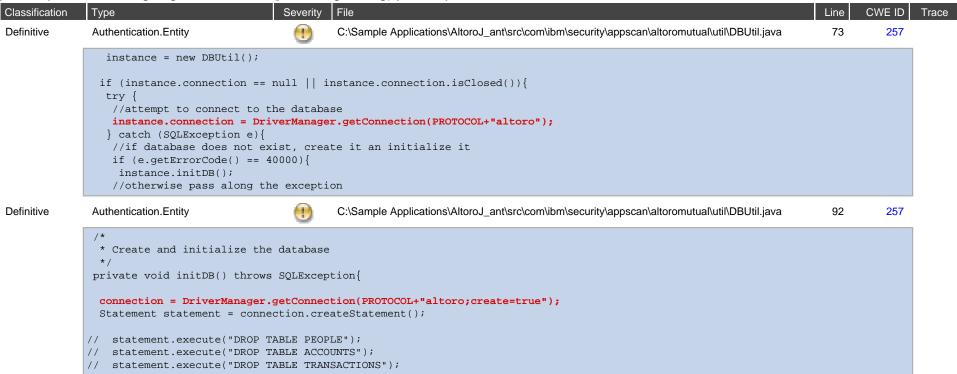


AltoroJ Ant - Findings By Fix Group Report

Scan Date: Jul 21, 2021 12:44:55 AM Report Generated: Jul 21, 2021 12:49:10 AM

Common API Call: Authentication.Entity

java.sql.DriverManager.getConnection(java.lang.String):java.sql.Connection



Common API Call: CrossSiteScripting

javax.servlet.jsp.JspWriter.print(java.lang.Object):void



```
<div style="font-weight: bold; font-size: 12px; color: red;" id="message"><</pre>
%=(request.getAttribute("message subscribe"
!=null)?request.getAttribute("message_subscribe"):"" %></div>
       >
         Email:
CrossSiteScripting
                                 C:\Sample Applications\AltoroJ_ant\WebContent\bank\transfer.jsp
                                                                                                   82
    
   <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><span style='color: Red'><</pre>
%=(request.getAttribute("message")==n
11)?"":request.getAttribute("message") %></span></span>
     <span id="soapResp" name="soapResp" align="center" />
```

javax.servlet.jsp.JspWriter.print(java.lang.String):void

Definitive



```
Definitive
                                                                                                                                   15
             CrossSiteScripting
                                                    C:\Sample Applications\AltoroJ_ant\WebContent\bank\customize.jsp
               <h1>Customize Site Language</h1>
               <form method="post">
                Curent Language: <%=(request.getParameter("lang")==null)?"":request.getParameter("lang")%>
                >
                You can change the language setting by choosing:
Definitive
             CrossSiteScripting
                                                    C:\Sample Applications\AltoroJ ant\WebContent\feedbacksuccess.isp
                                                                                                                                  20
               <div class="fl" style="width: 99%;">
               <h1>Thank You</h1>
               Thank you for your comments<%= (request.getAttribute("message feedback")!=null)?",</p>
             "+request.getAttribute("message_feedback
             ):"" %>. They will be reviewed by our Customer Service staff and given the full attention that they deserve.
               <% String email = (String) request.getParameter("email addr");</pre>
                boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL REGEXP);
                if (email != null && email.trim().length() != 0 && regExMatch) {%>
                Our reply will be sent to your email: <%= ServletUtil.sanitizeBasic(email.toLowerCase()) /*email.toLowerCase()*/ %>
               <% } else {%>
Definitive
             CrossSiteScripting
                                                    C:\Sample Applications\AltoroJ_ant\WebContent\feedbacksuccess.jsp
                                                                                                                                  24
               Thank you for your comments<%= (request.getAttribute("message_feedback")!=null)?",</p>
              "+request.getAttribute("message feedback
            ):"" %>. They will be reviewed by our Customer Service staff and given the full attention that they deserve.
               <% String email = (String) request.getParameter("email_addr");</pre>
                boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL_REGEXP);
                if (email != null && email.trim().length() != 0 && regExMatch) {%>
                Our reply will be sent to your email: <%= ServletUtil.sanitizeBasic(email.toLowerCase()) /*email.toLowerCase()*/ %>
              <% } else {%>
               However, the email you gave is incorrect (<%=email.toLowerCase() /*ServletUtil.sanitizeWeb(email.toLowerCase())*/%>) and you
            ll not receive a response.
              <% }%>
               CrossSiteScripting
                                                    C:\Sample Applications\AltoroJ ant\WebContent\feedbacksuccess.isp
Definitive
                <% String email = (String) request.getParameter("email_addr");</pre>
                boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL_REGEXP);
                if (email != null && email.trim().length() != 0 && regExMatch) {%>
```

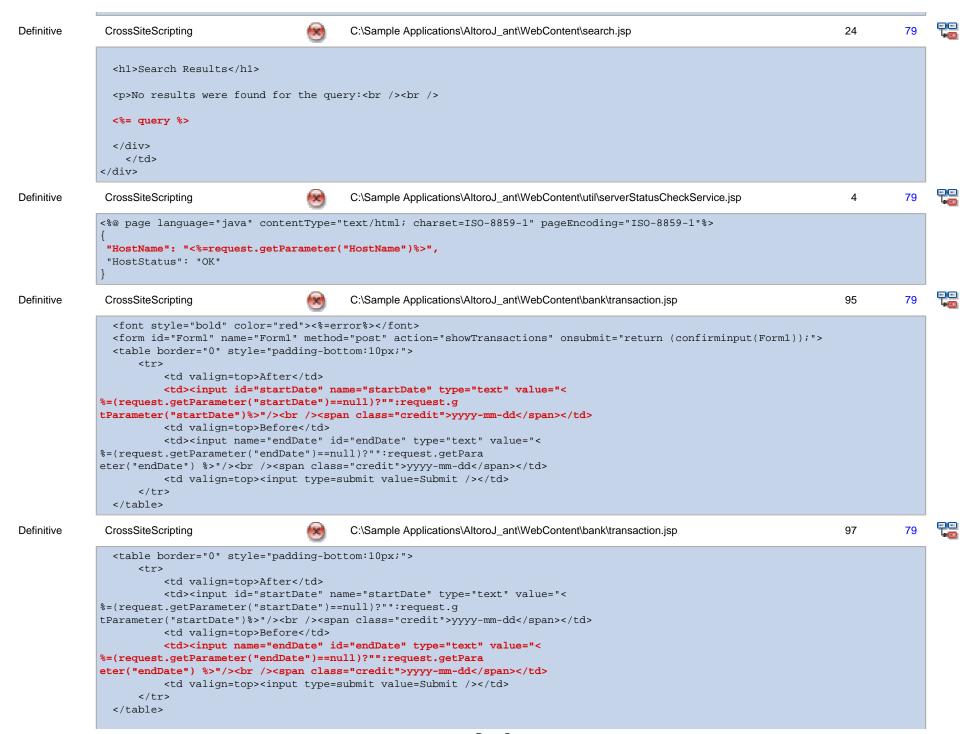
```
Our reply will be sent to your email: <%= ServletUtil.sanitizeBasic(email.toLowerCase()) /*email.toLowerCase()*/ %>
  <% } else {%>
  However, the email you gave is incorrect (<%=email.toLowerCase()) /*ServletUtil.sanitizeWeb(email.toLowerCase())*/%>) and you
11 not receive a response.
 <% }%>
  </div>
CrossSiteScripting
                                        C:\Sample Applications\AltoroJ ant\WebContent\admin\login.jsp
                                                                                                                       20
    >
  <!-- add captcha input here -->
      <strong>Enter the administrative password:</strong><br />
      <input id="password" name="password" type=password runat="server" /><br />
      <input type="submit" name="btnSubmit" value="Login">
    <span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
   java.lang.String error = (String)request.getAttribute("loginError");
  if (error != null && error.trim().length() > 0){
CrossSiteScripting
                                        C:\Sample Applications\AltoroJ_ant\WebContent\admin\login.jsp
                                                                                                                       27
   <%
   java.lang.String error = (String)request.getAttribute("loginError");
   if (error != null && error.trim().length() > 0){
   request.getSession().removeAttribute("loginError");
   out.print(error);
  응>
  </span>
  </form>
CrossSiteScripting
                                        C:\Sample Applications\AltoroJ_ant\WebContent\bank\queryxpath.jsp
                                                                                                                       16
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="<%=request.getRequestURL()%>">
    Search our news articles database
    <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="<%=(request.getParameter("query")==null)?"Enter title (e.g.</pre>
 Watch
ire)":request.getParameter("query")%>"/>
    <input type="submit" width=75 id="Button1" value="Query">
    <br /><br />
   <%
   if (request.getParameter("query") != null) {
    String[] results = ServletUtil.searchArticles(request.getParameter("query"),
 request.getSession().getServletContext().getReal
ath("/pr/Docs.xml"));
```

Definitive

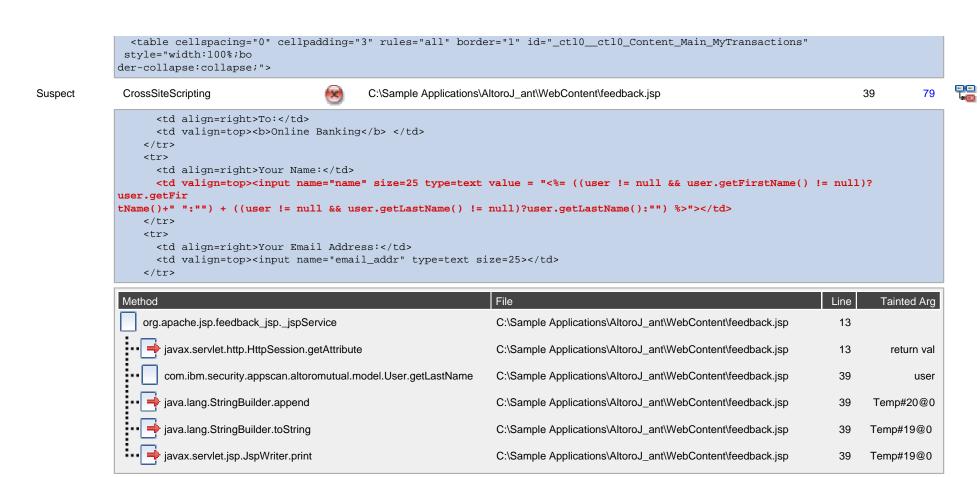
Definitive

Definitive

Page 4

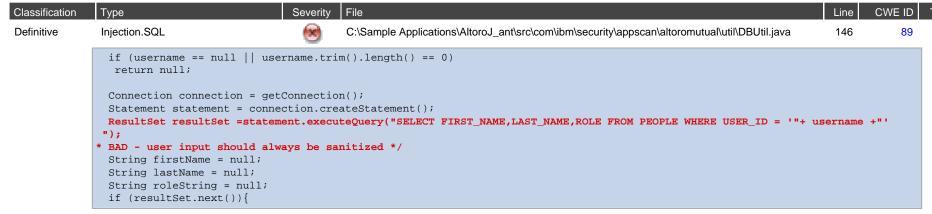


Page 5



Common API Call: Injection.SQL

java.sql.Statement.executeQuery(java.lang.String):java.sql.ResultSet



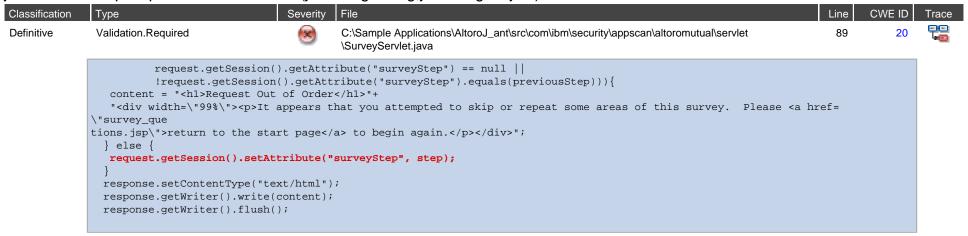
Common API Call: Validation. Encoding Required

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



javax.servlet.ServletRequest.setAttribute(java.lang.String;java.lang.Object):void

Classification	Туре	Severity	File	Line	CWE ID	Trace
Definitive	Validation.Required		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet \FeedbackServlet.java	40	20	
	<pre>return; } String name = request.getParameter("name"); if (name != null){</pre>					

```
request.setAttribute("message_feedback", name);
} else {
    request.removeAttribute("name");
}
RequestDispatcher dispatcher = request.getRequestDispatcher("/feedbacksuccess.jsp");

Definitive

Validation.Required

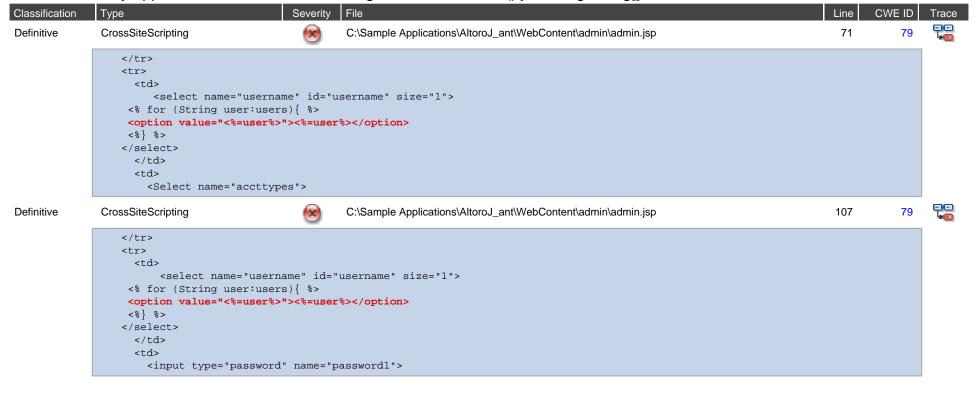
C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet
    \text{SubscribeServlet.java}

response.sendRedirect("index.jsp");
    return;
}

//don't actually subscribe the user
    request.setAttribute("message_subscribe", "Thank you. Your email " + email + " has been accepted.");
    RequestDispatcher dispatcher = request.getRequestDispatcher("subscribe.jsp");
    dispatcher.forward(request, response);
}
```

Common Fix Point: CrossSiteScripting

com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUsernames():java.lang.String[]



```
<select name="username" id="username" size="1">
<% for (String user:users){ %>
<option value="<%=user%>"><%=user%></option>
<%} %>
</select>
 <Select name="accttypes">
```

Method	File	Line	Tainted Arg
org.apache.jsp.admin.admin_jspjspService	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	12	
com.ibm.security.appscan.altoromutual.util.ServletUtil.getBankUsers	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	12	return val
com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUser names	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\ServletUtil.java	143	return val
java.sql.ResultSet.getString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	340	return val
java.util.ArrayList.add	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	341	name
java.util.ArrayList.toArray	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	344	users
javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	71	user

Suspect

Suspect

CrossSiteScripting



C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp

107

79

```
>
     <select name="username" id="username" size="1">
<% for (String user:users){ %>
<option value="<%=user%>"><%=user%></option>
<%} %>
</select>
 <input type="password" name="password1">
```

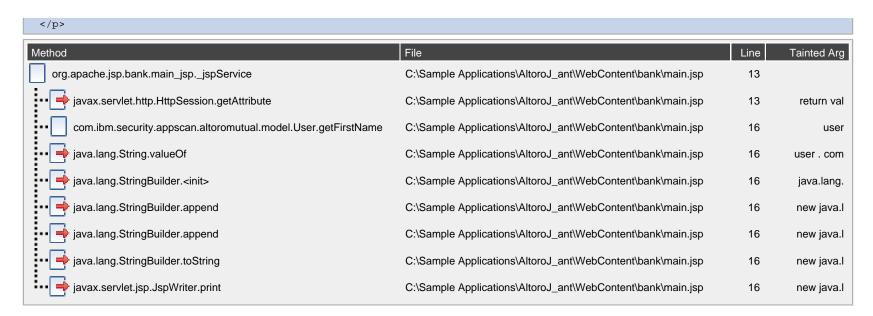
Method		File	Line	Tainted Arg
org.apac	ne.jsp.admin.admin_jspjspService	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	12	
com	ibm. security. apps can. alto romutual. util. Servlet Util. get Bank Users	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	12	return val
	com.ibm.security.appscan.altoromutual.util.DBUtil.getBankUser names	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\ServletUtil.java	143	return val
[➡ java.sql.ResultSet.getString	$\label{lem:combined} C:\Sample\ Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java$	340	return val

java.util.ArrayList.add java.util.ArrayList.toArray	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	341 344	name
javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	107	user

javax.servlet.jsp.JspWriter.print(java.lang.String):void

ssification		Severity	File		Line	
ect	CrossSiteScripting	×	C:\Sample Applications\A	AltoroJ_ant\WebContent\bank\main.jsp	16	5 79
	<pre>(com.ibm.security.apps).getAttribute("user");</pre>	can.altoromutua		t.getSession		
	welcome to Altoro M	utual Online.				
	Method			File	Line	Tainted Arg
	org.apache.jsp.bank.main	_jspjspService		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	
	javax.servlet.http.Http	Session.getAttribute		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	return val
	com.ibm.security.app	scan.altoromutual.m	odel.User.getLastName	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user
	java.lang.StringBuilde	er.append		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user . com
	java.lang.StringBuilde	er.toString		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
	javax.servlet.jsp.JspV	Vriter.print		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
ect	CrossSiteScripting	<u>®</u>	C:\Sample Applications\A	AltoroJ_ant\WebContent\bank\main.jsp	16	5 79
	<pre></pre>	can.altoromutua		t.getSession		
	Welcome to Altoro M	utual Online				

Page 10

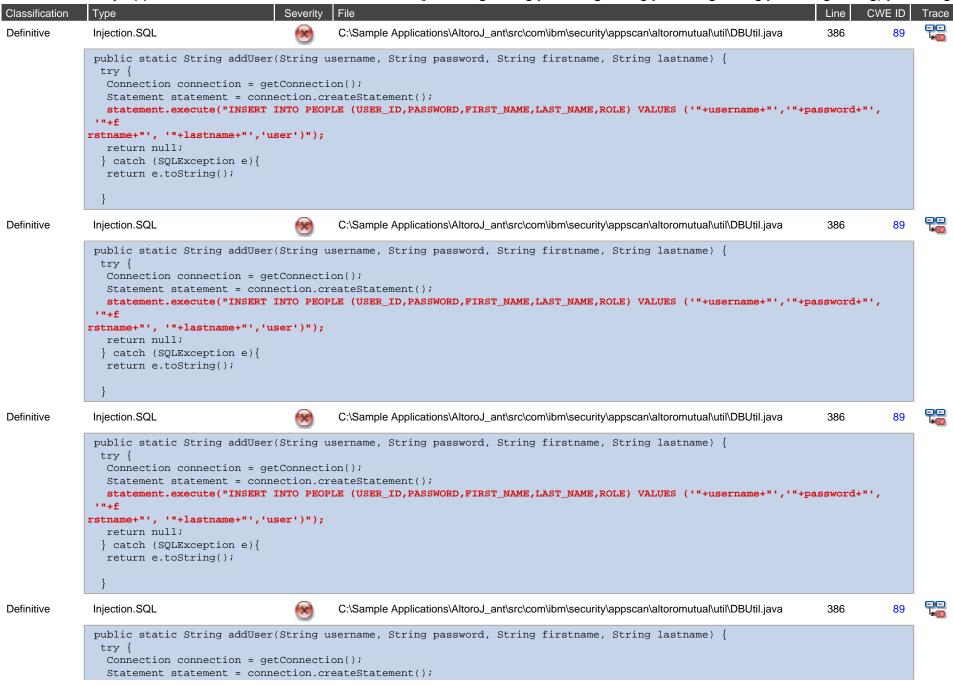


Common Fix Point: Injection.SQL

com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount(java.lang.String;java.lang.String):java.lang.String

Classification	Туре	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL	×	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	375	89	ue ue
	<pre>public static String addAccount(String username, String acctType) { try { Connection connection = getConnection(); Statement statement = connection.createStatement(); statement.execute("INSERT INTO ACCOUNTS (USERID, ACCOUNT_NAME, BALANCE) VALUES ('"+username+"','"+acctType+"', 0)"); return null; } catch (SQLException e) { return e.toString(); } </pre>					
Definitive	Injection.SQL	×	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	375	89	
<pre>public static String addAccount(String username, String acctType) { try { Connection connection = getConnection(); Statement statement = connection.createStatement(); statement.execute("INSERT INTO ACCOUNTS (USERID, ACCOUNT_NAME, BALANCE) VALUES ('"+username+"','"+acctType+"', 0)' return null; } catch (SQLException e) { return e.toString(); } </pre>						

com.ibm.security.appscan.altoromutual.util.DBUtil.addUser(java.lang.String;java.lang.String;java.lang.String;java.lang.String;java.lang.String;java.lang.String



com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword(java.lang.String;java.lang.String):java.lang.String



com.ibm.security.appscan.altoromutual.util.DBUtil.getAccounts(java.lang.String):com.ibm.security.appscan.altoromutual.model.Account[]

Classification	Туре	Severity	File	Line	CWE ID	Ţ
Definitive	Injection.SQL	×	$C: \label{lem:combined} C: \label{lem:combined} C: \label{lem:combined} Applications \label{lem:combined} $	180	89	(
	if (username == null use	rname.tri	m().length() == 0)			
	return null;					
	Connection connection = get					
	Statement statement = connection.createStatement();					
	ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+					
	username					
	+"' "); /* BAD - user input s					
	ArravList <account> accounts = new ArravList<account>(3);</account></account>					1

```
while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                       C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
                                                                                                                                        180
               if (username == null || username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
               ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+
              username
              +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                       C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
                                                                                                                                        180
               if (username == null | username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
               ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+
              username
              +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                       C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
                                                                                                                                        180
               if (username == null || username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
               ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+
              username
              +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                                                                                                        180
                                                       C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
               if (username == null || username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
```

Page 14

```
ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = ""+
              username
             +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
               long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                      C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
                                                                                                                                      180
               if (username == null || username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
               ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+
             +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
Definitive
              Injection.SQL
                                                      C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java
               if (username == null || username.trim().length() == 0)
                return null;
               Connection connection = getConnection();
               Statement statement = connection.createStatement();
               ResultSet resultSet =statement.executeQuery("SELECT ACCOUNT_ID, ACCOUNT_NAME, BALANCE FROM ACCOUNTS WHERE USERID = '"+
              +"' "); /* BAD - user input should always be sanitized */
               ArrayList<Account> accounts = new ArrayList<Account>(3);
               while (resultSet.next()){
                long accountId = resultSet.getLong("ACCOUNT_ID");
                String name = resultSet.getString("ACCOUNT_NAME");
```

com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(java.lang.String;java.lang.String;com.ibm.security.appscan.altoromutual.mo

Classification	Туре	Severity	File	Line	CWE ID	Tra
Definitive	Injection.SQL	×	$C: \label{lem:combined} C: \label{lem:combined} C: \label{lem:combined} Applications \label{lem:combined} $	307	89	T _e
	String query = "SELECT * FROM TRANSACTIONS WHERE (" + acctids.toString() + ") " + ((dateString==null)?"": "AND dateString + ") ") + "ORDER BY DATE DESC"; ResultSet resultSet = null;					
	<pre>try { resultSet = statement.exe } catch (SQLException e) { int errorCode = e.getError if (errorCode == 30000) throw new SQLException("</pre>	rCode();	query must be in the format of yyyy-mm-dd HH:mm:ss");			

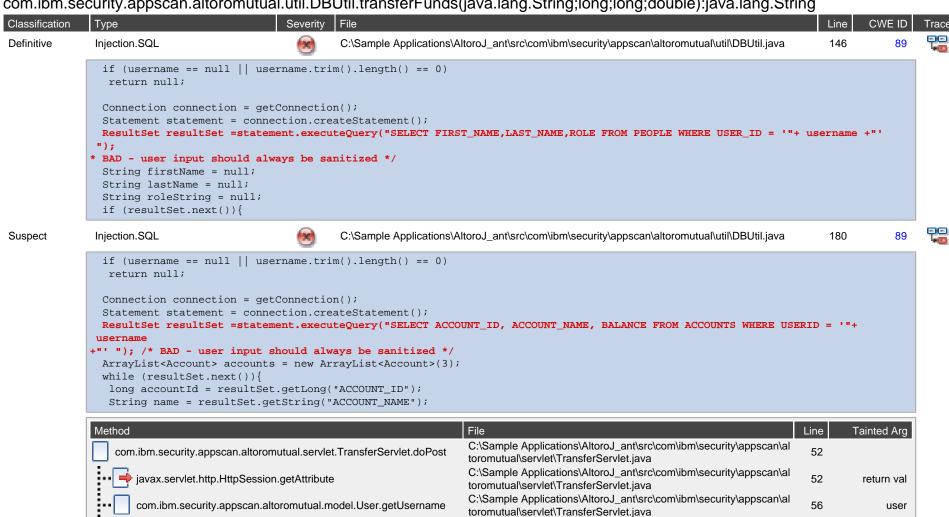
Definitive Injection.SQL C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java 307 String query = "SELECT * FROM TRANSACTIONS WHERE (" + acctids.toString() + ") " + ((dateString==null)?"": "AND (" + dateString + ") ") + "ORDER BY DATE DESC" ; ResultSet resultSet = null; try { resultSet = statement.executeQuery(query); } catch (SQLException e){ int errorCode = e.getErrorCode(); if (errorCode == 30000) throw new SQLException("Date-time query must be in the format of yyyy-mm-dd HH:mm:ss"); Definitive Injection.SQL C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java 307 String query = "SELECT * FROM TRANSACTIONS WHERE (" + acctlds.toString() + ") " + ((dateString==null)?"": "AND (" + dateString + ") ") + "ORDER BY DATE DESC" ; ResultSet resultSet = null; try { resultSet = statement.executeQuery(query); } catch (SQLException e){ int errorCode = e.getErrorCode(); if (errorCode == 30000) throw new SQLException("Date-time query must be in the format of yyyy-mm-dd HH:mm:ss");

com.ibm.security.appscan.altoromutual.util.DBUtil.isValidUser(java.lang.String;java.lang.String):boolean

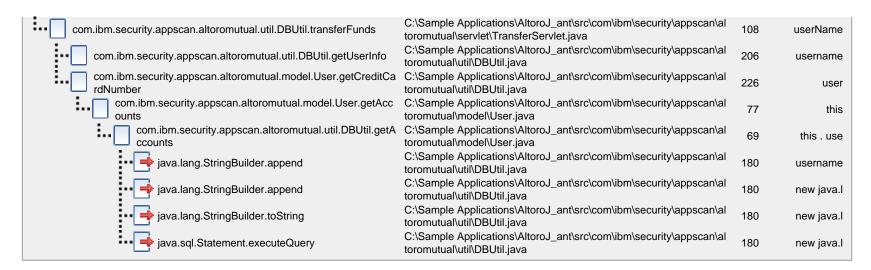


```
return false;
 Connection connection = getConnection();
 Statement statement = connection.createStatement();
 ResultSet resultSet = statement.executeQuery("SELECT COUNT(*)FROM PEOPLE WHERE USER ID = '"+ user +"' AND PASSWORD='" +
password
+ "'"); /* BAD - user input should always be sanitized */
 if (resultSet.next()){
   if (resultSet.getInt(1) > 0)
    return true;
```

com.ibm.security.appscan.altoromutual.util.DBUtil.transferFunds(java.lang.String;long;long;double):java.lang.String



Page 17



Common Fix Point: Validation.Required

javax.servlet.http.HttpSession.setAttribute(java.lang.String;java.lang.Object):void

	ax.servi	et.nttp.mttpsession.setAt	unbutetjava.iang.Sunig,java.i	iang.Object).void		
if (message != null) message = "Error: " + message; else message = "Requested operation has completed successfully."; request.getSession().setAttribute("message", message); response.sendRedirect("admin.jsp"); return; } Method com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword i	assification	Туре	Severity File		Line	CWE ID
message = "Error: " + message; else message = "Requested operation has completed successfully."; request.getSession().setAttribute("message", message); response.sendRedirect("admin.jsp"); return; } Method com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost	spect	Validation.Required		AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet	109	20
Method Com.ibm.security.appscan.altoromutual.servlet.doPost com.ibm.security.appscan.altoromutual.servlet.doPost com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword c:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet.java		<pre>message = "Error: " + m else message = "Requested op request.getSession().set response.sendRedirect("a</pre>	peration has completed successfu	lly.";		
toromutual/servlet/AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java		}		File	Line	Tainted Arg
toromutual\servlet\AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java		com.ibm.security.appscan.alto	oromutual.servlet.AdminServlet.doPost	=	94	
toromutual\util\DBUtil.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al 105 message		com.ibm.security.appscar	n.altoromutual.util.DBUtil.changePassword	1 ''' =	94	return val
toromutual\servlet\AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java 105 message C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al 105 new java.I		java.lang.Throwable.	toString		401	return val
toromutual\servlet\AdminServlet.java C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al message		java.lang.StringBuilder.ap	ppend	=	105	message
••• allow convict bits Hits Accion cot Δitribitie in the condition of the condition		java.lang.StringBuilder.to	String	=	105	new java.l
		javax.servlet.http.HttpSes	ssion.setAttribute	=	109	message

20



```
if (message != null)
  message = "Error: " + message;
else
  message = "Requested operation has completed successfully.";

request.getSession().setAttribute("message", message);
  response.sendRedirect("admin.jsp");
  return;
}
```

Method	File	Line	Tainted Arg
com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	40	
com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	40	return val
java.lang.Throwable.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	378	return val
java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	105	message
java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	105	new java.l
javax.servlet.http.HttpSession.setAttribute	$\label{lem:combined} C:\Sample\ Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java$	109	message

Suspect

Validation.Required



109

T.

```
if (message != null)
  message = "Error: " + message;
else
  message = "Requested operation has completed successfully.";

request.getSession().setAttribute("message", message);
response.sendRedirect("admin.jsp");
return;
}
```

Method	File	Line	Tainted Arg
com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	71	
com.ibm.security.appscan.altoromutual.util.DBUtil.addUser	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	71	return val
java.lang.Throwable.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	389	return val
java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	105	message
java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\AdminServlet.java	105	new java.l

Common Fix Point: Validation.Required.URL.Redirect

java.lang.StringBuilder.append(java.lang.String):java.lang.StringBuilder

