



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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Authentication.Entity		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	73	257	
<pre>instance = new DBUtil(); if (instance.connection == null instance.connection.isClosed()){ try { //attempt to connect to the database instance.connection = DriverManager.getConnection(PROTOCOL+"altoro"); } catch (SQLException e){ //if database does not exist, create it and initialize it if (e.getErrorCode() == 40000){ instance.initDB(); } //otherwise pass along the exception } }</pre>						
Definitive	Authentication.Entity		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	92	257	
<pre>/* * Create and initialize the database */ private void initDB() throws SQLException{ connection = DriverManager.getConnection(PROTOCOL+"altoro;create=true"); Statement statement = connection.createStatement(); // statement.execute("DROP TABLE PEOPLE"); // statement.execute("DROP TABLE ACCOUNTS"); // statement.execute("DROP TABLE TRANSACTIONS"); }</pre>						

Common API Call: CrossSiteScripting

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\subscribe.jsp	20	79	
<pre><form action="doSubscribe" method="post" name="subscribe" id="subscribe" onsubmit="return confirmEmail(txtEmail.value);"> <table></pre>						

```

        <tr>
        <td colspan="2">
            <div style="font-weight: bold; font-size: 12px; color: red;" id="message"><
            %=(request.getAttribute("message_subscribe"
            !=null)?request.getAttribute("message_subscribe")):"" %></div>
        </td>
        </tr>
        <tr>
        <td>
            Email:

```

Definitive

CrossSiteScripting



C:\Sample Applications\AltoroJ_ant\WebContent\bank\transfer.jsp

82

79



```

        <tr>
        <td colspan="2">&nbsp;</td>
        </tr>
        <tr>
        <td colspan="2" align="center">
            <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><span style='color: Red'><
            %=(request.getAttribute("message")==n
            ll)?":request.getAttribute("message") %></span></span>
            <span id="soapResp" name="soapResp" align="center" />
        </td>
        </tr>
        </table>
        </form>

```

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

Classification	Type	Severity	File	Line	CWE ID	Trace
----------------	------	----------	------	------	--------	-------

Definitive

CrossSiteScripting



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

42

79



```

<p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">
<%
java.lang.String error = (String)request.getSession().getAttribute("message");

if (error != null && error.trim().length() > 0){
    out.print(error);
}
%>
</span></p>

<h1>Edit User Information</h1>

```

Definitive

CrossSiteScripting



C:\Sample Applications\AltoroJ_ant\WebContent\bank\balance.jsp

37

79



```

%>



<!-- To modify account information do not connect to SQL source directly. Make all changes
through the admin page. -->

<h1>Account History - <%=accountName%></h1>

<table width="590" border="0">
<tr>

```



```
<td colspan=2>
  <table cellSpacing="0" cellPadding="1" width="100%" border="1">
```

Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\bank\customize.jsp	15	79	
------------	--------------------	---	--	----	----	---

```
<h1>Customize Site Language</h1>

<form method="post">
  <p>
    Current Language: <%= (request.getParameter("lang")==null)? "": request.getParameter("lang") %>
  </p>

  <p>
    You can change the language setting by choosing:
  </p>
```

Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\feedbacksuccess.jsp	20	79	
------------	--------------------	---	---	----	----	---

```
<div class="fl" style="width: 99%;">

  <h1>Thank You</h1>

  <p>Thank you for your comments<%= (request.getAttribute("message_feedback")!=null)?",
  "+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");
  boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL_REGEX);
  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	79	
------------	--------------------	---	---	----	----	---

```
  <p>Thank you for your comments<%= (request.getAttribute("message_feedback")!=null)?",
  "+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");
  boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL_REGEX);
  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
    will not receive a response.
  <% } %>

</p>
```

Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\feedbacksuccess.jsp	26	79	
------------	--------------------	---	---	----	----	---

```
<% String email = (String) request.getParameter("email_addr");
boolean regExMatch = email!=null && email.matches(ServletUtil.EMAIL_REGEX);
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
w
ll not receive a response.
    <% }%>

</p>

</div>

```

Definitive CrossSiteScripting  C:\Sample Applications\AltoroJ_ant\WebContent\admin\login.jsp 20 79 

```

<p>
<!-- add captcha input here -->
    <strong>Enter the administrative password:</strong><br />
    <input id="password" name="password" type=password runat="server" /><br /><br />
    <input type="submit" name="btnSubmit" value="Login">
</p>
<p><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){

```

Definitive CrossSiteScripting  C:\Sample Applications\AltoroJ_ant\WebContent\admin\login.jsp 27 79 

```

<%
    java.lang.String error = (String)request.getAttribute("loginError");

    if (error != null && error.trim().length() > 0){
        request.getSession().removeAttribute("loginError");
        out.print(error);
    }
    %>
</span></p>
</form>



```







Definitive CrossSiteScripting  C:\Sample Applications\AltoroJ_ant\WebContent\bank\queryxpath.jsp 16 79 

```

<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.
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	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\search.jsp	24	79	
<pre> <h1>Search Results</h1> <p>No results were found for the query:

 <%= query %> </div> </td> </pre>						
Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\util\serverStatusCheckService.jsp	4	79	
<pre> <%@ page language="java" contentType="text/html; charset=ISO-8859-1" pageEncoding="ISO-8859-1"%> { "HostName": "<%=request.getParameter("HostName")%>", "HostStatus": "OK" } </pre>						
Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\bank\transaction.jsp	95	79	
<pre> <%=error%> <form id="Form1" name="Form1" method="post" action="showTransactions" onsubmit="return (confirminput(Form1));"> <table border="0" style="padding-bottom:10px;"> <tr> <td valign=top>After</td> <td><input id="startDate" name="startDate" type="text" value="< %=(request.getParameter("startDate")==null)?"":request.g tParameter("startDate")%>" />
yyyy-mm-dd</td> <td valign=top>Before</td> <td><input name="endDate" id="endDate" type="text" value="< %=(request.getParameter("endDate")==null)?"":request.getPara eter("endDate") %>" />
yyyy-mm-dd</td> <td valign=top><input type="submit" value="Submit" /></td> </tr> </table> </pre>						
Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\bank\transaction.jsp	97	79	
<pre> <table border="0" style="padding-bottom:10px;"> <tr> <td valign=top>After</td> <td><input id="startDate" name="startDate" type="text" value="< %=(request.getParameter("startDate")==null)?"":request.g tParameter("startDate")%>" />
yyyy-mm-dd</td> <td valign=top>Before</td> <td><input name="endDate" id="endDate" type="text" value="< %=(request.getParameter("endDate")==null)?"":request.getPara eter("endDate") %>" />
yyyy-mm-dd</td> <td valign=top><input type="submit" value="Submit" /></td> </tr> </table> </pre>						

```
<table cellpadding="3" cellspacing="0" border="1" id="_ctl0__ctl0_Content_Main_MyTransactions" style="width:100%;border-collapse:collapse;">
```


Suspect CrossSiteScripting  C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp 39 79 

```
<td align=right>To:</td>
<td valign=top><b>Online Banking</b> </td>
</tr>
<tr>
<td align=right>Your Name:</td>
<td valign=top><input name="name" size=25 type=text value = "<%= ((user != null && user.getFirstName() != null)?
user.getFir
tName()+ " ":"") + ((user != null && user.getLastName() != null)?user.getLastName():"") %>"></td>
</tr>
<tr>
<td align=right>Your Email Address:</td>
<td valign=top><input name="email_addr" type=text size=25></td>
</tr>
```

Method	File	Line	Tainted Arg
 org.apache.jsp.feedback_jsp._jspService	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	13	
 javax.servlet.http.HttpSession.getAttribute	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	13	return val
 com.ibm.security.appscan.althoromutual.model.User.getLastName	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	39	user
 java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	39	Temp#20@0
 java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	39	Temp#19@0
 javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\feedback.jsp	39	Temp#19@0

Common API Call: Injection.SQL

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



Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\althoromutual\util\DBUtil.java	146	89	

```
if (username == null || username.trim().length() == 0)
return null;

Connection connection = getConnection();
Statement statement = connection.createStatement();
ResultSet resultSet =statement.executeQuery("SELECT FIRST_NAME, LAST_NAME, ROLE FROM PEOPLE WHERE USER_ID = '"+ username + "'");
* BAD - user input should always be sanitized */
String firstName = null;
String lastName = null;
String roleString = null;
if (resultSet.next()){
```

Common API Call: Validation.EncodingRequired



java.io.PrintWriter.write(java.lang.String):void

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Validation.EncodingRequired		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\SurveyServlet.java	92	116	

```
"<div width=\"99%\"><p>It appears that you attempted to skip or repeat some areas of this survey. Please <a href=
\"survey_que
tions.jsp\">return to the start page</a> to begin again.</p></div>";
} else {
    request.getSession().setAttribute("surveyStep", step);
}
response.setContentType("text/html");
response.getWriter().write(content);
response.getWriter().flush();
}
}
```



Common API Call: Validation.Required

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Validation.Required		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\servlet\SurveyServlet.java	89	20	

```
request.getSession().getAttribute("surveyStep") == null ||
!request.getSession().getAttribute("surveyStep").equals(previousStep)){
    content = "<h1>Request Out of Order</h1>"+
    "<div width=\"99%\"><p>It appears that you attempted to skip or repeat some areas of this survey. Please <a href=
\"survey_que
tions.jsp\">return to the start page</a> to begin again.</p></div>";
} else {
    request.getSession().setAttribute("surveyStep", step);
}
response.setContentType("text/html");
response.getWriter().write(content);
response.getWriter().flush();
```

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

Classification	Type	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	

```
return;
}
String name = request.getParameter("name");
if (name != null){
```

```

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
\SubscribeServlet.java

41

20



```

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[]

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	71	79	

```

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

```

Definitive

CrossSiteScripting



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

107

79










```

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

```











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

Method	File	Line	Tainted Arg
 org.apache.jsp.admin.admin_jsp._jspService	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\al toromutual\util\ServletUtil.java	143	return val
└─  java.sql.ResultSet.getString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	340	return val
└─  java.util.ArrayList.add	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	341	name
└─  java.util.ArrayList.toArray	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	344	users
└─  javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\admin\admin.jsp	71	user





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

Method	File	Line	Tainted Arg
 org.apache.jsp.admin.admin_jsp._jspService	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\al toromutual\util\ServletUtil.java	143	return val
└─  java.sql.ResultSet.getString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	340	return val

	java.util.ArrayList.add	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	341	name
	java.util.ArrayList.toArray	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	344	users
	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


Classification	Type	Severity	File	Line	CWE ID	Trace
Suspect	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	79	

```
<%
    com.ibm.security.appscan.althoromutual.model.User user =
    (com.ibm.security.appscan.althoromutual.model.User)request.getSession
    ).getAttribute( "user" );
    %>

    <h1>Hello <%= user.getFirstName() + " " + user.getLastName() %>
    </h1>

    <p>
        Welcome to Altoro Mutual Online.
    </p>
```










Method	File	Line	Tainted Arg
 org.apache.jsp.bank.main_jsp._jspService	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	
 javax.servlet.http.HttpSession.getAttribute	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	return val
 com.ibm.security.appscan.althoromutual.model.User.getLastName	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user
 java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user . com
 java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
 javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l

Suspect	CrossSiteScripting		C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	79	
---------	--------------------	---	---	----	----	---

```
<%
    com.ibm.security.appscan.althoromutual.model.User user =
    (com.ibm.security.appscan.althoromutual.model.User)request.getSession
    ).getAttribute( "user" );
    %>



    <h1>Hello <%= user.getFirstName() + " " + user.getLastName() %>
    </h1>

    <p>
        Welcome to Altoro Mutual Online.
    </p>
```

</p>			
Method	File	Line	Tainted Arg
 org.apache.jsp.bank.main_jsp._jspService	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	
 javax.servlet.http.HttpSession.getAttribute	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	13	return val
 com.ibm.security.appscan.althoromutual.model.User.getFirstName	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user
 java.lang.String.valueOf	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	user . com
 java.lang.StringBuilder.<init>	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	java.lang.
 java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
 java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
 java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l
 javax.servlet.jsp.JspWriter.print	C:\Sample Applications\AltoroJ_ant\WebContent\bank\main.jsp	16	new java.l

Common Fix Point: Injection.SQL



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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\althoromutual\uti\DBUtil.java	375	89	

```

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();
    }
}

```









Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\althoromutual\uti\DBUtil.java	375	89	
------------	---------------	---	---	-----	----	---

```

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();
    }
}

```

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



Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	386	89	
<pre>public static String addUser(String username, String password, String firstname, String lastname) { try { Connection connection = getConnection(); Statement statement = connection.createStatement(); statement.execute("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('"+username+"','"+password+"', '"+f rstname+"', '"+lastname+"','user')"); return null; } catch (SQLException e){ return e.toString(); } }</pre>						
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	386	89	
<pre>public static String addUser(String username, String password, String firstname, String lastname) { try { Connection connection = getConnection(); Statement statement = connection.createStatement(); statement.execute("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('"+username+"','"+password+"', '"+f rstname+"', '"+lastname+"','user')"); return null; } catch (SQLException e){ return e.toString(); } }</pre>						
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	386	89	
<pre>public static String addUser(String username, String password, String firstname, String lastname) { try { Connection connection = getConnection(); Statement statement = connection.createStatement(); statement.execute("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('"+username+"','"+password+"', '"+f rstname+"', '"+lastname+"','user')"); return null; } catch (SQLException e){ return e.toString(); } }</pre>						
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	386	89	
<pre>public static String addUser(String username, String password, String firstname, String lastname) { try { Connection connection = getConnection(); Statement statement = connection.createStatement();</pre>						

```

        statement.execute("INSERT INTO PEOPLE (USER_ID,PASSWORD,FIRST_NAME,LAST_NAME,ROLE) VALUES ('"+username+"','"+password+"',
        '"+f
rstname+"', '"+lastname+"','user')");
        return null;
    } catch (SQLException e){
        return e.toString();
    }
}

```



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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	398	89	

```

public static String changePassword(String username, String password) {
    try {
        Connection connection = getConnection();
        Statement statement = connection.createStatement();
        statement.execute("UPDATE PEOPLE SET PASSWORD = '"+ password +"' WHERE USER_ID = '"+username+"'");
        return null;
    } catch (SQLException e){
        return e.toString();
    }
}

```



Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	398	89	
------------	---------------	---	---	-----	----	---

```

public static String changePassword(String username, String password) {
    try {
        Connection connection = getConnection();
        Statement statement = connection.createStatement();
        statement.execute("UPDATE PEOPLE SET PASSWORD = '"+ password +"' WHERE USER_ID = '"+username+"'");
        return null;
    } catch (SQLException e){
        return e.toString();
    }
}

```

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	180	89	

```

    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 89 



```
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 89 


```
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 89 

```
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 89 

```
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	89	
------------	---------------	---	---	-----	----	---

```

    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	89	
------------	---------------	---	---	-----	----	---



```

    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");

```

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	307	89	

```

    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

89



```
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

89



```
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");
```

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	123	89	
<pre>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;</pre>						
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\util\DBUtil.java	123	89	


```

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



Classification	Type	Severity	File	Line	CWE ID	Trace
Definitive	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	146	89	

```

if (username == null || username.trim().length() == 0)
    return null;

Connection connection = getConnection();
Statement statement = connection.createStatement();
ResultSet resultSet =statement.executeQuery("SELECT FIRST_NAME, LAST_NAME, ROLE FROM PEOPLE WHERE USER_ID = '"+ username +"
");
* BAD - user input should always be sanitized */
String firstName = null;
String lastName = null;
String roleString = null;
if (resultSet.next()){

```




Suspect	Injection.SQL		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\altoromutual\uti\DBUtil.java	180	89	
---------	---------------	---	--	-----	----	---

```

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");
}

```

Method	File	Line	Tainted Arg
 com.ibm.security.appscan.altoromutual.servlet.TransferServlet.doPost	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\TransferServlet.java	52	
 javax.servlet.http.HttpSession.getAttribute	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\TransferServlet.java	52	return val
 com.ibm.security.appscan.altoromutual.model.User.getUsername	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\TransferServlet.java	56	user

com.ibm.security.appscan.altoromutual.util.DBUtil.transferFunds	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\TransferServlet.java	108	userName
com.ibm.security.appscan.altoromutual.util.DBUtil.getUserInfo	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	206	username
com.ibm.security.appscan.altoromutual.model.User.getCreditCa rdNumber	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	226	user
com.ibm.security.appscan.altoromutual.model.User.getAcc counts	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\model\User.java	77	this
com.ibm.security.appscan.altoromutual.util.DBUtil.getA ccounts	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\model\User.java	69	this . use
java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	180	username
java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	180	new java.l
java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	180	new java.l
java.sql.Statement.executeQuery	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	180	new java.l

Common Fix Point: Validation.Required

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

Classification	Type	Severity	File	Line	CWE ID	Trace
Suspect	Validation.Required		C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet \AdminServlet.java	109	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\al toromutual\servlet\AdminServlet.java	94	
com.ibm.security.appscan.altoromutual.util.DBUtil.changePassword	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	94	return val
java.lang.Throwable.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	401	return val
java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	message
java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	new java.l
javax.servlet.http.HttpSession.setAttribute	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	109	message



```

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
<input type="checkbox"/> com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	40	
<input type="checkbox"/> com.ibm.security.appscan.altoromutual.util.DBUtil.addAccount	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	40	return val
<input checked="" type="checkbox"/> java.lang.Throwable.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	378	return val
<input checked="" type="checkbox"/> java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	message
<input checked="" type="checkbox"/> java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	new java.l
<input checked="" type="checkbox"/> javax.servlet.http.HttpSession.setAttribute	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	109	message



```

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
<input type="checkbox"/> com.ibm.security.appscan.altoromutual.servlet.AdminServlet.doPost	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	71	
<input type="checkbox"/> com.ibm.security.appscan.altoromutual.util.DBUtil.addUser	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	71	return val
<input checked="" type="checkbox"/> java.lang.Throwable.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\util\DBUtil.java	389	return val
<input checked="" type="checkbox"/> java.lang.StringBuilder.append	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	message
<input checked="" type="checkbox"/> java.lang.StringBuilder.toString	C:\Sample Applications\AltoroJ_ant\src\com\ibm\security\appscan\al toromutual\servlet\AdminServlet.java	105	new java.l



javax.servlet.http.HttpServletResponse.sendRedirect

C:\Sample Applications\AltoraJ_ant\src\com\ibm\security\appscan\alt
oromutual\servlet\AccountViewServlet.java

44

new java.l