





## InputValidation\_ReflectedXSS\_preview\_Finding - Findings Report

Oct 26, 2007 7:07:24 PM

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	CrossSiteScripting		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\templates\default\editors\preview.jsp	22	79	
<p>Description:</p> <ol style="list-style-type: none"> <li>1. The preview.jsp uses the "action" parameter directly without validation/output encoding.</li> <li>2. The PreviewContent.jsp will output the edited text directly without output encoding.</li> </ol> <p>Recommendation:</p> <p>Output Encode the value rendered to the user. Use the "StringUtil.replaceEntities()" method.</p> <pre>&lt;form accept-charset="&lt;wiki:ContentEncoding/&gt;" method="post"   action="&lt;%=action%&gt;"   name="editForm" enctype="application/x-www-form-urlencoded"&gt;   &lt;p&gt;     &lt;!-- Edit.jsp &amp; Comment.jsp rely on these being found.  So be careful, if you make changes. --%&gt;     &lt;input name="author" type="hidden" value="&lt;%=session.getAttribute("author")%&gt;" /&gt;     &lt;input name="link" type="hidden" value="&lt;%=session.getAttribute("link")%&gt;" /&gt;     &lt;input name="remember" type="hidden" value="&lt;%=session.getAttribute("remember")%&gt;" /&gt;     &lt;input name="page" type="hidden" value="&lt;wiki:Variable var="pagename"/&gt;" /&gt;     &lt;input name="action" type="hidden" value="save" /&gt;</pre>						
Vulnerability	CrossSiteScripting		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\templates\default\editors\preview.jsp	23	79	
<p>Description:</p> <ol style="list-style-type: none"> <li>1. The preview.jsp uses the "action" parameter directly without validation/output encoding.</li> <li>2. The PreviewContent.jsp will output the edited text directly without output encoding.</li> </ol> <p>Recommendation:</p> <p>Output Encode the value rendered to the user. Use the "StringUtil.replaceEntities()" method.</p> <pre>  action="&lt;%=action%&gt;"   name="editForm" enctype="application/x-www-form-urlencoded"&gt;   &lt;p&gt;     &lt;!-- Edit.jsp &amp; Comment.jsp rely on these being found.  So be careful, if you make changes. --%&gt;     &lt;input name="author" type="hidden" value="&lt;%=session.getAttribute("author")%&gt;" /&gt;     &lt;input name="link" type="hidden" value="&lt;%=session.getAttribute("link")%&gt;" /&gt;     &lt;input name="remember" type="hidden" value="&lt;%=session.getAttribute("remember")%&gt;" /&gt;     &lt;input name="page" type="hidden" value="&lt;wiki:Variable var="pagename"/&gt;" /&gt;     &lt;input name="action" type="hidden" value="save" /&gt;     &lt;input name="edittime" type="hidden" value="&lt;%=pageContext.getAttribute("lastchange",</pre>						



## Description:

1. The preview.jsp uses the "action" parameter directly without validation/output encoding.
2. The PreviewContent.jsp will output the edited text directly without output encoding.

## Recommendation:

Output Encode the value rendered to the user. Use the "TextUtil.replaceEntities()" method.

```
This is a <strong>preview</strong>! Hit "Keep Editing" to go back to the editor,
or hit "Save" if you're happy with what you see.
</div>
<div class="previewcontent">
  <wiki:Translate><%=EditorManager.getEditedText(pageContext)%></wiki:Translate>
</div>
<div class="information">
  This is a <strong>preview</strong>! Hit "Keep Editing" to go back to the editor,
  or hit "Save" if you're happy with what you see.
```



## Description:

1. The preview.jsp uses the "action" parameter directly without validation/output encoding.
2. The PreviewContent.jsp will output the edited text directly without output encoding.

## Recommendation:

Output Encode the value rendered to the user. Use the "TextUtil.replaceEntities()" method.

```
<input name="page" type="hidden" value="<wiki:Variable var="pagename"/>" />
<input name="action" type="hidden" value="save" />
<input name="edittime" type="hidden" value="<%=pageContext.getAttribute("lastchange",
                                                                    PageContext.REQUEST_SCOPE )%>" />

  <input name="addr" type="hidden" value="<%=request.getRemoteAddr()%>" />

</p>
<textarea style="display:none;" readonly="true"
          id="editorarea" name="<%=EditorManager.REQ_EDITEDTEXT%>" rows="4"
cols="80"><%=TextUtil.replaceEntities(userText)%></textarea>
```



## Description:

1. The preview.jsp uses the "action" parameter directly without validation/output encoding.
2. The PreviewContent.jsp will output the edited text directly without output encoding.

## Recommendation:

Output Encode the value rendered to the user. Use the "TextUtil.replaceEntities()" method.

```
name="editForm" enctype="application/x-www-form-urlencoded">
<p>
  <!-- Edit.jsp & Comment.jsp rely on these being found. So be careful, if you make changes. --%>
  <input name="author" type="hidden" value="<%=session.getAttribute("author")%>" />
  <input name="link" type="hidden" value="<%=session.getAttribute("link")%>" />
  <input name="remember" type="hidden" value="<%=session.getAttribute("remember")%>" />
  <input name="page" type="hidden" value="<wiki:Variable var="pagename"/>" />
```

```
<input name="action" type="hidden" value="save" />
<input name="edittime" type="hidden" value="<%=pageContext.getAttribute("lastchange",
                                                                    PageContext.REQUEST_SCOPE )%>" />
```