

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

Oct 26, 2007 7:07:24 PM

| Classification | Type                         | Severity  | File   | Line | CWE ID | SmartTrace |
|----------------|------------------------------|---|--|------|--------|------------|
| Vulnerability  | CrossSiteScripting.Reflected |  | Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\templates\default\commonheader.jsp | 66   | 79     |            |

### XSS Example 1 Description: Line: 76:

The skin parameter is used directly without validation and/or output encoding via the TemplateDirectory tag. Since the commonheader.jsp is used throughout many/all JSPs, this attack may be triggered through a variety of vector. Also, not in this particular attack the <script> tags do not need to be injected since the reflected data is already inside existing script tags. The pagename value should be investigated as well as it is outputted without using the proper output encoding routine.

### XSS Example 1 Exploit:

[http://localhost:8080/JSPWiki/Wiki.jsp?page=Main&skin="\);alert\(document.cookie\);Wiki.loadBrowserSpecificCSS\("http://localhost:8080/JSPWiki/",](http://localhost:8080/JSPWiki/Wiki.jsp?page=Main&skin=)

### XSS Example 1 Recommendation:

Properly validate that the skin parameter for the template directory only contains alpha/numeric characters. It should be noted that the "TextUtil.replaceEntities" may not be sufficient since the input is already within script tags.

### XSS Example 2 Description: Line: 66:

The skinName value is outputted directly without output encoding.

### XSS Example 2 Recommendation:

Use the "TextUtil.replaceEntities" method to properly output encode the contents.

```

    for( Iterator i = skins.iterator(); i.hasNext(); )
    {
        String skinName = (String)i.next();
%>
        <link rel="alternate stylesheet" type="text/css" href="<wiki:Link format='url' templatefile='<%= "skins/" + skinName + "/skin.css"%>' />
        title="<%=skinName%>" />
    <%
    }
%>
<% if(prefSkinName != null) { %>

```