



InputValidation_ReflectedXSS_editors_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\src\com\ecyrd\jspwiki\tags\EditorTag.java	66	79	
<div> <div> Description: The editor related functionality contains a variety of different reflected XSS attacks. Please see below for the specific XSS detected. </div> <div> <div> 1. FCK.jsp - The "pageAsHtml" parameter is used without validation/output encoding. Also, note that this parameter is already embedded within existing <script></script> tags. An attacker would not need to inject these strings to successfully exploit this XSS. </div> <div> 2. WikiWizard.jsp/FCK.jsp - The "link" parameter is used directly without validation/output encoding.. Note this parameter is set via the Edit.jsp and used throughout all Editors. * Attack URL: <a "="" href="http://localhost:8080/JSPWiki/Comment.jsp?page=JOJO&link="><script>alert(document.cookie);</script>&preview=something </div> <div> 3. WikiWizard.jsp/plain.jsp - The "Accept-Language:" header is used directly without validation/output encoding. * Attack HTTP Payload: GET http://localhost:8080/JSPWiki/Edit.jsp?page=FOO&editor=WikiWizard&user=foo HTTP/1.1 Host: localhost:8080 User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: "><script>alert(document.cookie);</script> Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Proxy-Connection: keep-alive Cookie: JSPWikiAssertedName=127.0.0.1; JSPWikiSearchBox=favorites; JSESSIONID=44B8881F5C94CE828FDDF9F4B139FA24 If-Modified-Since: Thu, 01 Nov 2007 19:47:12 GMT </div> <div> 4. WikiWizard.jsp/plain.jsp - Also note there is potential for the "attString" to contain malicious payload here since it is not output encoded. However, the likelihood is reduced as it appears that the attachment process will validate the filename attributes at some level. However, it is recommended that it be output encoded here as well to further decrease the XSS potentials. </div> <div> 5. The editor drop down list is constructed without validation and outputs whatever value the user injects. * Attack URL: <a href="http://localhost:8080/JSPWiki/Edit.jsp?page=FOO&editor=<script>alert(document.cookie);</script>">http://localhost:8080/JSPWiki/Edit.jsp?page=FOO&editor=<script>alert(document.cookie);</script> </div> <div> Recommendation: Output Encode the value rendered to the user. Use the "StringUtil.replaceEntities()" method. In cases where the data is already rendered within existing script tags, consider very strong input validation and even removing this exclusion within existing script tags </div> </div> </div>						
<div> <div> <pre> m_wikiContext.getTemplate(), editorPath); if(page == null) { pageContext.getOut().println("Unable to find editor '"+editorPath+"'"); } else </pre> </div> </div>						

```
{  
  pageContext.include( page );  
}
```