

InputValidation\_ReflectedXSS\_IncludeTag\_skin\_paramter\_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\src\com\ecyrd\jspwiki\tags\IncludeTag.java	79	79	

Description: The Include Tag may print out an error message containing user input. Even though it is highly unlikely that this will contain malicious payload (since the logic only executes if page is null), best practices indicate using the standard output encoding routine to sanitize the data. Note this particular vulnerability may be triggered, via the use of the Include Tag, from 16 different vectors.

For example, "skin=<script>alert(document.cookie);</script>" might be attempted to be injected and the code were changed in the future to not check if null.

Recommendation: Output Encode the value rendered to the user. Use the "StringUtil.replaceEntities()" method.

```

                                                                    m_wikiContext.getTemplate(),
                                                                    m_page );

    if( page == null )
    {
        pageContext.getOut().println("No template file called '"+m_page+"'");
    }
    else
    {
        pageContext.include( page );
    }

```