

AccessControl_ForcedBrowsing_SecurityConfig_Finding - Findings Report

Oct 26, 2007 7:07:24 PM

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	AccessControl		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\admin\SecurityConfig.jsp	10	250	

Description:

Any users (unauthenticated/authenticated/asserted) can force browse to this page and gain pseudo sensitive information about the security configurations of the application. This pages details various security configuration of the site, including the access control definition, etc. Using this information an attacker can determine potential access control weaknesses or misconfiguration related to security. It appears that this page is intended to only be accessed by administrators, however the access control check on this page is not in place, allowing any user invocation.

URL: <http://localhost:8080/admin/SecurityConfig.jsp>

Recommendation:

Consider calling "wikiContext.hasAccess" and/or the appropriate authorization mechanism to ensure that only privileged administrative users can access this page.

```
<%@ page import="com.ecyrd.jspwiki.auth.*" %>
<%@ page errorPage="/Error.jsp" %>
<%!
    public void jspInit()
    {
        wiki = WikiEngine.getInstance( getServletConfig() );
    }
    Logger log = Logger.getLogger("JSPWiki");
    WikiEngine wiki;
    SecurityVerifier verifier;
%>
```