


Authentication_PasswordPolicyRulesNotAvailable_Finding - Findings Report

Oct 26, 2007 7:07:24 PM

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	Authentication		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java	425	287	
<div> <div>Description:</div> <div> <p>The application currently does not provide the means for application administrators to enforce strong password policies. Without strong password policies, it is highly likely that end users will select weak passwords and the application will allow the use of these weak passwords. If usability requirements dictate allowing of weaker passwords, it is still desirable for certain JSPWiki administrators to have this configurable option of enforcing certain password policies. Currently the only enforcement in place is that the password can not be null or be that of the username.</p> </div> </div> <div> <div>Recommendation:</div> <div> <p>Consider implementing the capability to allow for JSPWiki administrators the capability to enforce stronger password complexity policies. For example, consider password length, character enforcement rules dictating special characters, etc.</p> </div> </div> <div> <pre> } else { HttpServletRequest request = context.getHttpRequest(); String password2 = (request == null) ? null : request.getParameter("password2"); if (!password.equals(password2)) { session.addMessage("profile", "Passwords don't match"); } } } </pre> </div>						