



Authentication\_DetailedErrorMessageMayIncreaseCredentailGuess\_Finding - Findings
Oct 26, 2007 7:07:24 PM

Report

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	Authentication		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\Login.jsp	61	287	
<div> <div>Description:</div> <div>The application will provide detailed error messages to the user which may allow him to further refine his attack. In this particular case the authentication mechanism will inform the user if authentication has failed due to cases mismatch, this may increase the odds for an attacker to successfully guess a victims password.</div> <div>Recommendation:</div> <div>Typical security best practices indicate providing a generic end-user error message which does not reveal details which may allow attack refinement. Also, if usability requirements dictate this message, consider making it a configurable option for those who do now want to provide this detailed message.</div> </div> <div> <pre> log.info( "Successfully authenticated user " + uid + " (custom auth)" ); } else { log.info( "Failed to authenticate user " + uid ); if ( passwd.length() &gt; 0 &amp;&amp; passwd.toUpperCase().equals(passwd) ) { wikiSession.addMessage("Invalid login (please check your Caps Lock key)"); } else { </pre> </div>						
Vulnerability	Authentication		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\Login.jsp	61	287	
<div> <div>Description:</div> <div>The application will provide detailed error messages to the user which may allow him to further refine his attack. In this particular case the authentication mechanism will inform the user if authentication has failed due to cases mismatch, this may increase the odds for an attacker to successfully guess a victims password.</div> <div>Recommendation:</div> <div>Typical security best practices indicate providing a generic end-user error message which does not reveal details which may allow attack refinement. Also, if usability requirements dictate this message, consider making it a configurable option for those who do now want to provide this detailed message.</div> </div> <div> <pre> log.info( "Successfully authenticated user " + uid + " (custom auth)" ); } else { log.info( "Failed to authenticate user " + uid ); if ( passwd.length() &gt; 0 &amp;&amp; passwd.toUpperCase().equals(passwd) ) </pre> </div>						

```
{  
    wikiSession.addMessage("Invalid login (please check your Caps Lock key)");  
}  
else  
{
```