JSP on CF Enterprise can open a security Hole

Posted At : May 18, 2005 2:33 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

Recent discussions on a popular email list regarding some large hosts with many CF customers have reminded me of an often overlooked security problem that crops up from time to time on CF enterprise. If you install CF enterprise you get a full functioning JRUN server with it. If you intend to use the server as a shared server however, you should be aware that by default, the JRUN server will handle JSP pages. This gives users with JSP knowledge a way of hacking the server that circumvents the CF server (since JRUN is agnostic of the CF sandbox). It's easy to fix however...

This is another *very* good reason to examine your hosting company carefully if you plan on running CF on a shared hosting server. Many hosting companies "offer" coldfusion but a select few actually know how to correctly and securely configure it. To be honest **most** of the shared hosts I've seen have been pretty much wide open. I could (for example) get a list of the DSN's on the server and access all of them freely. Or I could grab the cf admin password, unecrypt it, and log into the CF admin. The nuances of sandboxes were pretty much lost on them. In my opinion, you are better off hosting something yourself - or using a host with a high level of expertise - even if it costs more. Think of it as insurance!

To disable JSP handling change the "default-web .xml" file to comment out the license server for JSP functionality. like so...

```
<!--
<servlet>
<servlet-name>JspLicenseServlet</servlet-name>
<servlet-class>coldfusion.license.JspLicenseServlet</servlet-class>
</servlet>
-->
```

Here's the relavent live doc:

Live Docs Article on disabling JSP