Coldfusion dropping session ID in fusebox application

Posted At : 2 July 2009 15:53 | Posted By : Shaun McCran
Related Categories: Security, Development, Coldfusion, Best practices

I recently rolled out beta version of a new application I've been writing, only to discover that there was a bizarre session problem that didn't exist in dev, but does in live.

I've worked it out, but I thought I'd explore it some more. It is a fusebox 5.5 non xml application. The error I had was that as soon as I made a call through a "new" circuit, IE one I hadn't called before ColdFusion would generate a new session ID, and thus invalidate my current active session.

Looking through my application CFC I had this line of code present.

```
<cfset this.SetClientCookies = false />
```

Setting this to true fixed the issue. This is because ColdFusion relies on the CFID and CFTOKEN to maintain the session state. You can either pass these two variables through the URL on every page request, which is a bit messy, or you can use a cookie. It is the variable above that lets the application use cookies on the user's session.

The problem with setClientCookies is that it is persistent, IE it is built for that session, and left on the user's pc, even after the session has expired, or they have left the application. Also some users will accept per-session cookies, but not persistent session cookies.

They are a lot more secure as per-session cookies, as they cannot be duplicated and hacked to spoof a previous user's session, and if you pass the token through the URL it is easy changed.

You could put something like this in your onRequestend function in application.cfc

```
<cfif IsDefined("Cookie.CFID") AND
   IsDefined("Cookie.CFTOKEN")>
 <cfset cfid_local = Cookie.CFID>
<cfset cftoken_local = Cookie.CFTOKEN>
<cfcookie name="CFID" value="#cfid_local#">
<cfcookie name="CFTOKEN" value="#cftoken_local#">
</cfif>
```

This will make them per-session. I originally thought that it was something to do with the Fusebox framework, but I had overlooked the simple fact that it was still a new page request, so would be lost. Although this doesn't explain why I wasn't getting this error in my development environment but did in live.