SQLi Results: No Errors

Posted At : August 13, 2008 7:00 AM | Posted By : Steve
Related Categories: ColdFusion, Page Controller

It has been interesting to see the results of the recent series of SQL injection attacks. I have been using <cfqueryparam> for all dynamic data for years, so I wasn't worried about the SQL injection. Still, even for sites with <cfqueryparam>, error email messages remain a problem.

Although I have gotten some errors from some sites, none from my newer sites. The reason is that earlier steps I have taken prevent errors from invalid URL variables.

The Page Controllers that I use have their own param() method that works *mostly* like <cfparam>.

It has three arguments:

- name: The name of the variable
- type: The variable type
- default: The default value

The big difference from this to <cfparam> is that &lt:cfparam> throws an error if the variable exists but isn't of the appropriate type whereas the param() method of the Page Controller will just go ahead and set the default value.

I would love it if this behavior was available as an option for <cfparam> as well.

Although this is my preferred technique, on some older sites I relied on try/catch:

```
<cftry>
   <cfparam name="url.id" type="numeric">
   <cfcatch>
      <cflocation url="index.cfm" addtoken="No">
   </cfcatch>
</cftry>
```

A cleaner approach that I have also used is Val(), which is effective in preventing errors:

```
<cfif isDefined("URL.id")>
   <cfset URL.id = Val(URL.id)>
<cfelse>
   <cfset URL.id = 0>
</cfif>
```

You can **read more about Page Controllers** or **view PageController.cfc**. Even if you don't like the concept of a Page Controller, I think the param() method is still useful by itself.