SQL Injection Attack going around

Posted At : 10 August 2008 19:26 | Posted By : Gareth
Related Categories: sql injection, coldfusion

I would imagine that most developers are already aware of this by now, but for those who haven't heard, there's a nasty sql injection attack going around. Details are here and you'll find plenty more on google:
http://www.rtraction.com/blog/devit/sql-injection-hack-using-cast.html

It's not specific to Coldfusion, but it is specific to MS SQL. ASP sites seem to have been targeted a few months ago, and Coldfusion ones in the last week or so, presumably because they are more likely to use MS SQL. There's even mention of it hitting php sites.

The good news, is that if you're a good coder and use **<cfqueryparam>** for all your query variables, you should be fine. If you're not sure if you do, there's a very good tool for checking on riaforge: http://qpscanner.riaforge.org/

One thing that queryparam can't sort though, is where you use variables for things like table and column names. An example would be:

```
SELECT col1
FROM #tablename#
ORDER BY #sort_col# #sort_dir#
```

You need to validate these variables before they enter the query.

It would be nice if cfqueryparam had this functionality. It's got me thinking about writing a custom tag to cover this missing functionality. Off the top of my head, I think you would want to be able to validate variables as:

- ASC or DESC
- A valid tablename
- A valid column name

These validations would be useful for situations where you have an html (or Flash) table, and the user can re-order them by clicking on column headers. The column name and direction would be passed as URL variables, and you could to put them straight into a query.

I did wonder if you would want it to validate sql statements such as SELECT, FROM and WHERE, but I can't imagine a scenario where this would ever be passed as user input.

If I've time over the next few weeks, I'll have a go at the custom tag, and post the code if it works. Feel free to add any suggestions in the comments below.