Disabling Backslash Escaping in MySQL

Posted At : May 16, 2008 9:31 AM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

For muse readers who read my **previous post** on SQL injection examples that use character rather than numeric fields, I offer this tip I picked up on CF-Talk from Azadi Saryev. It appears you can *disable* the ability to escape special characters using the backslash. Here is the exact note from Azadi.

> you can run MySQL in NO_BACKSLASH_ESCAPES mode. see chapter 5.2.6 in MySQL ref manual. This SQL mode also can be enabled automatically when the server starts by using the command-line option --sql-mode=NO_BACKSLASH_ESCAPES or by setting sql-mode=NO_BACKSLASH_ESCAPES in the server option file (for example, my.cnf or my.ini, depending on your system).
>
> there appears to be no jdbc connector option to change this behaviour, so have to do in server config/start...

Thanks Azadi, for a great tip! Readers with more MySQL experience than I can let me know about the nuances of this approach. While this solves the issue of the SQL injection using single quotes escaped with a backslash, I suspect that it may cause other problems. Are there other types of characters that would be precluded or need to be escaped in some way? Either way, it's nice to have another arrow in the quiver.