Rebellious Database Programming

Posted At : September 22, 2009 10:37 AM | Posted By : Mark Kruger
Related Categories: ColdFusion

> *Muse Reader Brian Asks:*
> Do you know of any way to SQL inject the following if the backend is MSSQL Server
>
> ```
> <cfquery ...>
> select *
> from table
> where username = '#FORM.username#'
> </cfquery>
> ```

Occasionally someone asks me this question about CFQUERYPARAM. "Must I use it here or there? In a boat? With a goat?" Yes Sam-I-Am you *should make it a habit* to use it everywhere. It should be a common part of your best practice guidelines. There are even reasons to use it that go beyond security. Do a quick search for CFQUERYPARAM on this blog and you will find all sorts of information about why to use it and the very rare exceptions (FYI in case you missed the tone here, there is rarely a good reason *not* to use it).

As for your specific question, I can think of no way to inject the query above. If you moved the query to a MySQL server you *might* run afoul of the alternate way of escaping single quotes, but on an MSSQL server the query above is safe *as far as I know*. Just remember, right now some clever hacker in Elbonia is experimenting with ancient character sets, time travel, and a dead cat which he swings over his head while chanting "...one ring to rule them all..." - all in an effort to try and crack into a query like the one above. So I reiterate, there is no way *as far as I know*. It's what I *don't* know that keeps me up at night. You really should just use the tag as a matter of course and stop looking for places to *not* use it. Let me illustrate with a little story my Dad used to tell me.

Foreign Intelligence

In the 1930's a man immigrated to America from a fascist country. He needed cash so he went to the bank to cash a check. Walking up to the teller the man presented his check and his ID and said "I vant cash pleaze" (if you hear an German accent it will help the story).

The teller looked at the check and noticed that the man had failed to sign it. "Sir, you must sign this check in order to get your money." the teller said in a friendly way.

The man, who was leery of being swindled in his unfamiliar new home, said quite forcefully, "I don't sign nutting!" The teller protested to the man that he simply couldn't cash the check unless the man chose to sign it. Finally the man said, "I don't need you... I go to other bank."

Leaving in a huff and crossing the street the man entered another bank and went up to the teller. Presenting his ID and check he said as before, "I vant cash pleaze."

Like the previous teller the man examined the check and said immediately, "You have to sign this check before I can give you the cash".

The man stiffened and reacted again saying, "I don't sign nuttin!" The teller looked at the man intently, then reached over the counter and grabbed him by the hair on the back of his head. Holding it firmly he banged the man's head on the counter two or three times. The man shook his head as if to clear it, then without a word he picked up a pen, signed the check and walked out with his cash.

The man immediately crossed the street to the *first* bank and, waiving his cash in the teller's face he crowed, "See... they give me cash."

The puzzled teller looked at him and asked accusingly, "But... you had to sign the check, right?"

Without missing a beat the man said, "Yes, but dey esplain it to me over der!"

Virtual "Esplanation"

So Brian, and all of you Muse readers out there who are looking for exceptions to the always-use-cfqueryparam rule. Try to sense what I am doing right now. I'm reaching through the screen and out into the Internet... to grab you by the hair and bang your head a few times on the table of whatever coffee shop you are currently frequenting. Hopefully that will esplain it to you. Now just use the dang tag will ya!