

Re: Real Simple Insert – doesn't work

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.adonet/2004-04/2144.html>

From: William Ryan eMVP (dotnetguru_at_comcast.nospam.net)

Date: 04/26/04

Date: Mon, 26 Apr 2004 10:03:00 -0400

First:

Have you put a breakpoint in your code and verified what the actual statement being passed is?

Second, it may not be your insert statement , but it most likely is. If your insert statement is legit, and you are sure of it, then look to another problem, maybe with the postback.

Third, Don't use Dynamic SQL. Especially on the Web. This is suicide today. Every single security and ASP.NET piece you can read today warns of this. There's a good reason. Concatenated dynamic SQL is error prone, a huge security vulnerability and inefficient...not to mention hard to code and maintain. Instead use Parameters:

```
strINSERT = "INSERT Newsletter (FName, SName, Email) Values (@FName, @SName, @Email)"
```

First, isn't this a lot easier to read and code? It's also safer, faster etc so trust me on this. Then assuming your types are all varchar(change them if they are not:

```
cmdInsert.Parameters.Add("@FName, SqlDbType.VarChar, 50).Value = FName.Text  
cmdInsert.Parameters.Add("@SName, SqlDbType.VarChar, 50).Value = SName.Text  
cmdInsert.Parameters.Add("@Email", SqlDbType.VarChar, 50).Value = Email.text
```

(I assumed the field size in your db is 50 for each field, change the size or the datatype to match what's in your db).

Here's my blog entry about the subject with an example that will walk you through it <http://msmvps.com/williamryan/posts/4063.aspx>

Trust me, it's a horrible habit on the desktop, but on the Web, you are potentially risking your whole database and YES, there are a ton of people who thought they were too insignificant for anyone to hack who've cost their company a lot by thinking this. Security through obscurity is not a real option any more.

HTH,

Bill

Let me know if you have any questions, I'll be glad to help. Didn't mean to lecture but just wanted to reinforce the point. Cheers,

Bill

>
> "dazzaLondon" <anonymous@discussions.microsoft.com> wrote in message
> news:DC6BBAE2-A438-41A9-A8AE-9E711544525A@microsoft.com...
> *Hey.*
>
> *Trying to do a real simple online Newsletter form – an Insert into a SQL*
> *Server DB, but when the submit button is pressed, the page refreshes, but*
> *nothing is added to the DB..*
>
> *Code:*
> *Dim ConDB As SqlConnection*
> *Dim strINSERT As String*
> *Dim cmdINSERT As SqlCommand*
>
> *ConDB = New SqlConnection("Persist Security Info=False;User*
> *ID=xxx;password=xxx;Initial Catalog=xxx;Data Source=xxx")*
> *strINSERT = "INSERT Newsletter " & _*
> *"(FName, SName, Email) " & _*
> *"Values ('" & FName.Text & "'," & SName.Text & "'," & Email.Text*
> *& "'")"*
>
> *cmdINSERT = New SqlCommand(strINSERT, ConDB)*
> *ConDB.Open()*
> *cmdINSERT.ExecuteNonQuery()*
> *ConDB.Close()*
>
>
> *appreciate your assistance guys.*