

Re: Sql insert Question

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2004-11/4671.html>

From: John M Deal (johndeal_at_necessitysoftware.com)

Date: 11/19/04

Date: Thu, 18 Nov 2004 19:04:39 -0800

What you are seeing is a classic example of a vulnerability to a SQL Injection attack. Obviously you want to fix this here, however you really need to fix this wherever you have concatenated SQL statements or you risk users (or potential hackers) really messing with your database (I won't preach but PLEASE!!! go look up information on SQL Injection and cross site scripting attacks).

To fix this there are four possibilities.

The best way to correct this is to migrate your sql statements into parameterized stored procedure calls.

If your database doesn't support parameterized stored procedures or you don't want to use stored procedures you should implement parameterized queries. To do this you would structure your query like:

```
string sql = "Update Products Set Discontinued=@Discontinued,
ProductName=@ProductName Where ProductId=@ProductId";
SqlCommand cmd = new SqlCommand(sql);
cmd.Parameters.Add("@Discontinued", SqlDbType.Bit).Value = chkBoxChecked;
cmd.Parameters.Add("@ProductName", SqlDbType.VarChar, 255).Value =
ProductName;
cmd.Parameters.Add("@ProductId", SqlDbType.Int).Value = ProductID;
cmd.ExecuteNonQuery();
```

This will fix the single quote issue. Not I realize it is in C# instead of VB.Net but I think you'll translate it with out a problem. Also it is setup for SQL Server but the concept should translate to whichever database object type you are working with.

Third if your database supports it you can try to replace each single quote with two single quotes (not double quotes but literally two single quotes). To do this you could do a

```
strSql.Replace("'", "''")
```

Finally, and probably worst of all you could try to filter out invalid characters but this could remove important data and/or miss things.

Hope this helps.

Have A Better One!

John M Deal, MCP
Necessity Software

Patrick.O.Ige wrote:

> *found my error i noticed i was inserting an apostrophe for example the word*
> *(code's) in into the DB..*
> *Whats the best way to replace this when inserting and editing and updating*
> *this..*
> *This problem come up especially when updating a field!!*
>
>
> *"Patrick.O.Ige" wrote:*
>
>
>>*Hi,*
>> *I have got this SQL below updating a textbox and a checkBox.*
>>
>>*strSql = "Update Products Set Discontinued=" & chkBoxChecked & ",ProductName*
>>*= "" & ProductName & "" Where ProductID=" & ProductID*
>>
>>*it outputs error :- Incorrect syntax near 's'. Unclosed quotation mark*
>>*before the character string ' Where ProductID=4'.*
>>
>>*I can't see what is wrong can somebody just look through this..*
>>*Maybe tired:(*
>>*Thx*