
Subject: PHP issue

Posted by [cnc95fan](#) on Fri, 05 Nov 2010 23:24:16 GMT

[View Forum Message](#) <> [Reply to Message](#)

I started learning PHP about 2 weeks ago and have gotten as far as small database things.. I decided as a first project I would make some sort of system for my school library, however I can't see what is wrong with this code. The page shows up blank (I had a "or die()" after the mysql_connect function) with no info on it.

```
<?php
$var = $_POST['bookid'];
if(isset($var)) {

$con = mysql_connect("localhost","root","1234");
mysql_select_db("library");
$bookinfo = mysql_query("SELECT * FROM books WHERE bookid = $_POST['bookid']");
while($row = mysql_fetch_array($bookinfo))
{
echo $row['bookid'] . $row['id'];
}
}
echo "Test echo";
?>
```

The form sending the POST data sends `<input type="text" name="bookid"/>`

I am able to connect to the mysql db as I have tried with another page (which simply shows text on it from a db).

The "Test echo" does not show.

Anybody able to shed some light on this?

Subject: Re: PHP issue

Posted by [Omar007](#) on Fri, 05 Nov 2010 23:46:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

I did do PHP but I think it has become a bit rusty
My SQL is pretty good though

Try this.

```
<?php
$var = $_POST['bookid'];
if(isset($var)) {

$con = mysql_connect("localhost","root","1234");
mysql_select_db("library");
$bookinfo = mysql_query("SELECT * FROM books WHERE bookid='$var'");
while($row = mysql_fetch_array($bookinfo))
{
```

```
echo $row['bookid'] . "-" . $row['id'];  
}  
}  
echo "Test echo";  
?>
```

`$row['id']` -> Do you have both 'bookid' and 'id?? :S'

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Fri, 05 Nov 2010 23:51:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

Yeah using `$var` instead of `$_POST['bookid']` makes much more sense anyway :v.
Thanks for that.
The bookid and id was a bit of English mix up as it should have been bookname and not bookid but I'm too lazy to change it in the SQL DB

Subject: Re: PHP issue
Posted by [Omar007](#) on Fri, 05 Nov 2010 23:55:15 GMT
[View Forum Message](#) <> [Reply to Message](#)

OK well as long as it's 'bookid' in your database, it should be good

You could also try to 'paste' the variable `$var` into the query btw.

```
$bookinfo = mysql_query("SELECT * FROM books WHERE bookid=" . $var . "');
```

Also some reference that might be useful:
PHP MySQL functions Reference: http://w3schools.com/php/php_ref_mysql.asp
PHP & MySQL: http://w3schools.com/php/php_mysql_intro.asp

Subject: Re: PHP issue
Posted by [Crimson](#) on Sat, 06 Nov 2010 00:18:43 GMT
[View Forum Message](#) <> [Reply to Message](#)

The problem was that you need to put curly braces around an array reference when it's in a string like that.

```
"SELECT * FROM books WHERE bookid = {$_POST['bookid']}"
```

The curly braces tell the PHP parser where the variable starts and ends because when you start

adding symbols, it gets confused.

The \$var way works, too, but it creates messier, harder-to-read code.

(Of course, since you're a beginner, I won't point out the XSS flaws.)

Subject: Re: PHP issue

Posted by [danpaul88](#) on Sat, 06 Nov 2010 10:03:17 GMT

[View Forum Message](#) <> [Reply to Message](#)

Actually I disagree Crimson, protecting database inputs against injection attacks is something you should learn as early as possible so that it becomes second nature when coding in PHP.

cnc95fan, consider what would happen if I submitted your search form with the following;

```
$_POST['bookid'] = '0; DROP TABLE books';
```

Based on your current code, this would result in the following query being run;

```
SELECT * FROM books WHERE bookid=0; DROP TABLE books;
```

Obviously this is a huge security problem, however there is a simple solution: Run anything from POST or GET which will go into a database through functions to verify it is valid. For numerical (int, float) values use something like;

```
function prepare_db_number($number)
{
    if ( is_numeric($number) )
    {
        return $number;
    }
    return 0;
}
```

This is an extremely simple function which checks the input is numeric and returns it if it is. If it is NOT numeric it returns 0, preventing any SQL injection attacks through that variable.

For strings you can use something a bit like this;

```
function prepare_db_string( $string, $encode_html_entities = FALSE )
{
    // If magic quotes are enabled then strip the existing slashes from the string first
    if(get_magic_quotes_gpc())
        $result = stripslashes(trim($string));
    else
        $result = trim($string);
}
```

```
// Encode HTML entities if required
if ( $encode_html_entities === TRUE )
    $result = htmlentities($result);

// Return MySQL safe string
return mysql_real_escape_string($result);
}
```

This function does several things - firstly it trims whitespace from around the input string (ie: spaces or tabs before or after any actual content) and, if magic quotes are enabled, it removes the slashes (otherwise you would end up with some things double escaped). Secondly, it optionally converts special characters to their HTML entities, this is useful if you know the string is going to be output directly to HTML and you need to ensure there are no HTML tags inside of it, for example a forum post.

Finally it uses `mysql_real_escape_string` to escape any character sequences which could be used to break out of the string and inject an additional query.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Mon, 08 Nov 2010 22:35:00 GMT
[View Forum Message](#) <> [Reply to Message](#)

Out of curiosity what do you do if you need the user to input `&/*`; etc?

Subject: Re: PHP issue
Posted by [danpaul88](#) on Mon, 08 Nov 2010 23:07:34 GMT
[View Forum Message](#) <> [Reply to Message](#)

`htmlentities` takes care of those for you

For example;
& will become &

Or, if you want to keep the raw input, just run it through `mysql_real_escape_string` on it's own, that will protect against injection attacks.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Thu, 11 Nov 2010 19:15:00 GMT
[View Forum Message](#) <> [Reply to Message](#)

```
$con = mysql_connect("localhost","root","1234");
mysql_select_db("test");
```

```
$regnum = rand(100000,999999);
mysql_query("INSERT INTO USERS ('id','user','password') VALUES
('$regnum','$_POST['user'],'$_POST['pass']");
mysql_close($con);
echo "test";
```

I can't see anything in there that would cause this to not work.. any ideas anyone?

Subject: Re: PHP issue

Posted by [danpaul88](#) on Thu, 11 Nov 2010 19:37:34 GMT

[View Forum Message](#) <> [Reply to Message](#)

cnc95fan wrote on Thu, 11 November 2010 19:15

```
mysql_query("INSERT INTO USERS ('id','user','password') VALUES
('$regnum','$_POST['user'],'$_POST['pass']");
```

You can't use things like `$_POST['pass']` directly in a string, you have to either put curly braces around the variables;

```
mysql_query("INSERT INTO USERS ('id','user','password') VALUES
('{ $regnum }', '{ $_POST['user'] }', '{ $_POST['pass'] }'");
```

Or concatenate them with the string

```
mysql_query("INSERT INTO USERS ('id','user','password') VALUES
('".$regnum."','".$_POST['user']."','".$_POST['pass']."");
```

My personal preference is the second method (concatenation), but it really doesn't matter which you use. The first variable (`$regnum`) is actually OK without these, but it's good practice to follow the same method for all variables as it makes it clear what you were intending to do.

For more information;

<http://www.php.net/manual/en/language.types.string.php#language.types.string.parsing>

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Thu, 11 Nov 2010 19:43:35 GMT

[View Forum Message](#) <> [Reply to Message](#)

Yeah that seems to have done the trick; on some other registration forms I was messing about with I have never had to do that before though, I always seemed to have gotten away with `'$_POST['x']':s`

Subject: Re: PHP issue

Posted by [danpaul88](#) on Thu, 11 Nov 2010 19:48:26 GMT

[View Forum Message](#) <> [Reply to Message](#)

\$_POST[x] would have worked, \$_POST['x'] wouldn't have done, unless you used one of the two methods outlined above. However it is always good practice to use quotes around array indexes which are strings, otherwise you could find that a constant you define in one place screws up a load of other scripts which used the name of that constant as an unquoted string array index.

EDIT;

Interestingly, I notice Crimson already mentioned using curly braces around array indexes in strings about 4 or 5 posts into this topic...

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Fri, 12 Nov 2010 23:06:58 GMT

[View Forum Message](#) <> [Reply to Message](#)

I know that; I assumed Omar's way also worked.

Subject: Re: PHP issue

Posted by [danpaul88](#) on Sat, 13 Nov 2010 09:02:51 GMT

[View Forum Message](#) <> [Reply to Message](#)

His way does work technically, so long as you apply it to every variable you want to use in the query, however that will soon produce rather a mess of code if you are using a lot of variables. Much better to insert them with {} or to concatenate them in directly.

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Sun, 14 Nov 2010 19:40:07 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
if($_POST['user'] != "" && $_POST['pwd'] != "")
{
$con = mysql_connect("localhost","root","1234");
mysql_select_db("test");
$regnum = rand(100000,999999);
$sqlone = mysql_query("SELECT * FROM users");
$sqlfetch = mysql_fetch_array($sqlone);
while($sqlone['id'] == $regnum)
{
$regnum = rand(100000,999999);
}
$regtitle = mysql_query("INSERT INTO titles (id) VALUES ('".$regnum."");
```

```
$reguser = mysql_query("INSERT INTO users (id,login,password) VALUES
('".$regnum."','".$_POST['user']."','".$_POST['pwd']."");
if($reguser)
{
    header("Location: index.php");
    exit;
}
else
{
    echo "SQL QUERY NOT COMPLETED.";
}
mysql_close($con);
}
else
{
    header("Location: register.php?login=failed&cause=".urlencode('Insert all values please'));
    exit;
}
```

This one has puzzled me. I have messed about commenting out parts to see where the problem is but I cannot find it.

I'm aware that the while loop is probably not the best way to go about doing something like that but this is just a small project I'm doing to learn PHP.. Any ideas?

Edit: It goes to the else "SQL QUERY NOT COMPLETED"

Subject: Re: PHP issue

Posted by [danpaul88](#) on Mon, 15 Nov 2010 13:28:43 GMT

[View Forum Message](#) <> [Reply to Message](#)

Add

```
echo mysql_error();
```

Above the SQL Query not completed line. That will print out WHY the query failed.

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Tue, 16 Nov 2010 22:09:09 GMT

[View Forum Message](#) <> [Reply to Message](#)

It will be the weekend before I get at the box again.

Out of curiosity though, how do functions work?

What does the return 0 in this function you wrote above do?

```
function prepare_db_number($number)
{
    if ( is_numeric($number) )
```

```
{
    return $number;
}
return 0;
}
```

Subject: Re: PHP issue
Posted by [danpaul88](#) on Tue, 16 Nov 2010 22:42:38 GMT
[View Forum Message](#) <> [Reply to Message](#)

It returns 0 as the result of the function...

Subject: Re: PHP issue
Posted by [Zion](#) on Tue, 16 Nov 2010 23:40:56 GMT
[View Forum Message](#) <> [Reply to Message](#)

danpaul88 wrote on Tue, 16 November 2010 22:42: It returns 0 as the result of the function...

Derp.

Subject: Re: PHP issue
Posted by [Ethenal](#) on Wed, 17 Nov 2010 05:44:06 GMT
[View Forum Message](#) <> [Reply to Message](#)

Zion wrote on Tue, 16 November 2010 17:40: danpaul88 wrote on Tue, 16 November 2010 22:42: It returns 0 as the result of the function...

Derp.

You didn't know what to do with a simple MySQL query. Just as bad.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Sat, 20 Nov 2010 20:51:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

I have yet another really weird issue, I've tried rewriting this thing about 4 times. Basically, inside a DB there is for arguments sake, 3 tables. The first table is an index, which contains 2 columns, id (as in some id in the URL) and a name. The page is supposed to select from the index where \$_GET['id'] is equal to id in the index, then look up the name in the same row. After getting the name it is then supposed to add on a postfix (such as x or y, so where the name would be renegade, the variable I assigned to the next task

would be renegadex).

```
$pid = $_GET['id'];
$index = mysql_query("SELECT * FROM index where id = ".$pid."") or die(mysql_error());
$row = mysql_fetch_array($index);
$thisvar = $row['name'];
$x = "x";
$query = mysql_query("SELECT * FROM ".$thisvar . $x." where uid = ".$_SESSION['id']."") or
die(mysql_error());
$row1 = mysql_fetch_array($query);
$uid = $row1['id'];
echo $uid;
```

The echo returns nothing so I'm assuming that one of the mysql_queries is failing somewhere...

Subject: Re: PHP issue

Posted by [Omar007](#) on Sat, 20 Nov 2010 23:04:46 GMT

[View Forum Message](#) <> [Reply to Message](#)

Does the first query return something? Also according to your code, if name = renegade then it will search in your next statement for the table renegadex. I'm assuming that table is present?

This is how I would write that piece of code. I don't think it matters but w/e

```
$pid = $_GET['id'];
$index = mysql_query("SELECT * FROM index where id = ".$pid."") or die(mysql_error());
$row = mysql_fetch_array($index);
$thisvar = $row['name'] . "x";
echo $thisvar; //Check here
$query = mysql_query("SELECT * FROM ".$thisvar." where uid = ".$_SESSION['id']."") or
die(mysql_error());
$row1 = mysql_fetch_array($query);
$uid = $row1['id'];
echo $uid;
```

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Sat, 20 Nov 2010 23:07:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

I rewrote this 4 times, and in between made adjustments to them so I tried the \$row['name'] . \$x; aswell. I didn't test to see if it was working in that sense but I ended up changing \$row['name'] var to the actual table name (excluding the \$x).

The table does indeed exist

Subject: Re: PHP issue

Posted by [danpaul88](#) on Sun, 21 Nov 2010 22:25:18 GMT

[View Forum Message](#) <> [Reply to Message](#)

In your query your checking if uid is equal to something, but then you try to echo id, do you have both a uid and id field in that table?

You might want to do something like this to check what results your actually getting back;

```
$query = mysql_query("SELECT * FROM table"); // Query here
echo "Query returned ".mysql_num_rows($query)." results;<br/><pre>"; // Output number of
results
while ( $result = mysql_fetch_assoc($query) ) // Iterate through each result row
{
    print_r($result); // Dump contents of current result row
    echo "<br/><br/>"; // Leave a gap between each result row
}
echo "</pre><br/>End of results<br/>";
mysql_data_seek($query,0); // Reset results pointer
```

FYI: The mysql_data_seek() call at the end just tells PHP to set the results pointer back to the first row so you can still process the results in the code which follows that block of code.

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Sun, 21 Nov 2010 23:14:52 GMT

[View Forum Message](#) <> [Reply to Message](#)

Thanks dp88;

Seemed to have fixed it. Just curious, I took up your suggestion there on learning security from the begining, so I'm inserting data using htmlspecialchars(), what would be the best way of printing that data on a page without those characters appearing (& etc).

Also is there any sites you know of that talk about security, as w3schools do not seem to

Subject: Re: PHP issue

Posted by [danpaul88](#) on Mon, 22 Nov 2010 16:56:23 GMT

[View Forum Message](#) <> [Reply to Message](#)

htmlspecialchars converts characters to their HTML equivilents, so outputting them to a HTML document like that should render them correctly without needing to make any further modifications to the values.

For example,

```
echo "<p>Thing &amp; another thing</p>";
```

Would appear something like this;

Thing & another thing

The idea of `htmlspecialchars` is to convert characters to HTML safe equivalents whilst ensuring they still output correctly. If they are outputting as `&`, `>`; etc then you are either calling `htmlspecialchars` multiple times or are not checking whether magic quotes are enabled before calling `htmlspecialchars`.

Subject: Re: PHP issue

Posted by [cnc95fan](#) on Mon, 06 Dec 2010 16:13:28 GMT

[View Forum Message](#) <> [Reply to Message](#)

Back here again...

I started working on making mysql query's more efficient as they seem to suck at the moment but that is another story.

To put it bluntly I am obviously missing some function that I do not know about.

I have a delete button for a comment (which is inputted by a user), the thing is these comments are echoed with an array, and I do not know how to pinpoint each number from the array to each comment.

page1.php

```
$commentquery = mysql_query("SELECT * FROM comments WHERE recipient = ".$sid."ORDER BY TIMESTAMP DESC");
while($get_comment_array = mysql_fetch_array($commentquery))
{
$sender = $get_comment_array['sender'];
$senderid = mysql_query("SELECT * FROM members WHERE uid = ".$sender."");
$memberarray = mysql_fetch_array($senderid);
$sendername = $memberarray['fullname'];
$_SESSION['cid'] = $get_comment_array['commentid'];
$recipient = $get_comment_array['recipient'];
$message = $get_comment_array['message'];
$timeofwriting = $get_comment_array['TIMESTAMP'];
echo "<div class='comments'>";
echo "<a style='color:blue;text-decoration:underline;'
href='profile.php?id=".$sender."'>".$sendername."</a> . " . $message . " <a style='float:right'
href='comment.php?type=member&action=del'><img src='delmessage.jpg'/></a>".<span
style='font-size:12px;color:grey;'>".$timeofwriting. . "</span>";
echo "</div>";
}
```

```
echo "<div class='comments'>";
$_SESSION['tid'] = $id;
// $id == $_GET['id']
```

```
page2.php (this is the deleting page)
if($_GET['type'] == "member" && $_GET['action'] == "del")
{
    mysql_select_db("user");
    $cid = $_SESSION['cid'];
    $delquery = mysql_query("DELETE FROM comments where commentid = ".$cid." AND sender
= ".$uid." OR recipient = ".$uid."") or die(mysql_error());
    header("Location: page1.php?id=".$tid."");
}
```

Subject: Re: PHP issue

Posted by [danpaul88](#) on Mon, 06 Dec 2010 17:00:46 GMT

[View Forum Message](#) <> [Reply to Message](#)

OK, the problem here is simple. Your setting the a session variable with the comment ID in... except you load MULTIPLE comments, so each comment overwrites the ID the previous one set, so if you use this variable on page2 to delete a comment it will ALWAYS delete the last comment loaded.

You should instead pass the comment ID to be deleted as a parameter to the delete page and use the \$_GET array to obtain it's value.

I have modified your code fragments below, look at the changes and you should be able to work out whats happening.

```
$commentquery = mysql_query("SELECT * FROM comments WHERE recipient = ".$id."ORDER
BY TIMESTAMP DESC");
while($get_comment_array = mysql_fetch_array($commentquery))
{
    $sender = $get_comment_array['sender'];
    $senderid = mysql_query("SELECT * FROM members WHERE uid = ".$sender."");
    $memberarray = mysql_fetch_array($senderid);
    $sendername = $memberarray['fullname'];
    $commentid = $get_comment_array['commentid'];
    $recipient = $get_comment_array['recipient'];
    $message = $get_comment_array['message'];
    $timeofwriting = $get_comment_array['TIMESTAMP'];
    echo "<div class='comments'>";
    echo "<a style='color:blue;text-decoration:underline;'
href='profile.php?id=".$sender."'>".$sendername."</a> . " . $message . " <a style='float:right'
```

```
href='comment.php?type=member&action=del&cid=".$commentid."><img
src='delmessage.jpg'/></a>".<span style='font-size:12px;color:grey;'>".$timeofwriting. .
"</span>";
echo "</div>";
}
echo "<div class='comments'>";
$_SESSION['tid'] = $id;
//$id == $_GET['id']
```

```
page2.php (this is the deleting page)
if($_GET['type'] == "member" && $_GET['action'] == "del")
{
    mysql_select_db("user");
    $cid = $_GET['cid'];
    $delquery = mysql_query("DELETE FROM comments where commentid = ".$cid." AND sender
= ".$uid."OR recipient = ".$uid."")or die(mysql_error());
    header("Location: page1.php?id=".$tid."");
}
```

Also, I am interested to know where page2.php gets the values of \$uid and \$tid from, as they are not set in that code fragment. I assume you do set theirs value correctly elsewhere in the script?

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Mon, 06 Dec 2010 18:30:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

Yeah they are set at the top of the script with mysql_connect() and session_start() etc;
With those modifications it still does the same thing strangely :/, although I could see where you are going with it.

Subject: Re: PHP issue
Posted by [danpaul88](#) on Mon, 06 Dec 2010 22:45:55 GMT
[View Forum Message](#) <> [Reply to Message](#)

You haven't actually told us WHAT it's currently doing which might help people find the cause of the problem. I just took a quick look at it earlier and pointed out the obvious issues.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Mon, 06 Dec 2010 22:56:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

The script reads from table "comments" based on the users id.
It then echos out these comments (which are collected in an array).

I'm trying to create a way of deleting a particular comment, so I created that session to store that comment id, where page2 reads that id and deletes it from the comments page, based on that id (provided the sender or the person whose page is the one deleting it)

As I said there's probably a much better way of doing this since I only started to look into MySQL query optimization last night

Subject: Re: PHP issue
Posted by [danpaul88](#) on Tue, 07 Dec 2010 12:33:37 GMT
[View Forum Message](#) <> [Reply to Message](#)

No, I mean what the RESULT of the code is at the moment, compared to what you EXPECT it to do.

IE: Does it give a mysql error? Does it format your C: drive? Etc?

EDIT;

And, as previously stated, session variables are NOT the right way to go about that. Sessions should be used for variables which persist for the duration of a session, such as the currently logged in user ID and any preferences they have set, such as their preferred font colour.

To pass a variable from one page to another, after which it is no longer needed, use GET (in the address string) or POST (submitted from a form with method POST).

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Tue, 07 Dec 2010 13:09:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

I want it to delete a specific comment, whilst at the moment it deletes them all (provided there is more than 1 comment on the page)
Is there a way to pass variables without using a form?

Subject: Re: PHP issue
Posted by [danpaul88](#) on Tue, 07 Dec 2010 18:26:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Yes, I showed you how to do that in the modified samples above. Add the ID to the address of the page you are linking to (page.php?action=delete&id=5 for example) and then use `$_GET['id']` to get the value of that parameter.

As I said before, if you look at the difference between the code I posted and your original code you will see what was changed, this being one of those things.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Tue, 07 Dec 2010 18:52:27 GMT
[View Forum Message](#) <> [Reply to Message](#)

Aye I'm aware of that and indeed I saw the changes you made;
The changes did not work, but I did a bit of messing about there and oddly enough, removing
sender = ".\$uid."OR seems to work...

Subject: Re: PHP issue
Posted by [danpaul88](#) on Tue, 07 Dec 2010 18:56:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ah, yes, your MySQL query has faulty logic.

You had;

Condition1 AND Condition2 OR Condition3

Which will always be true if Condition3 is true.

What you probably wanted was

Condition1 AND (Condition2 OR Condition3)

Which would be true if Condition1 was true and ONE of Condition2 or Condition3 were true.

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Tue, 07 Dec 2010 18:58:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

Brackets ftw then?

How would you go about learning how to make efficient queries? W3schools seem to only go so far and there's a lot of red in the status page on phpmyadmin...

Subject: Re: PHP issue
Posted by [cnc95fan](#) on Sun, 06 Feb 2011 17:14:52 GMT
[View Forum Message](#) <> [Reply to Message](#)

Anyone have any idea why `mysql_real_escape_string()` would effect my post data? Without it the queries execute fine but with it the variables which hold the POST data don't contain anything...
EDIT:
Never mind, I had the DB Connection after I escaped the data.....
