

Re: Microsoft JET Database Engine error '80040e10'

Source: <http://www.tech-archive.net/Archive/Data/microsoft.public.data.ado/2007-11/msg00098.html>

- *From:* "Bob Barrows [MVP]" <reb01501@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 29 Nov 2007 17:19:50 -0500
-

TonnyD wrote:

This is what I have for the script right now. I wasn't sure if I was supposed to remove the "Set rsPoll=" part or not.

You were.

```
<%
```

```
ID = CInt(Request.QueryString("ID"))
```

```
strSQL = "SELECT * FROM tblIP WHERE IP = " &  
request.ServerVariables("remote_addr") & " AND pollID=" & ID  
SET rsPoll = adoCon.execute(strSQL)
```

```
IF rsPoll.EOF Then
```

```
rsPoll.close  
strSQL="UPDATE tblCount SET " & Request.Form("txtOption") & "  
=" & Request.Form("txtOption") & " + 1 WHERE ID = " & ID  
SET rsPoll=adoCon.execute strSQL,,129  
Response.Write strSQL
```

OK, I misspoke in my prior message. The Response.Write needs to be after the statement that defines the string to be stored in strSQL, but BEFORE the Execute statement (it's the Execute statement that is raising the error). The goal is to write the statement to response before attempting to execute it so you can troubleshoot it. of course, once things are running smoothly, you will comment out those response.writes.

Anyways, it needs to look like this:

```
strSQL="UPDATE tblCount SET " & _  
Request.Form("txtOption") & "= " & _
```

Re: Microsoft JET Database Engine error '80040e10'

```
Request.Form("txtOption") & " + 1 WHERE ID = " & ID
```

```
Response.Write strSQL
```

```
adoCon.execute strSQL,,129
```

```
strSQL="INSERT INTO tblIP (IP, pollID) VALUES('" &  
Request.ServerVariables("REMOTE_ADDR") & "'," & ID & "')
```

```
Response.Write strSQL
```

```
adoCon.execute strSQL,,129
```

This was a ASP Poll script that was free. It has a faq teq page, but it only has errors for the databse. Nothing that includes this.

I guess you get what you pay for. This script is poorly written and insecure as well: the use of concatenation to form sql statements (aka dynamic sql) is leaving your site vulnerable to hackers using a technique called sql injection. When you're a little more comfortable with writing and debugging code, come back and ask about it. I've got some links that will prove enlightening to you.

Anyways, run the page, and then test each sql statement that was written to the browser screen using the Access Query Builder.

--

Microsoft MVP -- ASP/ASP.NET

Please reply to the newsgroup. The email account listed in my From header is my spam trap, so I don't check it very often. You will get a quicker response by posting to the newsgroup.

.