

Re: using Command to set Parameters and Recordset to retrieve the Query

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.asp.general/2004-03/0216.html>

From: Bob Barrows (*reb01501_at_NOyahoo.SPAMcom*)

Date: 03/03/04

Date: Wed, 3 Mar 2004 09:12:02 -0500

Bruno Alexandre wrote:

```
> Hi guys,
>
> without using SP, I want to be able to add a Parameter to the SQL
> Query and retrieve the Recordset so I can use the Paging property
> under the recordset object.... how can I do this?
>
> I'm stuck here.
>
>
>
> Set cnData = server.createObject("ADODB.Command")
> Set rsData = server.createObject("ADODB.RecordSet")
> ' set the page size
> rsData.PageSize = iPSize
> rsData.CursorLocation = adUseClient
>
> ' open the data
> sSQL = " SELECT * FROM vATSlistaAssistencias " & _
> " WHERE estado = 'ACTIVO' and estadoEsc not in ('FORA SERVICIO',
> 'NAO QUER', 'NAO TEM MAQUINA', 'OUTRA 2') and " & _
> " idDistribuidorAssistencia = @idDistAss and localidade like
> @localidade " & _
> " ORDER BY @coluna @ordem"
```

This will not work. The @variables are only usable in a stored procedure (see below). I strongly suggest using the solution I show below, but if for some reason you can't, you need to use the ODBC parameter placeholder (?) instead of the @variable names. Like this:

```
sSQL = " SELECT <list of columns - don't use * in production code>" & _
" FROM vATSlistaAssistencias " & _
" WHERE estado = 'ACTIVO' and estadoEsc not in " & _
" ('FORA SERVICIO', 'NAO QUER', 'NAO TEM MAQUINA', 'OUTRA 2')" & _
" and idDistribuidorAssistencia = ? and localidade like ? " & _
```

I have never tried this in the ORDER BY clause, so I am not sure it will work. If you try it and it works, please let us know.

" ORDER BY ? ?"

Even if this technique of using the parameters in the ORDER BY does work for you, I suspect that this will defeat your objective of preventing sql injection. You need to try putting some sql in the sOrdem variable to see if it will execute. Something harmless, like this:

```
sOrdem = "ASC; Select 'sql injected'"
```

Run the code and see if you have a second recordset (use the NextRecordset method to check for this).

Now, since you have the parameters marked with the ODBC placeholders, the following Command object code should work (assuming it is possible to use parameters in the ORDER BY clause, that is). However, I want to reiterate that you should not do it this way. See below for a more efficient solution using a stored procedure.

<Command code snipped>

>

> *I got an Error regarding the @idDistAss is not define in the query*

>

> *[Microsoft][ODBC SQL Server Driver][SQL Server]Must declare the*

> *variable '@idDistAss'*

You should use the SQLOLEDB provider, not ODBC. Here is an example:
For Standard Security

```
oConn.Open "Provider=sqloledb;" & _  
           "Data Source=myServerName;" & _  
           "Initial Catalog=myDatabaseName;" & _  
           "User Id=myUsername;" & _  
           "Password=myPassword"
```

For other examples, see:

http://www.able-consulting.com/MDAC/ADO/Connection/OLEDB_Providers.htm#OLEDBProviderForSQLServer

You should create a stored procedure on your sql server, like this:

```
CREATE PROCEDURE GetData (  
@idDistAss int,  
@localidade varchar(100)  
)  
AS  
SELECT <list of columns – don't use * in production code>  
FROM vATSlistaAssistencias  
WHERE estado = 'ATIVO' and estadoEsc not in ('FORA SERVICO', 'NAO  
QUER', 'NAO TEM MAQUINA', 'OUTRA 2') and  
idDistribuidorAssistencia = @idDistAss and localidade like @localidade
```

microsoft.public.inetserver.asp.general: Re: using Command to set Parameters and Recordset to retrieve the Query

You cannot use this syntax:

```
ORDER BY @coluna @ordem
```

The items in an ORDER BY list cannot be variables. Here are some options for you to consider:

<http://www.winnetmag.com/SQLServer/Article/ArticleID/16495/16495.html>

I will leave this part out of the example. You can put it in later after reading the article.

To execute this in ASP, just do this:

```
Set rsData = server.createObject("ADODB.RecordSet")
' set the page size
rsData.PageSize = iPSize
rsData.CursorLocation = adUseClient
oConn.Open
oConn.GetData idDistAssistencia,sLocalidade,rsData
if rsData.eof then
    'no records
else
    'do your stuff
end if
```

Once you figure out how to deal with the order by parameters, just do this:

```
oConn.GetData idDistAssistencia,sLocalidade, _
    sColuna,sOrdem,rsData
```

HTH,
Bob Barrows

--

Microsoft MVP - ASP/ASP.NET

Please reply to the newsgroup. This email account is my spam trap so I don't check it very often. If you must reply off-line, then remove the "NO SPAM"