

Re: Using sp_executesql to dynamically query xml

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.xml/2007-05/msg00017.html>

- *From:* Andy Webb <AndyWebb@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 8 May 2007 19:28:00 -0700
-

Dennis,

Thank you for your reply; I must have made an error in the XQuery in my hasty attempt to put together a simplified example. I was actually able to get the query to work fine if I did not use dynamic SQL, however my case requires the use of dynamic SQL because I do not know how the xml will be queried. The question that I wanted answered was: How do I do this using dynamic SQL in such a way that I avoid the possibility of SQL injection?

Thanks,
Andy

"Denis Ruckebusch [MSFT]" wrote:

It looks like your problems stem from the use of dynamic SQL but once your XQuery code doesn't look correct either.

To start, you should probably build a single string for your query, and not use parameters. Try something like this

```
DECLARE @Query nvarchar(255)

DECLARE @SqlCommand nvarchar(1000)

SET @Query = N'//*:Description/@title = "Project:A"'

SET @SqlCommand = 'SELECT * FROM ACTIVITY WHERE
ACTIVITY_DETAIL.value("'" + @Query + "',"bit") = cast(1 as bit)'

EXEC sp_executesql @SqlCommand
```

This will actually fail because of the static typing of XPath expression
//*:Description/@title = "Project:A"

Re: Using sp_executesql to dynamically query xml

It's hard to fix it without knowing exactly what you're trying to accomplish but if you want to retrieve the value of the *:Description element that contains an attribute title with a value equal to "Project:A" then the expression should be

```
(//*[Description[@title="Project:A"]][1]
```

I hope this helps. Please come back if you run into any more problems.

Denis Ruckebusch

<http://blogs.msdn.com/denisruc>

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Use of included script samples are subject to the terms specified at

<http://www.microsoft.com/info/copyright.htm>

"Andy Webb" <Andy Webb@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:1E37045D-ACF0-408B-8FFF-8BE22429C510@xxxxxxxxxxxxxxxxxxxx>

Hi,

I am writing a stored procedure which will allow callers to specify an XQuery that will be passed to the value function on an Xml column. I want to substitute this value into the query using sp_executesql to avoid the possibility of SQL Injection. However the following statement results in an error. How do I go about doing this without resorting to concatenating input parameters into my query.

```
DECLARE @Query nvarchar(255)  
DECLARE @SqlCommand nvarchar(1000)
```

```
SET @Query = N'//*[Description/@title = "Project:A"]'  
SET @SqlCommand = 'SELECT * FROM ACTIVITY WHERE  
ACTIVITY_DETAIL.value(@QUERY,"bit") = cast(1 as bit)'
```

```
EXEC sp_executesql @SqlCommand, N'@QUERY nvarchar(255)',  
@QUERY = @QUERY
```

This results in the the following error:

Msg 8172, Level 16, State 1, Line 1
The argument 1 of the xml data type method "value" must be a string literal.

Going one step further and quoting @QUERY does not help:

```
DECLARE @Query nvarchar(255)  
DECLARE @SqlCommand nvarchar(1000)
```

Re: Using sp_executesql to dynamically query xml

```
SET @Query = N'/*:Description/@title = "Project:A"  
SET @SqlCommand = 'SELECT * FROM ACTIVITY WHERE  
ACTIVITY_DETAIL.value("@QUERY","bit") = cast(1 as bit)'  
  
EXEC sp_executesql @SqlCommand, N'@QUERY nvarchar(255)',  
@QUERY = @QUERY
```

This results in the error

```
Msg 2390, Level 16, State 1, Line 1  
XQuery [ACTIVITY.ACTIVITY_DETAIL.value()]: Top-level attribute  
nodes are not  
supported
```

How can I work around these errors and provide a dynamic query without
using
concatenation?