SQL Injection (Lesson 1)
(Using SQL Server)

Injection یا همون تزریق دستورات SQL که به نفوذگر امکان دسترسی به بانک اطلاعاتی رو میده.

اول بگم چون این حملات با استفاده از پورت ۸۰ انجام می شود نگران Firewall ها نباشید.

قدم اول اینه که ببینیم سایت مورد نظر دارای آسیب پذیری هست یا نه؟

Login Page

Search Page

Feedback

HTML pages use POST command to send parameters to another ASP page

و بطور کلی هر صفحه ای که به شما اجازه Submit Data رو می دهد.

اما همیشه نیاز به Submit Page نیست و کارمون با صفحات (.jsp .cgi .php .asp) حل میشه مثلا:

http://site.com/index.asp?id=516

برای بررسی آسیب پذیر بودن سایت راه های گوناگونی بسته به هدف مورد نظر وجود داره.

استفاده از پارامتر های ویژه مثل: * - % " , ; '

into login, or password, or even in the URL. Example:

- Login: User'

- pass: Pass'

- http://Site.com.asp?id='hack

شاید مجبور باشیم تغیراتی در مکان بکار بردن پارامترهای ویژه بدیم:

into login, or password, or even in the URL. Example:

- Login: 'User

- pass: 'PAss

- http://Site.com.asp?id='516

یا بعضی از پارامترهای ویژه جواب نده و مجبوربشیم از پارامترهای دیگه یا ترکیب آنها استفاده کنیم:

into login, or password, or even in the URL. Example:

- Login: ';user

- pass: Pass;',

- http://Site.com.asp?id=;516

و موارد دیگه که تو مثالها برخورد می کنیم.(در درس۲ بیشتر توضیح میدم)

اگه بعد از وارد کردن پارامترهای ویژه ERRORهایی مثل زیر دریافت کردید سایت مورد نظر آسیب پذیر می باشد

The page cannot be displayed

There is a problem with the page you are trying to reach and it cannot be displayed.

ALL ODBC Error Messages
Microsoft OLE DB Provider for ODBC drivers error...

Microsoft OLE DB Provider for ODBC drivers error '80040e14'
[Microsoft][ODBC SQL Server] Incorrect syntax near the keyword 'or'.
/verify1.asp, line 5.

Microsoft OLE DB Provider for ODBC drivers error '80040e14'
[Microsoft] [ODBC SQL Server] Unclosed quotation mark before the
character string

Microsoft OLE DB Provider for ODBC Drivers error '80004005'
[Microsoft][ODBC Microsoft Access Driver]

Microsoft JET Database Engine error '80040e14'

چگونگی استفاده از این Errorها را در درسهای بعدی بررسی می کنیم.

Author: Mouse@Shabgard.org

Copyright © 2004 Shabgard.org. All rights reserved.

http://isun.Shabgard.org