حملات Sql Injection

ترجمه و تالیف

Silverhand

Mili2

درس سوم

Silverhand,Mili2

دوستان عزیز تا اینجا یاد گرفتید بفهمید که کجای سایت مورد نظر ما آسیب پذیر هست و از آن آسیب پذیری برای بدست آوردن تعداد **column** ها استفاده کردیم حالا از اینجا به بعد از چندین روش می توانیم نام **column** ها را به دست آوریم و **username** و **pass** را به دست بیاوریم که من در اینجا از یکی از آن روش ها یاد می کنم و دیگر روش ها به صورت **priv8** نزد خودم و گروهم باقی می مانند.

دوستان باید توجه داشته باشید که ما فقط یک نوع **web Application** از نوع **sql** نداریم و چندین نوع **web Application** وجود دارد. مانند:

Ms sql , Access , Oracle , DB2 , Postgres ,.....

البته باز هم هست ولی فکر نکنم زیاد به کارتان بیاید.

چون بیشتر از **ms sql** و **my sql** استفاده می شود. البته به نظر خودم **Access** قوی تر از این دو است چون وب سایت مجلس۸ و بانک کشاورزی و... از این نوع پایگاه داده استفاده می کنند.

*******اما من این مدل سایت ها را هک نمی کنم زیرا سایت های ایرانی هستند*******

خوب بریم سراغ درسمان

خوب حالا فرض کنید در دستور **order by** عدد ۱۵ خطا نداد ولی عدد ۱۶ خطا داد.

۱. فرمان بعدی که میخواهیم آموزش بدهیم دستور **null** است این اسکریپت فقط برای نمایش دادن فرمان های مورد دلخواه ماست و به ما نشان میدهد که در کدام **Column** می تواند اطلاعات فروم را استخراج کنیم.

```
index.phpid=null union all select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
```

و یا

```
index.phpid=union all select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
```

Silverhand,Mili2

-- برای توضیح این فرمان باید بگویم این فرمان را در آخر فرمان ها و خارج از اسکریپتی که تمایل داریم به آن پایان بدهیم اضافه میکنیم.

پس حالا به مرورگر خود نگاه کنید اگر شما هیچ عددی نمی بینید کافیست که در آن اعداد را کمی تغییر دهید (یعنی به قدری کم و زیاد کنید تا سه عدد در صفحه به نمایش درآید). برای مثال بیایید وانمود کنید Column های ۵و۷و۹ الان در حال نمایش هستند.

*******البته دوستان همان طور که در درس اول گفتم روش های زیادی وجود دارد و با یکبار آموزش کسی هکر نمی شود گرچه هک کردن web Application را نمی توان هک گفت(به دلیل ساده بودن)فیلم های زیادی را ببینید... مقالات زیادی را بخوانید... تمرین زیادی بکنید...

تا بتوانید به راحتی نفوذ کنید و مشکلی نداشته باشید*******

خوب درس ما تمام شد بچه ها انشاءالله اگر مدیرا قبول کنند می خواهم یک War Game راه بندازم تا شما رو بسنجم و خوبا رو گلچین کنم برای روز مبادا!! :D

****

راستی این id را Add کنید و یک pm به من بدهید و متن pm به این شکل باشه:

[SQL Injector]

ID: Amin.1991

****