Silverhand,Mili2

Sql Injection حملات

ترجمه

Silverhand

Mili2

درس اول

Silverhand,Mili2

دوستان عزیزی که این مطلب را می خوانند:

۱. این مطلب را با دقت کامل بخوانید.
۲. تمامی این تمرین ها رو با دقت انجام دهید.
۳. اگر مشکلی داشتید به من Pm بدهید.
۴. من دارم یه گروه می سازم و اگه کارتون خوب باشه شما رو به گروهمون دعوت می کنم.
۵. فقط به همین مطلب متکی نباشید.

Silverhand,Mili2

- **اطلاعات پیش زمینه**

۱. امروزه این آسیب پذیری در بیشتر صفحات وب وجود دارد.

۲. این عیب در برنامه های کاربردی و کم توجهی برنامه نویسان در وب است واشکال Data Base و یا Server نیست.

۳. تزریق میتونه وارد Cookies و Forms و پارامتر های آدرس سایت بشه.

- **واقعیت این درس ها**

۱. در تمامی مثال های این درس از بکار گیری دستور های MySQL درست شده.

۲. این درس برای دلایلی همچون چرا سایت ها آسیب پذیرند. واقعا" چطور می شود آنهارا Exploit کرد تهیه نشده .

۳. این درس تهیه شده ، مثال هایی از Sql Injection برای پارامتر های URL هستند.

۴. این درس مقدار کمی مثال از تکنیک های حیله گری را ارائه می دهد.

Silverhand,Mili2

- **قسمت اصلی درس**

بعضی از فرمان هایی که شما باید بدانید

Union All Select

در هم آمیختن دو یا چند دستور در یک پرسش برای به دست آوردن همه ی ردیف ها.

Order By()

برای مرتب سازی ردیف ها بعد از انتخاب کردن یک دستوری که، در حال نمایش است استفاده می شود.

Load_File()

باز کردن یک فایل از سایت یا سرور. برای مثال خواستن فایل .htaccess یا etcpasswd

---

Char()

برای تبدیل string به decimal ascii استفاده میشود.و با load_file ترکیب میشود.

Concat()

کار این دستور ترکیب کردن بیشتر از یک Column در یک خط است و Column های بیشتری مطابق انتخاب شده ها به غیر از عدد برای آنکه بر روی صفحه نمایش دهیم فراهم می کند.

--

Silverhand,Mili2

یک توضیح

"

شکل دیگر یک توضیح

- تزریق یک به یک پارامترها در URL

پس شما یک سایت به آدرس (www.site.com/index.php?id=5) پیدا کردید و دوست دارید اگر این سایت آسیب پزیر باشه با استفاده از روش sql injection به آن کد مخرب تزریق کنید.

۱. برای شروع بررسی این را امتحان کنید(index.php?id=5 and 1=0--)

اگر بعد از به اجرا در آوردن دستور بالا هیچ اتفاقی پیش نیامد و صفحه وب به همان شکل باقی ماند شما می توانید این را امتحان کنید.(index.php?id=')

اگر هیچ یک از کار های بالا عمل نکرد ، یک سایت دیگر را انتخاب کنید.

در غیر اینصورت اگر مرورگر یک صفحه ی خالی و یا صفحه ای حاوی خطا نشان داد باید بدانید که خوش شانس هستید!

در این سایت هایی که ضمیمه شده صفحه ی آسیب پذیر پیدا کنید و توسط فرومی که در سایت آشیانه درست کردم اعلام نمایید.

قابل ذکر است که این مثال ها توسط دوست عزیزم kouros جمع آوری شده.
