



Silverhand,Mili2

حملات Sql Injection

ترجمه

Silverhand Mili2

درس دوم



HACKERZ IR

Iran Hackerz Security Team

Silverhand, Mili2

حالا ما میخواهیم بفهمیم چگونه خیلی از **Column** ها را پیدا کرد و کدام یک نمایش داده میشوند زمانی که یک دستور را انتخاب می کنیم. پس ما می توانیم این را استفاده کنیم
(index.php?id=5 order by 20)

و یا

(index.php?id=5 order by 20--)

انتخاب این دو دستور بسته به آن است که **Web app** به ما خطایی همچون "--20" را می دهد یا نه . اگر داد باید از همان دستور اول استفاده کنید.

اگر در ادامه این دستور هیچ خطایی به شما نشان داده نشد عدد را تا جایی که به شما خطا نشان دهد حالا بدانید که عدد قبل از پیغام خطا تعداد درست **Column** ها را به ما نشان می دهد.