SQL Injection یک روش تزریق (injection) کد است که از یک آسیب پذیری امنیتی در لایه دیتابیسِ یک اپلیکیشن، در جهت حمله استفاده میکند. اگرچه SQL Injection غالبا در حمله به وب سایت ها کاربرد دارد اما از آن میتوان در حمله به هر دیتابیس SQL ای استفاده کرد.

**انتخاب قربانی (مقصد حمله)**

اولین قدم در اجرای یک حمله SQL Injection، پیدا کردن یک وب سایت آسیب پذیر است. این مرحله ممکن است از لحاظ زمانی بیشترین تایم را از کل زمان مورد نیاز برای حمله کامل بخود اختصاص دهد. امروزه اکثر وب سایت ها با استفاده از روش ها و تکنیک های مختلف خودشان را از تهدیدات SQL Injection مصون نگه داشته اند. این بدان معنی است که این مرحله یعنی پیدا کردن یک وب سایت آسیب پذیر، وقت زیادی را از شما میگیرد.یکی از ساده ترین راه های پیدا کردن وب سایت های آسیب پذیر "Google Dorking" نام دارد. یک Dork، در واقع یک درخواست جستجوی خاص برای پیدا کردن وب سایت هایی است که با پارامترهای ورودیِ درون این درخواست، مطابقت دارند. در زیر مثال هایی از Dork هایی آورده شده است که شما میتوانید بوسیله آن ها سایتی آسیب پذیر در برابر حمله SQL Injection پیدا کنید. فقط کافیست که هرکدام از این درخواست ها را درون گوگل سرچ کنید.

## شروع حمله

بعد از آنکه وب سایت اسیب پذیر را شناسایی کردید، نوبت آنست که از تعداد ستون های موجود در دیتابیس SQL آن سایت مطلع شوید و این که چه تعداد از این ستون ها قابلیت پذیرش کاراکتر و یا عبارت ورودی از طرف شما را دارند. عبارت "order by" را در انتهای URL اضافه میکنیم:

## اکسپلویت کردن دیتابیس

در این مرحله شما میدانید که از طریق کدام ستون ها باید مستقیما درخواست خود را تزریق کنید؛ بنابراین میتوانید کار اکسپلویت کردن دیتابیس را اغاز کنید. از این جا به بعد برای اجرای بسیاری از دستورالعمل ها به عبارت union select بسیار نیاز پیدا خواهید کرد. خوب دوستان دیدید انجام SQL Injection آنقدرها هم که از دور به نظر میاد، ترسناک نیست و میشود با یادگیری قواعد بازی و دستورالعمل ها تا حد زیادی کار را به جلو برد.