چرا SQL injection مهم است؟

حمله موفقیت آمیز تزریق SQL می تواند منجر به دسترسی غیرمجاز به داده های حساس ، مانند گذرواژه ها ، جزئیات کارت اعتباری یا اطلاعات شخصی کاربر شود. بسیاری از سناریو های نفوذ نقض در سال های اخیر نتیجه حملات از نوع تزریق SQL بوده است که منجر به آسیب به شهرت و جریمه های قانونی شده است. در برخی موارد ، یک مهاجم می تواند یک در پشتی مداوم در سیستم های یک سازمان به دست آورد ، که اورا قادر می سازد برای مدت طولانی بدون توجه باقی بماند.

1) مثالی از حمله SQLI از نوع Retrieving hidden data

یک برنامه خرید را در نظر بگیرید که محصولات را در دسته های مختلف نمایش می دهد. هنگامی که کاربر روی دسته هدایا کلیک می کند ، مرورگر آنها آدرس اینترنتی را درخواست می کند:

https://insecure-website.com/products?category=Gifts

این باعث می شود که برنامه یک درخواست SQL برای بازیابی جزئیات محصولات مربوطه از پایگاه داده ایجاد کند:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

این دستور SQL از پایگاه داده می خواهد که موارد زیر را برگرداند

1) تمامی جزییات
2) از جدول محصولات
3) جایی که نوع محصول کادو(هدیه) است
4) اندازه متغییر released برابر با 1 می باشد.

به کارگیری released =1 برای پنهان کردن محصولاتی که منتشر نمی شوند استفاده می شود. برای محصولات منتشر نشده ، احتمالاً مقدار این متغییر برابر 0 است. بنتبریان با این کد دستوری مهاجم قادر خواهد بود تمامی محصولات وبسایت را مشاهده کند.

2) مثالی از حمله SQLI از نوع Subverting application logic

دستور زیر را در نظر بگیرید.

```
SELECT * FROM users WHERE username = 'administrator'--' AND password =
''
```

استفاده از – پس `administrator` مهاجم را قادر می سازد چک کردن پاسورد را دور بزند و به سادگی وارد سیستم شود.

3) بازیابی داده از سایر جداول اطلاعاتی

در مواردی که نتایج یک دستور SQL در پاسخ های برنامه بازگردانده شود ، مهاجم می تواند از پتانسیل آسیب SQLI برای بازیابی اطلاعات از جداول دیگر در پایگاه داده استفاده کند. این کار با استفاده از کلمه کلیدی UNION انجام می شود ، که به شما امکان می دهد یک دستور SELECT اضافی را اجرا کرده و نتایج را به دستور اصلی اضافه کند. به عنوان مثال ، اگر برنامه ای درخواست زیر را که حاوی ورودی کاربر "هدایا" است اجرا کند:

```
SELECT name, description FROM products WHERE category = 'Gifts'
```

در ادامه مهاجم قادر است با وارد کردن دستور زیر

```
' UNION SELECT username, password FROM users—
```

این باعث می شود که برنامه همه نام کاربری و گذرواژه ها را به همراه نام و توضیحات محصولات برگرداند.