Date: ۱۴۰۰/۹/۲۸   ۹۷۵۲۱۰۱۸ راستین احسانی Subject: یادداشت کلاسی

★ SQL Injection

← قرار دادن کوئری داخل وب سایت
↳ Query

برای ← ۱- استخراج اطلاعات
۲- بدست آوردن ساختار پایگاه داده

← استخراج دیتا
دستکاری "
نفوذ

★ نمونه‌ای ← دستکاری query لاگین با استفاده از تکنیک semicolon برای تغییر رمز ادمین

★ یک نوع دیگر ← Blind SQL injection ← کورکورانه

http:// ~~~ ?id=۲۳۸

Select * from Products where id=۲۳۸

هدف ایجاد خطا در پایگاه داده است
← تا بخشی از کد نشان داده می‌شود
error reporting

from Users

id=۲۳۸ and 1=1 ← درست
id=۲۳۸ and 1=۲ ← ارور

Blind SQL injection ← با

اسم یکی از جداول Users است.

Date: / / Subject:

* تو خیلی از Framework های معروف بک های SQL هندل می‌شوند. لاراول و....

* Cross site Scripting (XSS)

- براساس ورودی ها مثلاً فرم کامنت

هکر به جای Message

- یک اسکریپت جاوا اسکریپت می‌گذارد و برای کلیه‌ی فرستنده

* البته cross site scripting بلاک می‌شود

- هکر باید با دامین خود سرور اسکریپت بنویسد

* هک؟ - استفاده از هر روشی برای هر نوع فرایندی در سطح وب

* هکر؟ - سارقین
- باج گیران
- آدم های سریع
- جنبش های مردمی و اجتماعی ← anonymous operation
- سازمان های حکومتی
- سازمان های جاسوسی

Date: / /

Subject: .....

* نتایج هک ←

- Deface
- Mass Deface
- Access
- Back Door
- Zone-H