محمد عبدالهی 9530153

1. ورودی زیر با هدف انجام عمل sql injection و تخلیه اطلاعات پایگاه داده و دیدن تمام یوزرها و پسورد آن ها انجام میشود.
بله تزریق کد ارائه شده شرط اولیه برابر درست شده و بقیه عبارت هم کامنت میشود و باعث گرفتن تمام اطلاعات دیتابیس میشود.

2. در این حمله کاربر مخرب سعی دارد تا با تزریق این ورودی به یک خطا دسترسی پیدا کند. این خطا به کاربر این امکان را میدهد اگر که فیلد ایمیل در دیتابیس موجود نباشد با خطای عدم وجود این فیلد رو به رو شده و میتوان از طریق کدهای مربوط به ارور نوع دیتابیس و ورژن آن را بدست آورد اما در صورتی که این فیلد موجود باشد کاربر بازهم میتواند به دیتابیس حمله کرده و اطلاعات را با توجه به ایمیلی که مورد نظر دارد بدست آورد. یا حتی کاربر میتواند با تغییر نام ایمیل به نام فیلد های دیگر موجود در دیتابیس هم دسترسی پیدا کند و اطلاعات آنها را استخراج کند.

3. در این حمله هم کاربر سعی دارد تا با گرفتن یک نوع خطا به اطلاعات دیتابیس دسترسی پیدا کند و از طریق ایجاد یه syntax error اطلاعاتی اعم از نوع دیتابیس و وژرن آن قابل دسترسی خواهد بود.

4. این payload بر روی sql server عمل میکند.
هدف این payload استخراج schema کلی دیتابیس بوده و این schema شامل ساختار کلی دیتابیس بوده یعنی جدول ها و فیلدهای آنها و روابط بین جدول ها و کلیه اطلاعات در مورد ساختار کلی دیتابیس را استخراج کرده و در آخر هم این اطلاعات را با دستور select که در آخر پیلود ما قرار دارد به نوع مناسب تبدیل کرده و نمایش میدهد که فکر میکنم خروجی ما به جای int باید از نوع char باشد.