# OWASP 01 – SQL Injection

## Walkthrough – Shop App

1. Navigate to the new account registration page and create an account
2. From the home page, select one of the items to open the item details page.
   1. Notice that the itemID is placed in the URL
3. Construct a new URL which attempts to break the GET request and probe the database
   1. http://localhost:3000/product?name=junk’
4. The return does not mention field names, so use the following query to discover it
   1. http://localhost:3000/product?name=name' or 1=1; select \* from products; -- c'
5. Use this information to construct a new request to update the item price in the database
   1. http://localhost:3000/product?name=name' or 1=1; update products set price=0 where id=1; -- comment'
6. Then, navigate to the product page for the changed item to see your attack success

## Exercises – Shop App

1. Create a new item in the database ‘Security Book’ made by ‘Tuffy’ price at ’49.99’ description ‘the latest and greatest in computer security knowledge’ using a SQL injection
2. Walk through the process of making a purchase and checking out. Notice that receipts are generated and saved. Create a SQL injection to create a false receipt which includes purchases of two different items with quantity 99. Hint: the database table to hold receipts is called ‘receipts’
3. Update the Shop application to be able to withstand a SQL injection throughout each feature