# OWASP 03 – Sensitive Data Exposure

## Walkthrough – Shop App

1. Navigate to the new account registration page and create an account
2. Add items to your cart and proceed to checkout
3. Complete the checkout form and view your receipt – notice the unnecessary credit card details that are retained by the application
4. Return to the log in page of the application
5. Construct a SQL injection to get all records from the appusers table
   1. a' OR 1=1; SELECT \* from appusers; --c
6. Notice that the appusers table contains personally identifiable information along with usernames and passwords

## Exercises – Shop App

1. Read the created.sql and populatedb.sql files of the application (03-Vulnerable-Shop). What is wrong with the schema?
2. Update the created.sql and populatedb.sql files to fix the issue
3. Update the shop application to reflect the changes in the .sql files to mitigate the sensitive data exposure vulnerability