# OWASP 05 – Broken Access Control

## Walkthrough – Shop App

1. Log in to the application
2. Fill your cart with items and check out
3. From the thankyou page, navigate to View Profile
4. Enter a date range that includes today into the search boxes
5. Search for the receipt
6. Notice that the URL bar contains the user\_id in the GET parameter



1. Log out of this account, and log in to or create another account
2. Fill your cart with items and check out
3. From the thankyou page, navigate to View Profile
4. Enter a date range that includes today into the search boxes
5. Search for the receipt
6. In the URL bar, replace the user\_id with the value from the previous search
7. Notice the receipt that was returned to the front end

## Exercises – Shop App

1. Construct a SQL injection to get the receipts of all users
2. Update the shop viewprofile.ejs template, and the shop application back end to use the user\_id from the appusers table based on the logged in user’s session to get the receipts instead