# OWASP 02 – Broken Authentication

## Walkthrough – Bank App

1. Navigate to the new account registration page
2. Create a new account and log in
3. Notice that the sessionID is in the url
4. Copy and paste the session ID into a text file
5. Clear the cache and local history from your web browser, or open up a private/incognito window
6. Navigate to the new account registration page
7. Create a new account and log in
8. Now, copy and paste the session ID from the previously saved session
9. Notice that the page now reflects the previous user’s account details

## Exercises – Bank App

1. Update the bank application to use a local session cache which rotates the session ID corresponding to the logged in user every time a user has accessed a page with that session ID
2. Update the bank application to remove the session ID from the GET parameter altogether