# OWASP 01 - SQL Injection

## Walkthrough – Bank App

1. Navigate to the new account registration page
2. Perform SQL injection ‘probing’ by supplying the following values to the login form (without quotes):
   1. “ junkdata' ”
3. Use the table names and attributes gathered from the error messages on the client side to construct a new SQL injection string to create an account
   1. “a' OR 1=1; USE users; INSERT INTO appusers(username, password, firstname, lastname, address) VALUES('hacker1', 'hacker1', 'hacker','hacker', 'I hacked you'); INSERT INTO accounts(amount , appuser\_id) VALUES (0.00 , LAST\_INSERT\_ID()); -- this is a comment"
   2. You will receive an error message
4. Try logging in with the account created in step 3. You should see the home page
5. Note the account number of one of the accounts
6. Log out and create a new account using the new account registration page
7. From the home page, navigate to the withdraw box
8. Perform SQL injection ‘probing’ by supplying the following values to the withdrawl amount box (without quotes):
   1. “ junkdata' “
9. Use the table names and attributes gathered from the error messages on the client side to construct a new SQL injection string to withdraw from another account (the one noted in the previous instruction
   1. “1 where accountnumber=<<ACCOUNT\_NUMBER>>;--"
   2. You will notice after executing the withdrawal, the account balance of the account you are currently logged in on does not change
10. Log out and log in to the account that was withdrawn from. You will notice that the withdrawal has been executed on the specified account

## Exercises – Bank App

1. Create a new user account then, add three accounts with zero dollars in each. Then, using a SQL injection, set the balances to be 1,000,000.00
2. Update the populatedb.sql file to add a new account with one million dollars. Create a SQL injection attack to transfer money from that account into one of your own
3. Update the Bank application to be able to withstand a SQL injection throughout each feature