DD1334 Databasteknik

Lab 2: Application Programing and Functional Dependancy

Andreas Gustafsson, Hedvig Kjellström and Michael Minock and John Folkesson

The purpose of Lab 2 is to learn simple application programing with databases and how to model relational data structures based on properties of the data. You will learn How to write code to interface with a database
The recommended reading for Lab 2 is that for Lectures 1-6 .

*Lab 2: **Come prepared to the review session!** Only one try is allowed – if you fail, you are not allowed to try again for a higher grade that session. The review will take 20 minutes or less, so have all papers in order. Passing requires:*

Completed Task 1 with an interface function that does take correct input from the user and makes insertions and deletions to the database, Task 2 with a customer interface that allows customers to see their own shipments but not any more (ie no injections). The program should not crash due to incorrect inputs by the user. Task 3 with a shipment interface that does not allow shipments if the book is not in stock and which keeps track of the stock by decrementing it. If the shipment is not inserted the stock should not be decremented and visa versa. The insertion of shipments using the interface should be made safe from concurrent insertions in different processes by using transactions.

The grades are based on lateness from the date due. See the course web page in for the due dates for the labs and the grading of late assignments.

Lab 2 is intended to take 26h to complete.

Task 1: Basic Application Program

Create your own private copy of Booktown as described in lab 1.

On the course canvas homepage under labs,
there are the code skeletons, customerInterface.py, shipmentInterface.py and interface.py. Start with interface.py and complete the two unfinished methods: *insert*, and *remove*. The program should handle correct user input and you need not worry about other cases here. You only need to show that you can insert or remove tuples from the tables. You will find helpful comments in the skeletons and are encouraged to seek help as needed from the web or you classmates.

Before the review: Comment your code so that you easily can explain what it does. Use descriptive variable names.

At the review: Show the code to the assistant and prepare an execution so that the assistant easily can test the interface. Both group members should be prepared to answer questions about the code.

The code skeletons provided are designed to run in Eclipse IDE on a CSC Ubuntu machine. You are welcome to work on your own machine, but no guarantees are made that they will function out of the box on any computer. The skeletons require a database connector.

For Python on Ubuntu, python-pygresql should work. The simplest way to run the code is to log on to u-shell.csc.kth.se as described above. The python skeleton is extensively commented to explain the code at a tutorial level as well as giving links to web resources that may help in extending it to the other 2 methods.

Task 2: Simple Application Program

Now you should complete the customerInterface.py skeleton. Here we pretend to give the interface to customers to do queries themselves. As ‘security’ we demand they provide a customer_id and name that matches our database. They can then see that customer’s shipment data. You task is to get the input of customer_id and name from the user, check it against the customers table and then print a listing of (shipment_id, ship_date, isbn, title) tuples. Now the program should not crash for incorrect input and should not allow SQL injection attacks. There are many hints in the comments.

Injections are attacks where unanticipated inputs given by the crafty user allow unauthorized access to the database. Protection against these is thus focused on the user input. One protection is to strongly type cast the input, so if you expect an integer you should put the input into an integer variable. Then trying to input text will raise an exception which can be caught. As in

```
try:

            varïblename = int(input("promt: "))

except (NameError,ValueError, TypeError,SyntaxError):

            print("That was not a number.... :(")

            return
```

Notice that python cares about indents. Another way to protect the input is using the built in function to remove escape characters such as ‘ or \:

```
variablename= pgdb.escape_string(raw_input("promt: ").strip())
```

Note that this function only removes some of the offending characters but it is sufficient for you to get the idea of injection protection.

Task 3: Not as Simple Application Program

Now you should complete the shipmentInterface.py skeleton. Here we pretend to give the interface to employees to enter shipments. We want to be sure that simultaneous insertions by different employees at different computers will not put the stock into an inconsistent state. Most of the code is in place but you need to finish the makeShipments function. You should do the same sort of type casting, escape removal and exception raising as on task 2. Here the main new issue is transactions. A transaction should be started at the right point in the code, rolled back if there is any problem and committed if all goes well. The version of SQL we are using for the labs does not have a command to start a transaction instead:

`self.conn.commit()` will both commit the current transaction and start a new one.
`self.conn.rollback()` will do the rollback to the last commit.

The code should ask for the shipment information then test if there is a book to ship then if so insert the shipment and decrement the database. Any failure should not change anything. It should not be possible for one user to check if there is a book then another remove the book from stock before the first user has done all the changes to stock and shipments.

Be prepared to explain why the transactions are started, rolled back, and committed where they are. Also to answer questions like what if we started a new transaction here, (pointing to some line in your code).