

Computer Science E-75
Lecture 4: SQL, Continued
Harvard Extension School
Monday, 3 March 2008

Login Modules

If you use a cookie to "Remember me" on a website, any adversary can go to the computer and present a username and the cookie to the website and log in as you.

Login9.php

Connects to the database

Selects the database (we could refer to a specific database every time, but since we only have one, we can set the database for the duration of the connection)

User login SQL query

Could get all the usernames and passwords and search through that to check if the provided credentials were correct, but we can make MySQL do that, since search is one of its purposes.

Therefore, we make MySQL return "1" if the combination of username and password was found

If the user is logged in, we set the "authentication" flag in their session to TRUE.

If the user wants to store their login

Save username and token in cookies

Record the token in our database

Triple equals (===) checks for equality of value AND of type. (0 == FALSE !== FALSE)

MySQL

CREATE TABLE - To create a table

DROP TABLE - To delete a table

These commands can become very complicated

Therefore, use phpMyAdmin - cs75.net-phpMyAdmin <<https://s75.net/phpMyAdmin/>>

Creating tables in phpMyAdmin

Table types

CHAR (uses a predictable amount of space for each field, regardless of the actual size)

VARCHAR (stores just enough characters for each string)

ENUM (can enumerate types ENUM('MA', 'NH'), - MySQL will accept only MA or NH for this field.

For Zip Code, we don't want to use an INT, because we care about leading zeroes.

Collation - The character encoding

Null - You can force your database to do error checking for you. If you set a field as "NOT NULL", MySQL will yell when you insert a row

without a zip code.

Default - The default value used when an empty field is inserted.

Keys

Primary Key - All rows in that field must be unique

For-free indexing

Make multiple fields a primary key?

Multiple fields may be needed to uniquely identify a row

Index

Optimizes SELECT queries based on that field

(MySQL automatically creates an index for the primary key)

Cuts down on search time as data sets grow large

Unique - This field is unique (imposing constraints)

Full Text - MySQL supports fulltext searches (how to optimize searches on that field).

Attributes -

Unsigned - make type unsigned (can represent higher numbers)

On update current timestamp - gives the current time whenever row is edited.

Extra

Auto-increment (whenever new row is added, this field gets a value one greater than the field value of the previously added row)

Race Conditions

Gone-for-milk concept (One roommate comes home, notices the milk is gone, and goes to buy some milk, the other roommate comes home while the first is out and sees that the milk is gone, and also goes to buy milk. Both come back with milk).

Can effect query databases as well (Money - implement a check to see if withdraw can happen, two queries happen. The first checks, and sees that the withdraw is possible, then the second checks and sees that the withdraw is possible since the first query hasn't changed anything yet. Result is that two withdraws happen, possible resulting in a negative balance.

Solution?

Lock whole table when queried -

Not efficient for very popular sites, with thousands of queries a day. Only one query can happen at a time.

Read lock - people can read, but not write

Write lock - no one can read or write

Use transactions

Do multiple queries (SELECT to check, UPDATE to withdraw) and only save them if all succeed.

Useful to check and modify multiple tables at once

ROLLBACK command tells database to ignore everything since you last called START TRANSACTION

Storage engines

MyISAM - does not support transactions, but has better performance
InnoDB - supports transactions, but with a hit to performance
Engines can be changed after database is created

Project 2

fgetcsv() function in php to use csv files.

Login - Users field, passwords field, uid

Register - Register users (insert info into database)

Get Quotes - Implement 1 php page with form that:

Submits to another page that will get the csv file from yahoo

Parse the file

Display the numbers

Sell stocks - See stocks that we own

If stock is owned, update table to sell and increment cash

Buy stocks - Search for stock to buy

Update portfolio, decrement cash

History - Show user history (possibly another table?)