School of Computing and Information Technology
University of Wollongong

Session: **Autumn 2016**
Lecturer: **Janusz R. Getta**

CSIT115/CSIT815 Database Management and Security
Laboratory 7

Scope

This laboratory includes the tasks related to the applications of `CREATE DATABASE`, `CREATE USER`, and `GRANT` statements of SQL.

This laboratory consists of 2 tasks and specification of each task starts from a new page.

It is strongly recommended to solve the problems included in this specification **before coming to a laboratory class** and bring the preliminary solutions to a laboratory class such that any doubts, question, problems, etc can be discussed with a tutor in a laboratory class. Such procedure allows for more effective use of time spent in a supervised laboratory class.

Prologue

Perform the following actions.

(1) Download and unzip a file `laboratory7-all-files.zip`. You should get the files `Laboratory7.pdf`, `dbcreate7.sql`, and `dbdrop7.sql`. Copy the files to your USB drive such that you can access both files either through command line interface mysql or graphical user interface MySQL Workbench.

(2) Connect to a database server as a user `root` with a password `root`.

(3) Create a database with the same name as a *prefix of your University email account*. For example, if your University email account is `xyz007@uow.edu.au` then a name of a database must be `xyz007`. Note, that if you create a user `xyz007` then you can be absolutely sure that you will get no marks for this laboratory work.

(4) Create three users with the following user names: *prefix of your University email account*`_1`, *prefix of your University email account*`_2`, and *prefix of your University email account*`_3`. For example, if a prefix of your University email account is `xyz007` then the names of users are `xyz007_1`, `xyz007_2`, and `xyz007_3`. All passwords are up to you.

(5) While connected as a user `root`, execute a script `dbcreate7.sql` to create the relational tables later on used in this laboratory class. All relational tables must be located in a database created in step (3).

There is no need to create and to submit any reports from the actions listed above.

Tasks

Task 1 (1 mark)

Implement SQL script `solution1.sql` that performs the following actions.

(1) The script operates on a database created in Prologue.

(2) The script grants a read privilege on entire database *prefix of your University email accoun*t to a user *prefix of your University email account*`_1`. The privilege must be granted such that a user *prefix of your University email account*`_1` is not allowed to grant the same privilege to another user.

(3) Next, the script grants the read and write privileges on a relational table `EMPLOYEE` located in a database *prefix of your University email account* to a user *prefix of your University email account*`_2`. The privileges must be granted such that a user *prefix of your University email account*`_2` is able to grant the same privileges to the other users.

(4) Next, the script grants a privilege to create relational tables located in a database *prefix of your University email account* to a user *prefix of your University email account*`_3`. The privilege must be granted such that a user *prefix of your University email account*`_3` is not allowed to grant the same privilege to another user.

(5) Next, the script grants a privilege to read the columns (`ENUM`, `FNAME`, `INITIALS`, `LNAME`) in a relational table `EMPLOYEE` located in a database *prefix of your University email account* to a user *prefix of your University email account*`_3`. The privilege must be granted such that a user *prefix of your University email account*`_3` is not allowed to grant the same privilege to another user.

(6) Finally, the script lists all privileges granted to the users *prefix of your University email account*`_1`, *prefix of your University email account*`_2`, and *prefix of your University email account*`_3`.

Deliverables

A file `solution1.rpt` with a report from processing of SQL script `solution1.sql`. The report MUST have no errors and the report MUST list all SQL statements processed.

A report that contains no listing of executed SQL statements scores no marks and report that contains errors also scores no marks !

Task 2 (1 mark)
Use mysql command line interface to perform the following actions.

(1) Start mysql command line interface and connect as a user *prefix of your University email account*_1.

(2) Execute a command `tee solution2.rpt`.

(3) Execute any SQL statement that shows the validity of any privilege granted to a user *prefix of your University email account*_1 in the previous task.

(4) Execute any SQL statement that shows a lack of privilege to access a database *prefix of your University email account* in write mode by a user *prefix of your University email account*_1.

(5) Exit mysql command line interface.

(6) Start mysql command line interface and connect as a user *prefix of your University email account*_2.

(7) Execute a command `tee solution2.rpt`.

(8) Execute any SQL statement that shows the validity of write privilege on a relational table `EMPLOYEE` located in a database *prefix of your University email account* and granted to a user *prefix of your University email account*_2 in the previous task.

(9) Execute any SQL statement that shows a lack of write privilege on a relational table `ADMIN` located in a database *prefix of your University email account* by a user *prefix of your University email account*_2 in the previous task.

(10) Exit mysql command line interface.

(11) Start mysql command line interface and connect as a user *prefix of your University email account*_3.

(12) Execute a command `tee solution2.rpt`.

(13) Execute any SQL statement that shows the validity of privilege to create a relational table located in a database *prefix of your University email account* and granted to a user *prefix of your University email account*_3 in the previous task.

(14) Execute any SQL statement that shows a lack of privilege to create a relational table in a database `csit115` by a user *prefix of your University email account*_3.

(15) Execute any SQL statement that shows the validity of privilege to read the columns (`ENUM`, `FNAME`, `INITIALS`, `LNAME`) from a relational table `EMPLOYEE` located in a database *prefix of your University email account* and granted to a user *prefix of your University email account*`_3` in the previous task.

(16) Execute any SQL statement that shows a lack of privilege to read a column other than (`ENUM`, `FNAME`, `INITIALS`, `LNAME`) from a relational table `EMPLOYEE` located in a database *prefix of your University email account* by a user *prefix of your University email account*`_3`.

(17) Execute a command `notee`.

(18) Exit mysql command line interface.

Deliverables

A file `solution2.rpt` with a report from processing of SQL statements implementing the actions listed above. The report MUST list all SQL statements processed.

A report that contains no listing of executed SQL statements scores no marks !

Note, that processing of some of SQL statements must return ERROR messages !

End of specification