Controlled sharing of information in a database

1 Overview

This lab introduces methods of using access control mechanisms to limit the sharing of information within a database. In this lab, you will perform the duties of a database administrator (DBA) working for a company that is implementing an online database to manage information about the company and its employees.

The company has an information security policy that you, as the DBA, must ensure is not violated by employees accessing the online database. This security policy is defined below, as are other management directives that prescribe access you are to provide to users of the database.

1.1 Security Policy

Senior management of the company defined an *information security policy* that limits access to sensitive company information. Your job is to provide employees access to the new database, but without violating the company's previously established information security policy, which includes the following directives:

- With the exception of HR, Finance and the president, employee's should not be able to observe other's salaries.
- Salary ranges for jobs shall not be observable except by HR, the president and the head of departments having employees holding those jobs.
- Only the president can add or change company departments and their locations.
- Only the president and HR can add or modify authoritative company records for each employee and the jobs that they might hold.
- Only the president and HR can view information about employee dependents (e.g., family information).

Note that the above policy has been in place long before the database was developed. Your are responsible for ensuring the policy is properly reflected within the database.

Company management has decided that the new database will be the authoritative record of company information, and thus they have concern about its implementation and structure. Management has issued the following security policy directives regarding the database itself:

- In order to maintain the integrity of its implementation, only the DBA is authorized to change the structure of the database and to provide users with access to data within the database.
- To ensure the availability of critical corporate information, the HR department shall be able to directly update the database to add and modify employee-related records and records related to the jobs that employees might perform.

To facilitate maintenance of the database, the DBA may update content at the direction of authorized individuals, e.g., the President can direct the DBA to modify department information.

1.2 Other Management Directives

In addition to ensuring the online database does not lead to violations of the security policy, you have been directed to make selected information from the database available for viewing by all employees. This is primarily for efficiency. For example, this would allow employee email and work phone numbers to be directly accessed from the database rather than separately distributing copies of that information. All employees shall be able to view:

- Employee name, email, phone, department, employee_id, and manager_id.
- All information about departments and their locations

Note that the "availability" policy stated earlier also requires that HR be able to update employee and job records.

Providing users with access to other information to which they are authorized is not your primary responsibility. For example, if the head of a department is not able to use the database to view the salary range for his department's jobs, that may be inefficient and inconvenient, but this would not violate the information security policy. However, if a department head can view the salary range of another department, that would be a violation of the security policy.

In this lab, you are not being directed to make salary range information available to heads of departments. Providing such access is challenging because SQL does not support a WHERE clause when establishing grants for a user account. To provide access to salary ranges for a specified department, you could consider creating a VIEW with employee job IDs, titles, and salary ranges. Then, grant user access to this VIEW to the head of that department. But you are not being asked to do that for this lab.

2 Lab Environment

In order to run the lab enter the following command from the labtainer-student directory:

labtainer db-access

2.1 Networked computers

The lab includes several networked computers. The "database" computer containers a MySQL database. A set of workstations are connected to the database computer on a LAN. The computers on the network can name each other using their names, e.g., "ping database" from one of the workstations.

2.2 Initial Database

The initial roll-out of the database includes information about employees and departments within the company. This information is organized into a MySQL database named myco with tables as follows: countries, departments, dependents, employees, jobs, locations, and regions. ***** a full description of the database can be viewed in the appendix section at the end of this document.** The database may also be viewed using the mysql-workbench tool described below in section 3.2, "Explore".

The previous DBA has defined and populated these tables, but left the database in a state that allows all users to access all information. You are required to establish access controls to ensure the policy is not violated and that users have access to information per the management directives.

2.3 Database Users

The lab environment includes workstations assigned to a subset of the company's employees. You will use these workstations to test and demonstrate controlled access to the database in accordance with the security policy and management directives. The initial users defined for this lab are:

Employee Name	Department	Job Title	Username	Password
Steven King	Executive	President	steven	pass4steven
Susan Mavris	Human Resources	HR Representative	susan	pass4susan
Nancy Greenberg	Finance	Finance Manger	nancy	pass4nancy
David Austin	IT	Programmer	david	pass4david
You	IT	DBA	admin	admin

3 Tasks

3.1 Prelab quiz

This lab includes a quiz developed to help you understand how the policy should be enforced before you perform the lab. Run the following command at the terminal from which you started the lab.

```
quiz -l db-access
```

3.2 Explore

Access the database from the different components and different users and note how all users have full access to the database. For example, from the finance computer, use:

```
mysql -h database -u nancy -ppass4nancy
```

to start a MySQL session as Nancy.

On the "database" computer, start a MySQL session as admin to explore and set user permissions:

```
mysql -u admin -padmin
```

If you prefer a GUI-based view of the database and its tables, you may use the mysql-workbench tool, which is installed on the "database" computer:

```
mysql-workbench &
```

Note that even if you use the GUI on the database computer, you will still be asked to run mysql commands on the other computers.

3.3 Control access to the database

As the DBA you must configure the database to enforce the information security policy that was stated in the Overview section, and to provide users with access to data as stated in the "Other Management Directives" subsection.

- Use SQL commands such as REVOKE and GRANT to change user permissions per the security policy. Don't forget to use FLUSH PRIVILEGES to apply your changes.
- Remember that all users are required to have access to view employee related information including name, email, phone, department, employee_id, and manager_id.

3.4 Check your work

The lab includes automated assessment via which you can check your work against the lab goals. Use the following command at the terminal from which you started the lab:

checkwork

NOTE: Inside of each of the workstations there is a <person>.sql file. These files are used for the purpose of checkwork. DO NOT MODIFY these files.

4 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

stoplab

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor.

Appendix

Database Schema

countries				
Field	Type	Null	Key	Extra
country_id	char(2)	NO	Primary	
country_name	varchar(40)	YES		
region_id	int(11)	NO	Foreign	

departments				
Field	Type	Null	Key	Extra
department_id	int(11)	NO	Primary	auto_increment
department_name	varchar(30)	NO		
location_id	int(11)	YES	Foreign	

dependents				
Field	Type	Null	Key	Extra
dependent_id	int(11)	NO	Primary	auto_increment
first_name	varchar(50)	NO		
last_name	varchar(50)	NO		
relationship	varchar(25)	NO		
employee_id	int(11)	NO	Foreign	

employees				
Field	Type	Null	Key	Extra
employee_id	int(11)	NO	Primary	auto_increment
first_name	varchar(20)	YES		
last_name	varchar(25)	NO		
email	varchar(100)	NO		
phone_number	varchar(20)	YES		
hire_date	date	NO		
job_id	int(11)	NO	Foreign	
salary	decimal(8,2)	No		

manager_id	int(11)	YES	Foreign	
department_id	int(11)	YES	Foreign	

jobs				
Field	Type	Null	Key	Extra
job_id	int(11)	NO	Primary	auto_increment
job_titile	varchar(35)	NO		
min_salary	decimal(8,2)	YES		
max_salary	decimal(8,2)	YES		

locations				
Field	Type	Null	Key	Extra
location_id	int(11)	NO	Primary	auto_increment
street_address	varchar(40)	YES		
postal_code	varchar(12)	YES		
city	varchar(30)	NO		
state_province	varchar(25)	YES		
country_id	char(2)	NO	Foreign	

regions				
Field	Type	Null	Key	Extra
region_id	int(11)	NO	Primary	auto_increment
region_name	varchar(25)	YES		