Lab 12 (Optional) - Admin and Security

Due May 16 at 11:59pm **Points** 44 **Questions** 9
Available after May 5 at 9am **Time Limit** None **Allowed Attempts** Unlimited

Instructions

This lab makes use of some basic security commands and functionalities of MySQL. We will be using the Largeco database from Lab 11 on Optimization. Please refer to that lab for a description of the dataset.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
KEPT	Attempt 2	1,549 minutes	10 out of 44 *
LATEST	Attempt 2	1,549 minutes	10 out of 44 *
	Attempt 1	1,461 minutes	0 out of 44 *

* Some questions not yet graded

Score for this attempt: **10** out of 44 *
Submitted May 7 at 11:23am
This attempt took 1,549 minutes.

Part 1: Views and Access Permissions

Question 1 **5 / 5 pts**

Add a new table to the Largeco database for USER_ACCOUNT. The table should track:

1. Username
2. First name
3. Last name
4. Enumeration of "employee" or "customer"
5. Foreign key reference to EMP_NUM in the LGEMPLOYEE table
6. Foreign key reference to CUST_CODE in the LGCUSTOMER table
7. Password

The "password" field needs to be a VARBINARY or BLOB datatype since we are storing hashed passwords there.

Leave the password field blank for now.

Populate your USER table with data from the lgcustomer and lgemployee table. Add 5 entities of each type "employee" and "customer".

Please paste your table creation DDL SQL code into the box below.

Your Answer:

```
use largeco;

CREATE TABLE USER_ACCOUNT(
   Username INT AUTO_INCREMENT,
   FName VARCHAR(50),
   LName VARCHAR(50),
   EMPorCUST ENUM('customer', 'employee'),
   EMP_NUM DECIMAL(6,0),
   CUST_CODE DECIMAL(38,0),
   Password VARBINARY(10),
   PRIMARY KEY ( Username ),
   FOREIGN KEY (EMP_NUM) REFERENCES lgemployee(EMP_NUM),
   FOREIGN KEY (CUST_CODE) REFERENCES
lgcustomer(CUST_CODE)
);

#Write a stored proceedure
#5 employees 5 Customer and insert into user acct
#select all row from employee
#limit to 5
```

```
#select all row from customer
#limit to 5
#insert into USER_ACCOUNT


INSERT INTO user_account (FName, LName, EMPorCUST, EMP_NUM,
Password)
SELECT EMP_FNAME, EMP_LNAME, 'employee', EMP_NUM,
'Password'
FROM lgemployee
LIMIT 5;

INSERT INTO user_account (FName, LName, EMPorCUST,
CUST_CODE, Password)
SELECT CUST_FNAME, CUST_LNAME, 'customer', CUST_CODE,
'Password'
FROM lgcustomer
LIMIT 5;
```

Question 2

5 / 5 pts

Create a VIEW "lg_recent_cust_purchases" that shows a joined table of recent customer purchases with the following fields:

1. Customer code, first name and last name
2. Invoice Number, Invoice Date
3. Each invoice line including line quantity and price
4. Product SKU, product description and product price

12#2.JPG (https://cilearn.csuci.edu/files/2877099/download)

Question 3

Not yet graded / 3 pts

Create a new MySQL user for your database. This user is a manager. Grant the manager user full access to the database.

Please paste your user creation and privileges DDL code below.

Your Answer:

use largeco;

CREATE USER 'Manager'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON * . * TO 'Manager'@'localhost';

localhost Manager	Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y
localhost mysql.infoschema	Y N N N N N N N N N N N N N N N N
localhost mysql.session	N N N N N N N Y N N N N N N N Y N N
localhost mysql.sys	N N N N N N N N N N N N N N N N N
localhost root	Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y

Question 4

Not yet graded / 3 pts

Create a new MySQL user for your database. This user is a regular employee. Grant the employee read only access to the database with the exception of LGINVOICE, LGLINE and LGCUSTOMER, for which they should be allowed to create and update records as well. The employee should also be prevented from accessing LGSALARY_HISTORY.

Please paste your creation and privileges SQL code below.

Your Answer:

use largeco;

SET PERSIST partial_revokes = ON;

CREATE USER 'Employee'@'localhost' IDENTIFIED BY 'password';

GRANT SELECT ON * . * TO 'Employee'@'localhost';
GRANT CREATE, UPDATE ON largeco.lginvoice TO 'Employee'@'localhost';
GRANT CREATE, UPDATE ON largeco.lgline TO 'Employee'@'localhost';
GRANT CREATE, UPDATE ON largeco.lgcustomer TO 'Employee'@'localhost';

REVOKE SELECT ON largeco.lgsalary_history TO 'Employee'@'localhost';

Question 5

Not yet graded / 3 pts

Create a new MySQL user for your database. This user is a seasonal employee. Grant the employee read only access to the custom view "lg_recent_cust_purchases" only.

Please paste your creation and privileges SQL code below.

Your Answer:

use largeco;

CREATE USER 'SeasonalEmployee'@'localhost' IDENTIFIED BY 'password';

GRANT SELECT ON largeco.lg_recent_cust_purchases TO 'SeasonalEmployee'@'localhost';

select * from mysql.user;

Part 2: Security Procedures and Functions

For this section, we will be writing a security procedure to encrypt and decrypt data, a procedure to report on permissions, and a function to check for a correct password.

Unanswered

Question 6

Not yet graded / 5 pts

Create a procedure "lg_encrypt_field_data" that takes in a table, primary key value, field, string data value, and passphrase and then uses AES encryption. Have the procedure put the encrypted value in the target field and then return the encrypted hash value.

Please upload a screenshot of your procedure and CALLs to the encrypt all user passwords in your USER table.

Unanswered

Question 7

Not yet graded / 5 pts

Create a procedure "lg_decrypt_field_data" that takes in a table, primary key value, field and passphrase and returned the unencrypted contents of the target field.

Please upload a screenshot of your procedure and a CALL to the decrypt a user password in your USER table.

Unanswered

Question 8

Not yet graded / 5 pts

Create a function that takes in a user id, password string and passphrase, and returns whether that password string is, in fact, the user's unencrypted password.

Please upload a screenshot of your function and select calls showing both success and failure in guessing a password.

Question 9

Not yet graded / 10 pts

Part 3: Find a Recent Leak

For this question, briefly research a well known security breach, and explain:

1. The type and kind of data stolen
2. The potential implications for that stolen data
3. How the breach occurred (with reference to specific technical details)
4. What the actual implications were for the entity from which the data was stolen.

250 words minimum.

Your Answer:

A engineer in Seattle hacked into a server holding customer information for Capital One. They were able to obtain the personal data of over 100 million people. According to the court papers and Capital One, They stole 140,000 Social Security numbers and 80,000 bank account numbers.

The implications could mean that people are permanently exposed to information being used or sold online. Today information is floating out on these servers and we are hoping the business we give our information to is secure. With more and more of these breaches going on, we really need to make sure we are not just supplying our information to anyone.

They had gained access to sensitive data through a "misconfiguration" of a firewall on a web application. That allowed the hacker to communicate with the server where Capital One was storing its information, and obtain customer files. Information posted on social media shows they worked at one time for Amazon, as a engineer for the same server business that court papers said Capital One was using.

Quiz Score: **10** out of 44