Assignment 2

CSCE 4357/5933: Database Systems Security

**Applying Access Controls to a MySQL Database**

(Spring 2023)

**Due Date: 03/15 @ 11:59pm | Points:** **100**  **| Late Policy: 10%**

**NOTE: Please write everything by your own and do not copy/paste, avoid plagiarism.**

# **Please, follow the guidelines in** “[**CSCE4357/5933-Assignment-2 - DB Guidence.pdf**](https://unt.instructure.com/courses/80527/files/20499567?wrap=1)what to submit.

# User Accounts:

## **a). [15pts] local-system-admin**

1. Login shall be allowed from IP address: `127.0.0.1` or localhost (default).

* In MySQL Workbench, open the "Users and Privileges" panel by clicking on the "Server" in the toolbar of the home screen.
* Select the user account for which you want to allow login from the specific IP address.
* In the "Login" tab, set the "Limit to Hosts Matching" field to 127.0.0.1 or localhost.

1. Only one session shall ever be allowed to connect to this account.

* In the "Account Limits" tab, set the "Concurrent connections" field to 1.

1. All global privileges.

* In the "Administrative Roles" tab , check the "DBA" checkbox to grant all global privileges.

1. All privileges on all tables.

* In the "Schema Privileges" tab, click on the "Add Entry" button.
* Select the schema that contains the tables you want to grant privileges for.
* Select all privileges checkboxes under the "Privileges" section, such as "SELECT", "INSERT", "UPDATE", "DELETE", etc. In this case, we can use the "Select \*ALL\*" button.
* Click on the "Apply" button to save the changes.

1. Password shall be a random string of **sufficient length**, stored offline on paper or a USB key.

* I have stored the password offline on paper.

**Rationale**: The use of this account shall be limited to short periods of maintenance, or emergencies.

The above user account configuration in MySQL Workbench for Local-System-Admin aims to ensure the security and integrity of the database.

The IP address restrictions and session limitations help prevent unauthorized access by limiting access to only the specified IP address, thus ensuring that only one session is allowed to connect to the user account.

Granting all global privileges and privileges on all tables in the database to the user account is necessary for allowing the user to perform all necessary tasks. However, granting all privileges to all tables could pose a security risk, so, it is important to ensure that the user account is secure, and password protected.

Storing the password offline on paper ensures that it is not susceptible to cyberattacks or hacking attempts. Using a strong and unique password of sufficient length also adds another layer of security to the user account.

In summary, the rationale behind this configuration is to prevent unauthorized access to the database, providing the user with the necessary privileges to perform their tasks, and ensuring the security and integrity of the database.

Top of Form

## **b). [15pts] data-entry**

1. Login shall be allowed ONLY from the local network, hosts matching `192.168.1.\*`.

* In MySQL Workbench, open the "Users and Privileges" panel by clicking on the "Server" in the toolbar of the home screen.
* Select the user for which you want to restrict login to the local network.
* In the "Login" tab, set the "Limit to Hosts Matching" field to 192.168.1.% to allow connections only from hosts matching 192.168.1.\*.

1. User shall be allowed ONLY to `INSERT, UPDATE` to database `terrorismdb`.

* In the "Schema Privileges" tab, click on the "Add Entry" button.
* Select the "terrorismdb" database.
* Select only the "INSERT" and "UPDATE" checkboxes under the "Object Rights" section.
* In the "Administrative Roles" tab, do not select any administrative roles.
* Click on the "Apply" button to save the changes.

**Rationale:** This user is meant to only enter new entries should such an automatically updating system be devised.

The above user account configuration in MySQL Workbench for data-entry aims to limit access and restrict the user's privileges to only the necessary actions for their job function.

Restricting login to only the local network through the "Limit to Hosts Matching" field ensures that the user can only access the database from a specific IP range, reducing the risk of unauthorized access. This helps to prevent outside attacks and protects the database from being compromised.

Limiting the user's privileges to only INSERT and UPDATE actions in the "terrorismdb" database helps by restricting their ability to modify or manipulate data beyond what is necessary for their job function. This reduces the risk of human error or intentional data tampering by the user, ensuring the integrity of the database.

Not granting any administrative roles to the user ensures that they do not have any additional privileges beyond what is required. This further restricts their ability to perform any unintended actions that could compromise the security of the database.

In summary, the rationale behind this configuration is to limit the user's access and privileges to only what is necessary, reduce the risk of unauthorized access and data tampering, and maintain the security and integrity of the database.

Top of Form

## **c). [15pts] data-view**

1. Login shall be allowed ONLY from the local network, hosts matching `192.168.1.\*`.

* In MySQL Workbench, open the "Users and Privileges" panel by clicking on the "Server" in the toolbar of the home screen.
* Select the user for which you want to restrict login to the local network.
* In the "Login" tab, set the "Limit to Hosts Matching" field to 192.168.1.% to allow connections only from hosts matching 192.168.1.\*.

1. User shall be allowed ONLY to `EXECUTE, SELECT, SHOW VIEW` from `terrorismdb`.

* In the "Schema Privileges" tab, click on the "Add Entry" button.
* Select the terrorismdb database.
* Select only the "EXECUTE", "SELECT", and "SHOW VIEW" checkboxes under the "Object Rights" section.
* In the "Administrative Roles" tab, do not select any administrative roles.
* Click on the "Apply" button to save the changes.

**Rationale**: This user is meant to retrieve and display data. It can also make reports and summarize data.

The user "data-view" has been configured with restrictions to ensure that login is allowed only from the local network and to grant limited privileges on the database "terrorismdb".

The first configuration ensures that login is only allowed from hosts matching the local network's IP address, which can help prevent unauthorized access from outside sources.

The second configuration grants the user limited privileges to execute, select, and show views on the "terrorismdb" database. This ensures that the user can only perform the necessary actions required for their data viewing tasks, reducing the risk of accidental or intentional modification or deletion of the data.

By implementing these restrictions, the "data-view" user can access the necessary data while maintaining the security and integrity of the database.

## **d). [55pts] data-backup**

1. Login shall be allowed from `127.0.0.1` only.

* In MySQL Workbench, open the "Users and Privileges" panel by clicking on the "Server" in the toolbar of the home screen.
* Select the user account for which you want to allow login from the specific IP address.
* In the "Login" tab, set the "Limit to Hosts Matching" field to 127.0.0.1 or localhost.

1. They have the following global privileges: `EVENT, LOCK TABLES, SELECT, SHOW DATABASES`

* In the "Administrative Roles" tab, select the "Event Scheduler", "Lock Tables", "Select", and "Show Databases" checkboxes. Or you can select the Role "BackupAdmin".

1. User shall be allowed ONLY to `SELECT` from `terrorismdb`.

* In the "Schema Privileges" tab, click on the "Add Entry" button.
* Select the terrorismdb database.
* Select only the "SELECT" checkboxes under the "Object Rights" section.
* Click on the "Apply" button to save the changes.

1. Backup tasks shall be automated.

* Click on the "Server" menu and select "Data Export".
* In the "Data Export" wizard, select the "Export to Self-Contained File" option and click on the "Start Export" button.
* In the "Select Objects" screen, select the database or databases that want to include in the backup. We can also choose to include or exclude specific tables, views, or stored procedures.
* In the "Options" screen, select the backup options that we want to use. We can choose to include or exclude data, select the format of the backup file, and specify compression options.
* In the "Export Progress" screen, monitor the progress of the backup process.
* Once the backup process is complete, we can find the backup file in the location that we specified in the "Options" screen.
* To restore the backup file, click on the "Server" menu and select "Data Import". In the "Data Import" wizard, select the backup file that we want to restore and follow the instructions in the prompts to restore the database.

1. Human login shall be limited to emergencies.

* We can set up a separate emergency user account with limited privileges and use it only in emergencies. For, example local-system-admin can be used for emergencies.

1. Backups shall be performed to a hardware-controlled cold storage array that maintains a **time period** worth of backups before they overwrite the other media.

* We can perform backups to a hardware-controlled cold storage array using the built-in MySQL Workbench Backup feature.

1. Password shall be a random string of **sufficient length**, stored offline on paper or a USB key.

* I have stored the password on paper.

**Rationale**: This user is meant to back up the database **periodically**, and nothing more.

The rationale for the "data-backup" user that we have created is as follows:

1. Limiting login to a specific IP address is a security measure that helps to prevent unauthorized access to the database. By allowing login from only the local machine, we ensure that only authorized users have access to the server.
2. The selected global privileges, "EVENT, LOCK TABLES, SELECT, SHOW DATABASES" are necessary for performing backups of the MySQL server. The "Event Scheduler" privilege is for scheduling backup events, the "Lock Tables" privilege is to lock tables during backups to prevent data inconsistencies, and the "Select" and "Show Databases" privileges are to access and select the appropriate databases and tables for backup.
3. Restricting the user to only use "SELECT" action on the "terrorismdb" database is to ensures that the user cannot modify the data in the database but can only view it.
4. Automating backup tasks is a best practice that helps to ensure that backups are performed regularly and consistently. The user has selected the built-in MySQL Workbench backup feature to perform backups and has specified the backup options that they want to use.
5. Limiting human login to emergencies is a security measure that helps to prevent unauthorized access to the MySQL server. The user suggests setting up a separate emergency user account with limited privileges and using it only in emergencies.
6. Storing backups in a hardware-controlled cold storage array is a best practice that ensures that backups are stored in a secure and reliable location. The user suggests using the built-in MySQL Workbench backup feature to perform backups to a hardware-controlled cold storage array.
7. Storing passwords offline on paper or a USB key is a security measure that helps to prevent unauthorized access to the MySQL server. The user suggests storing the password on paper, which is a secure and reliable method of storing passwords offline.

The user "data-backup" was created to manage backups of the MySQL database for the "terrorismdb" schema. This user is assigned specific privileges to perform backup tasks, but only has limited access to the database. The user is also required to log in from a specific IP address and has a password stored offline on paper, which enhances the security of the backup process. Additionally, the user has been set up with an emergency login account that is only to be used in emergencies. All these measures help to ensure that the backup process is secure, reliable, and can be carried out automatically as required.

# **Notes**

* Bolded words are standards of time, security, or other quantitative things that are up to you, the implementer of these recommendations, to decide.
* Please use the supporting document “[CSCE4357/5933-Assignment-2 - DB Guidence.pdf](https://unt.instructure.com/courses/80527/files/20499567?wrap=1)” that I have shared in canvas for further guidelines.

# References and Citations

“NVD - Control - AC-5 - SEPARATION OF DUTIES.” *NVD - CVE-2017-5638*, nvd.nist.gov/800-53/Rev4/control/AC-5.