# Apply filters to SQL queries

## Project description

My organization wants its systems secure. It is my job to ensure that systems are safe and secure, investigate all potential security issues and update employee computers as needed. Examples of how I have utilized SQL filters to carry out security-related tasks are shown in the following phases.

The organization database contains the following two tables:

* log\_in\_attempts
* employees

## log\_in\_attempts

The log\_in\_attempts table has the following columns:

* event\_id: The identification number assigned to each login event
* username: The username of the employee
* login\_date: The date the login attempt was recorded
* login\_time: The time the login attempt was recorded
* country: The country where the login attempt occurred
* ip\_address: The IP address of that employee’s machine
* success: The success of the login attempt; FALSE indicates a failed attempt

In the MariaDB shell, these columns are returned as:



## employees

The employees table has the following columns:

* employee\_id: The identification number assigned to each employee
* device\_id: The identification number assigned to each device used by the employee
* username: The username of the employee
* department: The department the employee is in
* office: The office the employee is located in

In the MariaDB shell, these columns are returned as:

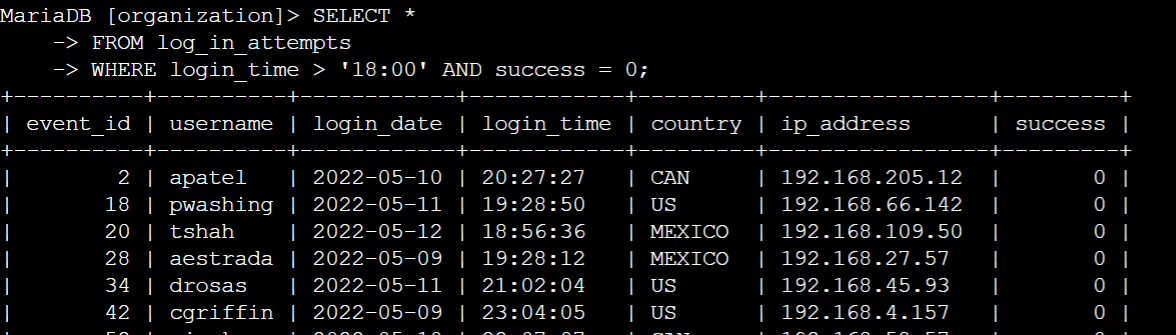


## Retrieve after hours failed login attempts

There was a potential security incident that occurred after business hours (after 18:00). All after

hours login attempts that failed need to be investigated.

The following snippet demonstrates how I created a SQL query to filter for failed login attempts that occurred after 1800 hours.



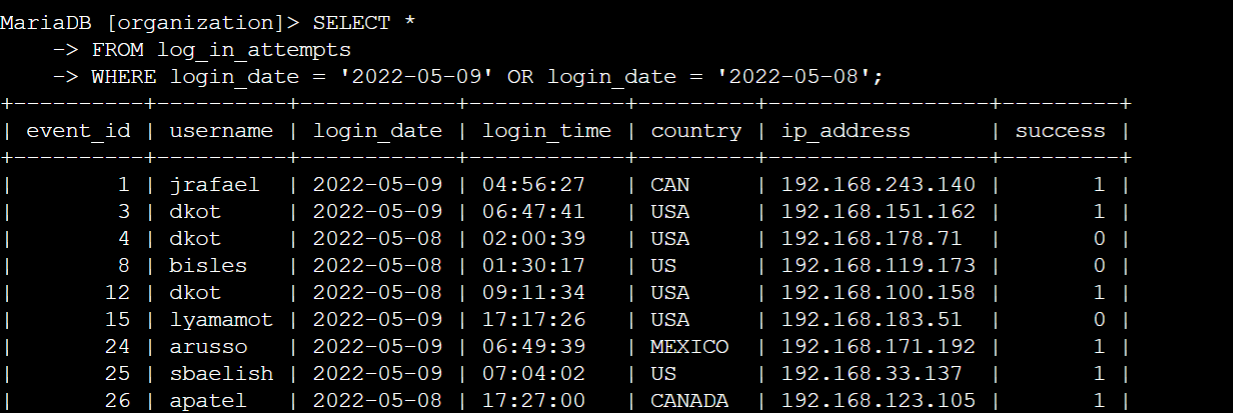
The first part of the snippet is my query, and the second part is the output. First, I selected the data from the log\_in\_attempts table. Then, I used the WHERE clause combined with an AND operator to filter my results based on two conditions. First condition is login\_time > '18:00' and the second condition is success = FALSE.

## Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. Any login activity that happened on 2022-05-09 or on the day before needs to be investigated.

The following snippet demonstrates how I created a SQL query to filter for login attempts that occurred on specific dates.

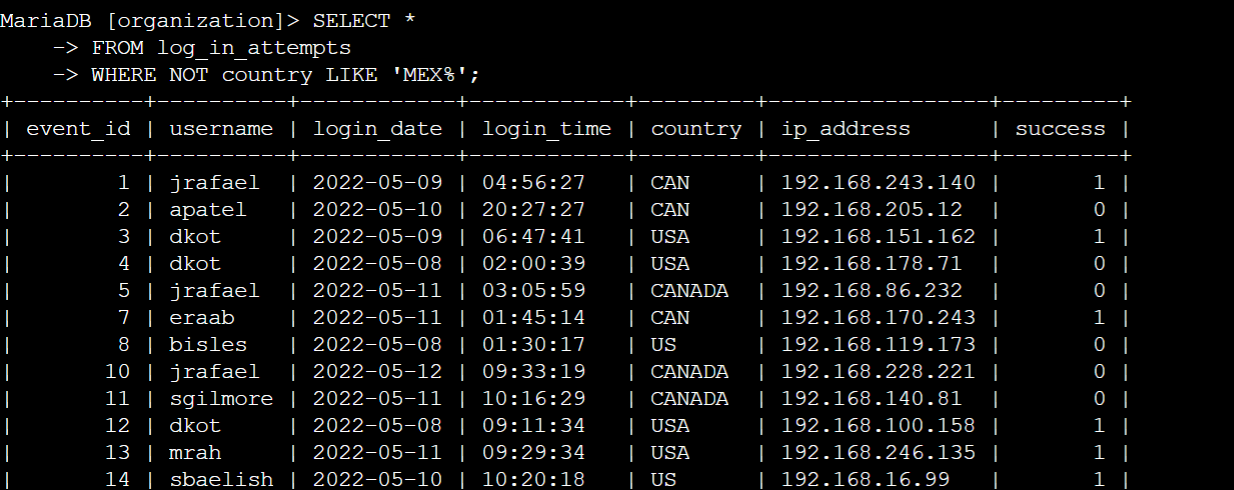
The first part of the snippet is my query, and the second part is the output. This query returns all login attempts that occurred on 2022-05-09 or 2022-05-08. First, I selected the data from the log\_in\_attempts table. Then, I used the WHERE clause combined with an OR operator to filter my results based on two conditions. First condition is login\_date = '2022-05-09' and the second condition is login\_date = '2022-05-08'.



## Retrieve login attempts outside of Mexico

After investigating the organization’s data on login attempts, I believe there is an issue with the login attempts that occurred outside of Mexico. These login attempts should be investigated.

The following snippet demonstrates how I created a SQL query to filter for login attempts that occurred outside of Mexico.

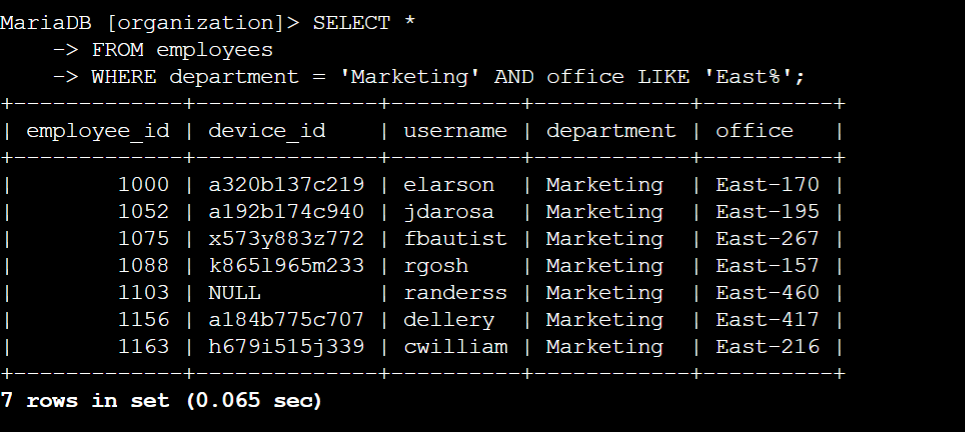


The first part of the snippet is my query, and the second part is the output. This query returns all login attempts that occurred in countries other than Mexico. First, I selected the data from the log\_in\_attempts table. Then, I used the WHERE clause combined with an NOT operator to filter for countries other than Mexico. I used LIKE with MEX% as the pattern to match because the dataset represents Mexico as MEX and MEXICO.

## Retrieve employees in Marketing

My team wants to update the computers for certain employees in the Marketing department. To do this, I have to get information on which employee machines to update.

The following snippet demonstrates how I created a SQL query to filter for employee machine details from the employees table in the Marketing department in the East building.



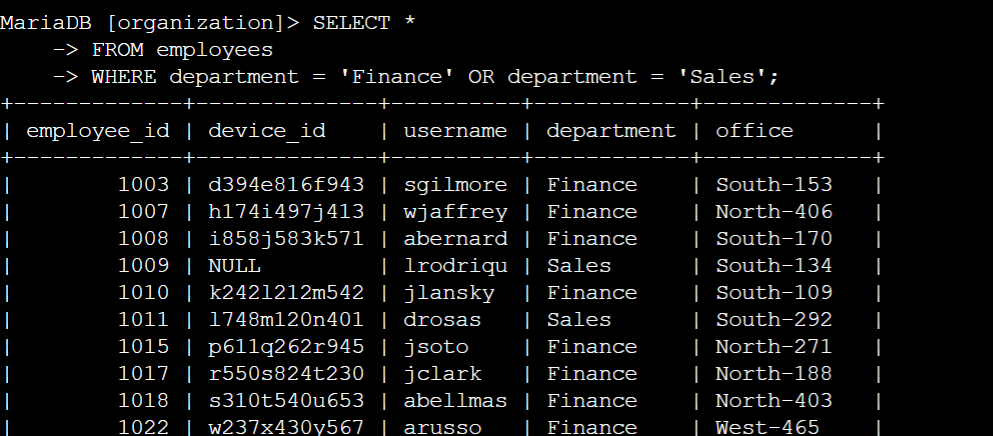
The first part of the snippet is my query, and the second part is the output. This query returns all employees in the Marketing department in the East building. First, I selected the data from the employees table. Then, I used the WHERE clause combined with an AND operator to filter my results based on two conditions. First condition is department = 'Marketing' and the second condition is office LIKE 'East%'.

## Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments.

The following snippet demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.

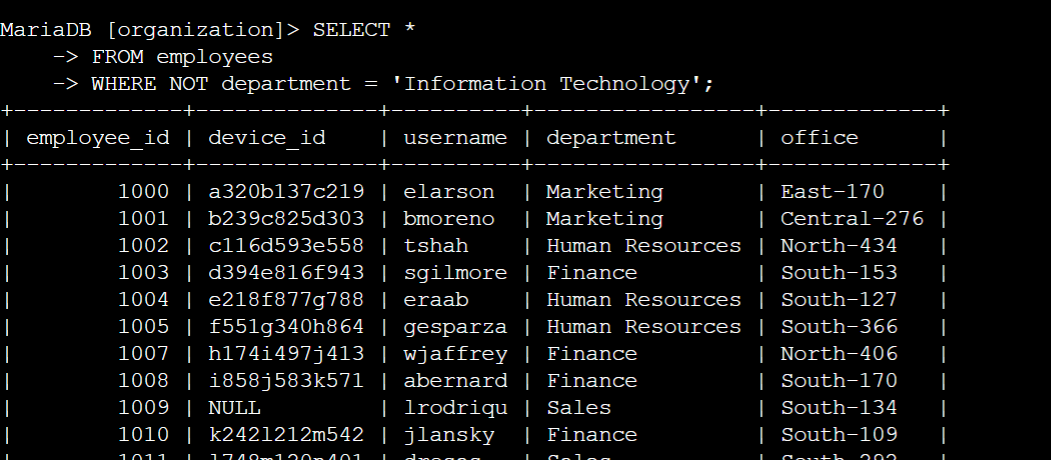
The first part of the snippet is my query, and the second part is the output. This query returns all login attempts that occurred on 2022-05-09 or 2022-05-08. First, I selected the data from the employees table. Then, I used the WHERE clause combined with an OR operator to filter my results based on two conditions. First condition is department = 'Finance' and the second condition is department = 'Sales'. I have used OR instead of AND in order to get employee details from both departments.



## Retrieve all employees not in IT

My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees.

The following snippet demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



The first part of the snippet is my query, and the second part is the output. This query returns all login attempts that occurred on 2022-05-09 or 2022-05-08. First, I selected the data from the employees table. Then, I used the WHERE clause combined with an NOT operator to filter employees not in the IT department.

## Summary

I applied filters to SQL queries to get specific information on login attempts and employee machines. I used two different tables, log\_in\_attempts and employees. I used the AND, OR, and NOT operators to filter for the specific information needed for each task. I also used LIKE and the percentage sign (%) wildcard to filter for patterns.