# Apply filters to SQL queries

## Project description

## Part of my job is to Investigate security issues to help keep the system secure. Recently I discovered some potential security issues that involve login attempts and employee machines. The following steps provide examples of how I used SQL with filters to perform security-related tasks.

## 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 code demonstrates how I created a SQL query to filter for failed login attempts that occurred after business hours.

A screen shot of a computer

Description automatically generated

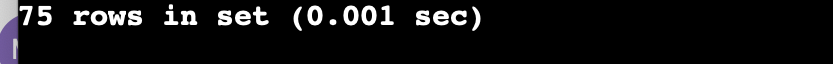
As per screenshot above, this is from organization database and need to query from log\_in\_attempts from log in time after 18:00. I used WHERE to fulfil the login\_time along with the symbol > and specifying failed attempts using ‘FALSE’ in the command line to get the total of 19 failed log in attempts **after** ‘18:00’.

## Retrieve login attempts on specific dates

## A suspicious event occurred on 2022-05-09. I wanted to review and investigete all login attempts which occurred on this day and the day before. I Used filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.

## 

## As per screenshot above, I am reviewing the login attempts that occurred on ‘2022-05-09’ or ‘2022-05-08’. From organizations database, run a query FROM log\_in\_attempts that covers the log in dates ‘2022-05-09’ typing OR ‘2022-05-08’ to cover the range of dates that is on the WHERE column to get the result that there are 75 attempts on these two days.



## Retrieve login attempts outside of Mexico

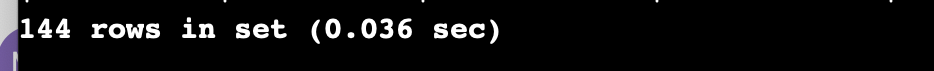
## There’s been suspicious activity with login attempts, but I determined that this activity didn't originate in Mexico. The following code demonstrates how I created a SQL query to filter for login attempts that occurred outside of Mexico.

A screen shot of a computer

Description automatically generated

As the image described from above, this is from organizations database understanding suspicious activity outside Mexico. So, this would be from log\_in\_attempts command and where would be specifying NOT country like ‘MEX%’. The percentage sign (%)

represents any number of unspecified characters when used with LIKE. As a result, there is 144 attempts outside of Mexico.



## Retrieve employees in Marketing

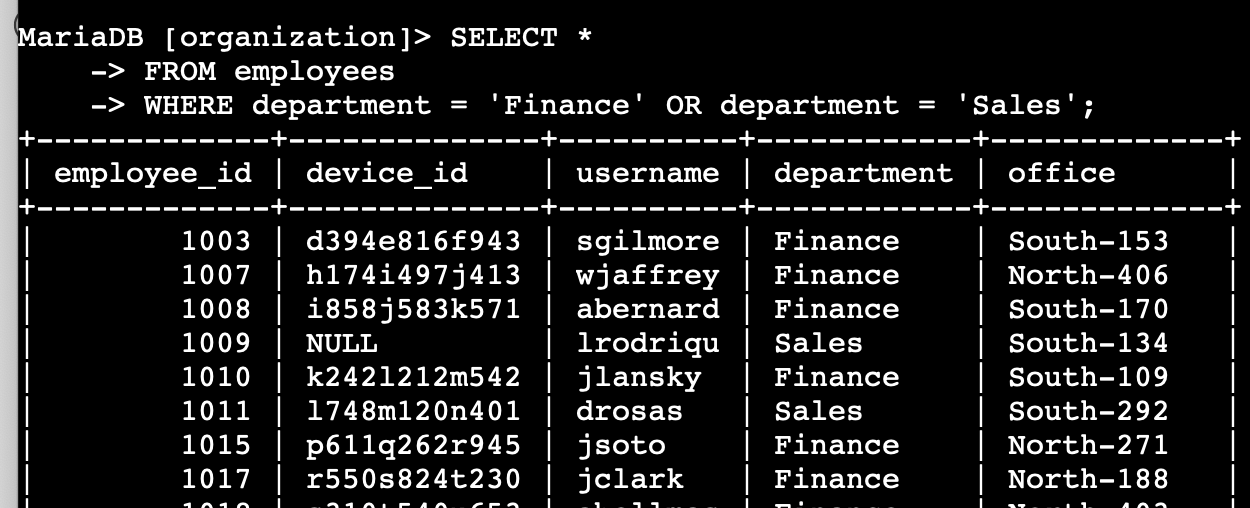
Our team wants to perform security updates on specific employee machines in the Marketing department. My task is getting information on these employee machines and will need to query the employee’s table. The following code demonstrates how I created a SQL query to filter for all employees identifying who is assigned in the Marketing department for all offices in the East building.

## 

As described from the screenshot below, to retrieve employees from Marketing that resides in the East part of the office, I used WHERE along with AND to filter the employees who is working in the Marketing department that situates in the East Building. By using the LIKE, office, and % to portion which part of the office does the employees work in the East side of the building.

## Retrieve employees in Finance or Sales

My team now needs to perform a different security update on machines for employees in the Sales and Finance departments. The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.

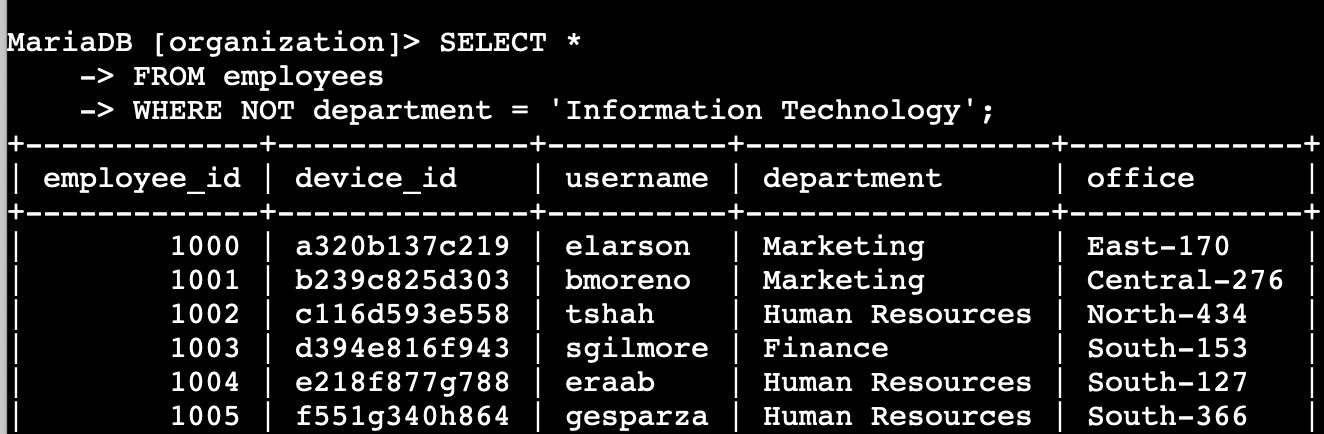


As per screenshot above, to retrieve employees from Finance or Sales, I applied filters specifying what department e.g., ‘Finance’ and using OR in between another department which is department equals ‘Sales’. That resulted into identifying all staff under Finance and Sales that totaled to 71.

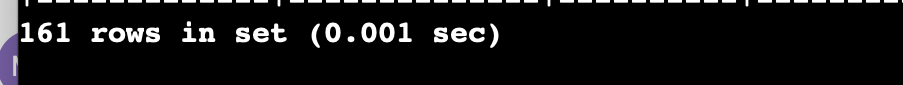


## Retrieve all employees not in IT

## My team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. The following demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



As per screenshot, the goal is simply to exclude the IT department. Basically, I put a command NOT to specify what department that I don’t want to include and specified ‘Information Technology’ to specify what argument. As a result, there are 161 roles that is not part of the IT department.



## Summary

I have performed and applied run SQL queries to retrieve information from a database using AND, OR, and NOT operators to filter SQL queries. I also filtered Select by using \* to include all database in the organization. In addition, I also applied codes log\_in\_attempts, employees, LIKE and % to trickle down the result desired.