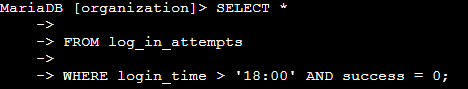
# Apply filters to SQL queries

## Project description

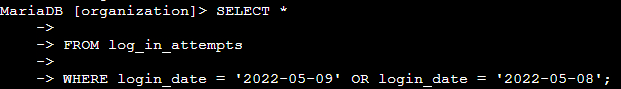
In this project, I applied SQL filtering techniques to investigate potential security issues within an organization’s employee and login data. By using operators such as AND, OR, NOT, and LIKE, I was able to refine queries to identify suspicious login attempts, filter by specific dates and times, and retrieve employee information based on department and office location. These queries demonstrate how SQL can be leveraged to extract precise information for cybersecurity analysis and incident response.

## Retrieve after hours failed login attempts



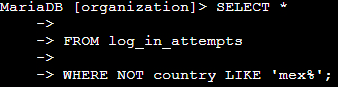
Using this query, we are able to select all rows where login time is AFTER 18:00 (6pm) which is outside of working hours, and where the login attempts fail. 0 as a boolean value means false, which also means the login failed. With times, we can use the greater than, less than operators to express time before and after as specified, for example here > ‘18:00’ means after 6pm.

## Retrieve login attempts on specific dates



With this query, we are able to filter all rows where log in dates were equal to 2022-05-09 or 2022-05-08 using the OR operator.

## Retrieve login attempts outside of Mexico



With this query, we are selecting all rows where the country is not Mexico using the NOT operator. In addition, we use LIKE and do not write out Mexico in full, as some inputs are MEX and some say Mexico. We use the % in conjunction with the LIKE operator to include Mexico and MEX in our query. Mex% allows us to search for any entry that starts with Mex, regardless of what characters come after.

## Retrieve employees in Marketing



Using this query, we are able to find all records of employees in the marketing department, but also work in any of the East offices. Again, using the LIKE operator, we can find all offices that start with East, whether it is East-170 or East-320 due to filtering for East%.

## Retrieve employees in Finance or Sales



Using the OR operator, we can query for all rows where the department of the employee is either Sales or Finance. That way we can list all employees in either department.

## Retrieve all employees not in IT



To query all employees except for those not in the Information Technology department, we use the NOT operator. By doing this, we can list all rows/data except for those where the department = information technology.

## Summary

Through this project, I demonstrated how SQL filters can be used to support real-world security investigations. I retrieved failed login attempts outside of business hours, analyzed suspicious login activity on specific dates, and excluded data from certain locations using the NOT and LIKE operators. I also applied logical operators to filter employee data by department and office. These tasks highlight the importance of SQL in narrowing down large datasets to uncover actionable insights that help strengthen organizational security.