

# Apply filters to SQL queries

## Project description

My organisation is aiming to have a more robust and secure system. I am responsible for ensuring our systems are safe, investigating potential security issues and patching employee computers as needed.

## Retrieve after hours failed login attempts

A potential security incident occurred after business hours (after 18:00). The login attempts made after hours need to be investigated.

Below is the query I constructed to select all data from the log\_in\_attempts table and filter failed login attempts after 18:00. I used the WHERE clause with the greater than '>' operator along with the AND operator to filter login attempts after 18:00 that were unsuccessful.

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE login_time > '18:00' AND success = FALSE;
```

event_id	username	login_date	login_time	country	ip_address	success
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12	0
18	pwashing	2022-05-11	19:28:50	US	192.168.66.142	0

## Retrieve login attempts on specific dates

There was a suspicious event on 2022-05-09. All login activity that occurred on 2022-05-09 or the day before needs to be investigated further.

Below is the query I constructed to output all login attempts made on or before 2022-05-09. I selected all data from the log\_in\_attempts table, then I used the WHERE clause with an OR operator to filter the output to include login attempts on or before 2022-05-09.

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	
1						
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162	

## Retrieve login attempts outside of Mexico

After investigating the data on the organisations login attempts, I believe the issue lies with login attempts outside of Mexico.

The below query I constructed will return login attempts made that are not from Mexico. First I selected all data from the log\_in\_attempts table, then I used the WHERE clause with the NOT operator to filter for countries other than Mexico. I used LIKE 'MEX%' as the pattern to match as the dataset refers to Mexico with MEX. The percentage sign will substitute for any number of other characters.

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE NOT country LIKE 'Mex%';
```

event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	

## Retrieve employees in Marketing

My Team wants to patch the computers for certain employees in the Marketing department from the East Building.

Below is the query I used to do this. First, I started by selecting all the data from the employees table. Then I used the WHERE clause with AND to filter employees who are in marketing and in the east building. I used LIKE with East% as the pattern to match as the office column in the dataset has East + the specific building number.

```
MariaDB [organization]> SELECT *  
  -> FROM employees  
  -> WHERE department = 'Marketing' AND office LIKE 'East%';  
+-----+-----+-----+-----+-----+  
| employee_id | device_id | username | department | office |  
+-----+-----+-----+-----+-----+  
|          1000 | a320b137c219 | elarson | Marketing | East-170 |  
|          1052 | a192b174c940 | jdarosa | Marketing | East-195 |  
|          1075 | x573y883z772 | fbautist | Marketing | East-267 |  
|          1088 | k865l965m233 | rgosh | Marketing | East-157 |  
|          1103 | NULL | randerss | Marketing | East-460 |  
|          1156 | a184b775c707 | dellery | Marketing | East-417 |  
|          1163 | h679i515j339 | cwilliam | Marketing | East-216 |  
+-----+-----+-----+-----+-----+  
7 rows in set (0.001 sec)
```

## Retrieve employees in Finance or Sales

The endpoints for employees in the Finance and Sales Teams also need to be updated. These 2 teams require a different update.

Below is the query I used to get the employee machines of employees in the Finance and Sales departments. First I selected all the data from the employees table. Then I used the WHERE clause with the OR operator to filter employees that are either in Finance or Sales. I used the OR operator instead of AND because I want to output employees who are in either department and not both.

```
MariaDB [organization]> SELECT *  
  -> FROM employees  
  -> WHERE department = 'Sales' OR department = 'Finance';  
+-----+-----+-----+-----+-----+  
| employee_id | device_id | username | department | office |  
+-----+-----+-----+-----+-----+  
|          1003 | d394e816f943 | sgilmore | Finance | South-153 |  
|          1007 | h174i497j413 | wjaffrey | Finance | North-406 |  
|          1008 | i858j583k571 | abernard | Finance | South-170 |  
+-----+-----+-----+-----+-----+
```

## Retrieve all employees not in IT

My Team needs to make one last security update on employee endpoints who are not in the IT department.

The query I made below shows how I got employees who are not in IT. First I selected all data from the employees table. Then I used the WHERE clause with NOT to filter for employees not in the department 'Information Technology'

```
MariaDB [organization]> SELECT *  
  -> FROM employees  
  -> WHERE NOT department = 'Information Technology';
```

employee_id	device_id	username	department	office
1000	a320b137c219	elarson	Marketing	East-170
1001	b239c825d303	bmoreno	Marketing	Central-276
1002	c116d593e558	tshah	Human Resources	North-434
1003	d394e816f943	sgilmore	Finance	South-153

## Summary

I utilised filters for my SQL queries to help me get the desired output on login attempts and employee machines. I used 2 tables, employees and log\_in\_attempts. The operators AND, OR and NOT were used to filter for specific information needed. LIKE and the wildcard '%' were used to filter for patterns.