Apply filters to SQL queries

by Engr Josué Ríos C.

Project description

My organization is working to make its systems more secure. My role is to ensure system protection, investigate all potential security issues, and update employee computers as needed.

In this project, I worked with the security team to analyze the `Chinook` database via the MariaDB terminal. This involved creating lists of login attempts, recovering login data, and retrieving employees by department.

Retrieve after hours failed login attempts

As a best practice, I first preview the table data when the schema is unavailable. For this task, I displayed five records from the `log_in_attempts` table using `LIMIT 5`. This revealed the six attributes: `event_id`, `username`, `login_time`, `login_date`, `country`, `ip_address`, and `success`.

```
MariaDB [organization]> SELECT * FROM log_in_attempts LIMIT 5;
+----------+----------+------------+------------+---------+----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address     | su
ccess |
+----------+----------+------------+------------+---------+----------------+---
------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |
    1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |
    0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |
    1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |
    0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |
    0 |
+----------+----------+------------+------------+---------+----------------+---
------+
5 rows in set (0.043 sec)
```

After understanding the table's structure, I completed the assigned task: A potential security incident occurred after business hours (after 18:00). It was necessary to

investigate all failed login attempts during this period.

I used a `WHERE` clause to filter the `login_time` for values greater than `'18:00'` and the `success` attribute equal to 0 (FALSE), indicating a failed attempt

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_time > '18:00'AND success
= 0;
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200  |       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232  |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
19 rows in set (0.002 sec)
```

The query showed **19 failed attempts** after 6:00 PM from various countries in North America.

Retrieve login attempts on specific dates

The next task was to retrieve login attempts from March 8th to 9th, 2022. This required a `WHERE` filter with the `OR` operator to capture events on either date.

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_date = '2022-05-09' OR log
in_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 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1 |
```

This query returned **75 log attempts** across the two specified dates.

```
|      170 | sbaelish | 2022-05-09 | 16:43:18   | USA     | 192.168.65.113  |       0 |
|      172 | mabadi   | 2022-05-08 | 08:06:50   | US      | 192.168.180.41  |       1 |
|      178 | sgilmore | 2022-05-08 | 12:27:22   | CAN     | 192.168.52.216  |       0 |
|      184 | alevitsk | 2022-05-08 | 03:09:48   | CAN     | 192.168.33.70   |       0 |
|      186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192.168.40.72   |       0 |
|      187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.168.77.137  |       0 |
|      189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.168.168.117 |       1 |
|      190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.168.25.60   |       0 |
|      191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168.7.187   |       0 |
|      193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.168.125.240 |       0 |
|      197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168.36.21   |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
75 rows in set (0.001 sec)
```

Retrieve login attempts outside of Mexico

After analyzing the organization's login attempt data, I suspect an issue with login attempts originating from outside Mexico. These attempts require further investigation.

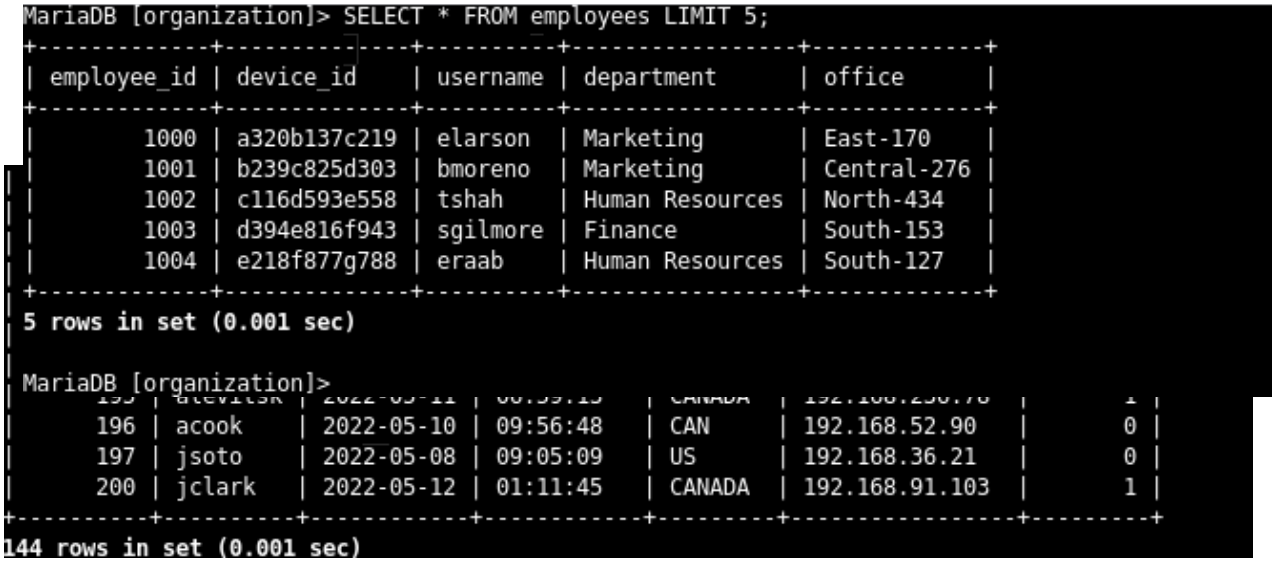
To find login attempts originating outside Mexico, I used a `WHERE` clause with the `NOT` operator to exclude records where the `country` matched the pattern `MEX%`. The `LIKE` statement with the `%` wildcard ensured we excluded any country starting with "MEX".

```
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 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
```

This query returned **144 login attempts** from countries other than Mexico.

Retrieve employees in Marketing

For the final tasks, I used the `employees` table. A preliminary query revealed its five columns: `employee_id`, `device_id`, `username`, `department`, and `office`.



```
MariaDB [organization]> SELECT * FROM employees LIMIT 5;
+-------------+--------------+----------+-----------------+-------------+
| 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   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127   |
+-------------+--------------+----------+-----------------+-------------+
5 rows in set (0.001 sec)

MariaDB [organization]>
|      196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168.52.90   |       0 |
|      197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168.36.21   |       0 |
|      200 | jclark   | 2022-05-12 | 01:11:45   | CANADA  | 192.168.91.103  |       1 |
+----------+----------+------------+------------+---------+-----------------+---------+
144 rows in set (0.001 sec)
```

Using `WHERE`, `LIKE`, and `AND` clauses, I retrieved records for employees in the Marketing department located in the East wing. The query identified **7 offices**.

```
MariaDB [organization]> SELECT * FROM employees WHERE office LIKE 'East%'AND department = 'M
arketing' ;
+-------------+-------------+----------+------------+----------+
| 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 (0.049 sec)
```

Retrieve employees in Finance or Sales

My team needs to update computers for specific employees in the Marketing department. To do this, I must first retrieve information on the employee devices that require updating.

I created an SQL query using a `WHERE` clause with the `OR` operator to filter for employees in the 'Finance' or 'Sales' departments. Using `OR` was crucial to include employees from *either* department, unlike `AND` which would have found employees in both simultaneously. The query successfully returned the complete list of targeted employees: 71 records.

```
MariaDB [organization]> SELECT * FROM  employees WHERE department = 'Finance' OR department
= 'Sales';
+-------------+-------------+----------+------------+-------------+
| 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   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k242l212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1175 | t959u687v394 | jclark2  | Finance    | North-194   |
|        1176 | u849v569w521 | nliu     | Sales      | West-220    |
|        1181 | z803a233b718 | sessa    | Finance    | South-207   |
|        1185 | d790e839f461 | revens   | Sales      | North-330   |
|        1186 | e281f433g404 | sacosta  | Sales      | North-460   |
|        1187 | f963g637h851 | bbode    | Finance    | East-351    |
|        1188 | g164h566i795 | noshiro  | Finance    | West-252    |
|        1195 | n516o853p957 | orainier | Finance    | East-346    |
+-------------+-------------+----------+------------+-------------+
71 rows in set (0.001 sec)
```

Retrieve all employees not in IT

My team also needed to perform a security update for all employees *not* in the Information Technology (IT) department.

```
MariaDB [organization]> SELECT * FROM employees WHERE NOT department = 'Information Technolo
gy';
+-------------+--------------+----------+-----------------+-------------+
| 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   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127   |
|        1005 | f551g340h864 | gesparza | Human Resources | South-366   |
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406   |
|        1008 | i858j583k571 | abernard | Finance         | South-170   |
|        1009 | NULL         | lrodriqu | Sales           | South-134   |
|        1010 | k242l212m542 | jlansky  | Finance         | South-109   |
```

For this task, I used a `WHERE` clause with the `NOT` operator to exclude employees from the IT department. This query successfully returned the 161 employees outside of IT.

```
|        1184 | c986d200e170 | ptsosie  | Human Resources | Central-247 |
|        1185 | d790e839f461 | revens   | Sales           | North-330   |
|        1186 | e281f433g404 | sacosta  | Sales           | North-460   |
|        1187 | f963g637h851 | bbode    | Finance         | East-351    |
|        1188 | g164h566i795 | noshiro  | Finance         | West-252    |
|        1189 | h784i120j837 | slefkowi | Human Resources | West-342    |
|        1190 | NULL         | kcarter  | Marketing       | Central-270 |
|        1191 | NULL         | shakimi  | Marketing       | Central-366 |
|        1194 | m340n287o441 | zwarren  | Human Resources | West-212    |
|        1195 | n516o853p957 | orainier | Finance         | East-346    |
|        1198 | q308r573s459 | jmartine | Marketing       | South-117   |
|        1199 | r520s571t459 | areyes   | Human Resources | East-100    |
+-------------+--------------+----------+-----------------+-------------+
161 rows in set (0.001 sec)
```

Summary

I applied SQL filters to retrieve specific login attempt and employee device information. Using the `log_in_attempts` and `employees` tables, I effectively used the `AND`, `OR`, and `NOT` operators for precise filtering, as well as the `LIKE` operator with the `%` wildcard for pattern matching.