Apply filters to SQL queries

Project description

SQL enables a security analyst to obtain specific pieces of information from a database. In order to use SQL effectively one needs to be familiar with SQL operators and how to interchange or combine operators to create complex filter queries. This project shows examples of using SQL to filter information.

Retrieve after hours failed login attempts

Here I was required to retrieve data of failed login attempts after 6pm, which is when office hours end. In order to do this I used the `SELECT` and `WHERE` clause together with the `AND` operator. The `success` column has either true or false with true=1 and false=0.

```
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     | succes
s |
+----------+----------+------------+------------+---------+----------------+-------
--+
|        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 |
```

Retrieve login attempts on specific dates

Here the task was retrieving login attempts that occurred on 2 days: `2022-05-09` and the day before, `2022-05-08`. Since the task required only 2 login dates, I used the `OR` operator. The `OR` operator uses the condition that either the login attempts took place on either of the 2 days or both to return data.

```
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      | succes
s |
+----------+----------+------------+------------+---------+-----------------+-------
--+
|        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 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |
```

Retrieve login attempts outside of Mexico

Here I was tasked with investing logins that were not from Mexico and retrieving that information. I used the WHERE NOT clause to specify the logins I need were only the ones originating from outside Mexico. Since it's possible to condense the name Mexico, I used the wildcard % together with an argument MEX as a filter. The operator LIKE is used when filtering for an argument that may have characters that are numerical or special.

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+-------
--+
| event_id | username | login_date | login_time | country | ip_address      | succes
s |
+----------+----------+------------+------------+---------+-----------------+-------
--+
|        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 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |
```

Retrieve employees in Marketing

The task was to retrieve employee data from the marketing department in the east side of the office. Since the conditions required are for the employee to be both in the marketing department and in the east office, I used the AND operator. The AND operator works on the condition that both statements are true. The LIKE operator is used after `office` as a filter for all `East` side employees.

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Marketing' AND o
ffice 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 | k8651965m233 | 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 task was to retrieve records of employees in the Finance or Sales department. I used the OR operator. The OR operator brings a result if there are employees in either of the departments or both, and there are.

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Finance' OR depa
rtment = '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 | k2421212m542 | 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    |
|        1024 | y976z753a267 | iuduike   | Sales      | South-215   |
|        1025 | z381a365b233 | jhill     | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco  | Finance    | East-156    |
|        1035 | j236k3031245 | bisles    | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson  | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin  | Sales      | North-208   |
```

Retrieve all employees not in IT

The task is retrieving records of all employees not in the IT department. The `WHERE NOT` clause is used to filter the information. `WHERE NOT` negates the statement `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   |
|        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 | k2421212m542  | jlansky  | Finance         | South-109   |
|        1011 | l748m120n401  | drosas   | Sales           | South-292   |
|        1015 | p611q262r945  | jsoto    | Finance         | North-271   |
|        1016 | q793r736s288  | sbaelish | Human Resources | North-229   |
|        1017 | r550s824t230  | jclark   | Finance         | North-188   |
|        1018 | s310t540u653  | abellmas | Finance         | North-403   |
|        1020 | u899v381w363  | arutley  | Marketing       | South-351   |
|        1022 | w237x430y567  | arusso   | Finance         | West-465    |
```

Summary

Filtering data in SQL requires understanding of operators and clauses. One can try mixing them up to get your preferred filtered information.