SQL: Apply more filters in SQL

3/4

Scenario

In this scenario, you're investigating a recent security incident.

You need to gather information about login attempts for certain dates and times. This will help in resolving a security incident.

Here's how you'll do this task: **First**, you'll retrieve login events made after a certain date. **Second**, you'll narrow the focus of the search to filter logins in a date range. **Third**, you'll investigate logins that were made at certain times. **Finally**, you'll filter login attempts based on their event IDs.

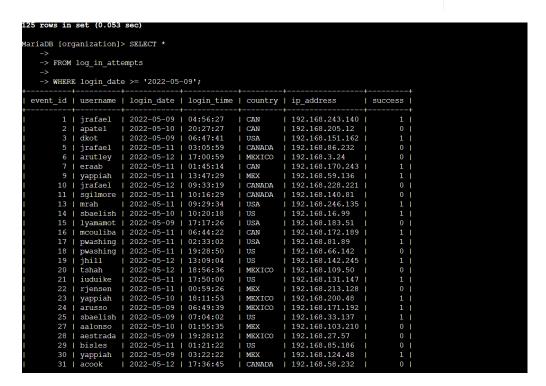It's time to get started and use operators to filter data from a table!

```
125 rows in set (0.053 sec)

MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date >= '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.136  |       1 |
|       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 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.245 |       1 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       23 | yappiah  | 2022-05-10 | 18:11:53   | MEXICO  | 192.168.200.48  |       1 |
|       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 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232  |       0 |
```

Figure 1 Query to select all login dates from the login attempts table that are greater than the date '2022-05-09'

```
165 rows in set (0.001 sec)

MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date BETWEEN '2022-05-09' AND '2022-05-11';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|        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 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.136  |       1 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       23 | yappiah  | 2022-05-10 | 18:11:53   | MEXICO  | 192.168.200.48  |       1 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       25 | sbaelish | 2022-05-11 | 07:04:02   | US      | 192.168.33.137  |       1 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |       0 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       35 | tshah    | 2022-05-10 | 15:26:08   | MEX     | 192.168.92.147  |       0 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
```

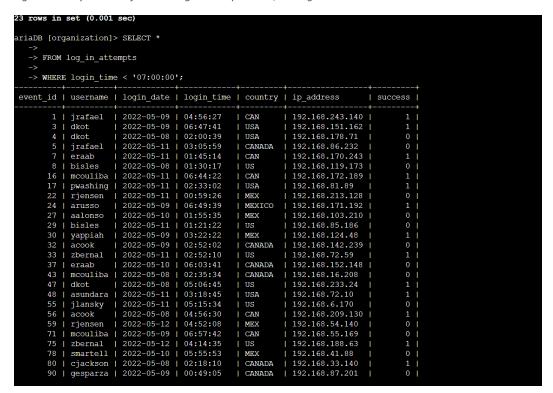*Figure 2 Query to select from the login attempts table, the login dates that are between '2022-05-09' and '2022-05-11'*

```
23 rows in set (0.001 sec)

MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time < '07:00:00';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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 |
|        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 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.128 |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.210 |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |       0 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208  |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.24  |       1 |
|       48 | asundara | 2022-05-11 | 03:18:45   | USA     | 192.168.72.10   |       1 |
|       55 | jlansky  | 2022-05-11 | 05:15:34   | US      | 192.168.6.170   |       0 |
|       56 | acook    | 2022-05-08 | 04:56:30   | CAN     | 192.168.209.130 |       1 |
|       59 | rjensen  | 2022-05-12 | 04:52:08   | MEX     | 192.168.54.140  |       0 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169  |       0 |
|       75 | zbernal  | 2022-05-12 | 04:14:35   | US      | 192.168.188.63  |       1 |
|       78 | smartell | 2022-05-10 | 05:55:53   | MEX     | 192.168.41.88   |       0 |
|       80 | cjackson | 2022-05-08 | 02:18:10   | CANADA  | 192.168.33.140  |       1 |
|       90 | gesparza | 2022-05-09 | 00:49:05   | CANADA  | 192.168.87.201  |       0 |
```

Figure 3 Query that selects from the login attempts table, the login times that are greater than '7:00:00'

```
-----------+----------+------------+------------+----------+------------------+---------+
57 rows in set (0.001 sec)

MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time BETWEEN '06:00:00' AND '07:00:00';
-----------+----------+------------+------------+----------+------------------+---------+
 event_id | username | login_date | login_time | country | ip_address       | success |
-----------+----------+------------+------------+----------+------------------+---------+
        3 | dkot     | 2022-05-09 | 06:47:41   | USA      | 192.168.151.162 |       1 |
       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN      | 192.168.172.189 |       1 |
       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO   | 192.168.171.192 |       1 |
       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA   | 192.168.152.148 |       0 |
       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN      | 192.168.55.169  |       0 |
       98 | gesparza | 2022-05-11 | 06:30:14   | CANADA   | 192.168.148.80  |       0 |
      106 | tmitchel | 2022-05-12 | 06:15:41   | MEXICO   | 192.168.3.252   |       1 |
      134 | iuduike  | 2022-05-09 | 06:46:40   | USA      | 192.168.22.115  |       1 |
      136 | mabadi   | 2022-05-10 | 06:56:44   | US       | 192.168.214.234 |       1 |
      142 | gesparza | 2022-05-11 | 06:31:14   | CANADA   | 192.168.117.56  |       1 |
      147 | yappiah  | 2022-05-08 | 06:04:34   | MEX      | 192.168.65.245  |       0 |
      148 | daquino  | 2022-05-08 | 06:15:55   | CANADA   | 192.168.135.6   |       1 |
      182 | lyamamot | 2022-05-10 | 06:01:31   | USA      | 192.168.106.52  |       0 |
      191 | cjackson | 2022-05-08 | 06:46:07   | CANADA   | 192.168.7.187   |       0 |
      195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA   | 192.168.236.78  |       1 |
-----------+----------+------------+------------+----------+------------------+---------+
15 rows in set (0.001 sec)

MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id >= 100;
-----------+----------+------------+
 event_id | username | login_date |
-----------+----------+------------+
```

Figure 4 Query to select from the same table, the login times between '06:00:00' and '07:00:00'

```
-----------+----------+------------+------------+----------+------------------+---------+
5 rows in set (0.001 sec)

MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id >= 100;
-----------+----------+------------+
 event_id | username | login_date |
-----------+----------+------------+
      100 | tmitchel | 2022-05-12 |
      101 | sbaelish | 2022-05-08 |
      102 | jreckley | 2022-05-09 |
      103 | jhill    | 2022-05-11 |
      104 | asundara | 2022-05-11 |
      105 | cjackson | 2022-05-12 |
      106 | tmitchel | 2022-05-12 |
      107 | bisles   | 2022-05-12 |
      108 | daquino  | 2022-05-09 |
      109 | mcouliba | 2022-05-10 |
      110 | mabadi   | 2022-05-09 |
      111 | aestrada | 2022-05-10 |
      112 | rjensen  | 2022-05-09 |
      113 | gesparza | 2022-05-10 |
      114 | smartell | 2022-05-10 |
      115 | ivelasco | 2022-05-10 |
      116 | tmitchel | 2022-05-10 |
      117 | bsand    | 2022-05-08 |
      118 | smartell | 2022-05-12 |
      119 | tmitchel | 2022-05-11 |
      120 | tmitchel | 2022-05-09 |
      121 | btang    | 2022-05-10 |
      122 | yappiah  | 2022-05-11 |
      123 | bmoreno  | 2022-05-10 |
      124 | asundara | 2022-05-12 |
      125 | bisles   | 2022-05-11 |
```

Figure 5 Query to select from the same table, all the event ids greater than 100

```
---------+---------+-----------+
01 rows in set (0.074 sec)

MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id BETWEEN 100 AND 150;
---------+---------+-----------+
 event_id | username | login_date |
---------+---------+-----------+
      100 | tmitchel | 2022-05-12 |
      101 | sbaelish | 2022-05-08 |
      102 | jreckley | 2022-05-09 |
      103 | jhill    | 2022-05-11 |
      104 | asundara | 2022-05-11 |
      105 | cjackson | 2022-05-12 |
      106 | tmitchel | 2022-05-12 |
      107 | bisles   | 2022-05-12 |
      108 | daquino  | 2022-05-09 |
      109 | mcouliba | 2022-05-10 |
      110 | mabadi   | 2022-05-09 |
      111 | aestrada | 2022-05-10 |
      112 | rjensen  | 2022-05-09 |
      113 | gesparza | 2022-05-10 |
      114 | smartell | 2022-05-10 |
      115 | ivelasco | 2022-05-10 |
      116 | tmitchel | 2022-05-10 |
      117 | bsand    | 2022-05-08 |
      118 | smartell | 2022-05-12 |
      119 | tmitchel | 2022-05-11 |
      120 | tmitchel | 2022-05-09 |
      121 | btang    | 2022-05-10 |
      122 | yappiah  | 2022-05-11 |
      123 | bmoreno  | 2022-05-10 |
      124 | asundara | 2022-05-12 |
      125 | bisles   | 2022-05-11 |
```

Figure 6 Query to select from the same table, all the event ids between 100 and 150