Apply filters to SQL queries

Project description:

Management at my company has asked me to investigate potential security issues and update employee's computers as required. As a Linux admin, I used SQL filters to perform security-related tasks.

Retrieve during off-hours failed logging attempts

Suspicious activities occurred during off business hours (after 1800). All after hours login attempts that failed during that time must be investigated.

I created a SQL query on MariaDB to filter such failed login attempts that occurred during such time.

```
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 |
|       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, 1 warning (0.116 sec)
```

The result is based on the log_in_attempts table where the login time column is after 18:00 and the login attempts are failed (0). The filter "select*" means to select everything (all columns) and from log_in_attempts means it is from the attempts log-in table. Successfully finding 19 failed log-in attempts occurring after 18:00.