

Apply filters to SQL queries

Project description

As a security professional at a large organization, part of my job is to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines.

My task is to examine the organization's data in their `employees` and `log_in_attempts` tables using SQL filters.

Retrieve after hours failed login attempts

This query uses `SELECT` and the `*` to indicate to display all columns in the `log_in_attempts` table. I am searching specifically for failed login attempts in the `login_time` column after 18:00. The `success = 0` part of the command is written this way because the computer interprets 1 as True and 0 as False.

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE login_time > '18:00' AND success = 0;
```

Retrieve login attempts on specific dates

Again, I am displaying all columns in the `log_in_attempts` table. I am looking for all login attempts in the `login_date` column on 05-08 and 05-09.

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

Retrieve login attempts outside of Mexico

Here I am searching for all attempts outside of Mexico using the `WHERE NOT` command to find all results with login attempts that do not originate from Mexico. The `%` symbol is used to find all results beginning with the letters `MEX`.

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE NOT country = 'MEXICO' AND NOT country LIKE 'MEX%';
```

Retrieve employees in Marketing

This query searches for all employees using the `WHERE` command to find all results in the Marketing department in the East office building. The `%` symbol is used to find all results beginning with the word East.

```
MariaDB [organization]> SELECT *  
-> FROM employees  
-> WHERE department = 'Marketing' AND office LIKE 'East%';
```

Retrieve employees in Finance or Sales

In this case I am displaying all columns in the `employees` table. I am searching for all employees using the `WHERE` command to find all results in the Finance or Sales department.

```
MariaDB [organization]> SELECT *  
-> FROM employees  
-> WHERE department = 'Finance' OR department = 'Sales';
```

Retrieve all employees not in IT

In this query I am searching for all employees using the `WHERE NOT` command to find all results that are not in the Information Technology department.

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

Summary

These commands give the SQL user the ability to filter for very detailed and defined results that can be either exclusive or inclusive. Knowledge of databases and SQL is a valuable skill as an IT professional and particularly as a Cloud or cybersecurity professional. Recognizing basic SQL queries and functions is also helpful in recognizing malicious attempts at SQL injections and other web based attacks.