Aplicación de Filtros en Consultas SQL

Descripción del Proyecto

La organización está llevando a cabo esfuerzos para mejorar la seguridad de su sistema. El rol del equipo de seguridad implica asegurar que el sistema esté protegido, investigar posibles vulnerabilidades y actualizar los equipos de los empleados cuando sea necesario. A continuación, se presentan ejemplos de cómo se utilizó SQL con filtros para abordar tareas relacionadas con la seguridad.

Recuperación de Intentos de Inicio de Sesión Fallidos Fuera del Horario Laboral

Se identificó un posible incidente de seguridad fuera del horario laboral (después de las 18:00). Fue crucial examinar todos los intentos de inicio de sesión fallidos ocurridos después del horario laboral.

El siguiente código ilustra cómo se construyó una consulta SQL para filtrar los intentos de inicio de sesión fallidos que ocurrieron después del horario laboral.

```
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 |
```

La primera sección de la captura de pantalla muestra una consulta SQL, mientras que la segunda sección presenta un fragmento del resultado obtenido. La consulta está diseñada para filtrar los intentos de inicio de sesión fallidos ocurridos después de las 18:00. En primer lugar, se seleccionaron todos los datos de la tabla log_in_attempts. Luego, se empleó una cláusula WHERE combinada con el operador AND para obtener únicamente los intentos de inicio de sesión fallidos posteriores a las 18:00. La primera condición especifica login_time > '18:00', que filtra los registros con intentos posteriores a esa hora. La segunda condición, success = FALSE, selecciona solo aquellos intentos que resultaron fallidos.

Recuperación de Intentos de Inicio de Sesión en Fechas Específicas

El 9 de mayo de 2022, se identificó un evento sospechoso, por lo que se requería investigar toda la actividad registrada en esa fecha o el día anterior.

El código a continuación ilustra cómo se elaboró una consulta SQL para filtrar los intentos de inicio de sesión que ocurrieron en fechas específicas.

```
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      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

La primera sección de la captura de pantalla presenta una consulta SQL, mientras que la segunda sección muestra un fragmento del resultado generado. La consulta está diseñada para recuperar todos los intentos de inicio de sesión que ocurrieron el 9 de mayo de 2022 o el 8 de mayo de 2022. Inicialmente, se seleccionaron todos los datos de la tabla log_in_attempts. Luego, se utilizó una cláusula WHERE con el operador OR para filtrar los resultados, con el objetivo de obtener únicamente los intentos de inicio de sesión correspondientes a las fechas especificadas. La primera condición login_date = '2022-05-09' filtra los registros de inicios de sesión del 9 de mayo de 2022, mientras que la segunda condición login_date = '2022-05-08' selecciona los registros del 8 de mayo de 2022.

Recuperación de Intentos de Inicio de Sesión Fuera de México

Después de analizar los datos de los intentos de inicio de sesión en la organización, se sospecha que podría haber un problema relacionado con los intentos realizados fuera de México. Es necesario investigar estos intentos de inicio de sesión para evaluar posibles problemas de seguridad.

El código que se presenta a continuación ilustra cómo se elaboró una consulta SQL para filtrar los intentos de inicio de sesión realizados fuera de México.

```
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 |       0 |
|        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 |       0 |
```

La primera sección de la captura de pantalla presenta una consulta SQL, mientras que la segunda sección muestra un fragmento del resultado obtenido. La consulta está diseñada para recuperar todos los intentos de inicio de sesión realizados fuera de México. Primero, se seleccionaron todos los datos de la tabla log_in_attempts. Posteriormente, se utilizó una cláusula WHERE con el operador NOT para excluir los países que no son México. Se aplicó el patrón LIKE con MEX% para capturar todas las representaciones de México, que en el conjunto de datos pueden aparecer como MEX o MEXICO. El carácter % en el patrón LIKE permite coincidir con cualquier secuencia de caracteres que sigue a MEX.

Recuperación de Empleados del Departamento de Marketing

El equipo tiene la intención de actualizar las computadoras de algunos empleados del departamento de Marketing. Para proceder, es necesario recopilar información sobre los equipos de estos empleados.

A continuación, se presenta el código que demuestra cómo se elaboró una consulta SQL para filtrar los equipos de los empleados que pertenecen al departamento de Marketing y se encuentran en el edificio Este (East).

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office 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 |
```

La primera sección de la captura de pantalla presenta una consulta SQL, mientras que la segunda sección muestra un fragmento del resultado obtenido. La consulta está diseñada para recuperar información sobre todos los empleados del departamento de Marketing ubicados en el edificio Este. Inicialmente, se seleccionaron todos los registros de la tabla employees. Luego, se aplicó una cláusula WHERE con el operador AND para filtrar a los empleados que pertenecen al departamento de Marketing y que trabajan en el edificio Este. Se utilizó el patrón LIKE 'East%' en la columna office para capturar todas las variaciones del nombre del edificio Este, el cual se representa con el número de oficina correspondiente. La primera condición department = 'Marketing' filtra los empleados del departamento de Marketing, mientras que la segunda condición office LIKE 'East%' selecciona a aquellos empleados ubicados en el edificio Este.

Recuperación de Empleados de Finanzas o Ventas

También se requiere actualizar los equipos de los empleados en los departamentos de Finanzas y Ventas. Debido a la necesidad de una actualización de seguridad específica, se debe obtener información exclusivamente de los empleados en estos dos departamentos.

El siguiente código ilustra cómo se elaboró una consulta SQL para filtrar los equipos de los empleados que pertenecen a los departamentos de Finanzas o Ventas.

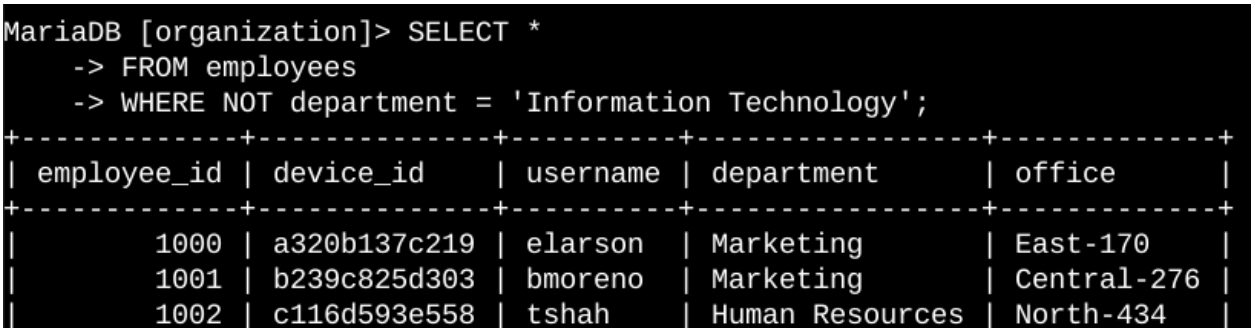
```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

La primera sección de la captura de pantalla muestra una consulta SQL, mientras que la segunda sección presenta un fragmento del resultado obtenido. La consulta está diseñada para recuperar información sobre todos los empleados de los departamentos de Finanzas y Ventas. En primer lugar, se seleccionaron todos los registros de la tabla `employees`. Luego, se utilizó una cláusula `WHERE` con el operador `OR` para filtrar los empleados que pertenecen a cualquiera de estos dos departamentos. Se empleó `OR` en lugar de `AND` para incluir a todos los empleados de ambos departamentos. La primera condición, `department = 'Finance'`, selecciona a los empleados del departamento de Finanzas, mientras que la segunda condición, `department = 'Sales'`, incluye a los empleados del departamento de Ventas.

Recuperación de Empleados que No Trabajan en TI

El equipo necesita llevar a cabo una actualización de seguridad adicional para los empleados que no están en el departamento de Tecnología de la Información. Para proceder con esta actualización, es esencial primero obtener información sobre los empleados que no forman parte de dicho departamento.

A continuación, se presenta una consulta SQL que ilustra cómo se filtraron los registros para obtener los datos de los empleados que no trabajan en el departamento de Tecnología de la Información.



```
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   |
```

La primera sección de la captura de pantalla presenta una consulta SQL, mientras que la segunda sección muestra un fragmento del resultado obtenido. Esta consulta está diseñada para recuperar la información de todos los empleados que no están asignados al departamento de Tecnología de la Información. Inicialmente, se extrajeron todos los datos de la tabla `employees`. Luego, se empleó una cláusula `WHERE` combinada con el operador `NOT` para filtrar aquellos empleados que no pertenecen al mencionado departamento.

RESUMEN

Se aplicaron filtros a consultas SQL para obtener datos específicos sobre intentos de inicio de sesión y equipos de empleados. Se utilizaron dos tablas distintas: `log_in_attempts` para los intentos de inicio de sesión y `employees` para la información de los empleados. Se emplearon los operadores `**AND**`, `OR` y `NOT` para filtrar la información relevante para cada tarea específica. Además, se utilizó el operador `LIKE` junto con el comodín de porcentaje (%) para ajustar los filtros a patrones específicos.