Applying Filters to SQL Queries – Security Log Analysis (Assignment Section)

Sample table: login_activity

Columns:

- id (INT)

- username (TEXT)

- login_time (DATETIME)

- ip_address (TEXT)

- location (TEXT)

- device_type (TEXT)

- success (BOOLEAN or INT: 1 = success, 0 = failed)

Example queries:

1) View all records:

```
SELECT * FROM login_activity;
```

2) Find all failed logins:

```
SELECT *
FROM login_activity
WHERE success = 0;
```

3) Find failed logins for a specific user:

```
SELECT *
FROM login_activity
WHERE username = 'alice'
AND success = 0;
```

4) Find logins from a suspicious IP pattern (using LIKE):

```
SELECT *

FROM login_activity

WHERE ip_address LIKE '192.168.1.%';
```

5) Find all logins outside the US (assuming location stores country):

```
SELECT *

FROM login_activity

WHERE location <> 'United States';
```

6) Order by most recent logins:

```
SELECT *

FROM login_activity

ORDER BY login_time DESC

LIMIT 20;
```

Summary:

These queries demonstrate using WHERE, AND, OR, comparison operators, LIKE, ORDER BY, and LIMIT to filter and analyze login data. This can help identify suspicious activity such as repeated failed logins, logins from unusual IP ranges, or access from unexpected locations.