

SQL & Security

Christian Rudder

August 2024

Contents

1	Introduction	3
2	SQL Basics	4
2.1	Creating Database & Tables	4
2.2	Queries	6
2.3	Mutating Data & Filtering	8
2.4	Joining Tables	11

This page is left intentionally blank.

1 Introduction

Hackers, Security issues, and exploits all exists, because the software we use isn't perfect. It's written by humans. One or two edge cases from the best programmers might slip through. This doesn't mean just software, but languages, and even hardware.

The languages we use are just solutions we thought would work. Binary is a solution, it's not the intrinsic solution, but it's a solution. So we built assembly on top, then C, Java, and so on abstracting the difficult parts. But the more we abstract, the more we lose control. A vulnerability can quickly cascade up a chain of abstractions.

2 SQL Basics

2.1 Creating Database & Tables

SQL stands for “*Structured Query Language*,” used to query against databases with tables containing columns of data, which most often relate to each other.

SQL uses key words like `SELECT`, `FROM`, `WHERE`, ignoring case. It’s good practice to use **all caps for SQL keywords**, and **lowercase for table and column names**. Here’s a simple example:

```
1 SELECT * FROM my_table
```

Selects all () columns from the table `my_table`.*

Now, we are a record company with bands, albums, and songs:

```
1 CREATE DATABASE test; -- creating a test database
2 DROP DATABASE test; -- deleting the test database
3
4
5 CREATE DATABASE concise_records; -- creating our database
6 USE concise_records; -- selecting our database to run commands on it
7
8
9 CREATE TABLE bandds (); -- creating a table for our bands
10 DROP TABLE bandds; -- deleting it because of our typo
11
12
13 -- Create bands table: artist name (at most 255 characters), CANNOT be NULL/EMPTY
14 CREATE TABLE bands (
15     name VARCHAR(255) NOT NULL
16 );
17
18
19 -- Add id column to bands, auto increment, not NULL, make this column important
20 ALTER TABLE bands
21 ADD COLUMN id INT NOT NULL AUTO_INCREMENT PRIMARY KEY;
```

We created the database, `concise_records`, and a table `bands` with two columns: `name` and `id`.

Pagination of commands don’t matter, for example:

```
1 -- We could have written the above
2 CREATE DATABASE concise_records; USE concise_records; CREATE TABLE bands (name VARCHAR
   (255) NOT NULL);
3
4 ALTER
5 TABLE
6 bands
7 ADD COLUMN id INT NOT NULL
8 AUTO_INCREMENT PRIMARY KEY;
```

Which is less readable. The **PRIMARY KEY** uniquely IDs each row in a table, helping draw a thread of relationships between tables where the ID is present.

Definition 2.1: Primary Key

A column which identifies each row in a table. It must be unique, and it cannot be [NULL](#).

To create our [albums](#) table:

```
1  -- Create albums table: album id, album names, release dates (optional)
2  CREATE TABLE albums (
3      id INT NOT NULL AUTO_INCREMENT,
4      name VARCHAR(255) NOT NULL,
5      release_date DATE,
6      PRIMARY KEY (id)
7  );
8
9
10 -- We need a way to link bands to albums
11 -- Create a column in albums pointing to bands' id column
12 ALTER TABLE albums
13 ADD COLUMN band_id INT NOT NULL FOREIGN KEY REFERENCES bands(id);
```

We created the [albums](#) table with three columns: [id](#), [name](#), and [release_date](#), and [band_id](#). A [FOREIGN KEY](#) uses the [PRIMARY KEY](#) of another table to establish a relationship between them.

Definition 2.2: Foreign Key

A column that references another table's [PRIMARY KEY](#).

So far we have:

```
1  -- DB: concise_records
2  --
3  --      bands
4  --      +-----+-----+
5  --      | id | name      |
6  --      +-----+-----+
7  --      |   |          |
8  --      +-----+-----+
9  --
10 --      albums
11 --      +-----+-----+-----+-----+
12 --      | id | name      | release_date | band_id |
13 --      +-----+-----+-----+-----+
14 --      |   |          |             |         |
15 --      +-----+-----+-----+-----+
```

- The database [concise_records](#)
- Tables [bands](#) and [albums](#).
- Column [band_id](#) references [id](#) in [bands](#).

Let's begin to add data to our tables:

```
1  -- Insert 'The Beatles', 'The Rolling Stones', 'The Who' into bands
2  INSERT INTO bands (name) VALUES ('The Beatles');
3  INSERT INTO bands (name) VALUES ('The Rolling Stones'), ('The Who');
4
5  -- DB: concise_records
6  --
7  --      bands
8  --      +-----+-----+
9  --      | id | name                |
10 --      +-----+-----+
11 --      | 1 | The Beatles         |
12 --      | 2 | The Rolling Stones  |
13 --      | 3 | The Who             |
14 --      +-----+-----+
15
16 -- Insert 'Abbey Road', 'Let It Bleed', 'Who's Next' into albums
17
18 INSERT INTO albums (name, release_date, band_id) VALUES ('Abbey Road', '1969', 1);
19 INSERT INTO albums (name, band_id) VALUES ('Let Be', '1970', 1), ('Who's Next', 3);
20
21 -- DB: concise_records
22 --
23 --      albums
24 --      +-----+-----+-----+-----+
25 --      | id | name                | release_date | band_id |
26 --      +-----+-----+-----+-----+
27 --      | 1 | Abbey Road         | 1969         | 1       |
28 --      | 2 | Let It Be          | 1970         | 1       |
29 --      | 3 | Who's Next         |              | 3       |
30 --      +-----+-----+-----+-----+
```

Note: Single quotes denote [strings](#). Double single quotes in strings act as single quotes, seen in the above with 'Who's next' becoming `Who's next`.

2.2 Queries

To retrieve data, we use [SELECT](#):

```
1  -- Retrieve all columns from bands
2  SELECT * FROM bands;
3
4  -- Query Result:
5  --      +-----+-----+
6  --      | id | name                |
7  --      +-----+-----+
8  --      | 1 | The Beatles         |
9  --      | 2 | The Rolling Stones  |
10 --      | 3 | The Who             |
11 --      +-----+-----+
```

Queries to a table return another table.

Examples:

1. `SELECT column`

```
1  -- Retrieve the name column from bands
2  SELECT name FROM bands;
3
4  -- Query Result:
5  -- +-----+
6  -- | name          |
7  -- +-----+
8  -- | The Beatles   |
9  -- | The Rolling Stones |
10 -- | The Who       |
11 -- +-----+
```

2. `LIMIT`

```
1  -- Retrieve the name column from bands, limit to 1
2  SELECT name FROM bands LIMIT 1;
3
4  -- Query Result:
5  -- +-----+
6  -- | name          |
7  -- +-----+
8  -- | The Beatles   |
9  -- +-----+
```

3. `AS`

```
1  -- Retrieve and give aliases to id and name columns from bands, limit to 1
2  SELECT id AS 'ID', name AS 'Band Name' LIMIT 1;
3
4  -- Query Result:
5  -- +-----+
6  -- | ID | Band Name          |
7  -- +-----+
8  -- | 1  | The Beatles        |
9  -- +-----+
```

4. `ORDER BY (DESC/ASC)`

```
1  -- Order bands by name in descending order
2  SELECT * FROM bands ORDER BY name DESC;
3
4  -- Query Result:
5  -- +-----+
6  -- | id | name              |
7  -- +-----+
8  -- | 1  | The Who           |
9  -- | 2  | The Rolling Stones |
10 -- | 3  | The Beatles       |
11 -- +-----+
12
13 -- Order bands in ascending order
14 SELECT * FROM bands ORDER BY name ASC;
15 -- which can be shortened to
16 SELECT * FROM bands ORDER BY name; -- as ASC is the default
```

Here we used the `LIMIT`, `AS`, and `ORDER BY (ASC/DESC)` commands.

5. DISTINCT

```
1  -- Say we had the following table:
2  -- DB: school_table
3  --
4  --      students
5  --      +-----+-----+
6  --      | id | name                |
7  --      +-----+-----+
8  --      | 1  | Joe                  |
9  --      | 2  | Joe                  |
10 --      | 3  | Joe                  |
11 --      | 4  | Alvin                |
12 --      +-----+-----+
13
14 -- Retrieve all unique names from students
15 USE school_table;
16 SELECT DISTINCT name FROM students;
17
18 -- Query Result:
19 --      +-----+
20 --      | name                |
21 --      +-----+
22 --      | Joe                  |
23 --      | Alvin                |
24 --      +-----+
```

2.3 Mutating Data & Filtering

Again, visiting our [concise_records](#) example:

```
1  -- DB: concise_records
2  --
3  --      bands
4  --      +-----+-----+
5  --      | id | name                |
6  --      +-----+-----+
7  --      | 1  | The Beatles         |
8  --      | 2  | The Rolling Stones  |
9  --      | 3  | The Who             |
10 --      +-----+-----+
11
12 --      albums
13 --      +-----+-----+-----+-----+
14 --      | id | name                | release_date | band_id |
15 --      +-----+-----+-----+-----+
16 --      | 1  | Abbey Road         | 1969         | 1       |
17 --      | 2  | Let It Be          | 1970         | 1       |
18 --      | 3  | Who's Next         |              | 3       |
19 --      +-----+-----+-----+-----+
```

We will begin to update and filter for specific entries.

To change the release date of **Who's Next** to '1971':

```
1  UPDATE albums SET release_date = '1971';
2  -- But that would result in all albums having the same release date
3  -- instead we use WHERE
4
5  UPDATE albums SET release_date = '1971' WHERE id = 3;
6
7  -- DB: concise_records
8  --
9  --   albums
10 --   +-----+-----+-----+-----+
11 --   | id | name          | release_date | band_id |
12 --   +-----+-----+-----+-----+
13 --   | 1 | Abbey Road   | 1969         | 1       |
14 --   | 2 | Let It Be    | 1970         | 1       |
15 --   | 3 | Who's Next   | 1971         | 3       |
16 --   +-----+-----+-----+-----+
```

We used **id**, as the **name** could change or be duplicated. **WHERE** filters rows based on conditions.
Examples:

1. **>, <, >=, <=**

```
1  -- Select all albums with a release date greater than 1969
2  SELECT * FROM albums WHERE release_date > 1969;
3
4  -- Query Result:
5  --   +-----+-----+-----+-----+
6  --   | id | name          | release_date | band_id |
7  --   +-----+-----+-----+-----+
8  --   | 2 | Let It Be    | 1970         | 1       |
9  --   | 3 | Who's Next   | 1971         | 3       |
10 --   +-----+-----+-----+-----+
```

2. **LIKE**

```
1  -- Select all albums that contain 'be' in their name
2  SELECT * FROM albums WHERE name LIKE '%be%';
3
4  -- Query Result:
5  --   +-----+-----+-----+-----+
6  --   | id | name          | release_date | band_id |
7  --   +-----+-----+-----+-----+
8  --   | 2 | Let It Be    | 1970         | 1       |
9  --   +-----+-----+-----+-----+
```

3. **OR**

```
1  -- Albums that contain 'x' in their name OR have a release date of 1969
2  SELECT * FROM albums WHERE name LIKE '%x%' OR band_id = 1;
3
4  -- Query Result:
5  --   +-----+-----+-----+-----+
6  --   | id | name          | release_date | band_id |
7  --   +-----+-----+-----+-----+
8  --   | 1 | Abbey Road   | 1969         | 1       |
9  --   | 3 | Who's Next   | 1971         | 3       |
10 --   +-----+-----+-----+-----+
```

4. AND

```
1  -- Select all albums that released in 1969 and have an band_id of 1
2  SELECT * FROM albums WHERE release_date = 1969 AND band_id = 1;
3
4  -- Query Result:
5  +-----+-----+-----+-----+
6  | id | name       | release_date | band_id |
7  +-----+-----+-----+-----+
8  | 1  | Abbey Road | 1969        | 1       |
9  +-----+-----+-----+-----+
```

5. BETWEEN

```
1  -- Select all albums that released between 1969 and 1971 (inclusive)
2  SELECT * FROM albums WHERE release_date BETWEEN 1969 AND 1971;
3
4  -- Query Result:
5  +-----+-----+-----+-----+
6  | id | name       | release_date | band_id |
7  +-----+-----+-----+-----+
8  | 1  | Abbey Road | 1969        | 1       |
9  | 2  | Let It Be  | 1970        | 1       |
10 | 3  | Who's Next | 1971        | 3       |
11 +-----+-----+-----+-----+
```

6a. IS NULL

```
1  -- Add a new album with a NULL release date
2  INSERT INTO albums (name, band_id) VALUES ('The Wall', 2);
3
4  -- Select all albums with a NULL release date
5  SELECT * FROM albums WHERE release_date IS NULL;
6
7  -- Query Result:
8  +-----+-----+-----+-----+
9  | id | name       | release_date | band_id |
10 +-----+-----+-----+-----+
11 | 4  | The Wall   |              | 2       |
12 +-----+-----+-----+-----+
```

6b. DELETE

```
1  -- Delete all albums
2  DELETE FROM albums;
3  -- lets not do this though, instead
4
5  -- Delete all albums with name 'The Wall' (added in previous example)
6  DELETE FROM albums WHERE name = 'The Wall';
7
8  -- albums
9  +-----+-----+-----+-----+
10 | id | name       | release_date | band_id |
11 +-----+-----+-----+-----+
12 | 1  | Abbey Road | 1969        | 1       |
13 | 2  | Let It Be  | 1970        | 1       |
14 | 3  | Who's Next | 1971        | 3       |
15 +-----+-----+-----+-----+
```

2.4 Joining Tables

We can **JOIN** tables based on common columns, this serves as their **relationship**. We have:

```
1  -- DB: concise_records
2  --
3  --      bands
4  --      +-----+-----+
5  --      | id | name           |
6  --      +-----+-----+
7  --      | 1 | The Beatles      |
8  --      | 2 | The Rolling Stones |
9  --      | 3 | The Who          |
10 --      +-----+-----+
11 --
12 --      albums
13 --      +-----+-----+-----+-----+
14 --      | id | name           | release_date | band_id |
15 --      +-----+-----+-----+-----+
16 --      | 1 | Abbey Road    | 1969         | 1       |
17 --      | 2 | Let It Be     | 1970         | 1       |
18 --      | 3 | Who's Next    | 1971         | 3       |
19 --      +-----+-----+-----+-----+
```

Examples:

1a. **JOIN**

```
1  -- Retrieve all columns from bands and albums
2  SELECT * FROM bands JOIN albums;
```

This command doesn't specify how to combine the tables, so the **Cartesian product** is returned.

Definition 2.3: Cartesian Product

Sets $A = \{a_1, a_2, \dots, a_n\}$, $B = \{b_1, b_2, \dots, b_m\}$ can match in ordered pairs, e.g., (a_2, b_5) or (a_9, b_3) . The set of all ordered pair combinations of A on B is the Cartesian product.

Denoted: $A \times B$.

1b.

```
1  -- Query Result:
2  -- +-----+-----+-----+-----+
3  -- | id | name           | id | name           | release_date | band_id |
4  -- +-----+-----+-----+-----+
5  -- | 1 | The Beatles      | 1 | Abbey Road    | 1969         | 1       |
6  -- | 1 | The Beatles      | 2 | Let It Be     | 1970         | 1       |
7  -- | 1 | The Beatles      | 3 | Who's Next    | 1971         | 3       |
8  -- | 2 | The Rolling Stones | 1 | Abbey Road    | 1969         | 1       |
9  -- | 2 | The Rolling Stones | 2 | Let It Be     | 1970         | 1       |
10 -- | 2 | The Rolling Stones | 3 | Who's Next    | 1971         | 3       |
11 -- | 3 | The Who          | 1 | Abbey Road    | 1969         | 1       |
12 -- | 3 | The Who          | 2 | Let It Be     | 1970         | 1       |
13 -- | 3 | The Who          | 3 | Who's Next    | 1971         | 3       |
14 -- +-----+-----+-----+-----+
```

2. JOIN ON

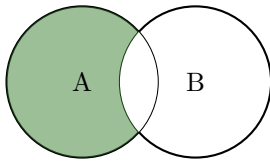
```
1  -- Retrieve all columns from bands and albums where band_id matches id
2  SELECT * FROM bands JOIN albums ON bands.id = albums.band_id;
3
4  -- Query Result:
5  -- +-----+-----+-----+-----+-----+-----+
6  -- | id | name           | id | name           | release_date | band_id |
7  -- +-----+-----+-----+-----+-----+-----+
8  -- | 1 | The Beatles    | 1 | Abbey Road     | 1969         | 1       |
9  -- | 1 | The Beatles    | 2 | Let It Be      | 1970         | 1       |
10 -- | 3 | The Who        | 3 | Who's Next     | 1971         | 3       |
11 -- +-----+-----+-----+-----+-----+-----+
```

3. INNER JOIN - (default join type)

```
1  -- Retrieve all columns from bands and albums where band_id matches id
2  SELECT * FROM bands INNER JOIN albums ON bands.id = albums.band_id;
3
4  -- Query Result:
5  -- +-----+-----+-----+-----+-----+-----+
6  -- | id | name           | id | name           | release_date | band_id |
7  -- +-----+-----+-----+-----+-----+-----+
8  -- | 1 | The Beatles    | 1 | Abbey Road     | 1969         | 1       |
9  -- | 1 | The Beatles    | 2 | Let It Be      | 1970         | 1       |
10 -- | 3 | The Who        | 3 | Who's Next     | 1971         | 3       |
11 -- +-----+-----+-----+-----+-----+-----+
```

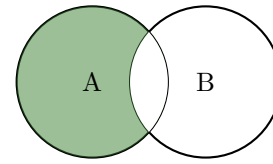
There are plenty of other join types, here's all of them:

1. INNER JOIN



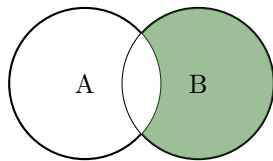
`SELECT * FROM A
INNER JOIN B ON A.Key = B.Key`

2. LEFT JOIN (LEFT OUTER JOIN)



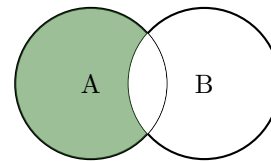
`SELECT * FROM A
LEFT JOIN B ON A.Key = B.Key`

3. RIGHT JOIN (RIGHT OUTER JOIN)



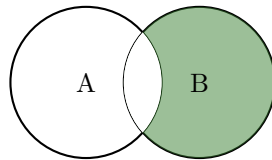
`SELECT * FROM A
RIGHT JOIN B ON A.Key = B.Key`

4. LEFT JOIN with NULL check



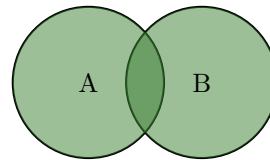
`SELECT * FROM A
LEFT JOIN B ON A.Key = B.Key WHERE B.Key IS NULL`

5. RIGHT JOIN with NULL check



`SELECT * FROM A
RIGHT JOIN B ON A.Key = B.Key WHERE A.Key IS NULL`

6. FULL OUTER JOIN



`SELECT * FROM A
FULL OUTER JOIN B ON A.Key = B.Key`