A database can be hacked in the following ways:

- Using SQL injection
- Cracking the database root password
- Running database exploits

Using SQL Injection

Step 1: Check to see if the database is at risk.

To use this strategy, you must be familiar with database statements. In your web browser, go to the database web interface login page and enter a'(single quote) in the username box. Choose "Login." The database is susceptible to SQL injections if you encounter an error message that reads something like "SQL Exception: quoted string not properly terminated" or "invalid character."

Step 2: Determine the number of columns.

Click into the browser's address bar to navigate back to the database's login page (or any other URL that ends in "id=" or "catid="). To enter, press Enter after typing order by 1 and the URL. Press Enter after increasing the number to 2. Increase till you encounter a problem. The number you typed before the one that caused the problem is the actual number of columns.

Step 3: Identify the columns that permit queries.

Replace the catid=1 or id=1 at the end of the URL in the address bar with catid=-1 or id=-1. Union pick 1,2,3,4,5,6 may be entered by using the space bar (if there are 6 columns). The numbers should be separated by commas and should add up to the entire number of columns. You can view the numbers for each column that will accept a query by pressing Enter.

Step 4: SQL statements should be inserted into the column.

For instance, if you want to place the injection in column 2 and know who the current user is, remove everything from the URL after id=1 and press the space key. Next, enter union choose 1, concat(user()), 3, 4, 5, and 6—. Once you press Enter, the name of the current database user will appear on the screen. For example, you may utilize lists of users and passwords to crack as well as any other SQL queries you wish to retrieve data.