

SQL injection



SQL injection is one of the most common web hacking techniques. It is the placement of malicious code in SQL statements via the web form.

For example, in our sign-up form, we ask the user for the email address. Provided we have no validation, the user could write instead of a regular email address something like this: **email OR 1=1**.

Now, imagine that we have the SQL statement where we directly use the content of the input element and we expect the email address.

The statement looks like this:

```
SELECT * FROM users WHERE user_email = $user_email;
```

By using the content of the input field without any precautions, we would send this query to the database:

```
SELECT * FROM users WHERE user_email = email OR 1=1;
```

Such a statement is valid and will return ALL rows from the users table, since OR 1=1 is always TRUE.

This is very bad because this way, the attacker could get access to all passwords, credit card numbers and so on.

That's why it's super important to never trust the content of the input fields.

In our case, we double check the validity, on the client side and on the server side, but nevertheless, we will take no chances and use placeholders as well.