**Programming Assignment 3: SQL Injection Attacks**

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. As an example of this type of attack we can take a look at the following example.

If we have the following code for handling email and password for login:  
SELECT \*  
 FROM users  
 WHERE email = 'user@email.com'  
 AND pass = 'password' LIMIT 1

If system does not check the password, we can enter following password as the password of any email address:

' or 1=1--

If you replace password with this one, we will have:

SELECT \*  
 FROM users  
 WHERE email = 'user@email.com'  
 AND pass = '' or 1=1--' LIMIT 1

And by running this code by sql you can easily break the password without having to guess the password.

You can see the implementation here:  
<https://www.hacksplaining.com/exercises/sql-injection>

Screenshots:





