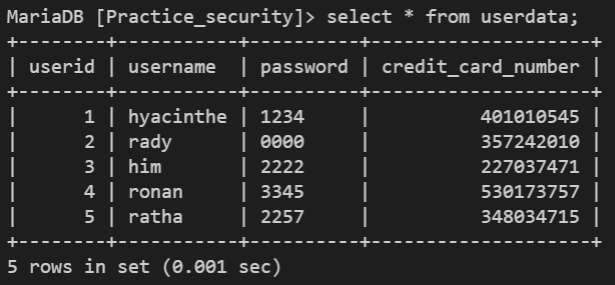
# C5-S2 – SQL INJECTION

# Create table userdata

Create database *Practice\_security*

Create table *userdata* in database *Practice\_security* and insert data from file *userdata.sql*



# Understand the project

* Run the project with PHP built-in server

php -S localhost:8080

* Try bad values for username and password:
  + What is the value of the variable *$query*?

**The value of the variable $query is a value that doesn’t exult input data.**

* + Which data is returned in *$list\_of\_users*?

**The returned in $list\_of\_users is practice\_seucrity that input.**

* + What error message do you see on the browser?   
    **I see on the browser the Wrong username or password!**
* Try with correct values for username and password (for example username = “hyacinthe” and password = “1234”).
  + What is the value of the variable *$query*?

**The value of the variable $query is an added value now shown in the browser.**

* + Which data is returned in *$list\_of\_users*?

**Returned in $list\_of\_users is $username.**

* + Check that you can see on the browser the credit card number of this user (and this user only)

**I see on the browser the credit card number of this user is 401010545.**

Perform SQL injection



Now let’s say that you are a hacker trying to steal credit card numbers from all users, without knowing their password.

To do this you can use well-chosen values for username and password:

Input these values in the form:

* username = “rady”
* password = “ ' OR True; ” (do not forget the first single quote in password value !)
* What is the value of the variable *$query*?

**The value of the variable $query shows tables all have in databases.**

* Which data is returned in *$list\_of\_users*?

**Returned in $list\_of\_users is $statement.**

* Can you see the credit card number of all users?

**I see the credit card numbers of all users is numbers all.**

* Why is this kind of attack called “SQL injection”?

**SQL injection doesn’t exult in the input. Because all data the Hecker is easy to steal give our data.**

Now try with password = “ ' OR True; DELETE FROM userdata; ”

* What is the value of the variable *$query*? Why is SQL injection a very serious security issue?

**The value of the variable $query doesn’t have value in tables. Because SQL injection serious security issue others can delete it and easily steal our data.**

.

# Free Images : antivirus, security, privacy, secured, safe, software, icon, clipart, os, yellow, green, laptop, computer, technology, communication, notebook pc, screen, equipment, electronics, keyboard, portable, connection, text, product, font, line ...Make the website safe!

## Use Prepared statements

You should never concatenate strings to build your query but use prepared statements instead!

After explanation from teacher, change the PHP code to use prepared statements

## Write cleaner code

You must always use prepared statements but if your code is clean, it is unlikely that an attacker can use SQL injection against your website

"SELECT username, credit\_card\_number FROM userdata WHERE username='$username' and password='$password';"

This query works but it is not a good way to check the password:

You should:

1. Get the password from database of the user whose username is *$username*
2. Check if the password is correct in PHP code, not in SQL query

Change the PHP code to use this better way to check the password

$list\_of\_users = $statement->fetchAll();

foreach ($list\_of\_users as $user) :

You expect only one record as result, so you should:

1. Fetch only one record, not All
2. Don’t loop, but display the only record

Change the PHP code to use this better way to display the results