**Lab presentation with some key points**[**here**](http://www.cs.ubbcluj.ro/~daniel/ss/lab10/ss_sql_injection.pdf)

**Complete lab presentation**[**here**](http://www.cs.ubbcluj.ro/~daniel/ss/lab10/SS_Vulnerabilitati_web.pdf)

**Lab setup and practice**

**It is recommended to run these exercises in a virtual machine!**

1. Download and install [XAMPP](https://www.apachefriends.org/download.html)
2. Download [login.txt](https://www.cs.ubbcluj.ro/~daniel/ss/lab10/login.txt) and rename it to login.php
3. Put login.php in c:\xampp\htdocs\
4. Download [tables.sql](https://www.cs.ubbcluj.ro/~daniel/ss/lab10/tables.sql)
5. Open in browser <http://localhost/phpmyadmin>
6. Select 'test' database from the menu on the left
7. From the upper menu, select the SQL option (allows entering SQL commands)
8. Paste the contents of tables.sql file in the text field, and click Go (lower-right corner)
9. Open in browser <http://localhost/login.php> and login with user=user and password=password

**Lab practice**

**EXERCISES**

1. **Authentication bypass**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE user='" . $\_POST['user'] . "' AND pass='" . $\_POST['pass'] . "'"

1. **Database enumeration (gasirea numarului de coloane din interogare)** Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Stabilirea formatului rezultatelor (corespondenta dintre coloanele din interogare si cele afisate)**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Extragerea de informatii**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Listarea tuturor tabelelor din baza de date selectata**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Listarea tuturor coloanelor dintr-un tabel**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Extragerea si listarea anumitor coloane din tabel**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Local file inclusion / Information disclosure**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

1. **Remote code execution**  
   Interogare vulnerabila:

"SELECT \* FROM users WHERE id=" . $\_POST['id']

**Extra practice:**

* [**YesWeHack**](https://github.com/yeswehack/vulnerable-code-snippets)
* [**PortSwigger**](https://portswigger.net/web-security/sql-injection)

**Homework: Write a login page (without any helper frameworks) using php/java/perl/python/.net that:**

* has two text input areas one for user name and one for password
* has a submit button that sends user name and password to server for validation
* validates the user name and password against a database of users and passwords
* returns a message to the user that informs about the validity of the input
* use stored procedures and/or prepared statements on the server side
* sanitize user input on client/server side
* use a db user with least privileges set for required task