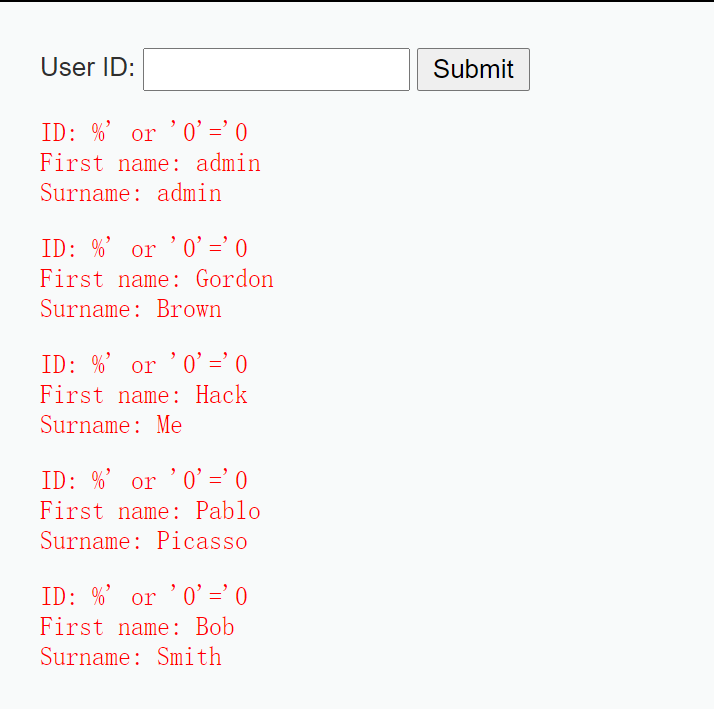
**DVWA SQL injection attack**

****

**Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?**

Ans: For the low level security, I use the always true query send to database in order to return everything I want even though I don’t have the authority. The User ID I submitted is %' or '0'='0, so, the complete query would be

SELECT first\_name, last\_name FROM users WHERE user\_id = '%' or '0'='0';

The above query will return the all first name and last name in the users table, because the condition is always true :　'0'='0' .the query will send to the server database because the server doesn’t check the user’s input, and return what the query ask for.

**If you switch the security level in DVWA to “Medium”, does the SQLi attack still work?**

Ans: If we switch the security level in DVWA to “Medium”, this method won't work, because there is no entry for user input, they use a drop down menu to prevent this.

**DVWA XSS attack**

****

**Describe the reflected XSS attack you used, how did it work?**

Ans: I sumbit <sCript>alert("Hello")</script> to server, and the browser will pop up a alert box with the message “Hello”. It’s because I submitted a Javascript code to the server, and server stored it into the database. Then, what I submitted would return to me, and my browser interpreted it and rendered it which is a JavaScript code to pop up a alert message.

**If you switch the security level in DVWA to “Medium”, does the XSS attack still work?**

Ans: yes, it will still work because the server only delete <script> pair tags in the exact form, but I am using a capital ‘C’ in <sCript>; Therefore, the attack will still work.

Reference:

<https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/index.html>