Exercise 08 – HTML, PHP & SQL

1. Download and unpack the ex-pack as usual.
   - **a.** Make sure the script didn't report any errors (errors should be listed as "ERROR: xxx"), **and DID print out**: "All done. Success.".
     If you do encounter any errors – please contact the teaching assistants.
   - b. On the script output, you will find the new contents of the DB. You can also find them in the db_info.txt file.
2. Your machine is hosting a web-server at port 80 (standard HTTP port).
   The root of the server is at "/var/www/" (so, if you browse "http://127.0.0.1/login.html", you'll get the file at "/var/www/login.html").
   Please refer to the "/var/www/login.html" and "/var/www/check_login.php" files for reference throughout the exercise.
3. Your machine also has a local MySQL server running. You will be using the credentials listed in the db_info.txt file.
4. **If you believe you have changed the DB and wish to restore it –** You may run the "./reset_tables.sh" command from your extracted exercise directory at any time. **Make sure to verify its output validity as you did when unpacking the exercise.**
5. **Please remember the new submission guidelines, and remember to submit all parts of your solution and any instructions needed to use and understand them.**

6. Create an HTML file at "/var/www/add_user.html" –
   (you may need to fix permissions / owner for the file. Use ls –l /var/www/ login.html as a reference)
   - a. Add a form with the following text fields:
     - i. Username
     - ii. Password
   - b. The form shall submit the data to "/add_user.php" via a POST request.
   - c. Please keep your HTML code clean and lean (and mean) – overly-complicated auto-generated HTML will be easy to spot and we may deduct points.
7. Create a PHP file at "/var/www/add_user.php"–
   (you may need to fix permissions / owner for the file. Use ls –l /var/www/check_login.php as a reference)
   - a. Get the user and password via POST.
   - b. Check the parameters for correctness
   - c. Add the new user to the 'users' table, and report to the user.
   - **d. If you believe you have changed the DB and wish to restore it – You may run the "./reset_tables.sh" command from your extracted exercise directory.**

8. Create a PHP file at "/var/www/show_users.php"–
   (you may need to fix permissions / owner for the file. Use ls –l /var/www/check_login.php as a reference)

a. List all the users in the 'users' table, and for each user show its –

i. ID

ii. Username

iii. Password

b. Print this info in a three (3) column HTML table.
(make sure your code works for any number of users, don't assume there will only be 4 entries in the DB).

9. Now, look at "/var/www/login.html" and "/var/www/check_login.php" (accessible at http://localhost/login.html and http://localhost/check_login.php)

a. When valid usernames and passwords are submitted, the output will be "Successful Login. Welcome, [USERNAME]."

b. Find a way to use SQL Injection to bypass authentication.

c. Write down where the vulnerability is, what should be submitted to the server and in what way.

10. Look at "/var/www/dbg/state/log/a/b/c/d/e/f/g/login2.html" and "/var/www/dbg/state/log/a/b/c/d/e/f/g/check_login2.php" (accessible at http://localhost/dbg/state/log/a/b/c/d/e/f/g/login2.html and http://localhost/dbg/state/log/a/b/c/d/e/f/g/check_login2.php)

a. This version requires the user to submit her username, id and password (the id is the same id from the database).

b. Find a way to use SQL Injection to bypass authentication.

c. Write down where the vulnerability is, what should be submitted to the server and in what way.

d. Try to find more than one way to accomplish this.

11. Now, look at "/var/www/dbg/state/log/a/b/c/d/e/f/g/login3.html" and "/var/www/dbg/state/log/a/b/c/d/e/f/g/check_login3.php" (accessible at http://localhost/dbg/state/log/a/b/c/d/e/f/g/login3.html and http://localhost/dbg/state/log/a/b/c/d/e/f/g/check_login3.php)

a. This version is very similar to login2.html and check_login2.php, and the same "tricks" will work.

b. However, this version allows an attacker to learn something. Can you figure out what it is?

c. Bonus: Figure out how you can make this method stronger by using ORDER BY.