[CS492B] Web Security Attack Lab.

Assignment #1 (due: Mar 25th 2022, 11:59 PM, KLMS)

T.A.: Jihwan Kim (payload@kaist.ac.kr), Sunnyeo Park (psnyeo88@kaist.ac.kr)

1. Skeleton code for Assignment #1

KLMS

2. Description

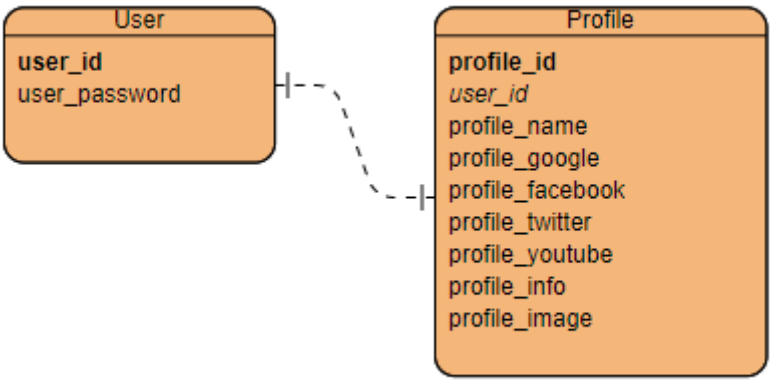
In this assignment, you will extend your previous lab work on the profile viewer webpage. Your profile webpage should handle user information and profile information using a database (MySQL) and supports various features such as registering users, login, or editing profiles. The followings are features you will implement in this assignment:

- (User) Register
- (User) Login
- (Profile) Create a new profile
- (Profile) Edit a profile
- (Profile) Remove a profile
- (Advanced) Profile Hiding

3. Problems

1) [10 points] Create a Database and Tables

Write a sql file that creates a database and table(s) with your own structure. Following is an example structure for this assignment, you can refer to it.



You do not have to consider any kinds of errors that can occur when a database or table already exists. And, you also do not have to submit an explanation of DB, you will submit only a single sql file.

2) [35 points] Implement user-related functions

a. Register

Complete the function `register` in `lib.user.php`. This function takes two parameters, userid, and password. In this function, you have to insert (userid, password) into the User table you created. The followings are constraints that must be satisfied:

- User ID can not be duplicated
- Passwords should be longer than 8 letters.

If any of the above 2 constraints are not satisfied, data must not be inserted, and the function should return -1. Otherwise, the function should return 0 in success.

b. Login

Complete the function `login` in `lib.user.php`. This function takes two parameters, userid, and password. In this function, you have to check whether (userid, password) is in the User table or not.

If there is a (userid, password) in the User table, the function should return 0. Otherwise, the function should return -1 on failure. After login success, userid will be saved in $_SESSION[“user”].

3) [40 points] Implement profile-related functions

a. Create

Complete the function `create` in `lib.profile.php`. This function takes a single parameter ‘userid’. In this function, you have to create a profile when the user has not created a profile yet.

If a user already created a profile, this function should return -1. Otherwise, return 0 in success.

b. Edit

Complete the function `modify` in `lib.profile.php`. This function may have any parameters you want. Also, you have to edit html elements to handle them correctly. Return 0 in success. Otherwise, return -1 for any errors.

Also, you have to complete `profile.php` to be worked with your `modify` function.

c. Remove

Complete the function `remove` in `lib.profile.php`. This function takes a single parameter ‘userid’. In this function, you have to delete a profile when the user created a profile.

If a user did not create a profile yet, this function should return -1. Otherwise, return 0 in success.

d. View

Complete the function `get_profile` in `lib.profile.php`. This function takes a single parameter ‘userid’. In this function, this function has to return the user's profile information correctly.

If a profile is not created yet, this function should return -1. Otherwise, return information properly.

Also, you have to complete `profile.php` to be worked with your `get_profile` function.

4) [10 points] Implement a ‘Hide Profile’ feature

Extend a profile page to prohibit other users from viewing someone’s profile. If the profile is marked as hidden, the only logged-in user who’s the owner of the profile can watch the profile. To implement this feature, you may need to extend a DB structure, and also edit some HTML.

3. Submission

You have to submit the following two things:

- An archived source code: **Assignment1_{StudentID}.tar.gz**
- A URL of your service (in KCLOUD VM): http://(NAT IP)/assignment1

Due date: March 25th, 2022, 11:59 PM

Extended Due: March 26th, 2022, 11:59 PM

- If you have late submission until Extended Due, you can get half of the score.
- If you have late submission after Extended Due, you can’t get any scores.