CIS 12
Lab Assignment 13

This lab uses elements from lab 5 (sitename database), lab 6 (forum database), lab 9 (Script 9.5), and lab 12 (Script 12.2) to validate data and to prevent attacks. I am going to need to see copies of the code for each of the parts of the lab, along with the screenshots requested.

For Parts 1 - 5 create a folder called **Ch13** and put the files created in there.

For Parts 6 and 7, you will be altering the register.php (Script 9.5) that you used in labs 9 and 12. Therefore, you should use **Ch12** folder for both parts.

Part 1 - Validating Data by Type Pg. 425

1. Follow steps 1 - 10 on pages 427 - 430 to create the **calculator.php** file.
2. Test it in your web browser by typing in the information from Pictures D and E on page 430
3. **Screenshot both before and after pictures.**

Part 2 - Validating Files by Type Pg. 431

1. Follow steps 1 - 12 on pages 431 - 434 to create the **upload_rtf.php** file.
2. Like lab 11, this file will upload a rich text file (rtf) to the uploads folder. If you do not have an uploads folder in **htdocs**, make one and make sure the permissions give read and write permissions to the administrator, as we've done previously.
3. Either download or create your own rtf file using MSWord. (I googled **sample rtf file** and clicked on the first link. I used that downloaded file.)
4. Upload the rtf file and screenshot the result of the webpage.
5. **Upload a file that's not an rtf and screenshot the result of the webpage.**

Part 3 - Preventing XSS Attacks Pg. 435

1. Follow steps 1 - 9 on pages 436 - 437 to create the **xss.php** file.
2. Enter the code from Picture A on page 435 in the text box and press submit. **Screenshot the result.**

Part 4 - Using the Filter Extension Pg. 438

1. Follow steps 1 - 45 on pages 439 - 441 to upgrade the **calculator.php** file.
2. Test the script in the web browser and type the information from Picture A on page 441, resulting in Picture B. **Screenshot both before and after pictures.**

Part 5 - Preventing SQL Injection Attacks Pg. 442

1. Turn on SQL Server
2. You are going to need to use the ch. 6 forum database. If you need the code, I have a copy for you to download on Canvas.
3. Instead of using a mysqli_connect.php file, we are going to implement code to connect to the database in the file that you create.
4. Follow steps 1 - 12 on pages 444 - 448 to create the **post_message.php** file. Be sure to use the settings on line 15 in your file that we've been using the entire time. Replace username with root and password with the empty string.
5. Test the script by typing in some html, like in Picture B on Page 446. Press Submit.
6. Check your database. It will strip the tags and turn the text into regular text, thus making the code entered harmless in the database. Go to your database and **screenshot the result in your database.**

Part 6 - Securing Passwords with PHP Pg. 449

1. Follow the steps 1 - 4 on pages 452 - 454 to update script 9.5, **register.php** from lab 9. You will be altering the script from lab 9, that was used in lab 12, so you should use the **Ch12** folder for this lab section. Replace the old register.php file with this new version of the script. This will create Script 13.7 in the text.
2. Test it by following step 4 on page 454 using Pictures C and D. Register a new user that is not previously in the database. **Screenshot both the result of Picture C and the result from the database in Picture D.** Picture D shows the CLI way of doing it. Choose whichever way works for you.

Part 7 - To update the login process Pg. 455

1. Follow the steps from 1 - 5 from pages 455 - 457 to update Script 12.2, **login_functions_inc.php**, from Lab 12. You are altering the file from lab 12, so you should use the **Ch12** folder for this lab section. This will create Script 13.8 in the text. There is a small discrepancy between the code on step 3 on page 455 and the file on line 55 on page 456. Go with the code on step 3 on page 455.
2. Register a new user and password using the register form in the website. Then login using that user from the browser and **screenshot the result**, which is from Picture E on page 457.