Report for second two weeks:

For these two weeks, I continued the unfinished work from first two weeks. At first I started working on client side validation of registration page, using JQUERY, as the validation criteria for most of the required validation are already built in JQUERY, so it was lot easier to write a client side validation this way compared to using JavaScript and writing everything manually.

After I was done with client side validation, I started working on the server side validation of the same registration page with PHP, as there ways to bypass client side validation using different web browser add-ons. So whenever users fill out registration form and submit the information, if information entered passes the client side validation, the PHP is script checks if user has used those add-ons to bypass client side validation. After information is validated with PHP script then, those information is further processed to insert into the database table.

The first step in process to insert information into database is clean up the information entered by the users as some of the hackers can use registration page for the purpose of SQL injection. So the information needed to be clean up using syntax like “mysqli_real_escape_string”. After that the data are inserted into the database tables using insert statement.

After I was done with registration part, I started working on user login. I and my employer we decided to put a small login form in right side of the home page (www.perilchute.com). Procedure for the user login was pretty similar to the user registration. Information are needed to be validated both on client side and server side, the information are needed to be cleaned up to prevent SQL injection. The only difference is compare statement is used to validate login information with the information in database tables. So if the result is positive user are directed to the www.perilchute.com/plan.php page. If not they sent back to login error page to enter the login information again.