WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Project Topic/Title : Minifacebook Web Application

Team members

1. Member 1, Sohan Chidvilas Bodapati , bodapass@mail.uc.edu
2. Member 2, Maheedhar Atmakuru, atmakuma@mail.uc.edu
3. Member 3, Bhanu Suraj kurella, kurelbj@mail.uc.edu

Project Management Information

Source code repository : https://github.com/waph-team16/waph-teamproject

Project homepage (public): https://waph-team16.github.io/

Project presentation demo video link (youtube) : https://www.youtube.com/watch?v=wYeu7cuiBPE

Revision History

Date	Version	Description
24/03/2024	1.0	Sprint 0
31/03/2024	2.0	Sprint 1
16/04/2024	3.0	Sprint 2
25/04/2024	4.0	Final Submission

Overview of Final Project

Our team has achieved a milestone with the completion of the miniFacebook web application, during the WAPH course. The project, developed through sprints showcases an integration of full stack web technologies and robust security practices. From designing the database foundation to implementing user features each stage demonstrates our teamwork and commitment.

The miniFacebook app provides users with a registration process. Ensures a secure social networking environment. We have prioritized user data protection by implementing HTTPS deployment hashed passwords and role based

access control. Additionally features like real time chat and superuser account management enhance user interaction and administrative capabilities.

Looking back on our journey we are proud of the approach we took in addressing requirements, alongside stringent security measures and meticulous attention to detail. Our project report, demo video and organized repository collectively showcase our expertise in web development and security principles.

System Analysis

The development of our social network application revolves around a steadfast commitment to fortifying security measures at every stage of its design and implementation. Through rigorous testing and meticulous validation processes, we ensure that our application remains impervious to common threats such as Cross-Site Scripting (XSS), SQL injection attacks, and Cross-Site Request Forgery (CSRF). By employing stringent input sanitization techniques, all user inputs undergo thorough scrutiny, mitigating the risk of malicious code injection and bolstering the application's resilience against potential vulnerabilities. Furthermore, sensitive user data is encrypted using robust hashing algorithms before storage in the database, ensuring enhanced data protection and safeguarding user privacy.

Complementing its robust security framework, our social network application offers a suite of advanced functionalities geared towards empowering administrators and enhancing user experience. With role-based access control mechanisms, administrators wield granular control over user privileges and application functionalities, enabling them to moderate posts, manage user accounts, and enforce security policies with ease. Real-time chat capabilities, facilitated through the Web Socket protocol, foster seamless communication between users while upholding data integrity and confidentiality. Continual updates and optimizations further ensure the application's scalability, performance, and resilience, reinforcing its position as a trusted platform for secure and engaging social interaction.

High-level Requirements

System Design

Our system design encapsulates a comprehensive integration of functional and non-functional requirements, augmented by robust security measures, culminating in the development of a fully-fledged networking website. Employing a three-tier architecture, we have orchestrated a seamless synergy between presentation, application, and data layers, with PHP serving as the primary backend language. The entire application is orchestrated atop the LAMP stack, harnessing the collective power of Linux, Apache, MySQL, and PHP technologies.

For data management, we have harnessed the efficiency and reliability of the MySQL database system, ensuring seamless storage and retrieval of user information while upholding stringent security standards. On the frontend, we have leveraged a combination of HTML, CSS, and JavaScript programming languages to craft an intuitive and visually captivating user interface.

Moreover, our system design places paramount emphasis on security sanitizations, encompassing a suite of measures to thwart potential threats such as XSS, SQL injection attacks, and CSRF vulnerabilities. By adhering to industry best practices and implementing stringent input sanitization techniques, we fortify the application against malicious exploits, safeguarding user data and privacy.

In essence, our meticulously crafted system design amalgamates cutting-edge technologies with rigorous security protocols, laying the foundation for a secure, scalable, and immersive networking experience.

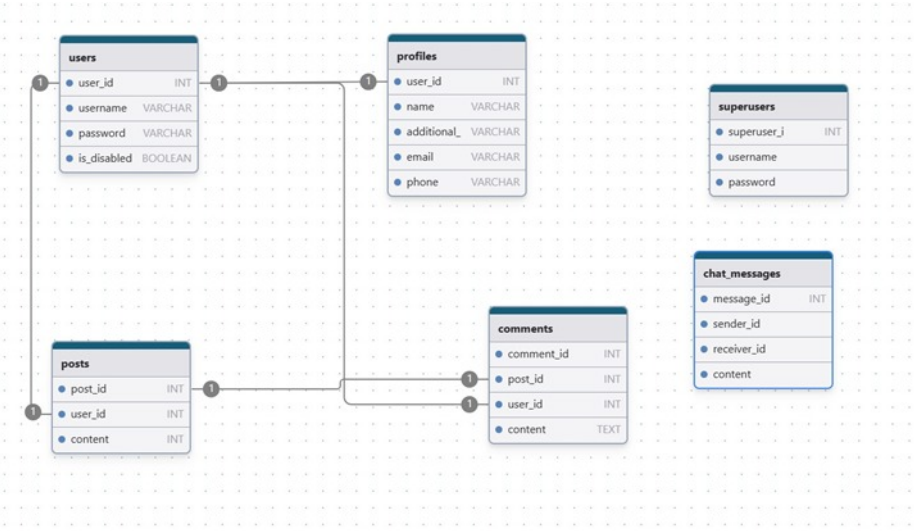

Figure 1: Database system design

User Registration:

Any user can create an account in our web application through register.,php page as shown below

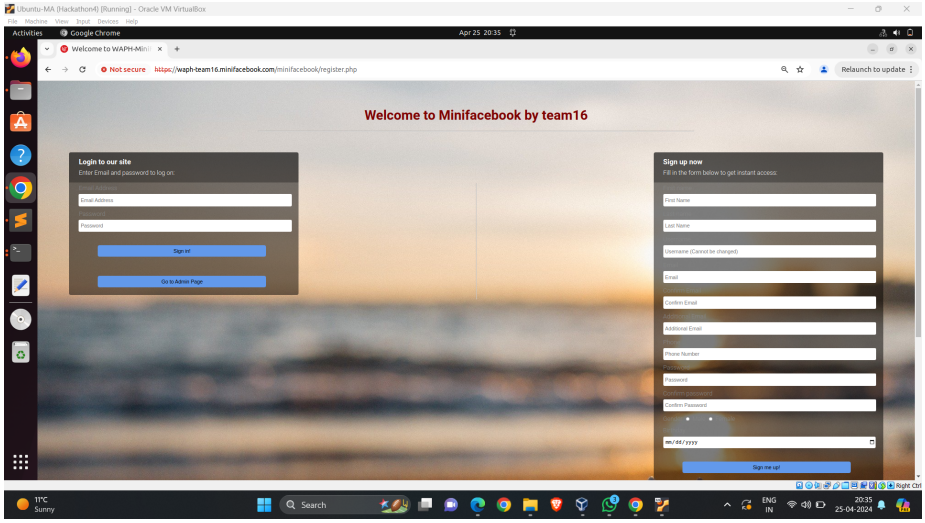

Figure 2: Registration Page

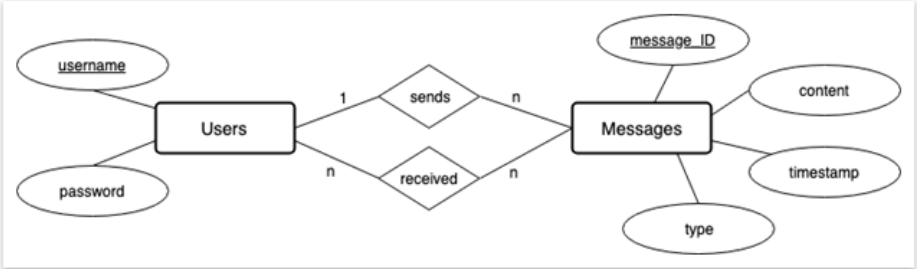

Figure 3: Registration Page

Database creation:

User Interface from previous sprints

Registration account:

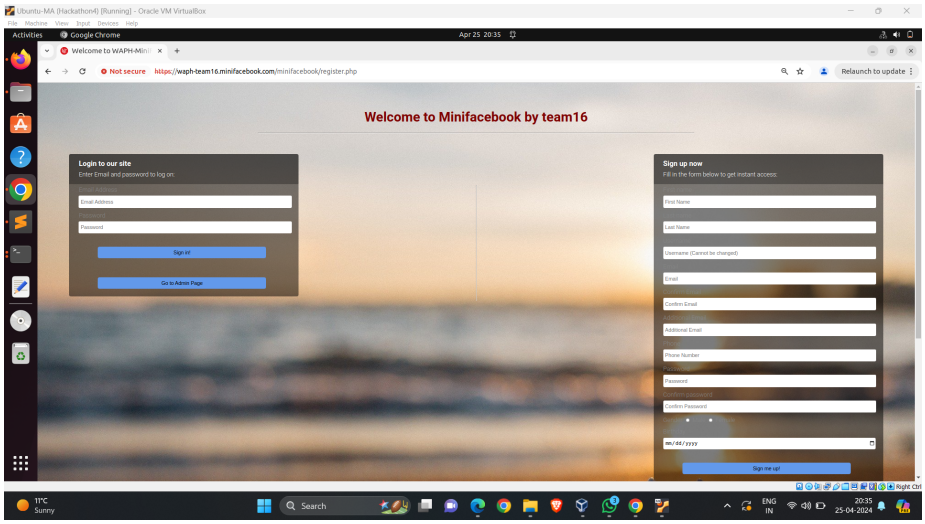

Figure 4: Registration Page

Change password page:

Add a new post:

New post can be added from the home page itself, User need to enter the post details and click on share button

Edit the post:

User can edit post by clicking on pen icon shown in home page, once he click on edit icon if he is the post owner system will allow him to edit the post page as shown below

Delete the post:

Only post owner or admin can delete the post from the application, User can click on delete icon beside post to delete the post

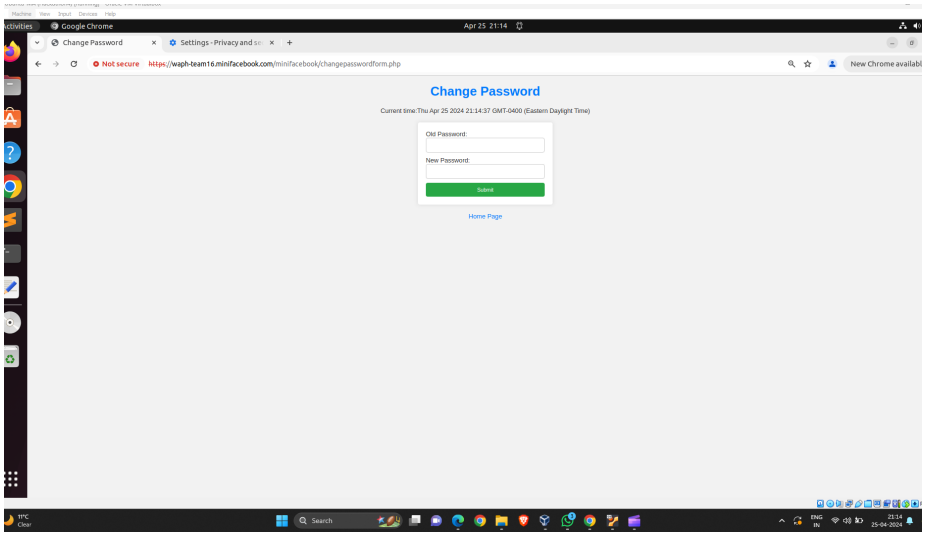

Figure 5: Change password page

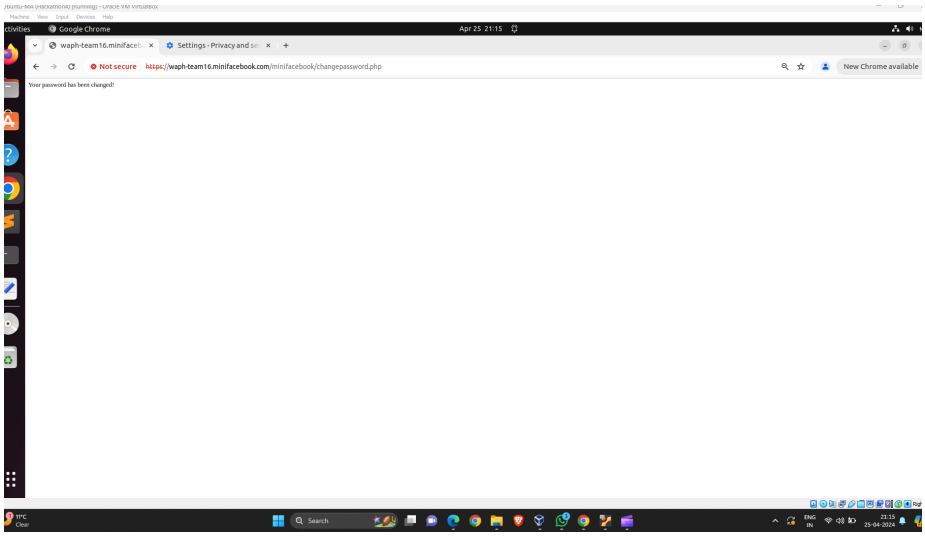

Figure 6: Password changed successfully

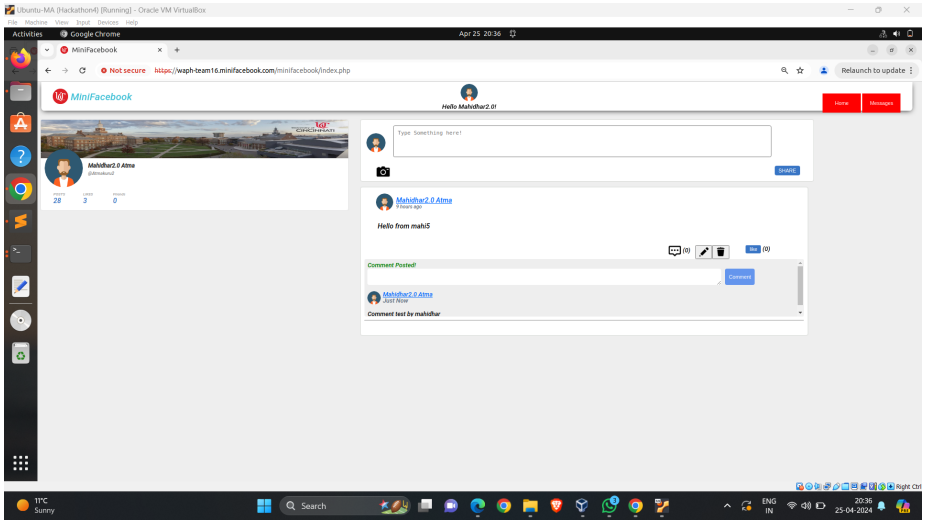

Figure 7: home page with post functionality

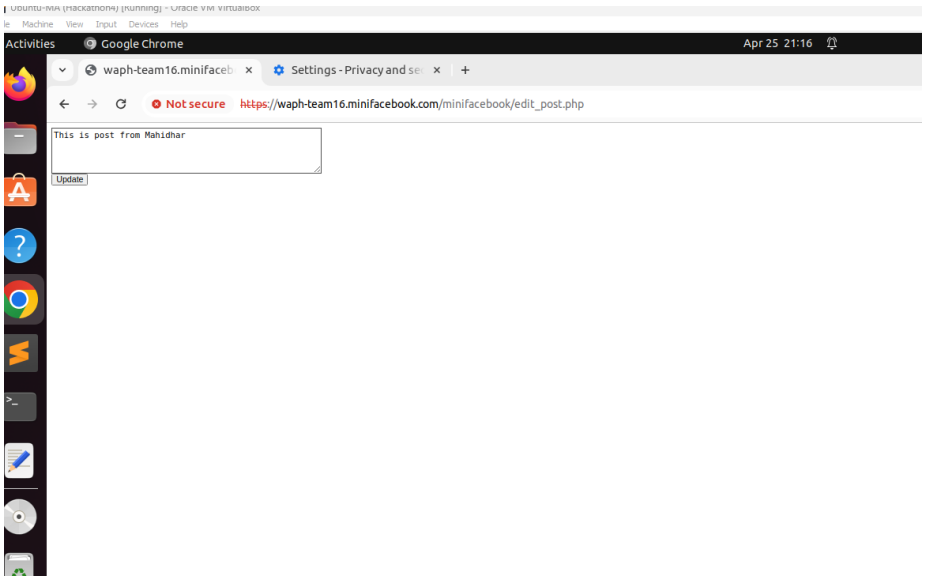

Figure 8: Edit post page

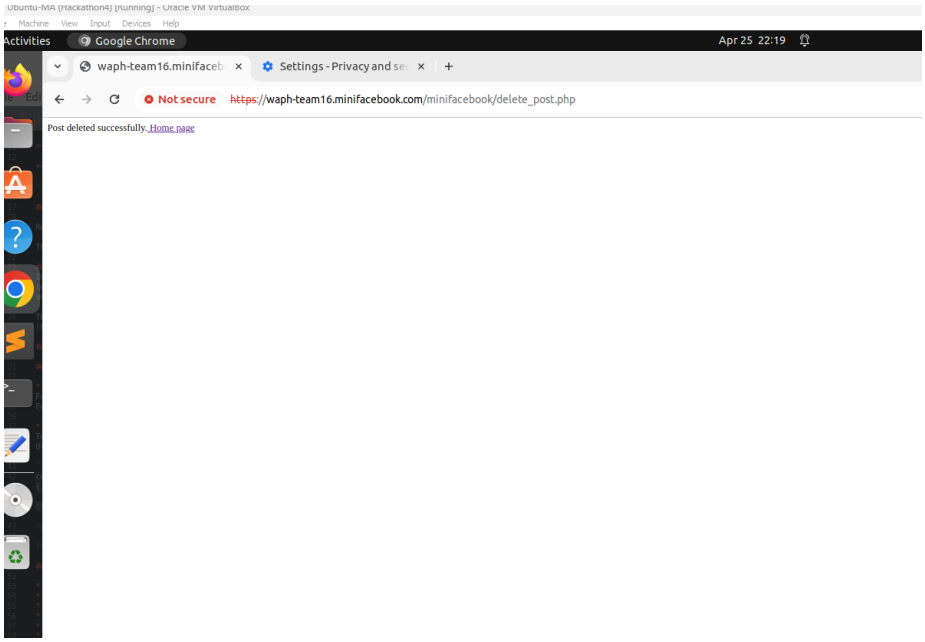

Figure 9: Delete post page

If the user tries to delete others page, system will throw error saying post cannot be deleted

Adding commments to the post:

Any user can add comments to his posts or others posts

Implementation of real time chat:

Super user:

Super user are users with higher privileges used to manage and control posts/comments posted by other users.

They can disable, enable , remove post forom the application

Login with the admin account (Database):

Below shown screenshot is landing page for superusers or admins. from there they can control the entire application content and users.

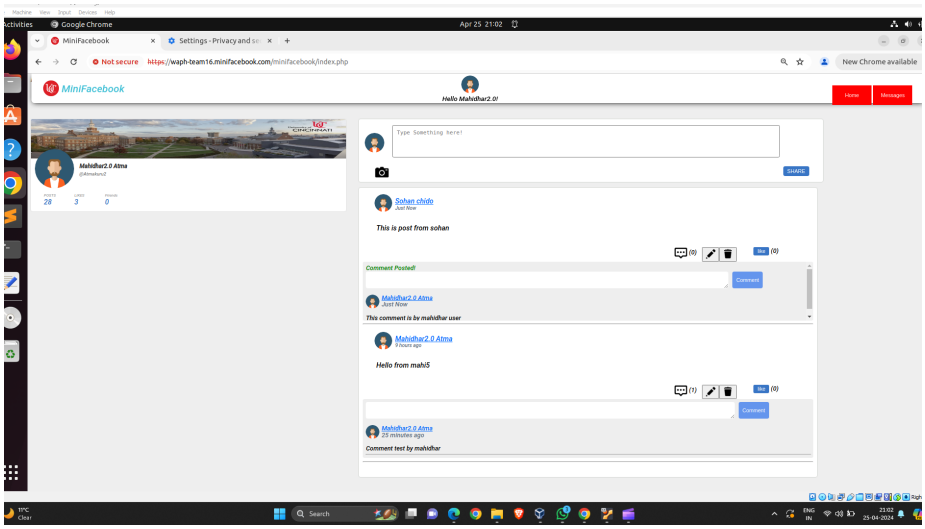

Figure 10: Comments page

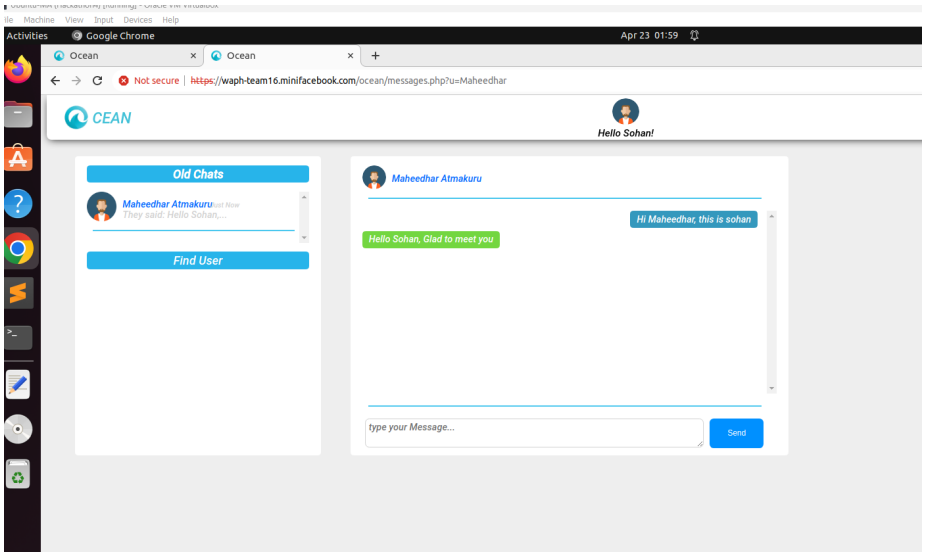

Figure 11: User can chat in real time with other users

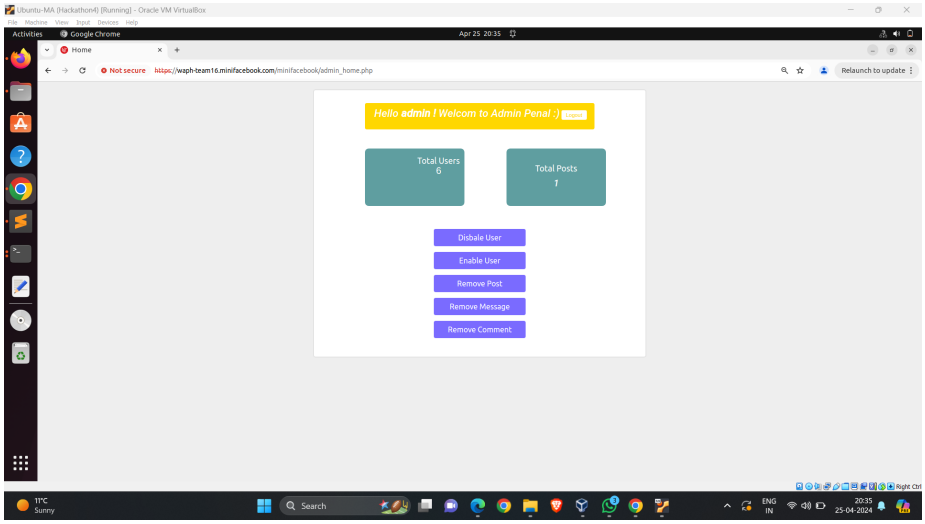

Figure 12: Super User home page

The registered users:

As we seperated the users and super users in database and also provided seperate login pages for them. A normal user cannot login from admin page.

Admin login page shown below is ony for admins

Disable users:

A super user can login into his homepage and disable other users by giving their username, once they are disabled they cannot login into system. System will throw error saying user disabled by admin

Enable users:

A disabled user can be enabled again by super user therough homepage as shown below

enabled user can login again same as before

Security analysis:

We have implemented certain prvention methodologies that includes **HTML ENTITIES** , ehich sanitizesthe user input. We also made application secure against XSS attacks, SQL Injections and CSRF attacks.

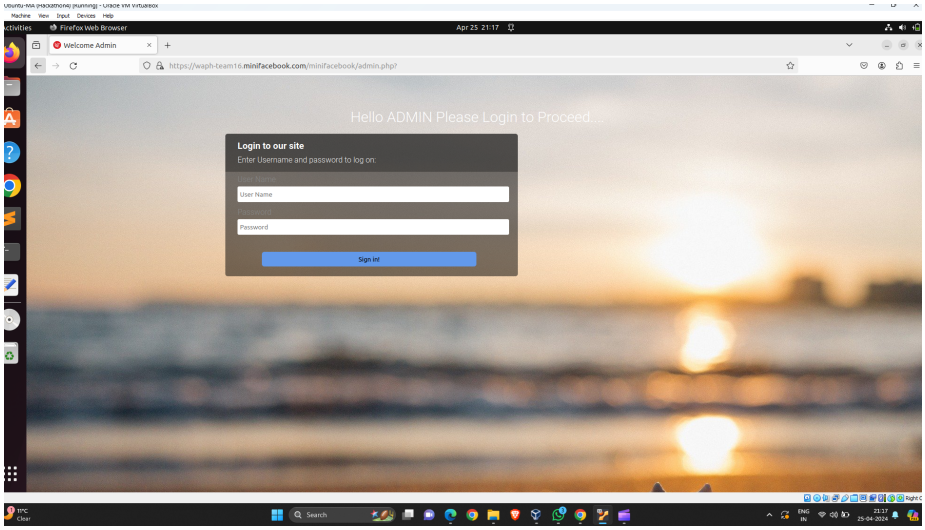

Figure 13: Admin Login Page

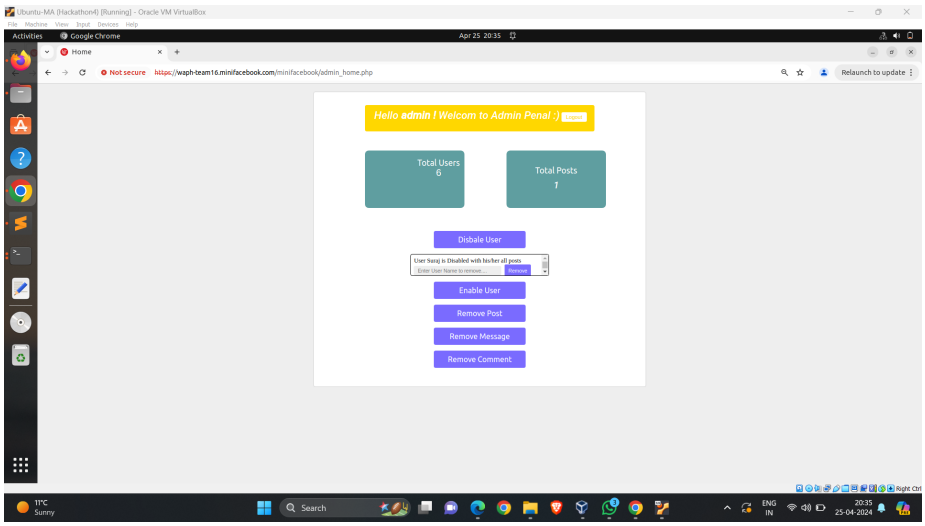

Figure 14: Disabling user from Admin Homepage

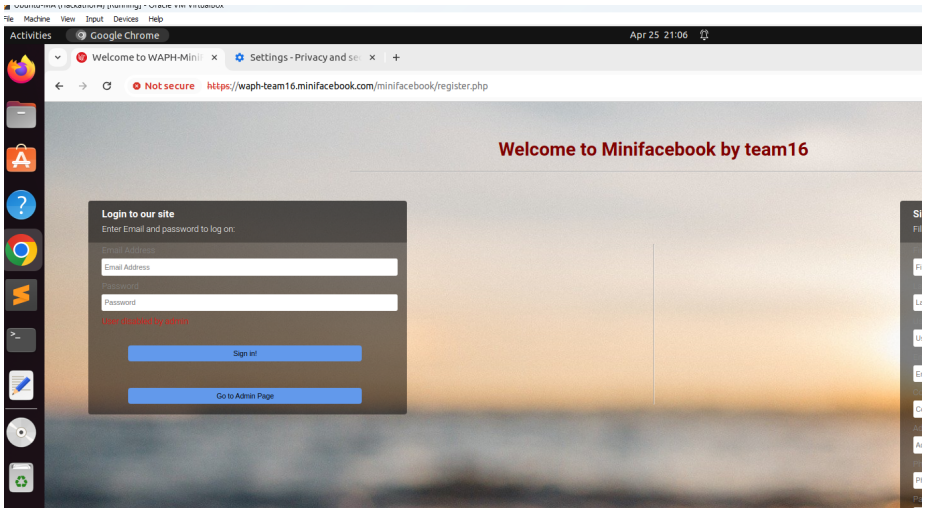

Figure 15: Error when disabled user login

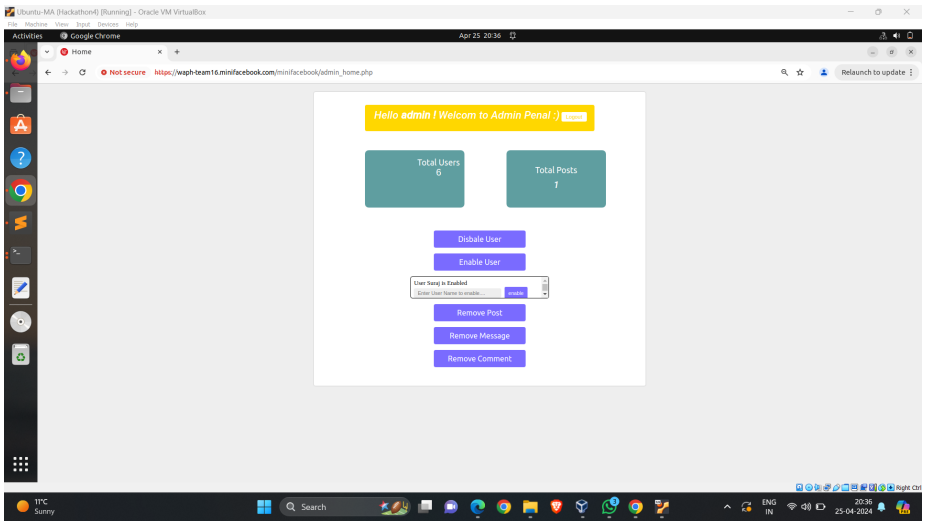

Figure 16: Disabling user from Admin Homepage

We performed thorough testing and resulted screenshots are provided below

HTTPS Deployment:

web app is deployed over https server as shown below

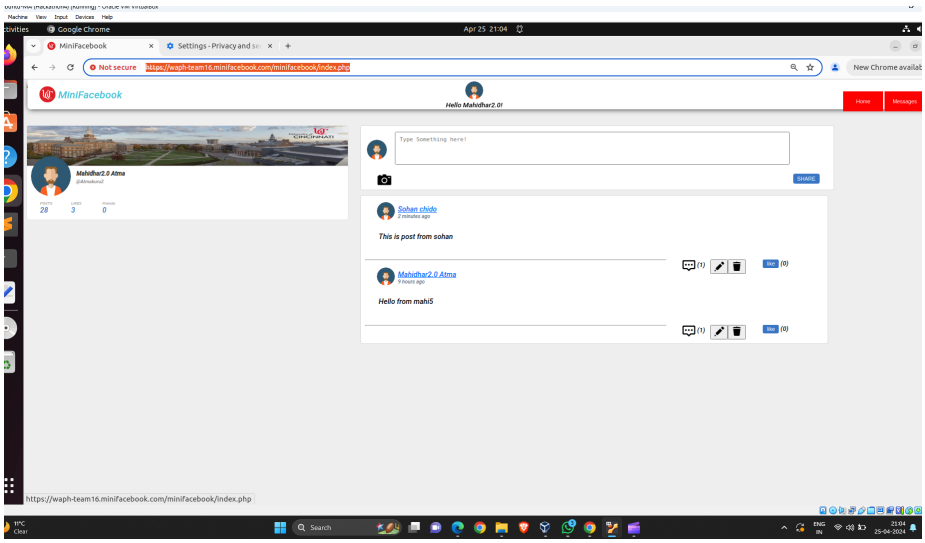

Figure 17: Web application running over https

Passwords being hashed:

passwords are hashed inside database

SQL in Prepared Statements:

All sql scripts are stored in database-data.sql file as shown in below

Input validation:

Input from users is validated and sanitized in all layes as shown below

HTML being sanitized:

In all html code the code is sanitized and output i

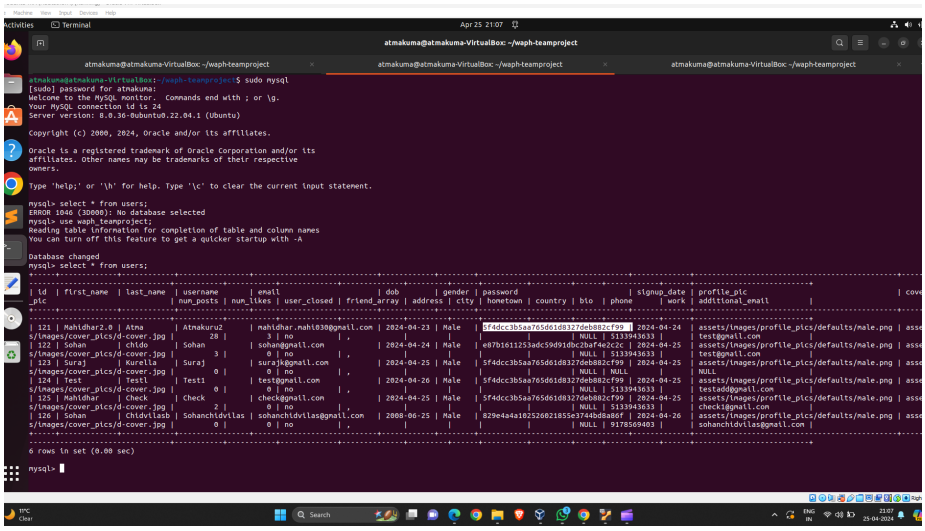

Figure 18: Hashed passwords stored inside database

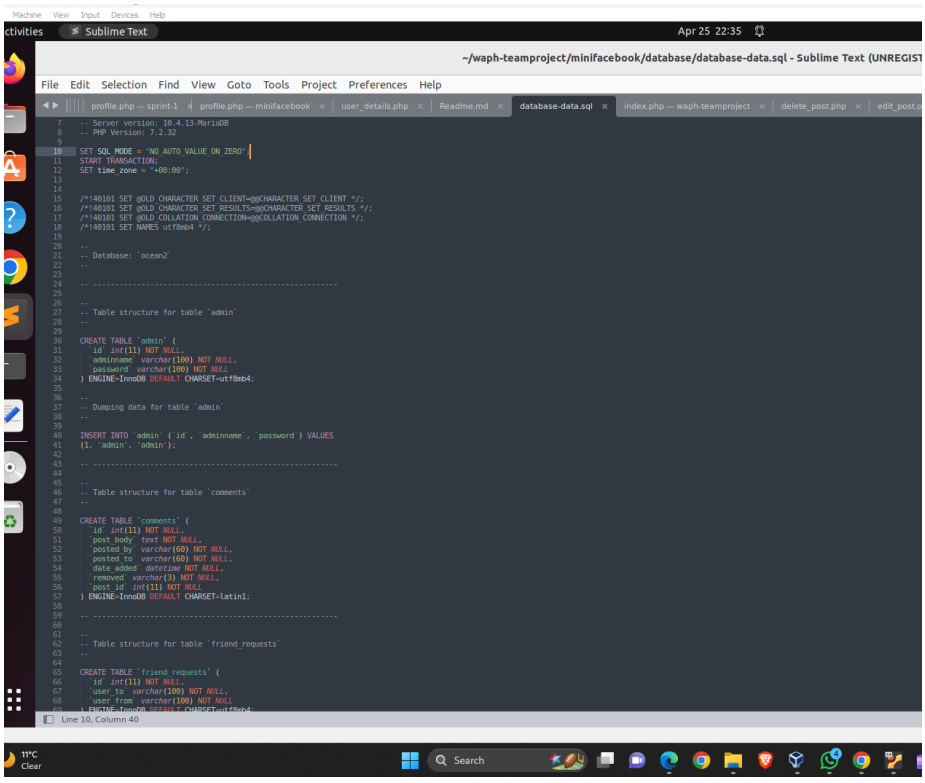

Figure 19: prepared statements in sql

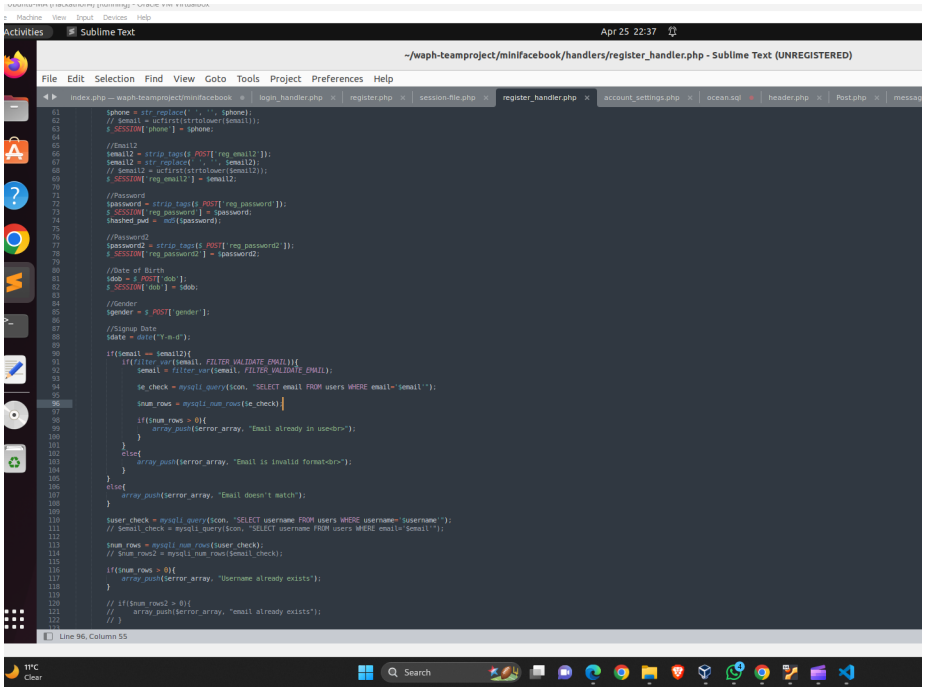

Figure 20: input validations on registration page

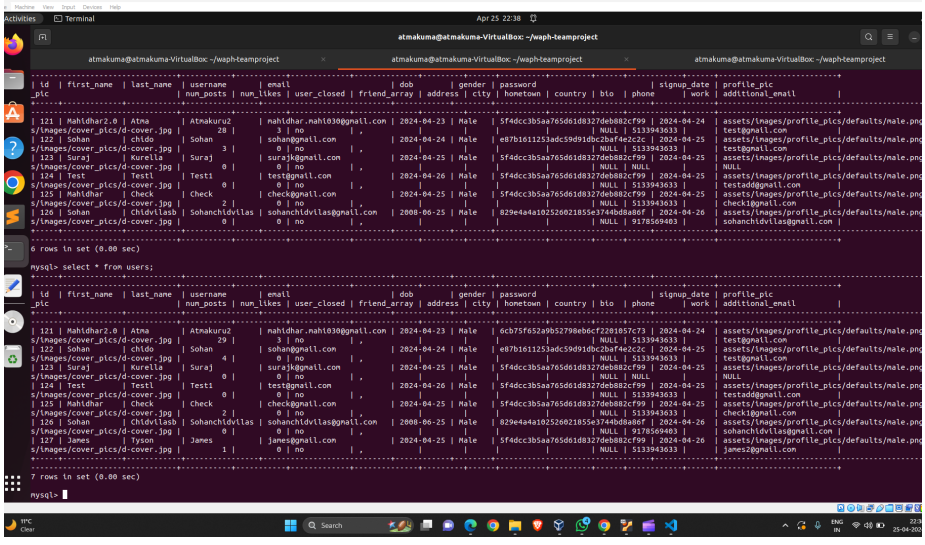

Figure 21: Sanitized db data

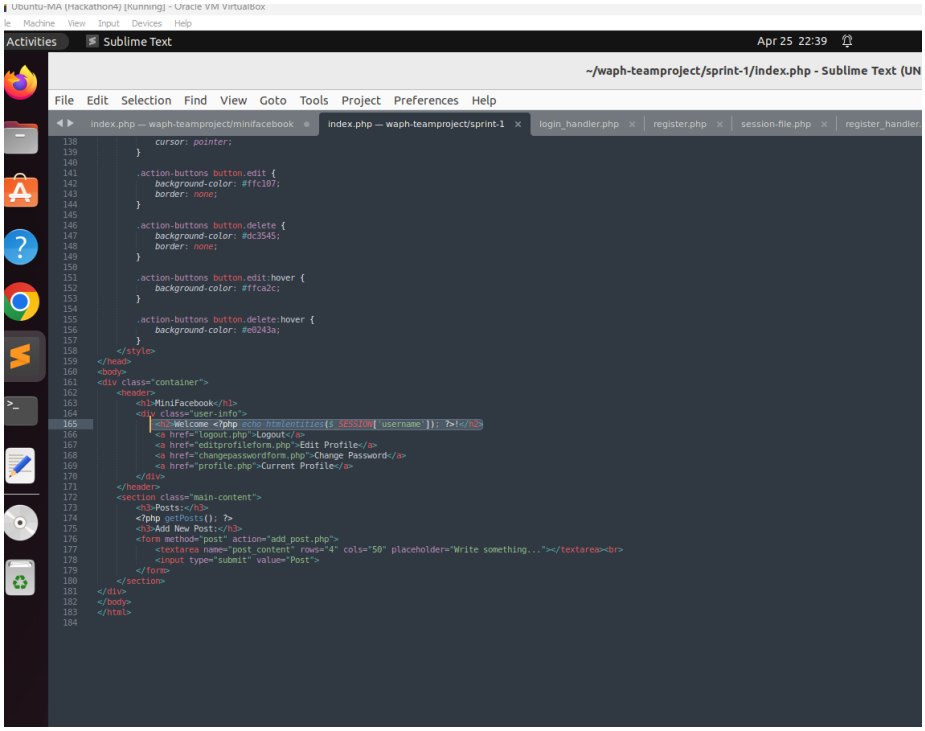

Figure 22: HTML ENTITIES used for input sanitization

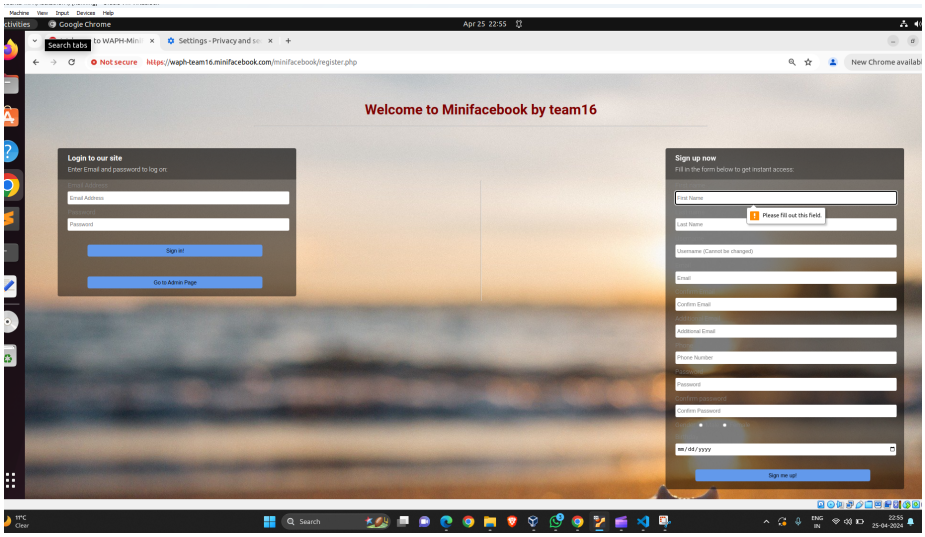

Figure 23: All html outputs are validated and sanitized

Role based access:

Regular user cannot login as super user as their login pages and tdatabase tables are seperated.

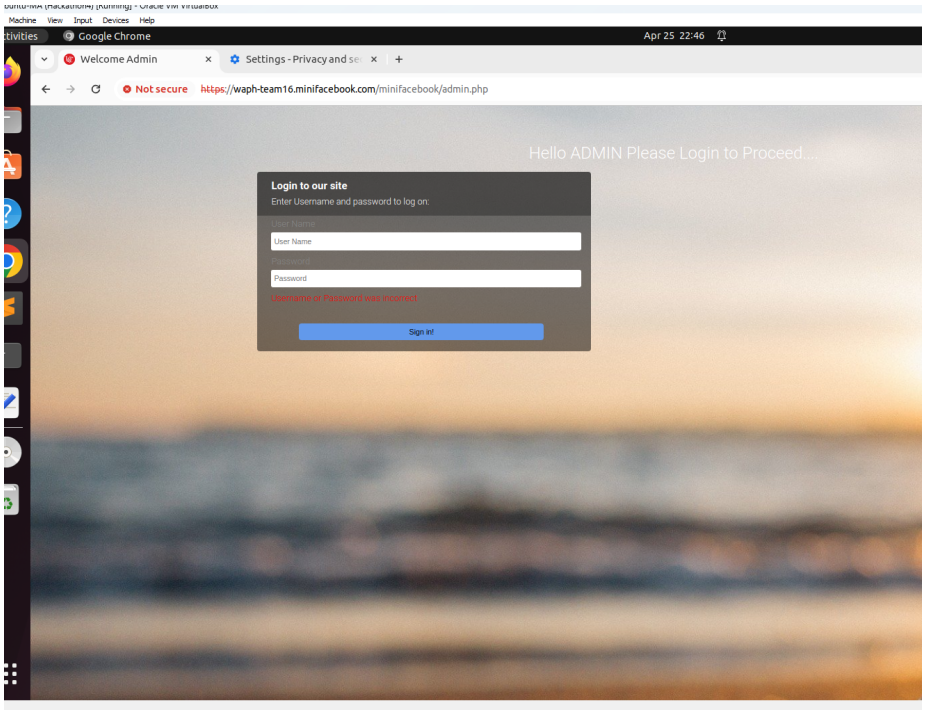

Figure 24: Regular user attempt to login as superuser

Normal user cannot edit or delete posts of other users when the attept system throws below error

Prevention of Session Authentication and Hijacking:

CSRF Protection of website:

CSRF check is performed against the web app and resulted image is shown below

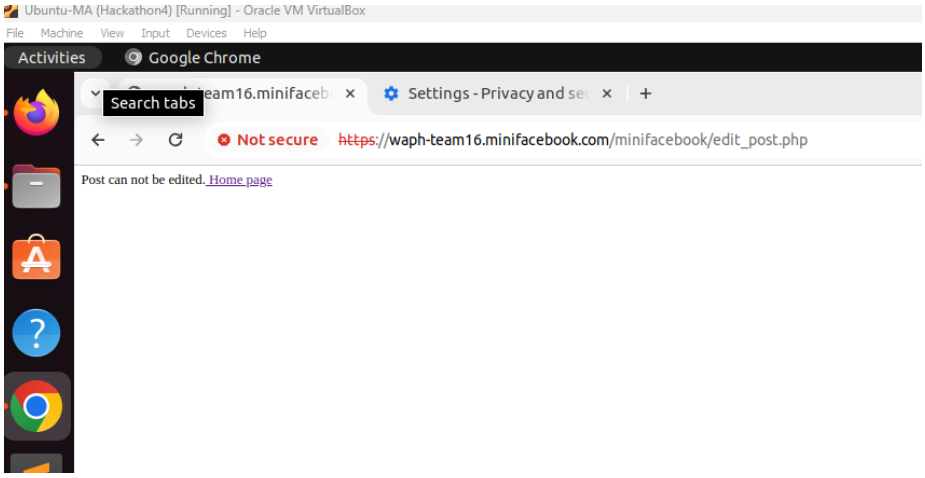

Figure 25: Post edit failed by other user

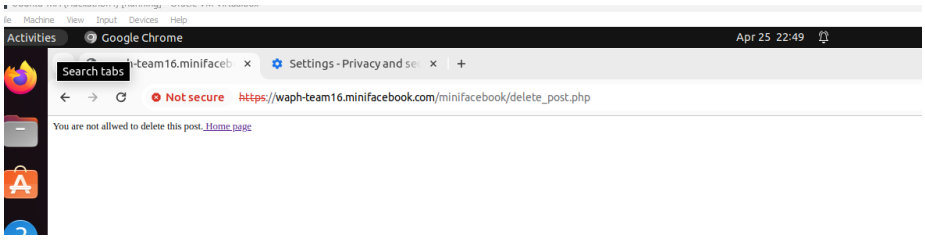

Figure 26: Post delete attempt by other user

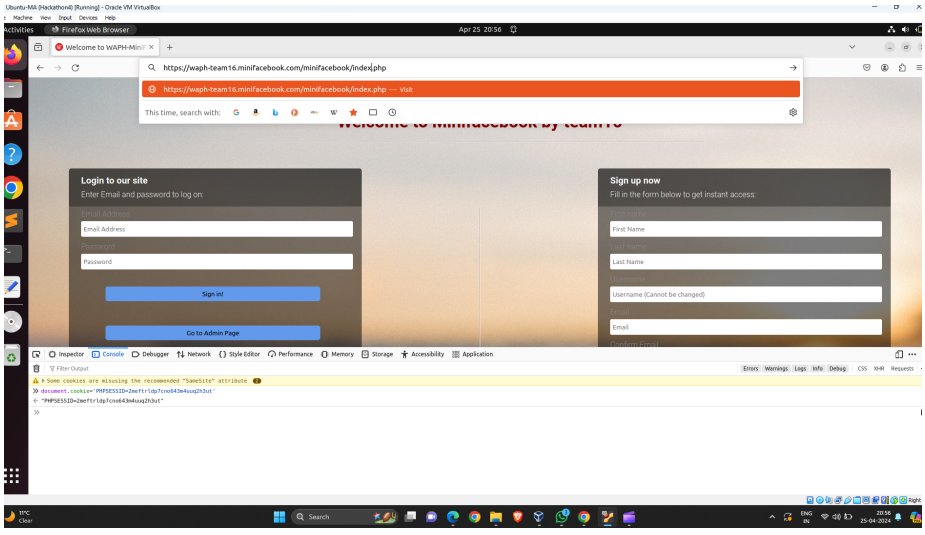

Figure 27: Session Hijacking test on Web application

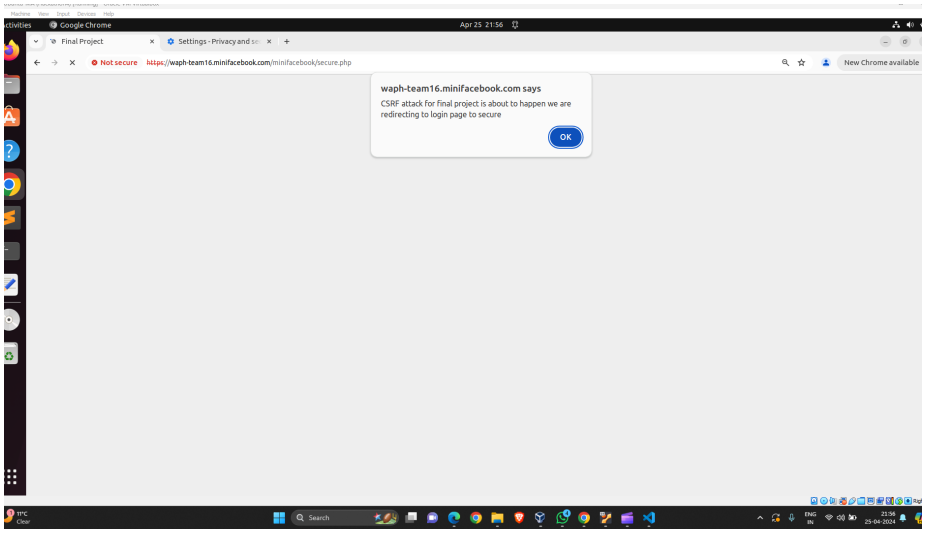

Figure 28: CSRF attack check

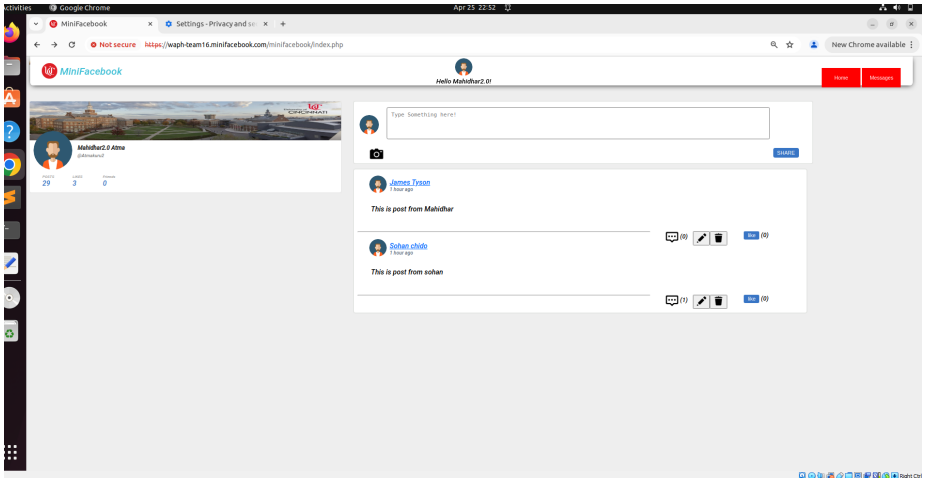

Figure 29: CSRF attack check

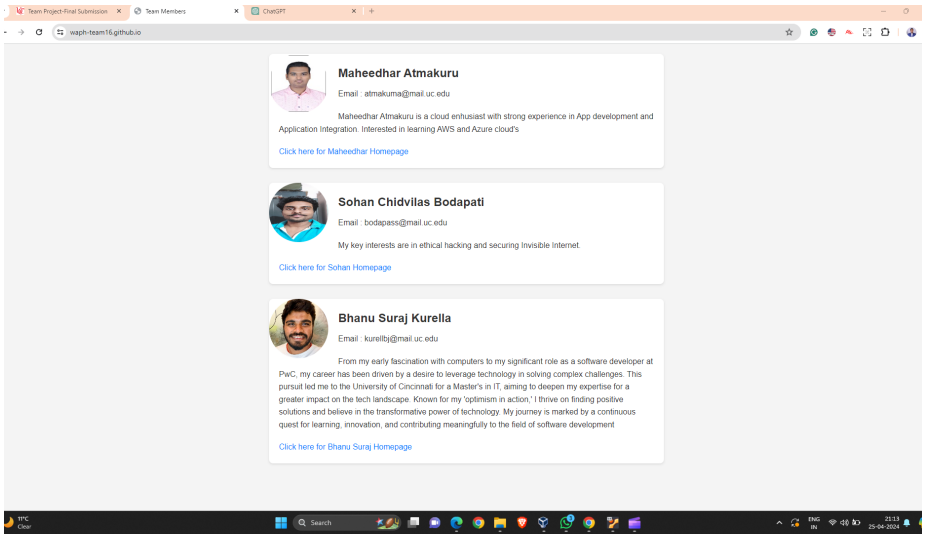

Figure 30: WAPH-team16 Website

Open source template of CSS:

A team project website:

Software Process Management

(Start from Sprint 0, keep updating)

Introduce how your team uses a software management process, e.g., Scrum, and how your teamwork collaborates.

Sprint 0: 11:59 pm March 24 Links to an external site. Sprint 0-Getting Started assignment aims to foster initial collaboration among team members using Scrum practices, enabling your team to become acquainted and prepare collaboratively for the entire project's scope. Sprint 1: 11:59 pm March 31

Sprint 2: 11:59 pm April 16 (changed from 11)

Sprint 3: No submission Links to an external site. A super user can disable/enable an account A disabled account cannot login Integrating the Chat system

Scrum process

Sprint 0

Completed Tasks: Links to an external site. Database Design and Implementation (can be incomplete and to be updated) User registration and login Logged

in users can Change password Edit their profile, including name, additional email, phone View posts from the database

Sprint 1

Duration: MM/DD/YYYY-MM/DD/YYYY

Completed Tasks: Links to an external site. Logged-in users can add a new post, and add a comment on any post Logged-in users can edit (update, delete) their own posts A user cannot edit posts of other users

Contributions:

1. Maheedhar Atmakuru, 140 commits, 180 hours, contributed in Code development and Setup
2. Sohan Chidvilas Bodapati, 25 commits, 60 hours, contributed Database Setup and Security implementation Code development
3. Bhanu Sura Kurella, 5 commits, 20 hours, contributed in Development and documentatin

Appendix

Source code to Markdown

/enable_user.php

```
<!-- enable user.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    include 'session-file.php';
    include 'database/classes/User.php';
    // include 'database/classes/Post.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }
```

```php
?>

<?php
    if(isset($_POST['search_user_btn']))
    {
        $user = $_POST['search'];
        // $query = mysqli_query($con, "delete from users where username='$user'") or die("
        $query = mysqli_query($con, "update users set user_closed='no' where username='$use
        if($query){
            echo "User $user is Enabled";
        }
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Remove User</title>
    <style>
        input[type="text"]{
            width: 70%;
            height: 25px;
            padding: 5px;
            border-radius: 5px;
            border: none;
            background: #eeeeee;
            padding-left: 10px;
        }

        input[type="submit"]{
            padding: 5px 10px;
            background: #7a6bff;
            border: none;
            border-radius: 3px;
            color: white;
            height: 32px;
            margin-left: 5px;
        }
    </style>
</head>
<body>
    <form action="enable_user.php" method="post">
        <input type="text" name="search" placeholder="Enter User Name to enable....">
        <input type="submit" name="search_user_btn" value="enable">
```

```
    </form>
</body>
</html>
```

/session-file.php

```
<!-- Session-file.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php


ob_start();
session_start();

$timezone = date_default_timezone_set("Asia/Kolkata");

$con = mysqli_connect("localhost","waph_team16","password","waph_teamproject");

if(mysqli_connect_errno()){
    echo "Failed to connect: " . mysqli_connect_errno();
}
// else{
//     echo'Connected';
// }

?>
```

/user_closed.php

```
<!-- User Closed.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php include 'database/header.php';?>

<style>
.user_closed_main_colum{
    width: 700px;
    background: white;
    margin-top: 150px;
    margin-bottom: 150px;
    margin-left: auto;
    margin-right: auto;
    border-radius: 5px;
```

```
    text-align: center;
    padding-top: 25px;
    padding-bottom: 30px;
    padding-left: 20px;
}



</style>

<div class="user_closed_main_colum">

    <h1> User closed </h1>

    This user is closed :(

    <a href="index.php"> click here to go back -></a>


</div>
```

/remove_msg.php

```
<!-- Remove msg.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->


<?php

    include 'session-file.php';
    include 'database/classes/User.php';
    include 'database/classes/Post.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }

?>
```

```php
<?php
    if(isset($_POST['search_msg_btn']))
    {
        $msg = $_POST['search'];
        $query = mysqli_query($con, "delete from messages where id='$msg'") or die("No msg
        if($query){
            echo "msg no. $msg is Deleted";
        }
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Remove Post</title>
    <style>
        input[type="text"]{
            width: 70%;
            height: 25px;
            padding: 5px;
            border-radius: 5px;
            border: none;
            background: #eeeeee;
            padding-left: 10px;
        }

        input[type="submit"]{
            padding: 5px 10px;
            background: #7a6bff;
            border: none;
            border-radius: 3px;
            color: white;
            height: 32px;
            margin-left: 5px;
        }
    </style>
</head>
<body>
    <form action="remove_msg.php" method="post">
        <input type="text" name="search" placeholder="Enter Message ID to remove....">
        <input type="submit" name="search_msg_btn" value="Remove">
    </form>
</body>
</html>
```

/request.php

```
<!-- Request.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php  include 'header.php';
    //   include 'classes/User.php';
    //   include 'classes/Post.php';
?>
<style>
    .main_column{
        width: 700px;
        background: white;
        margin-top: 95px;
        margin-bottom: 150px;
        margin-left: auto;
        margin-right: auto;
        border-radius: 5px;
        padding-top: 1px;
        padding-bottom: 30px;
        padding-left: 20px;
    }
    #accept{
        background: #0090ff;
        border: none;
        border-radius: 3px;
        padding: 5px 10px;
        margin-top: 5px;
        color: white;
    }

    #reject{
        background: darkorange;
        border: none;
        border-radius: 3px;
        padding: 5px 10px;
        margin-top: 5px;
        color: white;
    }

    #pro_pic{
        height: 55px;
        width: 55px;
        border-radius: 50%;
```

```
    }

    .name{
        margin-left: 65px;
        margin-top: -52px;
        margin-bottom: auto;
    }

    hr{
        margin-top: 13px;
        width: 350px;

    }


</style>

    <div class="main_column">

        <h4> Friend Request </h4>

        <div class="request_inner">

            <?php

            $query = mysqli_query($con, "select * from friend_requests where user_to='$userl
            if(mysqli_num_rows($query)==0){
                echo "No friend request";
            }
            else{

                while($row = mysqli_fetch_array($query)){
                    $user_from = $row['user_from'];
                    $get_pic_query = mysqli_query($con, "select * from users where username=
                    $get_pic = mysqli_fetch_array($get_pic_query);
                    $request_pic = $get_pic['profile_pic'];
                    $user_from_obj = new User($con, $user_from);
                    echo "<br><img id='pro_pic' src='".$request_pic."'><br><div class='name'
                    $user_from_friend_array = $user_from_obj->getFriendArray();

                    if (isset($_POST['accept'.$user_from])) {
                        $add_friend_query = mysqli_query($con, "update users set friend_arra
                        $add_friend_query = mysqli_query($con, "update users set friend_arra

                        $delete_query = mysqli_query($con, "delete from friend_requests wher
```

```
                echo $user_from . " and YOU are friend now!";
                header("Location: request.php");

            }
            if (isset($_POST['reject'. $user_from])) {
                $delete_query = mysqli_query($con, "delete from friend_requests wher

                echo "Request Denied!";
                header("Location: request.php");
            }

            ?>

            <form action="request.php" method="POST">

                <input type="submit" name="accept<?php echo $user_from ?>" id="accep
                <input type="submit" name="reject<?php echo $user_from ?>" id="rejec


            </form>
            </div>
            <?php
        }
    }
    ?>

</div>


</div>
```

/messages.php

```
<!-- Message.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php include 'header.php';
    //   include 'classes/User.php';
    //   include 'classes/Post.php';
    //   include 'classes/Message.php';


      //get the most recebt user from conversetion
      $message_obj = new Message($con, $userLoggedIn);
      if(isset($_GET['u']))
```

```
        $user_to = $_GET['u'];
        else {
            $user_to = $message_obj->getMostRecentUser();
            if ($user_to == false)
            $user_to = 'new';
          }

          if($user_to != "new")
              $user_to_obj = new User($con, $user_to);

      //geting data about the user_to
      $get_uset_to_data = mysqli_query($con, "select * from users where username='$user_to'");
      $user_to_info = mysqli_fetch_array($get_uset_to_data);

      if(isset($_POST['submit_msg'])){
          if(isset($_POST['msg_body'])){
              $body = $_POST['msg_body'];
              $body = mysqli_real_escape_string($con, $body); //egnore the ' in post boddy
              $date = date("Y-m-d H:i:s");
              $message_obj->sendMessage($user_to, $body, $date);
          }
      }

      if(isset($_POST['search_btn'])){
          $msg="";
          $user = $_POST['search'];
          $query = mysqli_query($con, "select * from users where username='$user'");
          if($query){
              header("Location: messages.php?u=$user");
          }
          else {
              $msg = "No User Found";
          }
      }

  ?>

  <style>
      .msg_main{
          width: 700px;
          height: 475px;
          position: fixed;
          background: white;
          margin-top: 95px;
          margin-bottom: 150px;
          margin-left: 515px;
```

```
    margin-right: auto;
    border-radius: 5px;
    padding-top: 1px;
    padding-bottom: 30px;
    padding-left: 20px;
    padding-right: 20px;
}

.old_chats{
    width: 375px;
    height: 475px;
    position: fixed;
    background: white;
    margin-top: 95px;
    margin-bottom: 150px;
    margin-left: 50px;
    margin-right: auto;
    border-radius: 5px;
    padding-top: 1px;
    padding-bottom: 30px;
    padding-left: 20px;
    padding-right: 20px;
}

.name{
    margin-top: auto;
    margin-bottom: auto;
    margin-left: 10px;
}

hr{
    width: 95%;
    background: rgb(73, 199, 238);
    border: none;
    height: 2px;
    margin-left: 10px;
    margin-bottom: 20px;
}

#msg_area{
    width: 80%;
    height: 37px;
    margin-right: 10px;
    margin-left: 5px;
    border-radius: 7px;
    border: 2px solid #D3D3D3;
```

```
    font-size: 16px;
    font-family: 'roboto';
    padding: 5px;
}

input[type="submit"]{
    padding: 5px 30px 5px 30px;
    height: 50px;
    background: #0090ff;
    color: white;
    border: none;
    border-radius: 7px;
    margin-top: auto;
    margin-bottom: auto;
    position: absolute;
}

.msg{
    border: 1px solid #000;
    border-radius: 5px;
    padding: 5px 10px;
    display: inline-block;
    color: #fff;
}

.msg#blue{
    background: #3498bd;
    border-color: #3498bd;
    float: right;
    margin-right: 15px;
    /* margin-bottom: 5px; */
}

.msg#green{
    background: #73d640;
    border-color: #73d640;
    float: left;
    /* margin-bottom: 5px; */
}

.load_msgs{
    height: 65%;
    overflow-y: scroll;
    margin-bottom: 20px
}
```

```
    .headding, .find_user{
        margin-top: 15px;
        margin-bottom: 15px;
        font-size: 20px;
        color: #ffffff;
        border: 1px solid #27b4ea;
        padding: 5px;
        border-radius: 5px;
        background: #27b4ea;
    }

    a{
        text-decoration-line: none;
    }

    .chat_name{
        margin-left: 60px;
        margin-top: -40px;
    }

    .other{
        margin-left: 60px;
        margin-top: -17px;
        color: #d3d3d3;
    }

    .time_sml{
        font-size: 12px;
        margin-left: 148px;
        color: #d3d3d3;
    }

    .chat_p{
        margin-top: 0px;
    }

    .chats{
        overflow-y: scroll;
    }


</style>

    <div class="msg_main">
        <div class="msg_heading" >
            <div class="heading_wreper" style="margin-top: 15px; display: flex;">
```

```
            <?php
                if($user_to != "new"){
                    echo "<span ><img style='height: 40px;margin-bottom: 3px;border-radi
                    echo "<span class='name'><a href='$user_to'>".$user_to_obj->getFname
                }
                else {
                    echo "New Message";
                }
            ?>
        </div>
    </div>
    <hr>
        <?php
            echo "<div class='load_msgs' id='scroll_msg'>";
                echo $message_obj->getMessages($user_to);
            echo "</div>";
        ?>
    <hr>
    <div class="send_msg">
        <div class="msg_wreper">
            <form action="" method="post">
                <?php
                    if ($user_to == "new") {
                        echo "Search the friend to start conversesion<br><br>";
                        echo "To : <input type='text' id='msg_area' name='search' placeh
                        echo "<input type='submit' name='search_btn' value='Search'>";
                        echo "<lable value='search_lbl'>";
                    }
                    else {
                        echo "<textarea name='msg_body' id='msg_area' placeholder='type
                        echo "<input type='submit' name='submit_msg' value='Send'>";
                    }
                ?>
            </form>
        </div>
    </div>
</div>

<script>//privent loading msgs from top
    var div = document.getElementById("scroll_msg");
    div.scrollTop = div.scrollHeight;
</script>

<div class="old_chats">
    <div class="chat_wreper">
        <div class="headding">
```

```
                <span class="head"><b><center>Old Chats</center></b></span>
            </div>
            <div class="chats">
                <?php echo $message_obj->getOtherChats(); ?>
            </div>
            <div class="find_user"><center><a style="color:white;" href="messages.php?u=new'
        </div>
    </div>
```

/changepassword.php

```
<?php
    session_start();


    $username = $_SESSION["username"];
    $old_password = $_POST["old_password"];
    $new_password = $_POST["password"];

    if (isset($username) && isset($old_password) && isset($new_password)) {
        if (authenticateUser($username, $old_password)) {
            if (changepassword($username, $new_password)) {
                echo "Your password has been changed!";
            } else {
                echo "Failed to change password!";
            }
        } else {
            echo "Authentication failed! Please check your old password.";
        }
    } else {
        echo "Incomplete data provided!";
    }

    function authenticateUser($username, $old_password) {
        // $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
        // if ($mysqli->connect_errno) {
        //     printf("Database connection failed: %s\n", $mysqli->connect_error);
        //     return false;
        // }

        // $prepared_sql = "SELECT password FROM users WHERE username = ?";
        // $stmt = $mysqli->prepare($prepared_sql);
        // $stmt->bind_param("s", $username);
        // $stmt->execute();
        // $result = $stmt->get_result();
        // $row = $result->fetch_assoc();
```

```
        // // Check if old password matches the stored password
        // if (password_verify($old_password, $row['password'])) {
        //     return true;
        // } else {
        //     return false;
        $con= mysqli_connect("localhost","waph_team16","password","waph_teamproject");
        $hashed_pwd = md5($old_password);
        $check_database_query = mysqli_query($con, "SELECT * FROM users WHERE username='$use
        $check_login_query = mysqli_num_rows($check_database_query);

        if($check_login_query == 1){
            return true;
                                    }
                                }

    // function changepassword($username, $new_password) {
    //     $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    //     if ($mysqli->connect_errno) {
    //         printf("Database connection failed: %s\n", $mysqli->connect_error);
    //         return false;
    //     }

    //     // Hash the new password before updating
    //     $hashed_password = password_hash($new_password, PASSWORD_DEFAULT);

    //     $prepared_sql = "UPDATE users SET password = ? WHERE username = ?";
    //     $stmt = $mysqli->prepare($prepared_sql);
    //     // Binding parameters
    //     $stmt->bind_param("ss", $hashed_password, $username);
    //     $stmt->execute();
    //     // Checking if the execution was successful
    //     if ($stmt->affected_rows == 1) {
    //         return true;
    //     } else {
    //         return false;
    //     }
    // }


        function changepassword($username, $password)
{
    $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    if ($mysqli->connect_errno) {
        printf("Database connection failed: %s\n", $mysqli->connect_error);
        return FALSE;
```

```
    }

    // Hash the password before updating
    $hashed_password = md5($password);

    $prepared_sql = "UPDATE users SET password = ? WHERE username = ?;";
    $stmt = $mysqli->prepare($prepared_sql);
    // Binding parameters
    $stmt->bind_param("ss", $hashed_password, $username);
    $stmt->execute();
    // Checking if the execution was successful
    if ($mysqli->affected_rows == 1)
        return TRUE;
    return FALSE;
}
?>
```

/handlers/register_handler.php

```
<!-- Register Hendler.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php


    $fname = "";
    $lname = "";
    $username = "";
    $password = "";
    $password2 = "";
    $email = "";
    $email2 = "";
    $add_email="";
    $phone="";
    $date = "";
    $dob = "";
    $gender = "";
    $add = '';
    $city = '';
    $home_town = '';
    $country = '';
    $work = '';
    $error_array = array();
    $success_array = array();

    if(isset($_POST['reg_user'])){
```

```php
//First Name
$fname = strip_tags($_POST['reg_fname']);
$fname = str_replace(' ', '', $fname);
$fname = ucfirst(strtolower($fname));
$_SESSION['reg_fname'] = $fname;

//Last Name
$lname = strip_tags($_POST['reg_lname']);
$lname = str_replace(' ', '', $lname);
$lname = ucfirst(strtolower($lname));
$_SESSION['reg_lname'] = $lname;

//Username
$username = strip_tags($_POST['username']);
$username = str_replace(' ', '', $username);
$username = ucfirst(strtolower($username));
$_SESSION['username'] = $username;

//Email
$email = strip_tags($_POST['reg_email']);
$email = str_replace(' ', '', $email);
// $email = ucfirst(strtolower($email));
$_SESSION['reg_email'] = $email;


//Additional Email
$add_email = strip_tags($_POST['add_email']);
$add_email = str_replace(' ', '', $add_email);
// $email = ucfirst(strtolower($email));
$_SESSION['add_email'] = $add_email;

//Phone
$phone = strip_tags($_POST['phone']);
$phone = str_replace(' ', '', $phone);
// $email = ucfirst(strtolower($email));
$_SESSION['phone'] = $phone;

//Email2
$email2 = strip_tags($_POST['reg_email2']);
$email2 = str_replace(' ', '', $email2);
// $email2 = ucfirst(strtolower($email2));
$_SESSION['reg_email2'] = $email2;

//Password
$password = strip_tags($_POST['reg_password']);
$_SESSION['reg_password'] = $password;
```

```php
$hashed_pwd =  md5($password);

//Password2
$password2 = strip_tags($_POST['reg_password2']);
$_SESSION['reg_password2'] = $password2;

//Date of Birth
$dob = $_POST['dob'];
$_SESSION['dob'] = $dob;

//Gender
$gender = $_POST['gender'];

//Signup Date
$date = date("Y-m-d");

if($email == $email2){
    if(filter_var($email, FILTER_VALIDATE_EMAIL)){
        $email = filter_var($email, FILTER_VALIDATE_EMAIL);

        $e_check = mysqli_query($con, "SELECT email FROM users WHERE email='$email''

        $num_rows = mysqli_num_rows($e_check);

        if($num_rows > 0){
            array_push($error_array, "Email already in use<br>");
        }
    }
    else{
        array_push($error_array, "Email is invalid format<br>");
    }
}
else{
    array_push($error_array, "Email doesn't match");
}

$user_check = mysqli_query($con, "SELECT username FROM users WHERE username='$userna
// $email_check = mysqli_query($con, "SELECT username FROM users WHERE email='$emai

$num_rows = mysqli_num_rows($user_check);
// $num_rows2 = mysqli_num_rows($email_check);

if($num_rows > 0){
    array_push($error_array, "Username already exists");
}
```

```
        // if($num_rows2 > 0){
        //     array_push($error_array, "email already exists");
        // }

        if(strlen($username) > 20 || strlen($username) < 2){
            array_push($error_array, "Username must be between 2 and 20");
        }

        else if(preg_match('/[^A-Za-z0-9]/', $username)){
            array_push($error_array, "You username can only contain english characters or nu
        }

        if(strlen($fname) > 25 || strlen($fname) < 2){
            array_push($error_array, "Your first name must be between 2 and 25 characters");
        }

        if(strlen($lname) > 25 || strlen($lname) < 2){
            array_push($error_array, "Your last name must be between 2 and 25 characters");
        }

        if($password != $password2){
            array_push($error_array, "Your passwords doesn't match");
        }
        // else{
        //     if(preg_match('/[^A-Za-z0-9]/', $password)){
        //         array_push($error_array, "Your password can only contain english characte
        //     }
        // }

        if(strlen($password) > 30 || strlen($password) < 5){
    array_push($error_array, "Your password must be between 5 and 30 characters or numbers")
}


        if(empty($error_array)){
            // echo $password;

            $password = $password;

            if($gender == "Male"){
                $profile_pic = "assets/images/profile_pics/defaults/male.png";
                $cover_pic = "assets/images/cover_pics/d-cover.jpg";
            }

            if($gender == "Female"){
                $profile_pic = "assets/images/profile_pics/defaults/female.png";
```

```
            $cover_pic = "assets/images/cover_pics/d-cover.jpg";
        }


        $query = "INSERT INTO users (first_name, last_name, username, email, dob, gender
        if(mysqli_query($con, $query))
        {
            $_SESSION['username'] = $username;
            // header('location: index.php');
            // echo "success :)";
            array_push($success_array, "success");
        }
        else{
            echo "fail". mysqli_connect_errno();
            array_push($success_array, "failed");
        }

    }

    // else{
    //     for ($i=0; $i < count($error_array); $i++) {
    //         echo $error_array[$i] . '<br>';
    //     }
    // }
}

?>
```

/handlers/login_handler.php

```
<!-- login Handler.PHP^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->
<?php

$lifetime = 15 * 60;
$path = "/";
$domain = "192.167.9.255";
$secure = TRUE;
$httponly = TRUE;
session_set_cookie_params($lifetime, $path, $domain, $secure, $httponly);
session_start();

$error_array_login = array();

if(isset($_POST['login_button'])){
    $email = filter_var($_POST['log_email'], FILTER_SANITIZE_EMAIL);
```

```
    $_SESSION['log_email'] = $email;
    $password = $_POST['log_password'];
    $hashed_pwd = md5($password);

    $check_database_query = mysqli_query($con, "SELECT * FROM users WHERE email='$email' AND
    $check_login_query = mysqli_num_rows($check_database_query);

    if($check_login_query == 1){
        $row = mysqli_fetch_array($check_database_query);
        $username = $row['username'];

        $user_closed_query = mysqli_query($con,"select * from users where email='$email' and
        if(mysqli_num_rows($user_closed_query) == 1){
            // $reopen_acc = mysqli_query($con, "update users set user_closed='no' where ema
            array_push($error_array_login, "User disabled by admin");
        }
        else {
        $_SESSION['username'] = $username;
        $_SESSION['authenticated'] = TRUE;
        header("Location: index.php");
        exit();
    }
    }
    else{
        array_push($error_array_login, "Email or Password was incorrect");
    }
}

?>
```

/delete_post.php

```
<?php
session_start();

if (!isset($_SESSION['authenticated']) || $_SESSION['authenticated'] !== TRUE) {
    echo "You are not logged in.";
    exit;
}

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if (isset($_POST['post_id'])) {
        $post_id = $_POST['post_id'];

        // Assuming you have a function to delete a post based on post ID
        if (deletePost($post_id)) {
```

```
            echo "Post deleted successfully.";
            echo '<a href="index.php"> Home page </a>';
        } else {
            echo "You are not allwed to delete this post.";
            echo '<a href="index.php"> Home page </a>';
        }
    } else {
        echo "Invalid request.";
        echo '<a href="index.php"> Home page </a>';
    }
} else {
    echo "Invalid request method.";
    echo '<a href="index.php"> Home page </a>';
}

function deletePost($post_id)
{
    // Check if the logged-in user is the author of the post
    if (!isPostAuthor($post_id)) {
        return false; // Unauthorized access
    }

    // Assuming you have already established a database connection
    $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    if ($mysqli->connect_errno) {
        printf("Database connection failed: %s\n", $mysqli->connect_error);
        exit();
    }

    // Delete comments associated with the post
    $sql_delete_comments = "DELETE FROM comments WHERE id=?";
    $stmt_delete_comments = $mysqli->prepare($sql_delete_comments);
    $stmt_delete_comments->bind_param("i", $post_id);
    $stmt_delete_comments->execute();

    // Delete the post
    $sql_delete_post = "DELETE FROM posts WHERE id=?";
    $stmt_delete_post = $mysqli->prepare($sql_delete_post);
    $stmt_delete_post->bind_param("i", $post_id);
    if ($stmt_delete_post->execute()) {
        return true;
    } else {
        return false;
    }
}
```

```php
function isPostAuthor($post_id)
{
    // Check if the logged-in user is the author of the post
    $username = $_SESSION['username'];

    // Assuming you have already established a database connection
    $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    if ($mysqli->connect_errno) {
        printf("Database connection failed: %s\n", $mysqli->connect_error);
        exit();
    }

    $sql = "SELECT added_by FROM posts WHERE id=? LIMIT 1";
    $stmt = $mysqli->prepare($sql);
    $stmt->bind_param("i", $post_id);
    $stmt->execute();
    $stmt->store_result();

    if ($stmt->num_rows === 1) {
        $stmt->bind_result($author);
        $stmt->fetch();
        $stmt->close();

        return $author === $username;
    }

    return false; // Post not found
}


function getUserName($username, $mysqli)
{
    $sql = "SELECT username FROM users WHERE username=?";
    $stmt = $mysqli->prepare($sql);
    $stmt->bind_param("s", $username);
    $stmt->execute();
    $result = $stmt->get_result();
    $row = $result->fetch_assoc();
    return $row['username'];
}
?>
```

/account_settings.php

```
<!-- Account setting.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->
```

```php
<?php include 'header.php';
      // include 'classes/Post.php';
     $msg = "";

    $user_detail_query = mysqli_query($con,"select * from users where username='$userLoggedI
    $user_array = mysqli_fetch_array($user_detail_query);

    if(isset($_POST['submit_cover_pic'])){
        $uploadOk = 1;
        $imageName = $_FILES['cover_pic']['name'];
        $errorMessage = "";

        if($imageName != ""){
            $targetDir = "assets/images/cover_pics/";
            $imageName = $targetDir . basename($imageName);
            $imageFileType = pathinfo($imageName, PATHINFO_EXTENSION);

            if($uploadOk){
                if(move_uploaded_file($_FILES['cover_pic']['tmp_name'], $imageName)){
                    //image Upload Okey
                    $errorMessage = "uploaded";
                }
                else{
                    $uploadOk = 0;
                    $errorMessage = "fail to upload";
                }
            }
        }

        if($uploadOk){
            $update_covet_pic = mysqli_query($con, "update users set cover_pic='$imageName'
            // header("Location: account_settings.php");
        }
        else{
            echo $errorMessage;
        }


    }

    if(isset($_POST['submit_profile_pic'])){
        $uploadOk = 1;
        $imageName = $_FILES['profile_pic']['name'];
        $errorMessage = "";

        if($imageName != ""){
```

```
        $targetDir = "assets/images/profile_pics/";
        $imageName = $targetDir . basename($imageName);
        $imageFileType = pathinfo($imageName, PATHINFO_EXTENSION);

        if($uploadOk){
            if(move_uploaded_file($_FILES['profile_pic']['tmp_name'], $imageName)){
                //image Upload Okey
                $errorMessage = "uploaded";
            }
            else{
                $uploadOk = 0;
                $errorMessage = "fail to upload";
            }
        }
    }

    if($uploadOk){
        $update_covet_pic = mysqli_query($con, "update users set profile_pic='$imageName
        // header("Location: account_settings.php");
    }
    else{
        echo $errorMessage;
    }


}

$Fname = "";
$Lname = "";
$DOB = "";
$h_town = "";

$error_array = array();

if(isset($_POST['submit_Fname'])){
    $Fname = $_POST['Fname'];
    $Fname = strip_tags($Fname); //remove thigs like <,>...etc tages
    $Fname = mysqli_real_escape_string($con, $Fname); //egnore the ' in post boddy
    $query = mysqli_query($con, "update users set first_name='$Fname' where username='$u
    if($query)
        array_push($error_array, "First name Updated :)");
    else
        array_push($error_array, "Fail to Updated First name :(");
    // header("Location: account_settings.php");
}
```

```php
if(isset($_POST['submit_Lname'])){
    $Lname = $_POST['Lname'];
    $Lname = strip_tags($Lname); //remove thigs like <,>...etc tages
    $Lname = mysqli_real_escape_string($con, $Lname); //egnore the ' in post boddy
    $query = mysqli_query($con, "update users set last_name='$Lname' where username='$us
    if($query)
        array_push($error_array, "last name Updated :)");
    else
        array_push($error_array, "Fail to Updated last name :(");
    // header("Location: account_settings.php");
}

if(isset($_POST['submit_email'])){
    $Lname = $_POST['addemail'];
    $Lname = strip_tags($Lname); //remove thigs like <,>...etc tages
    $Lname = mysqli_real_escape_string($con, $Lname); //egnore the ' in post boddy
    $query = mysqli_query($con, "update users set additional_email='$Lname' where userna
    if($query)
        array_push($error_array, "additional email Updated :)");
    else
        array_push($error_array, "Fail to Updated additional email :(");
    // header("Location: account_settings.php");
}

if(isset($_POST['submit_phonenum'])){
    $Lname = $_POST['phone'];
    $Lname = strip_tags($Lname); //remove thigs like <,>...etc tages
    $Lname = mysqli_real_escape_string($con, $Lname); //egnore the ' in post boddy
    $query = mysqli_query($con, "update users set phone='$Lname' where username='$userLo
    if($query)
        array_push($error_array, "phone number Updated :)");
    else
        array_push($error_array, "Fail to Updated phone number :(");
    // header("Location: account_settings.php");
}

if(isset($_POST['submit_date'])){
    $DOB = $_POST['DOB'];
    $DOB = strip_tags($DOB); //remove thigs like <,>...etc tages
    $DOB = mysqli_real_escape_string($con, $DOB); //egnore the ' in post boddy
    $query = mysqli_query($con, "update users set dob='$DOB' where username='$userLogge
    if($query)
        array_push($error_array, "Birth Date Updated :)");
    else
        array_push($error_array, "Fail to Updated Birth Date :(");
    // header("Location: account_settings.php");
```

```
    }

    if(isset($_POST['submit_htown'])){
        $h_town = $_POST['h_town'];
        $h_town = strip_tags($h_town); //remove thigs like <,>...etc tages
        $h_town = mysqli_real_escape_string($con, $h_town); //egnore the ' in post boddy
        $query = mysqli_query($con, "update users set hometown='$h_town' where username='$us
        if($query)
            array_push($error_array, "Hometown Updated :)");
        else
            array_push($error_array, "Fail to Updated Hometown :(");
        // header("Location: account_settings.php");
    }

?>

<style>
    .setting_main{
        width: 700px;
        height: auto;
        background: white;
        margin-top: 95px;
        margin-bottom: 150px;
        margin-left: auto;
        margin-right: auto;
        border-radius: 5px;
        padding-top: 25px;
        padding-bottom: 30px;
        padding-left: 20px;
    }
    img{
        height: 90%;
        width: 90%;
    }

    .imgs{
        height: 100px;
        width: 40%;
    }

    .setting_span{
        margin-left: 116px;
        position: absolute;
    }

    hr{
```

```
        width: 97%;
        margin-left: 0px;
    }

    center{
        font-size: 30px;
        margin-bottom: 20px;
    }

    input[type="text"]{
        margin-right: 10px;
        padding: 5px;
        border: 1px solid #7b7b7b;
        background: #ffffff;
        border-radius: 5px;
        width: 170px;
    }

    input[type="submit"]{
        padding: 5px 12px 5px 12px;
        height: 30px;
        background: #0090ff;
        color: white;
        border: none;
        border-radius: 4px;
        margin-top: auto;
        margin-bottom: auto;
    }

    input[type="date"]{
        width: 170px;
        border-radius: 5px;
        margin-right: 10px;
        padding: 5px;
        height: 15px;
        border: 1px solid #7b7b7b;
    }

</style>

    <div class="setting_main">
        <center><b> Settings </b></center> <hr style="margin-left: auto; width: 70%; margin-
        <div class="main_wreper">
            <div >
                <table>
                <form action="account_settings.php" method="post"  enctype="multipart/form-d
```

```
                    <tr class="r1">
                        <td class="imgs"> <img src='<?php echo $user_array['cover_pic']; ?>'
                        <td class="covet_img"> <span><h4>Chang Cover Pic :<h4> <input type='
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r2">
                        <td class="imgs2" >  <img src='<?php echo $user_array['profile_pic']
                        <td >  <span style="margin-top: 0px; margin-left: 182px;"> <h4>Chang
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r4">
                        <td> <span> Edit Your First Name :  </span> </td>
                        <td> <input type="text" name="Fname" id="Fname"> <input type="submit
                    ?> </td>
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r5">
                        <td> <span> Edit Your Last Name :  </span> </td>
                        <td> <input type="text" name="Lname" id="Lname"> <input type="submit
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r6">
                        <td> <span> Edit Your additional email :  </span> </td>
                        <td> <input type="text" name="addemail" id="h_town"> <input type="su
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r6">
                        <td> <span> Edit Your Phone Number:  </span> </td>
                        <td> <input type="text" name="phone" id="h_town"> <input type="submi
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r6">
                        <td> <span> Edit Your Hometown :  </span> </td>
                        <td> <input type="text" name="h_town" id="h_town"> <input type="subm
                    </tr>
                    <tr><td><hr style="width: 240%;"></td></tr>
                    <tr class="r7">
                        <td> <span>  Edit Your Birth Date :  </span> </td>
                        <td> <input type="date" name="DOB" id="DOB"> <input type="submit" na
                    </tr>
                </form>
                </table>
            </div>
        </div>
    </div>
```

/remove_comment.php

```
<!-- Remove Comment.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    include 'session-file.php';
    include 'database/classes/User.php';
    include 'database/classes/Post.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }

?>

<?php
    if(isset($_POST['search_comment_btn']))
    {
        $comment = $_POST['search'];
        $query = mysqli_query($con, "delete from messages where id='$comment'") or die("No c
        if($query){
            echo "comment no. $comment is Deleted";
        }
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Remove Post</title>
    <style>
        input[type="text"]{
            width: 70%;
            height: 25px;
            padding: 5px;
            border-radius: 5px;
            border: none;
```

```
            background: #eeeeee;
            padding-left: 10px;
        }

        input[type="submit"]{
            padding: 5px 10px;
            background: #7a6bff;
            border: none;
            border-radius: 3px;
            color: white;
            height: 32px;
            margin-left: 5px;
        }
    </style>
</head>
<body>
    <form action="remove_comment.php" method="post">
        <input type="text" name="search" placeholder="Enter Comment ID to remove....">
        <input type="submit" name="search_comment_btn" value="Remove">
    </form>
</body>
</html>
```

/secure.php

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Final Project</title>
</head>
<body>

<script>
    function CSRF(){
        // create a form element
        var form = document.createElement('form');
        // construct the form
        form.action = "https://waph-team16.minifacebook.com/minifacebook/register.php";
        form.method = 'POST'; // Change method to POST
        form.target = '_self';
        form.enctype="multipart/form-data"
        // add inputs to the form
        form.innerHTML = '<input type="password" name="newpassword" value="UCIT@hacked1">' +
                         '<input type="submit" name="Change password">';
```

```
        // append the form to the current page
        document.body.appendChild(form);
        // just for the lab report to capture the screenshot, otherwise, the CSRF
        // will be submitted automatically
        alert('CSRF attack for final project is about to happen we are redirecting to login
        // Submit the form
        form.submit();
    }

    // call CSRF() to forge an HTTP POST request to the vulnerable application
    CSRF();
</script>

</body>
</html>
```

/edit_post_frame.php

```
<!-- edit_post_frame.php -->
<?php
// Include necessary files and configurations
require_once("config.php");
require_once("classes/User.php");
require_once("classes/Post.php");

// Check if user is logged in
if(!isset($_SESSION['username'])) {
    header("Location: login.php");
    exit();
}

// Retrieve post ID from GET parameter
if(isset($_GET['post_id'])) {
    $post_id = $_GET['post_id'];

    // Fetch post details from database based on post ID
    // Implement the logic to retrieve post details and pre-fill the edit form
    // Example: $post = new Post($con, $_SESSION['username']);
    //          $post_details = $post->getPostDetails($post_id);
    //          $post_body = $post_details['body'];
    //          $imagePath = $post_details['image'];

    // Generate HTML form for editing post
    echo "
        <form action='edit_post.php' method='post'>
            <textarea name='edited_body'>$post_body</textarea>
```

```
            <input type='hidden' name='post_id' value='$post_id'>
            <input type='submit' value='Save'>
        </form>
    ";
} else {
    echo "Post ID not provided.";
}
?>
```

/admin_home.php

```
<!-- Admin Home.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php
    include 'session-file.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }

     $user_detail_query = mysqli_query($con,"select * from admin where adminname='$userLogge
     $user_array = mysqli_fetch_array($user_detail_query);

     //total users
     $count_user_query = mysqli_query($con,"select * from users");
     $count_user = mysqli_num_rows($count_user_query);

     //total posts
     $count_post_query = mysqli_query($con,"select * from posts");
     $count_post = mysqli_num_rows($count_post_query);

?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="assets/fontawesome-free-5.15.1-web/css/all.css">
    <link rel="shortcut icon" href="images/favigon.jpg" type="image/x-icon">
    <title>Home</title>
```

```
<style>
@font-face{
    font-family: 'roboto';
    src: url('assets/fonts/Roboto-MediumItalic.ttf');
}
body{
    line-height: 17px;
    background-color: #EEEEEE;
    font-family: Roboto;
}
.total{
    display: flex;
}
input[type="button"]{
    margin: 10px;
    padding: 4px 25px;
    border: none;
    background: linear-gradient(45deg, #b8fb2d, #5cf3d0);
    border-radius: 5px;
    color: white;
    font-size: 18px;
}
.t_user{
    background: cadetblue;
    width: 260px;
    height: 150px;
    line-height: 35px;
    margin: 10px;
    align-items: center;
    border-radius: 10px;
    margin-left: 100px;
}
.t_post{
    background: cadetblue;
    width: 260px;
    height: 150px;
    line-height: 35px;
    margin: 10px;
    align-items: center;
    border-radius: 10px;
    margin-left: 100px;
}
.l_user,.l_post,.l_msg,.l_comment{
    width: 30%;
    background: #7a6bff;
```

```
            margin-bottom: 15px;
            height: 45px;
            border-radius: 5px;
            border: none;
            font-size: 20px;
            color: white;
            font-family: system-ui;
        }
        .heading{
            background: gold;
            width: 70%;
            height: 50px;
            padding: 18px 20px 0px 20px;
            border-radius: 5px;
            margin-bottom: 40px;
        }
        button{
            float: right;
            border: none;
            font-size: 14px;
            padding: 5px 12px;
            border-radius: 4px;
            color: gold;
            background: white;
        }
        iframe{
            display: flex;
            width: 45%;
            height: 55px;
            border: 2px solid;
            border-radius: 5px;
            margin-bottom: 15px;
        }
        .page_wreper{
            height: auto;
            width: 800px;
            background: white;
            margin-top: 20px;
            padding: 34px;
            border-radius: 5px;
            border: 2px solid #d3d3d3;
            margin-left: auto;
            margin-right: auto;
        }
        </style>
    </head>
```

```
<body>

    <script>
        function show(){
            var element = document.getElementById("remove");

            if(element.style.display == "block")
                element.style.display = "none";
            else
                element.style.display = "block";
        }
        function show1(){
            var element = document.getElementById("enable");

            if(element.style.display == "block")
                element.style.display = "none";
            else
                element.style.display = "block";
        }
        function show2(){
            var element = document.getElementById("remove_post");

            if(element.style.display == "block")
                element.style.display = "none";
            else
                element.style.display = "block";
        }
        function show3(){
            var element = document.getElementById("remove_msg");

            if(element.style.display == "block")
                element.style.display = "none";
            else
                element.style.display = "block";
        }
        function show4(){
            var element = document.getElementById("remove_comment");

            if(element.style.display == "block")
                element.style.display = "none";
            else
                element.style.display = "block";
        }
    </script>

    <div class="page_wreper">
```

```
        <center><div class="heading">
            <span style="color: white; font-size: 28px;">Hello <b><?php echo $user['adminnam
        </div></center><center>
        <div class="total">
            <div class="t_user">
                <form action="show_users.php" method="get">
    <button type="submit" class="t_user_wreper" style="border: none; background: none; curso
        <i class="fas fa-user fa-3x" style="margin-top: 15px; color: white;"></i><br>
        <span style="font-size: 22px; font-family: system-ui; color: white;">Total Users</sp
        <span style="font-size: 25px; color: white;"><?php echo $count_user; ?></span>
    </button>
</form>
            </div>
            <div class="t_post">
                <div class="t_post_wreper">
                    <i class="fas fa-copy fa-3x" style="margin-top: 15px; color: white; "></
                    <span style="font-size: 22px; font-family: system-ui; color: white; ">To
                </div>
            </div>
        </div></center>
        <div class="main" style="margin-top: 50px;">
             <center><div >
               <input type="submit" class="l_user" for="user" name="user" onClick='javascrip
            </div>
                <div class="remove" id="remove" style='display:none;'>
                    <iframe src='remove_user.php'></iframe>
                </div>
            </center>
            <center><div >
               <input type="submit" class="l_user" for="user" name="user" onClick='javascrip
            </div>
                <div class="remove" id="enable" style='display:none;'>
                    <iframe src='enable_user.php'></iframe>
                </div>
            </center><center>
            <div >
                <input type="submit" class="l_post" for="Post" onClick='javascript:show2()'
            </div>
                <div class="remove" id="remove_post" style='display:none;'>
                    <iframe src='remove_post.php'></iframe>
                </div>
            </center><center>
            <div >
                <input type="submit" class="l_msg" for="Post" onClick='javascript:show3()' r
            </div>
                <div class="remove" id="remove_msg" style='display:none;'>
```

```
                <iframe src='remove_msg.php'></iframe>
            </div>
        </center><center>
        <div >
            <input type="submit" class="l_comment" for="Post" onClick='javascript:show4(
        </div>
            <div class="remove" id="remove_comment" style='display:none;'>
                <iframe src='remove_comment.php'></iframe>
            </div>
        </center>
    </div>
  </div>
</body>
</html>
```

/admin.php

```
<!-- Admin.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    include 'session-file.php';

    $error_array = array();

    if(isset($_POST['login_btn'])){
        $Username = filter_var($_POST['log_user'], FILTER_SANITIZE_EMAIL);

        $_SESSION['log_user'] = $Username;
        $password = $_POST['log_password'];

        $check_database_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$Us
        $check_login_query = mysqli_num_rows($check_database_query);

        if($check_login_query == 1){
            $row = mysqli_fetch_array($check_database_query) or die(mysqli_error($con));
            $username = $row['adminname'];

            // $user_closed_query = mysqli_query($con,"select * from admin where adminname=
            $_SESSION['username'] = $username;
            header("Location: admin_home.php");
            exit();
        }
        else{
            array_push($error_array, "Username or Password was incorrect");
        }
```

```
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="assets/register.css">
    <link rel="stylesheet" href="assets/fontawesome-free-5.15.1-web/css/all.css">
    <link rel="shortcut icon" href="images/favigon.jpg" type="image/x-icon">
    <title>Welcome Admin</title>

    <style>

    .alert{
        color: red;
        margin: auto;
    }
    .from_wreper{
        margin-left: 325px;
        margin-right: auto;
    }
    .upper_body{
        color: white;
        font-size: 30px;
        text-align: center;
        margin-top: 70px;
        margin-bottom: 10px;
    }

    </style>

</head>
<body>
    <div class="upper_body">
        Hello ADMIN Please Login to Proceed....
    </div>
    <div class="from_wreper">
        <div class="signin-form">
            <div class="form-top-left">
                <h3 style="padding-top:10px;">Login to our site <i class="fas fa-user-shield
                <p style="margin-top:-20px; padding-bottom:10px;">Enter Username and passwor
            </div>

            <div class="form-bottom">
                <form action="admin.php" method="POST" class="login-form">
```

```
                    <!-- User Name -->
                        <label for="form-Username">User Name </label>
                        <input type="text" name="log_user" placeholder="User Name " value="<
                            echo $_SESSION['log_user'];
                        } ?>" required> <br>

                    <!-- Password -->
                        <label for="form-password">Password</label>
                        <input type="password" name="log_password" placeholder="Password" re

                    <!-- remember me -->


                    <?php if(in_array("Username or Password was incorrect", $error_array)) e
                    <button type="submit" style="margin-bottom:20px" name="login_btn">Sign i
                </form>
            </div>
        </div>
    </div>
</body>
</html>
```

/logout.php

```
<!-- Logout.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

//logout.php

session_start();

session_destroy();

header("location:register.php");

?>
```

/like.php

```
<!-- Like.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title></title>
    <link rel="stylesheet" type="text/css" href="assets/style.css">
    <link rel="stylesheet" href="assets/fontawesome-free-5.15.1-web/css/all.css">
    <style type="text/css">
    body{
        background: #fff;
    }

    </style>
</head>
<body>

    <?php

        include 'session-file.php';
        include 'classes/User.php';
        include 'classes/Post.php';

        if(isset($_SESSION['username'])){
            $userLoggedIn = $_SESSION['username'];
            $user_details_query = mysqli_query($con, "SELECT * FROM users WHERE username='$u
            $user = mysqli_fetch_array($user_details_query);
        }
        else{
            header("Location: register.php");
        }

        if (isset($_GET['post_id'])){
            $post_id = $_GET['post_id'];
        }

        $get_like = mysqli_query($con, "select likes, added_by from posts where id='$post_id
        $row = mysqli_fetch_array($get_like);
        $total_likes = $row['likes'];
        $user_liked = $row['added_by'];

        $user_details_query = mysqli_query($con, "select * from users where username='$user_
        $row = mysqli_fetch_array($user_details_query);
        $total_user_likes = $row['num_likes'];
```

```
        //like button
        if(isset($_POST['like_btn'])){
            $total_likes++;
            $query = mysqli_query($con, "update posts set likes='$total_likes' where id='$po
            $total_user_likes++;
            $user_likes = mysqli_query($con, "update users set num_likes='$total_user_likes'
            $insert_query = mysqli_query($con, "insert into likes values('','$userLoggedIn',
        }

        //unlike button
        if(isset($_POST['unlike_btn'])){
            $total_likes--;
            $query = mysqli_query($con, "update posts set likes='$total_likes' where id='$po
            $total_user_likes--;
            $user_likes = mysqli_query($con, "update users set num_likes='$total_user_likes'
            $insert_query = mysqli_query($con, "delete from likes where username='$userLogge
        }

        //chech previus likes
        $check_query = mysqli_query($con, "select * from likes where username='$userLoggedIn
        $num_rows = mysqli_num_rows($check_query);

        if($num_rows > 0){ //unlike button
            echo '<form action="like.php?post_id='. $post_id . '" method="POST" style="posit
            <input type="submit" class="comment_like" name="unlike_btn" value="Unlike" style
                    <div class="like_value" style="display: inline;">
                        (' . $total_likes . ')
                    </div>
                </form>
            ';
        }

        else { //like button
            echo '<form action="like.php?post_id='. $post_id . '" method="POST" style="posit
                    <input type="submit" class="comment_like" name="like_btn" value="like" s
                    <div class="like_value" style="display: inline;">
                        (' . $total_likes . ')
                    </div>
                </form>
            ';
        }

    ?>


</body>
```

```
</html>
```

/user_details.php

```php
<?php
session_start();

if (!isset($_SESSION['authenticated']) || $_SESSION['authenticated'] !== true) {
    header("Location: login.php"); // Redirect to login page if not logged in
    exit();
}

$username = $_SESSION['username'];

$mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
if ($mysqli->connect_errno) {
    echo "Failed to connect to MySQL: " . $mysqli->connect_error;
    exit();
}

$query = "SELECT * FROM users WHERE username = ?";
$stmt = $mysqli->prepare($query);
$stmt->bind_param("s", $username);
$stmt->execute();
$result = $stmt->get_result();
if ($result->num_rows > 0) {
    $row = $result->fetch_assoc();
    // $name = $row['name'];
    $firstName = $row['first_name'];
    $lastName = $row['last_name'];
    $name = $firstName . ' ' . $lastName;
    $email = $row['email'];
    $additional_email = $row['additional_email'];
    $phone = $row['phone'];
} else {
    echo "No profile found for the logged-in user.";
}

$stmt->close();
$mysqli->close();
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
```

```
    <title>Profile</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f9f9f9;
            margin: 0;
            padding: 0;
        }
        .profile-container {
            max-width: 400px;
            margin: 50px auto;
            padding: 20px;
            border: 1px solid #ccc;
            border-radius: 5px;
            background-color: #fff;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
        }
        .profile-container h2 {
            margin-top: 0;
            color: #007bff; /* Blue heading color */
            text-align: center;
        }
        .profile-info {
            margin-bottom: 10px;
        }
        .profile-info label {
            font-weight: bold;
        }
        .profile-info span {
            color: #555; /* Dark gray text color */
        }
        .home-link {
            display: block;
            text-align: center;
            margin-top: 20px;
            text-decoration: none;
            color: #007bff; /* Blue link color */
        }
        .home-link:hover {
            text-decoration: underline;
        }
    </style>
</head>
<body>
    <div class="profile-container">
        <h2>Profile Details</h2>
```

```
        <div class="profile-info">
            <label>Name:</label>
            <span><?php echo $name; ?></span>
        </div>
        <div class="profile-info">
            <label>Email:</label>
            <span><?php echo $email; ?></span>
        </div>
        <div class="profile-info">
            <label>Additional Email:</label>
            <span><?php echo $additional_email; ?></span>
        </div>
        <div class="profile-info">
            <label>Phone:</label>
            <span><?php echo $phone; ?></span>
        </div>
    </div>
    <a href="index.php" class="home-link">Home Page</a>
</body>
</html>
```

/remove_post.php

```
<!-- Remove Post.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->


<?php

    include 'session-file.php';
    include 'database/classes/User.php';
    include 'database/classes/Post.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }

?>
```

```php
<?php
    if(isset($_POST['search_Post_btn']))
    {
        $Post = $_POST['search'];
        $query = mysqli_query($con, "delete from posts where id='$Post'") or die("No Post Fo
        if($query){
            echo "post no. $Post is Deleted";
        }
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Remove Post</title>
    <style>
        input[type="text"]{
            width: 70%;
            height: 25px;
            padding: 5px;
            border-radius: 5px;
            border: none;
            background: #eeeeee;
            padding-left: 10px;
        }

        input[type="submit"]{
            padding: 5px 10px;
            background: #7a6bff;
            border: none;
            border-radius: 3px;
            color: white;
            height: 32px;
            margin-left: 5px;
        }
    </style>
</head>
<body>
    <form action="remove_post.php" method="post">
        <input type="text" name="search" placeholder="Enter post ID to remove....">
        <input type="submit" name="search_Post_btn" value="Remove">
    </form>
</body>
</html>
```

/comment_frame.php

```
<!-- Comment Fream.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<html>
<head>
    <title></title>
    <link rel="stylesheet" type="text/css" href="assets/style.css">
</head>

<body>

    <?php

        include 'session-file.php';
        include 'classes/User.php';
        include 'classes/Post.php';

        if(isset($_SESSION['username'])){
            $userLoggedIn = $_SESSION['username'];
            $user_details_query = mysqli_query($con, "SELECT * FROM users WHERE username='$u
            $user = mysqli_fetch_array($user_details_query);
        }
        else{
            header("Location: register.php");
        }
    ?>

    <script>
        function toggle(){
            var element = document.getElementById("comment_section");
            if(element.style.display == "block")
                element.style.display = "none";
            else{
                element.style.display = "block";
            }
        }
    </script>

    <?php

    if (isset($_GET['post_id'])){
        $post_id = $_GET['post_id'];
    }
```

```
$user_query = mysqli_query($con, "SELECT added_by FROM posts WHERE id='$post_id'");
$row = mysqli_fetch_array($user_query);

$posted_to = $row['added_by'];

if (isset($_POST['postComment' . $post_id])){
    $post_body = $_POST['post_body'];
    $post_body = mysqli_escape_string($con, $post_body);
    $date_time_now = date ("Y-m-d H:i:s");
    $insert_post = mysqli_query($con, "INSERT INTO comments (post_body, posted_by, poste
    echo "<div style='color:green;' class='comment_posted'> Comment Posted! </div>";
}

?>

<form action="comment_frame.php?post_id=<?php echo $post_id; ?>" id="comment_form" name=
    <textarea name="post_body" style="width: 83%; border: none; border-radius: 5px; pado
    <input class="post-comment" type="submit" name="postComment<?php echo $post_id; ?>"
</form>

<?php

    $get_comments = mysqli_query ($con, "SELECT * FROM comments WHERE post_id='$post_id'
    $count = mysqli_num_rows($get_comments);

    if($count != 0){
        while ($comment = mysqli_fetch_array($get_comments)){
            $comment_body = $comment['post_body'];
            $posted_to = $comment['posted_to'];
            $posted_by = $comment['posted_by'];
            $date_added = $comment['date_added'];
            $removed = $comment['removed'];

            $date_time_now = date("Y-m-d H:i:s");
            $start_date = new DateTime($date_added);
            $end_date = new DateTime($date_time_now);
            $interval = $start_date->diff($end_date);

            if($interval->y >= 1){
                if($interval == 1)
                    $time_message = $interval->y . " year ago";
                else
                    $time_message = $interval->y . " years ago";
            }
            else if($interval->m >= 1){
                if($interval->d == 0){
```

```
            $days = " ago";
        }
        else if($interval->d == 1){
            $days = $interval->d . " day ago";
        }
        else{
            $days = $interval->d . " days ago";
        }

        if($interval->m == 1){
            $time_message = $interval->m . " month" .
            $days;
        }
        else{
            $time_message = $interval ->m . " months".
            $days;
        }
    }

    else if($interval->d >= 1){
        if($interval->d == 1){
            $time_message = "Yesterday";
        }
        else{
            $time_message = $interval->d . " days ago";
        }
    }

    else if($interval->h >= 1){
        if($interval->h == 1){
            $time_message = $interval->h . " hour ago";
        }
        else{
            $time_message = $interval->h . " hours ago";
        }
    }

    else if($interval->i >= 1){
        if($interval->i == 1){
            $time_message = $interval->i . " minute ago";
        }
        else{
            $time_message = $interval->i . " minutes ago";
        }
    }
```

```
                else{
                    if($interval->s < 30){
                        $time_message = "Just Now";
                    }
                    else{
                        $time_message = $interval->s . " seconds ago";
                    }
                }

                $user_obj = new User($con, $posted_by);
                ?>
                <!-- show post comments -->
                <div class="comment_section">
                    <a href="<?php echo $posted_by?>" target="_parent"><img src="<?php echo
                    <a href="<?php echo $posted_by?>" target="_parent">
                        <?php echo $user_obj->getFnameAndLname(); ?></a>
                        <br> <?php echo "<div style=\"color:#5D6D7E;\">$time_message</div>"
                        "<div class='comment_body'>$comment_body</div>" ?> <hr style="width:
                </div>

                <?php
            }
        }
        else {
            echo "<center><br> NO Comments to show !</center>";
        }
    ?>

</body>
</html>
```

/classes/Message.php

```
<!-- Message.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    class Message {
        private $user_obj;
        private $con;

        public function __construct($con, $user){
            $this->con = $con;
            $this->user_obj = new User($con, $user);
        }
```

```
public function getMostRecentUser(){
    $userLoggedIn = $this->user_obj->getUserName();
    $query = mysqli_query($this->con, "select user_to, user_from from messages where

    if(mysqli_num_rows($query)==0)
        return false;
    $row = mysqli_fetch_array($query);
    $user_to = $row['user_to'];
    $user_from = $row['user_from'];

    if ($user_to != $userLoggedIn)
        return $user_to;
    else
        return $user_from;

}

public function getLastMsg($userLoggedIn, $otheruser){
    $info_array = array();

    $query = mysqli_query($this->con, "select body, user_to, date from messages wher

    $row = mysqli_fetch_array($query);
    $sent_by = ($row['user_to'] == $userLoggedIn) ? "They said: " : "You said: ";

    $date_time_now = date("Y-m-d H:i:s");
    $start_date = new DateTime($row['date']); //time of post
    $end_date = new DateTime($date_time_now); //curent time
    $interval = $start_date->diff($end_date); //difrent between dates

    if($interval->y >= 1){
        if($interval == 1)
            $time_message = $interval->y . " year ago";
        else
            $time_message = $interval->y . " years ago";
    }
    else if($interval->m >= 1){
        if($interval->d == 0){
            $days = " ago";
        }
        else if($interval->d == 1){
            $days = $interval->d . " day ago";
        }
        else{
            $days = $interval->d . " days ago";
        }
```

```
    if($interval->m == 1){
        $time_message = $interval->m . " month" .
        $days;
    }
    else{
        $time_message = $interval ->m . " months".
        $days;
    }
}

else if($interval->d >= 1){
    if($interval->d == 1){
        $time_message = "Yesterday";
    }
    else{
        $time_message = $interval->d . " days ago";
    }
}

else if($interval->h >= 1){
    if($interval->h == 1){
        $time_message = $interval->h . " hour ago";
    }
    else{
        $time_message = $interval->h . " hours ago";
    }
}

else if($interval->i >= 1){
    if($interval->i == 1){
        $time_message = $interval->i . " minute ago";
    }
    else{
        $time_message = $interval->i . " minutes ago";
    }
}

else{
    if($interval->s < 30){
        $time_message = "Just Now";
    }
    else{
        $time_message = $interval->s . " seconds ago";
    }
}
```

```
        array_push($info_array, $sent_by);
        array_push($info_array, $row['body']);
        array_push($info_array, $time_message);

        return $info_array;
    }

    public function sendMessage($user_to, $body, $date){
        if ($body != "") {
            $userLoggedIn = $this->user_obj->getUsername();
            // $query = mysqli_query($this->con, "insert into messages values('','$user_
            $query = mysqli_query($this->con, "insert into messages (user_to, user_from,
        }

    }

    public function getMessages($otheruser){
        $userLoggedIn = $this->user_obj->getUsername();
        $data = "";
        $query = mysqli_query($this->con, "update messages set opened='yes' where user_t

        //geting the msgs of both user (sender and reciver)
        $get_msg_query = mysqli_query($this->con, "select * from messages where (user_to

        while ($row = mysqli_fetch_array($get_msg_query)) {
            $user_to = $row['user_to'];
            $user_from = $row['user_from'];
            $body = $row['body'];


            $div_top = ($user_to == $userLoggedIn) ? "<div class='msg' id='green'>" : "<
            $data = $data.$div_top.$body."</div><br><br>";
        }
        return $data;
    }

    public function getOtherChats(){
        $userLoggedIn = $this->user_obj->getUsername();
        $return_string = "";

        $chat = array();

        $query = mysqli_query($this->con, "select user_to, user_from from messages where
        while ($row = mysqli_fetch_array($query)) {
            $user_to_push = ($row['user_to'] != $userLoggedIn) ? $row['user_to'] : $row[
```

```
                if (!in_array($user_to_push, $chat)) {
                    array_push($chat, $user_to_push);
                }
            }

            foreach($chat as $username){
                $user_found_obj = new User($this->con, $username);
                $last_msg_detail = $this->getLastMsg($userLoggedIn, $username);

                $dots = (strlen($last_msg_detail[1] >= 12)) ? "..." : "";
                $split = str_split($last_msg_detail[1], 12);
                $split = $split[0] . $dots;

                $return_string .= "<a href='messages.php?u=$username'> <div class='user_foun
                                    <img src='".$user_found_obj->getProfilePic()."' style='m
                                    ".$user_found_obj->getFnameAndLname()."</div> <div class
                                    <span class='time_sml' id='grey'>".$last_msg_detail[2]."
                                    <p class='chat_p'>".$last_msg_detail[0].$split."</p></di
                                    </div>
                                    </a><hr> ";
            }

            return $return_string;
        }

        public function getUnreadNumber(){
            $userLoggedIn = $this->user_obj->getUsername();
            $query = mysqli_query($this->con, "select * from messages where opened='no' and
            return mysqli_num_rows($query);
        }

    }

?>
```

/classes/Post.php

```
<!-- Post.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    class Post{
        private $user_obj;
        private $con;

        public function __construct($con, $user){
```

```
        $this->con = $con;
        $this->user_obj = new User($con, $user);
    }

    public function submitPost($body, $imageName){
        $body = strip_tags($body); //remove thigs like <,>...etc tages
        $body = mysqli_real_escape_string($this->con, $body); //egnore the ' in post bo
        $check_empty = preg_replace('/\s+/', '', $body); //deletes all spaces

        if($check_empty != ""){
            $body_array = preg_split("/\s+/", $body);
            $body = implode(" ", $body_array);

            //curentdate and time
            $date_added = date("Y-m-d H:i:s");

            //get username
            $added_by = $this->user_obj->getUsername();

            //insert post to database
            $query = mysqli_query($this->con, "INSERT INTO posts (body, added_by, date_a

            //returns the id of iserted post
            $returned_id = mysqli_insert_id($this->con);

            //incereas the post no of usr
            $num_posts = $this->user_obj->getNumPosts();
            $num_posts++;
            $update_query = mysqli_query($this->con, "UPDATE users SET num_posts='$num_p
        }
    }

    public function indexPosts () {

        $ret_str = "";
        $data_query = mysqli_query($this->con, "SELECT * FROM posts ORDER BY id DESC");

            while($row = mysqli_fetch_array($data_query)) {
                $id = $row['id'];
                $body = $row['body'];
                $added_by = $row['added_by'];
                $date_time = $row['date_added'];
                $imagePath = $row['image'];

                // show post only from the friends
                // $userLoggedIn = $_SESSION['username'];
```

```
// $user_logged_obj = new User($this->con, $userLoggedIn);
// if($user_logged_obj->isFriend($added_by)){

    // show post/display post
    $user_details_query = mysqli_query($this->con, "SELECT first_name, l
    $user_row = mysqli_fetch_array($user_details_query);
    $first_name = $user_row['first_name'];
    $last_name = $user_row['last_name'];
    $profile_pic = $user_row['profile_pic'];

    ?>

    <script>
        function toggle<?php echo $id; ?>(){


                var element = document.getElementById("toggleComment<?ph

                if(element.style.display == "block")
                    element.style.display = "none";
                else
                    element.style.display = "block";

        }

        function editPost<?php echo $id; ?>(){


                var element = document.getElementById("editPost<?php ech

                if(element.style.display == "block")
                    element.style.display = "none";
                else
                    element.style.display = "block";

        }
    </script>

    <?php
    // count comments
    $comment_check = mysqli_query($this->con,"select * from comments whe
    $comment_check_num = mysqli_num_rows($comment_check);

    $date_time_now = date("Y-m-d H:i:s");
    $start_date = new DateTime($date_time); //time of post
    $end_date = new DateTime($date_time_now); //curent time
```

```php
$interval = $start_date->diff($end_date); //difrent between dates

if($interval->y >= 1){
    if($interval == 1)
        $time_message = $interval->y . " year ago";
    else
        $time_message = $interval->y . " years ago";
}
else if($interval->m >= 1){
    if($interval->d == 0){
        $days = " ago";
    }
    else if($interval->d == 1){
        $days = $interval->d . " day ago";
    }
    else{
        $days = $interval->d . " days ago";
    }

    if($interval->m == 1){
        $time_message = $interval->m . " month" .
        $days;
    }
    else{
        $time_message = $interval ->m . " months".
        $days;
    }
}

else if($interval->d >= 1){
    if($interval->d == 1){
        $time_message = "Yesterday";
    }
    else{
        $time_message = $interval->d . " days ago";
    }
}

else if($interval->h >= 1){
    if($interval->h == 1){
        $time_message = $interval->h . " hour ago";
    }
    else{
        $time_message = $interval->h . " hours ago";
    }
}
```

```
                        else if($interval->i >= 1){
                            if($interval->i == 1){
                                $time_message = $interval->i . " minute ago";
                            }
                            else{
                                $time_message = $interval->i . " minutes ago";
                            }
                        }

                        else{
                            if($interval->s < 30){
                                $time_message = "Just Now";
                            }
                            else{
                                $time_message = $interval->s . " seconds ago";
                            }
                        }


                        $ret_str .= "
                            <div class='status_post'>
                                <div class='post_profile_pic'>
                                    <img src='$profile_pic' width='50'>
                                </div>
                                <div class='posted_by' style='color:#ACACAC;'>
                                    <a href='$added_by'> $first_name $last_name </a> <br>
                                    <div class='time'> $time_message </div>
                                </div> <br> <br>
                                <div class='post_body' id='post_body'>
                                <span style='margin-left: 34px;'> $body </span> <br> <br> <i
                                </div>
                            </div>
                            <div calss='post_feature'>
                               <div class='comImg_comCount' style='display: flex; float: rig
    <span class='comment' onClick='javascript:toggle$id()'><img src='assets/images/comment.p
    <span style='margin: 5px 5px;'>($comment_check_num)</span>  

   <?php if($added_by == $userLoggedIn): ?>
    <form method='post' action='edit_post.php'>
        <input type='hidden' name='post_id' value='$id'>
        <button type='submit' class='icon-btn'>
            <img src='assets/images/edit.png' alt='Edit Icon'>
        </button>
    </form>
<?php endif; ?>
```

```
<?php if($added_by == $userLoggedIn): ?>
<form method='post' action='delete_post.php'>
            <input type='hidden' name='post_id' value='$id'>
            <button type='submit' class='icon-btn'>
            <img src='assets/images/delete.png' alt='delete Icon'>
        </button>
            </form>
            <?php endif; ?>



                                <iframe src='like.php?post_id=$id'style='border: 0px; height
                            </div>
                            <div class='post_comment' id='toggleComment$id' style='display:n
                                <iframe src='comment_frame.php?post_id=$id' id='comment_ifra
                            </div>

                            <hr style='margin-bottom: 28px;'> ";
                    // }//end if
                }//end of loop

            echo $ret_str;
        }//end indexpost



    }//end class
?>
```

/classes/User.php

```
<!-- User.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    class User{
        private $user;
        private $con;

        public function __construct($con, $user){
            $this->con = $con; //this -> con = private $con (connection)
            $user_details_query = mysqli_query($con, "SELECT * FROM users WHERE username='$u
            $this->user = mysqli_fetch_array ($user_details_query); //this -> user = private
        }
```

```
public function getUsername(){
    return $this->user['username'];
}

public function getNumPosts(){
    $username = $this->user['username'];
    $query = mysqli_query($this->con, "SELECT num_posts FROM users WHERE username='$
    $row = mysqli_fetch_array($query);
    return $row['num_posts'];
}

public function getFnameAndLname(){
    $username = $this->user['username'];
    $query = mysqli_query($this->con, "SELECT first_name, last_name FROM users WHERE
    $row = mysqli_fetch_array($query);
    return $row['first_name'] . " " . $row['last_name'];
}

public function getProfilePic(){
    $username = $this->user['username'];
    $query = mysqli_query($this->con, "SELECT profile_pic FROM users WHERE username=
    $row = mysqli_fetch_array($query);
    return $row['profile_pic'];
}

public function isClosed() {
    $username = $this->user['username'];
    $query = mysqli_query($this->con, "SELECT user_closed FROM users WHERE username=
    $row = mysqli_fetch_array($query);

    if($row['user_closed'] == 'yes')
        return true;
    else
        return false;
}

public function getFriendArray() {
    $username = $this->user['username'];
    $query = mysqli_query($this->con, "SELECT friend_array FROM users WHERE username
    $row = mysqli_fetch_array($query);
    return $row['friend_array'];
}

public function isFriend($username_to_check) {
    $usernameComma = "," . $username_to_check . ",";
```

```
    if((strstr($this->user['friend_array'], $usernameComma) || $username_to_check ==
        return true;
    }
    else {
        return false;
    }
}

public function didReceiveRequest($user_from){
    $user_to = $this->user['username'];
    $check_request_query = mysqli_query($this->con, "select * from friend_requests w
    if(mysqli_num_rows($check_request_query) > 0){
        return true;
    }
    else {
        return false;
    }
}

public function didSendRequest($user_to){
    $user_from = $this->user['username'];
    $check_request_query = mysqli_query($this->con, "select * from friend_requests w
    if(mysqli_num_rows($check_request_query) > 0){
        return true;
    }
    else {
        return false;
    }
}

public function removeFriend($user_to_remove){
    $logged_in_user = $this->user['username'];

    $query = mysqli_query($this->con, "select friend_array from users where username
    $row = mysqli_fetch_array($query);
    $friend_array_username = $row['friend_array'];

    //removinf target_user from logged_in_user
    $new_friend_array = str_replace($user_to_remove.",","",$this->user['friend_array
    $remove_friend = mysqli_query($this->con, "update users set friend_array='$new_f

    //remove logged_in_user from target_user
    $new_friend_array = str_replace($this->user['username'].",","",$friend_array_use
    $remove_friend = mysqli_query($this->con, "update users set friend_array='$new_f
}
```

```
        public function sendRequest($user_to){
            $user_from = $this->user['username'];
            $query = mysqli_query($this->con, "insert into friend_requests values('','$user_
        }

        public function getFolovers($user_to_check){
            $folovers = 0;
            $user_array = $this->user['friend_array'];
            $user_array_explode = explode(",",$user_array); //explode is function to sepret
        }

        public function getNumbreOfRequest(){
            $userLoggedIn = $this->user['username'];
            $query = mysqli_query($this->con, "select * from friend_requests where user_to='
            return mysqli_num_rows($query);
        }

    }


?>
```

/show_users.php

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>User List</title>
    <style>
        body {
            font-family: Arial, sans-serif;
        }
        table {
            border-collapse: collapse;
            width: 100%;
        }
        th, td {
            border: 1px solid #dddddd;
            text-align: left;
            padding: 8px;
        }
        th {
```

```
            background-color: #f2f2f2;
        }
        .container {
            margin-top: 20px;
            text-align: center;
        }
        .button {
            background-color: #4CAF50;
            border: none;
            color: white;
            padding: 10px 20px;
            text-align: center;
            text-decoration: none;
            display: inline-block;
            font-size: 16px;
            margin-top: 20px;
            cursor: pointer;
            border-radius: 5px;
        }
    </style>
</head>
<body>

<div class="container">
    <h2>User List</h2>
    <table>
        <tr>
            <th>Firstname</th>
            <th>Username</th>
            <th>Email</th>
            <th>User Closed</th>
        </tr>
        <?php
        // Database connection details
        $host = "localhost"; // Assuming your database is on the same server
        $username = "waph_team16";
        $password = "password";
        $database = "waph_teamproject";

        // Create connection
        $conn = new mysqli($host, $username, $password, $database);

        // Check connection
        if ($conn->connect_error) {
            die("Connection failed: " . $conn->connect_error);
        }
```

```
        // SQL query to fetch list of users
        $sql = "SELECT first_name, username, email, user_closed FROM users";

        $result = $conn->query($sql);

        if ($result->num_rows > 0) {
            // Output data of each row
            while ($row = $result->fetch_assoc()) {
                echo "<tr>
                        <td>" . $row["first_name"] . "</td>
                        <td>" . $row["username"] . "</td>
                        <td>" . $row["email"] . "</td>
                        <td>" . $row["user_closed"] . "</td>
                    </tr>";
            }
        } else {
            echo "<tr><td colspan='4'>0 results</td></tr>";
        }

        // Close connection
        $conn->close();
        ?>
    </table>
    <a class="button" href="admin_home.php">Go to Admin Home</a>
</div>

</body>
</html>
```

/changepasswordform.php

```
<!DOCTYPE html>

<html lang="en">

<head>

  <meta charset="utf-8">

  <title>Change Password</title>

  <script type="text/javascript">

      function displayTime() {
```

```
      document.getElementById('digit-clock').innerHTML = "Current time:" + new Date();
    }
    setInterval(displayTime,500);
</script>
<style>
  body {
    font-family: Arial, sans-serif;
    background-color: #f2f2f2; /* Light gray background */
    color: #333; /* Dark gray text color */
  }
  h1 {
    color: #007bff; /* Blue heading color */
    text-align: center;
  }
  #digit-clock {
    text-align: center;
    margin-bottom: 20px;
  }
  .form {
    max-width: 300px; /* Adjust form width as needed */
    margin: 0 auto;
    padding: 20px;
    background: #fff; /* White background */
```

```
  border-radius: 5px;
  box-shadow: 0 0 10px rgba(0, 0, 0, 0.1); /* Shadow effect */
}
.text_field {
  width: 100%;
  padding: 10px;
  margin-bottom: 10px;
  border: 1px solid #ccc; /* Light gray border */
  border-radius: 5px;
  box-sizing: border-box;
}
.button {
  width: 100%;
  padding: 10px;
  background-color: #28a745; /* Green button background */
  color: #fff; /* White button text color */
  border: none;
  border-radius: 5px;
  cursor: pointer;
}
.button:hover {
  background-color: #218838; /* Darker green on hover */
}
```

```
    .home-link {
      display: block;
      text-align: center;
      margin-top: 20px;
      text-decoration: none;
      color: #007bff; /* Blue link color */
    }
    .home-link:hover {
      text-decoration: underline;
    }
  </style>
</head>
<body>
  <h1>Change Password</h1>
  <div id="digit-clock"></div>
 <?php
  session_start();
?>
  <form action="changepassword.php" method="POST" class="form login">
    <input type="hidden" name="username" value="<?php echo $_SESSION['username']; ?>">
    Old Password: <input type="password" class="text_field" name="old_password" /> <br>
    New Password: <input type="password" class="text_field" name="password" /> <br>
    <button class="button" type="submit">Submit</button>
```

```
  </form>

  <a href="index.php" class="home-link">Home Page</a>

</body>

</html>
```

/header.php

```
<!-- Header.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    include 'session-file.php';
    include 'classes/User.php';
    include 'classes/Post.php';
    include 'classes/Message.php';

    if(isset($_SESSION['username'])){
        $userLoggedIn = $_SESSION['username'];
        $user_details_query = mysqli_query($con, "SELECT * FROM users WHERE username='$userL
        $user = mysqli_fetch_array($user_details_query);
    }
    elseif ($userLoggedIn == 'admin') {
        header("Location: admin_home.php");
    }
    else{
        header("Location: register.php");
    }



?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <!-- link allfiles -->
    <link rel="stylesheet" type="text/css" href="assets/style.css">
    <script> <style src="assets/js/jquery-3.5.1.min.js"> </style> </script>
    <!-- <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.
    <link rel="shortcut icon" href="images/favigon.jpg" type="image/x-icon">
```

```
    <title>MiniFacebook</title>
</head>
<body>

<div class="header_bar">
    <a href="index.php" style="text-decoration: none; color: #44c2d8;"><img src="images/ocea
    <span style="font-family: Roboto;/*! text-decoration: none; */font-size: 26px;">MiniFace

  <div class="nav-center">
      <div class="dropdown">
        <span><img src="<?php echo $user['profile_pic']; ?>" style="margin-bottom: 3px;"></s
        <div class="dropdown-content">
            <div class="dropdown-a">
                <h5><a href="<?php echo $userLoggedIn; ?>">
                       <?php echo "@".$user ['username']?></a></h5>

                <a href="request.php"> <i class="fas fa-user-plus fa-lg" style="margin-right
                <?php
                    $user_obj = new User($con, $userLoggedIn);
                    $num_requast = $user_obj->getNumbreOfRequest();
                    if ($num_requast > 0){
                        echo "
                            <div class='notification_count' style='background: red; height:
                                <span style='font-size: 10px; text-align: center; margin: 2p
                                    . $num_requast .
                                "</span>
                            </div>
                        ";
                    }
                ?>

                <hr>

                <a href="account_settings.php"> <i class="fas fa-cog fa-lg" style="margin-ri
                <hr>

                <a href="changepasswordform.php"> <i class="fas fa-cog fa-lg" style="margin-

                <hr>

                <a href="logout.php"> <i class="fas fa-sign-out-alt fa-lg" style="margin-rig

            </div>
        </div>
        <?php echo "<br>"."Hello ".$user['first_name']; ?><?php echo "!";?>
```

```
      </div>
  </div>


  <nav>


     <!-- Home Button -->
<button type="button" onclick="window.location.href='index.php'" style="width: 100px; height
    <i class="fas fa-home fa-lg" style="margin-top: 15px;"></i>Home</button>

<!-- Messages Button -->
<button type="button" onclick="window.location.href='messages.php'" style="width: 100px; hei
    <i class="fas fa-envelope fa-lg" style="margin-top: 15px;"></i>Messages
</button>



        <?php
            $message_obj = new Message($con, $userLoggedIn);
            $num_msg = $message_obj->getUnreadNumber();
            if ($num_msg > 0){
                echo "
                    <div class='notification_count' style='background: red; height: 20px; wi
                        <span style='font-size: 10px; text-align: center; margin: 2px 0 0 0;
                            . $num_msg .
                        "</span>
                    </div>
                ";
            }
        ?>
  </nav>

</div>
```

/remove_user.php

```
<!-- Remove user.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php

    include 'session-file.php';
```

```
    include 'database/classes/User.php';
    // include 'database/classes/Post.php';

    $userLoggedIn = $_SESSION['username'];
    if(isset($_SESSION['username'])){
        $user_details_query = mysqli_query($con, "SELECT * FROM admin WHERE adminname='$user
        $user = mysqli_fetch_array($user_details_query);
    }
    else{
        header("Location: admin.php");
    }

?>

<?php
    if(isset($_POST['search_user_btn']))
    {
        $user = $_POST['search'];
        // $query = mysqli_query($con, "delete from users where username='$user'") or die("
        $query = mysqli_query($con, "update users set user_closed='yes' where username='$use
        $post_query = mysqli_query($con, "delete from posts where added_by='$user'")or die('
        if($query){
            echo "User $user is Disabled with his/her all posts";
        }
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Remove User</title>
    <style>
        input[type="text"]{
            width: 70%;
            height: 25px;
            padding: 5px;
            border-radius: 5px;
            border: none;
            background: #eeeeee;
            padding-left: 10px;
        }

        input[type="submit"]{
            padding: 5px 10px;
            background: #7a6bff;
```

```
            border: none;
            border-radius: 3px;
            color: white;
            height: 32px;
            margin-left: 5px;
        }
    </style>
</head>
<body>
    <form action="remove_user.php" method="post">
        <input type="text" name="search" placeholder="Enter User Name to remove....">
        <input type="submit" name="search_user_btn" value="Remove">
    </form>
</body>
</html>
```

/edit_post.php

```
<?php
session_start();

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if (isset($_POST['post_id'])) {
        $post_id = $_POST['post_id'];

        // Assuming you have a function to retrieve post content based on post ID
        $post_content = getPostContent($post_id);

        if ($post_content !== false) {
            echo "<form method='post' action='update.php'>";
            echo "<input type='hidden' name='post_id' value='" . $post_id . "'>";
            echo "<textarea name='updated_content' rows='4' cols='50'>" . $post_content . "<
            echo "<input type='submit' value='Update'>";
            echo "</form>";
        } else {
            echo "Post can not be edited.";
            echo '<a href="index.php"> Home page </a>';
        }
    } else {
        echo "Invalid request.";
        echo '<a href="index.php"> Home page </a>';
    }
} else {
    echo "Invalid request method.";
    echo '<a href="index.php"> Home page </a>';
}
```

```php
function getPostContent($post_id)
{
    // Assuming you have already established a database connection
    $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    if ($mysqli->connect_errno) {
        printf("Database connection failed: %s\n", $mysqli->connect_error);
        exit();
    }

    // Check if the logged-in user is the author of the post
    $username = $_SESSION['username'];

    $sql = "SELECT body FROM posts WHERE id=? AND added_by=?";
    $stmt = $mysqli->prepare($sql);
    $stmt->bind_param("is", $post_id, $username);
    $stmt->execute();
    $result = $stmt->get_result();

    // Debugging statements using JavaScript console.log()
    echo "<script>";
    echo "console.log('SQL: " . $sql . "');";
    echo "console.log('Post ID: " . $post_id . "');";
    echo "console.log('Username: " . $username . "');";
    echo "</script>";

    if ($result->num_rows == 1) {
        $row = $result->fetch_assoc();
        return $row['body'];
    } else {
        return false;
    }
}



function getUserName($username, $mysqli)
{
    $sql = "SELECT username FROM users WHERE username=?";
    $stmt = $mysqli->prepare($sql);
    $stmt->bind_param("s", $username);
    $stmt->execute();
    $result = $stmt->get_result();
    $row = $result->fetch_assoc();
    return $row['username'];
}
```

```
?>
```

/register.php

```
<!-- Register.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php
include 'session-file.php';
include 'handlers/register_handler.php';
include 'handlers/login_handler.php';
?>


<!DOCTYPE html>
<html lang="en">
<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Welcome to WAPH-MiniFacebook</title>

    <!-- CSS -->
    <link rel="stylesheet" href="assets/register.css">
    <!-- <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.
    <style>
        .alert{
            color: red;
            margin: auto;
        }
        .pswd_icon_bg{
            background: white;
            height: 32px;
            width: 30px;
            position: absolute;
            display: flex;
            align-content: center;
            overflow: hidden;
            margin: 0 0 0 525px;
        }
    </style>


    <!-- favigon -->
```

```
    <link rel="shortcut icon" href="images/favigon.jpg" type="image/x-icon">
    <!-- <link rel="stylesheet" href="assets/fontawesome-free-5.15.1-web/css/all.css"> -->

</head>

<body>

    <div class="top-content">
        <h1 style="font-size:35px; color: maroon;">Welcome to Minifacebook by team16</h1>
        <hr style="width: 50%; color: white; margin-bottom:25px; margin-top:25px;">
    </div>

    <div class="wreper">
        <div class="signin-form">
            <div class="form-top-left">
                <h3 style="padding-top:10px;">Login to our site</h3>
                <p style="margin-top:-20px; padding-bottom:10px;">Enter Email and password t
            </div>
            <div class="form-bottom">
                <form action="register.php" method="POST" class="login-form">
                    <!-- Email Addresss -->
                        <label for="form-email">Email Address</label>
                        <input type="email" name="log_email" placeholder="Email Address" val
                            echo $_SESSION['log_email'];
                        } ?>" required> <br>

                    <!-- Password -->
                        <label for="form-password">Password</label>
                        <span class="pswd_icon_bg"  onclick="log_pswd_toggale()"><i class="f
                        <input type="password" id="login_pswd" name="log_password" placehold

                    <!-- remember me -->


                    <?php if(in_array("Email or Password was incorrect", $error_array_login)
                    <?php if(in_array("User disabled by admin", $error_array_login)) echo "<
                    <button type="submit" style="margin-bottom:20px" name="login_button">Sig
                </form>
                <form action="admin.php" method="GET">
        <button type="submit" style="margin-bottom:20px">Go to Admin Page</button>
    </form>
            </div>
        </div>

        <hr style="height:300px; color:white; margin-top:110px;">
```

```
<div class="signup-form">
    <div class="form-top-left">
        <h3 style="padding-top:10px;">Sign up now</h3>
        <p style="margin-top:-20px; padding-bottom:10px;">Fill in the form below to
    </div>
    <div class="form-bottom">
        <form action="register.php" method="POST">

            <!-- First Name -->
            <label>First name</label>
            <input type="text" name="reg_fname" placeholder="First Name" value="<?ph
                echo $_SESSION['reg_fname'];
            } ?>" required>
            <?php if (in_array("Your first name must be between 2 and 25 characters'
                  {
                      echo "<p class='alert'>Your first name must be between 2 and 2
                  }
            ?>

            <!-- Last Name -->
            <label>Last name</label>
            <input type="text" name="reg_lname" placeholder="Last Name" value="<?php
                echo $_SESSION['reg_lname'];
            } ?>" required>
            <?php if (in_array("Your last name must be between 2 and 25 characters"
            ?>

            <!-- Username -->
            <label>Username</label>
            <input type="text" name="username" placeholder="Username (Cannot be char
                echo $_SESSION['username'];
            } ?>" required>
            <?php
                if(in_array("Username already exists", $error_array)) echo "<p class
                else if(in_array("Username must be between 2 and 20", $error_array))
                else if(in_array("You username can only contain english characters c
            ?>

            <!-- Email -->
            <label>Email</label>
            <input type="email" name="reg_email" placeholder="Email" value="<?php if
                echo $_SESSION['reg_email'];
            } ?>" required>

             <!-- Confirm Email -->
            <label>Confirm Email</label>
```

```
<input type="email" name="reg_email2" placeholder="Confirm Email" value=
    echo $_SESSION['reg_email2'];
} ?>" required>

<!-- Additional Email -->
<label>Additional Email</label>
<input type="email" name="add_email" placeholder="Additional Email" valu
    echo $_SESSION['add_email'];
} ?>" required>

<!-- phone -->
<label>Phone</label>
<input type="text" name="phone" placeholder="Phone Number" value="<?php
    echo $_SESSION['phone'];
} ?>" required>


<?php
    if (in_array("Email already in use", $error_array)) echo "<p class="
    else if (in_array("Email is invalid format", $error_array)) echo "<p
    else if (in_array("Email doesn't match", $error_array)) echo "<p cla
?>

<!-- Password -->
<label>Password</label>
<span class="pswd_icon_bg"  onclick="reg_pswd_toggale()"><i class="fa-re
<input type="password" id="register_pswd" name="reg_password" placeholde
<?php

?>

<!-- Confirm Password -->
<label>Confirm password</label>
<span class="pswd_icon_bg"  onclick="reg_conf_pswd_toggale()"><i class="
<input type="password" id="register_conferm_pswd" name="reg_password2" p
<?php
    if(in_array("Your passwords doesn't match", $error_array)) echo "<p
    else if(in_array("Your password can only contain english characters
    else if(in_array("Your password must be between 5 and 30 characters
?>

<!-- Gender -->
<label>Gender</label>
<tr>
    <td>
        <input style="width:10px; height:10px;" type="radio" name="gende
```

```
                        ?> checked <?php
                        } ?> required> Male
                        <input style="width:10px; height:10px;" type="radio" name="gende
                        ?> checked <?php
                        } ?> required> Female
                    </td>
                </tr>

                <!-- Birthday -->
                <br>
                <!-- <label>Birthday</label> -->
                <tr>
                    <td>Birthday
                      
                    <input type="date" name="dob" value="<?php if (isset($_SESSION['dob'
                        echo $_SESSION['dob'];
                    } ?>" requred>
                    </td>
                </tr>


                <!-- Submit Button -->
                <button type="submit"  style="margin-bottom:20px" name="reg_user" >Sign
                 <?php
                    if(in_array("success", $success_array)) echo "<p class='alert'>User
                    else if(in_array("failed", $success_array)) echo "<p class='alert'>U
                ?>

            </form>
        </div>
    </div>
</div>

<hr style="color:white; margin-top:265px; width:40%;">

<!-- Footer -->
<footer>
    <div class="footer">
        <a style="text-decoration-line: none; color: #977AFF;" href="admin.php"><i class
        <p> ©2020 All Rights Reserved <BR> Website designed and developed by <strong><U
    </div>
</footer>

<script>
    function log_pswd_toggale() {
        var x = document.getElementById("login_pswd");
```

```
            var img = document.getElementById("pswd_show");
            if (x.type === "password") {
                img.className = "fa-regular fa-eye-slash"
                x.type = "text";
            } else {
                img.className = "fa-regular fa-eye"
                x.type = "password";
            }
        }
        function reg_pswd_toggale() {
            var y = document.getElementById("register_pswd");
            var img = document.getElementById("reg_pswd_show");
            if (y.type === "password") {
                img.className = "fa-regular fa-eye-slash"
                y.type = "text";
            } else {
                img.className = "fa-regular fa-eye"
                y.type = "password";
            }
        }
        function reg_conf_pswd_toggale() {
            var z = document.getElementById("register_conferm_pswd");
            var img = document.getElementById("reg_conf_pswd_show");
            if (z.type === "password") {
                img.className = "fa-regular fa-eye-slash"
                z.type = "text";
            } else {
                img.className = "fa-regular fa-eye"
                z.type = "password";
            }
        }
    </script>

</body>

</html>
```

/profile.php

```
<!-- Profile.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php include 'header.php';
    //   include 'classes/User.php';
    //   include 'classes/Post.php';
```

```
    if(isset($_GET['profile_username'])){
        $username = $_GET['profile_username'];
        $user_detail_query = mysqli_query($con,"select * from users where username='$usernam
        $user_array = mysqli_fetch_array($user_detail_query);
    }
    $num_friends = (substr_count($user_array['friend_array'],","))-1;

    if(isset($_POST['remove_friend'])){
        $user = new User($con, $userLoggedIn);
        $user->removeFriend($username);
    }

    if(isset($_POST['add_friend'])){
        $user = new User($con, $userLoggedIn);
        $user->sendRequest($username);
    }

    if(isset($_POST['accept_request'])){
        header("Location: request.php");
    }

    if(isset($_POST['send_msg'])){
        header("Location: messages.php?u=$username");
    }
?>
<style>
    .wreper_left{
        margin-left: 100px;
        margin-top: 30px;
        width: 20%;
    }

    .wreper_right{
        margin-left: 350px;
        margin-top: -40px;
    }

    .left_info_wreper{
        margin-left: 50px;
        line-height: 25px;
        display: flex;
    }

</style>
            <div class="profile_top">
```

```
                    <img class="cover" src='<?php echo $user_array['cover_pic']; ?>'>
                    <img class="profile" src='<?php echo $user_array['profile_pic']; ?>'>
                    <?php $FirstAndLastName = $user_array['first_name']." ". $user_array['last_n
                        echo "<span class='FastAndLastName'>".$FirstAndLastName."</span>";
                        $username = $user_array['username'];

                        echo "<span class='username'>@$username</span>";
                    ?>
                    <div class="btns" style="display: flex; margin: -15px 500px;">
                        <form action="#" method="POST">
                            <button class="message" name="send_msg"><i class="fas fa-comment-alt
                        </form>
                        <form action="user_details.php" method="GET">
    <button type="submit" name="show_details">Show Details</button>
</form>

                        <form action="<?php echo $username; ?>" method="POST">

                            <?php

                                $profile_user_obj = new User($con, $username);
                                if($profile_user_obj->isClosed()){
                                    header("Location: user_closed.php");
                                }
                                $logged_in_user_obj = new User($con, $userLoggedIn);
                                if($userLoggedIn != $username){
                                    if($logged_in_user_obj->isFriend($username)){
                                        echo '<span  class="addFriend"  style="background: #ff5
                                    }
                                    else if ($logged_in_user_obj->didReceiveRequest($username))
                                        echo '<span  class="addFriend"  style="background: #73d6
                                    }
                                    else if ($logged_in_user_obj->didSendRequest($username)) {
                                        echo '<span  class="addFriend"  style="background: #73d6
                                    }
                                    else {
                                        echo '<span style="margin-left: 575px;" class="addFriend
                                    }
                                }
                            ?>


                        </form>
                    </div>
                </div>
```

```
<div class="main-coluam">
    <?php
            $username = $user_array['username'];
            $ret_str = "";
            $data_query = mysqli_query($con, "SELECT * FROM posts ORDER BY id DE

                while($row = mysqli_fetch_array($data_query)) {
                    $id = $row['id'];
                    $body = $row['body'];
                    $added_by = $row['added_by'];
                    $date_time = $row['date_added'];
                    $imagePath = $row['image'];

                    if($username == $added_by){

                        // show post/display post
                        $user_details_query = mysqli_query($con, "SELECT first_n
                        $user_row = mysqli_fetch_array($user_details_query);
                        $first_name = $user_row['first_name'];
                        $last_name = $user_row['last_name'];
                        $profile_pic = $user_row['profile_pic'];

                        ?>

                        <script>
                            function toggle<?php echo $id; ?>(){


                                var element = document.getElementById("toggl

                                if(element.style.display == "block")
                                    element.style.display = "none";
                                else
                                    element.style.display = "block";

                            }
                        </script>

                        <?php
                        // count comments
                        $comment_check = mysqli_query($con,"select * from commen
                        $comment_check_num = mysqli_num_rows($comment_check);

                        $date_time_now = date("Y-m-d H:i:s");
                        $start_date = new DateTime($date_time); //time of post
```

```php
$end_date = new DateTime($date_time_now); //curent time
$interval = $start_date->diff($end_date); //difrent betu

if($interval->y >= 1){
    if($interval == 1)
        $time_message = $interval->y . " year ago";
    else
        $time_message = $interval->y . " years ago";
}
else if($interval->m >= 1){
    if($interval->d == 0){
        $days = " ago";
    }
    else if($interval->d == 1){
        $days = $interval->d . " day ago";
    }
    else{
        $days = $interval->d . " days ago";
    }

    if($interval->m == 1){
        $time_message = $interval->m . " month" .
        $days;
    }
    else{
        $time_message = $interval ->m . " months".
        $days;
    }
}

else if($interval->d >= 1){
    if($interval->d == 1){
        $time_message = "Yesterday";
    }
    else{
        $time_message = $interval->d . " days ago";
    }
}

else if($interval->h >= 1){
    if($interval->h == 1){
        $time_message = $interval->h . " hour ago";
    }
    else{
        $time_message = $interval->h . " hours ago";
    }
```

```
}

else if($interval->i >= 1){
    if($interval->i == 1){
        $time_message = $interval->i . " minute ago";
    }
    else{
        $time_message = $interval->i . " minutes ago";
    }
}

else{
    if($interval->s < 30){
        $time_message = "Just Now";
    }
    else{
        $time_message = $interval->s . " seconds ago";
    }
}


$ret_str .= "
    <div class='status_post'>
        <div class='post_profile_pic'>
            <img src='$profile_pic' width='50' style='bo
        </div>
        <div class='posted_by' style='color:#ACACAC;'>
            <a href='$added_by'> $first_name $last_name
            <div class='time'> $time_message </div>
        </div> <br> <br>
        <div class='post_body' id='post_body'>
        <span style='margin-left: 34px;'> $body </span>
        </div>
    </div>
    <div calss='post_feature'>
        <span class='comment' style='color: #3875c5; for
        <iframe src='like.php?post_id=$id'style='
        border: 0px;
        height: 25px;
        width: 120px;
        margin-left: 35px;
    ' scrolling='no'></iframe>
    </div>
    <div class='post_comment' id='toggleComment$id' styl
        <iframe src='comment_frame.php?post_id=$id' id='
    </div>
```

```
                                <hr style='margin-bottom: 28px;'> ";
                            }//end if

                        }//end of loop

                    echo $ret_str;

            ?>
        </div>

        <div class="profile_left">
            <div class="left_wreper">
                <div class="wreper_top">
                    <center><h2> <?php echo $FirstAndLastName ?> </h2></center>
                    <center><span> @<?php echo $username ?> </span></center>
                </div>
                <hr>
                <div class="wreper_left">
                    <div class="post"> <b> Posts </b> </div> <br>
                    <div class="num_post"  style="margin-left: 15px;"> <?php echo $user_
                </div>
                <hr style="transform: rotate(90deg); margin-top: -19px; width: 75px;">
                <div class="wreper_right">
                    <div class="post"> <b> Friends </b> </div> <br>
                    <div class="num_friend" style="margin-left: 15px;"> <?php echo $num_
                </div>
            </div>
        </div>

        <!-- <div class="left_info">
            <div class="left_info_wreper">
                <div class="lable"> Bio <br>
                 e-Mail   <br>
                 Ph. no.   <br>
                 country   <br>
                 city  <br>
                 </div>
                 <div class="op" style="margin-left: 60px;">
                    <?php echo $user_array['bio'] ?> <br>
                    <?php echo $user_array['email'] ?> <br>
                    <?php echo $user_array['phone'] ?> <br>
                    <?php echo $user_array['country'] ?> <br>
                    <?php echo $user_array['city'] ?> <br>
                 </div>
            </div>
        </div> -->
```

```
        </div>

    </body>

</html>
```

/update.php

```
<?php
session_start();

if (!isset($_SESSION['authenticated']) || $_SESSION['authenticated'] !== TRUE) {
    echo "You are not logged in.";
    exit;
}

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if (isset($_POST['post_id']) && isset($_POST['updated_content'])) {
        $post_id = $_POST['post_id'];
        $updated_content = $_POST['updated_content'];

        // Assuming you have a function to update a post based on post ID
        if (updatePost($post_id, $updated_content)) {
            echo "Post updated successfully.";
            echo '<a href="index.php"> Home page </a>';
        } else {
            echo "Failed to update post.";
            echo '<a href="index.php"> Home page </a>';
        }
    } else {
        echo "Invalid request.";
        echo '<a href="index.php"> Home page </a>';
    }
} else {
    echo "Invalid request method.";
    echo '<a href="index.php"> Home page </a>';
}

function updatePost($post_id, $updated_content)
{
    // Assuming you have already established a database connection
    $mysqli = new mysqli('localhost', 'waph_team16', 'password', 'waph_teamproject');
    if ($mysqli->connect_errno) {
        printf("Database connection failed: %s\n", $mysqli->connect_error);
        exit();
```

```
    }

    $sql = "UPDATE posts SET body=? WHERE id=?";
    $stmt = $mysqli->prepare($sql);
    $stmt->bind_param("si", $updated_content, $post_id);
    if ($stmt->execute()) {
        return true;
    } else {
        return false;
    }
}
?>
```

/index.php

```
<!-- Index.php^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ -->

<?php
        include 'header.php';

    // Start session with secure settings
    session_set_cookie_params([
        'lifetime' => 3600, // Lifetime in seconds
        'path' => '/',
        'domain' => 'localhost', // Change to your domain
        'secure' => true, // HTTPS only
        'httponly' => true // HTTP only
    ]);
    session_start();

    // Function to sanitize user inputs
    function sanitize($input) {
        return htmlentities($input, ENT_QUOTES, 'UTF-8');
    }
    if (!isset($_SESSION['authenticated']) || $_SESSION['authenticated'] !== TRUE) {
        session_destroy();
        echo "<script>alert('You have not logged in. Please log in first!');</script>";
        header("Refresh: 0; url=register.php");
        die();
    }

    if(isset($_SESSION['last_visit'])) {
        $lastVisit = $_SESSION['last_visit'];
        echo "Last visit: $lastVisit"; // Echo last visit time
    }
```

```php
// Update last visit time
$_SESSION['last_visit'] = date("Y-m-d H:i:s");



if(isset($_POST['post'])){
    $uploadOk = 1;
    $imageName = sanitize($_FILES['fileToUpload']['name']);
    $errorMessage = "";

    // Rest of your code
}

// Rest of your code

// Validate session to prevent hijacking
if(isset($_SESSION['user_agent']) && $_SESSION['user_agent'] !== $_SERVER['HTTP_USER_AGE
    // Session hijacked, destroy session
    session_destroy();
    // Perform further actions like redirecting to login page
echo "<script>alert('Session hijacking attack detected!');</script>";
header("Refresh: 0; url=register.php");
die();
}

// Update user agent in session
$_SESSION['user_agent'] = $_SERVER['HTTP_USER_AGENT'];

if(isset($_POST['post'])){
    $uploadOk = 1;
    $imageName = $_FILES['fileToUpload']['name'];
    $errorMessage = "";

    if($imageName != ""){
        $targetDir = "assets/images/posts/";
        $imageName = $targetDir . uniqid() . basename($imageName);
        $imageFileType = pathinfo($imageName, PATHINFO_EXTENSION);

        if($uploadOk){
            if(move_uploaded_file($_FILES['fileToUpload']['tmp_name'], $imageName)){
                //image Upload Okey
                $errorMessage = "uploaded";
            }
            else{
                $uploadOk = 0;
```

```
                    $errorMessage = "fail to upload";
                }
            }
        }

        if($uploadOk){
            $post = new Post($con, $userLoggedIn);
            $post->submitPost($_POST['post_text'], $imageName);
        }
        else{
            echo "<div style='text-align: center;' class='alert alert-danger'> $errorMessage
        }
    }

    $user_detail_query = mysqli_query($con,"select * from users where username='$userLoggedI
    $user_array = mysqli_fetch_array($user_detail_query);
    $num_friends = (substr_count($user_array['friend_array'],","))-1;

?>

<div class="index-wrapper">
    <div class="info-box">
        <div class="info-inner">
            <div class="info-in-head">
                <a href="<?php echo $userLoggedIn; ?>"><img src="<?php echo $user['cover_pic
            </div>
            <div class="info-in-body">
                <div class="in-b-box">
                    <div class="in-b-img">
                        <a href="<?php echo $userLoggedIn; ?>"><img src="<?php echo $user['p
                    </div>
                </div>
                <div class="info-body-name">
                    <div class="in-b-name">
                        <div><a href="<?php echo $userLoggedIn; ?>"><?php echo $user['first_
                        </div>
                        <span><small><a href="<?php echo $userLoggedIn; ?>"><?php echo "@" .
                    </div>
                </div>
            </div>
            <div class="info-in-footer">
                <div class="number-wrapper">
                    <div class="num-box">
                        <div class="num-head">
                            POSTS
                        </div>
```

```
                        <div class="num-body">
                            <?php echo $user['num_posts']; ?>
                        </div>
                    </div>
                    <div class="num-box">
                        <div class="num-head">
                            LIKES
                        </div>
                        <div class="num-body">
                            <span class="count-likes">
                                <?php echo $user['num_likes']; ?>
                            </span>
                        </div>
                    </div>
                    <div class="num-box">
                        <div class="num-head">
                            Friends
                        </div>
                        <div class="num-body">
                            <?php echo $num_friends ?>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </div>

    <div class="post-wrap">
        <div class="post-inner">
            <div class="post-h-left">
                <div class="post-h-img">
                    <a href="<?php echo $userLoggedIn; ?>"><img src="<?php echo $user['profi
                 </div>
            </div>

            <div class="post-body">
                <form class="post_form" action="index.php" method="POST" enctype="multipart/
                    <textarea class="status" name="post_text" id="post_text" placeholder="Ty
                    <div class="hash-box">
                        <ul>
                        </ul>
                    </div>
            </div>
                <div class="post-footer">
                    <div class="p-fo-left">
                        <ul>
```

```
                                <input type="file" name="fileToUpload" id="fileToUpload"/>
                                <label for="fileToUpload"> <img src="assets/images/camera.png" a
                                <span class="tweet-error"></span>
                                <input id="sub-btn" type="submit" name="post" value="SHARE">
                            </ul>
                        </form>
                        </div>
                    </div>
                </div>
            </div>
        </div>
        <div class="show_post">
            <?php
                $post = new Post($con, $userLoggedIn) ;
                $post->indexPosts();
            ?>
        </div>
    </div>
    </body>
    </html>
```