Website:

“CARE”



Online Post Office Management System

# PROJECT GROUP MEMBERS

|  |  |
| --- | --- |
| Students Id | Student Name |
| **Student1424628** | **Ifra Khan** |
| **Student1425119** | **Asad Afzal** |
| **Student1424612** | **Hanzala Khan** |
| **Student1417959** | **Moiz Khan** |

## CURRICULUM BATCH

**6740 2210B3**

## FACULTY

**Sir. Ebad Uddin Ahmed**

## CO-ORDINATOR

**MS. Munazzah Khan**

Online Post Office Management System

**Appointment Controller**

if (isset($\_POST["submit"])) {

    $name = $\_POST["pname"];

    $email = $\_POST["pemail"];

    $doctor = $\_POST["pdoctor"];

    $specialization = $\_POST["pspecialization"];

    $date = $\_POST["pday"];

    $time = $\_POST["ptime"];

    // print\_r($\_POST);

    // die();

    $insert = "INSERT INTO `appointment` (`pname`, `pemail`, `pdoctor`, `pspecialization`, `pday`, `ptime`) VALUES ('$name', '$email', '$doctor', '$specialization', '$date', '$time')";

    $connection\_insert = mysqli\_query($connection, $insert);

    if ($connection\_insert) {

        echo "

        <script>

        alert('Your Appointment Sent to Hospital. Once its checked your appointment will be set as per date and time.')

</script>";

        echo '<script> window.location.href="appointmentview.php";</script>';

    } else {

        echo "

        <script>

        alert('Your Appointment not set.')

        </script>";

        }

    }

?>

Online Post Office Management System

**Appointment View Controller**

<?php $username = $\_SESSION['useremail'];

                    $fetch = "SELECT \* FROM `appointment` AS a INNER JOIN `doctors` AS d

                        ON a.`pdoctor` = d.`id` WHERE `pemail` = '$username'";

                    $querry = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($querry) > 0) {

                        ?>

                        <table class="table table-bordered table-dark table-striped">

                            <thead>

                                <tr>

                                    <th>ID</th>

                                    <th>Patient Name</th>

                                    <th>Patient Email</th>

                                    <th>Doctor</th>

                                    <th>Specialization</th>

                                    <th>Day</th>

                                    <th>Time</th>

                                </tr>

                            </thead>

                            <tbody>

                                <?php

                                while ($row = mysqli\_fetch\_assoc($querry)) {

                                    ?>

                                    <tr>

                                        <td>

                                            <?php echo $row['pid'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['pname'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['pemail'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['Dusername'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['specialization'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['pday'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['ptime'] ?>

                                        </td>

                                    </tr>

                                    <?php

                                }

                    }

                    ?>

Online Post Office Management System

Doctor Controller

$fetch = "SELECT \* FROM `doctors` WHERE `Dstatus` = '1'";

$query = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($query) > 0) {

    ?>

                <?php while ($row = mysqli\_fetch\_assoc($query)) {

                    ?>

                    <div class="col-lg-4 wow slideInUp" data-wow-delay="0.3s">

                        <div class="team-item">

                            <div class="position-relative rounded-top" style="z-index: 1;">

        <img class="img-fluid rounded-top w-100" style="height: 300px;"

              src="<?php echo 'doctors/doctorimg/' . $row['Dimage'] ?>" alt="Doctor Image">

                            </div>

<div class="team-text position-relative bg-light text-center rounded-bottom p-4 pt-5">

                                <h4 class="mb-2">

                                    <?php echo $row['Dusername'] ?>

                                </h4>

                                <p class="text-primary mb-0">

                                    <?php echo $row['specialization'] ?>

                                </p>

                            </div>

                        </div>

                    </div>

                    <?php

                }

}

?>

Online Post Office Management System

**Patient Controller**

<?php

include('includes/navebar.php');

include('includes/config.php');

$email = $\_SESSION['useremail'];

$fetch = "SELECT \* FROM `Patient` WHERE `email` = '$email'";

$query = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($query) > 0) {

    ?>

 <?php

 while ($row = mysqli\_fetch\_assoc($query)) {

    <div class="col-12 col-sm-12">

    <input type="hidden" name="id" value="<?php echo $row['id'] ?>" class="form-control">

    <div id="image-container">

<img id="selected-image" src="<?php echo 'userimg/' . $row['PImage'] ?>"alt="Selected Image" height="200px" width="200px"style="border-radius: 200px; border:2px groove black;">

                    <button id="change-image" style="display: none;">Change Image</button>

                         </div>

                              </div>

<div class="col-12 col-sm-12">

<input type="file" id="image-input" name="imgs" class="form-control"style="display: none;">

<label for="image-input" class="custom-file-upload" name="imgs">Upload Image</label>

</div>

<div class="col-12 col-sm-12">

<input type="text" name="name" class="form-control bg-light border-0 "value="<?php echo $row['name'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="email" name="email" class="form-control bg-light border-0 " value="<?php echo $row['email'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="phone" name="phone" class="form-control bg-light border-0 " value="<?php echo $row['phone'] ?>" style="height: 55px;">

</div>

<div class="col-12">

<button class="btn btn-dark w-100 py-3" name="submit" type="submit">Edit Profile</button></div>

} ?>

**Search Controller**

<?php

require('Includes/config.php');

if (isset($\_GET['query'])) {

    $query = $\_GET['query'];

    $sql = "SELECT `id`, `specialization` FROM `doctors` WHERE `specialization` LIKE '%$query%'";

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

    if ($result->num\_rows > 0) {

        while ($row = $result->fetch\_assoc()) {

            echo '<li class="suggestion" data-hospital-id="' . $row['id'] . '" style="margin-left: 30px; margin-top:20px; color: white; list-style-type: none; text-decoration: none;"

            onmouseover="this.style.color=\'blue\';" onmouseout="this.style.color=\'white\';">' . $row['specialization'] . '</li>';

        }

    } else {

        echo "No results found";

    }

}

$connection->close();

?>

Online Post Office Management System

**Signup Controller**

<?php

require 'vendor/autoload.php'; // Composer se install kiya hua ho to yeh line add karein

// PHPMailer Integration

use PHPMailer\PHPMailer\PHPMailer;

use PHPMailer\PHPMailer\SMTP;

use PHPMailer\PHPMailer\Exception;

if (isset($\_POST['register'])) {

  $name = $\_POST['username'];

  $email = $\_POST['email'];

  $Password = $\_POST['password'];

  $hashPass = password\_hash($Password, PASSWORD\_BCRYPT);

  $check\_email = "SELECT \* from `patient` where email = '$email' ";

  $run\_email = mysqli\_query($connection, $check\_email);

  if (mysqli\_num\_rows($run\_email) > 0) {

    echo "</script> alert('Email already exist') </script>";

  } else {

    // User ka email address $user\_email variable mein store karein

    $user\_email = $email;

    // PHPMailer configuration

    $mail = new PHPMailer(true);

    try {

      // Server settings

      $mail->isSMTP();

      $mail->Host = 'smtp.gmail.com'; // SMTP server

      $mail->SMTPAuth = true;

      $mail->Username = 'ifrakhan2804@gmail.com'; // Sender's email address

      $mail->Password = 'wwuq dupp rnbo tcww';

      $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; // TLS encryption

      $mail->Port = 587; // Port for TLS

      // Recipient settings

      $mail->setFrom('ifrakhan2804@gmail.com', 'Ifra');

      $mail->addAddress($user\_email, $name); // User ka email address

      // Email content

      $mail->isHTML(true);

      $mail->Subject = 'Welcome to Our Website';

      $mail->Body = 'Thank you for registering on our website.';

      $mail->send();

    } catch (Exception $e) {

      echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

    }

    $insert = "INSERT INTO `patient` (`name`, `email`, `password`) VALUES ('$name', '$email','$hashPass')";

    $connect\_insert = mysqli\_query($connection, $insert);

  }

  header("location:login.php");

}

?>

**Login Controller**

<?php

include('includes/config.php');

include('includes/navebar1.php');

// include('header.php');

if (isset($\_POST['Login'])) {

  $Email = $\_POST['L\_email'];

  $Password = $\_POST['L\_Pass'];

  $login\_query = "SELECT \* from `patient` where email = '$Email'";

  $get\_from\_db = mysqli\_query($connection, $login\_query);

  if (mysqli\_num\_rows($get\_from\_db)) {

    $row = mysqli\_fetch\_assoc($get\_from\_db);

    $db\_pass = $row['password'];

    $pass\_decode = password\_verify($Password, $db\_pass);

    if ($pass\_decode) {

      $\_SESSION['useremail'] = $row['email'];

      $\_SESSION['username'] = $row['name'];

      echo "<script> alert('login secsesfully')

        window.location.href='index.php'

        </script>";

    } else {

      echo "<script> alert('Invalid Password')</script>";

    }

  } else {

    echo "<script> alert('Invalid Email')</script>";

  }

}

?>

Online Post Office Management System

**Logout Controller**

<?php

session\_start();

session\_unset();

session\_destroy();

header('location:signup.php');

?>

Online Post Office Management System

Update Password Controller

<?php

include('includes/navebar.php');

include('includes/config.php');

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

    $currentPassword = $\_POST["current\_password"];

    $newPassword = $\_POST["new\_password"];

    $confirmPassword = $\_POST["confirm\_password"];

    $username = $\_SESSION["useremail"];

    $query = "SELECT `password` FROM `patient` WHERE `email` = '$username'";

    $result = $connection->query($query);

    if (mysqli\_num\_rows($result) > 0) {

        $row = $result->fetch\_assoc();

        $dbPassword = $row["password"];

        if (password\_verify($currentPassword, $dbPassword)) {

            if ($newPassword == $confirmPassword) {

                $hashedPassword = password\_hash($newPassword, PASSWORD\_DEFAULT);

                $updateQuery = "UPDATE `patient` SET `password` = '$hashedPassword' WHERE `email` = '$username'";

                if ($connection->query($updateQuery) === TRUE) {

                    echo ' <script>

                    document.getElementById("dose1Alert").style.display = "block";

                    </script>';

                } else {

                    echo ' <script>

                    document.getElementById("dose2Alert").style.display = "block";

                    </script>';

                }

            } else {

                echo ' <script>

                    document.getElementById("dose3Alert").style.display = "block";

                    </script>';

            }

        } else {

            echo ' <script>

                    document.getElementById("dose4Alert").style.display = "block";

                    </script>';

        }

    } else {

        echo ' <script>

                    document.getElementById("dose5Alert").style.display = "block";

                    </script>';

    }

}

?>

**Update Profile Controller**

<?php

require("Includes/config.php");

session\_start();

if (!isset($\_SESSION["useremail"])) {

    echo '<script> window.location.href="login.php"</script>';

    exit();

}

$user\_id = $\_POST['id'];

$img = $\_FILES['imgs']['name'];

$img\_tmp = $\_FILES['imgs']['tmp\_name'];

$img\_size = $\_FILES['imgs']['size'];

$user\_name = mysqli\_real\_escape\_string($connection, $\_POST['name']);

$user\_email = mysqli\_real\_escape\_string($connection, $\_POST['email']);

$user\_phone = mysqli\_real\_escape\_string($connection, $\_POST['phone']);

$username = $\_SESSION["useremail"]; // Assuming that "hospital" is the session variable where the username is stored

// Update query with correct column names

$updateQuery = "UPDATE `patient` SET `name` = '$user\_name', `email` = '$user\_email', `phone` = '$user\_phone', `PImage` = '$img' WHERE `email` = '$username'

";

if (move\_uploaded\_file($img\_tmp, 'userimg/' . $img)) {

    $res = mysqli\_query($connection, $updateQuery);

    if (!$res) {

        die("Query failed");

    } else {

        echo "

        <script>alert('Profile Has Been Updated Successfully')

</script>";

        echo "<script>window.location.href='profile.php'</script>";

    }

} else {

    echo "

    <script>alert('Profile Update failed Successfully')

    </script>";

}

?>

Online Post Office Management System

**Doctors Controls**

**Doctor Login Controller**

<?php

include('../includes/config.php');

include('../includes/navbar1.php');

if (isset($\_POST['submit'])) {

  $Email = $\_POST['email'];

  $Password = $\_POST['password'];

  $login\_query = "SELECT \* from `doctors` where Demail = '$Email'";

  $get\_from\_db = mysqli\_query($connection, $login\_query);

  if (mysqli\_num\_rows($get\_from\_db)) {

    $row = mysqli\_fetch\_assoc($get\_from\_db);

    $db\_pass = $row['Dpassword'];

    $pass\_decode = password\_verify($Password, $db\_pass);

    if ($pass\_decode) {

      $\_SESSION['doctor'] = $row['Demail'];

      // $\_SESSION['doctor'] = $row['Dusername'];

      echo "<script> alert('login secsesfully')

        window.location.href='index.php'

        </script>";

    } else {

      echo "<script> alert('Invalid Password')</script>";

    }

  } else {

    echo "<script> alert('Invalid Email')</script>";

  }

}

?>

Online Post Office Management System

**Doctor Signup Controller**

<?php

require 'vendor/autoload.php'; // Composer se install kiya hua ho to yeh line add karein

// PHPMailer Integration

use PHPMailer\PHPMailer\PHPMailer;

use PHPMailer\PHPMailer\SMTP;

use PHPMailer\PHPMailer\Exception;

if(isset($\_POST['submit'])){

  $name = $\_POST['Dusername'];

  $email = $\_POST['Demail'];

  $Password = $\_POST['Dpassword'];

  $special = $\_POST['specialization'];

  $city = $\_POST['Dcity'];

  $days = $\_POST['Ddays'];

  $time = $\_POST['Dtime'];

  $hashPass = password\_hash($Password, PASSWORD\_BCRYPT);

  $check\_email = "SELECT \* from `doctors` where Demail = '$email' ";

  $run\_email = mysqli\_query($connection, $check\_email);

  if (mysqli\_num\_rows($run\_email) > 0) {

    echo "<script> alert('Email already exist') </script>";

  } else {

    // User ka email address $user\_email variable mein store karein

    $user\_email = $email;

    // PHPMailer configuration

    $mail = new PHPMailer(true);

    try {

      // Server settings

      $mail->isSMTP();

      $mail->Host = 'smtp.gmail.com'; // SMTP server

      $mail->SMTPAuth = true;

      $mail->Username = 'ifrakhan2804@gmail.com'; // Sender's email address

      $mail->Password = 'wwuq dupp rnbo tcww';

      $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; // TLS encryption

      $mail->Port = 587; // Port for TLS

      // Recipient settings

      $mail->setFrom('ifrakhan2804@gmail.com', 'Ifra');

      $mail->addAddress($user\_email, $name); // User ka email address

      // Email content

      $mail->isHTML(true);

      $mail->Subject = 'Welcome to Our Website';

      $mail->Body = 'Thank you for registering on our website.';

      $mail->send();

    } catch (Exception $e) {

      echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

    }

    $insert = "INSERT INTO `doctors` (`Dusername`, `Demail`, `Dpassword`, `specialization`, `Dcity`, `Days`, `Dtime`) VALUES ('$name', '$email', '$hashPass', '$special', '$city', '$days', '$time')";

    $connect\_insert = mysqli\_query($connection, $insert);

  }

  header("location:doc\_login.php");

}

?>

<?php

    $fetchcity = "SELECT \* FROM `cities`";

    $fetchcities = mysqli\_query($connection, $fetchcity);

    if (mysqli\_num\_rows($fetchcities) > 0){

    ?>

        <?php

        while($row=mysqli\_fetch\_assoc($fetchcities)){

        ?>

      <option value="<?php echo $row['cid']?>"><?php echo $row['Cities']?></option>

      <?php

      }

    }

    ?>

**Doctor process Controller**

<?php

include('connection.php');

// Database connection

// $db = new mysqli('localhost', 'root', ' ', 'care');

// if ($db->connect\_error) {

//     die("Connection failed: " . $db->connect\_error);

// }

// Get user input

$username = $\_POST['name'];

$email = $\_POST['email'];

$password = $\_POST['password'];

// Check if the username is already taken

$check\_query = "SELECT id FROM doctors WHERE email=?";

$stmt = $db->prepare($check\_query);

$stmt->bind\_param("s", $email);

$stmt->execute();

$stmt->store\_result();

if ($stmt->num\_rows > 0) {

    header("Location: doc\_signup.php?error=1");

} else {

    // Insert new admin

    $insert\_query = "INSERT INTO doctors (name,email, password) VALUES (?, ?)";

    $stmt = $db->prepare($insert\_query);

    $stmt->bind\_param("ss", $username, $email, $password);

    $stmt->execute();

    header("Location: ds\_success.php");

}

$stmt->close();

$db->close();

?>

**Doctor Appointment View**

                    <?php

                    $doctor\_name = $\_SESSION['doctor'];

                    $sql = "SELECT \* FROM appointment as a INNER JOIN doctors as d on a.pdoctor = d.id WHERE d.demail = '$doctor\_name'";

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

                    if ($result->num\_rows > 0) {

                        ?>

                        <table class="table table-bordered table-dark table-striped">

                            <thead>

                                <tr>

                                    <th>ID</th>

                                    <th>Patient Name</th>

                                    <th>Doctor</th>

                                    <th>Specialization</th>

                                    <th>Day</th>

                                    <th>Time</th>

                                </tr>

                            </thead>

                            <tbody>

                                <?php

                                while ($row = $result->fetch\_assoc()) {

                                    ?>

                                    <tr>

                                        <td>

                                            <?php echo $row['pid'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['pname'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['Dusername'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['specialization'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['pday'] ?>

                                        </td>

                                        <td>

                                            <?php echo $row['ptime'] ?>

                                        </td>

                                    </tr>

                                    <?php

                                }

                    } else {

                        echo "<h3> No appointments found for this doctor.</h3>";

                    }

                    ?>

**Doctor Logout Controller**

<?php

session\_start();

session\_unset();

session\_destroy();

header('location:doc\_signup.php');

?>

**Doctor Profile Controller**

<?php

include('../includes/navbar.php');

include('../includes/config.php');

$email = $\_SESSION['doctor'];

$fetch = "SELECT \* FROM `doctors` WHERE `Demail` = '$email'";

$query = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($query) > 0) {

    ?>

<?php

while ($row = mysqli\_fetch\_assoc($query)) {

<div class="col-12 col-sm-12">

<input type="hidden" name="id" value="<?php echo $row['id'] ?>" class="form-control">

<div id="image-container">

<img id="selected-image" src="<?php echo 'doctorimg/' . $row['Dimage'] ?>"alt="Selected Image" height="200px" width="200px"style="border-radius: 200px; border:2px groove black;">

<button id="change-image" style="display: none;">Change Image</button>

</div>

</div>

<div class="col-12 col-sm-12">

<input type="file" id="image-input" name="imgs" class="form-control" style="display: none;">

<label for="image-input" class="custom-file-upload" name="imgs">Upload Image</label>

</div>

<div class="col-12 col-sm-12">

<input type="text" name="dusername" class="form-control bg-light border-0 " value="<?php echo $row['Dusername'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="email" name="demail" class="form-control bg-light border-0 " value="<?php echo $row['Demail'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="text" name="specialization" class="form-control bg-light border-0 "value="<?php echo $row['specialization'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="text" name="Days" class="form-control bg-light border-0 " value="<?php echo $row['Days'] ?>" style="height: 55px;">

</div>

<div class="col-12 col-sm-6">

<input type="text" name="dtime" class="form-control bg-light border-0 " value="<?php echo $row['Dtime'] ?>" style="height: 55px;">

</div>

<div class="col-12">

<button class="btn btn-dark w-100 py-3" name="submit" type="submit">EditProfile</button>

</div>

} ?>

**Doctor Update Password Controller**

<?php

include('../includes/config.php');

include('../includes/navbar.php');

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

    $currentPassword = $\_POST["current\_password"];

    $newPassword = $\_POST["new\_password"];

    $confirmPassword = $\_POST["confirm\_password"];

    $username = $\_SESSION["doctor"];

    $query = "SELECT `Dpassword` FROM `doctors` WHERE `Demail` = '$username'";

    $result = $connection->query($query);

    if (mysqli\_num\_rows($result) > 0) {

        $row = $result->fetch\_assoc();

        $dbPassword = $row["Dpassword"];

        if (password\_verify($currentPassword, $dbPassword)) {

            if ($newPassword == $confirmPassword) {

                $hashedPassword = password\_hash($newPassword, PASSWORD\_DEFAULT);

                $updateQuery = "UPDATE `doctors` SET `Dpassword` = '$hashedPassword' WHERE `Demail` = '$username'";

                if ($connection->query($updateQuery) === TRUE) {

                    echo ' <script>

                    document.getElementById("dose1Alert").style.display = "block";

                    </script>';

                } else {

                    echo ' <script>

                    document.getElementById("dose2Alert").style.display = "block";

                    </script>';

                }

            } else {

                echo ' <script>

                    document.getElementById("dose3Alert").style.display = "block";

                    </script>';

            }

        } else {

            echo ' <script>

                    document.getElementById("dose4Alert").style.display = "block";

                    </script>';

        }

    } else {

        echo ' <script>

                    document.getElementById("dose5Alert").style.display = "block";

                    </script>';

    }

}

?>

**Doctor Update Profile Controller**

<?php

require("../Includes/config.php");

session\_start();

if (!isset($\_SESSION["doctor"])) {

    echo '<script> window.location.href="login.php"</script>';

    exit();

}

$user\_id = $\_POST['id'];

$img = $\_FILES['imgs']['name'];

$img\_tmp = $\_FILES['imgs']['tmp\_name'];

$img\_size = $\_FILES['imgs']['size'];

$user\_name = mysqli\_real\_escape\_string($connection, $\_POST['dusername']);

$user\_email = mysqli\_real\_escape\_string($connection, $\_POST['demail']);

$user\_sp = mysqli\_real\_escape\_string($connection, $\_POST['specialization']);

$user\_day = mysqli\_real\_escape\_string($connection, $\_POST['Days']);

$user\_time = mysqli\_real\_escape\_string($connection, $\_POST['dtime']);

$username = $\_SESSION["doctor"];

// print\_r($\_POST);

// print\_r($\_FILES);

// die();

// Assuming that "hospital" is the session variable where the username is stored

// Update query with correct column names

$updateQuery = "UPDATE `doctors` SET `Dusername`='$user\_name',`Demail`='$user\_email',`specialization`='$user\_sp',`Days`='$user\_day',`Dtime`='$user\_time',`Dimage`='$img' WHERE `demail` = '$username'

";

if (move\_uploaded\_file($img\_tmp, '../doctors/doctorimg/' . $img)) {

    $res = mysqli\_query($connection, $updateQuery);

    if (!$res) {

        die("Query failed");

    } else {

        echo "

        <script>alert('Profile Has Been Updated Successfully')

</script>";

        echo "<script>window.location.href='profile.php'</script>";

    }

} else {

    echo "

    <script>alert('Profile Update failed')

    </script>";

}

?>

**ADMIN CONTROLS**

**Add Doctor Controller**

<?php

                    $fetch = "SELECT \* FROM `doctors` AS d INNER JOIN `cities` AS c ON d.`Dcity` = c.`cid` WHERE d.`dstatus` = '1'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dusername'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Demail'] ?>

                                </td>

                                <td>

                                    <?php echo $row['specialization'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Days'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dtime'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-primary"

                                        href="modifydoctor.php?id=<?php echo $row['id'] ?>">Modify</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="trashdoctor.php?id=<?php echo $row['id'] ?>">Trash</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

**Add Blog Controller**

<?php

                    $fetch = "SELECT \* FROM `doctors` AS d INNER JOIN `cities` AS c ON d.`Dcity` = c.`cid` WHERE d.`dstatus` = '1'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dusername'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Demail'] ?>

                                </td>

                                <td>

                                    <?php echo $row['specialization'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Days'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dtime'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-primary"

                                        href="modifydoctor.php?id=<?php echo $row['id'] ?>">Modify</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="trashdoctor.php?id=<?php echo $row['id'] ?>">Trash</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

**ADD Cities Controller**

                    <?php

                    $fetch = "SELECT \* FROM `cities` WHERE `Cstatus` = '1'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['cid'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-primary"

                                        href="modifycity.php?cid=<?php echo $row['cid'] ?>">Modify</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="trashcity.php?cid=<?php echo $row['cid'] ?>">Trash</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

**ADD City Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

if (isset($\_POST['submits'])) {

  $city = $\_POST['city'];

  $check\_city = "SELECT \* from `cities` where Cities = '$city' ";

  $run\_city = mysqli\_query($connection, $check\_city);

  if (mysqli\_num\_rows($run\_city) > 0) {

    echo "<script> alert('City already exist') </script>";

  } else {

    $insert\_city = "INSERT INTO `cities` (`Cities`) VALUES ('$city')";

    $connect\_inserts = mysqli\_query($connection, $insert\_city);

    echo "<script> window.location.href='addcities.php'</script>";

  }

}

?>

**ADD Doctor Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

require '../vendor/autoload.php'; // Composer se install kiya hua ho to yeh line add karein

// PHPMailer Integration

use PHPMailer\PHPMailer\PHPMailer;

use PHPMailer\PHPMailer\SMTP;

use PHPMailer\PHPMailer\Exception;

if (isset($\_POST['submit'])) {

  $name = $\_POST['Dusername'];

  $email = $\_POST['Demail'];

  $Password = $\_POST['Dpassword'];

  $special = $\_POST['specialization'];

  $city = $\_POST['Dcity'];

  $days = $\_POST['Ddays'];

  $time = $\_POST['Dtime'];

  $hashPass = password\_hash($Password, PASSWORD\_BCRYPT);

  $check\_email = "SELECT \* from `doctors` where Demail = '$email' ";

  $run\_email = mysqli\_query($connection, $check\_email);

  if (mysqli\_num\_rows($run\_email) > 0) {

    echo "<script> alert('Email already exist') </script>";

  } else {

    // User ka email address $user\_email variable mein store karein

    $user\_email = $email;

    // PHPMailer configuration

    $mail = new PHPMailer(true);

    try {

      // Server settings

      $mail->isSMTP();

      $mail->Host = 'smtp.gmail.com'; // SMTP server

      $mail->SMTPAuth = true;

      $mail->Username = 'ifrakhan2804@gmail.com'; // Sender's email address

      $mail->Password = 'wwuq dupp rnbo tcww';

      $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; // TLS encryption

      $mail->Port = 587; // Port for TLS

      // Recipient settings

      $mail->setFrom('ifrakhan2804@gmail.com', 'Ifra');

      $mail->addAddress($user\_email, $name); // User ka email address

      // Email content

      $mail->isHTML(true);

      $mail->Subject = 'Welcome to Our Website';

      $mail->Body = 'Thank you for registering on our website.';

      $mail->send();

    } catch (Exception $e) {

      echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

    }

    $insert = "INSERT INTO `doctors` (`Dusername`, `Demail`, `Dpassword`, `specialization`, `Dcity`, `Days`, `Dtime`) VALUES ('$name', '$email', '$hashPass', '$special', '$city', '$days', '$time')";

    $connect\_insert = mysqli\_query($connection, $insert);

    echo "<script> window.location.href='add.php'</script>";

  }

}

?>

        <?php

        $fetchcity = "SELECT \* FROM `cities`";

        $fetchcities = mysqli\_query($connection, $fetchcity);

        if (mysqli\_num\_rows($fetchcities) > 0) {

          while ($row = mysqli\_fetch\_assoc($fetchcities)) {

            ?>

            <option value="<?php echo $row['cid'] ?>">

              <?php echo $row['Cities'] ?>

            </option>

            <?php

          }

        }

        ?>

**Add More Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

if (isset($\_POST['submit'])) {

    $name = $\_POST['bname'];

    $des = $\_POST['bdescription'];

    $time = $\_POST['btime'];

    $date = $\_POST['bdate'];

    $Image = $\_FILES['bimage']['name'];

    $Imagetmp = $\_FILES['bimage']['tmp\_name'];

    $Imagesize = $\_FILES['bimage']['size'];

    $insert = "INSERT INTO `blogs` (`bname`, `bdescription`, `btime`, `bdate`, `bimage`) VALUES ('$name', '$des', '$time', '$date', '$Image')";

    $connect\_insert = mysqli\_query($connection, $insert);

    move\_uploaded\_file($Imagetmp, 'blogimg/' . $Image);

    echo "<script> window.location.href='addblog.php'</script>";

}

?>

**Add Patient Controller**

                    <?php

                    $fetch = "SELECT \* FROM `patient` WHERE `pstatus` = '1'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['name'] ?>

                                </td>

                                <td>

                                    <?php echo $row['email'] ?>

                                </td>

                                <td>

                                    <?php echo $row['phone'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-primary"

                                        href="modifypatient.php?id=<?php echo $row['id'] ?>">Modify</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="trashpatient.php?id=<?php echo $row['id'] ?>">Trash</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

**Add Patients Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

require '../vendor/autoload.php'; // Composer se install kiya hua ho to yeh line add karein

// PHPMailer Integration

use PHPMailer\PHPMailer\PHPMailer;

use PHPMailer\PHPMailer\SMTP;

use PHPMailer\PHPMailer\Exception;

if (isset($\_POST['register'])) {

  $name = $\_POST['username'];

  $email = $\_POST['email'];

  $Password = $\_POST['password'];

  $phone = $\_POST['phone'];

  $hashPass = password\_hash($Password, PASSWORD\_BCRYPT);

  $check\_email = "SELECT \* from `patient` where email = '$email' ";

  $run\_email = mysqli\_query($connection, $check\_email);

  if (mysqli\_num\_rows($run\_email) > 0) {

    echo "<script> alert('Email already exist') </script>";

  } else {

    // User ka email address $user\_email variable mein store karein

    $user\_email = $email;

    // PHPMailer configuration

    $mail = new PHPMailer(true);

    try {

      // Server settings

      $mail->isSMTP();

      $mail->Host = 'smtp.gmail.com'; // SMTP server

      $mail->SMTPAuth = true;

      $mail->Username = 'ifrakhan2804@gmail.com'; // Sender's email address

      $mail->Password = 'wwuq dupp rnbo tcww';

      $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; // TLS encryption

      $mail->Port = 587; // Port for TLS

      // Recipient settings

      $mail->setFrom('ifrakhan2804@gmail.com', 'Ifra');

      $mail->addAddress($user\_email, $name); // User ka email address

      // Email content

      $mail->isHTML(true);

      $mail->Subject = 'Welcome to Our Website';

      $mail->Body = 'Thank you for registering on our website.';

      $mail->send();

    } catch (Exception $e) {

      echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

    }

    $insert = "INSERT INTO `patient` (`name`, `email`, `password`, `phone`) VALUES ('$name', '$email','$hashPass' ,'$phone')";

    $connect\_insert = mysqli\_query($connection, $insert);

    echo "<script> window.location.href='addpatients.php'</script>";

  }

}

?>

**Admin Profile Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$email = $\_SESSION['admin'];

$fetch = "SELECT \* FROM `admin` WHERE `Aemail` = '$email'";

$query = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($query) > 0) {

    ?>

    <!-- Team Start -->

    <div class="container-fluid wow fadeInUp mt-4" data-wow-delay="0.1s">

        <div class="container">

            <div class="row gx-5">

                <div class="col-lg-12">

                    <div class="appointment-form h-100 d-flex flex-column justify-content-center text-center wow zoomIn"

                        data-wow-delay="0.6s">

                        <h1 class="text-dark mb-2">Profile</h1>

                        <form method="post" action="updateprofile.php" class="form-group" enctype="multipart/form-data">

                            <div class="row g-3">

                                <?php

                                while ($row = mysqli\_fetch\_assoc($query)) {

                                    ?>

                                    <div class="col-12 col-sm-12">

                                        <input type="hidden" name="id" value="<?php echo $row['Aid'] ?>" class="form-control">

                                        <div id="image-container">

                                            <img id="selected-image" src="<?php echo 'adminimg/' . $row['AImage'] ?>"

                                                alt="Selected Image" height="100px" width="100px"

                                                style="border-radius: 400px; border:2px groove black;">

                                            <button id="change-image" style="display: none;">Change Image</button>

                                        </div>

                                    </div>

                                    <div class="col-12 col-sm-12">

                                        <!-- <label for="text">Image</label> -->

                                        <input type="file" id="image-input" name="imgs" class="form-control"

                                            style="display: none;">

                                        <label for="image-input" class="custom-file-upload" name="imgs">

                                            Upload Image

                                        </label>

                                    </div>

                                    <div class="col-12 col-sm-12">

                                        <input type="text" name="name" class="form-control bg-light border-0 "

                                            value="<?php echo $row['Aname'] ?>" style="height: 55px;">

                                    </div>

                                    <div class="col-12 col-sm-12">

                                        <input type="email" name="email" class="form-control bg-light border-0 "

                                            value="<?php echo $row['Aemail'] ?>" style="height: 55px;">

                                    </div>

                                    <div class="col-12">

                                        <button class="btn btn-dark w-100 py-3" name="submit" type="submit">Edit

                                            Profile</button>

                                    </div>

                                    <?php

                                }

} ?>

**Delete Cities Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['cid'];

$delete = "DELETE from `cities` where `cid` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$result) {

    die("Query Failed");

} else {

    echo '<script> alert("Your Data Has been Deleted") </script>';

    echo '<script> window.location.href="trashcit.php" </script>';

}

?>

**Delete Patients Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "DELETE from `patient` where `id` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$result) {

    die("Query Failed");

} else {

    echo '<script> alert("Your Data Has been Deleted") </script>';

    echo '<script> window.location.href="trashpat.php" </script>';

}

?>

**Delete Doctors Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "DELETE from `doctors` where `id` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$result) {

    die("Query Failed");

} else {

    echo '<script> alert("Your Data Has been Deleted") </script>';

    echo '<script> window.location.href="trashdoc.php" </script>';

}

?>

**Delete Blogs Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['bid'];

$delete = "DELETE from `blogs` where `bid` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$result) {

    die("Query Failed");

} else {

    echo '<script> alert("Your Data Has been Deleted") </script>';

    echo '<script> window.location.href="trashblogs.php" </script>';

}

?>

**Index**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$fetch = "SELECT \* FROM `patient`";

$cos = mysqli\_query($connection, $fetch);

$num = mysqli\_num\_rows($cos);

$fetch1 = "SELECT \* FROM `doctors`";

$cos1 = mysqli\_query($connection, $fetch1);

$num1 = mysqli\_num\_rows($cos1);

$fetch2 = "SELECT \* FROM `cities`";

$cos2 = mysqli\_query($connection, $fetch2);

$num2 = mysqli\_num\_rows($cos2);

$fetch3 = "SELECT \* FROM `appointment`";

$cos3 = mysqli\_query($connection, $fetch3);

$num3 = mysqli\_num\_rows($cos3);

?>

<div class="container-fluid pt-4 px-4">

                <div class="row g-4">

                    <div class="col-sm-6 col-xl-3">

                        <div class="bg-light rounded d-flex align-items-center justify-content-between p-4">

                            <i class="fa fa-chart-line fa-3x text-primary"></i>

                            <div class="ms-3">

                                <p class="mb-2">Patients</p>

                                <h6 class="mb-0"><?php echo $num ?></h6>

                            </div>

                        </div>

                    </div>

                    <div class="col-sm-6 col-xl-3">

                        <div class="bg-light rounded d-flex align-items-center justify-content-between p-4">

                            <i class="fa fa-chart-bar fa-3x text-primary"></i>

                            <div class="ms-3">

                                <p class="mb-2">Doctors</p>

                                <h6 class="mb-0"><?php echo $num1 ?></h6>

                            </div>

                        </div>

                    </div>

                    <div class="col-sm-6 col-xl-3">

                        <div class="bg-light rounded d-flex align-items-center justify-content-between p-4">

                            <i class="fa fa-chart-area fa-3x text-primary"></i>

                            <div class="ms-3">

                                <p class="mb-2">Cities</p>

                                <h6 class="mb-0"><?php echo $num2 ?></h6>

                            </div>

                        </div>

                    </div>

                    <div class="col-sm-6 col-xl-3">

                        <div class="bg-light rounded d-flex align-items-center justify-content-between p-4">

                            <i class="fa fa-chart-pie fa-3x text-primary"></i>

                            <div class="ms-3">

                                <p class="mb-2">Appointments</p>

                                <h6 class="mb-0"><?php echo $num3 ?></h6>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

            <!-- Sale & Revenue End -->

                            <?php

                    $fetch = "SELECT \* FROM `doctors` AS d INNER JOIN `cities` AS c ON d.`Dcity` = c.`cid` WHERE d.`dstatus` = '1'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                                <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dusername'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Demail'] ?>

                                </td>

                                <td>

                                    <?php echo $row['specialization'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Days'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dtime'] ?>

                                </td>

                                    </tr>

                                    <?php

                        }

                    }

                    ?>

**Admin Logout Controller**

<?php

session\_start();

session\_unset();

session\_destroy();

header('location:signin.php');

?>

**Modify Back Controller**

<?php

include('../includes/config.php');

$id = $\_POST['id'];

$name = $\_POST['Dusername'];

$email = $\_POST['Demail'];

$specialization = $\_POST['specialization'];

$city = $\_POST['Dcity'];

$day = $\_POST['Ddays'];

$time = $\_POST['Dtime'];

// print\_r($\_POST);

// die();

$update = "UPDATE `doctors` SET

`Dusername` = '$name',

`Demail` = '$email',

`specialization` = '$specialization',

`Dcity` = '$city',

`Days` = '$day',

`Dtime` = '$time'

WHERE `id` = '$id'

";

$result = mysqli\_query($connection, $update);

if ($result) {

    echo "<script> alert('Doctor Profile Modify Succesfully') </script>";

    echo "<script> window.location.href='add.php' </script>";

} else {

    die("Query Failed");

}

?>

**Modify Backp Controller**

<?php

include('../includes/config.php');

$id = $\_POST['id'];

$name = $\_POST['name'];

$email = $\_POST['email'];

$phone = $\_POST['phone'];

$update = "UPDATE `patient` SET

`name` = '$name',

`email` = '$email',

`phone` = '$phone'

WHERE `id` = '$id'

";

$result = mysqli\_query($connection, $update);

if ($result) {

    echo "<script> alert('Patient Profile Modify Succesfully') </script>";

    echo "<script> window.location.href='addpatient.php' </script>";

} else {

    die("Query Failed");

}

?>

**Modify Backps Controller**

<?php

include('../includes/config.php');

$id = $\_POST['bid'];

$name = $\_POST['bname'];

$des = $\_POST['bdescription'];

$time = $\_POST['btime'];

$date = $\_POST['bdate'];

$image = $\_FILES['bimage']['name'];

$image\_tmp = $\_FILES['bimage']['tmp\_name'];

$image\_size = $\_FILES['bimage']['size'];

$update = "UPDATE `blogs` SET

`bname` = '$name',

`bdescription` = '$des',

`btime` = '$time',

`bdate` = '$date',

`bimage` = '$image'

WHERE `bid` = '$id'

";

$result = mysqli\_query($connection, $update);

move\_uploaded\_file($image\_tmp, 'blogimg/' . $image);

if ($result) {

    echo "<script> alert('Blog Modify Succesfully') </script>";

    echo "<script> window.location.href='addblog.php' </script>";

} else {

    die("Query Failed");

}

?>

**Modify Backs Controller**

<?php

include('../includes/config.php');

$cid = $\_POST['id'];

$city = $\_POST['city'];

$update = "UPDATE `cities` SET

`Cities` = '$city'

WHERE `cid` = '$cid'

";

$result = mysqli\_query($connection, $update);

if ($result) {

    echo "<script> alert('Cities Modify Succesfully') </script>";

    echo "<script> window.location.href='addcities.php' </script>";

} else {

    die("Query Failed");

}

?>

**Modify Blogs Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$get = $\_GET['bid'];

$fetch = "SELECT \* FROM `blogs` WHERE `bid` = '$get'";

$cons = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($cons) > 0) {

    while ($row = mysqli\_fetch\_assoc($cons)) {

        ?>

        <div class="container mt-2">

            <h2 class="text-center" style="color:#06A3DA;">Modify Blog</h2>

            <form class="row g-3 form-group " method="post" action="modifybackps.php" enctype="multipart/form-data">

                <input type="hidden" name="bid" class="form-control" id="validationDefault01"

                value="<?php echo $row['bid'] ?>">

                <div class="col-md-12">

                    <label for="validationDefault01" class="form-label">Name</label>

                    <input type="text" name="bname" class="form-control" id="validationDefault01" placeholder="Blog Name"

                        value="<?php echo $row['bname'] ?>" required>

                </div>

                <div class="col-md-6">

                    <label for="validationDefault02" class="form-label">Description</label>

                    <input type="text" name="bdescription" class="form-control" id="validationDefault02"

                        placeholder="Description" value="<?php echo $row['bdescription'] ?>" required>

                </div>

                <div class="col-md-6">

                    <label for="validationDefaultUsername" class="form-label">Time</label>

                    <input type="time" name="btime" class="form-control" id="validationDefault02" placeholder="07:35 pm"

                        value="<?php echo $row['btime'] ?>" required>

                </div>

                <div class="col-md-6">

                    <label for="validationDefault04" class="form-label">Date</label>

                    <input type="date" name="bdate" class="form-control" id="validationDefault02" placeholder="23/07/2033"

                        value="<?php echo $row['bdate'] ?>" required>

                </div>

                <div class="col-md-6">

                    <label for="validationDefault03" class="form-label">Image</label>

                    <input type="file" class="form-control" name="bimage" id="validationDefault03" value="<?php echo $row['bimage'] ?>" required>

                </div>

                <div class="col-12">

                    <button class="btn btn-primary" name="submit" type="submit">Modify Blog</button>

                </div>

            </form>

        </div>

        <?php

    }

}

include('../includes/adminfooter.php');

?>

**Modify Cities Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$get = $\_GET['cid'];

$fetch = "SELECT \* FROM `cities` WHERE `cid` = '$get'";

$cons = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($cons) > 0) {

    while ($row = mysqli\_fetch\_assoc($cons)) {

        ?>

        <div class="container mt-5">

            <h2 class="text-center" style="color:#06A3DA;">Cities Modify</h2>

            <form class="row g-3 form-group mt-2" method="post" action="modifybacks.php">

                <div class="col-md-12">

                    <input type="hidden" name="id" class="form-control" id="validationDefault01"

                        value="<?php echo $row['cid'] ?>">

                    <label for="validationDefault01" class="form-label">Cities</label>

                    <input type="text" name="city" class="form-control" id="validationDefault01" required

                        value="<?php echo $row['Cities'] ?>">

                </div>

                <div class="col-12">

                    <button class="btn btn-primary" name="submit" type="submit">Modify form</button>

                </div>

            </form>

        </div>

        <?php

    }

}

include('../includes/adminfooter.php');

?>

**Modify Doctor Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$get = $\_GET['id'];

$fetch = "SELECT \* FROM `doctors` AS D INNER JOIN `cities` AS c ON D.`Dcity` = c.`cid` WHERE d.`id` = '$get'";

$cons = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($cons) > 0) {

    while ($row = mysqli\_fetch\_assoc($cons)) {

        ?>

        <div class="container mt-5">

            <h2 class="text-center" style="color:#06A3DA;">Doctors Modify</h2>

            <form class="row g-3 form-group mt-2" method="post" action="modifyback.php">

                <div class="col-md-12">

                    <input type="hidden" name="id" class="form-control" id="validationDefault01"

                        value="<?php echo $row['id'] ?>">

                    <label for="validationDefault01" class="form-label">Name</label>

                    <input type="text" name="Dusername" class="form-control" id="validationDefault01" required

                        value="<?php echo $row['Dusername'] ?>">

                </div>

                <div class="col-md-12">

                    <label for="validationDefault02" class="form-label">Email</label>

                    <input type="email" name="Demail" class="form-control" id="validationDefault02" required

                        value="<?php echo $row['Demail'] ?>">

                </div>

                <div class="col-md-6">

                    <label for="validationDefault04" class="form-label">Specialization</label>

                    <select class="form-select" name="specialization" id="validationDefault04" required>

                        <option selected value="<?php echo $row['specialization'] ?>">

                            <?php echo $row['specialization'] ?>

                        </option>

                        <option>Neuro Sergon</option>

                        <option>Gynecologist</option>

                        <option>General physician</option>

                        <option>Dermatologist</option>

                        <option>Pediatrician</option>

                        <option>Radiologist</option>

                        <option>Dentist</option>

                        <option>Cardiologist</option>

                    </select>

                </div>

                <div class="col-md-6">

                    <label for="validationDefault03" class="form-label">City</label>

                    <select class="form-select" name="Dcity" id="validationDefault04" required>

                        <option selected value="<?php echo $row['cid'] ?>">

                            <?php echo $row['Cities'] ?>

                        </option>

                        <?php

                        $fetchcity = "SELECT \* FROM `cities`";

                        $fetchcities = mysqli\_query($connection, $fetchcity);

                        if (mysqli\_num\_rows($fetchcities) > 0) {

                            while ($rows = mysqli\_fetch\_assoc($fetchcities)) {

                                ?>

                                <option value="<?php echo $rows['cid'] ?>">

                                    <?php echo $rows['Cities'] ?>

                                </option>

                                <?php

                            }

                        }

                        ?>

                    </select>

                </div>

                <div class="col-md-6">

                    <label for="validationDefault03" class="form-label">Days</label>

                    <input type="text" class="form-control" name="Ddays" id="validationDefault03" required

                        value="<?php echo $row['Days'] ?>">

                </div>

                <div class="col-md-6">

                    <label for="validationDefault03" class="form-label">Timimg</label>

                    <input type="text" class="form-control" name="Dtime" id="validationDefault03" required

                        value="<?php echo $row['Dtime'] ?>">

                </div>

                <div class="col-12">

                    <button class="btn btn-primary" name="submit" type="submit">Modify form</button>

                </div>

            </form>

        </div>

        <?php

    }

}

include('../includes/adminfooter.php');

?>

**Modify Patients Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

$get = $\_GET['id'];

$fetch = "SELECT \* FROM `patient` WHERE `id` = '$get'";

$cons = mysqli\_query($connection, $fetch);

if (mysqli\_num\_rows($cons) > 0) {

    while ($row = mysqli\_fetch\_assoc($cons)) {

        ?>

        <div class="container mt-5">

            <h2 class="text-center" style="color:#06A3DA;">Patient Modify</h2>

            <form class="row g-3 form-group mt-2" method="post" action="modifybackp.php">

                <div class="col-md-12">

                    <input type="hidden" name="id" class="form-control" id="validationDefault01"

                        value="<?php echo $row['id'] ?>">

                    <label for="validationDefault01" class="form-label">Name</label>

                    <input type="text" name="name" class="form-control" id="validationDefault01" required

                        value="<?php echo $row['name'] ?>">

                </div>

                <div class="col-md-6">

                    <label for="validationDefault02" class="form-label">Email</label>

                    <input type="email" name="email" class="form-control" id="validationDefault02" required

                        value="<?php echo $row['email'] ?>">

                </div>

                <div class="col-md-6">

                    <label for="validationDefault03" class="form-label">Phone</label>

                    <input type="text" class="form-control" name="phone" id="validationDefault03" required

                        value="<?php echo $row['phone'] ?>">

                </div>

                <div class="col-12">

                    <button class="btn btn-primary" name="submit" type="submit">Modify form</button>

                </div>

            </form>

        </div>

        <?php

    }

}

include('../includes/adminfooter.php');

?>

**Restore Blogs Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['bid'];

$delete = "UPDATE `blogs` SET `bstatus` = '1' where `bid` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been Restore") </script>';

    echo '<script> window.location.href="trashblogs.php" </script>';

}

?>

**Restore Cities Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['cid'];

$delete = "UPDATE `cities` SET `Cstatus` = '1' where `cid` = $user\_id";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been Restore") </script>';

    echo '<script> window.location.href="trashcit.php" </script>';

}

?>

**Restore Doctors Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "UPDATE `doctors` SET `dstatus` = '1' where `id` = $user\_id";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been Restore") </script>';

    echo '<script> window.location.href="trashdoc.php" </script>';

}

?>

**Restore Patients Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "UPDATE `patient` SET `pstatus` = '1' where `id` = $user\_id";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been Restore") </script>';

    echo '<script> window.location.href="trashpat.php" </script>';

}

?>

**Admin Signin Controller**

<?php

include('../includes/adminheader1.php');

include('../includes/config.php');

if (isset($\_POST['Login'])) {

  $Email = $\_POST['L\_email'];

  $Password = $\_POST['L\_Pass'];

  $login\_query = "SELECT \* from `admin` where Aemail = '$Email'";

  $get\_from\_db = mysqli\_query($connection, $login\_query);

  if (mysqli\_num\_rows($get\_from\_db)) {

    $row = mysqli\_fetch\_assoc($get\_from\_db);

    $db\_pass = $row['Apassword'];

    $pass\_decode = password\_verify($Password, $db\_pass);

    if ($pass\_decode) {

      $\_SESSION['admin'] = $row['Aemail'];

      echo "<script> alert('login secsesfully')

        window.location.href='index.php'

        </script>";

    } else {

      echo "<script> alert('Invalid Password')</script>";

    }

  } else {

    echo "<script> alert('Invalid Email')</script>";

  }

}

?>

**Admin Signup Controller**

  } else {

    // User ka email address $user\_email variable mein store karein

    $user\_email = $email;

    // PHPMailer configuration

    $mail = new PHPMailer(true);

    try {

      // Server settings

      $mail->isSMTP();

      $mail->Host = 'smtp.gmail.com'; // SMTP server

      $mail->SMTPAuth = true;

      $mail->Username = 'ifrakhan2804@gmail.com'; // Sender's email address

      $mail->Password = 'wwuq dupp rnbo tcww';

      $mail->SMTPSecure = PHPMailer::ENCRYPTION\_STARTTLS; // TLS encryption

      $mail->Port = 587; // Port for TLS

      // Recipient settings

      $mail->setFrom('ifrakhan2804@gmail.com', 'Ifra');

      $mail->addAddress($user\_email, $name); // User ka email address

      // Email content

      $mail->isHTML(true);

      $mail->Subject = 'Welcome to Our Website';

      $mail->Body = 'Thank you for registering on our website.';

      $mail->send();

    } catch (Exception $e) {

      echo "Message could not be sent. Mailer Error: {$mail->ErrorInfo}";

    }

    $insert = "INSERT INTO `admin` (`Aname`, `Aemail`, `Apassword`) VALUES ('$name', '$email','$hashPass')";

    $connect\_insert = mysqli\_query($connection, $insert);

  }

  header("location:signin.php");

}

?>

**Trash Blog Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['bid'];

$delete = "UPDATE `blogs` SET `bstatus` = '0' where `bid` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been move to Trash") </script>';

    echo '<script> window.location.href="trashblogs.php" </script>';

}

?>

**Trash Blogs Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

?>

                <tbody>

                    <?php

                    $fetch = "SELECT \* FROM `Blogs` WHERE `bstatus` = '0'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['bid'] ?>

                                </td>

                                <td>

                                    <?php echo $row['bname'] ?>

                                </td>

                                <td>

                                    <?php echo $row['bdescription'] ?>

                                </td>

                                <td>

                                    <?php echo $row['btime'] ?>

                                </td>

                                <td>

                                    <?php echo $row['bdate'] ?>

                                </td>

                                <td>

                                    <img src="<?php echo 'blogimg/' . $row['bimage'] ?>" alt="blog Image" height="40px"

                                        width="40px">

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-success"

                                        href="restoreblog.php?bid=<?php echo $row['bid'] ?>">Restore</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="deleteblog.php?bid=<?php echo $row['bid'] ?>">Delete</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

                </tbody>

            </table>

        </div>

</div>

</div>

<?php

include('../includes/adminfooter.php');

?>

**Trash City Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

?>

<div class="container-fluid pt-4">

    <div class="bg-light text-center rounded p-4">

        <div class="d-flex align-items-center justify-content-between mb-4">

            <h6 class="mb-0">Cities</h6>

        </div>

        <div class="table-responsive">

            <table id="example"

                class="table mt-3 text-center align-middle table-bordered table-striped table-hover mb-0">

                <thead>

                    <tr class="text-dark">

                        <th scope="col">Id</th>

                        <th scope="col">Cities</th>

                        <th scope="col">Action</th>

                    </tr>

                </thead>

                <tbody>

                    <?php

                    $fetch = "SELECT \* FROM `cities` WHERE `Cstatus` = '0'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['cid'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-success"

                                        href="restorecit.php?cid=<?php echo $row['cid'] ?>">Restore</a>

                                    <a class="btn btn-sm btn-danger" href="delete.php?cid=<?php echo $row['cid'] ?>">Delete</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

                </tbody>

</table>

        </div>

    </div>

</div>

<?php

include('../includes/adminfooter.php');

?>

**Trash Cities Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['cid'];

$delete = "UPDATE `cities` SET `Cstatus` = '0' where `cid` = '$user\_id'";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been move to Trash") </script>';

    echo '<script> window.location.href="trashcit.php" </script>';

}

?>

**Trash Doctor Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

?>

<div class="container-fluid pt-4">

    <div class="bg-light text-center rounded p-4">

        <div class="d-flex align-items-center justify-content-between mb-4">

            <h6 class="mb-0">Doctors</h6>

        </div>

        <div class="table-responsive">

            <table id="example"

                class="table mt-3 text-center align-middle table-bordered table-striped table-hover mb-0">

                <thead>

                    <tr class="text-dark">

                        <th scope="col">Id</th>

                        <th scope="col">Name</th>

                        <th scope="col">Email</th>

                        <th scope="col">Specialization</th>

                        <th scope="col">Cities</th>

                        <th scope="col">Days</th>

                        <th scope="col">Time</th>

                        <th scope="col">Action</th>

                    </tr>

                </thead>

                <tbody>

<?php

                    $fetch = "SELECT \* FROM `doctors` AS d INNER JOIN `cities` AS c ON d.`Dcity` = c.`cid` WHERE d.`dstatus` = '0'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dusername'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Demail'] ?>

                                </td>

                                <td>

                                    <?php echo $row['specialization'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Cities'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Days'] ?>

                                </td>

                                <td>

                                    <?php echo $row['Dtime'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-success"

                                        href="restoredoc.php?id=<?php echo $row['id'] ?>">Restore</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="delete2.php?id=<?php echo $row['id'] ?>">Delete</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

                </tbody>

            </table>

        </div>

    </div>

</div>

<?php

include('../includes/adminfooter.php');

?>

**Trash Doctors Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "UPDATE `doctors` SET `dstatus` = '0' where `id` = $user\_id";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been move to Trash") </script>';

    echo '<script> window.location.href="trashdoc.php" </script>';

}

?>

**Trash patient Controller**

<?php

                    $fetch = "SELECT \* FROM `patient` WHERE `pstatus` = '0'";

                    $fetch2 = mysqli\_query($connection, $fetch);

                    if (mysqli\_num\_rows($fetch2) > 0) {

                        while ($row = mysqli\_fetch\_assoc($fetch2)) {

                            ?>

                            <tr>

                                <td>

                                    <?php echo $row['id'] ?>

                                </td>

                                <td>

                                    <?php echo $row['name'] ?>

                                </td>

                                <td>

                                    <?php echo $row['email'] ?>

                                </td>

                                <td>

                                    <?php echo $row['phone'] ?>

                                </td>

                                <td>

                                    <a class="btn btn-sm btn-success"

                                        href="restorepat.php?id=<?php echo $row['id'] ?>">Restore</a>

                                    <a class="btn btn-sm btn-danger"

                                        href="delete1.php?id=<?php echo $row['id'] ?>">Delete</a>

                                </td>

                            </tr>

                            <?php

                        }

                    }

                    ?>

**Trash patient Controller**

<?php

include('../Includes/config.php');

$user\_id = $\_GET['id'];

$delete = "UPDATE `patient` SET `pstatus` = '0' where `id` = $user\_id";

$result = mysqli\_query($connection, $delete);

if (!$delete) {

    die("Query Failed");

} else {

    echo '<script> alert("Your data has been move to Trash") </script>';

    echo '<script> window.location.href="trashpat.php" </script>';

}

?>

**Update Password Controller**

<?php

include('../includes/adminheader.php');

include('../includes/config.php');

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

    $currentPassword = $\_POST["current\_password"];

    $newPassword = $\_POST["new\_password"];

    $confirmPassword = $\_POST["confirm\_password"];

    $username = $\_SESSION["admin"];

    $query = "SELECT `Apassword` FROM `admin` WHERE `Aemail` = '$username'";

    $result = $connection->query($query);

    if (mysqli\_num\_rows($result) > 0) {

        $row = $result->fetch\_assoc();

        $dbPassword = $row["Apassword"];

        if (password\_verify($currentPassword, $dbPassword)) {

            if ($newPassword == $confirmPassword) {

                $hashedPassword = password\_hash($newPassword, PASSWORD\_DEFAULT);

                $updateQuery = "UPDATE `admin` SET `Apassword` = '$hashedPassword' WHERE `Aemail` = '$username'";

                if ($connection->query($updateQuery) === TRUE) {

                    echo ' <script>

                    document.getElementById("dose1Alert").style.display = "block";

                    </script>';

                } else {

                    echo ' <script>

                    document.getElementById("dose2Alert").style.display = "block";

                    </script>';

                }

            } else {

                echo ' <script>

                    document.getElementById("dose3Alert").style.display = "block";

                    </script>';

            }

        } else {

            echo ' <script>

                    document.getElementById("dose4Alert").style.display = "block";

                    </script>';

        }

    } else {

        echo ' <script>

                    document.getElementById("dose5Alert").style.display = "block";

                    </script>';

    }

}

?>

**Update Profile Controller**

<?php

require("../Includes/config.php");

session\_start();

if (!isset($\_SESSION["admin"])) {

    echo '<script> window.location.href="login.php"</script>';

    exit();

}

$user\_id = $\_POST['id'];

$img = $\_FILES['imgs']['name'];

$img\_tmp = $\_FILES['imgs']['tmp\_name'];

$img\_size = $\_FILES['imgs']['size'];

$user\_name = mysqli\_real\_escape\_string($connection, $\_POST['name']);

$user\_email = mysqli\_real\_escape\_string($connection, $\_POST['email']);

$username = $\_SESSION["admin"]; // Assuming that "hospital" is the session variable where the username is stored

// Update query with correct column names

$updateQuery = "UPDATE `admin` SET `Aname` = '$user\_name', `Aemail` = '$user\_email', `AImage` = '$img' WHERE `Aemail` = '$username'";

if (move\_uploaded\_file($img\_tmp, 'adminimg/' . $img)) {

    $res = mysqli\_query($connection, $updateQuery);

    if (!$res) {

        die("Query failed");

    } else {

        echo "

        <script>alert('Profile Has Been Updated Successfully')

</script>";

        echo "<script>window.location.href='admin\_pro.php'</script>";

    }

} else {

    echo "

    <script>alert('Profile Update failed Successfully')

    </script>";

}

?>