```php
<?php
/* Practical-10: Write a PHP script to implement “Forget Password” functionality.

Name: Angat Shah
Enrollment No: 202203103510097
Branch: B.Tech Computer Science and Engineering */

session_start();
$error = array();
require "mail.php";
 if(!$con = mysqli_connect("localhost","root","","forgot_db")){

   die("could not connect");
 }
 $mode = "enter_email";
 if(isset($_GET['mode'])){
   $mode = $_GET['mode'];
 }
 //something is posted
 if(count($_POST) > 0){

   switch ($mode) {
     case 'enter_email':
       // code...
       $email = $_POST['email'];
       //validate email
       if(!filter_var($email,FILTER_VALIDATE_EMAIL)){
         $error[] = "Please enter a valid email";
       }elseif(!valid_email($email)){
         $error[] = "That email was not found";
       }else{

         $_SESSION['forgot']['email'] = $email;
         send_email($email);
         header("Location: forgot.php?mode=enter_code");
         die;
       }
       break;
     case 'enter_code':
       // code...
       $code = $_POST['code'];
       $result = is_code_correct($code);

       if($result == "the code is correct"){

         $_SESSION['forgot']['code'] = $code;
         header("Location: forgot.php?mode=enter_password");
         die;
       }else{
         $error[] = $result;
       }
       break;
     case 'enter_password':
       // code...
       $password = $_POST['password'];
       $password2 = $_POST['password2'];

       if($password !== $password2){
```

```
        $error[] = "Passwords do not match";
      }elseif(!isset($_SESSION['forgot']['email']) || !isset($_SESSION['forgot']['code'])){
        header("Location: forgot.php");
        die;
      }else{
        save_password($password);
        if(isset($_SESSION['forgot'])){
          unset($_SESSION['forgot']);
        }

        header("Location: login.php");
        die;
      }
      break;

    default:
      // code...
      break;
  }
}
function send_email($email){
  global $con;
  $expire = time() + (60 * 1);
  $code = rand(10000,99999);
  $email = addslashes($email);
  $query = "insert into codes (email,code,expire) value ('$email','$code','$expire')";
  mysqli_query($con,$query);
  //send email here
  send_mail($email,'Password reset',"Your code is " . $code);
}
function save_password($password){
  global $con;
  $password = password_hash($password, PASSWORD_DEFAULT);
  $email = addslashes($_SESSION['forgot']['email']);
  $query = "update users set password = '$password' where email = '$email' limit 1";
  mysqli_query($con,$query);
}
function valid_email($email){
  global $con;
  $email = addslashes($email);
  $query = "select * from users where email = '$email' limit 1";
  $result = mysqli_query($con,$query);
  if($result){
    if(mysqli_num_rows($result) > 0)
    {
      return true;
    }
  }
  return false;
}
function is_code_correct($code){
  global $con;
  $code = addslashes($code);
  $expire = time();
  $email = addslashes($_SESSION['forgot']['email']);
  $query = "select * from codes where code = '$code' && email = '$email' order by id desc limit 1";
  $result = mysqli_query($con,$query);
  if($result){
    if(mysqli_num_rows($result) > 0)
```

```
    {
      $row = mysqli_fetch_assoc($result);
      if($row['expire'] > $expire){

        return "the code is correct";
      }else{
        return "the code is expired";
      }
    }else{
      return "the code is incorrect";
    }
   return "the code is incorrect";
  }
?>
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <title>Forgot</title>
</head>
<body>
<style type="text/css">

  *{
    font-family: tahoma;
    font-size: 13px;
  }

  form{
    width: 100%;
    max-width: 200px;
    margin: auto;
    border: solid thin #ccc;
    padding: 10px;
  }

  .textbox{
    padding: 5px;
    width: 180px;
  }
</style>

    <?php

      switch ($mode) {
        case 'enter_email':
          // code...
          ?>
            <form method="post" action="forgot.php?mode=enter_email">
              <h1>Forgot Password</h1>
              <h3>Enter your email below</h3>
              <span style="font-size: 12px;color:red;">
              <?php
                foreach ($error as $err) {
                  // code...
                  echo $err . "<br>";
                }
```

```
        ?>
        </span>
        <input class="textbox" type="email" name="email" placeholder="Email"><br><br>
        <br style="clear: both;">
        <input type="submit" value="Next">
        <br><br>
        <div><a href="login.php">Login</a></div>
      </form>
    <?php
    break;

  case 'enter_code':
    // code...
    ?>
      <form method="post" action="forgot.php?mode=enter_code">
        <h1>Forgot Password</h1>
        <h3>Enter your the code sent to your email</h3>
        <span style="font-size: 12px;color:red;">
        <?php
          foreach ($error as $err) {
            // code...
            echo $err . "<br>";
          }
        ?>
        </span>

        <input class="textbox" type="text" name="code" placeholder="12345"><br><br>
        <br style="clear: both;">
        <input type="submit" value="Next" style="float: right;">
        <a href="forgot.php">
          <input type="button" value="Start Over">
        </a>
        <br><br>
        <div><a href="login.php">Login</a></div>
      </form>
    <?php
    break;

  case 'enter_password':
    // code...
    ?>
      <form method="post" action="forgot.php?mode=enter_password">
        <h1>Forgot Password</h1>
        <h3>Enter your new password</h3>
        <span style="font-size: 12px;color:red;">
        <?php
          foreach ($error as $err) {
            // code...
            echo $err . "<br>";
          }
        ?>
        </span>

        <input class="textbox" type="text" name="password" placeholder="Password"><br><br>
        <input class="textbox" type="text" name="password2" placeholder="Retype Password"><br>
        <br style="clear: both;">
        <input type="submit" value="Next" style="float: right;">
        <a href="forgot.php">
          <input type="button" value="Start Over">
```

```
            </a>
            <br><br>
            <div><a href="login.php">Login</a></div>
          </form>
        <?php
        break;

      default:
        // code...
        break;
    }
  ?>
</body>
</html>

// practical10_2.php
<?php

 if(!$con = mysqli_connect("localhost","root","","forgot_db")){

   die("could not connect");
 }
/*  $password = password_hash('password', PASSWORD_DEFAULT);
 $query = "update users set password = '$password' ";
 mysqli_query($con,$query);
*/
?>
<!DOCTYPE html>
<html>
<head>
 <meta charset="utf-8">
 <title>Home</title>
</head>
<body>
<h1>Home Page</h1>
</body>
</html>

// practical10_3.php
<!DOCTYPE html>
<html>
<head>
   <meta charset="utf-8">
   <title>Login</title>
</head>
<body>
   <form    method="post">
   <h1>Login</h1>
   <input type="email" name="email" placeholder="Email"><br><br>
   <input type="text" name="password" placeholder="Password"><br>
   <br style="clear: both;">
   <input type="submit" value="Login">
   <br><br>
   <div><a href="forgot.php">Forgot password?</a></div> </form>
</body>
</html>

// practical10_4.php
```

```php
<?php
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\Exception;
require 'PHPMailer-master/src/Exception.php';
require 'PHPMailer-master/src/PHPMailer.php';
require 'PHPMailer-master/src/SMTP.php';
function    send_mail($recipient,$subject,$message)
{
    $mail = new    PHPMailer();
    $mail->IsSMTP();
    $mail->SMTPDebug  = 0;
    $mail->SMTPAuth   = TRUE;
    $mail->SMTPSecure = "tls";
    $mail->Port       = 587;
    $mail->Host       = "smtp.gmail.com";
    $mail->Username   = "phptest041@gmail.com";
    $mail->Password   = "bpcz uyjn zvuq fwzy";
    $mail->IsHTML(true);
    $mail->AddAddress($recipient, "esteemed customer"); $mail->SetFrom("phptest041@gmail.com", "My website");
    $content = $message;
    $mail->MsgHTML($content);
    if(!$mail->Send()) {
        return false;
    } else {
        return True;
    }
}
?>
```