

```

1 <?php
2 /* Practical-10: Write a PHP script to implement "Forget Password" functionality.
3
4 Name: Angat Shah
5 Enrollment No: 202203103510097
6 Branch: B.Tech Computer Science and Engineering */
7
8 session_start();
9 $error = array();
10 require "mail.php";
11 if(!$con = mysqli_connect("localhost","root","","forgot_db")){
12
13     die("could not connect");
14 }
15 $mode = "enter_email";
16 if(isset($_GET['mode'])){
17     $mode = $_GET['mode'];
18 }
19 //something is posted
20 if(count($_POST) > 0){
21
22     switch ($mode) {
23         case 'enter_email':
24             // code...
25             $email = $_POST['email'];
26             //validate email
27             if(!filter_var($email,FILTER_VALIDATE_EMAIL)){
28                 $error[] = "Please enter a valid email";
29             }elseif(!valid_email($email)){
30                 $error[] = "That email was not found";
31             }else{
32
33                 $_SESSION['forgot']['email'] = $email;
34                 send_email($email);
35                 header("Location: forgot.php?mode=enter_code");
36                 die;
37             }
38             break;
39         case 'enter_code':
40             // code...
41             $code = $_POST['code'];
42             $result = is_code_correct($code);
43
44             if($result == "the code is correct"){
45
46                 $_SESSION['forgot']['code'] = $code;
47                 header("Location: forgot.php?mode=enter_password");
48                 die;
49             }else{
50                 $error[] = $result;
51             }
52             break;
53         case 'enter_password':
54             // code...
55             $password = $_POST['password'];
56             $password2 = $_POST['password2'];
57
58             if($password != $password2){

```

```

59     $error[] = "Passwords do not match";
60 }elseif(!isset($_SESSION['forgot']['email']) || !isset($_SESSION['forgot']['code'])){
61     header("Location: forgot.php");
62     die;
63 }else{
64     save_password($password);
65     if(isset($_SESSION['forgot'])){
66         unset($_SESSION['forgot']);
67     }
68
69     header("Location: login.php");
70     die;
71 }
72 break;
73
74 default:
75     // code...
76     break;
77 }
78 }
79 function send_email($email){
80     global $con;
81     $expire = time() + (60 * 1);
82     $code = rand(10000,99999);
83     $email = addslashes($email);
84     $query = "insert into codes (email,code,expire) value ('$email','$code','$expire)";
85     mysqli_query($con,$query);
86     //send email here
87     send_mail($email,'Password reset',"Your code is " . $code);
88 }
89 function save_password($password){
90     global $con;
91     $password = password_hash($password, PASSWORD_DEFAULT);
92     $email = addslashes($_SESSION['forgot']['email']);
93     $query = "update users set password = '$password' where email = '$email' limit 1";
94     mysqli_query($con,$query);
95 }
96 function valid_email($email){
97     global $con;
98     $email = addslashes($email);
99     $query = "select * from users where email = '$email' limit 1";
100    $result = mysqli_query($con,$query);
101    if($result){
102        if(mysqli_num_rows($result) > 0)
103        {
104            return true;
105        }
106    }
107    return false;
108 }
109 function is_code_correct($code){
110     global $con;
111     $code = addslashes($code);
112     $expire = time();
113     $email = addslashes($_SESSION['forgot']['email']);
114     $query = "select * from codes where code = '$code' && email = '$email' order by id desc limit 1";
115     $result = mysqli_query($con,$query);
116     if($result){
117         if(mysqli_num_rows($result) > 0)

```

```

118 {
119     $row = mysqli_fetch_assoc($result);
120     if($row['expire'] > $expire){
121
122         return "the code is correct";
123     }else{
124         return "the code is expired";
125     }
126 }else{
127     return "the code is incorrect";
128 }
129 }
130 return "the code is incorrect";
131 }
132 ?>
133 <!DOCTYPE html>
134 <html>
135 <head>
136     <meta charset="utf-8">
137     <title>Forgot</title>
138 </head>
139 <body>
140 <style type="text/css">
141
142     *{
143         font-family: tahoma;
144         font-size: 13px;
145     }
146
147     form{
148         width: 100%;
149         max-width: 200px;
150         margin: auto;
151         border: solid thin #ccc;
152         padding: 10px;
153     }
154
155     .textbox{
156         padding: 5px;
157         width: 180px;
158     }
159 </style>
160
161 <?php
162
163     switch ($mode) {
164         case 'enter_email':
165             // code...
166             ?>
167             <form method="post" action="forgot.php?mode=enter_email">
168                 <h1>Forgot Password</h1>
169                 <h3>Enter your email below</h3>
170                 <span style="font-size: 12px;color:red;">
171                 <?php
172                     foreach ($error as $err) {
173                         // code...
174                         echo $err . "<br>";
175                     }

```

```

176     />
177 </span>
178 <input class="textbox" type="email" name="email" placeholder="Email"><br><br>
179 <br style="clear: both;">
180 <input type="submit" value="Next">
181 <br><br>
182 <div><a href="login.php">Login</a></div>
183 </form>
184 <?php
185 break;
186
187 case 'enter_code':
188     // code...
189     ?>
190     <form method="post" action="forgot.php?mode=enter_code">
191         <h1>Forgot Password</h1>
192         <h3>Enter your the code sent to your email</h3>
193         <span style="font-size: 12px;color:red;">
194             <?php
195                 foreach ($error as $err) {
196                     // code...
197                     echo $err . "<br>";
198                 }
199             ?>
200         </span>
201
202         <input class="textbox" type="text" name="code" placeholder="12345"><br><br>
203         <br style="clear: both;">
204         <input type="submit" value="Next" style="float: right;">
205         <a href="forgot.php">
206             <input type="button" value="Start Over">
207         </a>
208         <br><br>
209         <div><a href="login.php">Login</a></div>
210     </form>
211 <?php
212 break;
213
214 case 'enter_password':
215     // code...
216     ?>
217     <form method="post" action="forgot.php?mode=enter_password">
218         <h1>Forgot Password</h1>
219         <h3>Enter your new password</h3>
220         <span style="font-size: 12px;color:red;">
221             <?php
222                 foreach ($error as $err) {
223                     // code...
224                     echo $err . "<br>";
225                 }
226             ?>
227         </span>
228
229         <input class="textbox" type="text" name="password" placeholder="Password"><br><br>
230         <input class="textbox" type="text" name="password2" placeholder="Retype Password"><br>
231         <br style="clear: both;">
232         <input type="submit" value="Next" style="float: right;">
233         <a href="forgot.php">
234             <input type="button" value="Start Over">

```

```

235     </a>
236     <br><br>
237     <div><a href="login.php">Login</a></div>
238 </form>
239 <?php
240     break;
241
242     default:
243         // code...
244         break;
245     }
246     ?>
247 </body>
248 </html>
249
250 // practical10_2.php
251 <?php
252
253 if(!$con = mysqli_connect("localhost","root","","forgot_db")){
254
255     die("could not connect");
256 }
257 /* $password = password_hash('password', PASSWORD_DEFAULT);
258 $query = "update users set password = '$password' ";
259 mysqli_query($con,$query);
260 */
261 ?>
262 <!DOCTYPE html>
263 <html>
264 <head>
265     <meta charset="utf-8">
266     <title>Home</title>
267 </head>
268 <body>
269 <h1>Home Page</h1>
270 </body>
271 </html>
272
273 // practical10_3.php
274 <!DOCTYPE html>
275 <html>
276 <head>
277     <meta charset="utf-8">
278     <title>Login</title>
279 </head>
280 <body>
281     <form method="post">
282     <h1>Login</h1>
283     <input type="email" name="email" placeholder="Email"><br><br>
284     <input type="text" name="password" placeholder="Password"><br>
285     <br style="clear: both;">
286     <input type="submit" value="Login">
287     <br><br>
288     <div><a href="forgot.php">Forgot password?</a></div> </form>
289 </body>
290 </html>
291
292 // practical10_4.php

```

```
293 <?php
294 use PHPMailer\PHPMailer\PHPMailer;
295 use PHPMailer\PHPMailer\Exception;
296 require 'PHPMailer-master/src/Exception.php';
297 require 'PHPMailer-master/src/PHPMailer.php';
298 require 'PHPMailer-master/src/SMTP.php';
299 function send_mail($recipient,$subject,$message)
300 {
301     $mail = new PHPMailer();
302     $mail->IsSMTP();
303     $mail->SMTPDebug = 0;
304     $mail->SMTPAuth = TRUE;
305     $mail->SMTPSecure = "tls";
306     $mail->Port = 587;
307     $mail->Host = "smtp.gmail.com";
308     $mail->Username = "phptest041@gmail.com";
309     $mail->Password = "bpcz uyjn zvuq fwzy";
310     $mail->IsHTML(true);
311     $mail->AddAddress($recipient, "esteemed customer"); $mail->SetFrom("phptest041@gmail.com", "My
website");
312     $content = $message;
313     $mail->MsgHTML($content);
314     if(!$mail->Send()) {
315         return false;
316     } else {
317         return True;
318     }
319 }
320 ?>
```