

```

1  <?php
2      $allFieldsEntered=true;
3      session_start();
4      if(array_key_exists("logout", $_GET))
5      {
6          unset($_SESSION);
7          setcookie("id", "", time() - 60*60);
8          $_COOKIE["id"]="";
9      }
10     else if((array_key_exists("id", $_SESSION) AND $_SESSION['id']) OR
11             (array_key_exists("id", $_COOKIE) AND $_COOKIE['id']))
12     {
13         header("Location: diary.php");
14     }
15     //check if at least one has been entered
16     if(array_key_exists('emailSU', $_POST) OR array_key_exists('passwordSU', $_POST)
17         OR array_key_exists('emailLI', $_POST) OR array_key_exists('passwordLI', $_POST))
18     {
19         if($_POST['signUp']=='0')
20         {
21             $emailLI="";
22             $_POST["emailLI"]="";
23
24             if(!$_POST['emailSU'])
25             {
26                 echo "<p>Email was not entered</p>";
27                 $allFieldsEntered=false;
28             }
29
30             if(!$_POST['passwordSU'])
31             {
32                 echo "<p>Password was not entered</p>";
33                 $allFieldsEntered=false;
34             }
35
36             if($allFieldsEntered)
37             {
38                 $conn = mysqli_connect(XXX);
39                 if(!$conn)
40                 {
41                     die("<p>Error encountered while connecting to the database</p>");
42                 }
43
44                 $query = "SELECT email FROM diaryUsers WHERE
45                           email='".mysqli_real_escape_string($conn, $_POST['emailSU'])."'
46                           LIMIT 1";
47                 if($result = mysqli_query($conn, $query))
48                 {
49                     if(mysqli_num_rows($result) > 0)
50                     {
51                         echo "<p>Email already taken.</p>";
52                     }
53                     else
54                     {
55                         $query="INSERT INTO diaryUsers (email,password,diary) VALUES
56                               ('"
57                               .mysqli_real_escape_string($conn, $_POST['emailSU'])."', '"
58                               .mysqli_real_escape_string($conn, $_POST['passwordSU'])."', '"
59                               if(mysqli_query($conn, $query))
60                               {
61                                   $id=mysqli_insert_id($conn);
62
63                                   $_session['id']=mysqli_insert_id($conn);
64
65                                   $query = "UPDATE diaryUsers SET password =
66                                             '"
67                                             .md5(md5(mysqli_insert_id($conn)).$_POST["passwordSU
68                                             "))."'
69                                             WHERE id='".mysqli_insert_id($conn)."' LIMIT 1"; //most
69                                             recently received ID from INSERT query
70                                   mysqli_query($conn, $query);
71                                   if($_POST['CBSU'] == '1')
72                                   {

```

```

63
64         $cookieName = "id";
65         $cookieValue = $id;
66         setcookie($cookieName,$cookieValue, time() +
            (60*60*24*365));
67     }
68     header("location: diary.php");
69 }
70 else
71 {
72     echo "<p>Could not update database.</p>";
73 }
74 }
75 }
76 }
77 }
78
79
80 if($_POST['signUp']=='1')
81 {
82     $emailSU="";
83     $_POST["emailSU"]="";
84
85     if(!$_POST['emailLI'])
86     {
87         echo "</p>Email was not entered</p>";
88         $allFieldsEntered=false;
89     }
90
91     if(!$_POST['passwordLI'])
92     {
93         echo "<p>Password was not entered</p>";
94         $allFieldsEntered=false;
95     }
96
97     if($allFieldsEntered)
98     {
99         $conn = mysqli_connect(xxx);
100        if(!$conn)
101        {
102            die("<p>could not connect to the database</p>");
103        }
104        $query="SELECT * FROM diaryUsers WHERE email='".
105        mysqli_real_escape_string($conn,$_POST["emailLI"])."' LIMIT 1";
106        if($result=mysqli_query($conn, $query))
107        {
108            $row=mysqli_fetch_array($result);
109            if( $row[password]==md5(md5($row['id']).$_POST["passwordLI"]))
110            {
111                $_SESSION['id']=$row['id'];
112                if($_POST['CBLI']=='1')
113                {
114                    $cookieName = "id";
115                    $cookieValue = $row['id'];
116                    setcookie($cookieName,$cookieValue, time() +
                        (60*60*24*365));
117                }
118                header("location: diary.php");
119            }
120            else
121            {
122                echo "<p>Wrong username/password, try again!</p>";
123            }
124        }
125        else
126        {
127            echo "<p>Query Error!</p>".$query;
128        }
129    }
130 }
131 }
132

```

```

133     ?>
134
135     <!--<form method="post">
136         <p>
137             <input type="email" name="emailSU" id="emailSU" placeholder="Your Email"
138                 value="<? echo htmlentities($emailLI); ?>">
139             <input type="password" name="passwordSU" id="passwordSU"
140                 placeholder="Password">
141             <input type="checkbox" name="CBSU" id="CBSU" value="1">
142             <input type="hidden" name="signUp" id="signUp" value="0">
143             <button type="submit" name="submitSU" id="submitSU">Sign Up!</button>
144         </p>
145     </form>
146
147     <form method="post">
148         <p>
149             <input type="email" name="emailLI" id="emailLI" placeholder="Your Email"
150                 value="<? echo htmlentities($emailSU); ?>">
151             <input type="password" name="passwordLI" id="passwordLI"
152                 placeholder="Password">
153             <input type="checkbox" name="CBLI" id="CBLI" value="1">
154             <input type="hidden" name="signUp" id="signUp" value="1">
155             <button type="submit" name="submitLI" id="submitLI">Log In!</button>
156         </p>
157     </form>-->
158
159     <!DOCTYPE html>
160     <html lang="en">
161         <head>
162             <!-- Required meta tags -->
163             <meta charset="utf-8">
164             <meta name="viewport" content="width=device-width, initial-scale=1,
165                 shrink-to-fit=no">
166
167             <!-- Bootstrap CSS -->
168             <link rel="stylesheet"
169                 href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/css/bootstrap.min.css"
170                 integrity="sha384-rwoIResjU2yc3z8GV/NPeZWAv56rSmLldC3R/AZzGRnGxQQKnKkoFVhFQhNU
171                 wEyJ" crossorigin="anonymous">
172
173             <style type="text/css">
174             </style>
175         </head>
176         <body>
177             <h1>Hello, world!</h1>
178
179             <!-- jQuery first, then Tether, then Bootstrap JS. -->
180             <script src="https://code.jquery.com/jquery-3.1.1.slim.min.js"
181                 integrity="sha384-A7FZj7v+d/sdmMqp/nOQwliLvUsJfDHW+k9Omg/a/EheAdgtzNs3hpfag6Ed
182                 950n" crossorigin="anonymous"></script>
183
184             <script
185                 src="https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js"
186                 integrity="sha384-DztdAPBWPRXSA/3eYEEUWrWCy7G5KFbe8fFjk5JAIxUYHKkDx6Qin1DkWx51
187                 bBrb" crossorigin="anonymous"></script>
188
189             <script
190                 src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-alpha.6/js/bootstrap.min.
191                 js"
192                 integrity="sha384-vBWWz1ZJ8ea9aCX4pEW3rVHjgjt7zpkNpZk+02D9phzyeVKE+jo0ieGizqPL
193                 Forn" crossorigin="anonymous"></script>
194
195             <script type="text/javascript">
196             </script>
197         </body>
198     </html>

```