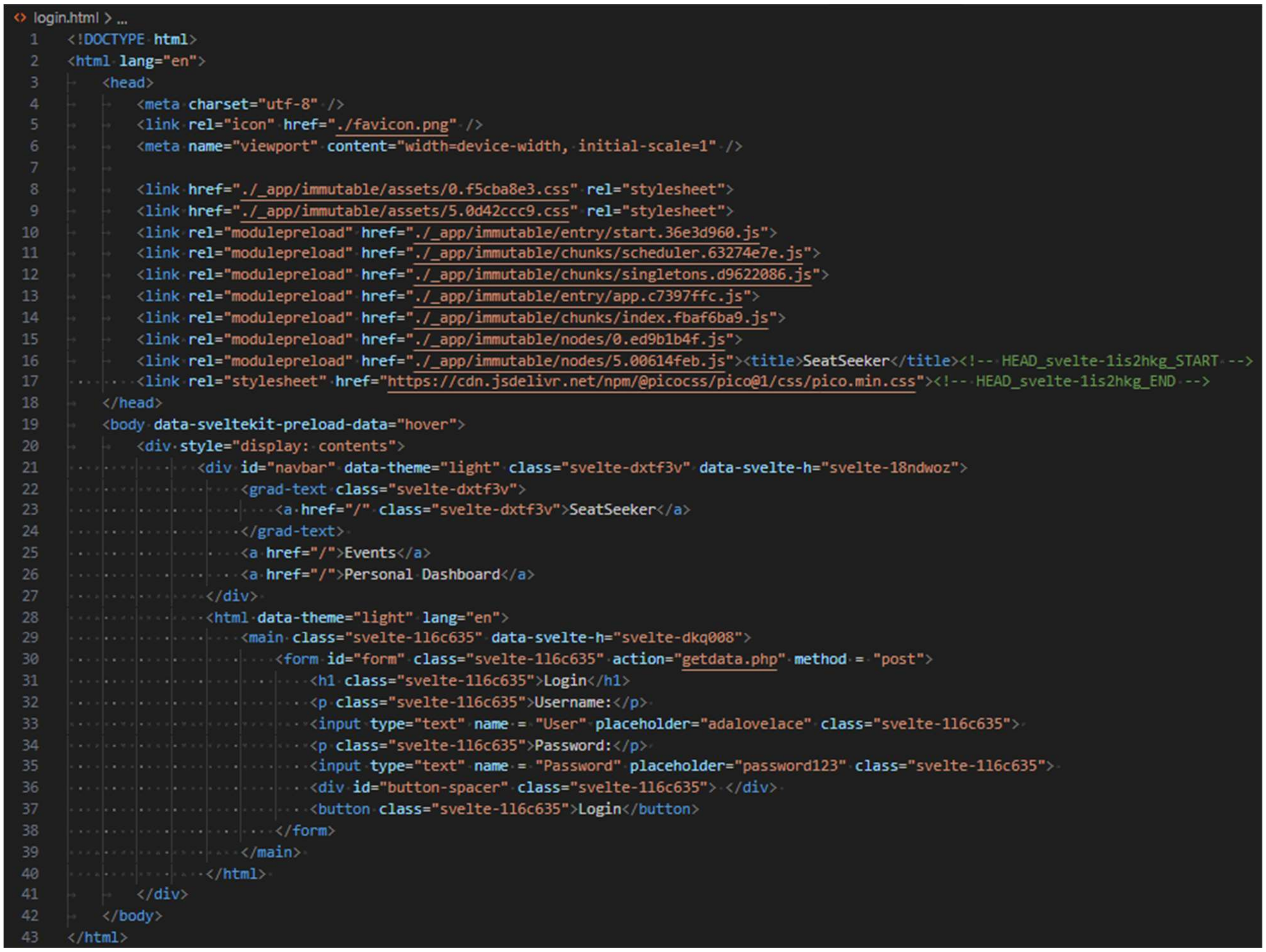
Justis Watkins jcw200002
Nicholas Zolton ngz200000
Keshav Santhanam krs200008
Roj Pawig rzp200000
Dalton Brua tdb200000
11/20/2023

Assignment 6

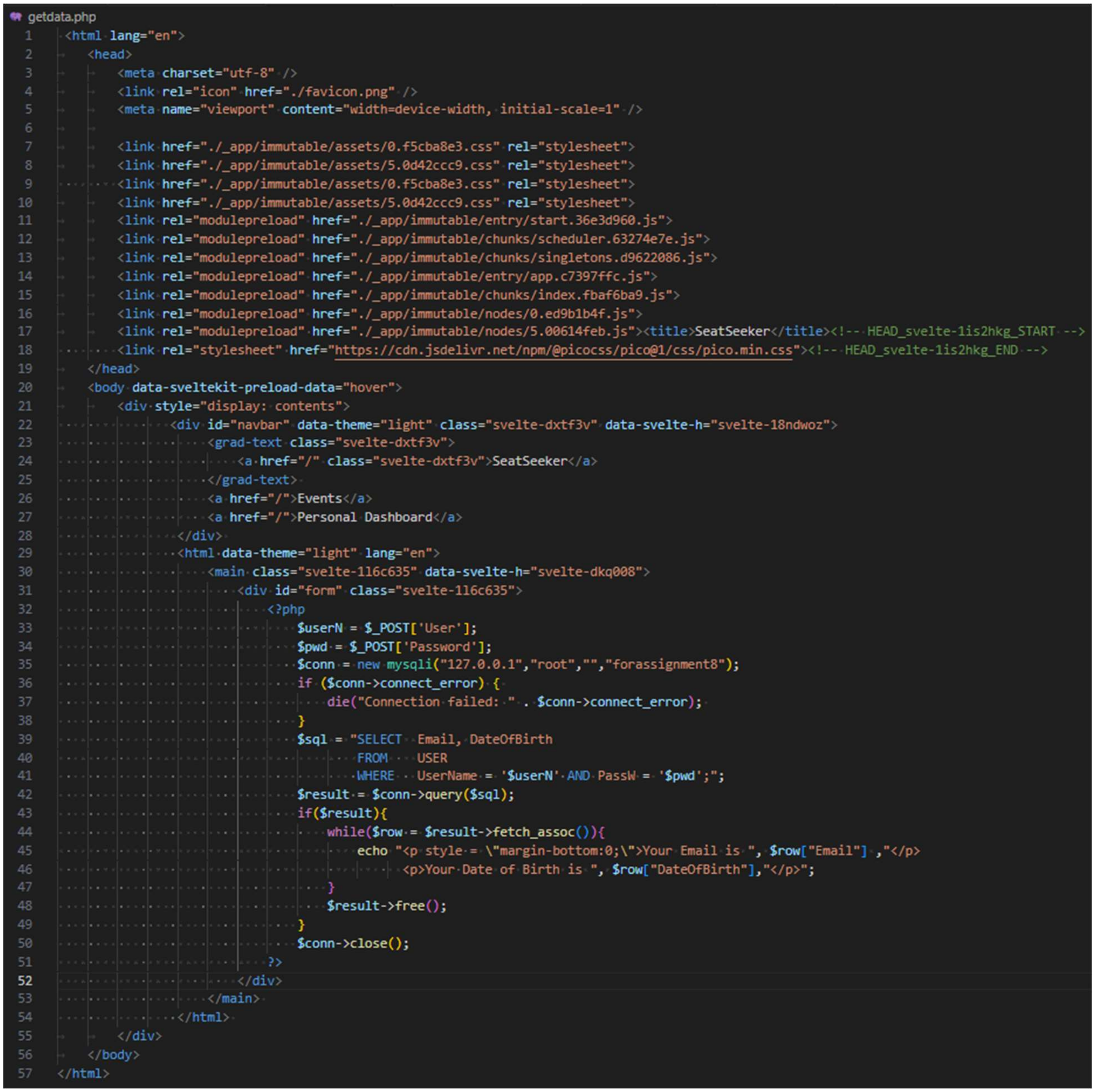
a)

login.html



```html
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8" />
        <link rel="icon" href="./favicon.png" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />

        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
        <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
    </head>
    <body data-sveltekit-preload-data="hover">
        <div style="display: contents">
               <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    <grad-text class="svelte-dxtf3v">
                        <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                    </grad-text>
                    <a href="/">Events</a>
                    <a href="/">Personal Dashboard</a>
                </div>
                <html data-theme="light" lang="en">
                    <main class="svelte-116c635" data-svelte-h="svelte-dkq008">
                        <form id="form" class="svelte-116c635" action="getdata.php" method = "post">
                            <h1 class="svelte-116c635">Login</h1>
                            <p class="svelte-116c635">Username:</p>
                            <input type="text" name = "User" placeholder="adalovelace" class="svelte-116c635">
                            <p class="svelte-116c635">Password:</p>
                            <input type="text" name = "Password" placeholder="password123" class="svelte-116c635">
                            <div id="button-spacer" class="svelte-116c635"> </div>
                            <button class="svelte-116c635">Login</button>
                        </form>
                    </main>
                </html>
        </div>
    </body>
</html>
```

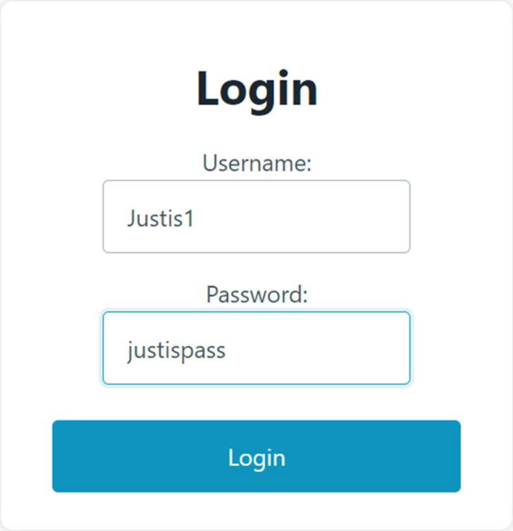
getdata.php



getdata.php

```
<html lang="en">
    <head>
        <meta charset="utf-8" />
        <link rel="icon" href="./favicon.png" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />

        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
        <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
    </head>
    <body data-sveltekit-preload-data="hover">
        <div style="display: contents">
               <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    <grad-text class="svelte-dxtf3v">
                        <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                    </grad-text>
                    <a href="/">Events</a>
                    <a href="/">Personal Dashboard</a>
                </div>
                <html data-theme="light" lang="en">
                    <main class="svelte-116c635" data-svelte-h="svelte-dkq008">
                        <div id="form" class="svelte-116c635">
                            <?php
                                $userN = $_POST['User'];
                                $pwd = $_POST['Password'];
                                $conn = new mysqli("127.0.0.1","root","","forassignment8");
                                if ($conn->connect_error) {
                                    die("Connection failed: " . $conn->connect_error);
                                }
                                $sql = "SELECT  Email, DateOfBirth
                                        FROM   USER
                                        WHERE  UserName = '$userN' AND PassW = '$pwd';";
                                $result = $conn->query($sql);
                                if($result){
                                    while($row = $result->fetch_assoc()){
                                        echo "<p style = \"margin-bottom:0;\">Your Email is ", $row["Email"] ,"</p>
                                              <p>Your Date of Birth is ", $row["DateOfBirth"],"</p>";
                                    }
                                    $result->free();
                                }
                                $conn->close();
                            ?>
                        </div>
                    </main>
                </html>
        </div>
    </body>
</html>
```

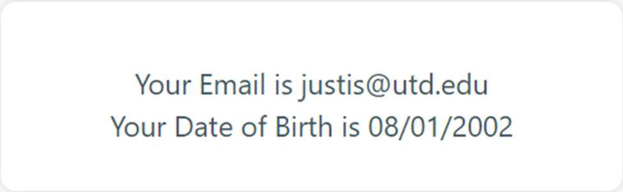
Intended Use and Result:



Login

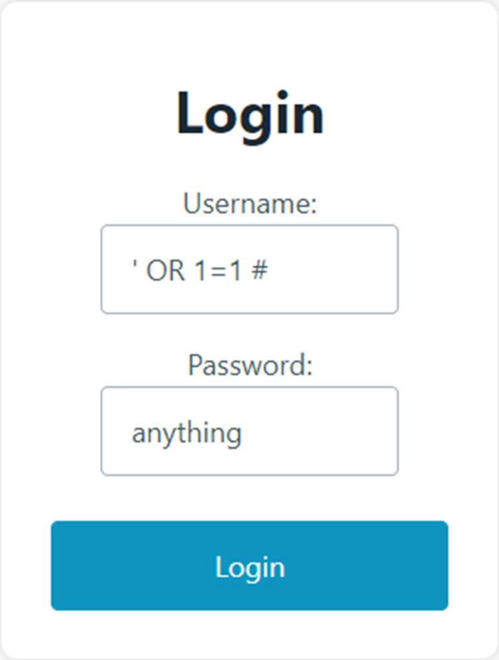
Username: Justis1

Password: justispass



Your Email is justis@utd.edu
Your Date of Birth is 08/01/2002

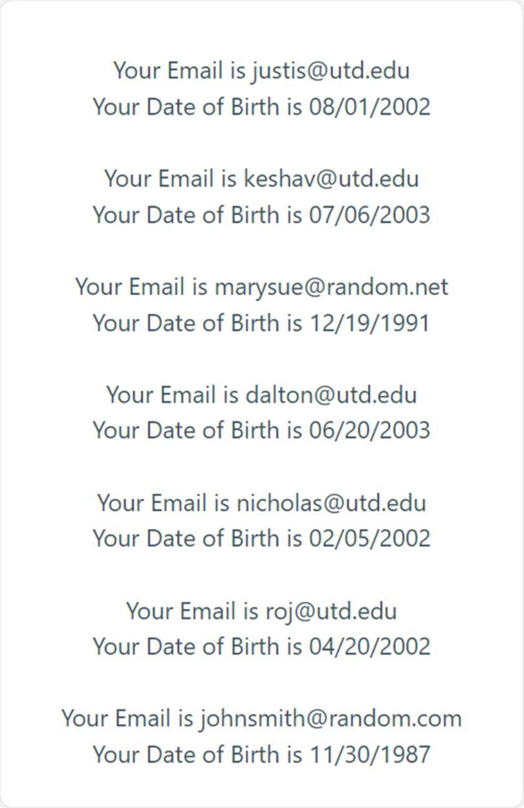
Injected SQL and Result:



Login

Username: ' OR 1=1 #

Password: anything



Your Email is justis@utd.edu
Your Date of Birth is 08/01/2002

Your Email is keshav@utd.edu
Your Date of Birth is 07/06/2003

Your Email is marysue@random.net
Your Date of Birth is 12/19/1991

Your Email is dalton@utd.edu
Your Date of Birth is 06/20/2003

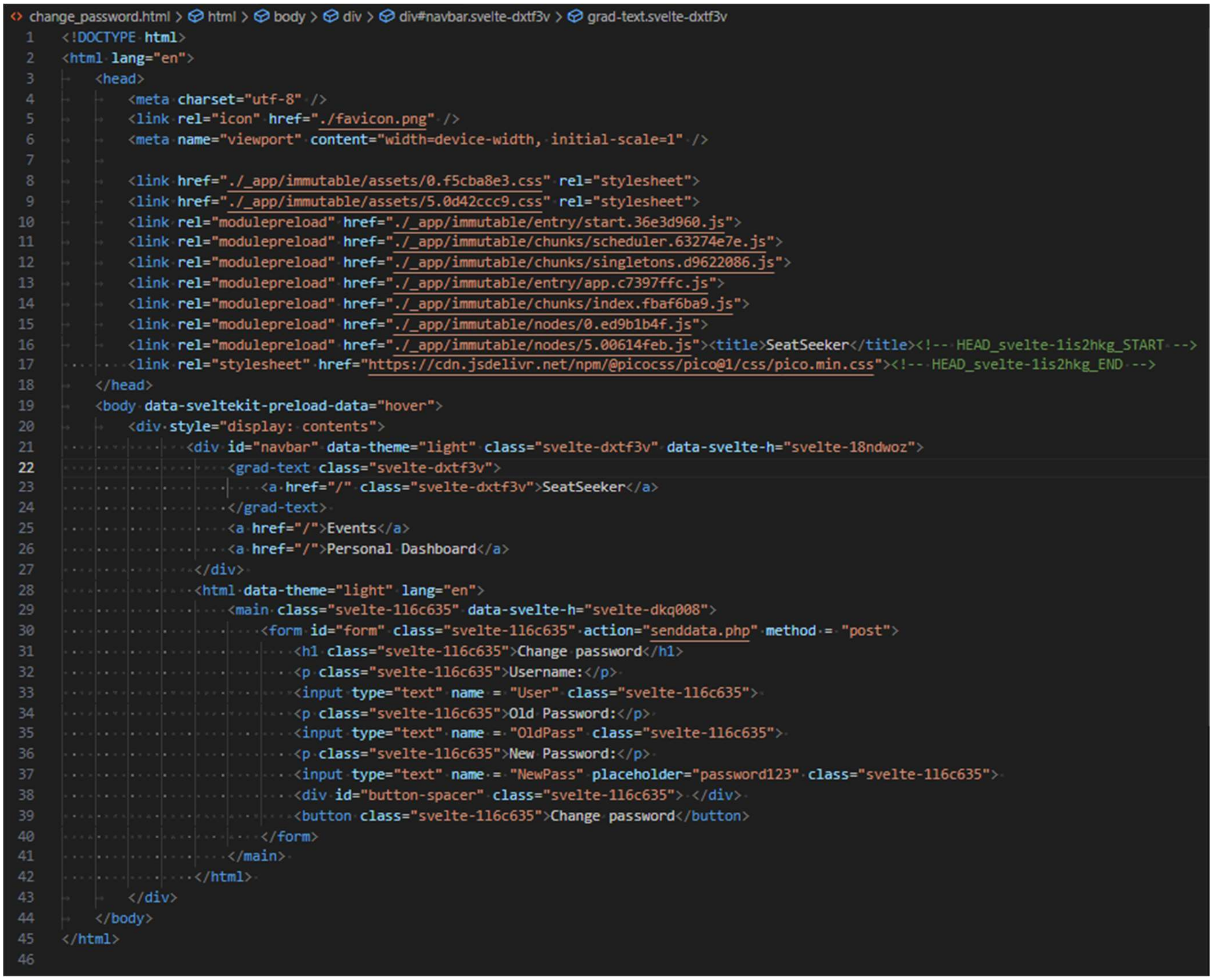
Your Email is nicholas@utd.edu
Your Date of Birth is 02/05/2002

Your Email is roj@utd.edu
Your Date of Birth is 04/20/2002

Your Email is johnsmith@random.com
Your Date of Birth is 11/30/1987

b)

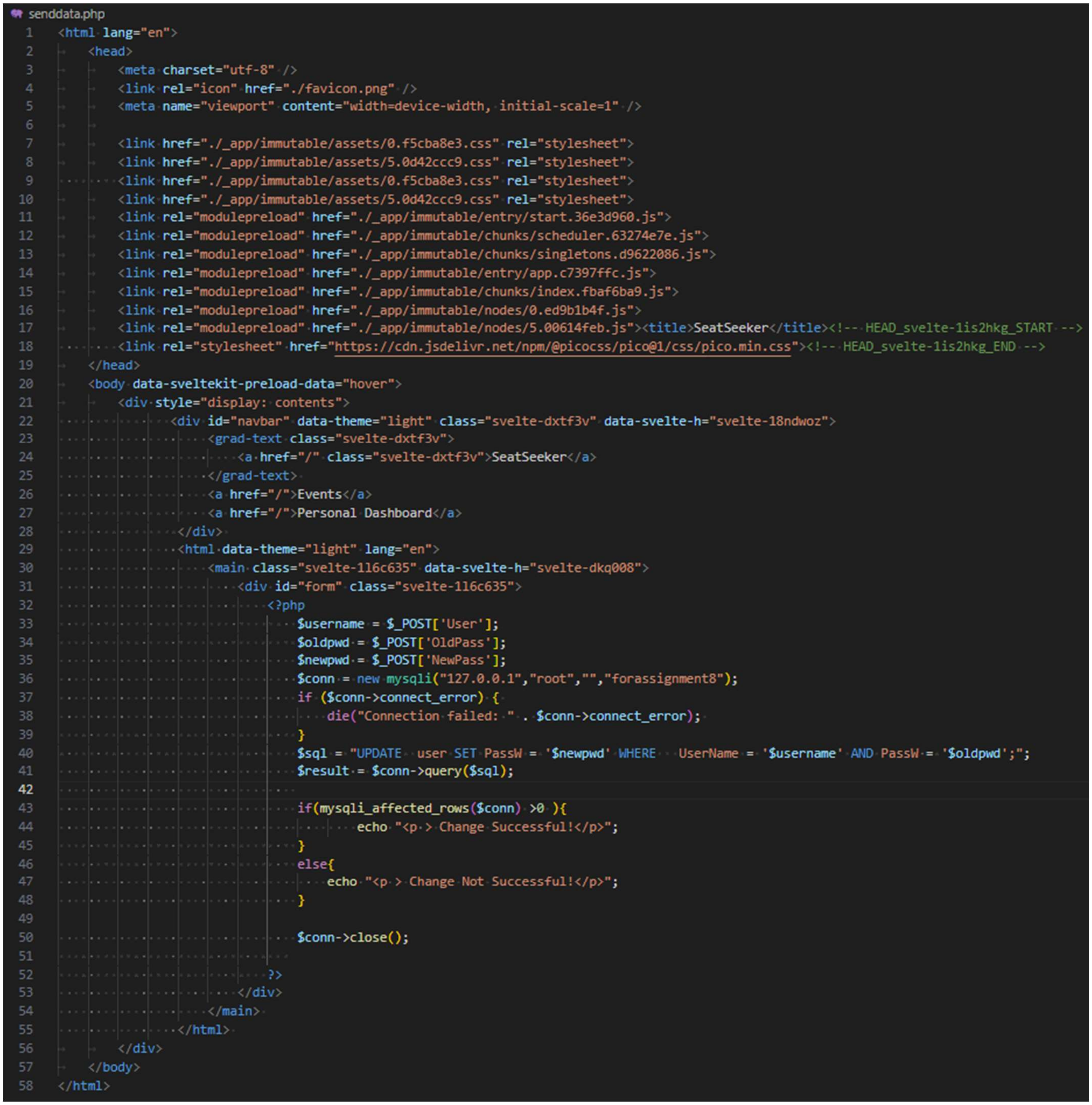
change_password.html



change_password.html > html > body > div > div#navbar.svelte-dxtf3v > grad-text.svelte-dxtf3v

```html
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8" />
        <link rel="icon" href="./favicon.png" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />

        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
        <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
    </head>
    <body data-sveltekit-preload-data="hover">
        <div style="display: contents">
                <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    <grad-text class="svelte-dxtf3v">
                        <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                    </grad-text>
                    <a href="/">Events</a>
                    <a href="/">Personal Dashboard</a>
                </div>
                <html data-theme="light" lang="en">
                    <main class="svelte-1l6c635" data-svelte-h="svelte-dkq008">
                        <form id="form" class="svelte-1l6c635" action="senddata.php" method = "post">
                            <h1 class="svelte-1l6c635">Change password</h1>
                            <p class="svelte-1l6c635">Username:</p>
                            <input type="text" name = "User" class="svelte-1l6c635">
                            <p class="svelte-1l6c635">Old Password:</p>
                            <input type="text" name = "OldPass" class="svelte-1l6c635">
                            <p class="svelte-1l6c635">New Password:</p>
                            <input type="text" name = "NewPass" placeholder="password123" class="svelte-1l6c635">
                            <div id="button-spacer" class="svelte-1l6c635"> </div>
                            <button class="svelte-1l6c635">Change password</button>
                        </form>
                    </main>
                </html>
        </div>
    </body>
</html>
```

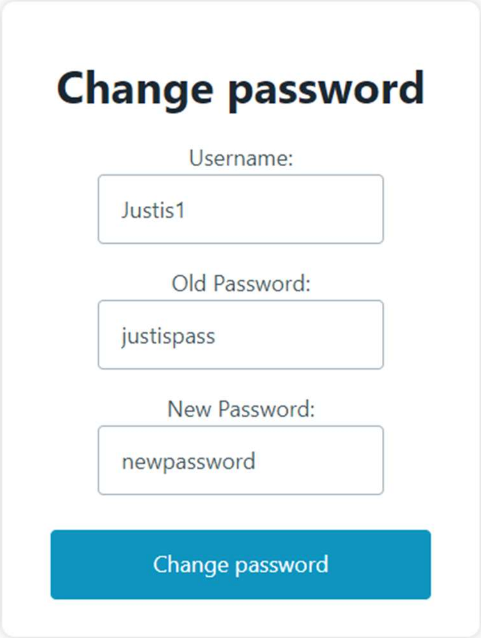
senddata.php



senddata.php

```
<html lang="en">
    <head>
        <meta charset="utf-8" />
        <link rel="icon" href="./favicon.png" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />

        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
        <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
    </head>
    <body data-sveltekit-preload-data="hover">
        <div style="display: contents">
                <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    <grad-text class="svelte-dxtf3v">
                        <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                    </grad-text>
                    <a href="/">Events</a>
                    <a href="/">Personal Dashboard</a>
                </div>
                <html data-theme="light" lang="en">
                    <main class="svelte-116c635" data-svelte-h="svelte-dkq008">
                        <div id="form" class="svelte-116c635">
                            <?php
                                $username = $_POST['User'];
                                $oldpwd = $_POST['OldPass'];
                                $newpwd = $_POST['NewPass'];
                                $conn = new mysqli("127.0.0.1","root","","forassignment8");
                                if ($conn->connect_error) {
                                    die("Connection failed: " . $conn->connect_error);
                                }
                                $sql = "UPDATE  user SET PassW = '$newpwd' WHERE   UserName = '$username' AND PassW = '$oldpwd';";
                                $result = $conn->query($sql);

                                if(mysqli_affected_rows($conn) >0 ){
                                        echo "<p > Change Successful!</p>";
                                }
                                else{
                                    echo "<p > Change Not Successful!</p>";
                                }

                                $conn->close();

                            ?>
                        </div>
                    </main>
                </html>
        </div>
    </body>
</html>
```

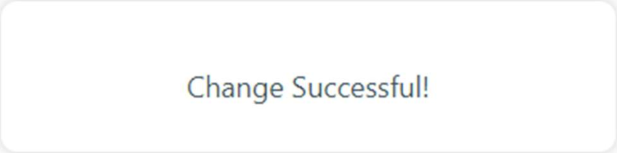
Intended Use and Result:


Change password

Username: Justis1

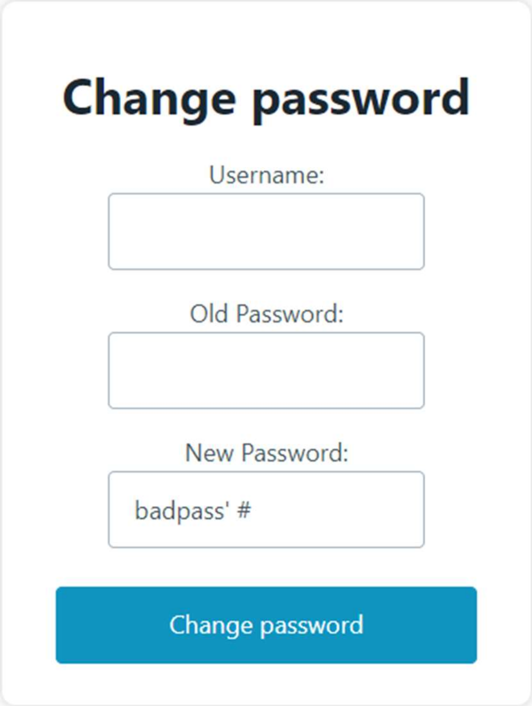
Old Password: justispass

New Password: newpassword


Change Successful!

Changed the user with Username = ‘Justis1’ password to ‘newpassword’ if their old password was ‘justispass’.

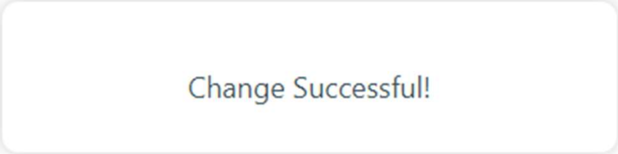
Injected SQL and Result:


Change password

Username:

Old Password:

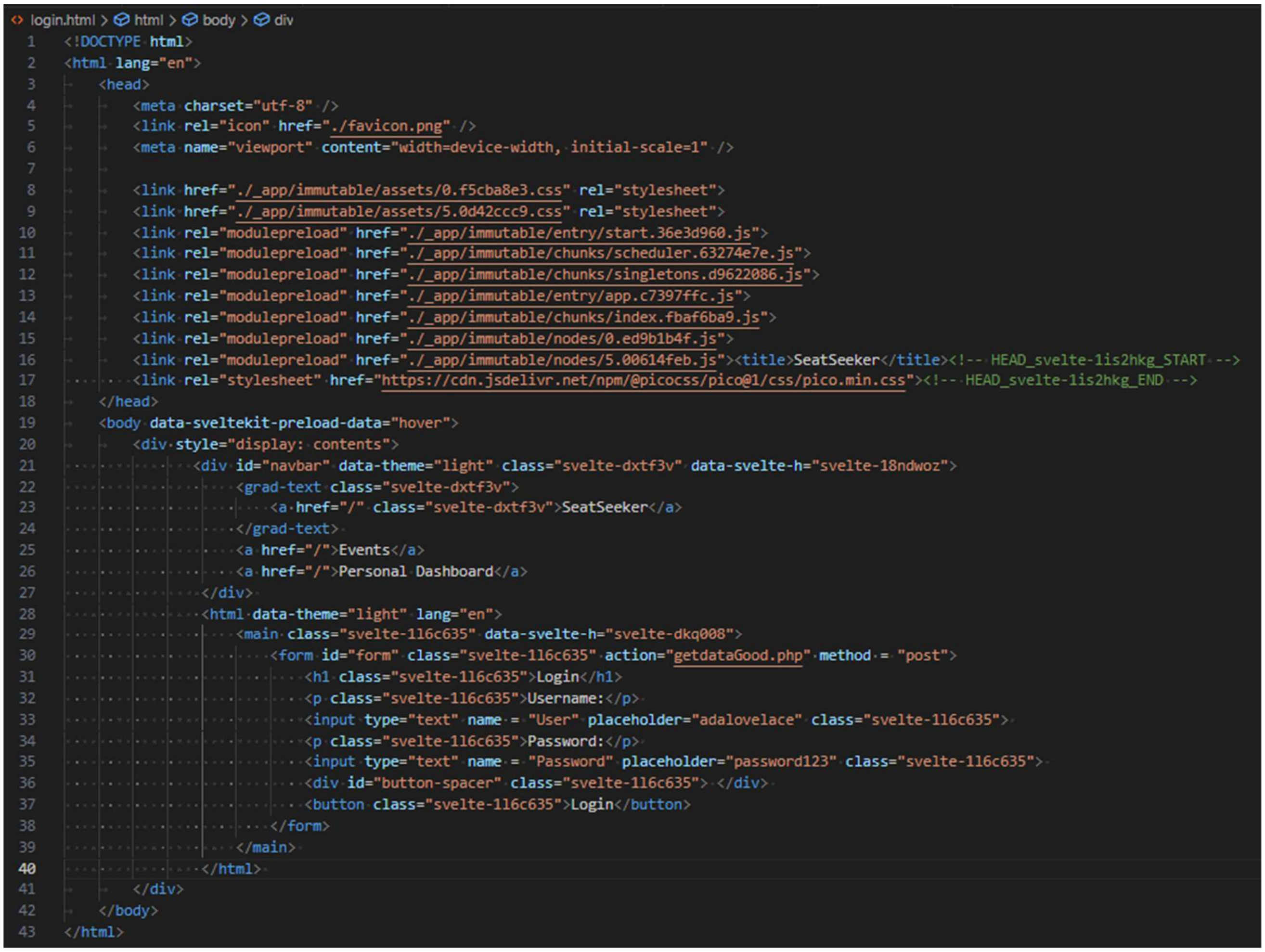
New Password: badpass' #


Change Successful!

Changes the password of all users to ‘badpass’ regardless of what their username is or what their password is.

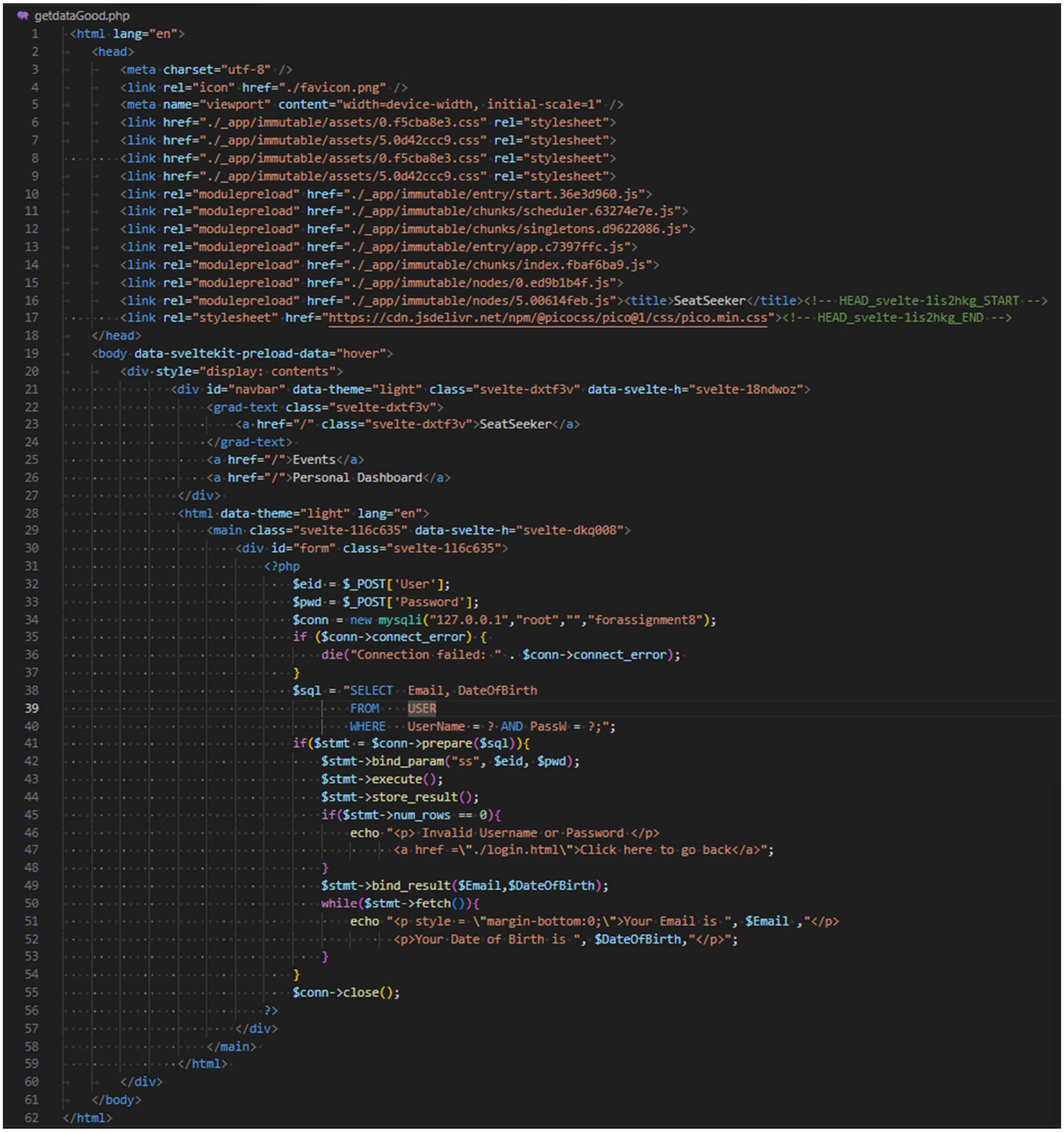
c)

login.html



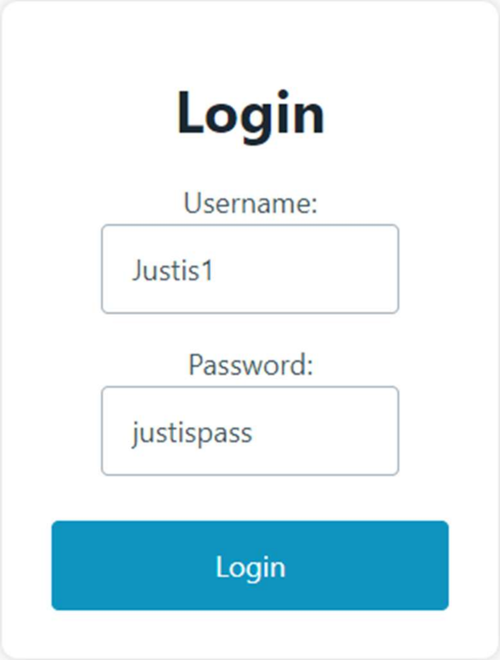
```html
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8" />
        <link rel="icon" href="./favicon.png" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />

        <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
        <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
        <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
        <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
        <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
        <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
    </head>
    <body data-sveltekit-preload-data="hover">
        <div style="display: contents">
               <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    <grad-text class="svelte-dxtf3v">
                        <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                    </grad-text>
                    <a href="/">Events</a>
                    <a href="/">Personal Dashboard</a>
                </div>
                <html data-theme="light" lang="en">
                    <main class="svelte-116c635" data-svelte-h="svelte-dkq008">
                        <form id="form" class="svelte-116c635" action="getdataGood.php" method = "post">
                            <h1 class="svelte-116c635">Login</h1>
                            <p class="svelte-116c635">Username:</p>
                            <input type="text" name = "User" placeholder="adalovelace" class="svelte-116c635">
                            <p class="svelte-116c635">Password:</p>
                            <input type="text" name = "Password" placeholder="password123" class="svelte-116c635">
                            <div id="button-spacer" class="svelte-116c635"> </div>
                            <button class="svelte-116c635">Login</button>
                        </form>
                    </main>
                </html>
        </div>
    </body>
</html>
```

getdatagood.php



```
<html lang="en">
   <head>
       <meta charset="utf-8" />
       <link rel="icon" href="./favicon.png" />
       <meta name="viewport" content="width=device-width, initial-scale=1" />
       <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
       <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
       <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
       <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
       <link rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
       <link rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
       <link rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
       <link rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
       <link rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
       <link rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">
       <link rel="modulepreload" href="./_app/immutable/nodes/5.00614feb.js"><title>SeatSeeker</title><!-- HEAD_svelte-1is2hkg_START -->
       <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@picocss/pico@1/css/pico.min.css"><!-- HEAD_svelte-1is2hkg_END -->
   </head>
   <body data-sveltekit-preload-data="hover">
       <div style="display: contents">
              <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                   <grad-text class="svelte-dxtf3v">
                       <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                   </grad-text>
                   <a href="/">Events</a>
                   <a href="/">Personal Dashboard</a>
               </div>
               <html data-theme="light" lang="en">
                   <main class="svelte-116c635" data-svelte-h="svelte-dkq008">
                       <div id="form" class="svelte-116c635">
                           <?php
                               $eid = $_POST['User'];
                               $pwd = $_POST['Password'];
                               $conn = new mysqli("127.0.0.1","root","","forassignment8");
                               if ($conn->connect_error) {
                                   die("Connection failed: " . $conn->connect_error);
                               }
                               $sql = "SELECT  Email, DateOfBirth
                                       FROM   USER
                                       WHERE  UserName = ? AND PassW = ?;";
                               if($stmt = $conn->prepare($sql)){
                                   $stmt->bind_param("ss", $eid, $pwd);
                                   $stmt->execute();
                                   $stmt->store_result();
                                   if($stmt->num_rows == 0){
                                       echo "<p> Invalid Username or Password </p>
                                             <a href =\"./login.html\">Click here to go back</a>";
                                   }
                                   $stmt->bind_result($Email,$DateOfBirth);
                                   while($stmt->fetch()){
                                       echo "<p style = \"margin-bottom:0;\">Your Email is ", $Email ,"</p>
                                             <p>Your Date of Birth is ", $DateOfBirth,"</p>";
                                   }
                               }
                               $conn->close();
                           ?>
                       </div>
                   </main>
               </html>
       </div>
   </body>
</html>
```

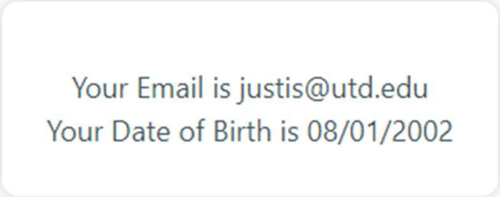
Intended use and result:



Login

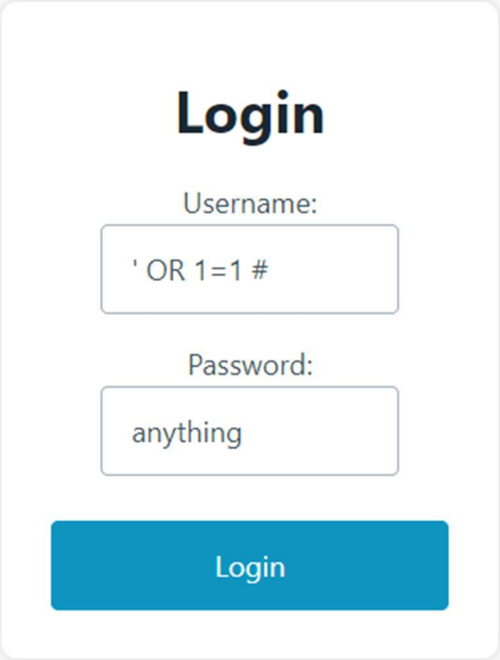
Username: Justis1

Password: justispass



Your Email is justis@utd.edu
Your Date of Birth is 08/01/2002

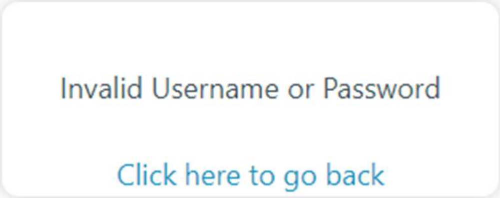
SQL Injection and result:



Login

Username: ' OR 1=1 #

Password: anything



Invalid Username or Password