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

Assignment 6

a)

login.html

```
<!DOCTYPE-html>
<html lang="en">
        <meta charset="utf-8" />
        dlink 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/chunks/singletons.d9622086.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/chunks/index.fbaf6ba9.js")
         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 --->
    <body data-sveltekit-preload-data="hover">
                <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                    grad-text class="svelte-dxtf3v"
· · · <button class="svelte-116c635">Login</button>
```

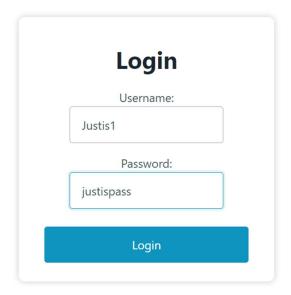
getdata.php

```
getdata.php
     <html lang="en">
            <meta charset="utf-8" />
            k.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";</pre>
            <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/scheduler.63274e7e.js">
<link.rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
\link.rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">

           k rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
k rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">

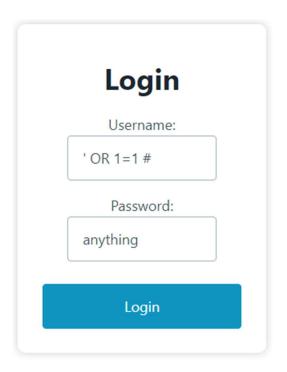
<pr
     <body data-sveltekit-preload-data="hover">
                   </div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                      ... <grad-text-class="svelte-dxtf3v
                           <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                  ···<html·data-theme="light" lang="en">
             <div id="form" class="svelte-116c635">
                                     $userN = $_POST['User'];
                                    $pwd:= $_POST['Password'];
$conn = new mysqli("127.0.0.1","root","","forassignment8");
                                    $sql = "SELECT" Email, DateOfBirth
                                            --FROM----USER
--WHERE---UserName-=-'$userN'-AND-PassW-=-'$pwd';";
                                     $result = $conn->query($sq1);
                                     if($result){
                                         while($row = $result->fetch_assoc()){
                                             $result->free();
                                     $conn->close();
```

Intended Use and Result:



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

Injected SQL and Result:



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

change_password.html

```
change_password.html > ♦ html > ♦ body > ♦ div > ♦ div#navbar.svelte-dxtf3v > ♦ grad-text.svelte-dxtf3v
    <!DOCTYPE - html>
    <html lang="en">
            <meta charset="utf-8" />
             <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">
            k rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
k rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
k rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
k rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">

            rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
            k rel="modulepreload" href="./_app/immutable/nodes/0.ed9b1b4f.js">

<
        <body data-sveltekit-preload-data="hover">
            <div-style="display: contents"
                   </div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                             <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                     ····</grad-text>
                   ·····<a href="/">Events</a>

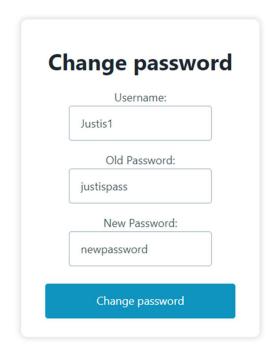
.....<a href="/">Personal Dashboard</a>
....
```

senddata.php

```
<html-lang="en">
           <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/5.0d42ccc9.css" rel="stylesheet">
      color="ink href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
           <link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
           k rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
           k 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/5.00614feb.js"><title>SeatSeeker</title><!--- HEAD_svelte-1is2hkg_START--->
     <body data-sveltekit-preload-data="hover">
           <div-style="display: contents";</pre>
                  <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>
                color="block">
class="svelte-116c635" data-svelte-h="svelte-dkq008">
class="svelte-116c635">
class="svelte-116c635">
                                 $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);
42
                                 if(mysqli_affected_rows($conn) >0 ){
                                       echo " Change Successful!";
                                 elsef
                                     echo " Change Not Successful!";
                                 $conn->close();
```

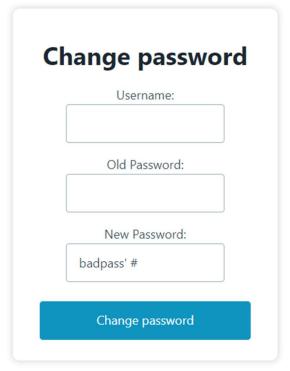
Intended Use and Result:



Change Successful!

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

Injected SQL and Result:



Change Successful!

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

login.html

```
login.html > ♦ html > ♦ body > ♦ div
            <!DOCTYPE-html>
             <html-lang="en":
                               <meta charset="utf-8" />
                               <link href="./_app/immutable/assets/0.f5cba8e3.css" rel="stylesheet">
<link href="./_app/immutable/assets/5.0d42ccc9.css" rel="stylesheet">
                                k rel="modulepreload" href="./_app/immutable/entry/start.36e3d960.js">
                               clink rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
clink rel="modulepreload" href="./_app/immutable/chunks/scheduler.63274e7e.js">
clink rel="modulepreload" href="./_app/immutable/chunks/singletons.d9622086.js">
clink rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js">
clink rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
clink rel="modulepreload" href="./_app/immutable/chunks
              - <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--->
                      <body data-sveltekit-preload-data="hover">
                                <div-style="display: contents"
                                               <div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                                                                     <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                      ··<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:
                                                         verified by class="svelte-116c635">Password:
                                                        <input type="text" name = "Password" placeholder="password123" class="svelte-116c635">
                                                         ......div id="button-spacer" class="svelte-116c635"> </div>
                                                                           ...<button class="svelte-116c635">Login</button>
40
```

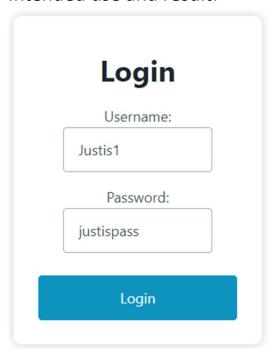
getdatagood.php

```
m getdataGood.php
            <html lang="en">
                       <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/5.0d42ccc9.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/singletons.d9622086.js">
                       k rel="modulepreload" href="./_app/immutable/entry/app.c7397ffc.js"
                       rel="modulepreload" href="./_app/immutable/chunks/index.fbaf6ba9.js">
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--->
                 <body data-sveltekit-preload-data="hover">
                       <div-style="display: contents"
                                 </div id="navbar" data-theme="light" class="svelte-dxtf3v" data-svelte-h="svelte-18ndwoz">
                                    </
                                                  <a href="/" class="svelte-dxtf3v">SeatSeeker</a>
                .....
                //div>------</div>-------</html-data-theme="light" lang="en">
                       cmain class="svelte-116c635" data-svelte-h="svelte-dkq008">
cmain class="svelte-dkq008">
c
                                                          $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);
            FROM · · · USER

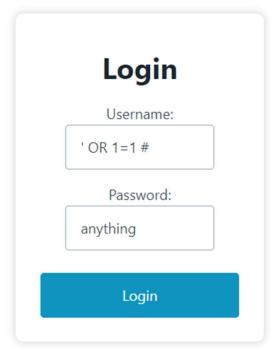
WHERE · · UserName · = ? · AND · PassW = · ?;";
 39
                                                                 if($stmt = $conn->prepare($sql)){
                                                                 $stmt->bind_param("ss", $eid, $pwd);
                                                                   ...$stmt->execute();
                                                                 $stmt->store_result();
                                                                   if($stmt->num_rows == 0){
                                                                        $stmt->bind_result($Email,$DateOfBirth);
                                                                      while($stmt->fetch()){
                                                                           echo "Your Email is ", $Email ,"
                                                                                    Your Date of Birth is ", $DateOfBirth,"";
                                                                 $conn->close();
```

Intended use and result:



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

SQL Injection and result:



Invalid Username or Password

Click here to go back