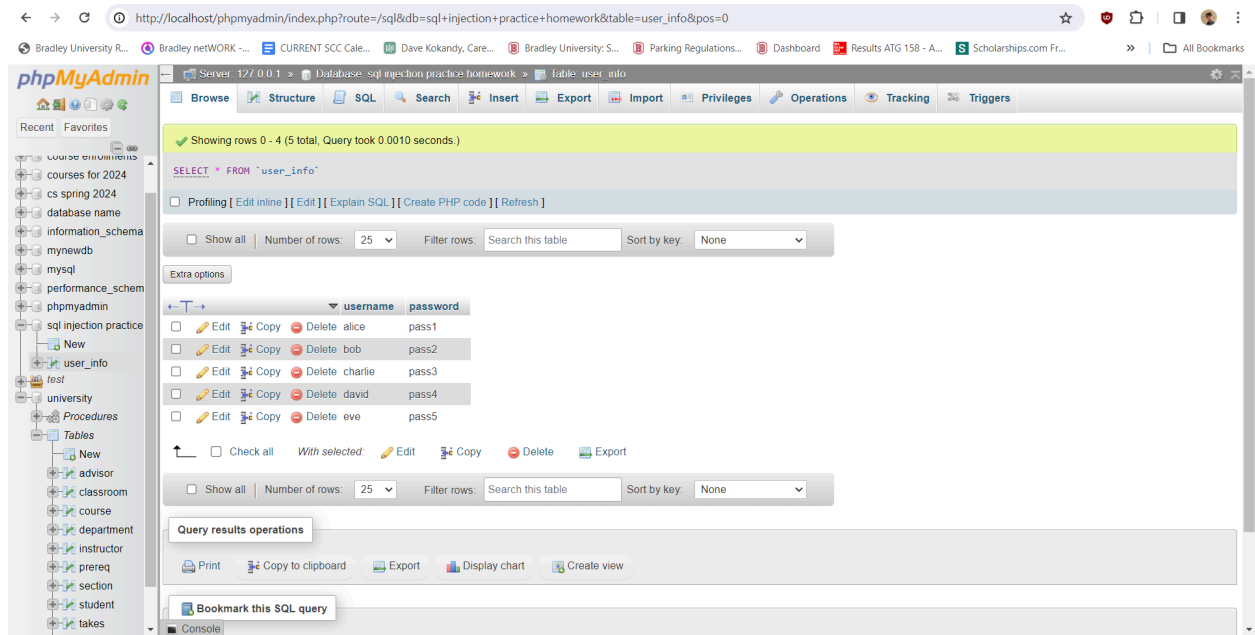
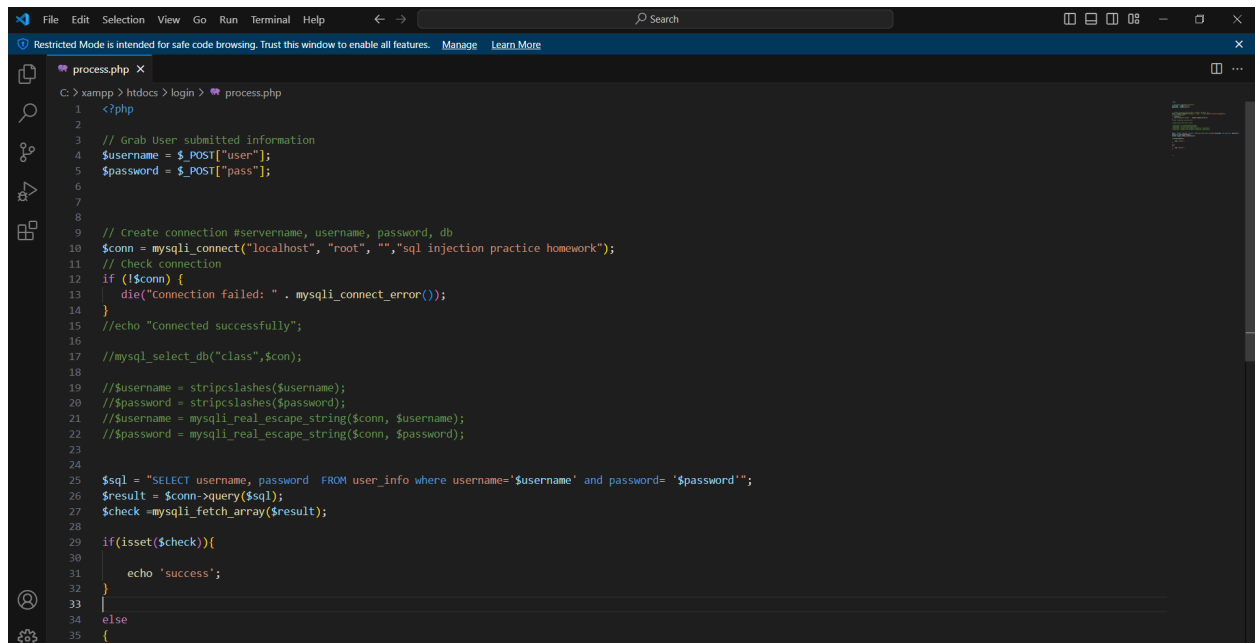


Isaac Sullivan
Injection Homework
CS 370
4/1/2024

Created database with given values:



Changed the \$conn line in process.php to sql injection practice homework:

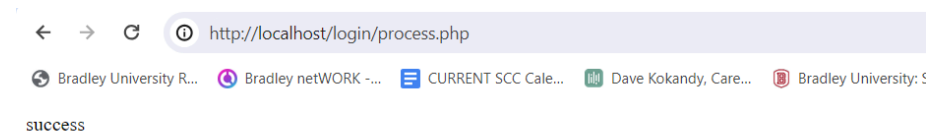


Testing correct username and password:

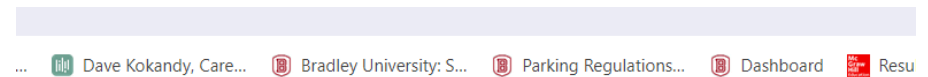
Sql injction test!

User Name Password

Login



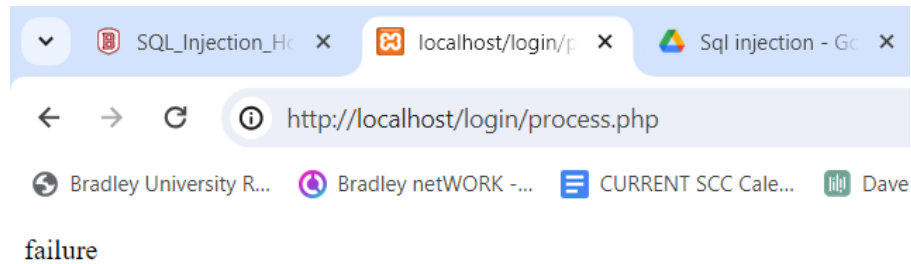
Testing incorrect username and password:



Sql injction test!

User Name Password

Login



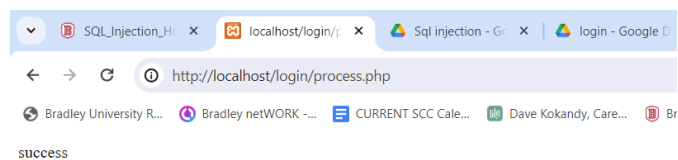
SQL Injection:



Sql injcetion test!

User Name Password

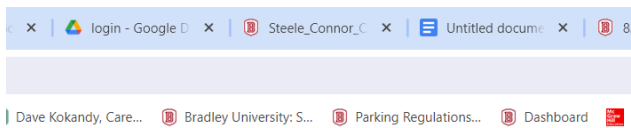
Login



SQL injection prevention:

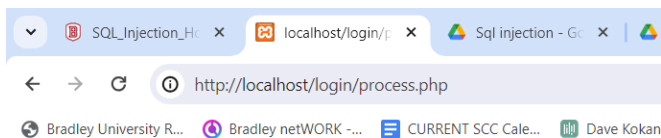
```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

process.php
C:\xampp\htdocs> login > process.php
1 <?php
2
3 // Grab user submitted information
4 $username = $_POST["user"];
5 $password = $_POST["pass"];
6
7
8
9 // Create connection #servername, username, password, db
10 $conn = mysqli_connect("localhost", "root", "", "sql injection practice homework");
11 // Check connection
12 if (!$conn) {
13     die("connection failed: " . mysqli_connect_error());
14 }
15 //echo "connected successfully";
16
17 //mysql_select_db("class",$conn);
18
19 $username = stripslashes($username);
20 $password = stripslashes($password);
21 $username = mysqli_real_escape_string($conn, $username);
22 $password = mysqli_real_escape_string($conn, $password);
23
24
25 $sql = "SELECT username, password FROM user_info where username=' $username' and password= '$password'";
26 $result = $conn->query($sql);
27 $check = mysqli_fetch_array($result);
28
29 if(isset($check)){
30     echo 'success';
31 }
32 |
33
34 else
```



Sql injection test!

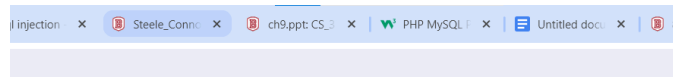
User Name Password



failure

Homework:

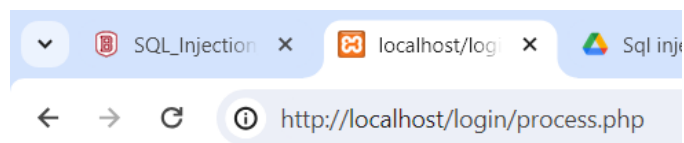
```
7
8
9 // Create connection #servername, username, password, db
10 $conn = mysqli_connect("localhost", "root", "", "sql injection practice homework");
11 // Check connection
12 if (!$conn) {
13     die("Connection failed: " . mysqli_connect_error());
14 }
15 //echo "Connected successfully";
16
17 //mysql_select_db("class",$con);
18
19 //$username = stripslashes($username);
20 //$password = stripslashes($password);
21 //$username = mysqli_real_escape_string($conn, $username);
22 //$password = mysqli_real_escape_string($conn, $password);
23
24 // prepare and bind
25 $stmt = $conn->prepare("SELECT username, password FROM user_info WHERE username = ? AND password = ?");
26 $stmt->bind_param("ss", $username, $password);
27
28 // set parameters and execute
29 $stmt->execute();
30
31 //Store the results
32 $stmt->store_result();
33
34 if ($stmt->fetch()) {
35     echo 'success';
36 } else {
37     echo 'failure';
38 }
39
40 $stmt->close();
41 $conn->close();
```



NT SCC Cale... Dave Kokandy, Care... Bradley University: S... Parking Regulations... Dashboard Result

Sql injection test!

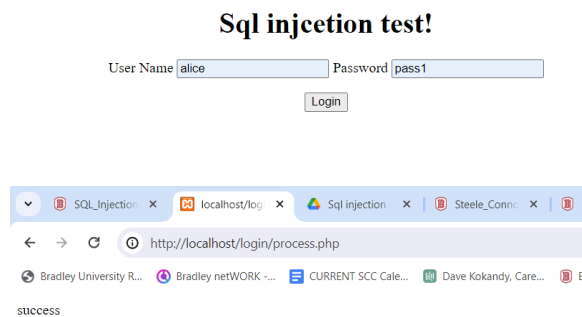
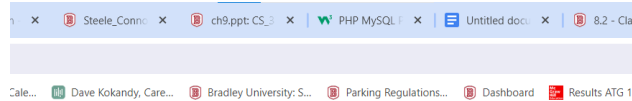
User Name Password



Bradley University R... Bradley netWORK -... CURRENT

failure

Query Test:



Homework Part 2:

```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

process.php
C:\> xampp> htdocs> login > process.php
1 <?php
2
3 // Grab User submitted information
4 $username = $_POST["user"];
5 $password = $_POST["pass"];
6
7
8
9 // Create connection #servername, username, password, db
10 $conn = mysqli_connect("localhost", "root", "", "sql injection practice homework");
11 // Check connection
12 if (!$conn) {
13     die("Connection failed: " . mysqli_connect_error());
14 }
15 //echo "Connected successfully";
16
17 //mysql_select_db("class",$conn);
18
19 //strip slashes
20 $username = stripslashes($username);
21 $password = stripslashes($password);
22 //escape special characters
23 $username = mysqli_real_escape_string($conn, $username);
24 $password = mysqli_real_escape_string($conn, $password);
25
26 // prepare and bind
27 $stmt = $conn->prepare("INSERT INTO user_info (username, password) VALUES (?, ?)");
28 $stmt->bind_param("ss", $username, $password);
29
30 // set parameters and execute
31 $username = "alice";
32 $password = "pass1";
33 $stmt->execute();
34
35 $username = "bob";
36 $password = "pass2";
37 $stmt->execute();
38
39 $username = "charlie";
40 $password = "pass3";
41 $stmt->execute();
42
43 $username = "david";
44 $password = "pass4";
45 $stmt->execute();
46
47 $username = "eve";
48 $password = "pass5";
49 $stmt->execute();
50
51 echo "New records created successfully";
52
53 $stmt->close();
54 $conn->close();
55
56 // $sql = "SELECT username, password FROM user_info where username=' $username' and password= '$password'";
57 // $result = $conn->query($sql);
58 // $check = mysqli_fetch_array($result);
59
60 // if(isset($check)){
61
62 // echo 'success';
63 // }
64
65 // else
```