Aoyan Sarkar

Quiz 2

**Part 1**

1.1. Explain three possible features of a web application that require (or, at least, made easier by) a server-side component written in a language such as PHP. Don't just mention the feature, explain in detail what it involves.

One feature that requires a server-side component is allowing users to access data from other devices. For example, if the website is a note-taking application, there needs to be a server to store the notes so that if a user signs into the app from their phone and on their computer, they have access to the same set of notes. This requires a server to store the notes in a database and then return them to the user when they go to their notes page. Another feature that requires a server-side component is to give users different privileges. If authorization was done entirely on the client side, then a user could read the source code to find out the “admin only” features and edit the client-side JavaScript to make themselves an administrator. The server therefore has to have the final say on who is authorized to take which actions. A third feature that requires a server-side component is allowing users to collaborate on the same document. For example, if Wikipedia was entirely client side, all the text in an article would be downloaded up front but no changes could be stored for other people to see. If a user wanted to fix a typo in an article, there would be no way for them to upload the change for other people, only for themselves, so a server has to sit and accept user input.

1.2. Explain two actions that can be taken to secure a web application. These may be related to user-authentication & authorization, server configuration, codebase, and/or network infrastructure. Don’t just mention the feature, explain in detail what it involves.

One action that can be taken to secure a web application is to sanitize any user input. This means to make sure that there are no malicious HTML tags in user input, otherwise a user can input a script tag that links to a script that will open a banking website and steal their password. Malicious HTML tags can be removed by find-and-replacing the < and > characters with their entity versions. These entity versions (< and >) look the same as the actual symbol but the browser will not treat them like tags but instead treat them like text. Another action that can be taken to

secure a web application is to properly sanitize SQL queries that use user input. If SQL sanitization is not done, a user could possibly delete all tables in the site, leading to data loss, or they could turn themselves from a normal user into an administrator. Most SQL libraries in PHP have a **prepared statements** function, which will make sure that any input fields cannot be executed as SQL.

**Part 2**

Explain this code segment in two different ways: first, explain the overall picture without using any technical jargon, as if you were explaining the code to someone who doesn't understand any programming, and; second, explain in as exacting detail as possible, line by line, what the code is doing. If there are any mistakes or errors in the code, fix them inline using a different color. If you come up to me to tell me there are mistakes, -5 points.

The purpose of the code is to output the first and last name of customers that have a specific last name, or if there is no last name given, the code will output the first and last name of all customers. The first line checks to see if the 'lname' query parameter was provided, and the second line checks to see if the value of the 'lname' query parameter is not empty. If both conditions are met, an SQL query is prepared that returns all fields in the customers table where the last name is equal to the given last name, and the last name stored in the 'lname' query parameter is bound to the statement. If the first condition is met but the second condition is not met, a message informing that no last name is echoed, and an SQL query is prepared that returns all fields in the customers table for all rows in the table. Then, the statement is executed. Finally, for every row that is returned from the database, the 'fname' and 'lname' values of the row are printed.

```
if (isset($_GET['lname']) && $_GET['lname'] != '') {
      $pstmt = $conn->prepare('SELECT * from customers WHERE lname =
:ln');
      $pstmt->bindParam('ln', $_GET['lname'], PDO::PARAM_STR);
} else {
      echo "lname not given, outputting entire file";
      $pstmt = $conn->prepare('SELECT * from customers');
}
$pstmt->execute();
while ($row = $pstmt->fetch()) {
```

```
        printf("%s %s",$row['fname'],$row['lname']);
}
```

**Part 3**

Link:
https://sarkaa3rpi169285.eastus.cloudapp.azure.com/itws2110-sarkaa3/quiz2/index.php

How to get new MBE courses:

1. Click ‘Create lectures’
2. Click ‘Create labs’
3. Click ‘View New Table’
4. A new ‘Switch Between WebSys and MBE’ button will appear that allows you to switch.

To get back, just click the ‘View New Table’ button again

**Extra Credit 1**

*Here's to old RPI, her fame may never die.*
*Here's to old Rensselaer, she stands today without a peer.*
*Here's to those olden days,*
*Here's to those golden days,*
*Here's to the friends we made at dear old RPI.*

**Extra Credit 2**

Wait for 11/28/2023.