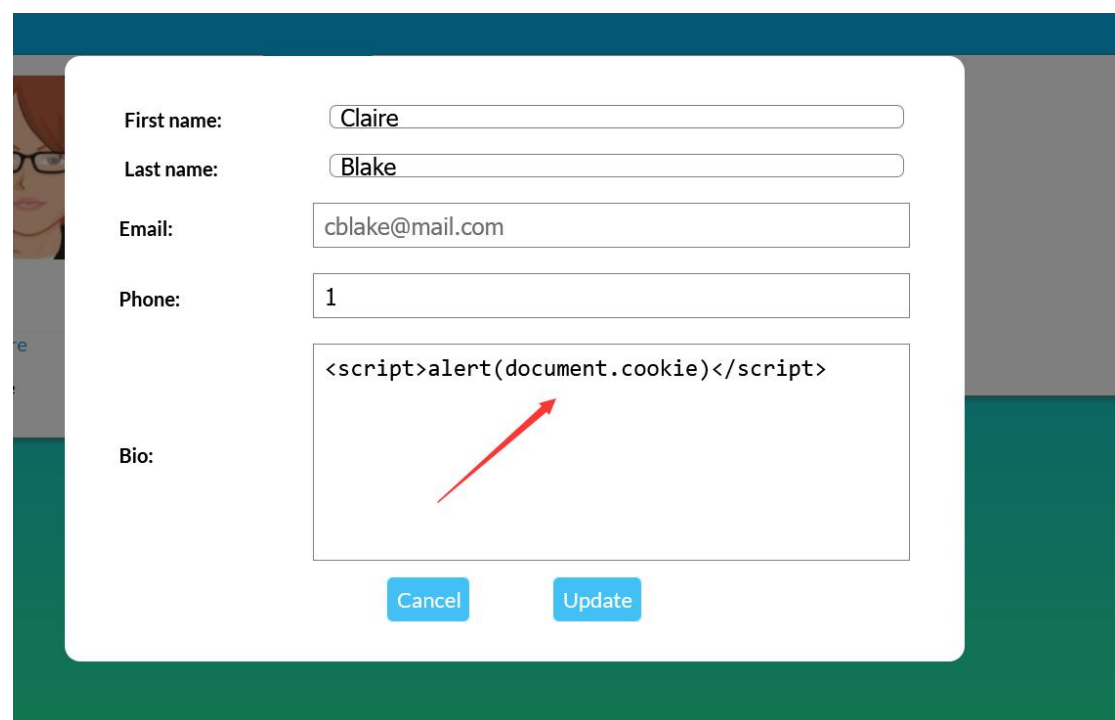
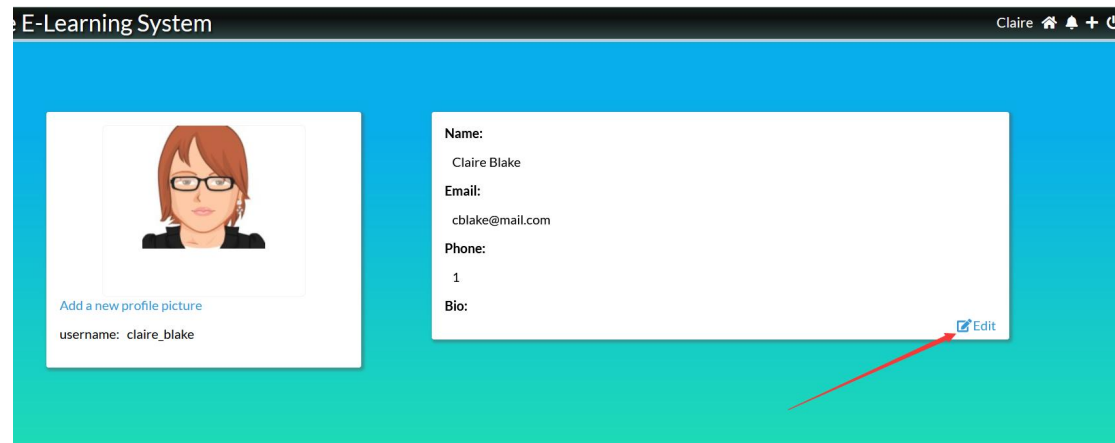


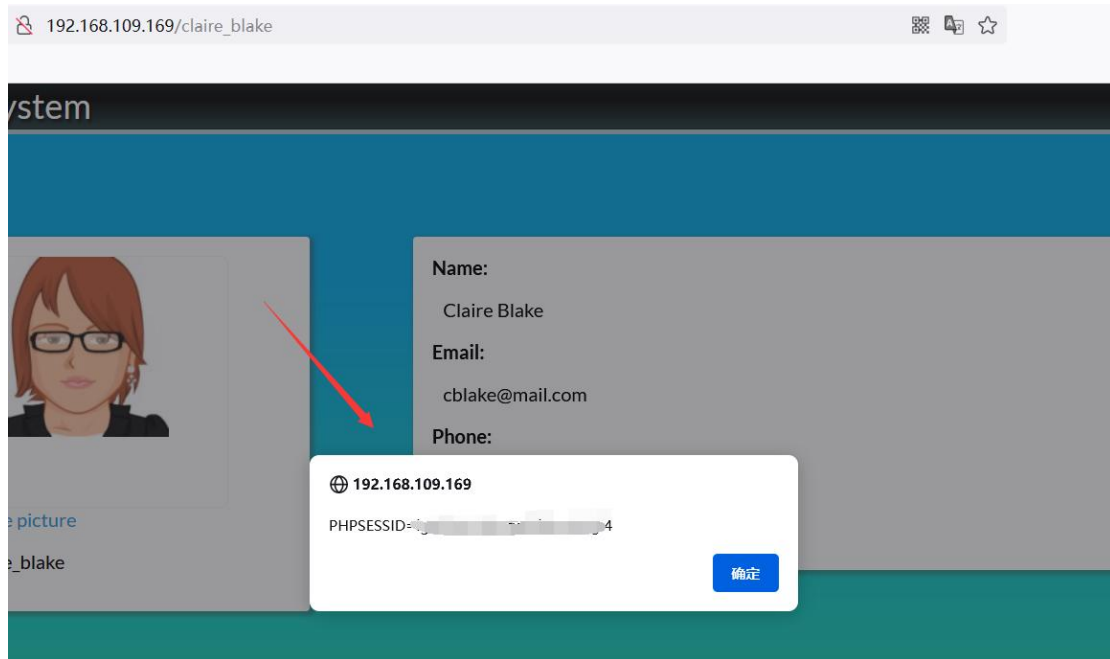
In the E-learning System, the modified Bio content of personal data is not filtered, resulting in Xss vulnerability. Attackers can use this vulnerability to steal malicious data.

```
if (isset($_POST['profile-updateBtn'])) {  
    $firstName = $_POST['firstName'];  
    $lastName = $_POST['lastName'];  
    $phoneNumber = $_POST['phoneNumber'];  
    $bio = $_POST['bio'];  
    $query = mysqli_query($con, "UPDATE users SET first_name = '$firstName' WHERE username LIKE '$username'");  
    $query1 = mysqli_query($con, "UPDATE users SET last_name = '$lastName' WHERE username LIKE '$username'");  
    $query2 = mysqli_query($con, "UPDATE users SET phoneNumber = '$phoneNumber' WHERE username LIKE '$username'");  
    $query3 = mysqli_query($con, "UPDATE users SET bio = '$bio' WHERE username LIKE '$username'");  
    header("Location: $username");  
}
```

Process to demonstrate



Vulnerability to prove



Download the source code

...

<https://www.sourcecodester.com/php-simple-e-learning-system-source-code>

...