


 main ▾

...

water_cve / E-learning System personal data modification XSS vulnerability.pdf

 E1CHO Add files via upload

History

1 contributor

242 KB

...

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 phone_number = '$phoneNumber' WHERE username LIKE '$username'");  
    $query3 = mysqli_query($con, "UPDATE users SET bio = '$bio' WHERE username LIKE '$username'");  
    header("Location: $username");  
}
```

Process to demonstrate

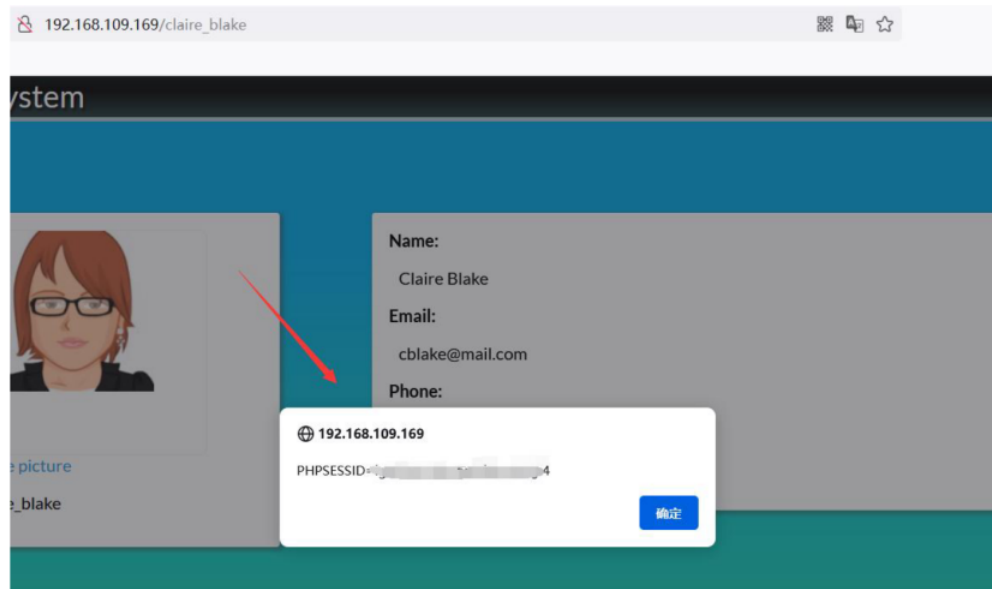
The image shows two screenshots from an "E-Learning System" interface. The top screenshot displays a user profile for "Claire Blake" with fields for Name, Email, Phone, and Bio. A red arrow points to an "Edit" button. The bottom screenshot shows the "Edit" modal, where the Bio field contains the malicious payload `<script>alert(document.cookie)</script>`. A red arrow points to this payload. The modal includes "Cancel" and "Update" buttons.

E-Learning System Claire

Name: Claire Blake
Email: cblake@mail.com
Phone: 1
Bio: [Edit](#)

First name: Claire
Last name: Blake
Email: cblake@mail.com
Phone: 1
Bio: `<script>alert(document.cookie)</script>`
[Cancel](#) [Update](#)

Vulnerability to prove



Download the source code

'''

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

'''

