

Instantly share code, notes, and snippets.

Xib3rR4dAr / [wp-simple-banner-2.11.0_multiple-vulns.md](#)

Secret

Created 4 months ago

☆ Star

<> Code  Revisions 1

Wordpress Simple Banner <= 2.11.0 Plugin Multiple vulnerabilities

 [wp-simple-banner-2.11.0_multiple-vulns.md](#)

Wordpress Simple Banner <= 2.11.0 Plugin Multiple vulnerabilities

Exploit Author: Muhammad Zeeshan (Xib3rR4dAr)

Vulnerable Plugin: [Simple Banner](#)

Plugin Slug: simple-banner

Active Plugin Installations: 50,000+

Vulnerable Version: <= 2.11.0 (latest version as of discovery)

Tested on: Wordpress v6.0.1

Vulnerability: Authenticated Stored XSS

Discovery date: July 19, 2022 Fix: Update plugin to version 2.12.0 or higher

Proof of Concept:

Login as admin and visit: <http://127.0.0.1/wp-admin/admin.php?page=simple-banner-settings>

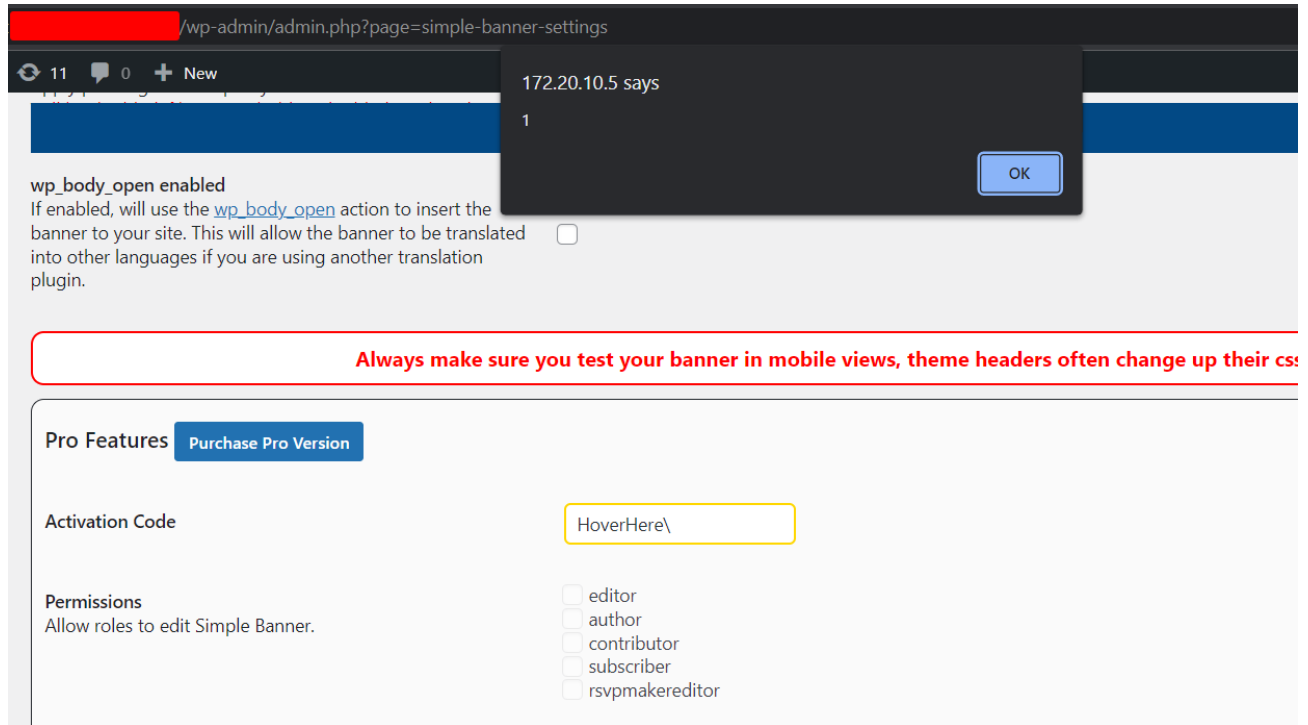
>> In "Activation Code" field enter XSS payload as `HoverHere" onmouseover=alert(1) a`

>> Click Save Changes

Stored XSS will trigger when any user having ability to manage "Simple Banner" visits: <http://127.0.0.1/wp-admin/admin.php?page=simple-banner-settings> and hovers on "Activation Code" text box.

User input is escaped by escaping quotes with backslash, that doesnot prevent XSS in html context. Instead, user input should be sanitized or HTML entities be encoded before displaying to user.

This vulnerability can be exploited by any user with any role even by subscriber if subscriber is given permissions to use the plugin. Therefore a subscriber user can exploit XSS to perform actions on behalf of other users.



Furthermore plugin has option to allow users of any role to access "Simple Banner" plugin. Other vulnerability classified as problematic is that, when using the plugin, an admin can allow any role to access the plugin.

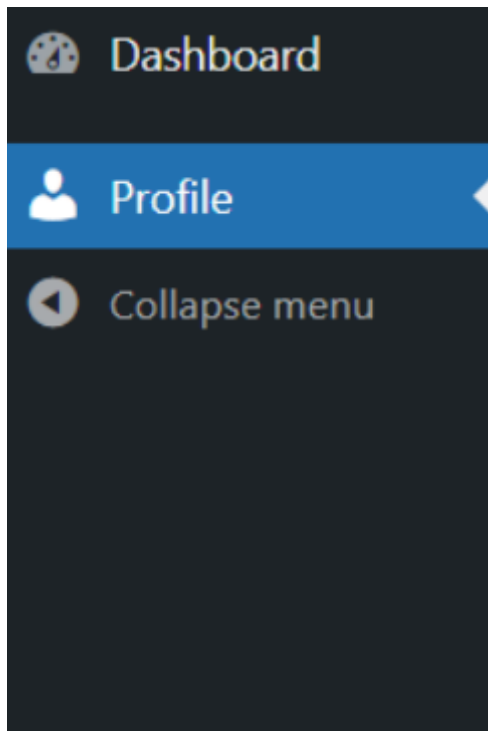
Expected behavior of feature: Role would be able to access "Simple Banner" plugin only

Actual Behavior: Role can access other plugins also other than "Simple Banner".


Admin would think that role would only be able to access "Simple Banner" but the role in actual would be able to access other plugins also since it adds capability of managing roles to users.

```
simple-banner.php X
simple-banner.php
203     echo '<script id="simple-banner-site-custom-js-dummy" type="text/javascript"></script>';
204 }
205 }
206
207 add_action('admin_menu', 'simple_banner_menu');
208 function simple_banner_menu() {
209     $manage_simple_banner = 'manage_simple_banner';
210     $manage_options = 'manage_options';
211     // Add admin access
212     $admin = get_role( 'administrator' );
213     if ($admin) {
214         $admin->add_cap( $manage_simple_banner );
215     }
216
217     $permissions_array = get_option('permissions_array');
218
219     // Add permissions for other roles
220     foreach (get_editable_roles() as $role_name => $role_info) {
221         if ( $role_name !== 'administrator' ) {
222             if (in_array($role_name, explode(",", $permissions_array))) {
223                 $add_role = get_role( $role_name );
224                 $add_role->add_cap( $manage_simple_banner );
225                 $add_role->add_cap( $manage_options );
226             } else {
227                 $remove_role = get_role( $role_name );
228                 // only remove capabilities if they were previously added
229                 if ($remove_role->has_cap( $manage_simple_banner )){
230                     $remove_role->remove_cap( $manage_simple_banner );
231                     $remove_role->remove_cap( $manage_options );
232                 }
233             }
234         }
235     }
```


Before allowing subscriber to access "Simple banner": (No plugin accessible to a user with subscriber role)




After allowing subscriber to access "Simple banner": (Plugins other than "Simple Banner" also accessible to subscriber)


 Dashboard





 Elementor

 Templates


 Profile

 Tools

 Settings

 Simple Banner



 Collapse menu