Description: WordPress before 4.8.2 does not sanitize plugin folder name when being embedded in a HTML tag, the tag will be printed out, this causes a stored XSS vulnerability. Refer to a piece of code in single_row() method of WP_Plugins_List_Table class:

```
640         if ( ( ! is_multisite() || $screen->in_admin( 'network' ) ) && current_user_can( 'edit_plugins' )
641             /* translators: %s: plugin name */
642             $actions['edit'] = '<a href="plugin-editor.php?file=' . $plugin_file . '" class="edit" aria-la
643         }
644     } // end if $context
```

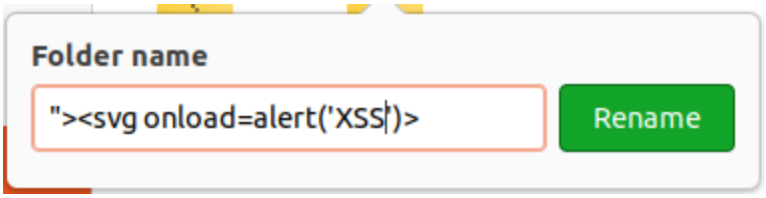
PoC:

Step 1 - Download a plugin file. You can choose whatever you want (https://downloads.wordpress.org/plugin/poll-maker.3.6.4.zip)

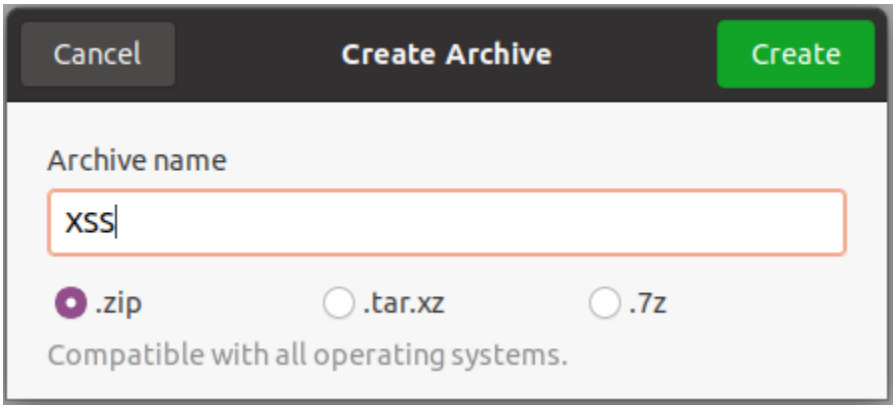
Step 2 - Extract the plugin

```
$ unzip -x poll-marker.3.6.4.zip
```

Step 3 - Change directory name.

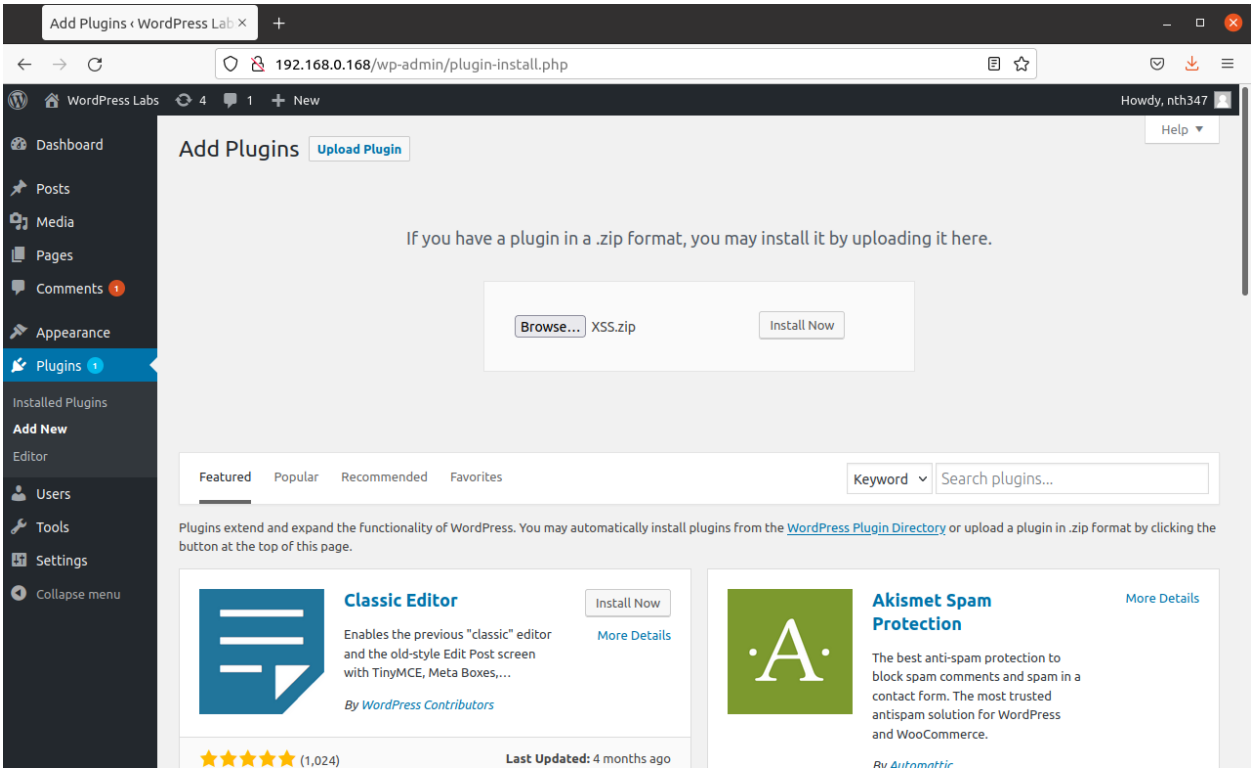


Step 4 - Compress the plugin directory.

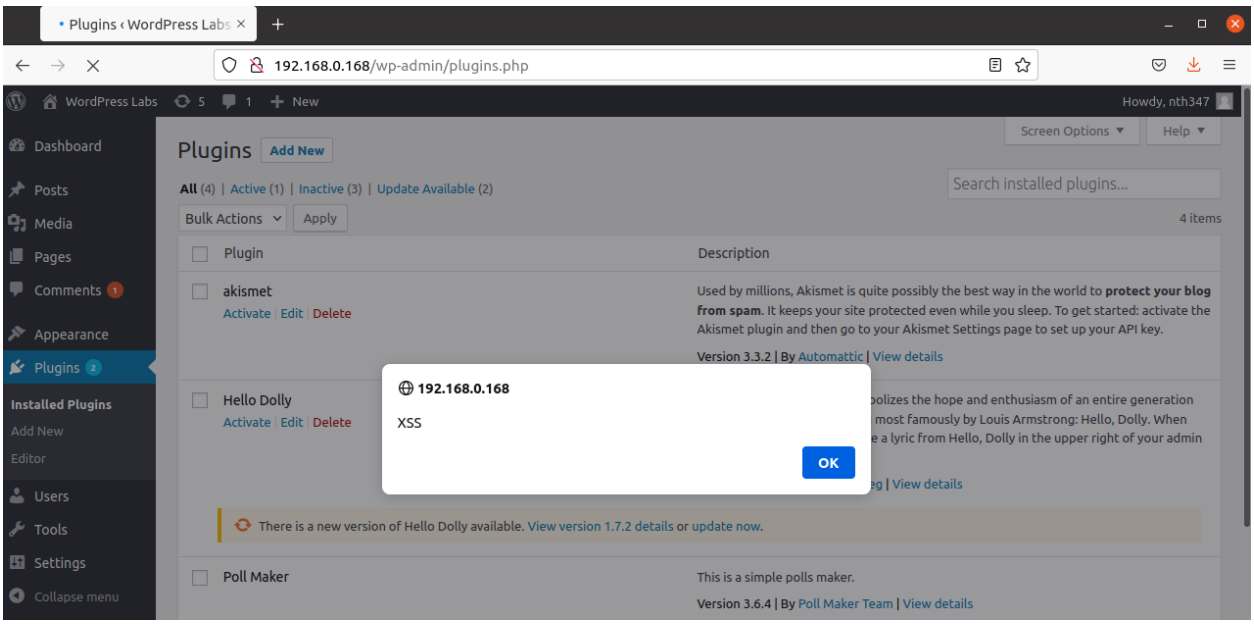


Step 5 - Login into your WordPress with administrator credentials.

Step 6 - Go to plugin upload module at http:/IP/wp-admin/plugin-install.php, choose XSS.zip, click Install Now.



8 - Access http://IP/wp-admin/plugins.php to trigger XSS payload:



This PoC tested on WordPress 4.7 and 4.8.1.