

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Exploiting an Arbitrary File Upload Vulnerability \[Pics/Video\]](#)

-DownFall - January 13, 2012, 12:52 am

Exploiting An Arbitrary File Upload Vulnerability

An arbitrary file upload vulnerability, is a vulnerability that can be exploited by malicious users to compromise a system. In this case, it's incorrectly validating the file extension on any uploaded file. Well....that pretty much speaks for itself. If used correctly, it can lead to shelling, executing remote code..all that good stuff.

First off, since I've been getting tons of PMs about the FireFox Add on and Theme I'm using, I'd figure I should just link them here.

[FTDeepDark Theme](#)
[HackBar](#)

Requirements

Now for this tutorial, you're going to need FireFox, and an add on called Tamper Data.

You can download it [here](#)

Once you got it installed, restart FireFox and you can get started.

Finding Vulnerabilities

Now what you're going to want to do is find a vulnerable upload form. How do you find these? A pretty common method known around here, using google dorks.

Here's the example I'll be using in this tutorial.

Code inurl:/upload.php intext:Image Upload

Now you can create your own, find your own, and use your own dorks.

Once you've found your site, you should be at an upload form.

It should look something like this.

Spoiler [\(Click to View\)](#)

Testing The Upload Form

Now try and upload your shell in regular format, to see if you'll need to continue.

Spoiler [\(Click to View\)](#)

Code Unrecognized image type

Now try and upload it in image format.

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

Modifying The POST Content

It worked, now we're going to go back, re upload, and modify the POST content.

Go back to your upload form, select your shell in image format, and go to Tools > Options > Tamper Data.

It should look something like this..

Spoiler ([Click to View](#))

Now click start tamper, and upload your file.

A popup will come up and ask you if you want to continue tampering. If it's sending information about the upload form, click continue tampering and click tamper.

Spoiler ([Click to View](#))

Now a whole new form should come up, it looks like this.

Spoiler ([Click to View](#))

Everything on the right is where we change our file extension. That is the POST data.

Now find your filename and remove your nullbyte and spoofed extension. Here's an example of what it should be changed to.

Code WSO.php%00.jpg

Code WSO.php

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

Now click OK, and your file should upload. Now all you have to do is find your shell, sometimes you can right click it (if it's a broken image), other times it'll be in the page source. This will work with several different upload forms, inside administrator panels, and other things as well. Hope you guys understand, good luck and happy hacking. Shoutout to Zer0Lulz!

Resources

[Test Site](#) - This site will get raped by everyone anyways....

[Shell Pack \(Image Format\)](#) || [Virus Scan](#)

[Tamper Data](#)

Video

Sorry, I had to re-do the video around 5 times, and it got annoying, so I skipped the text in notepad and just showed you what happens in action. It's here if you want to read it. My Camtasia studio ran out too, that explains the quality.

[Video: <http://www.youtube.com/watch?v=JcXK7GXRHww>]

Code Today I'm gonna be showing you how to get your shell uploaded via exploiting an arbitrary file upload vulnerability. Once you found your vulnerable form, try uploading your shell in PHP format..

"Unrecognized image type".

As you can see, it filters PHP image uploads. That doesn't mean we cant shell it though :3

Now we want to try and upload it in it's image format.

No error this time, it worked fine! Of course the shell won't work like this, but we're only 1 step

away.

Go back to your upload form, and go to tools > options > tamper data.

Now select your shell in image format again. Now start tamper, and upload your shell.

this is where we change our file extension, in the POST_DATA field.
Remove your nullbyte and file extension, and leave .php on there.

Click OK, and let it do it's work.

Uploaded our shell, just like that. Lets check if it worked...
Woot!

If you liked the video, comment/rate/sub!
Peace.

ProN0ob - January 13, 2012, 12:55 am
Good job.

A little question : Can this work on any forum/website with image uploader or just using the specified dork?

Thanks

BeggFoMercy - January 13, 2012, 12:56 am

nice TUT mate keep up the good work ... xD!

-DownFall - January 13, 2012, 12:59 am
(Jan 13, 2012 01:55 AM)ProN0ob Wrote: [\[CITE\]](#) Good job.

A little question : Can this work on any forum/website with image uploader or just using the specified dork?

Thanks

It all depends. I've came across about 10 forums with that dork and it never worked. There's really no signs that tell you if you'll be successful or not, you just try it out and see how it works for you.

.Satan - January 13, 2012, 1:03 am
I love your tutorials! keep up the amazing work bro, forums usally have protection against that kind of stuff but some stuff like free image upload scripts im pretty sure wouldnt

-DownFall - January 13, 2012, 1:10 am
(Jan 13, 2012 02:03 AM)Snow Wrote: [\[CITE\]](#) I love your tutorials! keep up the amazing work bro, forums usally have protection against that kind of stuff but some stuff like free image upload scripts im pretty sure wouldnt
Thanks for the feedback, it's the appreciative users like you that I make tuts for. Odds are of this working on a forum are small. Though I DID shell around 8 sites in an hour doing this, with that dork alone. Sorry about the video quality, I tried about 5 screen recorders before I gave up and used that

crappy one. Added this to my mega-thread too, and fixed the images.
Anything else I should add?

Dead_Code - January 13, 2012, 1:13 am

nice and good work for you (^_^)/

.Satan - January 13, 2012, 1:30 am

Here are some more dorks for everyone, Downfall you can add these to the main post if you would like

```
"Powered By JAKCMS"  
inurl:"wp-content/plugins/1-flash-gallery"  
inurl:"user/auth/forgot"  
"Powered By Digitalus cms"
```

There are alot more but i dont want to search through every Exploit

http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=&filter_exploit_text=Arbitrary+File+Upload&filter_author=&filter_platform=0&filter_type=0&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve=

-DownFall - January 13, 2012, 2:16 am

(Jan 13, 2012 02:30 AM)Snow Wrote: [\[CITE\]](#) Here are some more dorks for everyone, Downfall you can add these to the main post if you would like

```
"Powered By JAKCMS"  
inurl:"wp-content/plugins/1-flash-gallery"  
inurl:"user/auth/forgot"  
"Powered By Digitalus cms"
```

There are alot more but i dont want to search through every Exploit

http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=&filter_exploit_text=Arbitrary+File+Upload&filter_author=&filter_platform=0&filter_type=0&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve=

Thanks, these are just a few examples, there's no limit to creativity :3

HaxOr? - January 13, 2012, 6:20 am

I always jizz on your tutorials.
Nice job mate. :)

Sql Ruined My life - January 13, 2012, 6:21 am

<3 you DOWNFALL „Great As always.. Your tutorials are SO great And awesome. I had a Newfolder in my PC "DOWNFALL'S TUTORIALS" where all your tutorials are saved ? „loved each and every tutorial of yours ?

Prominent - January 13, 2012, 6:49 am

I jizzed a hundred times more than haxor on this one.

NaKiMiJasi????????????? - January 13, 2012, 7:12 am

nice TUT mate keep up the good work ... xD!

Hooded Robin - January 13, 2012, 7:31 am

Another nice tutroial DownFall, great share!

PS - My camtasia died too, but im working on finding a way to wipe registry clean so we can re-install will let you know if I get it working properly...

-DownFall - January 13, 2012, 2:51 pm

Thanks for all the feedback everyone! If you find a way to get our trials working again hit me up ^^

.Satan - January 13, 2012, 4:27 pm

(Jan 13, 2012 08:31 AM)Hooded Robin Wrote: [\[CITE\]](#) Another nice tutroial DownFall, great share!

PS - My camtasia died too, but im working on finding a way to wipe registry clean so we can re-install will let you know if I get it working properly...

CamStudio is a good free alternative <http://camstudio.org/>

it has all the basic features you need

-DownFall - January 13, 2012, 4:29 pm

(Jan 13, 2012 05:27 PM)Snow Wrote: [\[CITE\]](#) CamStudio is a good free alternative

<http://camstudio.org/>

it has all the basic features you need

Tried it out, and it lagged like hell. Plus it didn't record sound, and when I uploaded one of the videos to youtube the quality was so horrible, you couldn't even read anything.

Hooded Robin - January 13, 2012, 4:33 pm

I use it as an alternative but it doesnt even come close to the detail and customizability of camtasia. Not even close...

-DownFall - January 13, 2012, 4:36 pm

The main page is already defaced, I knew this site would get raped lol.

cheatson - January 13, 2012, 7:04 pm

ed as also deserves views along side the other one posted today on the same subject. Both these tuts were good, for completeness; other things to try are making a real image and putting your php code in the header of the file, uploading it as whatever.php or whatever.php;.jpg bypasses serverside fingerprinting that isn't fooled by the mere changing of the extension. Also, uploading a modified .htaccess file that allows php extension or instructs the processing of other extensions to be treated as php would be the next step if these don't work.

dude2410 - January 13, 2012, 7:15 pm

damn, book-marked, thanks for the shells as well, and feel free to post more ttus, I've been reading almost all of yours, they're very easy to understand and follow.

-DownFall - January 13, 2012, 7:15 pm

(Jan 13, 2012 08:04 PM)cheatson Wrote: [\[CITE\]](#) ed as also deserves views along side the other one posted today on the same subject. Both these tuts were good, for completeness; other things to try are making a real image and putting your php code in the header of the file, uploading it as whatever.php or whatever.php;.jpg bypasses serverside fingerprinting that isn't fooled by the mere changing of the extension. Also, uploading a modified .htaccess file that allows php extension or instructs the processing of other extensions to be treated as php would be the next step if these don't work.

Nice tips, thanks a lot cheatson! Never tried either of these methods.

IDrinkMooMooMilk - January 15, 2012, 11:26 am

(Jan 13, 2012 03:51 PM)-DownFall Wrote: [\[CITE\]](#) Thanks for all the feedback everyone! If you find a way to get our trials working again hit me up ^^

Damn nice tutorial mate :-)

Also here's another dork:

Code inurl:.php "Please wait while the file is uploaded, it may take several minutes depending by the size of the file and by your internet bandwidth."

-DownFall - January 17, 2012, 11:16 am

(Jan 15, 2012 12:26 PM)IDrinkMooMooMilk Wrote: [\[CITE\]](#) Damn nice tutorial mate :-)

Also here's another dork:

Code inurl:.php "Please wait while the file is uploaded, it may take several minutes depending by the size of the file and by your internet bandwidth."

Thanks for the reply, and for the dork! Comes up with quite a few results actually..

K4M1N4 - January 18, 2012, 10:56 am

What is there not to love? Nothing!

I love your tutorials -Downfall, they work wonders!

gatopardos - January 18, 2012, 11:27 am

Nice tut .. old skool! ;) they used it in facebook before it got patched lol..

Oh btw thats RFI

Quote:Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

Code execution on the web server

Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS).

Denial of Service (DoS)

Data Theft/Manipulation

bad - February 11, 2012, 10:22 am

One word to describe Ur thread!! Awesome !! ;)

Sw1x - February 11, 2012, 1:28 pm

One of HF more HQ distributors, never leave us!

TeslaHack - February 11, 2012, 5:33 pm

Great tutorial very detailed :).
.
.
.
.

.

..

-DownFall - February 12, 2012, 7:05 am

(Feb 11, 2012 02:28 PM)Sw1x Wrote: [\[CITE\]](#) One of HF more HQ distributors, never leave us!
Never say never, I might get my life back sometime soon lol, no joke.
Thanks though man, means a lot to me.

Sw1x - February 16, 2012, 1:33 pm

(Feb 12, 2012 08:05 AM)-DownFall Wrote: [\[CITE\]](#) Never say never, I might get my life back
sometime soon lol, no joke.
Thanks though man, means a lot to me.
No problem, I just want to be polite so you don't think that we don't care about your threads. :)

geuks - June 8, 2012, 6:42 pm

Bro, it's my exploit ..
<http://pastebin.com/xUFzuAW2>

look the date ..

And thanks for the tuto.

-DownFall - June 30, 2012, 1:56 pm

(Jun 8, 2012 06:42 PM)geuks Wrote: [\[CITE\]](#) Bro, it's my exploit ..
<http://pastebin.com/xUFzuAW2>

look the date ..

And thanks for the tuto.

Not really, and even if it was, all I did was make a tutorial on it. Thanks anyways though ^.^

leizhiyuanxy - December 29, 2012, 5:51 pm

download link is bad ..and can't download to study ..

N3p BoY - December 30, 2012, 8:08 am

Nice tutorial bro :)
i learned many from your tutorial

cheakyjay - September 17, 2013, 4:37 pm

Every time i do this my tamper data just freezez is there any solution for this?

-Cheakyjay ?

w3areanonymous - October 28, 2013, 1:18 pm

Your tutorials are the best. awesome job bro :) One question so , the Tamper-data is used to upload
or your using a default PHP script to do that?

-DownFall - October 28, 2013, 1:40 pm

(Oct 28, 2013 01:18 PM)w3areanonymous Wrote: [\[CITE\]](#) Your tutorials are the best. awesome job
bro :) One question so , the Tamper-data is used to upload or your using a default PHP script to do
that?

Tamper Data is only used to change the POST data, tricking the webserver into thinking the shell is
still an image. The uploading is all done by the server, that's their faulty upload script. Thanks again

for your opinions and feedback on my threads, it's greatly appreciated.

Driverfury - *August 18, 2015, 6:30 am*

Does it work on this forum when you upload an image? A good question...

Th3PonyWizard - *August 18, 2015, 7:31 am*

(Aug 18, 2015 06:30 AM)Driverfury Wrote: [\[CITE\]](#) Does it work on this forum when you upload an image? A good question...Use your head for a minute ?

Learner Boy - *August 18, 2015, 10:50 am*

Nice Tutorial Mate.

Keep it up

takmenarik - *August 22, 2015, 12:36 am*

Its amazing brother for noob like me .. thanks ?

XxTheHackerxX - *August 23, 2015, 6:31 pm*

Nice tutorial. Keep up the great work! :)

Medicinal - *August 23, 2015, 6:32 pm*

This is just an amazing tutorial thanks for this!

AURUM - *August 24, 2015, 11:45 pm*

Thank you for sharing and HQ tut.

Thanks, OP!

telefoon - *August 25, 2015, 7:23 am*

Thanks for the reply, and for the dork!