

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How To Upload A Shell \[/Tutorial\]](#)

SIM-1241186 - December 22, 2013, 11:27 am

I'm bored, and feel like making a tutorial.

This one will teach you how to upload a shell to a server using the most common method.

Note: It is possible to spawn a shell using SQL Injection, but the method is very rare. This tutorial will not cover that method, but you can read it here.

Credits to HaxOr?;

<https://hackforums.net/showthread.php?tid=3806775>

Now without further adue;

What is a shell?

Code A backdoor shell is a malicious piece of code (e.g. PHP, Python, Ruby) that can be uploaded to a site to gain access to files stored on that site. Once it is uploaded, the hacker can use it to edit, delete, or download any files on the site, or upload their own.

Source:

http://en.wikipedia.org/wiki/Backdoor_Shell

Most commonly, shells are PHP. But you can find ASP shells, CGI, etc.

This tutorial will assume you've already done some post-exploitation. That you've done some SQL Injection, or XSS / whatever other method, and you have access to the most common place to upload a shell; administration panel.

First, we need to find the admin panel of our site.

There are lot's of admin scanning tools you can use.

As garbage as Havij is, it has a half decent admin scanner, which you can customize and add more appendings to.

There's some free web based ones online as well;

<http://y-shahinzadeh.ir/af/>

I will use this site for example:

www.artemisiabb.it

Our administration page is located at;

www.artemisiabb.it/login.php (In this case it's just a normal login with administrator info, and redirects us to admin panel).

After logging in, we look for any place we can upload an image / file.

Now for the different methods to upload a shell:

Method #1 - Straightforward:

Always try uploading as shell.php first. This could save you a lot of time. If they don't have any filtering in place, you can get away with uploading a .php script through an image uploader.

Now if you're lucky, you can right click an image, copy image location, and try to view the directory in which images are being uploaded to. This makes it much easier for finding your shell.

In this case, we don't have it that easy.

First we navigate to where the content is being placed;

<http://www.artemisiabb.it/camere.php>

I named my shell "1" so, we see a "1" on the page. We click it.

<http://www.artemisiabb.it/camera.php?id=49>

Now we can view page source, and find our shell;

Success! we have our shell:

<http://www.artemisiabb.it/uploads/camere/20131222194029.php>

Method #2 - Trickery:

Okay, let's be honest. Method #1 is just a quick way to push aside what's most unlikely to work. But we're not at a loss yet.

Image uploading scripts expect, well, images. Often times you can upload as shell.php.jpg - this suffices the .jpg check, and so your file gets uploaded. When you navigate to it, sometimes the server will execute it as .php and ignore the trailing .jpg

Let's see if it works here;

<http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg>

Code The image <http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg> can not be displayed because it contains errors.

Damn. This method only works sometimes, but it's worth a shot.

Screw this site. I want to give you guys a working example. So let's try another site;

<http://www.55communityguide.com/includes/editor/image.php>

Success!

http://www.55communityguide.com/upload/editor_files/shell.php.jpg

Now you may run into another problem, some uploaders are picky, and want your images to be specific dimensions! otherwise, they reject.

Luckily, we have a tool we can use to workaround that. It's called "edjpgcom" - you can Google for it, and download.

Let's say our sites upload script specifies that images must be 105x105 px.

So, we open up Paint, or whatever, and create a JPG file with those dimensions.

Save it as whatever.jpg

Now click & drag it over edjpgcom, and you will get a window to input code. There is a maximum number of lines, so I suggest you use a small script!

Click OK.

Next, open CMD, and type "ren whatever.jpg whatever.php.jpg"

If your site won't accept straight .php files, you can combine this trick with what you have learned so far.

Anyways, let's try to upload it. I'll upload as .php.jpg

http://www.55communityguide.com/upload/editor_files/whatever.php.jpg

Success!

Code Warning: system(): Cannot execute a blank command in
/home/retirement/public_html/upload/editor_files/whatever.php.jpg

Let's test it out;

Code http://www.55communityguide.com/upload/editor_files/whatever.php.jpg?cmd=ls -la

From here, we could use wget to get a real shell. But I'll continue on with tutorial.

Method #3 - Obfuscation & Fuckery:

There's loads of tricks you can do to get a shell up. Just be creative. Adapt your file to the situation. Filters often skip things. You can try to obfuscate your files extension.

Try uploading as the following:

.php%00.jpg - The infamous nullbyte! it will delete (in most cases) everything trailing after it.

.php;.jpg

.PhP.jpg

.php5 / .php4 / .php3 are valid php extensions, and are often overlooked in filters.

Just the tip of the ice burgh on this one. Plenty of other obfuscation methods you can use. Do some research.

Method #4 - Modifying POST Data:

Personally, I find this method to work the most often. You can use Firefox Addons such as Tamper Data, or Live HTTP Headers, to modify the POST data during the uploading process.

I will show you how to do it with Tamper Data;

- 1: Open up Tamper Data
- 2: Select our file shell.php.jpg
- 3: Click "Start Tamper"
- 4: Click "Upload File"

A dialogue box should come up, asking if you want to tamper.

Click Tamper.

You now have the POST data. Scroll through and find your file.jpg.php and rename it to .php

Click OK, and keep pressing Submit through any dialogue boxes you get.

Assuming it worked, your shell should be uploaded as .php

Method #5 - Uploading Other Files:

Sometimes you're going to run into problems where php files aren't executing properly. It might be worth your time to upload an .htaccess which treats image files as PHP.

There's lots of tricks you can do with an .htaccess - I suggest you look into it on your own, as going into it here is an entirely different subject.

If all else fails, and there's absolutely no place to upload a file, check and see if you have any place you can edit content at all. If you can edit the page source of anything, you might be able to insert your own uploading script, and from there, proceed to uploading a shell.

You can also try uploading an upload script as upload.phtml

If successful, you should be able to upload a file / shell.

This information is all available freely scattered around the internet. I just compiled it in a somewhat neat format.

If I've made a mistake, or you feel I can improve upon something, feel free to let me know. Just do so in a constructive way. "This thread is poorly written, I feel you could edit ... and ... to be more concise, and add more pictures to help people understand easier" is better than saying "This thread fucking sucks. Skid. Not helpful at all".

Hope you guys learned some new tricks!

Happy web hacking.

Merry Christmas.

lilsam - December 22, 2013, 11:36 am

OMG really HG tuts!!!! thanks bro and keep it up :)

meery Xmas

SIM-1241186 - December 22, 2013, 11:39 am

(Dec 22, 2013 12:36 PM)lilsam Wrote: [\[CITE\]](#) OMG really HG tuts!!!! thanks bro and keep it up :)

meery Xmas

Thanks. I'm going to make it look a little more pretty. This is just the rough skeleton, as I've posted it about 5 minutes ago.

Glad you liked it ?

PickledHax - December 22, 2013, 12:14 pm

Nice tut man, I'm going to bookmark this for later...

Im gone brah - December 22, 2013, 12:24 pm

Read it all your old rat (:, great guide and well written. Keep it up?

John Rogers - December 22, 2013, 12:50 pm

You should make the title more jazzy, like "Top-notch methods of evading upload script filters".

Also, you forgot to scrub this bit out on one of your images, REMOVED lol:

[img]dicks[/img]

SIM-1241186 - December 22, 2013, 1:16 pm

(Dec 22, 2013 01:50 PM)John Rogers Wrote: [\[CITE\]](#) You should make the title more jazzy, like "Top-notch methods of evading upload script filters".

It's not really top notch or anything. All of this information can be found scattered around the internet. I've just compiled it. And thanks for pointing out my little error. I've sent you a PM.

edit: thanks

133720 - December 22, 2013, 6:13 pm

Thanks for the great tut.

Good man keep it up

SIM-1241186 - December 23, 2013, 3:17 pm

(Dec 22, 2013 07:13 PM)133720 Wrote: [\[CITE\]](#) Thanks for the great tut.

Good man keep it up

Thanks. We have so many of these but most only go into one method, or just show you quickly how to do it with tamper data.

t.pro - December 23, 2013, 5:04 pm

very nice compiling - thx for sharing my friend!

Atrocious? - December 23, 2013, 6:33 pm

You can add this in method #3 :)

- 1.shell.php.
- 2.shell.php#
- 3.shell.php.pjpeg
- 4.shell.php4
- 5.shell.php5
- 6.shell.php?

SIM-1980240 - December 23, 2013, 6:37 pm

Wow thanks for this! I already know how to do this, but I'll give this a bookmark for later. Looks like a good tutorial. :)

Anon?M ID - December 23, 2013, 6:41 pm

i'm so sad edjpgcom can't run on my windows 8 :(

[\[img\]http://s5.postimg.org/w1cr9czmf/screenshot_284.png\[/img\]](http://s5.postimg.org/w1cr9czmf/screenshot_284.png)

SIM-1241186 - December 23, 2013, 9:35 pm

(Dec 23, 2013 07:41 PM)Anon?M ID Wrote: [\[CITE\]](#) i'm so sad edjpgcom can't run on my windows 8 :(

[\[img\]http://s5.postimg.org/w1cr9czmf/screenshot_284.png\[/img\]](http://s5.postimg.org/w1cr9czmf/screenshot_284.png)

Try running it in a Windows 7 Virtual Machine? If it's really that important, you could just run it on that and create your file.

Anon?M ID - December 23, 2013, 10:53 pm

i tried it. but still not working :/
damnit.

cheatson - December 24, 2013, 4:15 am

(Dec 23, 2013 11:53 PM)Anon?M ID Wrote: [\[CITE\]](#) i tried it. but still not working :/
damnit.

EXIFPilot! <http://hackers2devnull.blogspot.co.uk/2013/05/how-to-shell-server-via-image-upload.html>
Nice tutorial, easy to follow.

Anon?M ID - December 24, 2013, 4:36 am

(Dec 24, 2013 05:15 AM)cheatson Wrote: [\[CITE\]](#) EXIFPilot!

<http://hackers2devnull.blogspot.co.uk/2013/05/how-to-shell-server-via-image-upload.html>

Nice tutorial, easy to follow.
thank you. i'm going to check it out.
cheers

Shiiza - December 24, 2013, 5:48 am

GOOD work Bro!

Keep up the gud work.

-KillerHawx

Cyllon - December 24, 2013, 5:59 am

Well written tutorial, thanks for posting and taking your time to make it ?

TDK - December 25, 2013, 8:32 am

Thank you for this tutorial, man. ;)

.vemla - December 25, 2013, 9:18 am

Well explained, buddy.
HQ Tutorial.

Take care all.
Merry Christmas.
Cheers! ?

Ascendon - December 25, 2013, 9:22 am

R.I.P man :'(
You will be missed.
April 2012 - 25 December 2013

.vemla - December 25, 2013, 9:25 am

(Dec 25, 2013 10:22 AM)Ascendon Wrote: [\[CITE\]](#) R.I.P man :'(
You will be missed.

April 2012 - 25 December 2013Is it confirmed yet?
Did I miss anything? ?

Ascendon - December 25, 2013, 9:27 am

He is committing suicide today. He hasn't replied in a while. I guess it is.

Guwop - December 25, 2013, 11:42 am

Thanks now i know how to upload a shell but I think you should include places to get shells.

pwngekill - December 27, 2013, 11:56 am

Wow this is a really good tutorial keep it up

If you didn't kill yourself.

vFainted - December 27, 2013, 12:54 pm

Very Nice I'm Going To bookmark This!.

=)

FearTheBob - December 27, 2013, 1:38 pm

Great tutorial will be pointing everyone to this from now on.

adnanalimk - January 6, 2014, 8:21 pm

very nice tutorial bro keep it ip thnxx

jacknax - January 7, 2014, 12:46 am

Its a very nice tut about uploading shell, thanks brother, & keep posting...

Joshua174 - January 7, 2014, 6:38 am

Good tutorial but all of these "attacks" are very easy to prevent and if the web developpee was smart he would just disable the php engine with in upload directories with htaccess.

supermanozos - February 24, 2014, 2:58 am

@ hackforumspang

Great tutorial. Thanks for sharing. ^^

FFHE - February 24, 2014, 7:44 am

(Dec 22, 2013 12:27 PM)hackforumspang Wrote: [\[CITE\]](#) Source:

http://en.wikipedia.org/wiki/Backdoor_Shell

Jesus christ this article blows. I might be arsed to actually edit it because it's so bad.

Opheus - February 24, 2014, 1:46 pm

(Dec 22, 2013 12:27 PM)hackforumspang Wrote: [\[CITE\]](#) I'm bored, and feel like making a tutorial.

This one will teach you how to upload a shell to a server using the most common method.

Note: It is possible to spawn a shell using SQL Injection, but the method is very rare. This tutorial will not cover that method, but you can read it here.

Credits to HaxOr?;

<https://hackforums.net/showthread.php?tid=3806775>

Now without further adue;

What is a shell?

Code A backdoor shell is a malicious piece of code (e.g. PHP, Python, Ruby) that can be uploaded to a site to gain access to files stored on that site. Once it is uploaded, the hacker can use it to edit, delete, or download any files on the site, or upload their own.

Source:

http://en.wikipedia.org/wiki/Backdoor_Shell

Most commonly, shells are PHP. But you can find ASP shells, CGI, etc.

This tutorial will assume you've already done some post-exploitation. That you've done some SQL Injection, or XSS / whatever other method, and you have access to the most common place to upload a shell; administration panel.

First, we need to find the admin panel of our site.

There are lot's of admin scanning tools you can use.

As garbage as Havij is, it has a half decent admin scanner, which you can customize and add more appendings to.

There's some free web based ones online as well;

<http://y-shahinzadeh.ir/af/>

I will use this site for example:

www.artemisiabb.it

Our administration page is located at;

www.artemisiabb.it/login.php (In this case it's just a normal login with administrator info, and redirects us to admin panel).

After logging in, we look for any place we can upload an image / file.

Now for the different methods to upload a shell:

Method #1 - Straightforward:

Always try uploading as shell.php first. This could save you a lot of time. If they don't have any filtering in place, you can get away with uploading a .php script through an image uploader.

Now if you're lucky, you can right click an image, copy image location, and try to view the directory in which images are being uploaded to. This makes it much easier for finding your shell.

In this case, we don't have it that easy.

First we navigate to where the content is being placed;

<http://www.artemisiabb.it/camere.php>

I named my shell "1" so, we see a "1" on the page. We click it.

<http://www.artemisiabb.it/camera.php?id=49>

Now we can view page source, and find our shell;

Success! we have our shell:

<http://www.artemisiabb.it/uploads/camere/20131222194029.php>

Method #2 - Trickery:

Okay, let's be honest. Method #1 is just a quick way to push aside what's most unlikely to work. But we're not at a loss yet.

Image uploading scripts expect, well, images. Often times you can upload as shell.php.jpg - this suffices the .jpg check, and so your file gets uploaded. When you navigate to it, sometimes the server will execute it as .php and ignore the trailing .jpg

Let's see if it works here;

<http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg>

Code The image <http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg> can not be displayed because it contains errors.

Damn. This method only works sometimes, but it's worth a shot.

Screw this site. I want to give you guys a working example. So let's try another site;

<http://www.55communityguide.com/includes/editor/image.php>

Success!

http://www.55communityguide.com/upload/editor_files/shell.php.jpg

Now you may run into another problem, some uploaders are picky, and want your images to be specific dimensions! otherwise, they reject.

Luckily, we have a tool we can use to workaround that. It's called "edjpgcom" - you can Google for it, and download.

Let's say our sites upload script specifies that images must be 105x105 px.

So, we open up Paint, or whatever, and create a JPG file with those dimensions.

Save it as whatever.jpg

Now click & drag it over edjpgcom, and you will get a window to input code. There is a maximum number of lines, so I suggest you use a small script!

Click OK.

Next, open CMD, and type "ren whatever.jpg whatever.php.jpg"

If your site won't accept straight .php files, you can combine this trick with what you have learned so far.

Anyways, let's try to upload it. I'll upload as .php.jpg

http://www.55communityguide.com/upload/editor_files/whatever.php.jpg

Success!

Code Warning: system(): Cannot execute a blank command in /home/retirement/public_html/upload/editor_files/whatever.php.jpg

Let's test it out;

Code http://www.55communityguide.com/upload/editor_files/whatever.php.jpg?cmd=ls -la

From here, we could use wget to get a real shell. But I'll continue on with tutorial.

Method #3 - Obfuscation & Fuckery:

There's loads of tricks you can do to get a shell up. Just be creative. Adapt your file to the situation. Filters often skip things. You can try to obfuscate your files extension.

Try uploading as the following:

.php%00.jpg - The infamous nullbyte! it will delete (in most cases) everything trailing after it.

.php;.jpg

.PhP.jpg

.php5 / .php4 / .php3 are valid php extensions, and are often overlooked in filters.

Just the tip of the ice burgh on this one. Plenty of other obfuscation methods you can use. Do some research.

Method #4 - Modifying POST Data:

Personally, I find this method to work the most often. You can use Firefox Addons such as Tamper Data, or Live HTTP Headers, to modify the POST data during the uploading process.

I will show you how to do it with Tamper Data;

- 1: Open up Tamper Data
- 2: Select our file shell.php.jpg
- 3: Click "Start Tamper"
- 4: Click "Upload File"

A dialogue box should come up, asking if you want to tamper.

Click Tamper.

You now have the POST data. Scroll through and find your file.jpg.php and rename it to .php

Click OK, and keep pressing Submit through any dialogue boxes you get.

Assuming it worked, your shell should be uploaded as .php

Method #5 - Uploading Other Files:

Sometimes you're going to run into problems where php files aren't executing properly. It might be worth your time to upload an .htaccess which treats image files as PHP.

There's lots of tricks you can do with an .htaccess - I suggest you look into it on your own, as going into it here is an entirely different subject.

If all else fails, and there's absolutely no place to upload a file, check and see if you have any place you can edit content at all. If you can edit the page source of anything, you might be able to insert your own uploading script, and from there, proceed to uploading a shell.

You can also try uploading an upload script as upload.phtml

If successful, you should be able to upload a file / shell.

This information is all available freely scattered around the internet. I just compiled it in a somewhat

neat format.

If I've made a mistake, or you feel I can improve upon something, feel free to let me know. Just do so in a constructive way. "This thread is poorly written, I feel you could edit ... and ... to be more concise, and add more pictures to help people understand easier" is better than saying "This thread fucking sucks. Skid. Not helpful at all".

Hope you guys learned some new tricks!

Happy web hacking.

Merry Christmas.

Trying to use tamper data
in a Joomla admin
when ever i click tamper my mozilla hangs
besides this places thats f*ckd up
every other tampering. dont knw what to do
thinkin

SIM-1241186 - February 24, 2014, 4:17 pm

(Jan 7, 2014 07:38 AM)Joshua174 Wrote: [\[CITE\]](#) Good tutorial but all of these "attacks" are very easy to prevent and if the web developpee was smart he would just disable the php engine with in upload directorys with htaccess.

SQL Injection is easy to prevent.

Does that stop anyone from conducting it on poorly sanitized user input?

Nope.

I've got nearly 90-100 shells up.

Admins are dumb.

Verdande - February 24, 2014, 4:18 pm

seems like you put a lot of work into this, thanks for sharing!

MechWarrior67 - February 24, 2014, 5:28 pm

How do you spoof the shell extension? Do you just change it manually like shell.php -> shell.php.jpg?

SIM-1241186 - February 24, 2014, 5:40 pm

(Feb 24, 2014 02:46 PM)Opheus Wrote: [\[CITE\]](#) Trying to use tamper data
in a Joomla admin

when ever i click tamper my mozilla hangs
besides this places thats f*ckd up
every other tampering. dont knw what to do
thinkin

Was it entirely necessary to quote the whole fucking post?

There's other ways to shell Joomla.

smartwater - February 24, 2014, 5:41 pm

(Dec 22, 2013 12:27 PM)hackforumspang Wrote: [\[CITE\]](#) I'm bored, and feel like making a tutorial.

This one will teach you how to upload a shell to a server using the most common method.

Note: It is possible to spawn a shell using SQL Injection, but the method is very rare. This tutorial

will not cover that method, but you can read it here.

Credits to HaxOr?;

<https://hackforums.net/showthread.php?tid=3806775>

Now without further adue;

What is a shell?

Code A backdoor shell is a malicious piece of code (e.g. PHP, Python, Ruby) that can be uploaded to a site to gain access to files stored on that site. Once it is uploaded, the hacker can use it to edit, delete, or download any files on the site, or upload their own.

Source:

http://en.wikipedia.org/wiki/Backdoor_Shell

Most commonly, shells are PHP. But you can find ASP shells, CGI, etc.

This tutorial will assume you've already done some post-exploitation. That you've done some SQL Injection, or XSS / whatever other method, and you have access to the most common place to upload a shell; administration panel.

First, we need to find the admin panel of our site.

There are lot's of admin scanning tools you can use.

As garbage as Havij is, it has a half decent admin scanner, which you can customize and add more appendings to.

There's some free web based ones online as well;

<http://y-shahinzadeh.ir/af/>

I will use this site for example:

www.artemisiabb.it

Our administration page is located at;

www.artemisiabb.it/login.php (In this case it's just a normal login with administrator info, and redirects us to admin panel).

After logging in, we look for any place we can upload an image / file.

Now for the different methods to upload a shell:

Method #1 - Straightforward:

Always try uploading as shell.php first. This could save you a lot of time. If they don't have any filtering in place, you can get away with uploading a .php script through an image uploader.

Now if you're lucky, you can right click an image, copy image location, and try to view the directory in which images are being uploaded to. This makes it much easier for finding your shell.

In this case, we don't have it that easy.

First we navigate to where the content is being placed;

<http://www.artemisiabb.it/camere.php>

I named my shell "1" so, we see a "1" on the page. We click it.

<http://www.artemisiabb.it/camera.php?id=49>

Now we can view page source, and find our shell;

Success! we have our shell:

<http://www.artemisiabb.it/uploads/camere/20131222194029.php>

Method #2 - Trickery:

Okay, let's be honest. Method #1 is just a quick way to push aside what's most unlikely to work. But we're not at a loss yet.

Image uploading scripts expect, well, images. Often times you can upload as shell.php.jpg - this suffices the .jpg check, and so your file gets uploaded. When you navigate to it, sometimes the server will execute it as .php and ignore the trailing .jpg

Let's see if it works here;

<http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg>

Code The image <http://www.artemisiabb.it/uploads/camere/20131222194901.php.jpg> can not be displayed because it contains errors.

Damn. This method only works sometimes, but it's worth a shot.

Screw this site. I want to give you guys a working example. So let's try another site;

<http://www.55communityguide.com/includes/editor/image.php>

Success!

http://www.55communityguide.com/upload/editor_files/shell.php.jpg

Now you may run into another problem, some uploaders are picky, and want your images to be specific dimensions! otherwise, they reject.

Luckily, we have a tool we can use to workaround that. It's called "edjpgcom" - you can Google for it, and download.

Let's say our sites upload script specifies that images must be 105x105 px.

So, we open up Paint, or whatever, and create a JPG file with those dimensions.

Save it as whatever.jpg

Now click & drag it over edjpgcom, and you will get a window to input code. There is a maximum number of lines, so I suggest you use a small script!

Click OK.

Next, open CMD, and type "ren whatever.jpg whatever.php.jpg"

If your site won't accept straight .php files, you can combine this trick with what you have learned so

far.

Anyways, let's try to upload it. I'll upload as .php.jpg

http://www.55communityguide.com/upload/editor_files/whatever.php.jpg

Success!

Code Warning: system(): Cannot execute a blank command in
/home/retirement/public_html/upload/editor_files/whatever.php.jpg

Let's test it out;

Code http://www.55communityguide.com/upload/editor_files/whatever.php.jpg?cmd=ls -la

From here, we could use wget to get a real shell. But I'll continue on with tutorial.

Method #3 - Obfuscation & Fuckery:

There's loads of tricks you can do to get a shell up. Just be creative. Adapt your file to the situation. Filters often skip things. You can try to obfuscate your files extension.

Try uploading as the following:

.php%00.jpg - The infamous nullbyte! it will delete (in most cases) everything trailing after it.

.php;.jpg

.PhP.jpg

.php5 / .php4 / .php3 are valid php extensions, and are often overlooked in filters.

Just the tip of the ice burgh on this one. Plenty of other obfuscation methods you can use. Do some research.

Method #4 - Modifying POST Data:

Personally, I find this method to work the most often. You can use Firefox Addons such as Tamper Data, or Live HTTP Headers, to modify the POST data during the uploading process.

I will show you how to do it with Tamper Data;

- 1: Open up Tamper Data
- 2: Select our file shell.php.jpg
- 3: Click "Start Tamper"
- 4: Click "Upload File"

A dialogue box should come up, asking if you want to tamper.

Click Tamper.

You now have the POST data. Scroll through and find your file.jpg.php and rename it to .php

Click OK, and keep pressing Submit through any dialogue boxes you get.

Assuming it worked, your shell should be uploaded as .php

Method #5 - Uploading Other Files:

Sometimes you're going to run into problems where php files aren't executing properly. It might be worth your time to upload an .htaccess which treats image files as PHP.

There's lots of tricks you can do with an .htaccess - I suggest you look into it on your own, as going into it here is an entirely different subject.

If all else fails, and there's absolutely no place to upload a file, check and see if you have any place you can edit content at all. If you can edit the page source of anything, you might be able to insert your own uploading script, and from there, proceed to uploading a shell.

You can also try uploading an upload script as upload.phtml
If successful, you should be able to upload a file / shell.

This information is all available freely scattered around the internet. I just compiled it in a somewhat neat format.

If I've made a mistake, or you feel I can improve upon something, feel free to let me know. Just do so in a constructive way. "This thread is poorly written, I feel you could edit ... and ... to be more concise, and add more pictures to help people understand easier" is better than saying "This thread fucking sucks. Skid. Not helpful at all".

Hope you guys learned some new tricks!

Happy web hacking.

Merry Christmas.was it paint you used to draw that image? im stuck on this part. thank you.

SIM-1241186 - February 24, 2014, 6:03 pm

(Feb 24, 2014 06:28 PM)MechWarrior67 Wrote: [\[CITE\]](#) How do you spoof the shell extension? Do you just change it manually like shell.php -> shell.php.jpg?

You can do it manually if you have hide file extensions for known file types turned off.

Personally, I just use CMD;
ren shell.php shell.php.jpg

MechWarrior67 - February 24, 2014, 9:29 pm

(Feb 24, 2014 07:03 PM)hackforumspang Wrote: [\[CITE\]](#) You can do it manually if you have hide file extensions for known file types turned off.

Personally, I just use CMD;
ren shell.php shell.php.jpg

Thank you for the reply, very much appreciated. Also thanks for the tutorial, I hope to see more ?

SIM-1241186 - February 24, 2014, 9:58 pm

(Feb 24, 2014 10:29 PM)MechWarrior67 Wrote: [\[CITE\]](#) Thank you for the reply, very much appreciated. Also thanks for the tutorial, I hope to see more ?

You're welcome.

It's nice to see people actually come back to the thread to see if their question was answered, rather than just ask and forget they even posted.

smartwater - February 24, 2014, 10:10 pm

(Feb 24, 2014 10:58 PM)hackforumspang Wrote: [\[CITE\]](#) You're welcome.

It's nice to see people actually come back to the thread to see if their question was answered, rather than just ask and forget they even posted.I'm very offended, you haven't answered my question

also, why are you impersonating me?

SIM-1241186 - February 25, 2014, 12:04 am

(Feb 24, 2014 11:10 PM)smartwater Wrote: [\[CITE\]](#) I'm very offended, you haven't answered my question

also, why are you impersonating me?

I seriously don't understand your mindset.

You PM me asking for homosexual innuendo, I repeatedly tell you that I've nothing against others sexual preferences, however as my own personal preference I am not interested.

I add you to my ignore list, and you make some trash thread pretending to be me asking for help with Havij.

Now you come here?

What in the hell are you trying to accomplish?

I've been around this forum longer than you. Lots of users have seen my replies, and tutorials, and know who I am in this section.

If you think for a second replicating my avatar, and saying my name on threads is going to make people believe you're me, you have some serious logic issues.

You didn't even copy my signature.

You don't even have the same fucking reputation or warning level.

Fuck off, or you're getting a report.

I was originally too fucking lazy to get around to doing it, I also don't like bothering with that fucking shit. But you're starting to piss me off now.

smartwater - February 25, 2014, 12:05 am

(Feb 25, 2014 01:04 AM)hackforumspang Wrote: [\[CITE\]](#) I seriously don't understand your mindset.

You PM me asking for homosexual innuendo, I repeatedly tell you that I've nothing against others sexual preferences, however as my own personal preference I am not interested.

I add you to my ignore list, and you make some trash thread pretending to be me asking for help with Havij.

Now you come here?

What in the hell are you trying to accomplish?

I've been around this forum longer than you. Lots of users have seen my replies, and tutorials, and know who I am in this section.

Fuck off, or you're getting a report.

I was originally too fucking lazy to get around to doing it, I also don't like bothering with that fucking shit. But you're starting to piss me off now. Dude all I want is for you to answer my question on the previous page

Thanks.

SIM-1241186 - February 25, 2014, 12:12 am

(Feb 25, 2014 01:05 AM)smartwater Wrote: [\[CITE\]](#) Dude all I want is for you to answer my question on the previous page

Thanks.

It was paint.

However, off-topic, I'm pretty sure I know exactly who you are.

There's only one sadistic retard stupid enough to talk the way you do.

I definitely know who this is.
Fuck off.

smartwater - February 25, 2014, 12:13 am

(Feb 25, 2014 01:12 AM)hackforumspang Wrote: [\[CITE\]](#) It was paint.
However, off-topic, I'm pretty sure I know exactly who you are.
There's only one sadistic retard stupid enough to talk the way you do.
I definitely know who this is.
Fuck off.I don't have paint to make a drawing... does that mean I can't upload a shell using that method?? Thanks.

SIM-1241186 - February 25, 2014, 12:16 am

(Feb 25, 2014 01:13 AM)smartwater Wrote: [\[CITE\]](#) I don't have paint to make a drawing... does that mean I can't upload a shell using that method?? Thanks.
Pretty sure your names Kyle.
Anywho, getting the report out.
Sick of seeing you here.

smartwater - February 25, 2014, 12:19 am

(Feb 25, 2014 01:16 AM)hackforumspang Wrote: [\[CITE\]](#) Pretty sure your names Kyle.
Anywho, getting the report out.
Sick of seeing you here.nothing to report I'm asking real questions

can you answer the previous one?
thanks dude!

SIM-1241186 - February 25, 2014, 12:25 am

(Feb 25, 2014 01:19 AM)smartwater Wrote: [\[CITE\]](#) nothing to report I'm asking real questions

can you answer the previous one?
thanks dude!
You've been blatantly seen attempting to impersonate me.
Continuously harassing me.
Worth a report.
I'll take my chances.

Not answering any more shit from you.
The more you post the deeper hole you're getting yourself into.
Bye now.

palkarz - April 5, 2014, 1:00 am

I have wife and comming soon daughter ... but i love u :)

optimus2112 - April 5, 2014, 1:07 am

Damnt nice tutorial,keep it up and thanks mate xD

palkarz - April 5, 2014, 1:11 am

Not comp1337 ... much more is about this subject (maby u will have time and power to update it)
but its awsome starter :) and can give some nice ideas...
good work Sir

SIM-1241186 - April 5, 2014, 9:57 pm

(Apr 5, 2014 01:11 AM)palkarz Wrote: [\[CITE\]](#) Not comp1337 ... much more is about this subject (

maby u will have time and power to update it) but its awsome starter :):) and can give some nice ideas...

good work Sir

Umm... what?

Other than the compliment, I don't understand what it is you're trying to say.

Keybored - April 5, 2014, 10:21 pm

Thanks for the TUT man it really helped me out

Contender - April 6, 2014, 12:05 pm

Great tutorial thanks for sharing, you're great!

Tea. - April 6, 2014, 5:06 pm

cool writeup pang thank you for the share!

jamie45 - April 6, 2014, 5:07 pm

(Apr 5, 2014 09:57 PM)hackforumspang Wrote: [\[CITE\]](#) Umm... what?

Other than the compliment, I don't understand what it is you're trying to say. Translation:

There is more information about this subject. Maybe you will be able to update it to give us good ideas, but this is a good starter.

legend_x - April 18, 2014, 1:04 pm

Very nice and comprehensive. Keep up the good work bro.

maigel - April 18, 2014, 4:16 pm

There's some concepts in here that I hadn't thought of, thanks for the tut!

palkarz - April 18, 2014, 5:00 pm

(Dec 22, 2013 12:27 PM)hackforumspang Wrote: [\[CITE\]](#)

There's lots of tricks you can do with an .htaccess - I suggest you look into it on your own, as going into it here is an entirely different subject.

If all else fails, and there's absolutely no place to upload a file, check and see if you have any place you can edit content at all. If you can edit the page source of anything, you might be able to insert your own uploading script, and from there, proceed to uploading a shell.

Could u give some more details about those two solutions ?? Maby examples ??

HinduMonster - April 18, 2014, 6:02 pm

thank you for this, your contribution is appreciated :)

CobraEffect - May 30, 2015, 9:58 am

+ thx for sharing nice job

AnonRobot - May 30, 2015, 5:55 pm

this is pretty good

gj op this will help dem kidz <3

Culperring722 - May 30, 2015, 6:27 pm

Good tut you got here keep em coming

-RENWA- - May 31, 2015, 4:35 am

cool there is also LFI , RFI , SQL methods

JamesOG - May 31, 2015, 5:04 pm

Hey OP I find this tutorial very clear and comprehensive, really nice job. I have a question though. Is there any way around it if the image being compressed and renamed while being uploaded on the site? :) It gets renamed to user_randomhash.jpg (example: 7830650_7b4c44dbe6.jpg), and when i downloaded the compressed image again and opened it in 'edjpgcom' it gave me this comment: "CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100". I'm guessing this is the program that does that compression ? Is there any possible exploits here? tnx :)

Coffee-ass - October 3, 2017, 10:26 am

(May 31, 2015 05:04 PM)JamesOG Wrote: [\[CITE\]](#) Hey OP I find this tutorial very clear and comprehensive, really nice job. I have a question though. Is there any way around it if the image being compressed and renamed while being uploaded on the site? :) It gets renamed to user_randomhash.jpg (example: 7830650_7b4c44dbe6.jpg), and when i downloaded the compressed image again and opened it in 'edjpgcom' it gave me this comment: "CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100". I'm guessing this is the program that does that compression ? Is there any possible exploits here? tnx :)

Do you have a solution for that ?

I have found: [\[github\]/fakhrizulkifli/Defeating-PHP-GD-imagecreatefromjpeg](#)

But that don't work for me i don't know how to run the payload --', because if running of payload.php is needed is not necessary to use that exploit is ridiculous --'

I have backdoor a very very important website, successfull upload shell, but he show me a miniature of file encrypt by that same of you but me files are renamed with hash_md5
I want know the path of original files or how to exploit gd-jpeg v1.0

If anyone help me i offer Big amount in BTC \$\$\$

David Laid - October 4, 2017, 6:35 am

(Oct 3, 2017 10:26 AM)Coffee-ass Wrote: [\[CITE\]](#) Do you have a solution for that ?

I have found: [\[github\]/fakhrizulkifli/Defeating-PHP-GD-imagecreatefromjpeg](#)

But that don't work for me i don't know how to run the payload --', because if running of payload.php is needed is not necessary to use that exploit is ridiculous --'

I have backdoor a very very important website, successfull upload shell, but he show me a miniature of file encrypt by that same of you but me files are renamed with hash_md5
I want know the path of original files or how to exploit gd-jpeg v1.0

If anyone help me i offer Big amount in BTC \$\$\$

I have also very similar problem as you guys, i sucesfully uploaded shell but when i open it its renamed to "15646546.jpg" and the site says: this image is broken etc.
anyway to bypass this?