

Forum:[Hack Forums](#)

Thread: [\[TUT\]How to Upload a Shell\[PICS SOON\]](#)

ParsingError - August 30, 2010, 10:40 pm

How to Upload a Shell

First of all, when uploading a shell, you MUST be able to problem solve. Some of the techniques I have compiled in this guide aren't exactly easy for most of you.

I am separating this guide into steps, and sometimes, this won't always work. In fact, most of the time (If the coder was that bright at all), these techniques will NOT work. So don't go posting away about it not working for you on one site..

First though, you need some form of upload script. I don't care if it's a public upload script, or one off an admin page.

Step 1

First off, try the shell with the regular php extension. I've seen this work for admin panels a lot of the time, because the coder doesn't think anyone but the site admin will be messing with it.. He doesn't stop to think about security.

Step 2

If step 1 doesn't work, you're going to have to try different extensions that also execute php on most servers. These would include .php2, .php3, .php4, .php5, .phtml, .htm (rare cases), .html (rare cases), and no extension at all (rare cases). Also, you can attempt using a null to make it work.

Examples:

Code shell.php.jpg%00

shell.php.jpg;;

shell.php.jpg%;

shell.php.jpg%:

shell.php.jpg;

shell.php.jpg;%00

shell.php.jpg%00;

shell.php.jpg%00;;Step 3

Now on to step 3, it seems that step 2 didn't work for you. Sometimes, (now this is occasional), the file extensions it will accept are in the source of the page itself.. this is most common for java uploaders and similar. So to check for this, obviously view the source of the page and check it over for anything that looks like file extensions. If you do find any, you are going to want to use a tool like Firebug (Addon for Firefox), to edit the source to include the extension "php".

Step 4

Next, maybe the script is just blocking the .php, .php2, .php3, ect. scripts from being uploaded. The best way to counter-act this is to upload a .htaccess file. Go into notepad or w/e and paste this in:

Code AddType application/x-httpd-php .shell .other .jpg .gif .png .mov .pdfThen upload the shell with one of those extensions. It should execute as php even with the wierd extension.

Step 5

Last but not least, is the header modification trick. This one is a little complicated (Will add pics in a min..) To do this, you need something like the Tamper Data addon for Firefox. In this example, I'll

use that addon. What you want to do is after you attempt to send the post data, tamper the data before it sends. Then you will want to scroll through the raw data until you find the header data.. let's say our header is Application/Data... you would want to change that to something appropriate to the scripts intended purpose, like Image/Jpeg for an image upload script.

That concludes my guide for how to upload a shell for now, will add more to it later, and of course, adding pictures later as well. (Decided not to on this one) As for now, enjoy!

Shades - August 30, 2010, 10:42 pm

You know you can just add a null to the file so it executes as a PHP but the website recognizes it as a .jpg, right?

i3urn - August 31, 2010, 1:26 am

(Aug 30, 2010 10:42 PM)shadeS Wrote: [\[CITE\]](#) You know you can just add a null to the file so it executes as a PHP but the website recognizes it as a .jpg, right?

That does not all ways work most time the upload system reads past it and still puts .php on the end.

Google.com - August 31, 2010, 2:02 am

seems like a pretty epic guide. Good job

RoyalNuDeS - August 31, 2010, 3:14 am

Null Bytes are really uncommon via poison uploads mainly because the file is read in image format but considering its formatted in PHP the image itself doesn't execute, thus an error.

You can always try using other formats such as:

```
shell.php.jpg%00
shell.php.jpg;;
shell.php.jpg%;
shell.php.jpg%:
shell.php.jpg;
shell.php.jpg;%00
shell.php.jpg%00;
shell.php.jpg%00;;
```

You can also try setting up a basic ajax backdoor as a plugin and then you can execute global commands such as wget to install you're shell. Quite useful if you're doing it from the webroot directory considering it can be accessed easier.

FTP is useful and all but mput is usually unsuccessful considering it just reads it as a source, FTP clients usually help get the actual file embedded on the FTP server (once done you can access <ftp.siteName.com/shell.php>) .

The htaccess trick usually doesn't work because its standards are viewed as a simple txt file and the web server usually can't read from that and execute it (you don't just GET read/write access) .

You can always use /proc/self/environ and identify server banner information and then poison you're User Agent to a system() command and read from a wget statement to you're shell. Uncommon but it can happen.

Good tutorial bro.

koolkid - March 17, 2011, 10:41 am

<http://ankitthehacker.wordpress.com/2011/03/02/how-to-upload-a-shell/>

Mr.thinker - March 19, 2011, 4:06 am

Well Null Bytes Never Works For Me :)

sumit8510 - March 19, 2011, 4:22 am

nice tut bro.
thanks for it.

cybecomputing - April 15, 2011, 11:48 am

<http://ankitthehacker.wordpress.com/2011/03/02/how-to-upload-a-shell/>

Phizo - April 15, 2011, 11:54 am

This should be in the website hacking section.

Scavok - April 15, 2011, 12:57 pm

Thats a good guide thank you for it :)

full2softwares - October 17, 2011, 11:34 pm

I have uploaded a php shell but i cant execute them as i blv the admin has mentioned in root .htaccess that all the file uploaded in files folder with .php as extension anywhere cant be executed. I have tried uploading html file and than using .htaccess(in sub folder) to execute it as php but no success. Any help?

Techie??? - October 17, 2011, 11:40 pm

(Mar 17, 2011 10:41 AM)hackdeveto Wrote: [\[CITE\]](#)

<http://ankitthehacker.wordpress.com/2011/03/02/how-to-upload-a-shell/>

Well. This is the original link.

Anyway thanks.

ParsingError - May 28, 2013, 11:56 pm

(Oct 17, 2011 11:40 PM)Techie???

Wrote: [\[CITE\]](#) Well. This is the original link.

Anyway thanks.
Inb4 gravedig.

I am the original author. Look @ post date in OP.

benison321 - May 29, 2013, 12:27 am

thankx... for sharing.. mate...! Keep it up...

Agonised - May 29, 2013, 1:05 am

Shells ? Don't they just have nets for those now ?

JollyBean - May 29, 2013, 5:12 am

What shell is the best?
Would like to use a really good one

MajinVegeta - May 29, 2013, 8:14 am

thank you mate :)

gonna read it later, saved it to browser/favorites

decent l33t - *April 26, 2016, 8:42 pm*

i tried but not working bro