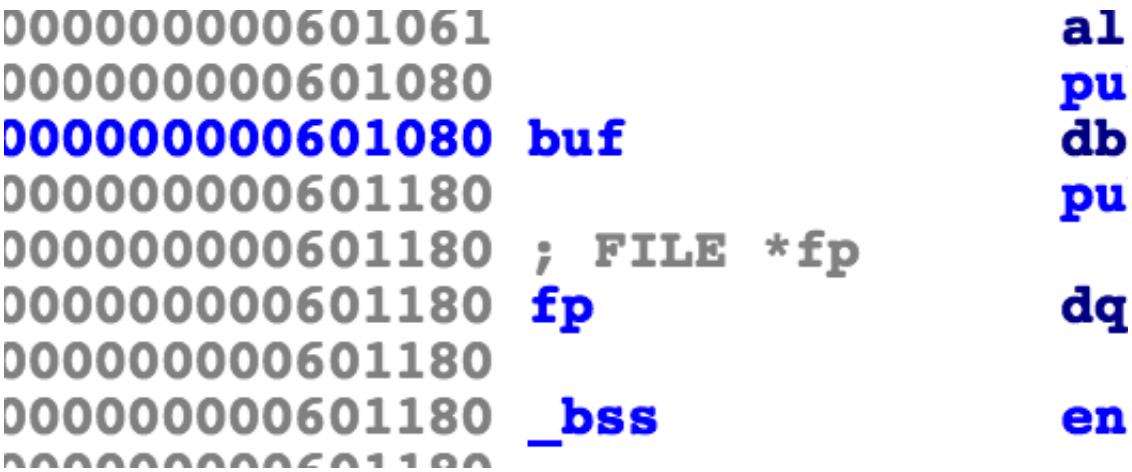
io-file

例子：example1 libc2.23

```
#include <stdio.h>
char buf[0x100]="";
FILE *fp ;
void shell(){
    system("/bin/sh");
}
int main(){
    fp = fopen("test.txt","r");
    gets(buf);
    fclose(fp);
}
```

这是一个简单的 io file 的题，这里面是伪造了一个file 然后修改了 vtable的的值 这个要先了解vtable是如何工作的。



右上图可知 我们可以通过填充buf来改写 fp指针。中间相差0x100

我们先构造一个payload

```
pay = '\0' * 100 + p64(buf_addr)
```

我们现在运行一下 是crash在了

```
 0x7f8f75bd238c <fclose+300>     cmp    r8, QWORD PTR [rdx+0x8]
```

这个位置

我们查看一下 rdx的内容是0x0 ， rdx+0x8 是一个 无效的地址 ， 于是程序就 crash掉了 。我们现在往上看一下 rdx的值是谁给的。

```
mov    edx, DWORD PTR [rbx+0x88]
```

rbx的值 是 buf_addr的地址 （同时也是fp指针指向的地址）。

现在有一个知识点就是 fp——>lock 就是 fp指向的地址+0x88 ， 当lock为0时，就可以跳过这个比较，所以我们现在要做的事情就是让他为0.（lock也是一个指针 是指向的地址的内容为0）

然后我们又构造下一个payload

。

接下来的内容请看 lowkey在xman的ppt