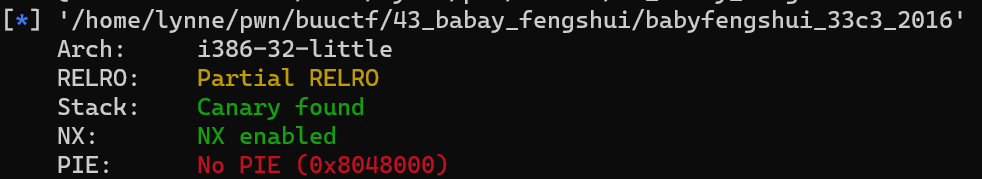
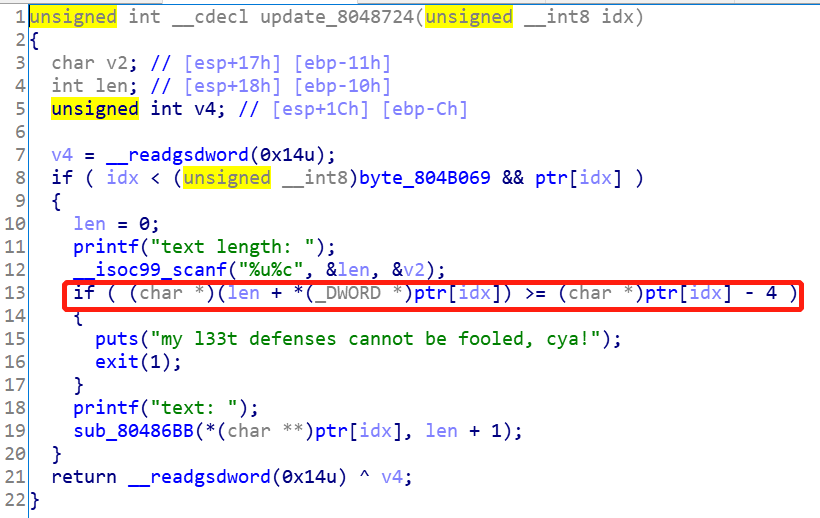
## 漏洞挖掘

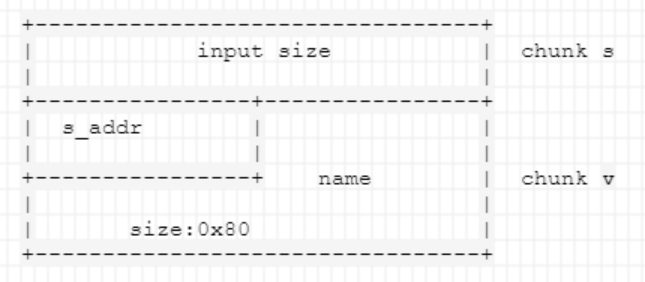


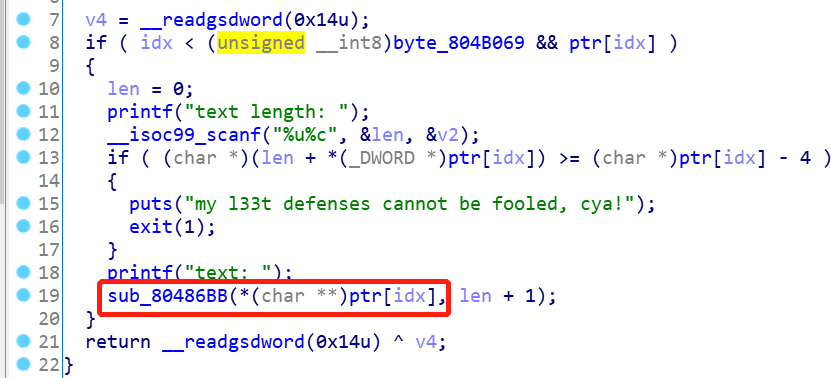
又是一个菜单题，漏洞点在这里



这个地方的校验存在问题，只判断了s的地址+input size 要低于v的地址。

需要整理一下堆的分布情况，在add的时候：





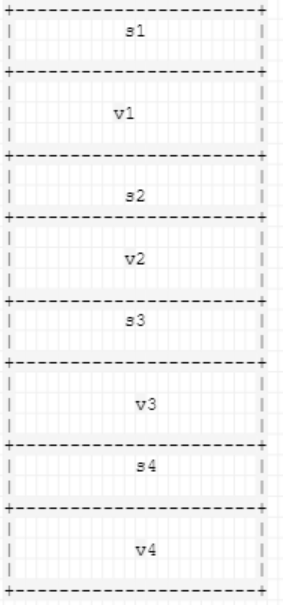
所有的读写内存，都是通过v操作的。v解引用后前四个字节得到s的地址，然后往s里面 读写内存。

根据堆的分配原则，我们只需要更换一样释放顺序，利用fastin的后进先出和unsortedbin的先进先出。

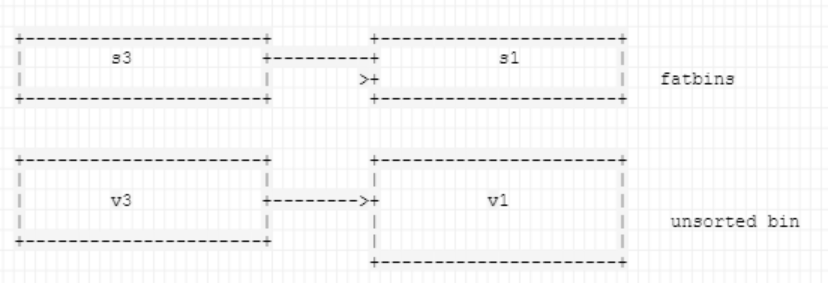
## 利用

分配4块内存：

堆的情况：



然后释放3，1

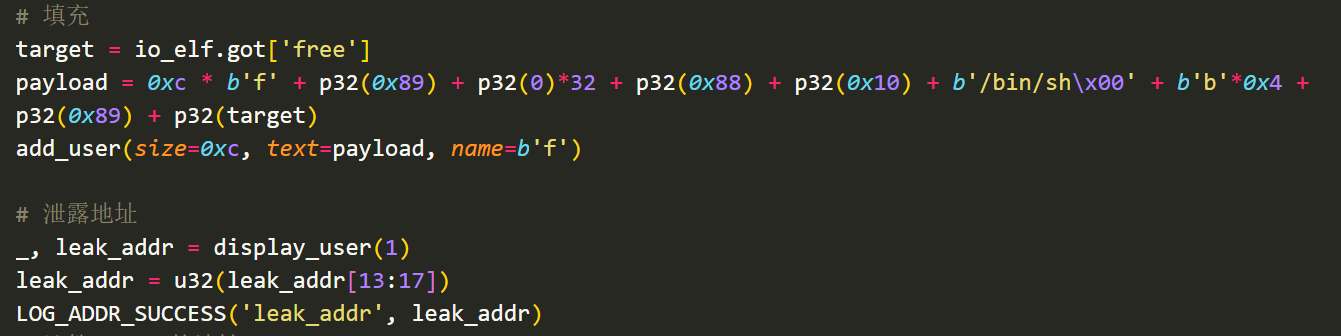


再分配一下：

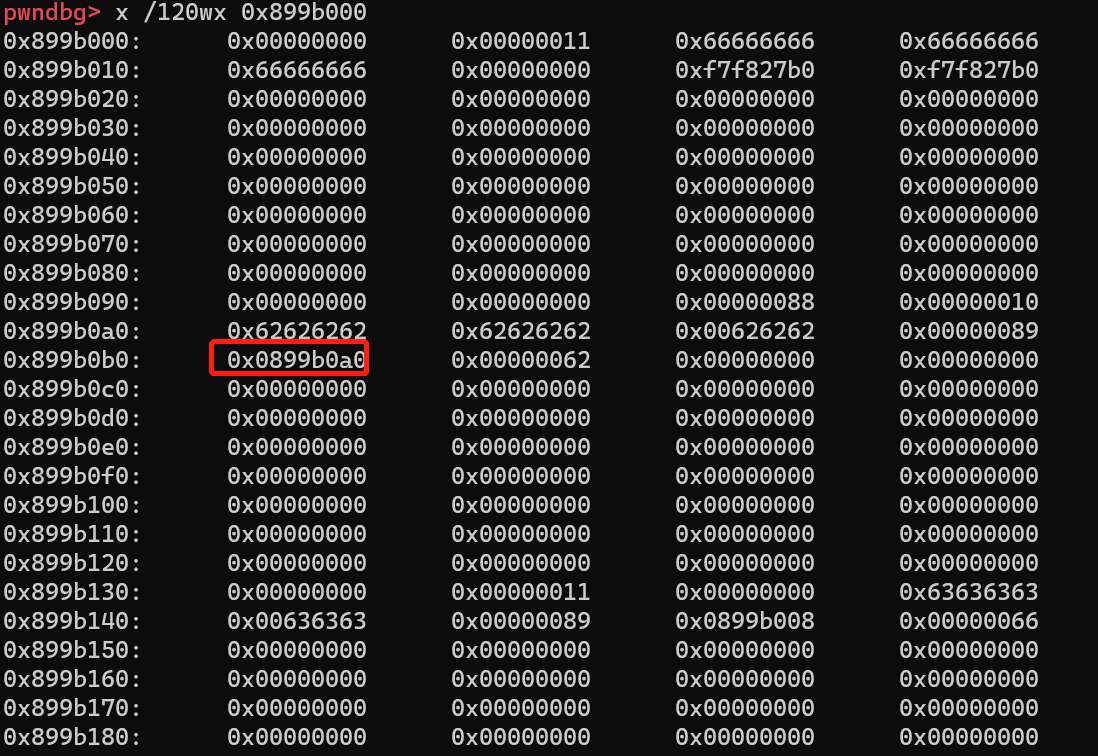
会得到s1 + v3的组合。

这样就可以覆盖s2的地址。

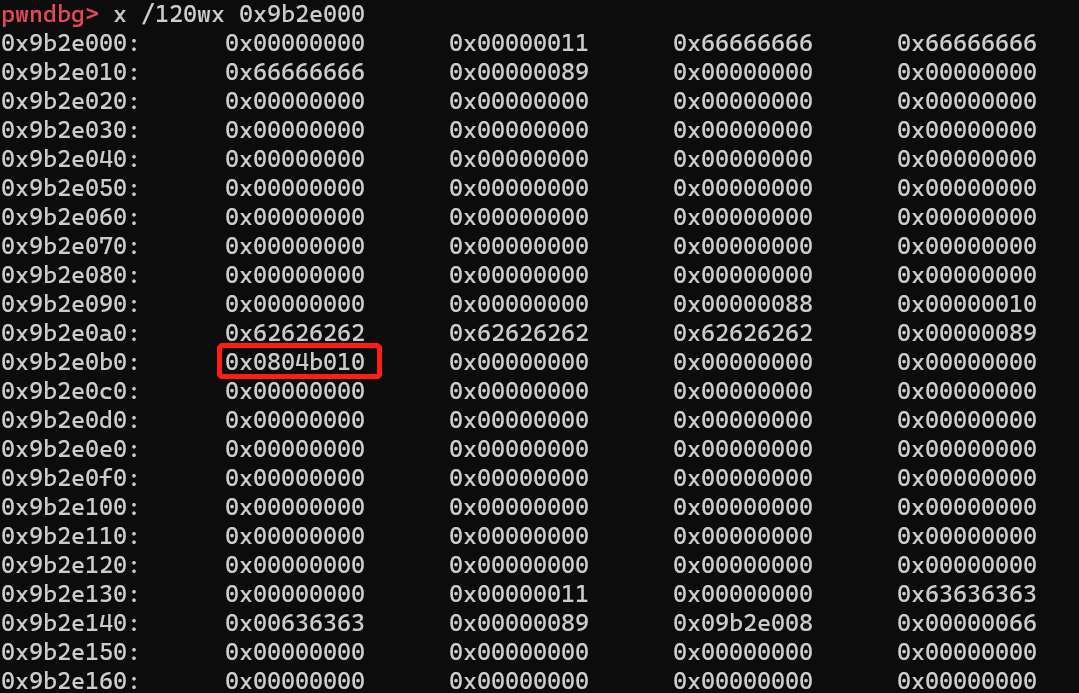
我们就可以修改s2的前四个字节为free的got表地址，就可以泄露出system的地址。

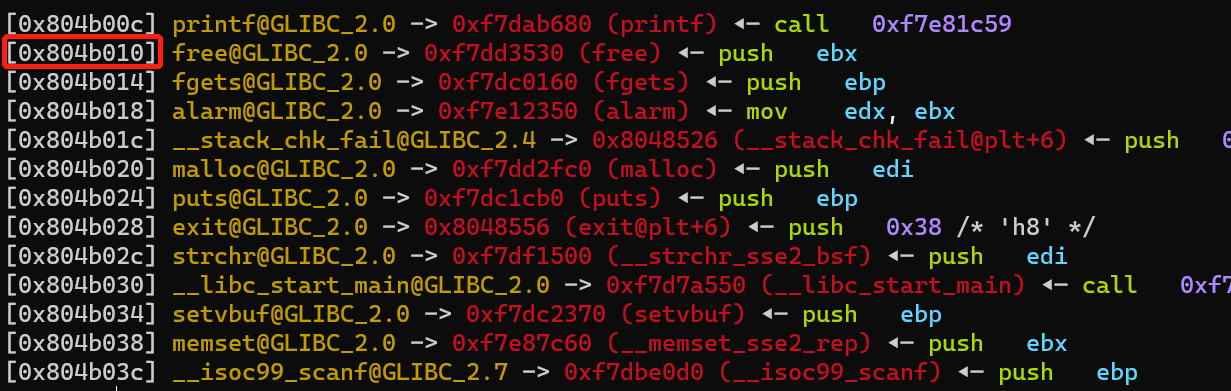


填充前：



填充后：





然后再更新s2为system地址即可。最后释放s4，提前写好/bin/sh。

就执行了system /bin/sh。