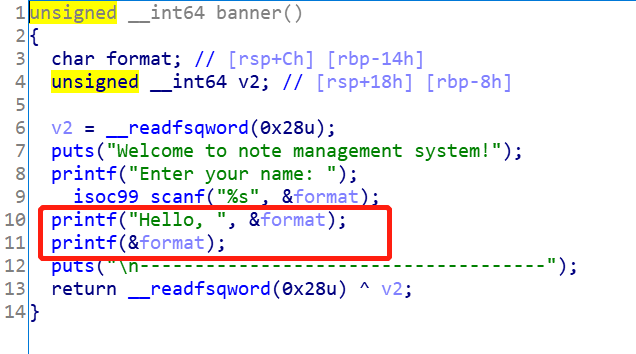


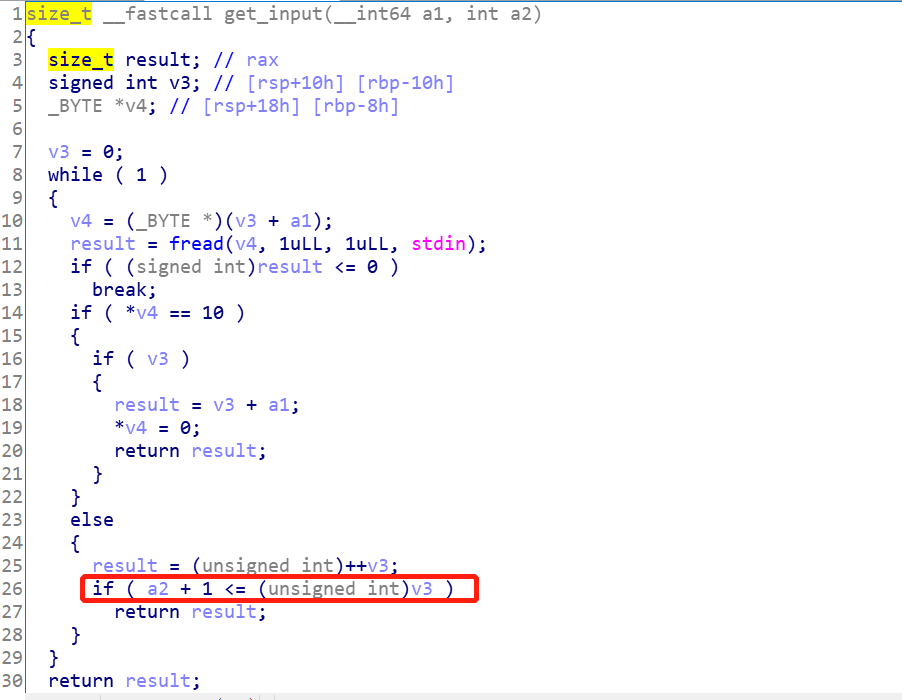
漏洞点在于：



可以泄露处程序的基地址和libc的基地址，分别为：



然后还有一个off by one，太隐蔽了 找了半天。。。



使用unlink

改写地址为free\_hook

然后写入system地址即可。

