




# buuctf easyheap

原创

轩渊  于 2020-02-09 16:41:38 发布  340  收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：[https://blog.csdn.net/weixin\\_44932880/article/details/104236900](https://blog.csdn.net/weixin_44932880/article/details/104236900)

版权

## 主要知识

堆块的结构，fastbin任意地址构造堆块的检查机制，  
对题目流程的认真分析

- 1.检查文件没有地址偏移的保护
- 2.查看功能。
- 3.通过堆的溢出生成一块假堆块
- 4.假堆块可覆盖heaparray[0]为free的got表的地址.
- 5.通过更改heaparray[0]存的堆块的内容，将free的got覆盖为system的地址。
- 6.调用free函数并在前面将参数填充为"/bin/shx00"
- 7.获得sh

1. malloc 0x68.  
 2. malloc 0x68.  
 3. malloc 0x68.  
 4. free 3.  
 5. 编辑堆块2.  
 "/bin/sh\x00"并覆盖3的fd位  
 6. malloc. 0x68.  
 7. malloc 0x68. 将0x60200d分配出来  
 8. 编辑堆块3, 覆盖 heaparray [0], 使指向 free 的 got 表.  
 9. 编辑堆块0,  
 改写 got(free) 为 system 函数  
 10. free 堆块2 执行  
 system("/bin/sh\x00");

堆块

prevsize	size
fd	bk

heaparray [0]	[1]	[2]	[3]
got[free]	2	3	0x60200d

[https://blog.csdn.net/weixin\\_44932880](https://blog.csdn.net/weixin_44932880)



创作打卡挑战赛 >

赢取流量/现金/CSDN周边激励大奖