buuctf easyheap

原创

轩渊 于 2020-02-09 16:41:38 发布 340 收藏

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/sh\x00"
7.获得sh