



漏洞点在这里，可以自己指定大小进行读写chunk。

经典的fastbin attack

所以攻击思路如下：

1、 首先分配三块chunk

2、 释放第2块

3、 然后通过第1块去修改第二块的fd

4、 分配到item\_list处，修改地址为free 的got表地址

5、 将system地址写入free的got表中

6、free一个/bin/sh\x00的块

但是实际上，这样做是有问题的：

Free修改之后会报错，调整后如下：

修改malloc的got表内地址为system地址

申请内存，参数改成/bin/sh\x00的地址即可。

