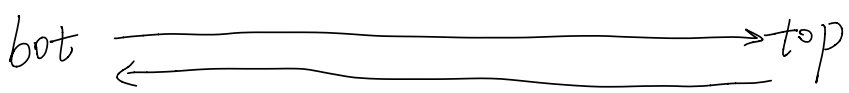
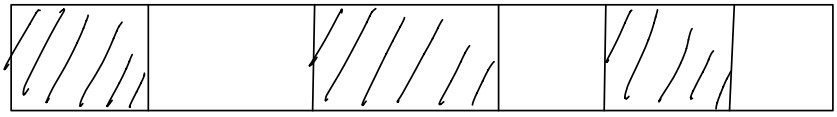
arena

初始化：



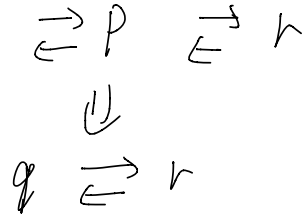
分配内存：

释放内存

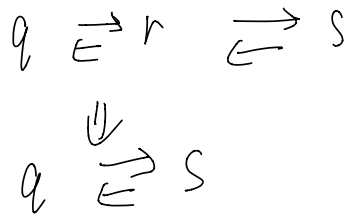


free(p)

① 前后间：



② 合并相同

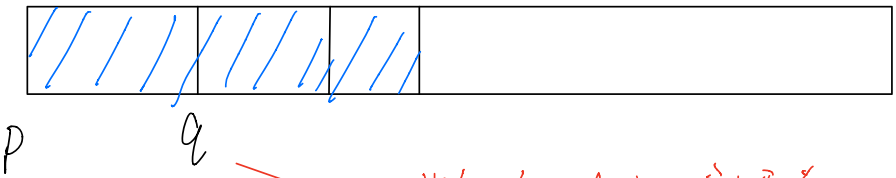


漏洞：

① 分配 P.q

② 释放 P.q (但没有置为 NULL)

③ 分配 P



→ q指针的（和r被覆盖
（既是数据也是指针）

④ 释放 q

如果③中构造数据使得

q.C(q) = &shellcode

q.r = 返回地址

并且 shellcode 为偶数 (GET-FREEBIT)

那么有

(p → s.r → s.l = q)

⇓

(返回地址 = shellcode)