mergeheap

mearge逻辑里用了strcpy，会导致溢出。先构造tcache链，然后构造一个chunk，输入大小为0，但是malloc会malloc至少0x20大小的chunk，一直merge直到填到下一个chunk中存下一个tcache块的地方，然后改到libc的free_hook上，然后分配一个块把free_hook改成one_gadget地址即可。