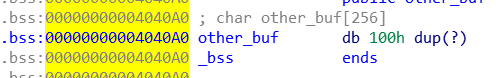
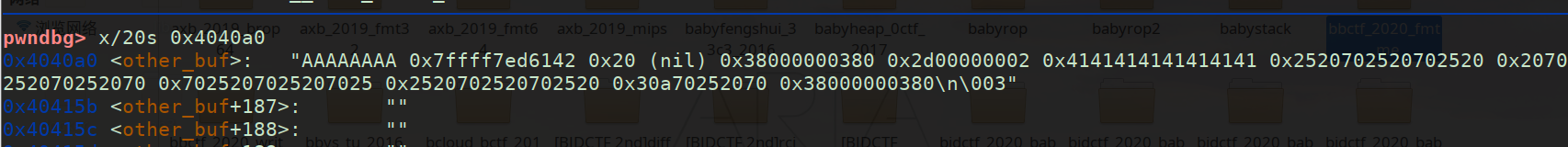


snprintf 格式化漏洞 用gdb查看第一个参数的内容即可观察



参数位置在bss 0x4040a0



偏移为6

那么依据题目的意思 可以将atoi 改为system\_plt; 将system\_got改为main返回再次输入/bin/sh获得shell

完整ex

