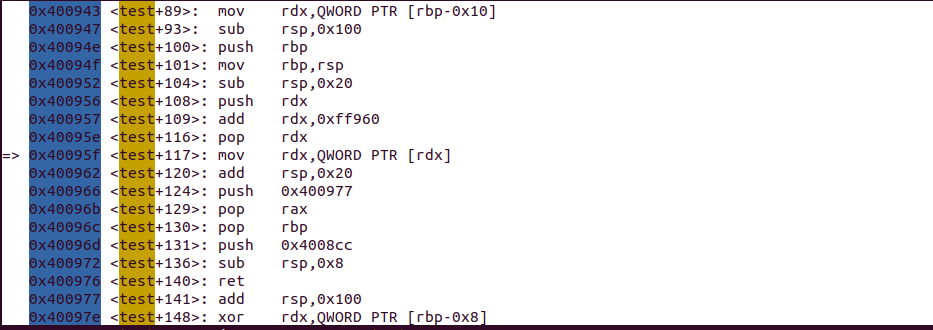
覆盖canary验证

定位：Canary定义在堆中，无法修改无法泄漏

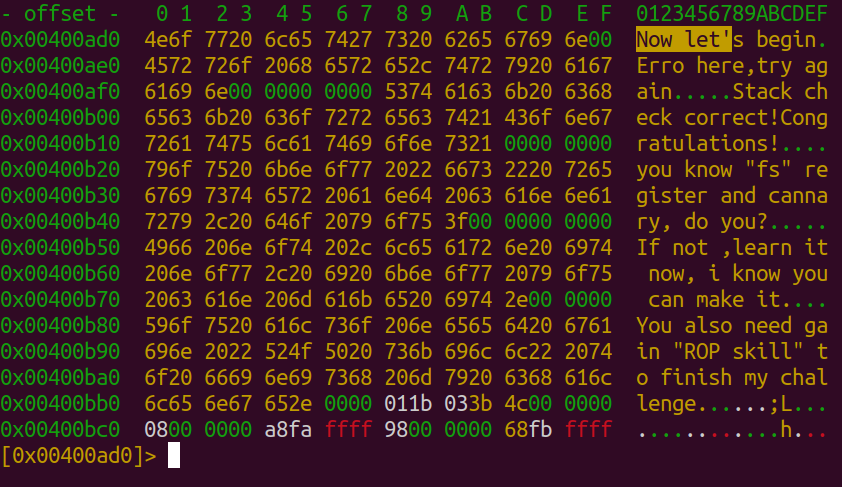


但是验证操作时canary在栈中，

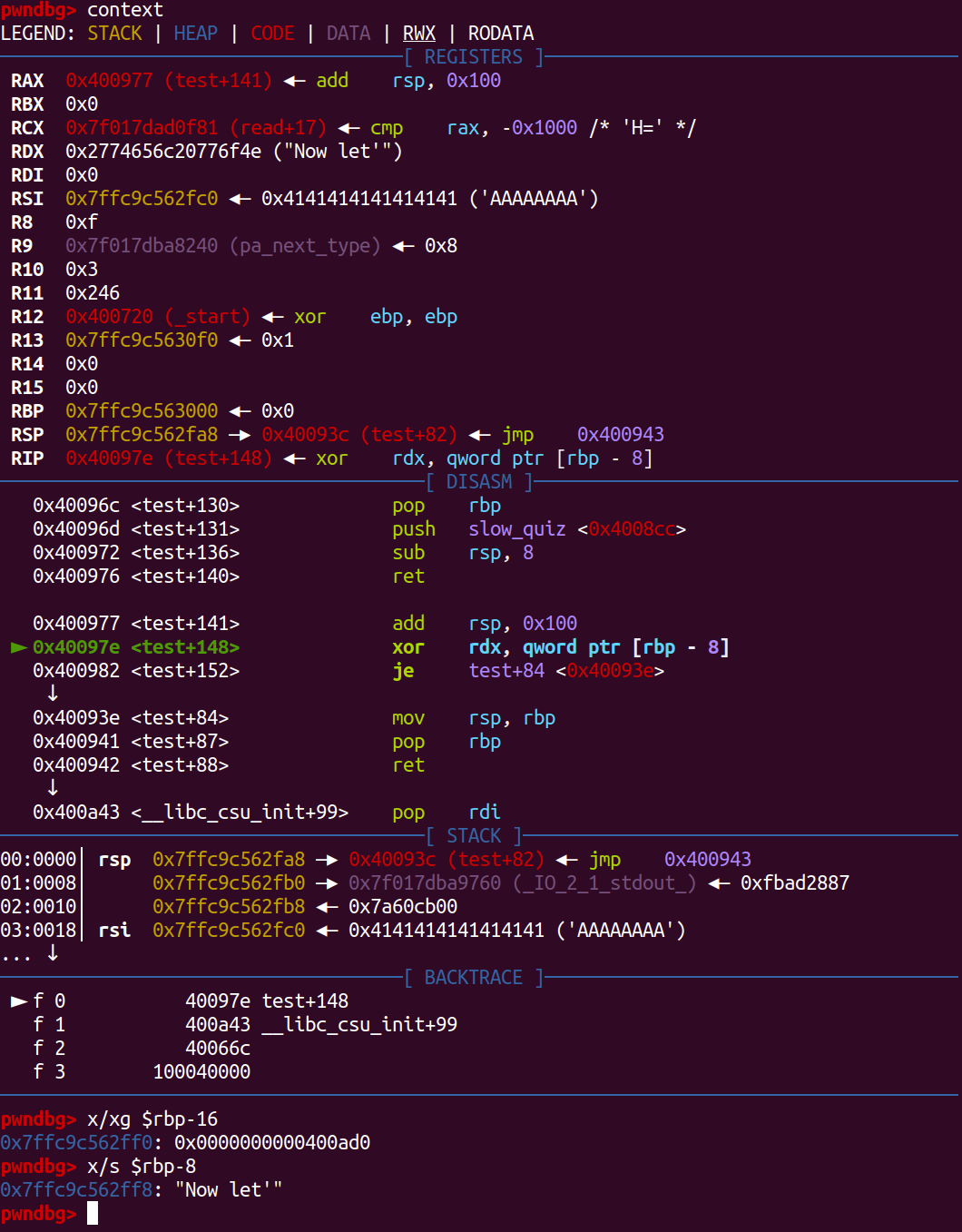
地址：正确值指针rbp-16 输入值rbp-8

read\_buf+48 read\_buf+56

覆盖canary：将rbp-16指针覆盖为内容已知的指针，在rbp-8处输入该内容



如 rbp-16 <- 0x0400ad0, rbp-8 <- Now let’

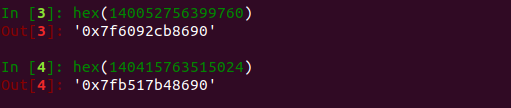


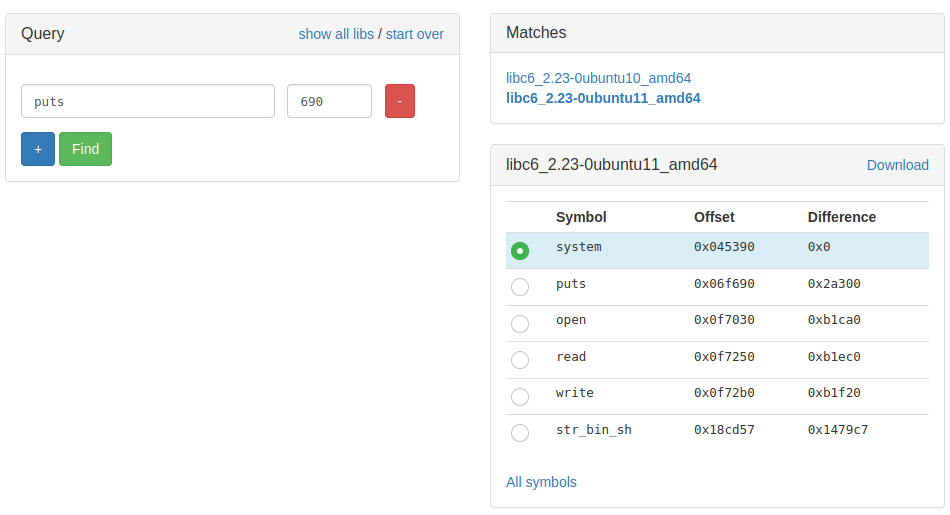
验证通过。

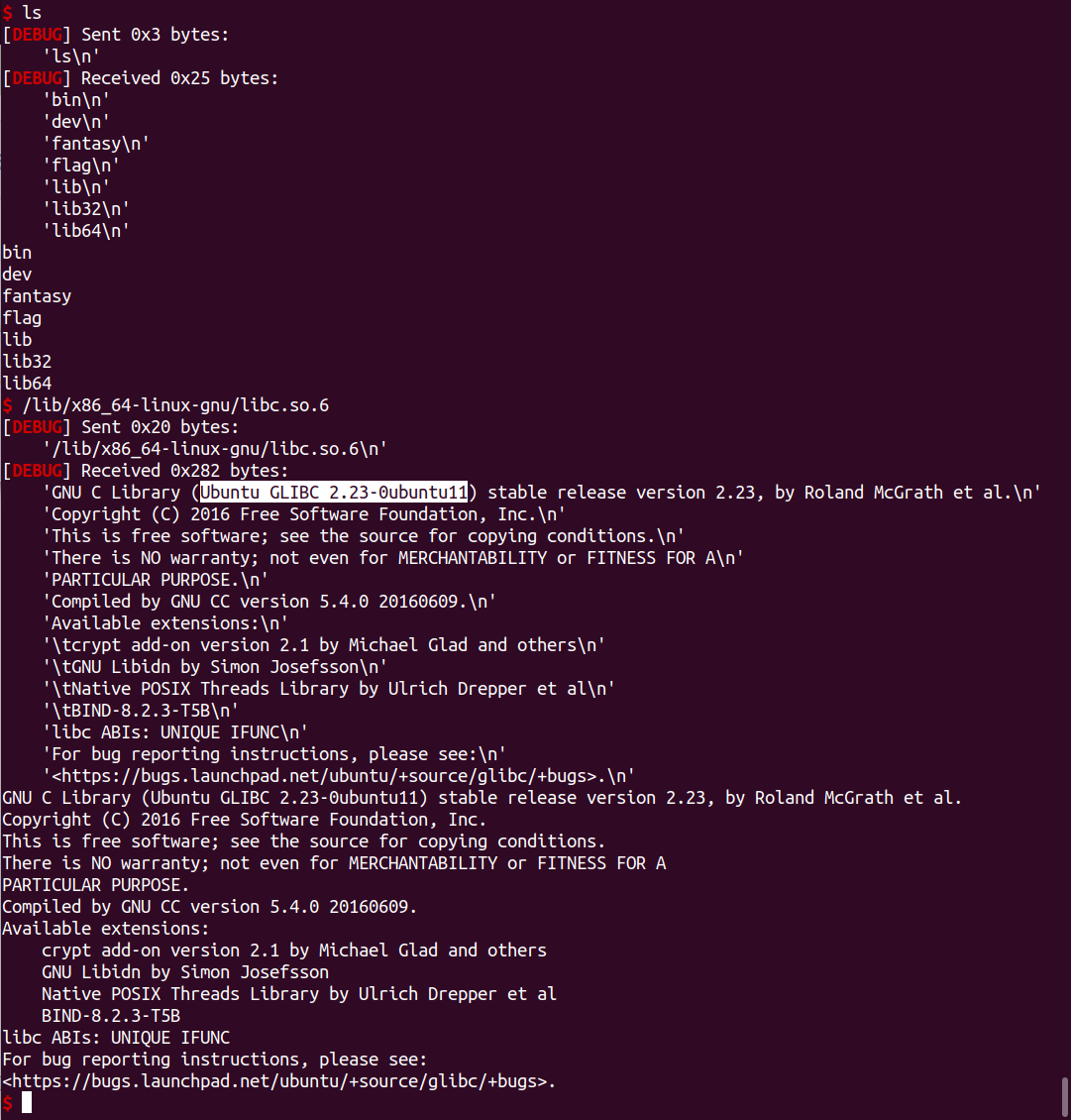


返回地址位于read\_buf+72

首先，构造rop链，用puts函数泄漏libc基址







然后，第二个rop链利用程序自带call ssytem ，执行system(“/bin/sh”)即可

