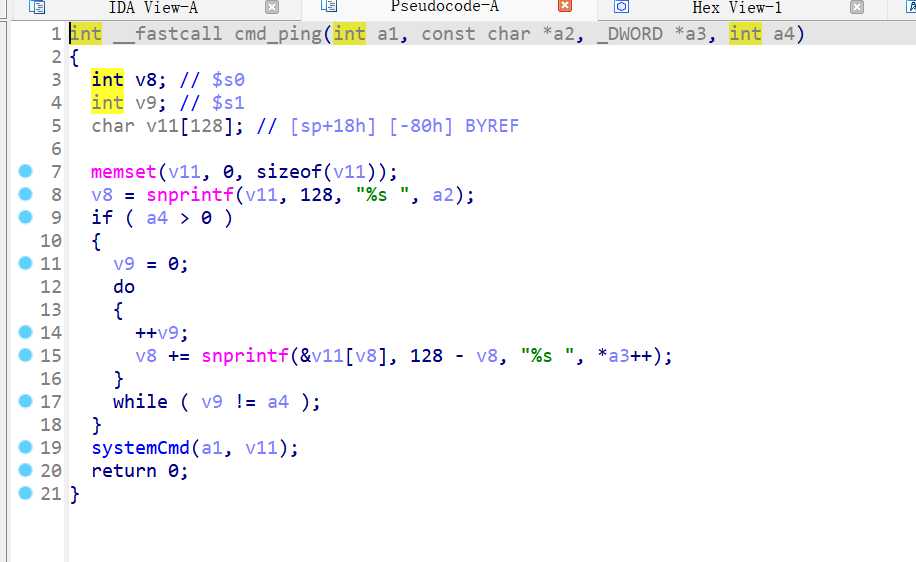


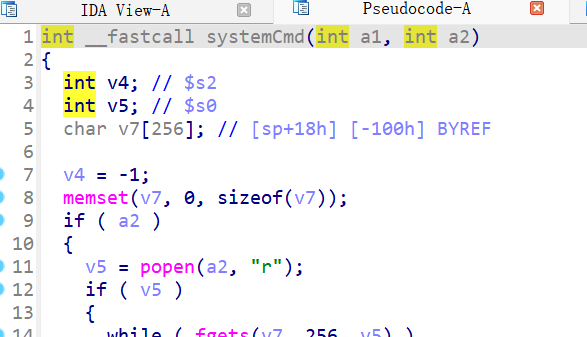
在lighttpd中的http\_parse函数可以直接通过访问/start\_telnet开启telnetd服务，指向的是/usr/bin/cli

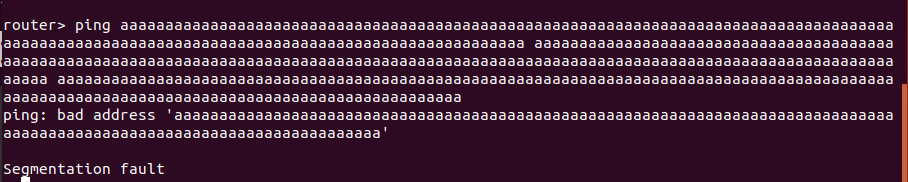
但是cli里的cmd\_ping函数输入的数据在栈中，

并没有对输入的命令长度进行校验，存在缓存区溢出漏洞



后续命令直接传入到popen中进行执行，进行巧妙构造后可以实现任意命令执行





缓冲区溢出演示