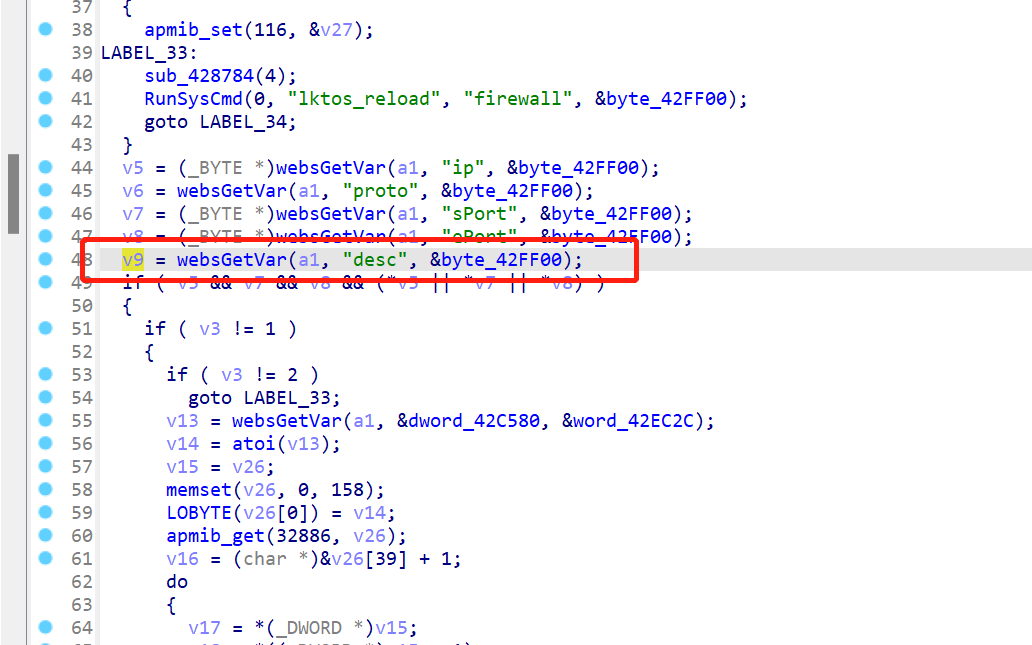
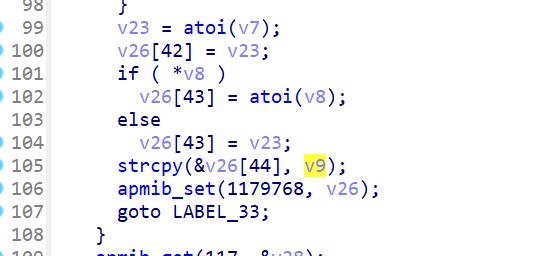
函数中的desc字段没有经过任何长度的检查就通过strcpy函数放进了栈中





通过正确设置一些参数的值就可以到达strcpy函数的逻辑处

