# 程序说明

* vulnerabilities
  + 命名：buffer\_overflow\_code\_injection\_write\_file
  + 漏洞：缓冲区溢出漏洞
  + 攻击：代码注入攻击
  + Shellcode：写文件,
  + 在漏洞程序中通过获取环境变量ATTACH来判断程序是否处于调试中
    - ATTACH=TRUE/FALSE为TRUE调试程序，为FALSE运行程序
  + 在漏洞程序中通过获取环境变量NORMAL来判断程序是否正常运行
    - NORMAL=TRUE/FALSE为TRUE读入正常输入，为FALSE读入shellcode
  + 编译命令及aslr信息已经写入Config
* Input
  + buffer\_overflow\_code\_injection\_write\_file.txt此文件为shellcode，其功能为向output文件夹中的buffer\_overflow\_code\_injection\_write\_file.txt文件中写入字符串buffer\_overflow\_code\_injection\_write\_file attack success
  + buffer\_overflow\_code\_injection\_write\_file\_normal.txt此文件为正常输入
* output
  + 如果攻击成功会产生buffer\_overflow\_code\_injection\_write\_file.txt文件，文件内容为buffer\_overflow\_code\_injection\_write\_file attack success
  + 如果攻击失败，将不产生文件，或文件为空
* check
  + 命名：buffer\_overflow\_code\_injection\_write\_file
  + 通过环境变量OUTPUT\_buffer\_overflow\_code\_injection\_write\_file\_PATH获取output文件夹下buffer\_overflow\_code\_injection\_write\_file.txt文件的路径
  + 如果此文件不存在，或为空，返回失败信息，否则将此文件中的信息返回
* Config
  + type=buffer\_overflow,code\_injection
  + compile=gcc -fPIC -shared buffer\_overflow\_code\_injection\_write\_file.c -o buffer\_overflow\_code\_injection\_write\_file.so
  + aslr=off
* shellcode 生成
  + 用汇编写一段满足攻击要求的程序hello.asm
  + 按照如下命令生成shellcode

nasm -felf64 hello.asm -o hello64.o

ld -s -o hello64 hello64.o

for i in $(objdump -d hello64 |grep "^ " |cut -f2); do echo -n '\x'$i; done; echo