# 分析过程：

x86中参数都是保存在栈上,但在x64中前六个参数依次保存在RDI, RSI, RDX, RCX, R8和 R9寄存器里，如果还有更多的参数的才会保存在栈上。

利用ROP攻击执行系统调用execv(“/bin/sh”)，系统调用号为0x3b，将系统调用号保存到寄存器rax中，其中execv()所需的参数”/bin/sh”保存在rdi寄存器中，rdx和rsi中置0，。

利用ROPGadget在/lib/x86\_64-linux-gnu/libc.so.6中搜素所需gadget从而获得gadget的地址。

构造payload：首先找到漏洞程序中返回地址rip距离buf的偏移(40)，

然后确定gadget的位置以及参数”/bin/sh”的位置。

payload = "a"\*offset + ret1\_addr + binsh\_addr + ret2\_addr + ret3\_addr + data1 + ret4\_addr + data2 + data3 + ret5\_addr

# 所用gadget：

pop %rdi; ret

xor %rax %rax; ret

pop %rax; ret

pop %rdx; pop %rsi; ret

syscall