## v1.1 Spirnt1渗透测试记录

## R1.1 Sprint1 Penetration Test Record

**Sprint 1：**

[【developer】vnc接口实现](https://gitee.com/OSDT/dashboard?issue_id=I2EDQ9)

[【developer】vnc界面设计和开发](https://gitee.com/OSDT/dashboard?issue_id=I2EDQ5)

**测试用例：EG-TST-SEC-007** 越权

**测试方法：**

尝登录vnc，查看能否对预期之外的文件进行操作（读/写/执行等）

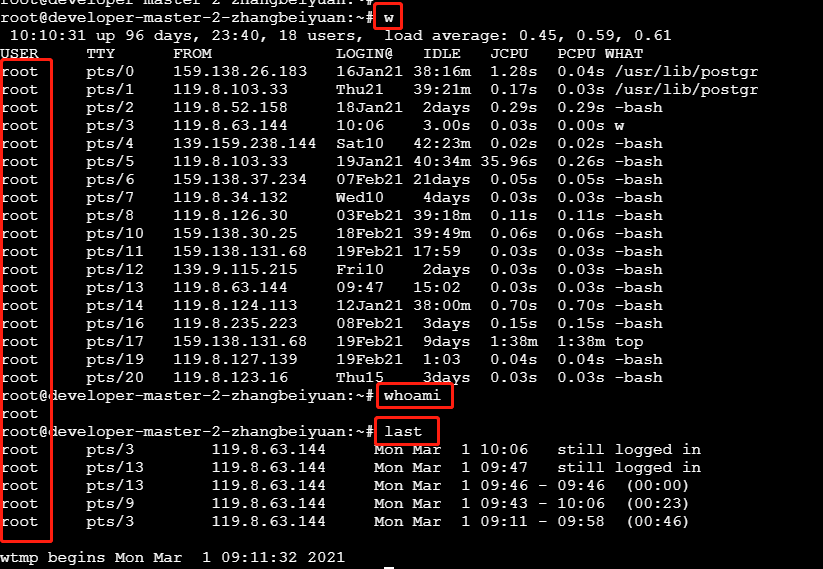
**测试过程**：

①登录developer，正常建立应用，部署调测，成功

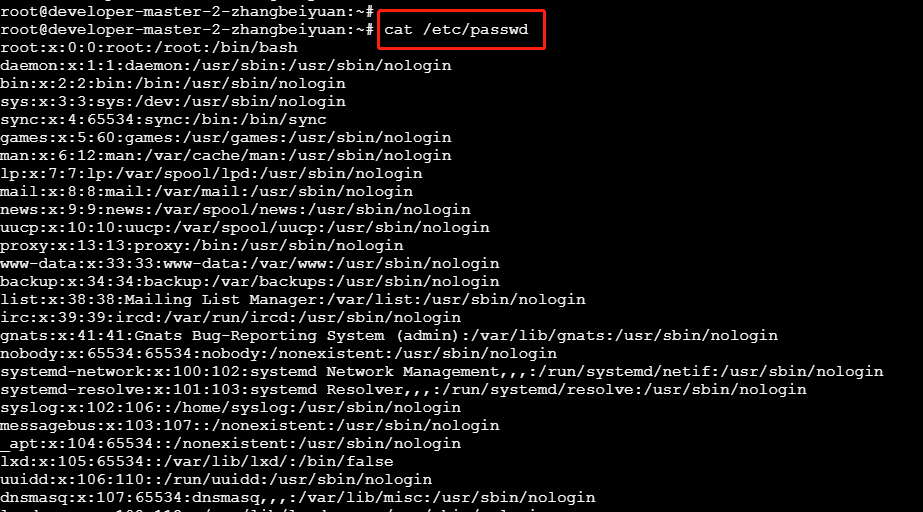


②点击“VNC”按钮，进入vnc调试界面。  
③输入"curl ifconfig.me"，可以看到实际访问ip为 119.8.63.144（开发环境）

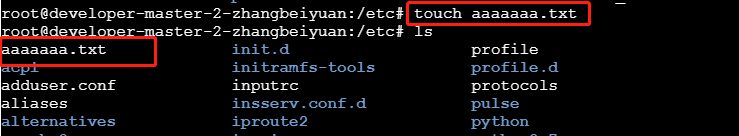
④查看当前用户，可以看到用户是root。（这里存在用户权限过高问题）



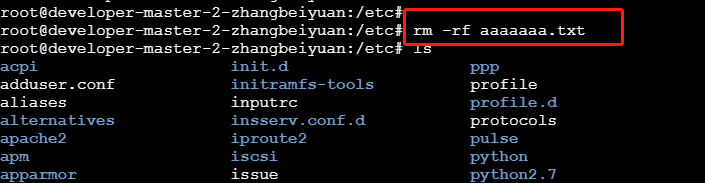
⑤尝试在工作目录之外（如/etc）新建/删除文件，均可以操作成功，说明vnc操作者可以任意操作目标服务器的文件。  
成功读取任意文件



成功新建



成功删除



**测试结论**：**Not PASS**

**不通过原因：VNC登录用户权限/目录权限过大，可以操作服务器任意文件。**

[【UserMgmt】用户统一管理功能支持对用户停用/启用](https://gitee.com/OSDT/dashboard?issue_id=I2E9MB)

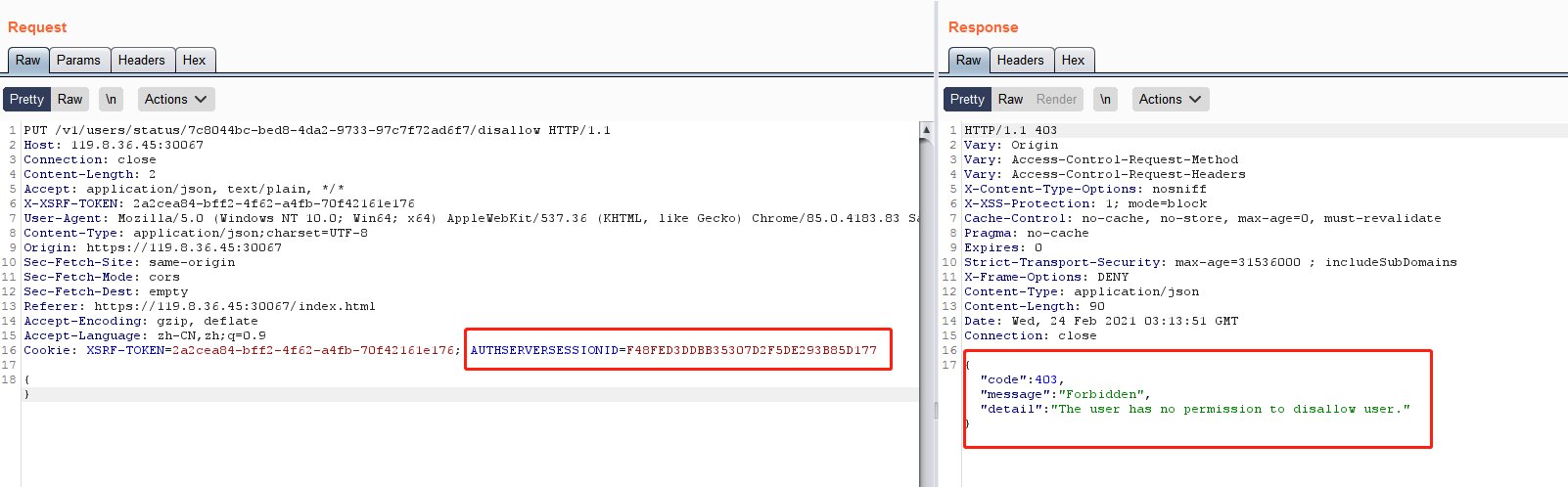
**测试用例：EG-TST-SEC-007** 越权

**测试方法：**

尝试使用普通用户访问用户启用/停用接口，看能否设置成功

**测试过程**：

抓取admin设置角色的请求包，将cookie更换为普通用户，提交后报403forbidden，ok

****

**测试结论**：**PASS**

[【UserMgmt】支持用户统一管理基本查询展示功能](https://gitee.com/OSDT/dashboard?issue_id=I2E9M8)

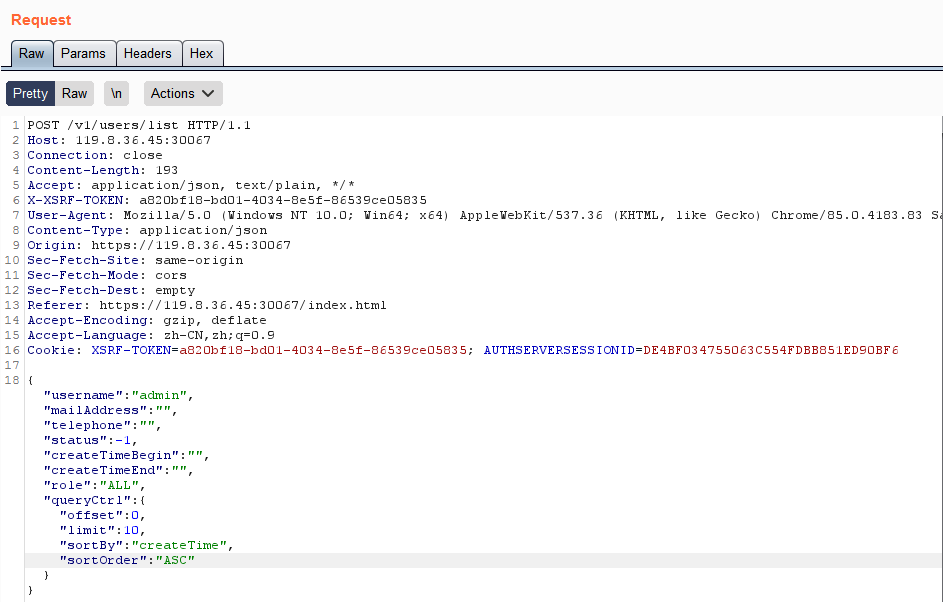
**测试用例：EG-TST-SEC-005** SQL注入

**测试说明**：

对数据库查询进行SQL注入测试，尝试挖掘SQL注入漏洞。

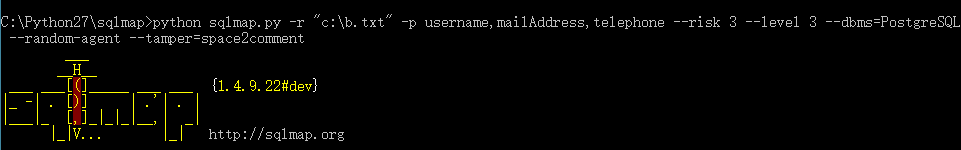
**测试过程**：

对查询功能抓包，并将请求内容保存为.txt格式文件。

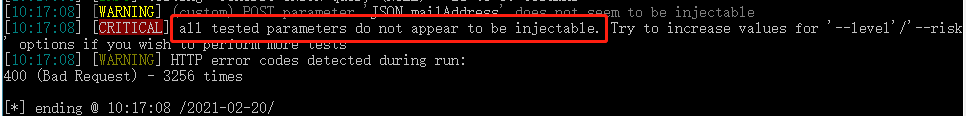


打开sqlmap，使用以下命令尝试SQL注入：

python sqlmap.py -r "c:\b.txt" -p username,mailAddress,telephone --risk 3 --level 3 --dbms=PostgreSQL --random-agent --tamper=space2comment



注入结果：无法注入。Ok



**测试结论**：**PASS**

[【UserMgmt】用户统一管理功能支持设置用户所属角色](https://gitee.com/OSDT/dashboard?issue_id=I23FRE)

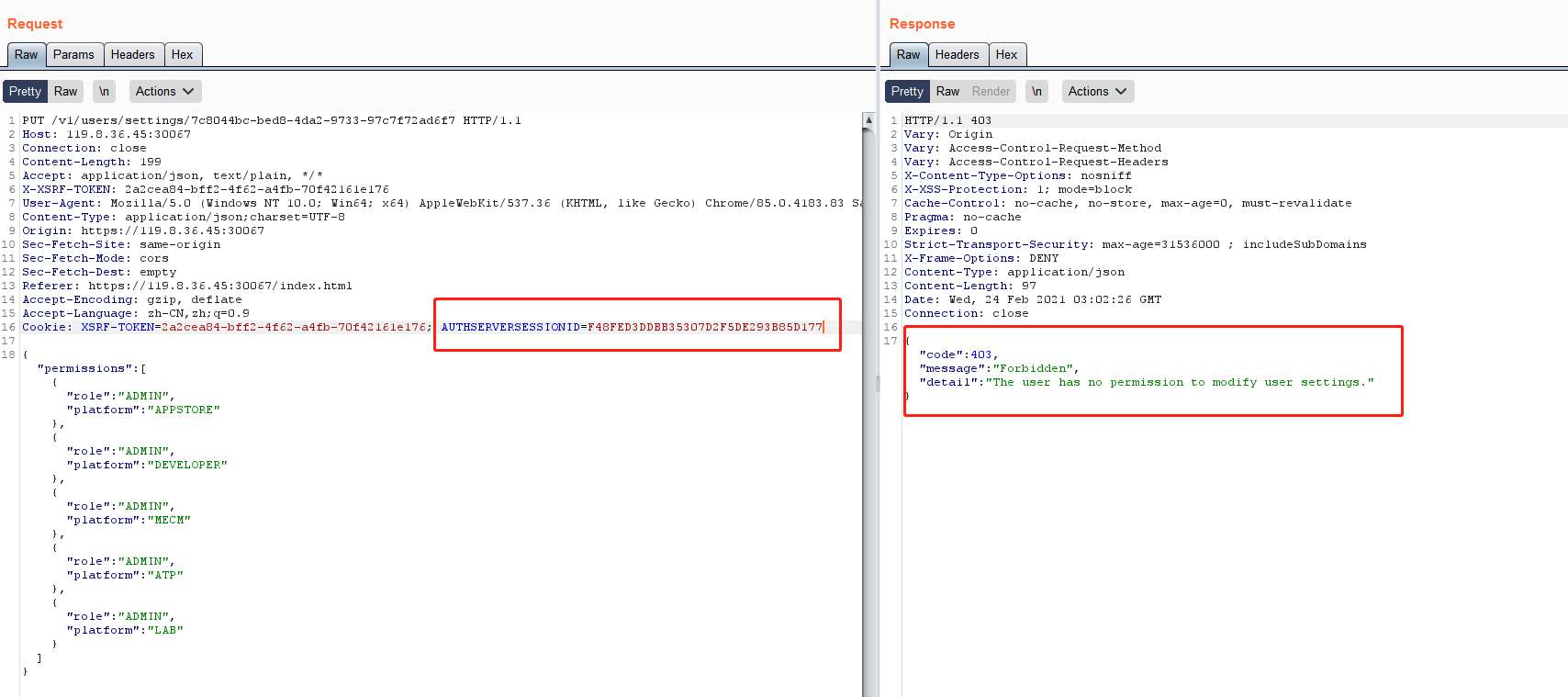
**测试用例：EG-TST-SEC-007** 越权

**测试方法：**

尝试使用普通用户访问设置角色接口，看能否设置成功

**测试过程**：

抓取admin设置角色的请求包，将cookie更换为普通用户，提交后报403forbidden，ok



**测试结论**：**PASS**