成都职业技术学院getshell

无描述...

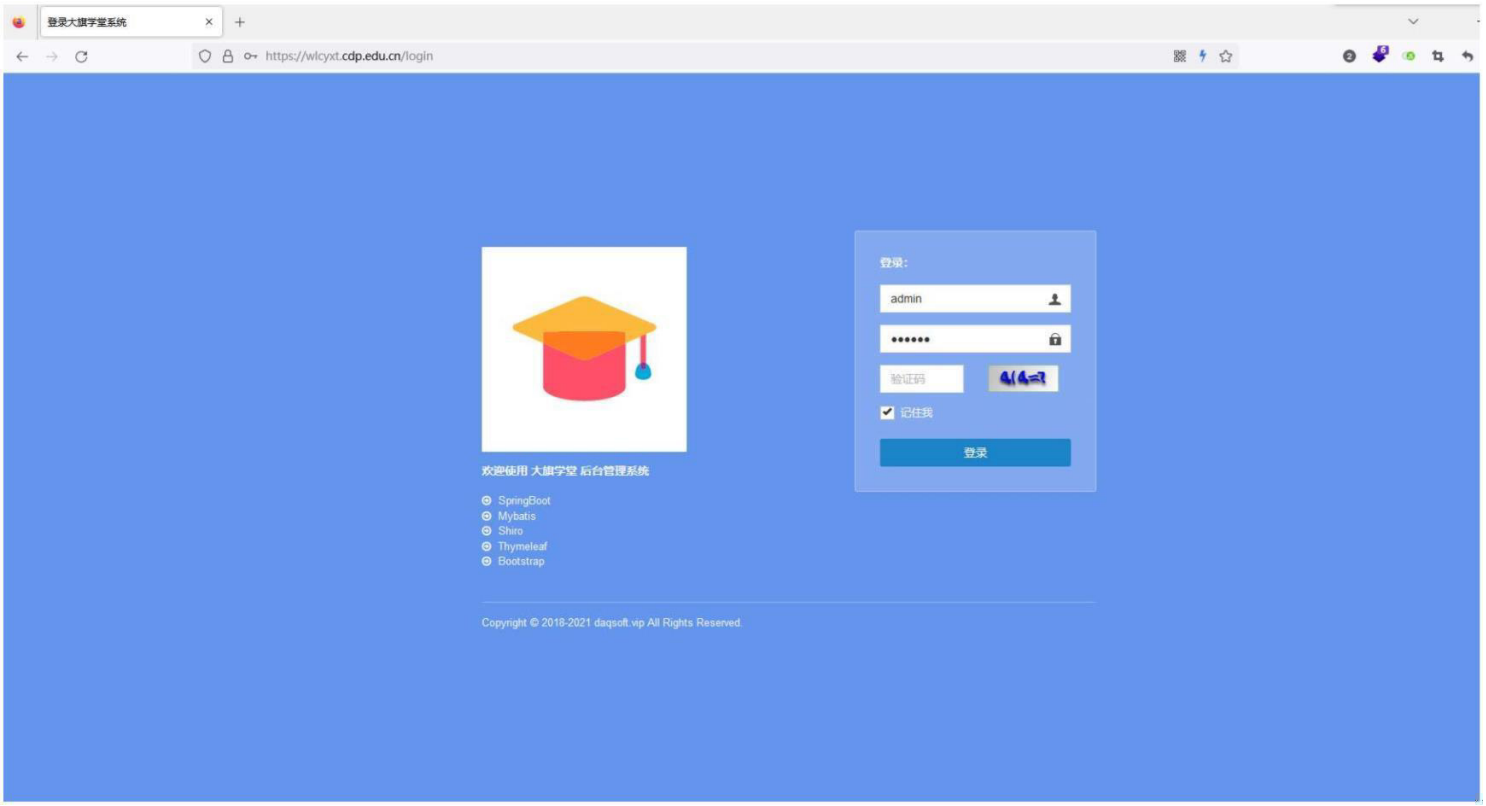
1.漏洞地址：https://wlcyxt.cdp.edu.cn/login

2.漏洞名称：成都职业技术学院大旗学堂系统存在shrio反序列化漏洞可获得root权限

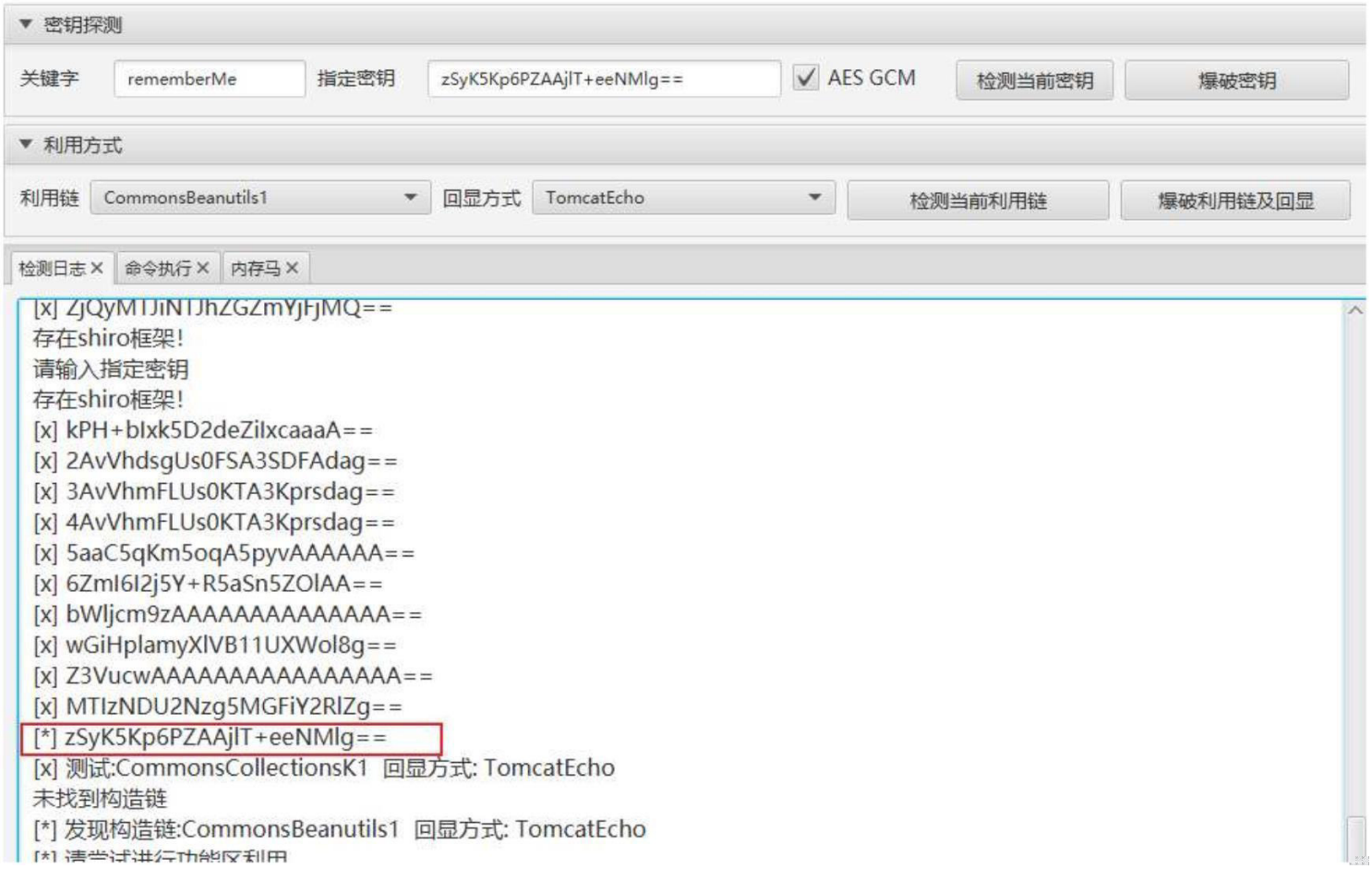
3.漏洞描述：

（1）资产确认：https://wlcyxt.cdp.edu.cn/，确认为成都职业技术学院资产

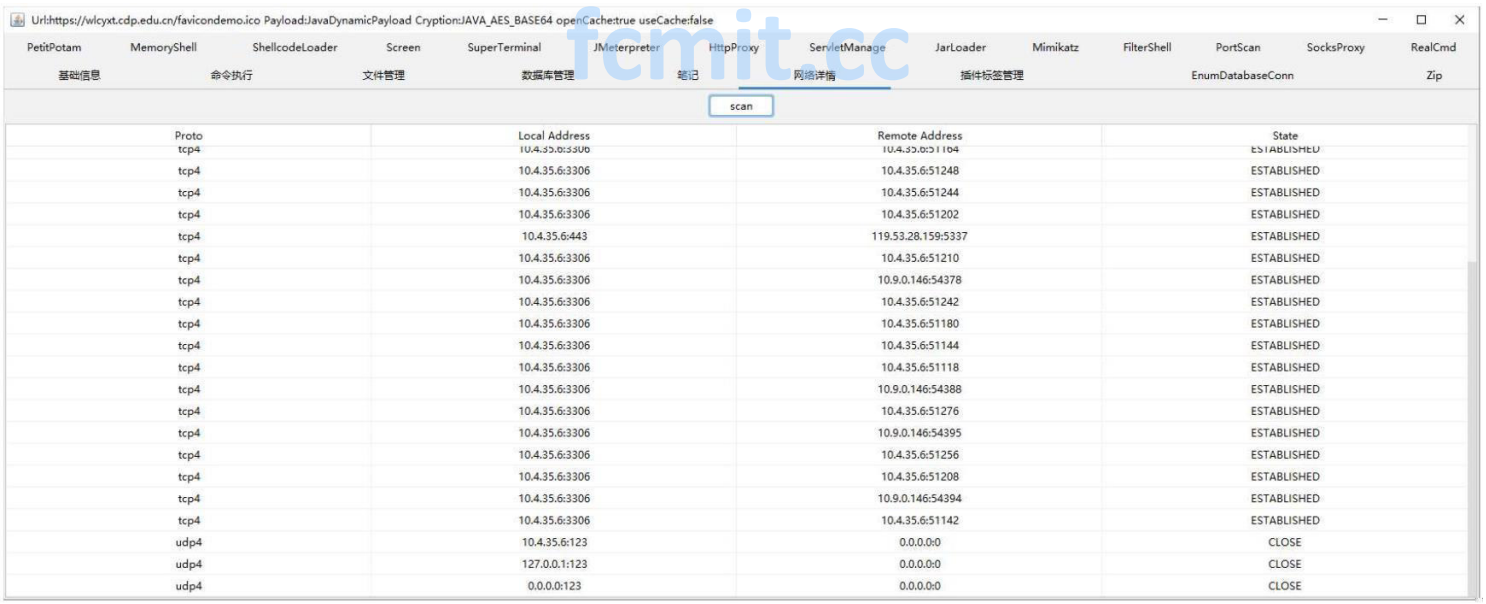
（2）抓取登录报文，截取响应报文，发现了rememberMe=deleteMe为shrio框架特征

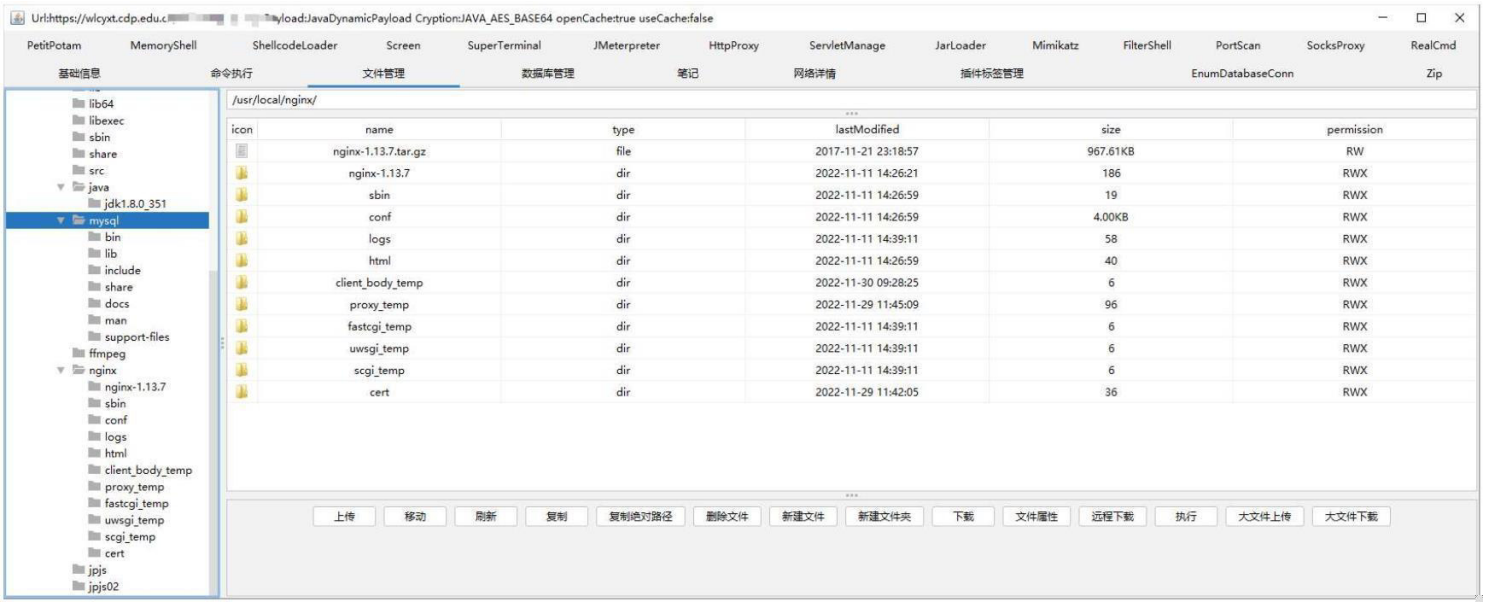


（3）利用工具爆破KEY，KEY为zSyK5Kp6PZAAjlT+eeNMlg==



（4）利用链用：构造链:CommonsBeanutils1 回显方式: TomcatEcho，上传木马，webshell成功连接





（5）内网地址为10.4.35.0/24段地址，登录权限为root权限，存在mysql数据库。

（6）个人声明：**本人未对数据进行上传下载修改操作，所上传木马已自行清除**，请管理员及时修复漏洞。

（7）修复建议：

修复方案一：升级Shiro依赖版本

Apache官方的漏洞修复采用了在代码中随机生成密钥的方式，因此可以采用升级Shiro版本为1.2.5及以上。
此方案适用于开发初期或代码依赖库较简单不会产生依赖冲突。

修复方案二：私有化硬编码密钥

采用在Shiro配置文件中加入rememberMeManager管理器来硬编码指定加密密钥，此密钥建议采用私有密钥，切勿采用网络上已有密钥。此方案适用于代码的保密性较强或用于练习的项目。

修复方案三：随机生成密钥

在项目中新建随机生成AES加解密密钥的方法，在Shiro配置文件的rememberMeManager中调用该方法进行密钥动态生成。此方案与升级Shiro版本的本质策略相同。此方案适用于项目后期漏洞修复，可最小化对原有项目的影响。