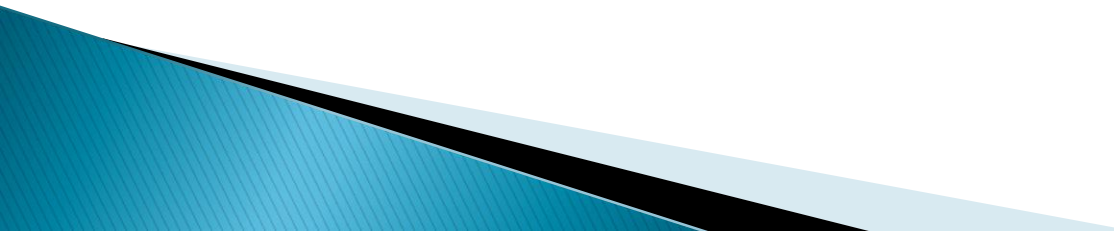


# Attacking JBoss

Like a Boss

# What is JBoss?

- ▶ Open source Java EE application server
  - ▶ Developed by JBoss, a division of Red Hat
  - ▶ Abstracts the infrastructure of Java-based web applications
  - ▶ Very large and complex
- 

# JBoss Security

- ▶ “We have over the years had the understanding that JBoss AS will be primarily used by Java EE developers on their desktop to develop business applications. When they are ready to deploy those applications in production, they will have the practical sense to follow guidelines on securing jboss (which has been available in multiple forms in our wiki).

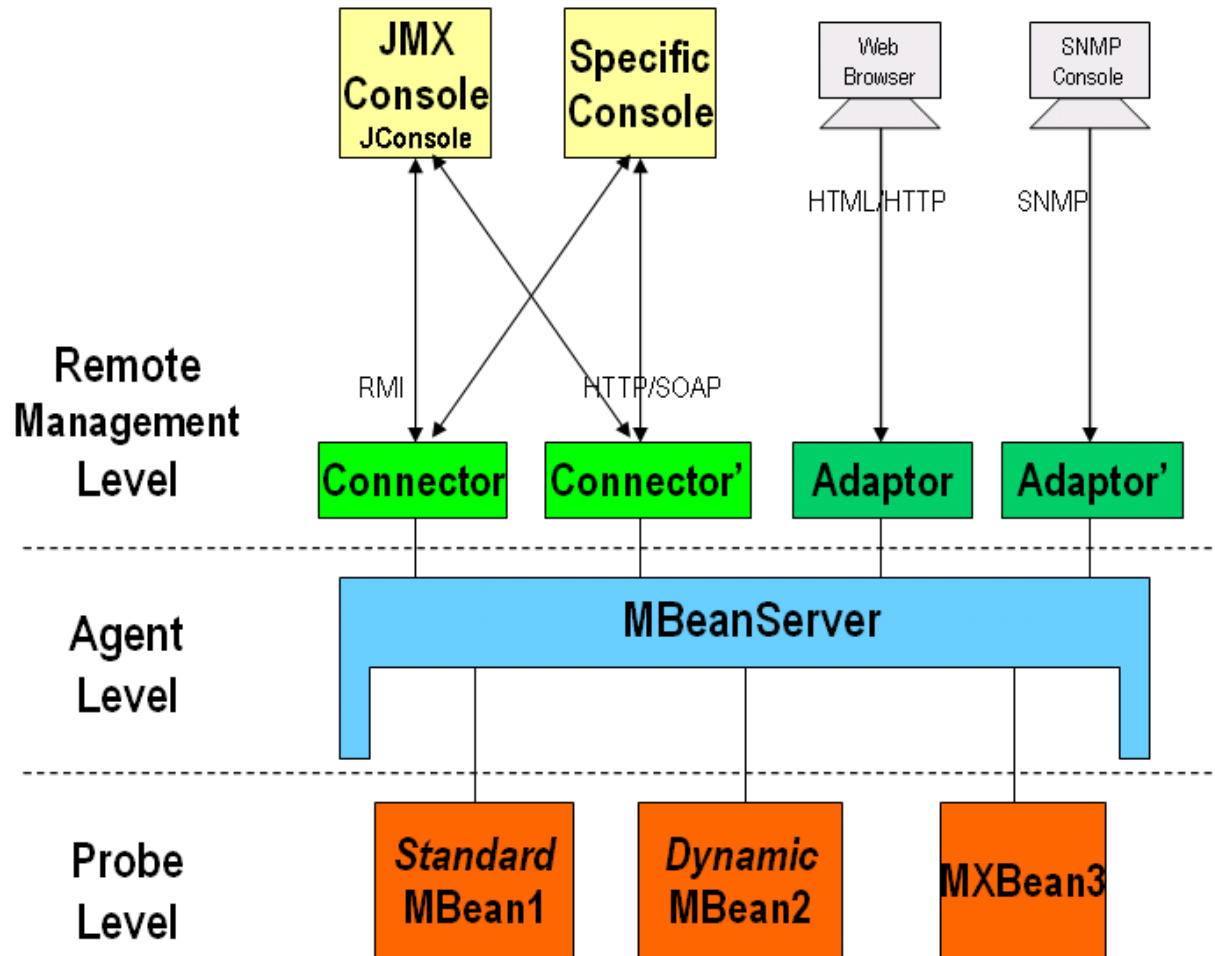
There are no reasonable defaults in security to secure the shipped community version of JBoss AS.”

**Anil Saldhana**

**Lead JBoss Security Architect at JBoss, A Division of Red Hat**

<http://anil-identity.blogspot.com/2010/04/security-community-jboss-as-versus.html>

# JMX? RMI? MBeans?



Source: Wikipedia

# Welcome to JBoss™



## JBoss Online Resources

- [JBoss 4.0 documentation](#)
- [JBoss Wiki](#)
- [JBoss forums](#)







## JBoss Management

- [Tomcat status \(full\) \(XML\)](#)
  - [JMX Console](#)
  - [JBoss Web Console](#)
-

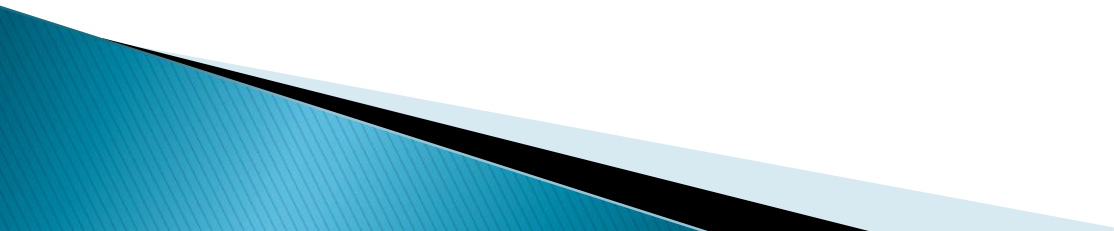
# JMX Console

- ▶ Provides a web interface to MBeans
- ▶ From the JBoss wiki:

## Things to do with the JMX Console:

-  Display the JNDI tree
-  Generate a thread dump
-  Display the memory pool usage
-  Manage the deployment scanner
-  Redeploy an application
-  [Shut down JBoss](#)

# JMX Console

- ▶ Installed by default with no security
  - ▶ JBoss provides recommendations for securing the JMX Console
    - Some of which have been proven wrong
    - And some issues are simply not addressed
- 

# JMX Console – Password Protection

- ▶ <http://community.jboss.org/wiki/securethejmxconsole>
- ▶ Default login module in login-config.xml is:
  - org.jboss.security.auth.spi.UsersRolesLoginModule
- ▶ This module does not provide
  - Enforced password complexity
  - Password lockouts
  - Etc.

# JMX Console -Default Misconfiguration

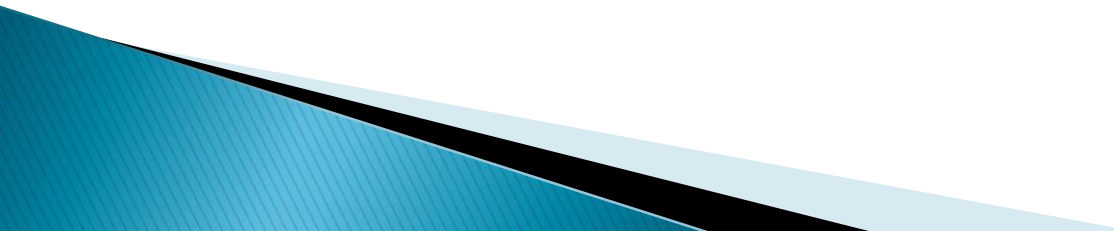
- ▶ Notice anything?

```
<web-resource-collection>  
<web-resource-name>HtmlAdaptor  
  </web-resource-name>  
<description>An example security config  
  that only allows users with the  
  role JBossAdmin to access the HTML JMX  
  console web application  
</description>  
<url-pattern>/*</url-pattern>  
<http-method>GET</http-method>  
<http-method>POST</http-method>  
</web-resource-collection>
```

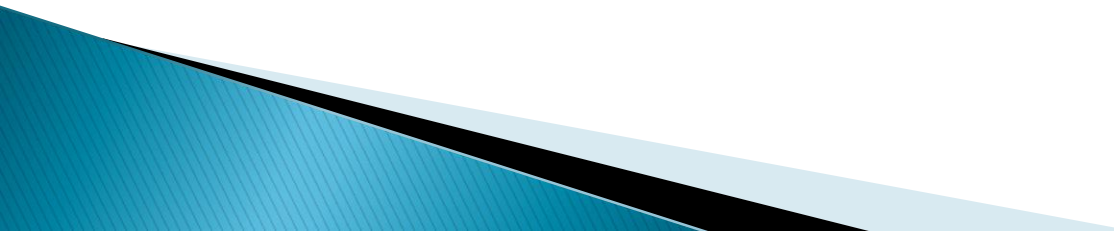
# XSS, CSRF

- ▶ Persistent XSS – get admin JSESSIONID
- ▶ CSRF – execute any functionality

# login-config.xml

- ▶ Specify the module used for authentication per application
  - ▶ `jboss.security:service=XMLLoginConfig`
  - ▶ Load new login-config.xml from arbitrary URL
- 

# RMIAdaptor Service

- ▶ MBeans are exposed over RMI
  - ▶ Same functionality as JMX console
  - ▶ DIFFERENT authentication mechanism!
  - ▶ JBoss also recommends you secure this
  - ▶ Occasionally the JMX console is protected or absent, but this service is available
  - ▶ Twiddle
- 

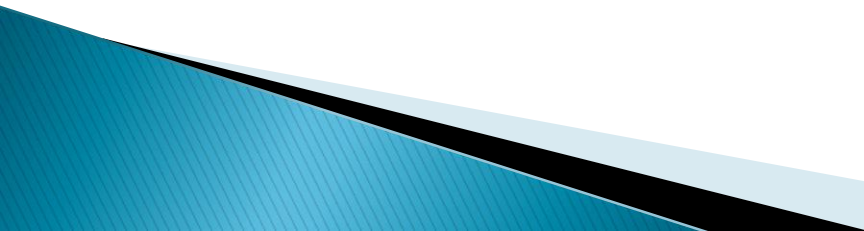
# More?

- ▶ /web-console/Invoker
- ▶ /invoker/JMXInvokerServlet

# Main Deployer Exploit

- ▶ Use deployment mechanisms to deploy arbitrary code
  - Deploy over HTTP
  - BeanShell Deployer
- ▶ JBoss 4 and lower

# DeploymentFileRepository Exploit

- ▶ Upload a JSP to an existing app
  - ▶ Reported in 2006 and “fixed”
  - ▶ Directory traversal is not the real issue
  - ▶ JBoss 5.x IS vulnerable
  - ▶ Note that DeploymentFileRepository is part of the web console, not JMX console
- 

# Server Shutdown



# Status

- ▶ Often available even when JMX console or RMI service is not
- ▶ It's just status, right?

# “Secret” Tokens

- ▶ Don't put secret tokens into URLs

www.██████████.net POST /QMServlet/QMDownload/20142902/purchase.zip HTTP/1.1

- ▶ From Google cache

GET ██████search.seam?actionMethod=search.jsp%3AInitializationBean&cn=null&sn=3100&tech=internal&userid=██████&passwd=██████

- ▶ And other interesting things

-----  
91.98.125.161 www.██████████.org GET /cmd/cmd.jsp?cmd=ping%204.2.2.4 HTTP/1.1

# Deployed Applications

- ▶ ?full=true

## Application list

[localhost/](#)  
[localhost/██████services](#)  
[localhost/██████kiosk](#)  
[localhost/invoker](#)  
[localhost/jbossws](#)  
[localhost/jbossmq-httpil](#)

## Application list

[direct-admin-ui/work](#)  
[localhost/web-console](#)  
[direct-admin-ui/conf](#)  
[localhost/jbossmq-httpil](#)  
[express-ui/lib](#)  
[oak-ui/data](#)  
[oak-ui/log](#)  
[localhost/jmx-console](#)  
[oak-ui/conf](#)  
[express-ui/](#)  
[express-ui/deploy](#)  
[express-ui/data](#)  
[oak-ui/work](#)  
[localhost/jbossws](#)  
[oak-ui/tmp](#)  
[oak-ui/deploy](#)  
[direct-admin-ui/data](#)  
[direct-admin-ui/](#)  
[localhost/invoker](#)  
[express-ui/conf](#)  
[express-ui/log](#)  
[express-ui/work](#)  
[express-ui/tmp](#)  
[oak-ui/](#)  
[direct-admin-ui/tmp](#)  
[direct-admin-ui/lib](#)  
[oak-ui/lib](#)  
[localhost/](#)  
[direct-admin-ui/deploy](#)  
[direct-admin-ui/log](#)

# Finding JBoss

- ▶ <http://www.jboss.com/customers/>
- ▶ X-Powered-By
  - “Servlet X; JBoss Y” or “Servlet X; Tomcat Y/JBoss Z”
- ▶ Shodan
  - Results 1 – 10 of about 12811 for "x-powered-by" "jboss"
- ▶ Auth realm “JBoss JMX Console”
- ▶ And obviously...

---

Results 1 - 10 of about 549,000 for inurl:"jmx-console/HtmlAdaptor". (0.32 seconds)

# References

- ▶ <http://www.redteam-pentesting.de/en/publications/jboss>
- ▶ <https://media.blackhat.com/bh-eu-10/presentations/Papathanasiou/BlackHat-EU-2010-Papathanasiou-Abusing-JBoss-slides.pdf>
- ▶ <http://blog.mindedsecurity.com/2010/04/good-bye-critical-jboss-0day.html>