

Hacking weblogic

Hacking a default weblogic server using a web browser

Ammara reda
SySmox
Web security
Info@sysmox.com



We provide to a client a comprehensive Website Security Report, outlining security threats and current set of measures taken to prevent these threats, alongside with practical recommendation how to increase the security of the website.

[Http://www.sysmox.com](http://www.sysmox.com)

Table of Contents:

1 Introduction	2
2 Web logic	2
3 Default installation.....	3
3.1 The web application.....	4
3.2 deploy it	5
3.3 Backdooring the weblogic.....	6
4 Securing.....	7

1. Introduction:

Brief paper about how attackers can use the default password to hack the weblogic.

1.2 Weblogic :

Owned by Oracle Corporation, Oracle WebLogic consists of a Java EE platform product-family that includes:

- a Java EE application server, WebLogic Application Server
- an enterprise portal, WebLogic Portal
- an Enterprise Application Integration platform
- a transaction server and infrastructure, WebLogic Tuxedo
- a telecommunication platform, WebLogic Communication Platform
- an HTTP web server

2. Default installation :

A moderately high number of weblogic server keep the default password during the instalation . it is quite easy for an hacker to enter to the weblogic console and gain access to privat and sensitive information and data center ,This attack can be used for hackers in diferent ways .

Most WebLogic Administration Console start witht the default password:

Username : **weblogic** and the default Password is **weblogic**. Attacker need just to browse bLogic Server is `http://hostname:port`, where hostname is the name of the server where WebLogic is installed and port is the WebLogic port number (by default, 7001).

[Http://localhost:7001/console](http://localhost:7001/console)

Hackers can use different way to get list of web server running weblogics .

Here are list of default passwords:

<http://cirt.net/passwords?criteria=weblogic>

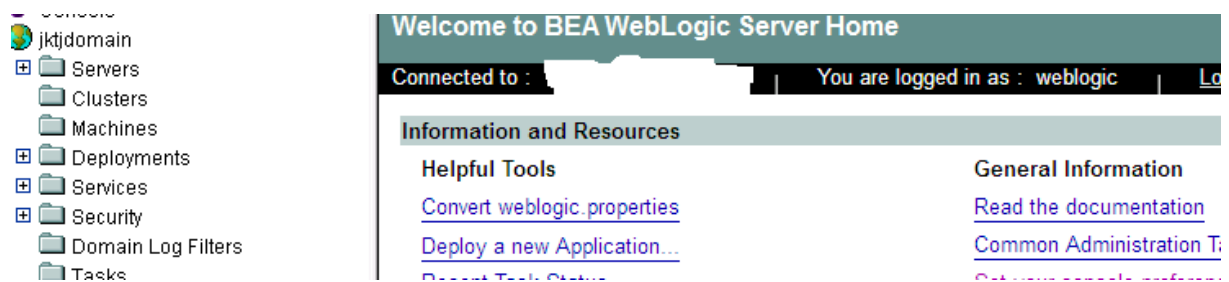
WebLogic Server Administration Console

Sign in to work with the WebLogic Server domain **jktjdomain**

Username:

Password:

Into the console:



The screenshot displays the WebLogic Server Administration Console. The left-hand side features a navigation tree with the following items: Servers, Clusters, Machines, Deployments, Services, Security, Domain Log Filters, and Tasks. The main content area is titled 'Welcome to BEA WebLogic Server Home'. Below the title, it shows 'Connected to : [redacted]' and 'You are logged in as : weblogic'. A section titled 'Information and Resources' is divided into two columns. The left column, 'Helpful Tools', includes links for 'Convert weblogic.properties', 'Deploy a new Application...', and 'Recent Task Status'. The right column, 'General Information', includes links for 'Read the documentation', 'Common Administration T...', and 'Get your console preferences...'.

3.1 The web application:

In order to deploy a web application via console:

Deploy => web application modules => Deploy a new Web Application Module...
=>upload your file(s) =>Deploy

In Web Application Modules :

A Web application on WebLogic Server includes the following files:

- At least one servlet or JSP, along with any helper classes.
- A `web.xml` deployment descriptor, a J2EE standard XML document that describes the contents of a WAR file.
- Optionally, a `weblogic.xml` deployment descriptor, an XML document containing WebLogic Server-specific elements for Web applications.
- A Web application can also include HTML and XML pages with supporting files such as images and multimedia files.

3.2 .Deploy it:

Attacker can upload a backdoor.war

Deployment Targets

This Web Application module will be deployed to the following locations:

sample will be deployed to
Servers - myserver

Source Accessibility

Since this is a single server environment, no further stage configuration is required. The server will access this Web Application module's files from the location specified.

Entity

Enter a name to be used to identify this Web Application module.

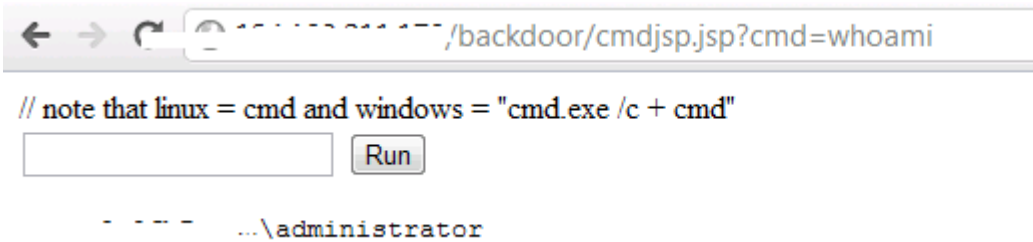
Name:

The name of this Web application deployment.

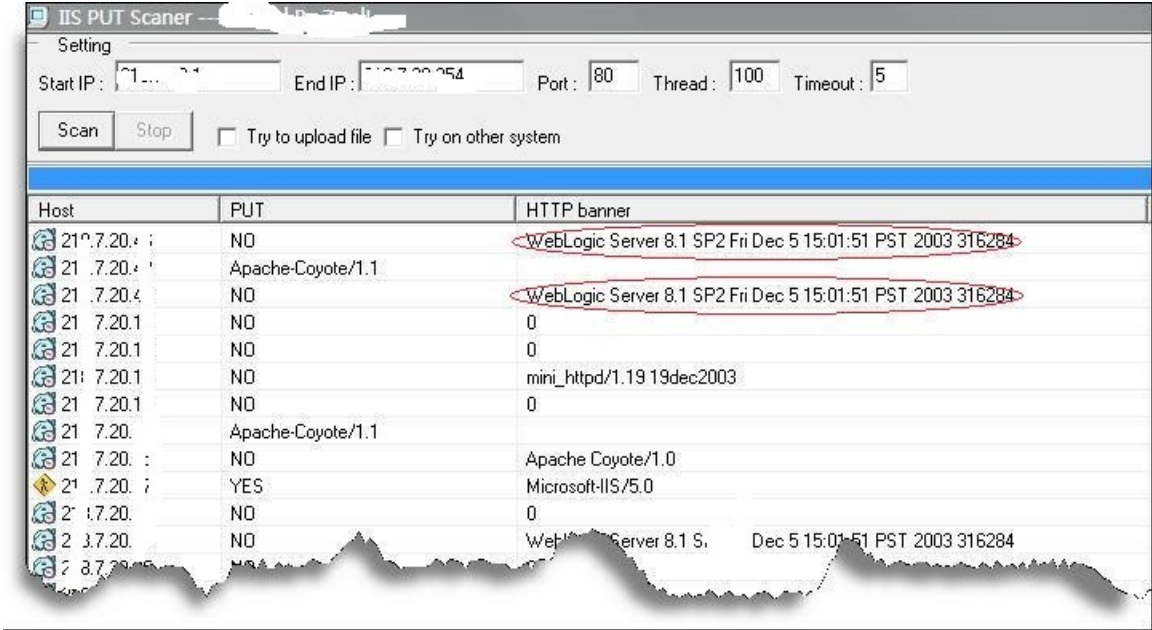
It is necessary to create a WAR file with WEB-INF a JSP to execute system commands. The WAR file should be deployed and and run commands using the cmdshell.jsp. These commands will be executed with the privileges of the weblogic server.

3.3 Backdooring the weblogic:

Here is a short example



Attackers can use different scanner to get weblogic server as google dork



4 .Securing the weblogic:

http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenvirom/configWLS.html#wp1099454

The main mission of sysmox is to conduct researches of different application and system vulnerabilities. The result of this work is then used by the experts of the sysmox Security audit department for assessing the security level of information systems with the use of active audit methods and also while carrying out penetration tests .

[Http://www.sysmox.com](http://www.sysmox.com)

