

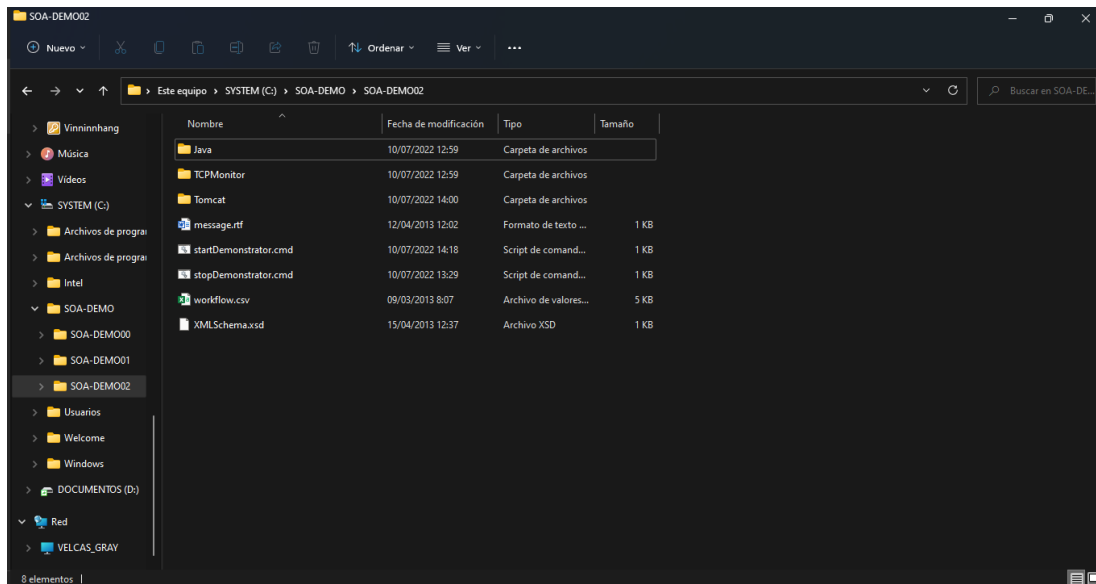
Asignatura	Datos del alumno	Fecha
Seguridad en Aplicaciones Online	GRUPO 29	11/07/2022
	Angel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	

Contenido

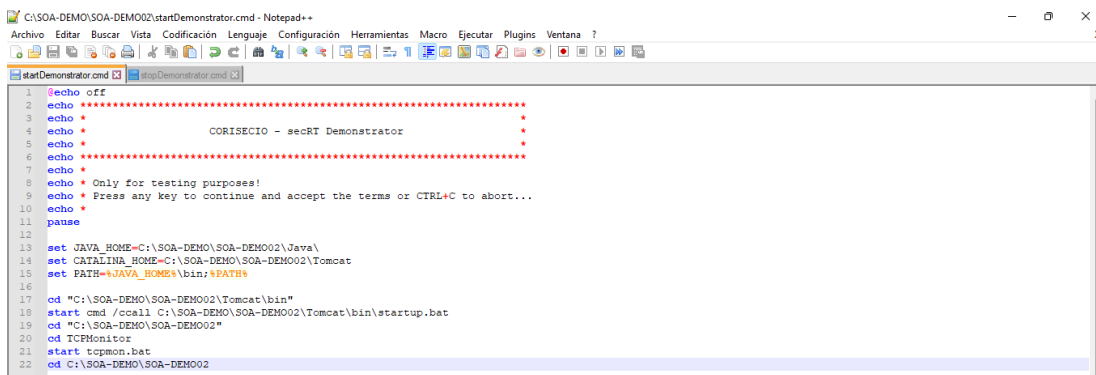
Configuraciones Iniciales	2
Tienda sin Seguridad – Sin Configurar	5
Conectores.....	9
Conector Consumer	10
Conector Provider	14
Conector Payment	16
Configuración de Open XML Gateway.....	17
Entity Consumer.....	18
Entity Provider	18
Request	19
Prueba de Bloqueo.....	21
Log Satisfactorio	22

Configuraciones Iniciales

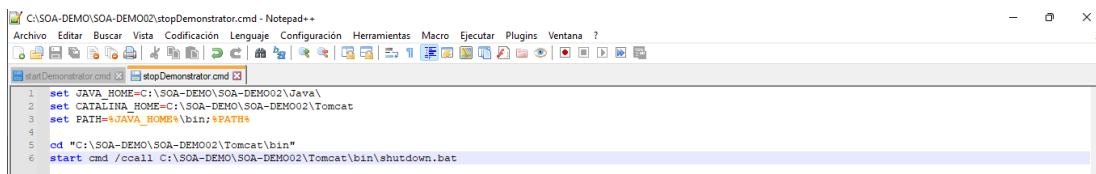
Se descarga SOA Demonstrator y se descomprime en este caso se le agrega un dígito a la carpeta de manera identificativa SOA-DEMO02 para posteriormente ejecutar el archivo startDemonstrator.cmd donde hay que actualizar las rutas de instalación del producto para un correcto arranque de TOMCAT con la versión de JAVA que trae consigo.



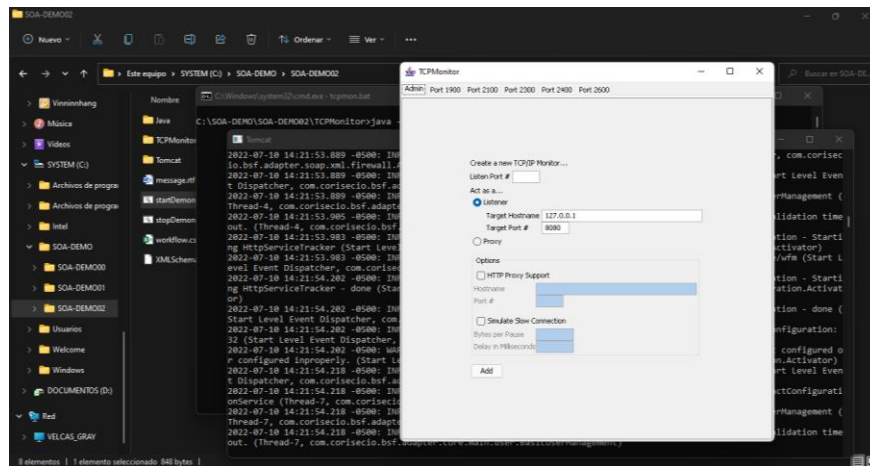
Se establecen las rutas necesarias para la ejecución del script startDemonstrator.cmd.



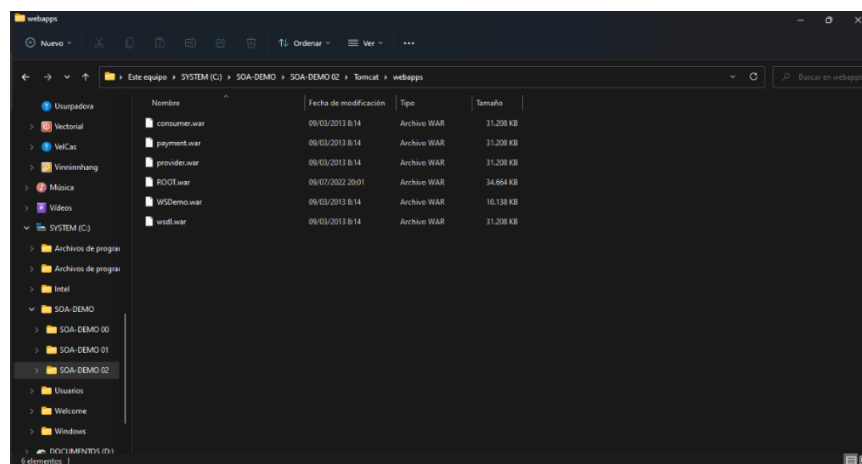
Es necesario crear el script stopDemonstrator.cmd para parar el servidor APACHE, con el siguiente contenido necesario como señala la siguiente imagen.



Posteriormente se ejecuta el script startDemostrator.cmd como administrador.

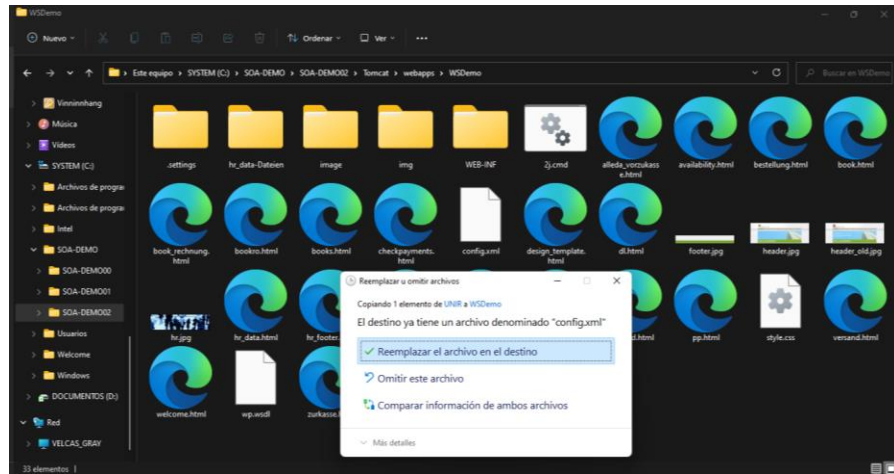


Posteriormente se copia ROOT.war a la carpeta webapps del del servidor TOMCAT Apache.

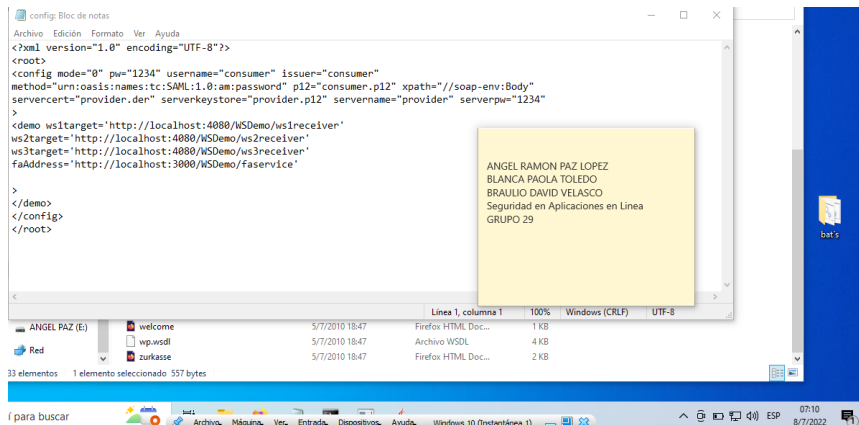


Arranque de Tomcat con las soluciones de seguridad y la aplicación TCPmonitor:

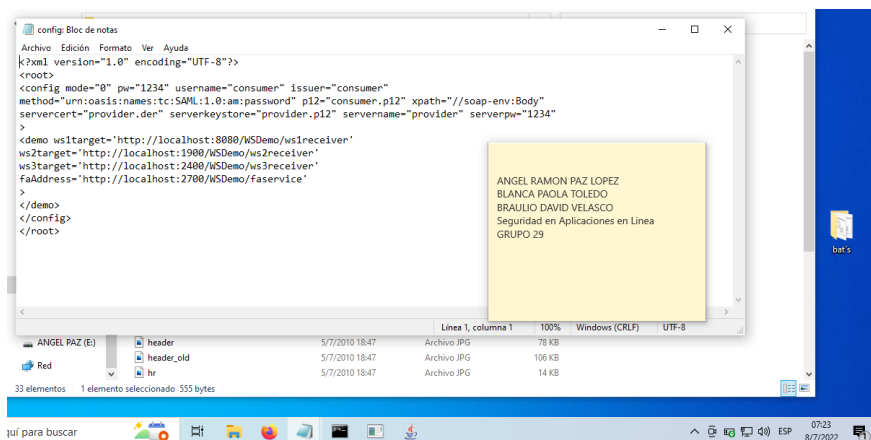
- Se ejecuta startDemonstrator.cmd arranca Tomcat, despliega SOA DEMOSTRATOR y XMLGATEWAY y arranca TCPMONITOR.
- Después de arrancar el servidor se descarga el fichero config.xml de:
 - o <https://www.dropbox.com/sh/cgkzwq2z6qyy1kd/viPuZUC2ln>
- Una vez descargado, hay que sustituir el fichero config.xml que viene por defecto en la instalación que tiene la parametrización correcta de puertos, para navegar a través de los puertos de TCPMONITOR en la ubicación:
 - o C:\SOA-DEMO\SOA-DEMO02\Tomcat\webapps (En nuestro caso GRUPO-29)



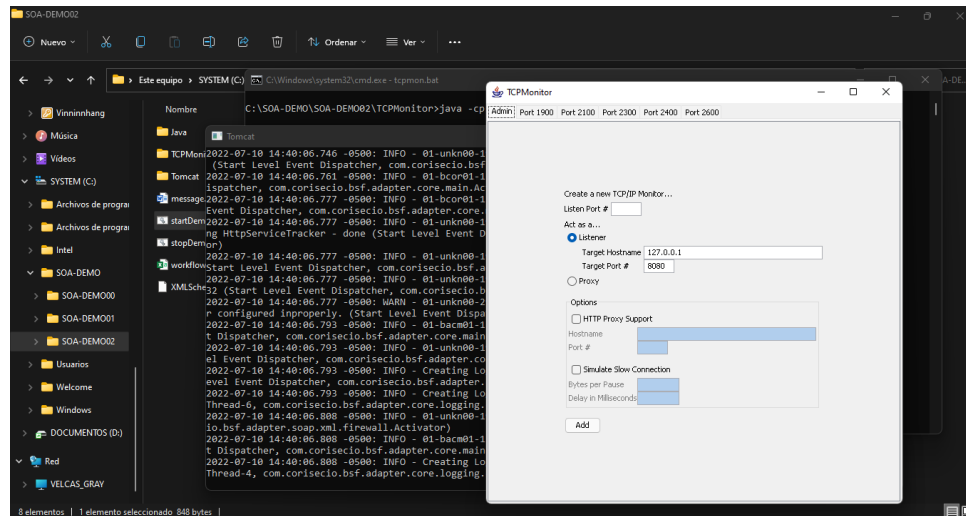
CONFIG POR DEFAULT



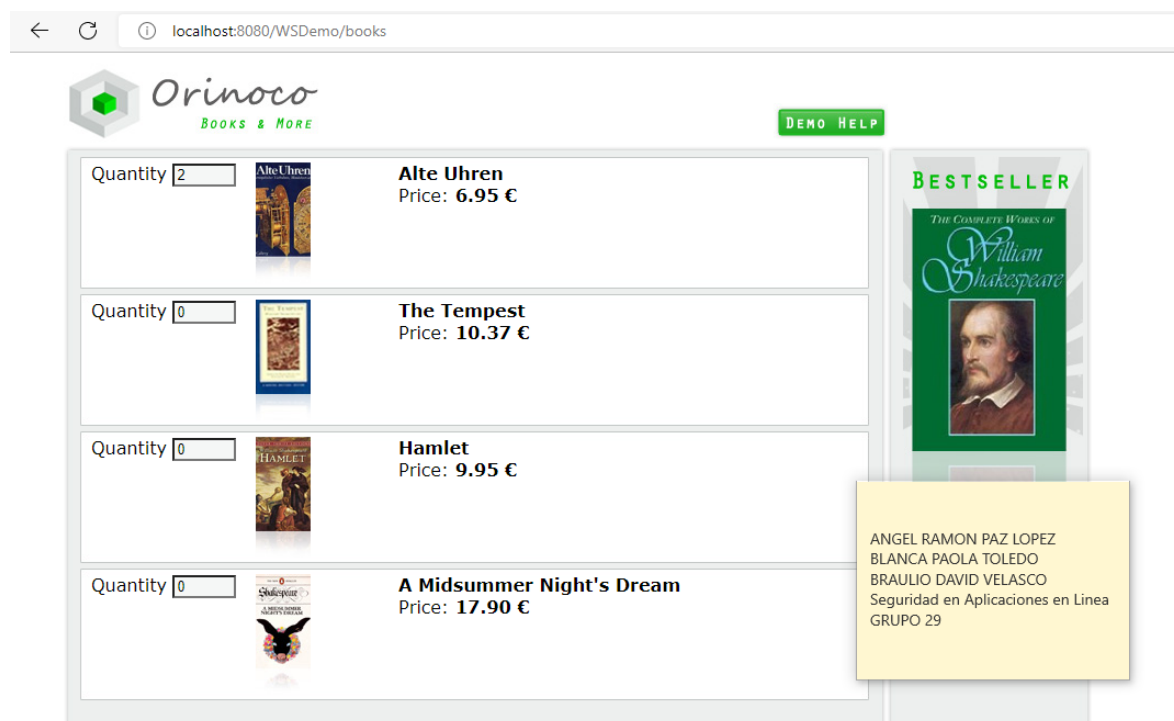
CONFIG DESCARGADO



Seguidamente ejecutamos el script startDemonstrator.cmd para que se cargue la nueva configuración de TOMCAT Apache y realice el acceso a los diversos conectores de seguridad de SOA demonstrator y GATEWAY XML



Tienda sin Seguridad – Sin Configurar



Please enter the required information.

Lastname:
 Firstname:
 Street:
 ZIP:
 City:
 E-Mail:
 Credit Card:
 Credit Card validation:
 Security Code:

BESTSELLER

ANGEL RAMON PAZ LOPEZ
 BLANCA PAOLA TOLEDO
 BRAULIO DAVID VELASCO
 Seguridad en Aplicaciones en Linea
 GRUPO 29

Orinoco
BOOKS & MORE

The following articles have been ordered.

2 x Alte Uhren a 6.95 €

Total 13.90 Euro

ANGEL RAMON PAZ LOPEZ
 BLANCA PAOLA TOLEDO
 BRAULIO DAVID VELASCO
 Seguridad en Aplicaciones en Linea
 GRUPO 29

BESTSELLER

Ahora revisamos el TCP Monitor

TCPMonitor

Admin Port 1900 Port 2100 Port 2300 Port 2400 Port 2600 Port 4080

Listen Port: 4080 Host: 127.0.0.1 Port: 8080 ☐ Proxy

State	Time	Request Host	Target Host	Request...
---	Most Recent	---	---	---
Done	2022-07-11 08:08:00	127.0.0.1	127.0.0.1	POST /WSDemo/ws1receiver HTTP/...
Done	2022-07-11 08:10:24	127.0.0.1	127.0.0.1	POST /WSDemo/ws2receiver HTTP/...
Done	2022-07-11 08:10:24	127.0.0.1	127.0.0.1	POST /WSDemo/ws3receiver HTTP/...

```

Pragma: no-cache
User-Agent: Java/1.5.0_20
Host: 127.0.0.1:4080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 520

<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope">
  <soap-env:Header>
    <soap-env:HeaderFault fault="1" faultcode="s:ReceiverNotFound" faultactor="http://schemas.xmlsoap.org/soap/envelope/ReceiverNotFound" faultreason="s:ReceiverNotFound" />
  </soap-env:Header>
  <soap-env:Body>
    <soap-env:BodyFault fault="1" faultcode="s:ReceiverNotFound" faultactor="http://schemas.xmlsoap.org/soap/envelope/ReceiverNotFound" faultreason="s:ReceiverNotFound" />
  </soap-env:Body>
</soap-env:Envelope>
  
```

HTTP/1.1 200 OK
 Server: Apache-Coyote/1.1
 Content-Type: text/xml; charset=utf-8
 Content-Length: 388

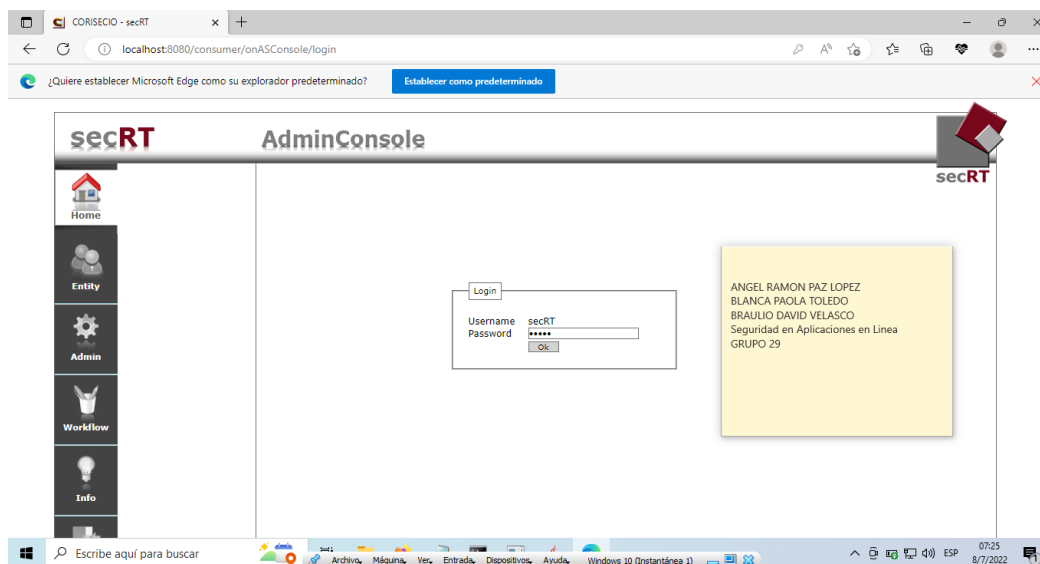
☐ XML Format ☐ Numeric

Y podemos ver la información en texto claro

```
<s:customer s:name="mond" s:vname="uval" s:strasse="vegas" s:plz="44556" s:ort="eua" s:mail=""><s:paymentInformation><s:creditCard s:cc="9525488554611111" s:ccv1="
```

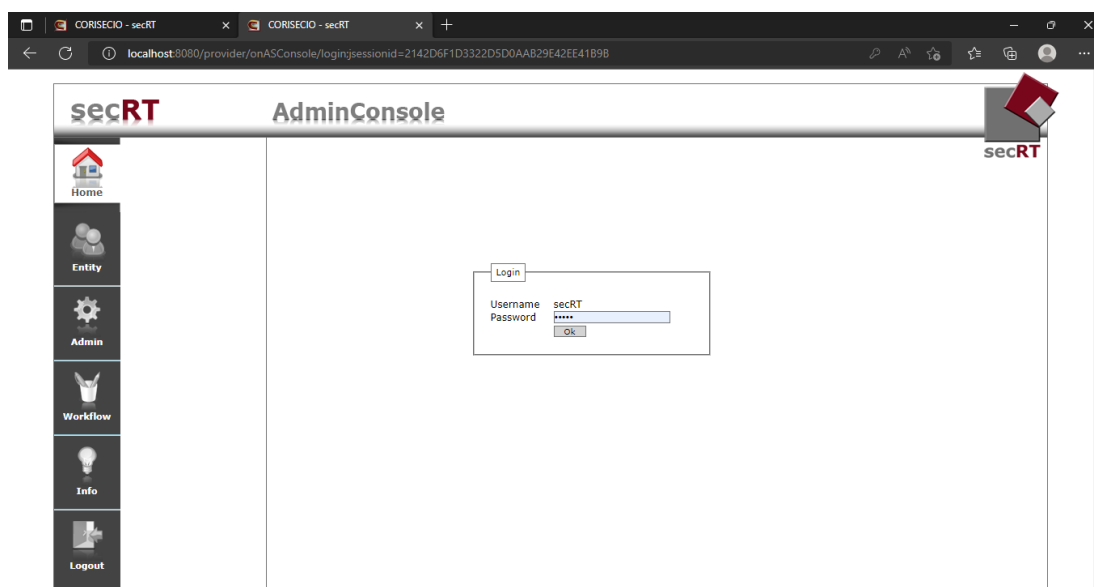
Ahora, es posible desplegar en nuestro navegador la siguiente dirección para consumidores:

o <http://localhost:8080/consumer>



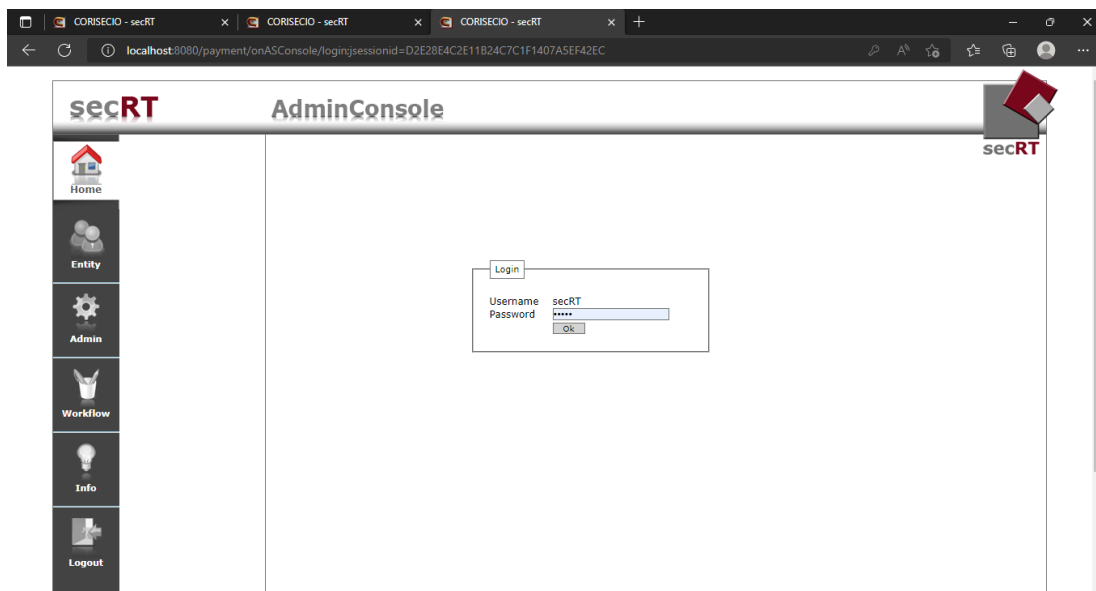
Hacemos lo mismo para proveedores.

o <http://localhost:8080/provider>



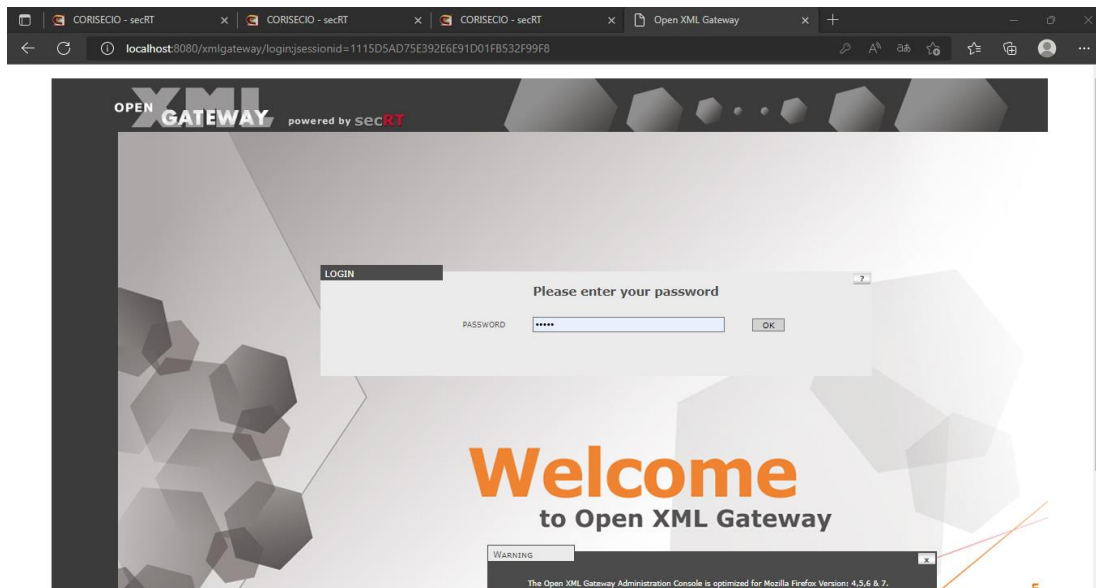
Por último, el link de pagos:

o <http://localhost:8080/payment>



Ahora procedemos a ingresar Open Gateway XML con:

o <http://localhost:8080/XMLGATEWAY>



Conectores

Antes de que se pueda utilizar el conector, la conexión a la base de datos debe configurarse mediante el menú en Data Store. Esto al iniciar sesión por primera vez en cada conector como señala (CORISECIO, 2011).

- o Se realiza con los conectores Consumer, Provider y Payment.

The screenshot shows the 'Configuration Wizard' window for the 'Consumer' connector. The interface includes a sidebar with icons for Home, Entity, Admin, and Workflow. The main content area contains a welcome message and instructions for configuring the data store. The configuration fields are as follows:

Path	C:\SOA-DEMO\SOA-DEM002\consumer
Username	secRT
Password	secRT
Encryption Key	1E1BAA356088EBB4693380CE3F3E1FD6

An 'Apply' button is located at the bottom of the configuration fields.

The screenshot shows the 'Configuration Wizard' window for the 'Provider' connector. The interface is identical to the previous one, but the configuration fields are for the 'Provider' connector:

Path	C:\SOA-DEMO\SOA-DEM002\provider
Username	secRT
Password	secRT
Encryption Key	0EA238C6536FC92990FAFE2EA18123C

An 'Apply' button is located at the bottom of the configuration fields.

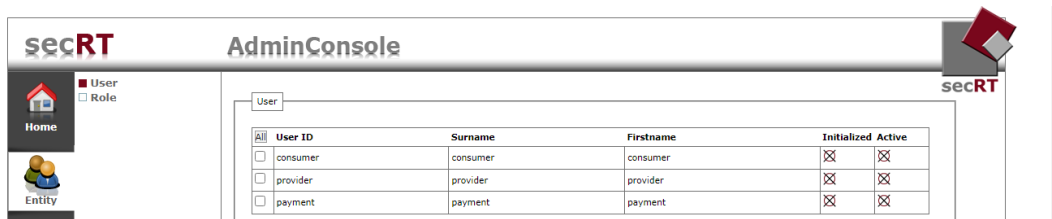
The screenshot shows the 'Configuration Wizard' window for the 'Payment' connector. The interface is identical to the previous ones, but the configuration fields are for the 'Payment' connector:

Path	C:\SOA-DEMO\SOA-DEM002\payment
Username	secRT
Password	secRT
Encryption Key	1C085A301DF9FE902EF52CB04DBA2F90

An 'Apply' button is located at the bottom of the configuration fields.

Conector Consumer

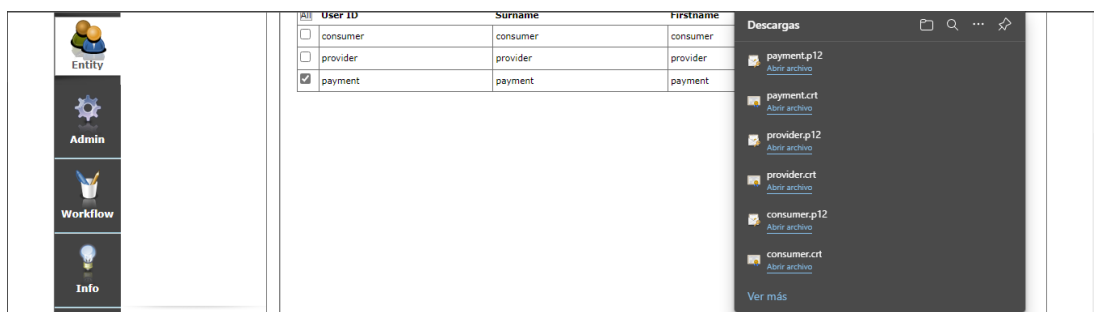
Se crean los usuarios en el conector consumer para posteriormente exportarlos y ser importados a los demás conectores



Se puede realizar el proceso de inicialización de todos los usuarios a la vez



Para descargar el Certificado y el Keystore se tiene que hacer individualmente (consumer, provider y payment), ya que no soporta múltiples selecciones.



Se crean los roles de usuarios para posteriormente exportarlos e importarlos al resto de los conectores

AdminConsole

Role

All	Name	Description
<input type="checkbox"/>	rol_consumer	
<input type="checkbox"/>	rol_provider	
<input type="checkbox"/>	rol_payment	

ANGEL RAMON PAZ LOPEZ
BLANCA PAOLA TOLEDO
BRAULIO DAVID VELASCO
Seguridad en Aplicaciones en Línea
GRUPO 29

Se asignan roles de cada usuario

secRT AdminConsole

■ User
□ Role

Home

Entity

Assign roles to [consumer]

Name	All
rol_consumer	<input checked="" type="checkbox"/>
rol_provider	<input type="checkbox"/>
rol_payment	<input type="checkbox"/>

secRT AdminConsole

■ User
□ Role

Home

Entity

Assign roles to [provider]

Name	All
rol_consumer	<input type="checkbox"/>
rol_provider	<input checked="" type="checkbox"/>
rol_payment	<input type="checkbox"/>

secRT AdminConsole

■ User
□ Role

Home

Entity

Assign roles to [payment]

Name	All
rol_consumer	<input type="checkbox"/>
rol_provider	<input type="checkbox"/>
rol_payment	<input checked="" type="checkbox"/>

Exportamos usuarios, roles de usuarios, asignación de usuarios para importar al resto de conectores

secRT AdminConsole

■ Import / Export
□ Policy Subscription
□ Data Store
□ Root Certificate
□ Change Password
□ WSDL-API
□ API User

Home

Entity

Admin

Workflow

Import

User Elegir archivo No se ha seleccionado ningún archivo

Import

Export

Userroles

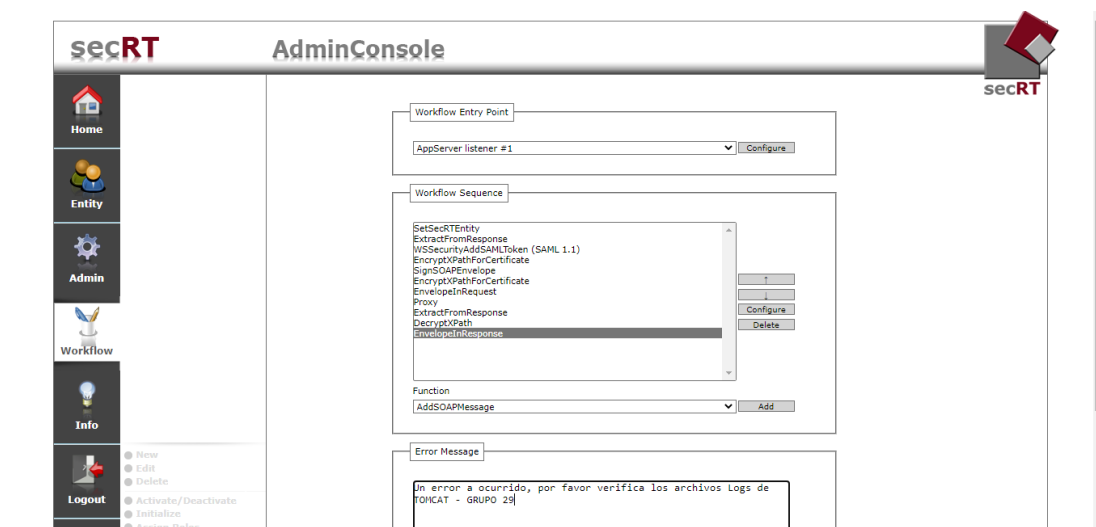
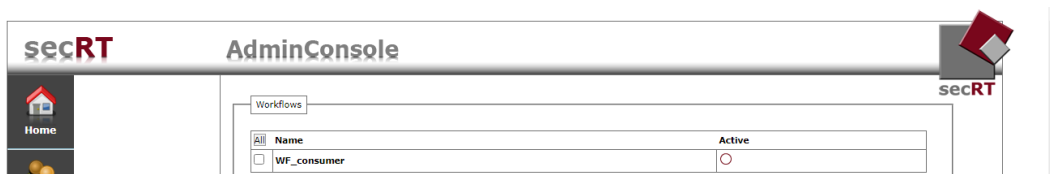
Export

Descargas

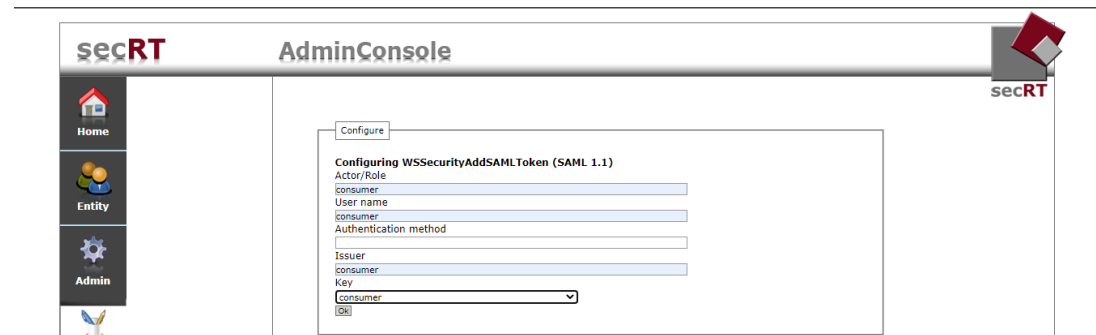
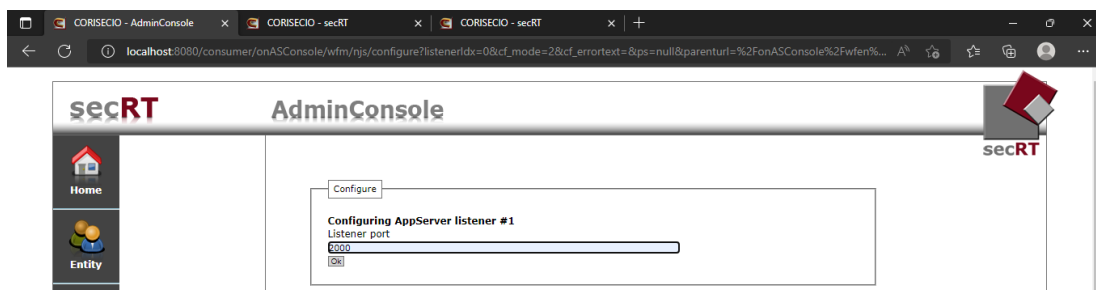
- import (2).csv [Abrir archivo](#)
- import (1).csv [Abrir archivo](#)
- import.csv [Abrir archivo](#)
- payment.p12 [Abrir archivo](#)
- payment.crt [Abrir archivo](#)
- provider.p12 [Abrir archivo](#)
- provider.crt [Abrir archivo](#)
- consumer.p12 [Abrir archivo](#)
- consumer.crt [Abrir archivo](#)

Ver más

Se crea el Workflow de consumer donde se aplican y configuran las funciones de seguridad de autenticación, firma y cifrado de la petición-respuesta en cada conector de seguridad desplegados en el servidor de aplicaciones Apache Tomcat y en donde también están desplegados los servicios web.



Se establecen las principales configuraciones.



secRT

AdminConsole

secRT

Home

Entity

Admin

Workflow

Configure

Configuring EncryptXPathForCertificate

Encryption certificate

☒ Internal

payment

☐ External

Change

XPath

//*[local-name()='paymentInformation']

OK

secRT

AdminConsole

secRT

Home

Entity

Admin

Workflow

Configure

Configuring EncryptXPathForCertificate

Encryption certificate

☒ Internal

provider

☐ External

Change

XPath

//*[local-name()='Order']

OK

secRT

AdminConsole

secRT

Home

Entity

Admin

Workflow

Info

Logout

Configure

Configuring Proxy

Schema

http

Target address

127.0.0.1

Target port

2100

Rewrite content types

Rewrite content types

New

Edit

Delete

Request rewrite rules

Rewriting rule

New

Edit

Delete

Response rewrite rules

Rewriting rule

New

Edit

Delete

Trusted SSL certificates

secRT

AdminConsole

secRT

Home

Entity

Configure

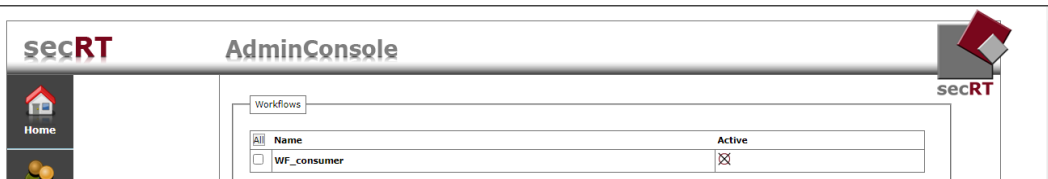
Configuring DecryptXPath

XPath

//*[local-name()='OrderingResult']

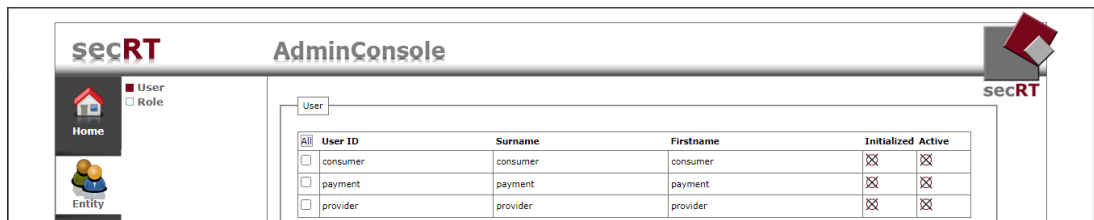
OK

Podemos visualizar el Workflow activado

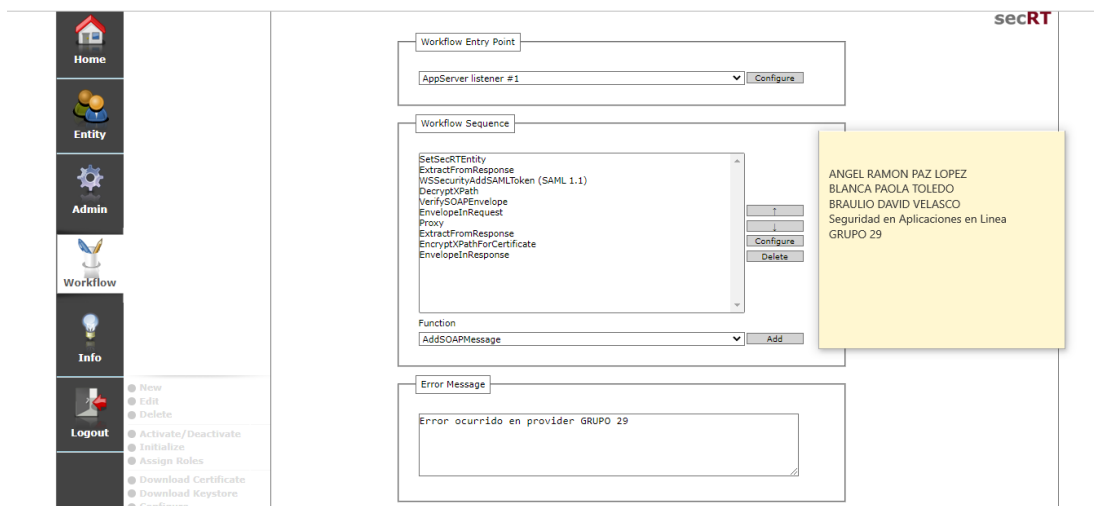


Conector Provider

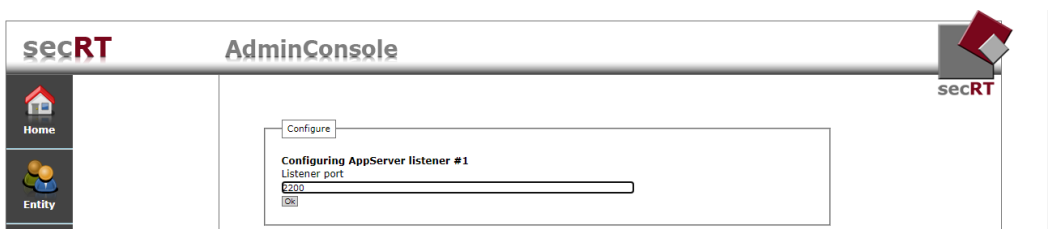
Como primer paso en el conector Provider se procede a importar los usuarios, roles de usuarios y roles asignados que con anterioridad fueron exportados.

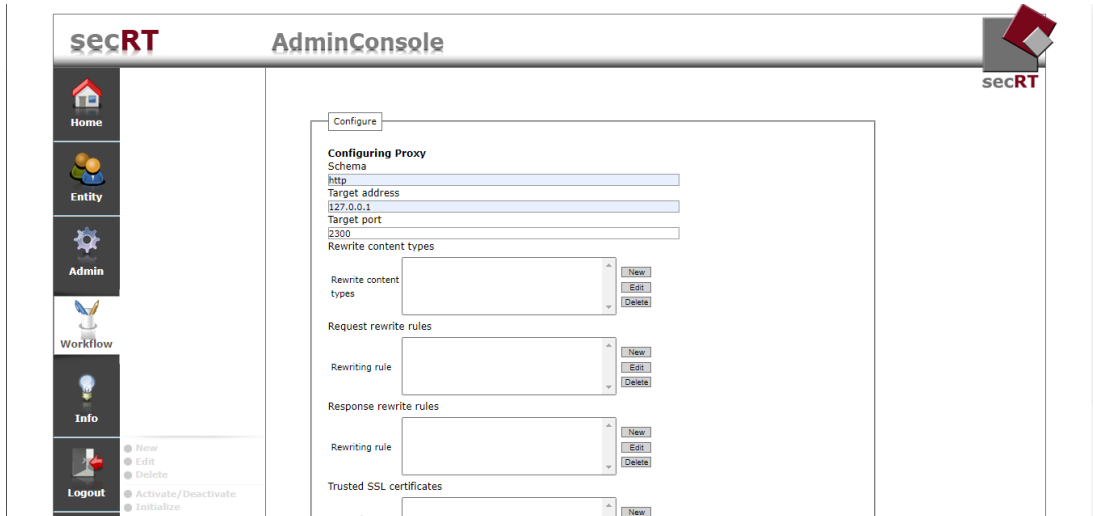


Se crea el Workflow Provider encargado de descifrar la petición. Es decir, descifra el elemento Order de la petición del consumer y verifica la firma. Configurando y agregando las siguientes funciones:

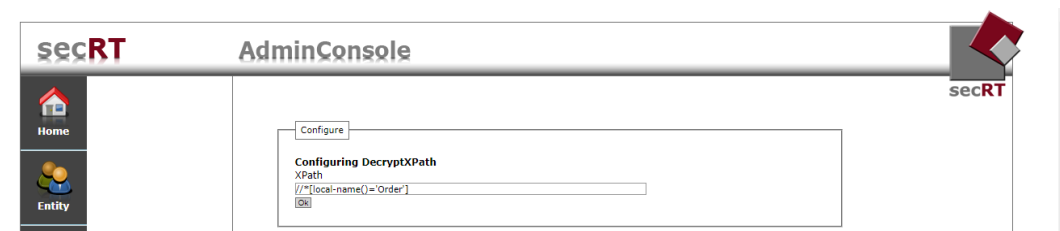


Se establecen las siguientes configuraciones de cada función del conector Provider.



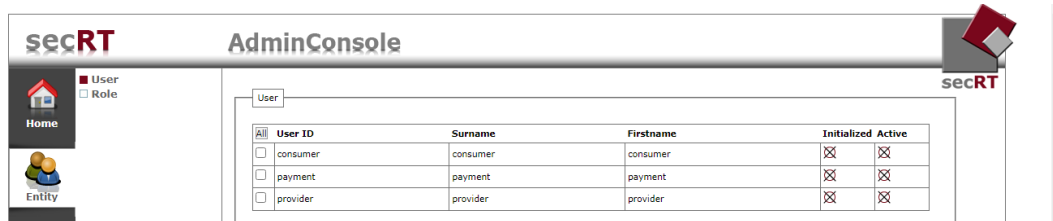


Podemos visualizar el Workflow activado:



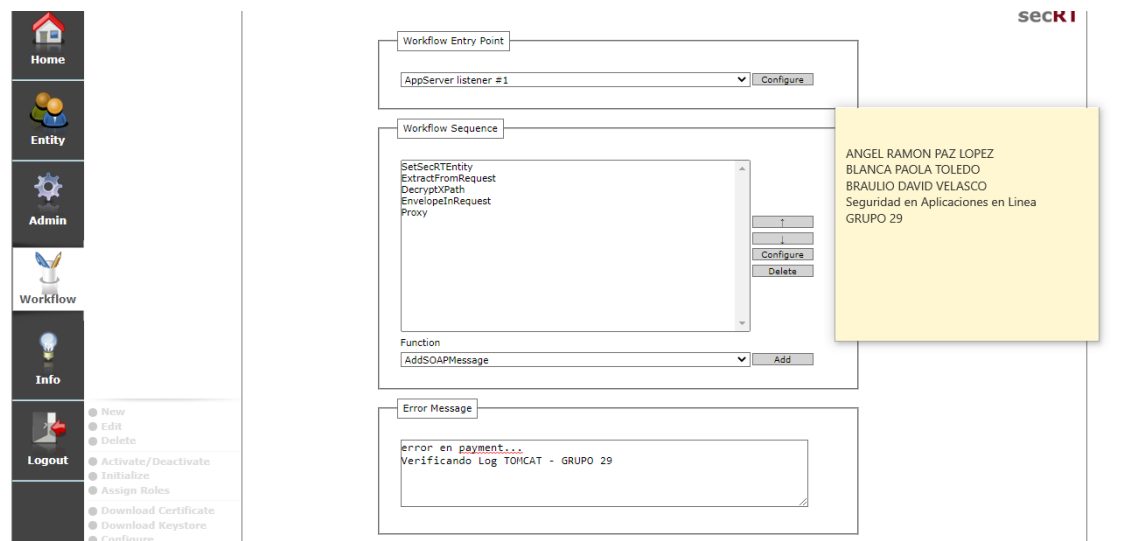
Conector Payment

Se realiza primeramente en EL conector payment la importación de usuarios, roles de usuarios y asignación de roles que fueron exportados con anterioridad.



User ID	Surname	Firstname	Initialized	Active
consumer	consumer	consumer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
payment	payment	payment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
provider	provider	provider	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Se procede a crear el Workflow Payment el cual se encargará de descifrar la información de pago. Para ello se debe configurar y agregar las siguientes funciones en el menú WORKFLOW.



Workflow Entry Point: AppServer listener #1

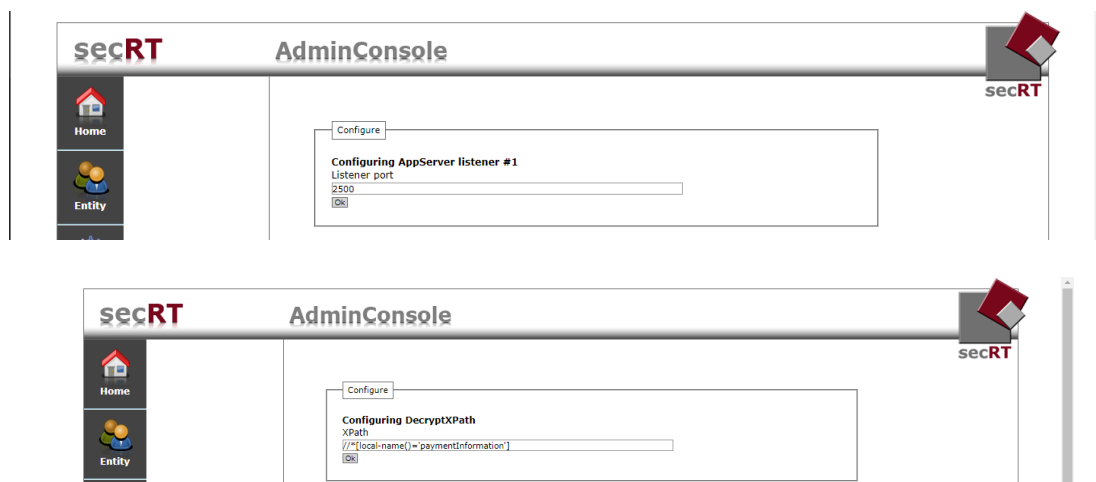
Workflow Sequence:

- SetSecRTEntity
- ExtractFromRequest
- DecryptXPath
- EnvelopeInRequest
- Proxy

Function: AddSOAPMessage

Error Message: error en payment... Verificando Log TOMCAT - GRUPO 29

Configuraciones de las funciones en Payment.



Configure

Configuring AppServer listener #1

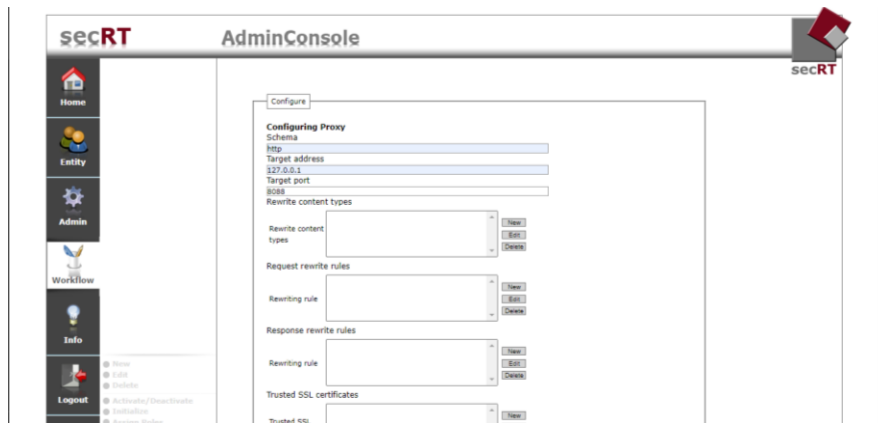
Listener port: 2500

Configure

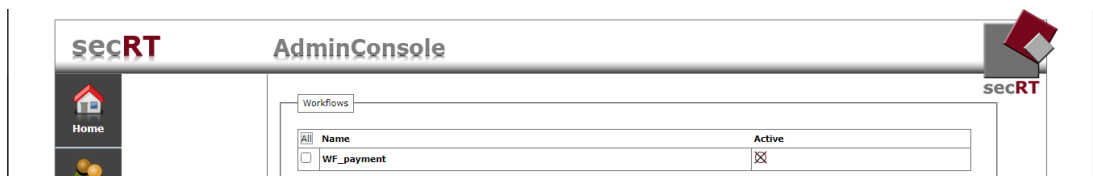
Configure

Configuring DecryptXPath

XPath: `//*[local-name()='paymentInformation']`

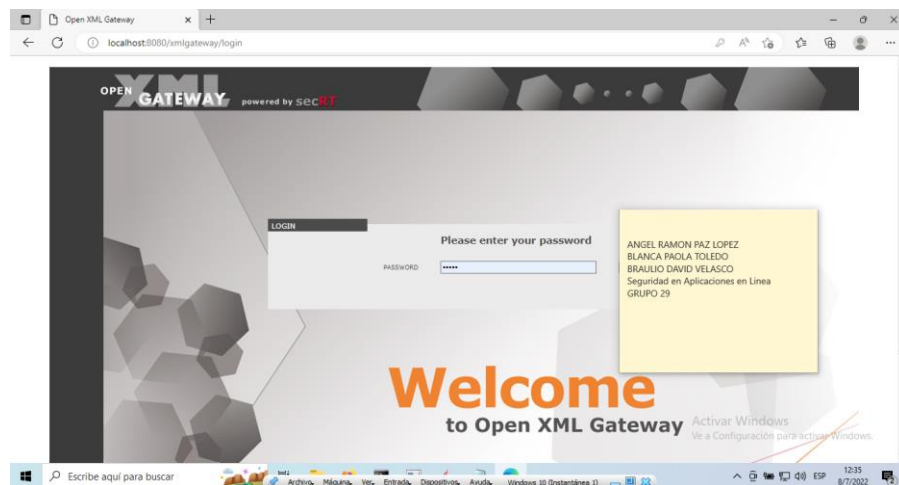


Podemos visualizar el Workflow activado.



Configuración de Open XML Gateway.

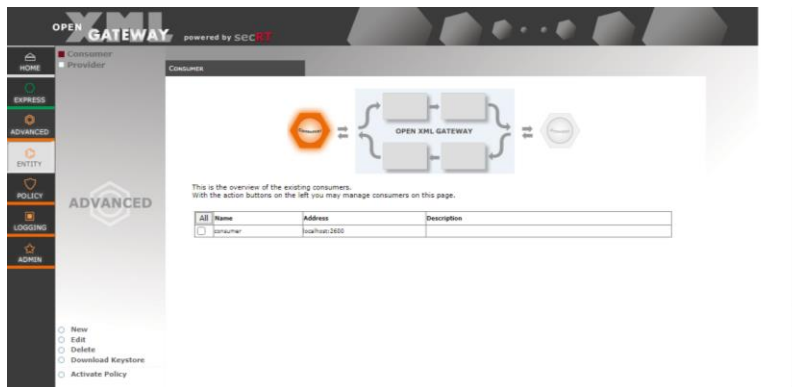
Se ingresa a la dirección: <http://localhost:8080/xmlgateway> donde se ingresa el password: secRT para el inicio de sesión.



A la vez al seleccionar el apartado de Entity se puede configurar el Consumidor y el Proveedor. En los consumidores están clientes autorizados y en el proveedor es la identidad que usa para la firma y tokens SAML como señala la guía de administración de open Gateway XML. Por ello es necesario la creación de un usuario en Consumer y Provider

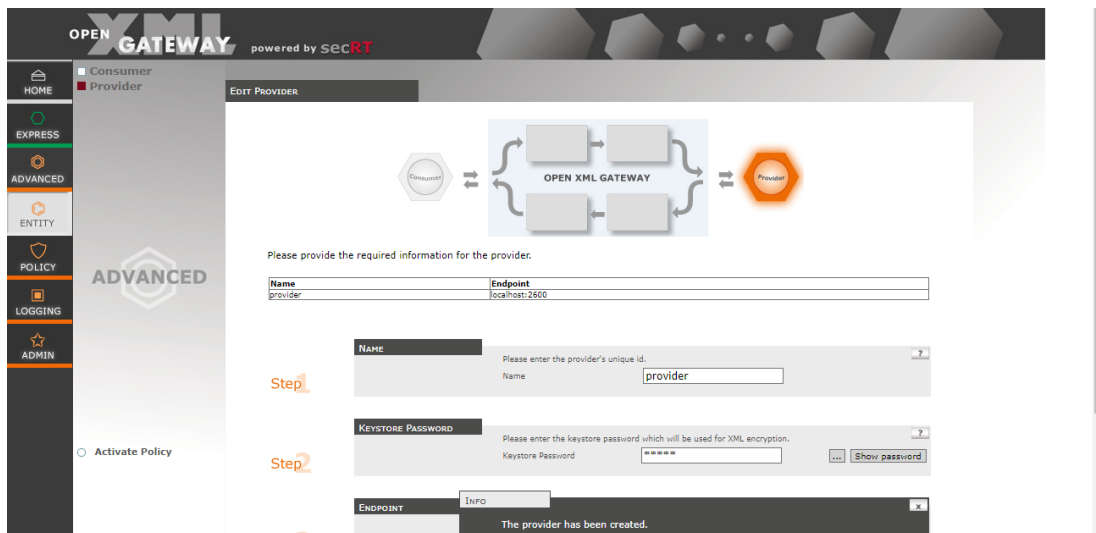
Entity Consumer.

Se crea un nuevo usuario consumer como señala la siguiente imagen

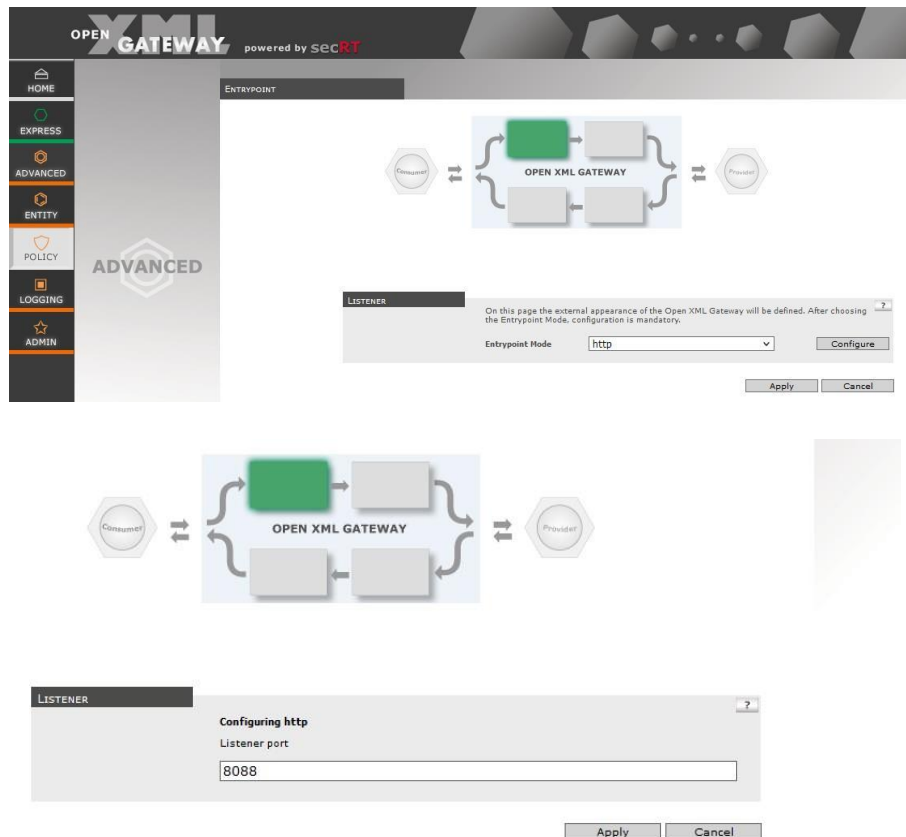


Entity Provider

De la misma manera se crea un nuevo usuario Provider configurando los siguientes apartados

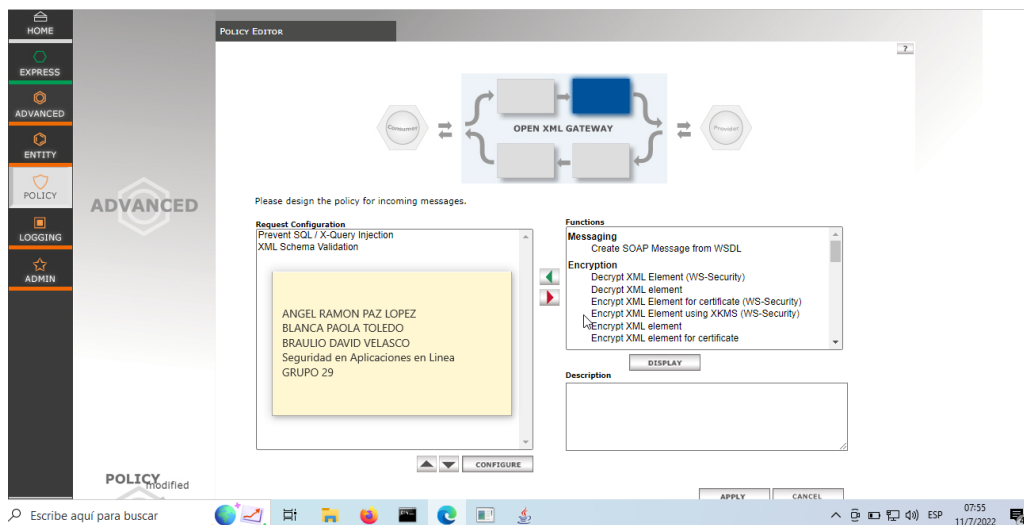


Mediante el Editor de directivas se configura la Puerta de enlace XML que se encuentra en el apartado Policy. En donde se selecciona un elemento para ser configurado; creando primeramente un Listener y su configuración de puerto de escucha.



Request

Se selecciona una Solicitud y se configura el procesamiento de la solicitud. En donde en el lado izquierdo se observa la configuración actual de la Política (Solicitud de Configuración lista) y en el lado derecho todas las funciones disponibles como la indica la guía de administración de open Gateway xml



OPEN XML GATEWAY powered by SecRT

HOME

EXPRESS

ADVANCED

ENTITY

POLICY

LOGGING

ADMIN

ADVANCED

POLICY

modified

ATTENTION

CONFIGURE

```

graph LR
    Consumer[Consumer] --> Gateway[OPEN XML GATEWAY]
    Gateway --> Provider[Provider]

```

NEW ENTRY

New entry

Name

Ataque SQL

Regular expression

/([%27])(\^)([!-~])([%23])([=])/ix (BROADCOM, 2004)

Apply

Cancel

OPEN XML GATEWAY

powered by secRT

HOME

Overview

About

Help

EXPRESS

ADVANCED

LOGOUT

HOME

Info

Status

OVERVIEW

STATUS

Welcome to the Open XML Gateway, a security solution based on CORISECIO secRT.

Using the Open XML Gateway you can protect your company's XML based communication against attacks. It provides standard WS Security methods like encryption and signature and even includes XML Firewall functionality against XML attacks.

Open XML Gateway provides an easy configurable user interface. It offers two operating modes - Express Mode and Advanced Mode.

The Express Mode enables the user to configure the Open XML Gateway in just a few steps. Three security levels are provided in this mode - low, medium and high. Please see the security level page for further details.

The Advanced Mode provides enhanced configuration options for experts. It relies on the security levels provided by the Express Mode, but you may also modify the settings or even create new security configurations.

Thank you for choosing CORISECIO Open Source XML Gateway.

Open XML Gateway

RUNNING

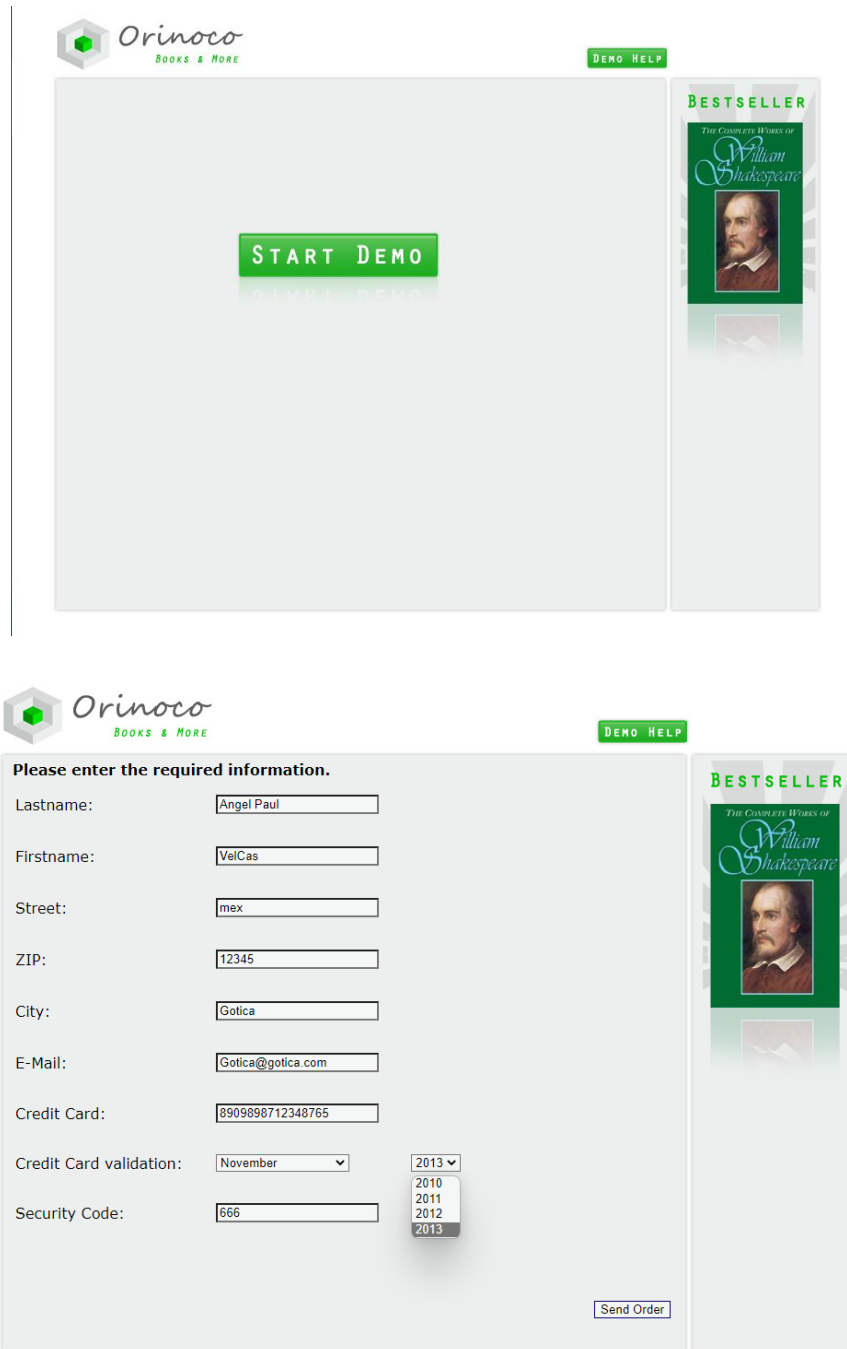
Restart

Stop

Prueba de Bloqueo.

Se realiza la selección de la orden de libros y se procede a llenar el formulario de la orden de pago en donde se pretende realizar un ataque de inyección en la siguiente dirección:

- <http://localhost:8080/WSDemo/welcome>

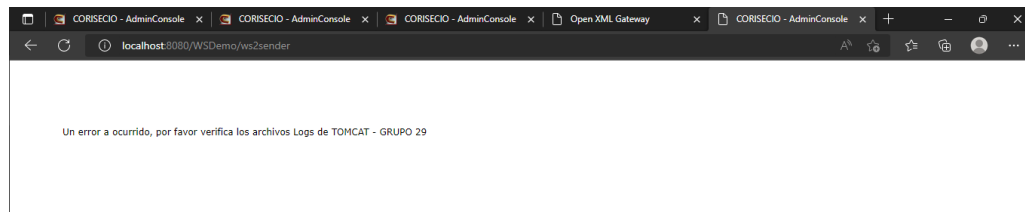


The screenshot shows the Orinoco Books & More website. The header includes the Orinoco logo and a 'DEMO HELP' button. The main content area features a large 'START DEMO' button. On the right side, there is a 'BESTSELLER' section displaying 'The Complete Works of William Shakespeare' with a portrait of Shakespeare.

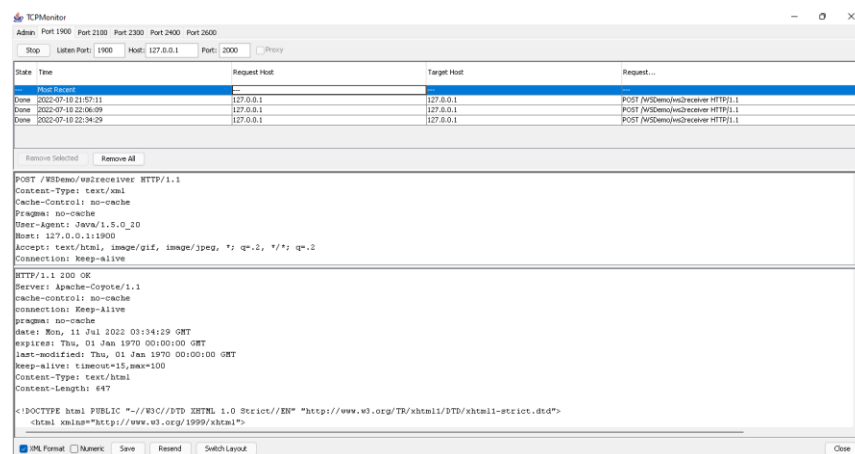
Please enter the required information.

Lastname:	<input type="text" value="Angel Paul"/>
Firstname:	<input type="text" value="VelCas"/>
Street:	<input type="text" value="Imex"/>
ZIP:	<input type="text" value="12345"/>
City:	<input type="text" value="Gotica"/>
E-Mail:	<input type="text" value="Gotica@gotica.com"/>
Credit Card:	<input type="text" value="8909898712348765"/>
Credit Card validation:	<input type="text" value="November"/> <input type="text" value="2013"/>
Security Code:	<input type="text" value="666"/>

El ataque no es satisfactorio para el usuario y se obtiene la respuesta que se colocó en el mensaje.



De tal manera se corrobora en el apartado de logs de Open XML Gateway como el mensaje es bloqueado.



Log Satisfactorio

OPEN XML GATEWAY powered by secRT

LOGGING

Please select the required time range for the log information. Log events will be displayed in the histogram below.

From: 2022-07-10 00:00:00 To: 2022-07-10 23:59:59 Show

time

Log Messages Message Count: 3





Status	Date	Message ID	Source
Red	2022-07-10 21:57:11.857 -0500	1625637482777-236504	127.0.0.1
Green	2022-07-10 22:06:14.647 -0500	1625642094394-055516	127.0.0.1
Green	2022-07-10 22:34:29.636 -0500	1625642714636-821743	127.0.0.1

Message Details

Message blocked. An SQL Injection was found in the message. The specific rule Ataque SQL matched.


Message

<?xml version="1.0" encoding="UTF-8"?><soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/"><soap-env:Header/><soap-env:Body><s:CheckPayment s:date="2022-07-10" xmlns:s="http://demo-book-shop/ns"><s:customer s:mail=" s:name="Angel Paul" s:ort="Gotica" s:plz="12345" s:stراس="max" s:vname="VelCae"><s:paymentInformation><s:creditCard s:amount="75.00" s:cc="890898712348765" s:cvt1="November" s:ccv2="2013" s:code="666"/></s:paymentInformation></s:customer></s:CheckPayment></soap-env:Body></soap-env:Envelope>

Quantity <input type="text" value="1"/>		Alte Uhren Price: 6.95 €
Quantity <input type="text" value="2"/>		The Tempest Price: 10.37 €
Quantity <input type="text" value="1"/>		Hamlet Price: 9.95 €
Quantity <input type="text" value="0"/>		A Midsummer Night's Dream Price: 17.90 €

BESTSELLER

The Complete Works of
William Shakespeare




Please enter the required information.

Lastname:
 Firstname:
 Street:
 ZIP:
 City:
 E-Mail:
 Credit Card:
 Credit Card validation:
 Security Code:

BESTSELLER

The Complete Works of
William Shakespeare



The following articles have been ordered.

1 x Hamlet a 9.95 €
 2 x The Tempest a 10.37 €
 1 x Alte Uhren a 6.95 €

Total 37.64 Euro

BESTSELLER

The Complete Works of
William Shakespeare





Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNumber	CCValid	CCCheckNumber	Amount
20210707	waldo drt	mex	467	mexico		5288439105506911	January/2010	103	27.00
20210707	waldo drt	mex	467	mexico		5288439105506911	January/2010	103	27.00
20210707	durp ray	mex	467	mexico		5288439105506911	January/2010	103	27.00
20210707	durp kardom	mex	467	mexico		4907627910001234	July/2011	643	27.00
20210707	uvald mond	vegas	445556	eua		4907627910001234	January/2010	643	37.00



Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNummer	CCValid
2021-07-07	waldo drt	mex	467	mexico		5288439105506911	January/2010

Artikel	Menge	Preis
The Tempest	2	20.74
Alte Uhren	1	6.95

Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNummer	CCValid
2021-07-07	waldo drt	mex	467	mexico		5288439105506911	January/2010

Artikel	Menge	Preis
The Tempest 2		20.74
Alte Uhren 1		6.95

Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNummer	CCValid
2021-07-07	durp ray	mex	467	mexico		5288439105506911	January/2010

Artikel	Menge	Preis
The Tempest 2		20.74
Alte Uhren	1	6.95

Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNumber	CCValid
2021-07-07	durp kardom	mex	467	mexico		4907627910001234	July/2011

Artikel	Menge	Preis
Alte Uhren	1	6.95
The Tempest	2	20.74

Datum	Kunde	Strasse	PLZ	Ort	Mail	CCNummer	CCValid
2021-07-07	uvald mond	vegas	44556	eua		4907627910001234	January/2010

Artikel	Menge	Preis
Hamlet	1	9.95
The Tempest	2	20.74
Alte Uhren	1	6.95