



OWASP

Open Web Application
Security Project

Atacando servicios web en el mundo real

OWASP Latam Tour 2017

Luis Quispe Gonzales

Abril 2017

Presentación



Luis Quispe Gonzales

CISA, CPTE, BNS, Sec+, COBIT 5

luis.quispegonzales@gmail.com

Ingeniero Informático con más de seis años de experiencia profesional en temas de ciberseguridad, especialmente en servicios relacionados a: hacking de aplicaciones (web, móvil), ethical hacking externo e interno (redes e infraestructura), gestión de vulnerabilidades, revisión de la seguridad de código fuente, revisión seguridad de plataformas (Windows, Linux, AIX, MSSQL, Oracle, Cisco, entre otros), revisiones forenses y consultorías de ciberseguridad.

Agenda

- ¿Qué son los servicios web?
- Arquitectura de los servicios web
- Ataques a servicios web
- Más por explorar

¿Qué son los servicios web?

¿Qué son los servicios web?

Descripción general

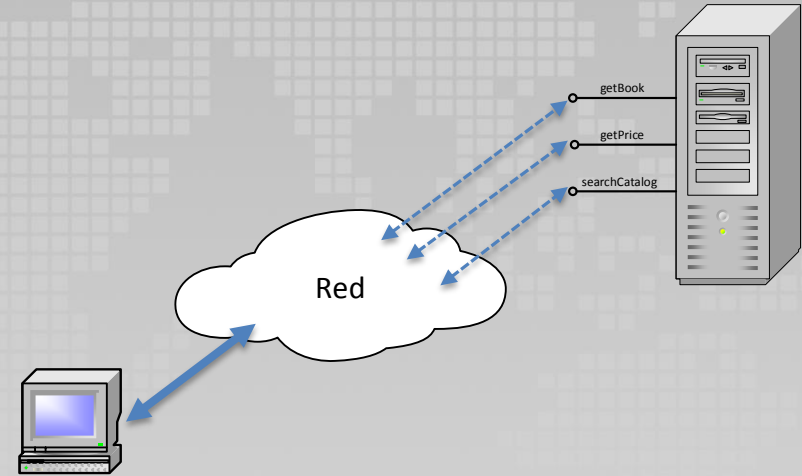
Funciones o métodos que están publicados en un servidor web...



¿Qué son los servicios web?

Descripción general

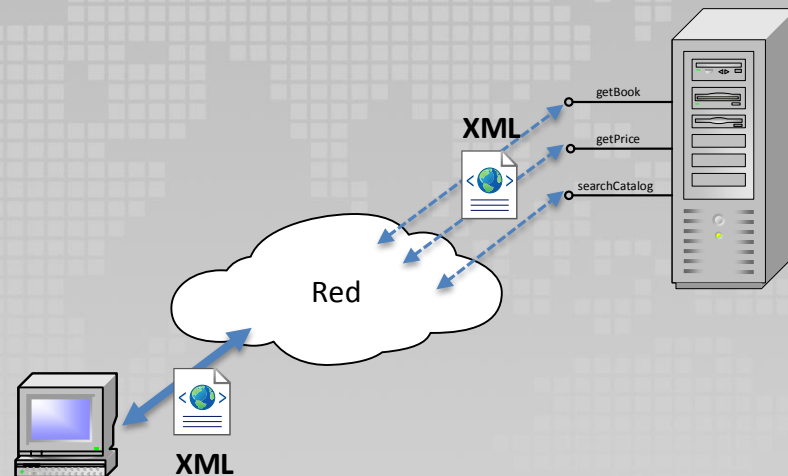
Funciones o métodos que están publicados en un servidor web y que pueden ser invocados desde Internet o intranet...



¿Qué son los servicios web?

Descripción general

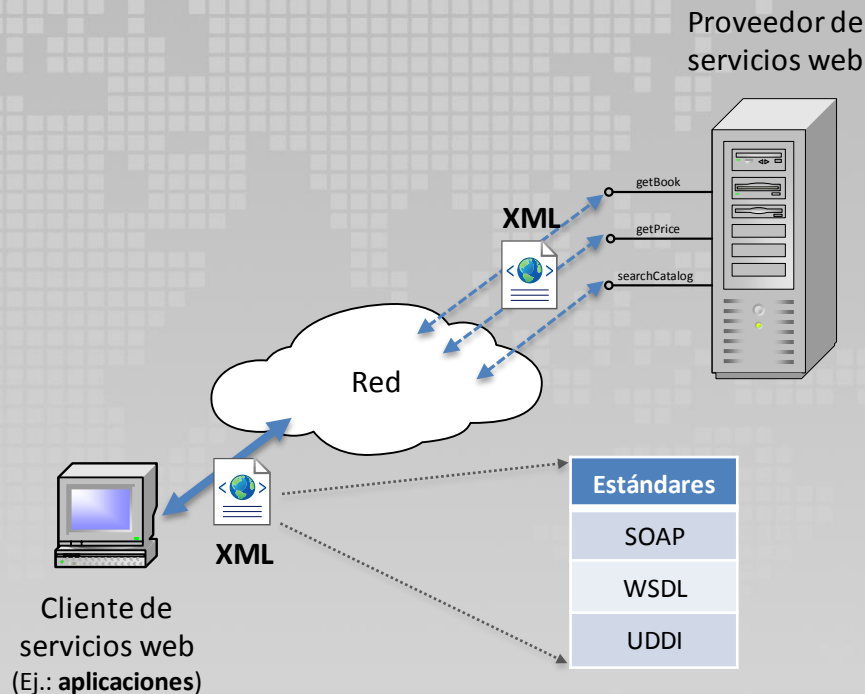
Funciones o métodos que están publicados en un servidor web y que pueden ser invocados desde Internet o intranet usando mensajería XML...



¿Qué son los servicios web?

Descripción general

Funciones o métodos que están publicados en un servidor web y que pueden ser invocados desde Internet o intranet usando mensajería XML basada en estándares como SOAP, WSDL y UDDI.



¿Qué son los servicios web?

Entendiendo XML

```
<?xml version="1.0" encoding="UTF-8"?>
<bookstore>
  <book category="cooking">
    <title lang="en">Everyday Italian</title>
    <author>Giada De Laurentiis</author>
    <year>2005</year>
    <price>30.00</price>
  </book>
  <book category="children">
    <title lang="en">Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    <price>29.99</price>
  </book>
  <book category="web">
    <title lang="en">Learning XML</title>
    <author>Erik T. Ray</author>
    <year>2003</year>
    <price>39.95</price>
  </book>
</bookstore>
```

Imagen extraída de la web https://www.w3schools.com/xml/xml_tree.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo XML

- XML es un (meta)lenguaje que permite la organización y etiquetado de documentos.

```
<?xml version="1.0" encoding="UTF-8"?>
<bookstore>
  <book category="cooking">
    <title lang="en">Everyday Cooking</title>
    <author>Giada De Laurentiis</author>
    <year>2005</year>
    <price>30.00</price>
  </book>
  <book category="children">
    <title lang="en">Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    <price>29.99</price>
  </book>
  <book category="web">
    <title lang="en">Learning XML</title>
    <author>Erik T. Ray</author>
    <year>2003</year>
    <price>39.95</price>
  </book>
</bookstore>
```

Uso de etiquetas para organizar la información en el documento.

Imagen extraída de la web https://www.w3schools.com/xml/xml_tree.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo XML

- XML es un (meta)lenguaje que permite la organización y etiquetado de documentos.
- Permite almacenar datos de manera jerárquica.

```
<?xml version="1.0" encoding="UTF-8"?>
<bookstore>
  <book category="italian">
    <title lang="it">Italian</title>
    <author>Gianfrancesco Guarnieri</author>
    <year>2005</year>
    <price>30.00</price>
  </book>
  <book category="children">
    <title lang="en">Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    <price>29.99</price>
  </book>
  <book category="wiley">
    <title lang="en">Learning XML</title>
    <author>Erik T. Ray</author>
    <year>2003</year>
    <price>39.95</price>
  </book>
</bookstore>
```

Jerarquía de etiquetas

Almacenamiento de datos.

Imagen extraída de la web https://www.w3schools.com/xml/xml_tree.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo XML

- XML es un (meta)lenguaje que permite la organización y etiquetado de documentos.
- Permite almacenar datos de manera jerárquica.
- Cuenta con mecanismos de validación de su estructura (ejemplos: DTD, XML Schema)

```
<?xml version="1.0" encoding="UTF-8"?>
<bookstore>
  <book category="cooking">
    <title lang="en">Everyday Italian</title>
    <author>Giada De Laurentiis</author>
    <year>2005</year>
    <price>30.00</price>
  </book>
  <book category="children">
    <title lang="en">Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    [ ]
  </book>
  <book category="web">
    [ ]
    <author>Erik T. Ray</author>
    <year>2003</year>
    <price>39.95</price>
  </book>
</bookstore>
```

Faltan algunas etiquetas en el documento XML.

Imagen extraída de la web https://www.w3schools.com/xml/xml_tree.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

XML Schema Definition (XSD)

```
<?xml version="1.0"?>

<note
xmlns="https://www.w3schools.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="https://www.w3schools.com note.xsd">
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Imagen extraída de la web https://www.w3schools.com/xml/schema_schema.asp



¿Qué son los servicios web?

XML Schema Definition (XSD)

Archivo **note.xsd**

```
<?xml version="1.0"?>

<note
  xmlns="https://www.w3schools.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://www.w3schools.com note.xsd">
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Imagen extraída de la web https://www.w3schools.com/xml/schema_schema.asp

El documento XML
hace referencia al
archivo **note.xsd**

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="https://www.w3schools.com"
  xmlns="https://www.w3schools.com"
  elementFormDefault="qualified">

  <xs:element name="note">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="to" type="xs:string"/>
        <xs:element name="from" type="xs:string"/>
        <xs:element name="heading" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

Imagen extraída de la web https://www.w3schools.com/xml/schema_howto.asp

¿Qué son los servicios web?

XML Schema Definition (XSD)

```
<?xml version="1.0"?>

<note
xmlns="https://www.w3schools.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="https://www.w3schools.com note.xsd">
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Imagen extraída de la web https://www.w3schools.com/xml/schema_schema.asp

Archivo **note.xsd**

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="https://www.w3schools.com"
xmlns="https://www.w3schools.com"
elementFormDefault="qualified">

  <xs:element name="note">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="to" type="xs:string"/>
        <xs:element name="from" type="xs:string"/>
        <xs:element name="heading" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

Se definen las etiquetas a utilizar en el documento XML, su jerarquía y secuencia.

Imagen extraída de la web https://www.w3schools.com/xml/schema_howto.asp

¿Qué son los servicios web?

XML Schema Definition (XSD)

```
<?xml version="1.0"?>

<note
xmlns="https://www.w3schools.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="https://www.w3schools.com note.xsd">
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Imagen extraída de la web https://www.w3schools.com/xml/schema_schema.asp

Archivo **note.xsd**

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="https://www.w3schools.com"
xmlns="https://www.w3schools.com"
elementFormDefault="qualified">

  <xs:element name="note">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="to" type="xs:string"/>
        <xs:element name="from" type="xs:string"/>
        <xs:element name="heading" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

También se definen
los tipos de datos
de cada elemento.

Imagen extraída de la web https://www.w3schools.com/xml/schema_howto.asp

¿Qué son los servicios web?

Entendiendo SOAP

- Protocolo basado en XML para el intercambio de información entre aplicaciones.
- Cuenta con un esquema XML (XSD) determinado.
- Independiente del lenguaje de programación o plataforma.

```
<!--
  Schema defined in the SOAP Version 1.2 Part 1 specification
  Recommendation:
  http://www.w3.org/TR/2003/REC-soap12-part1-20030624/
  $Id: soap-envelope.xsd,v 1.2 2006/12/20 20:43:36 ylafon Exp $

  Copyright (C)2003 W3C(R) (MIT, ERCIM, Keio), All Rights Reserved.
  W3C viability, trademark, document use and software licensing rules
  apply.
  http://www.w3.org/Consortium/Legal/

  This document is governed by the W3C Software License [1] as
  described in the FAQ [2].

  [1] http://www.w3.org/Consortium/Legal/copyright-software-19980720
  [2] http://www.w3.org/Consortium/Legal/IPR-FAQ-20000620.html#DTD
-->
<?xml:
  <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:tns="http://www.w3.org/2003/05/soap-envelope"
    targetNamespace="http://www.w3.org/2003/05/soap-envelope"
    elementFormDefault="qualified">
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
      schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <!-- Envelope, header and body -->
    <xs:element name="Envelope" type="tns:Envelope"/>
    <xs:complexType name="Envelope">
      <xs:sequence>
        <xs:element ref="tns:Header" minOccurs="0"/>
        <xs:element ref="tns:Body" minOccurs="1"/>
      </xs:sequence>
      <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>
    <xs:element name="Header" type="tns:Header"/>
  </xs:schema>
```

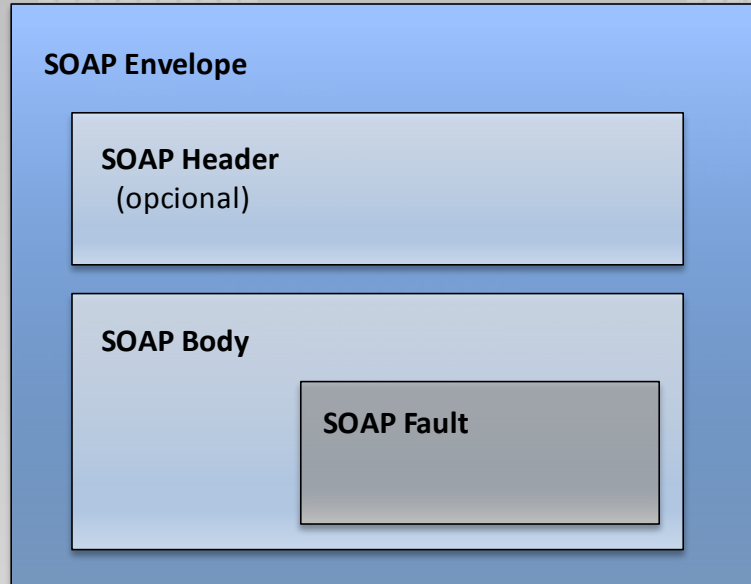
Imagen extraída de la web <https://www.w3.org/2003/05/soap-envelope/>



OWASP
Open Web Application
Security Project

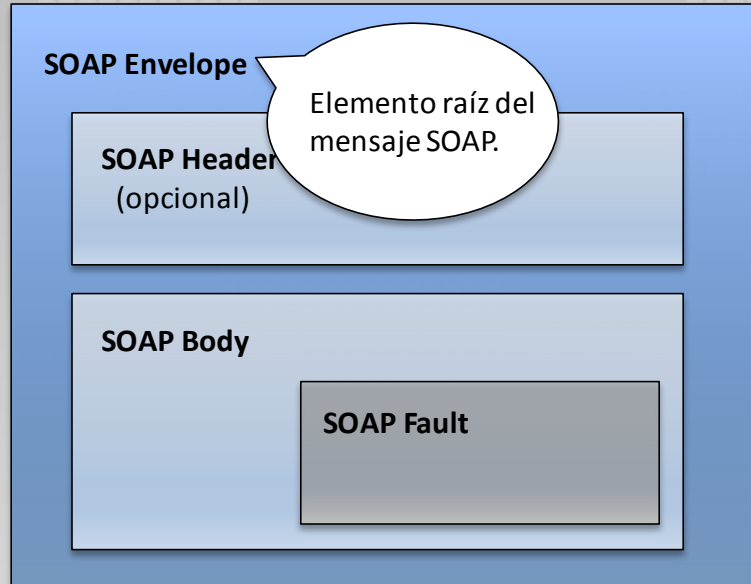
¿Qué son los servicios web?

Estructura del mensaje SOAP



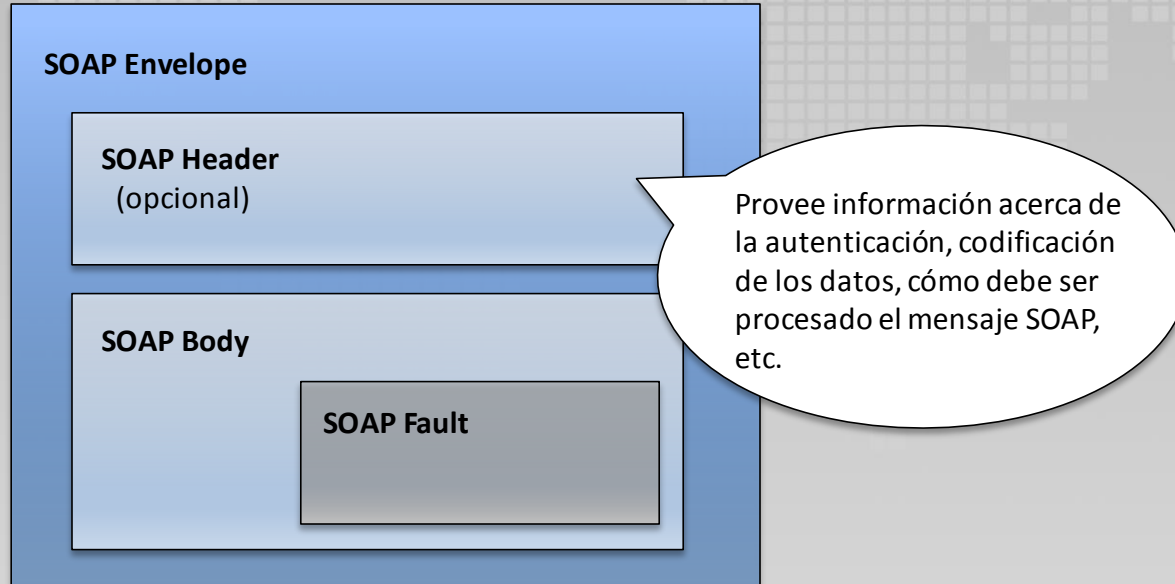
¿Qué son los servicios web?

Estructura del mensaje SOAP



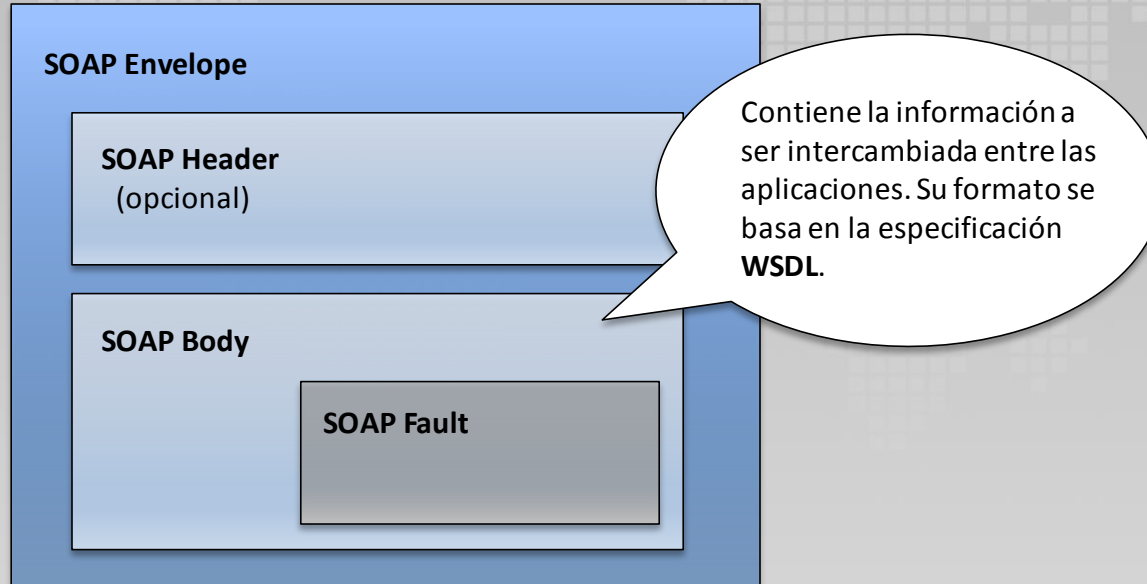
¿Qué son los servicios web?

Estructura del mensaje SOAP



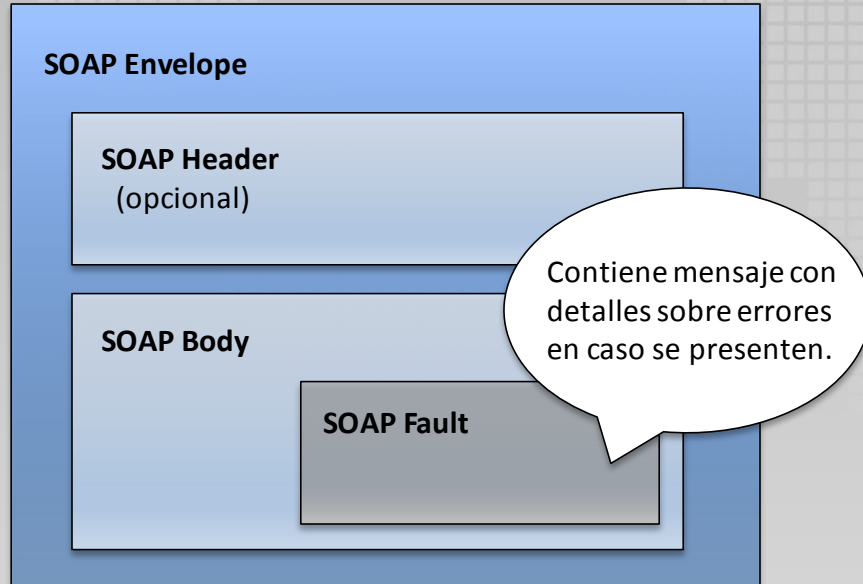
¿Qué son los servicios web?

Estructura del mensaje SOAP



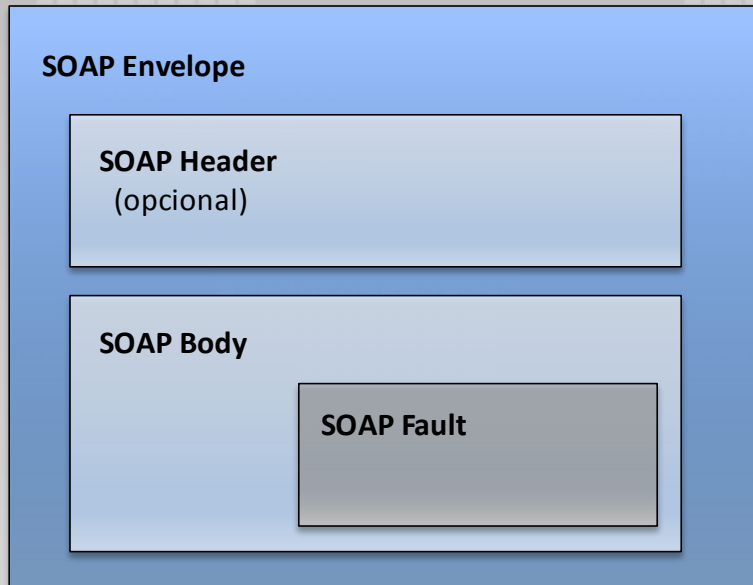
¿Qué son los servicios web?

Estructura del mensaje SOAP



¿Qué son los servicios web?

Estructura del mensaje SOAP



```
<?xml version="1.0"?>

<soap:Envelope
xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
soap:encodingStyle="http://www.w3.org/2003/05/soap-encoding">

  <soap:Header>
  ...
</soap:Header>

  <soap:Body>
  ...
    <soap:Fault>
    ...
    </soap:Fault>
  </soap:Body>

</soap:Envelope>
```

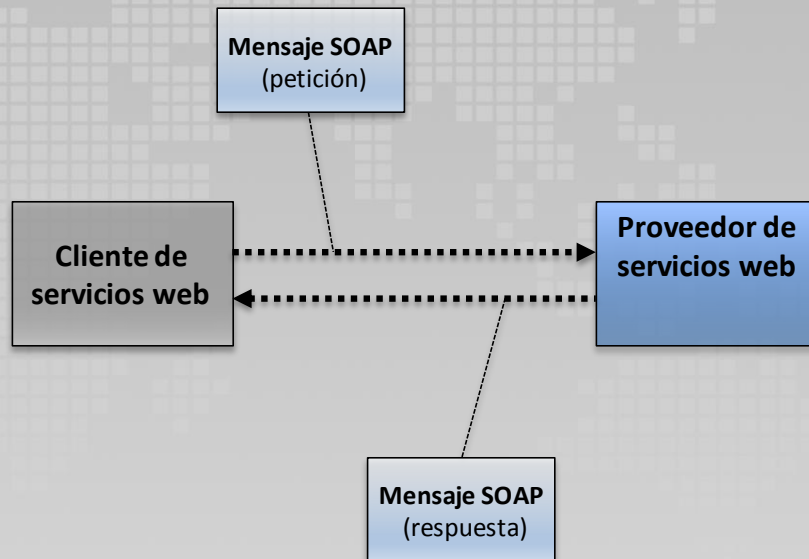
Documento XML correspondiente al mensaje SOAP.

Imagen extraída de la web https://www.w3schools.com/xml/xml_soap.asp

¿Qué son los servicios web?

SOAP HTTP binding

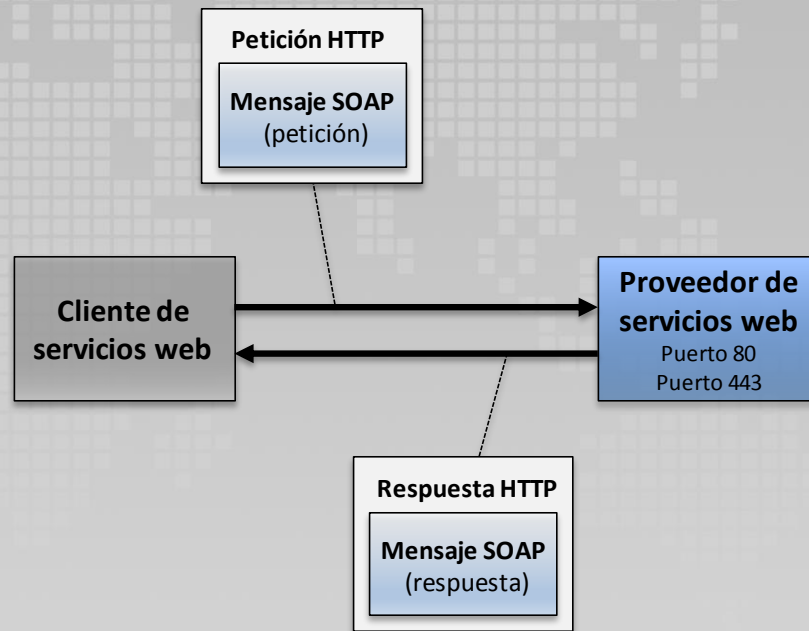
- La especificación SOAP define la estructura de los mensajes SOAP, no cómo son intercambiados.



¿Qué son los servicios web?

SOAP HTTP binding

- La especificación SOAP define la estructura de los mensajes SOAP, no cómo son intercambiados.
- SOAP HTTP binding permite que los mensajes SOAP sean intercambiados usando los protocolos HTTP/HTTPS como medio de “transporte”.



¿Qué son los servicios web?

SOAP HTTP binding

```
POST /InStock HTTP/1.1
Host: www.example.org
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>

<soap:Envelope
xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
soap:encodingStyle="http://www.w3.org/2003/05/soap-encoding">

  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPrice>
      <m:StockName>IBM</m:StockName>
    </m:GetStockPrice>
  </soap:Body>

</soap:Envelope>
```

Cabecera de
petición HTTP.

Ejemplo de petición
HTTP con mensaje SOAP

Cuerpo de petición HTTP
representado mediante
un mensaje SOAP.

Imagen extraída de la web https://www.w3schools.com/xml/xml_soap.asp

¿Qué son los servicios web?

SOAP HTTP binding

Ejemplo de respuesta
HTTP con mensaje SOAP

Cabecera de
respuesta HTTP.

Cuerpo de respuesta
HTTP representado
mediante un mensaje
SOAP.

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>

<soap:Envelope
  xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
  soap:encodingStyle="http://www.w3.org/2003/05/soap-encoding">

  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPriceResponse>
      <m:Price>34.5</m:Price>
    </m:GetStockPriceResponse>
  </soap:Body>

</soap:Envelope>
```

Imagen extraída de la web https://www.w3schools.com/xml/xml_soap.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

- Documento XML que describe un servicio web.
- Especifica la ubicación del servicio web y cómo acceder a los métodos de dicho servicio.
- Cuenta con 5 componentes: “types”, “message”, “portType”, “binding” y “service”.

```
<definitions>

<types>
  data type definitions.....
</types>

<message>
  definition of the data being communicated....
</message>

<portType>
  set of operations.....
</portType>

<binding>
  protocol and data format specification....
</binding>
```

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

- Documento XML que describe un servicio web.
- Especifica la ubicación del servicio web y cómo acceder a los métodos de dicho servicio.
- Cuenta con 5 componentes: “types”, “message”, “portType”, “binding” y “service”.

```
<definitions>

<types>
  data type definitions.....
</types>

<message>
  definition of the message communicated....
</message>

<portType>
  set of operations
</portType>

<binding>
  protocol and data format specification....
</binding>
```

Define los tipos de datos usados por el servicio web. Normalmente se utiliza el XML Schema.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp

¿Qué son los servicios web?

Entendiendo WSDL

```
<message name="getTermRequest">  
  <part name="term" type="xs:string"/>  
</message>
```

```
<message name="getTermResponse">  
  <part name="value" type="xs:string"/>  
</message>
```

```
<portType name="glossaryTerms">  
  <operation name="getTerm">  
    <input message="getTermRequest"/>  
    <output message="getTermResponse"/>  
  </operation>  
</portType>
```

Define la funcionalidad del servicio web: las operaciones disponibles y los mensajes involucrados.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<message name="getTermRequest">
  <part name="term" type="xs:string"/>
</message>

<message name="getTermResponse">
  <part name="value" type="xs:string"/>
</message>

<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>
```

Puede existir más de una operación (método) y en cada una se especifican los mensajes relacionados al input/output.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<message name="getTermRequest">  
  <part name="term" type="xs:string"/>  
</message>
```

```
<message name="getTermResponse">  
  <part name="value" type="xs:string"/>  
</message>
```

```
<portType name="glossaryTerms">  
  <operation name="getTerm">  
    <input message="getTermRequest"/>  
    <output message="getTermResponse"/>  
  </operation>  
</portType>
```

El nombre de la variable input, así como su tipo de dato se especifican en un componente "message".

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<message name="getTermRequest">  
  <part name="term" type="xs:string"/>  
</message>
```

```
<message name="getTermResponse">  
  <part name="value" type="xs:string"/>  
</message>
```

```
<portType name="glossaryTerms">  
  <operation name="getTerm">  
    <input message="getTermRequest"/>  
    <output message="getTermResponse"/>  
  </operation>  
</portType>
```

Análogamente, el nombre de la variable output, así como su tipo de dato se especifican en otro componente "message".

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



¿Qué son los servicios web?

Entendiendo WSDL

```
<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>

<binding type="glossaryTerms" name="b1">
  <soap:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http" />
  <operation>
    <soap:operation soapAction="http://example.com/getTerm"/>
    <input><soap:body use="literal"/></input>
    <output><soap:body use="literal"/></output>
  </operation>
</binding>
```

Define principalmente el protocolo de transporte a utilizar y dónde se ubican las operaciones del servicio web.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>

<binding type="glossaryTerms" name="b1">
  <soap:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http" />
  <operation>
    <soap:operation soapAction="http://example.com/getTerm"/>
    <input><soap:body use="literal"/></input>
    <output><soap:body use="literal"/></output>
  </operation>
</binding>
```

Referencia al "portType" definido anteriormente.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



¿Qué son los servicios web?

Entendiendo WSDL

```
<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>

<binding type="glossaryTerms" name="b1">
  <soap:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http" />
  <operation>
    <soap:operation soapAction="http://example.com/getTerm"/>
    <input><soap:body use="literal"/></input>
    <output><soap:body use="literal"/></output>
  </operation>
</binding>
```

Define cada operación
expuesta por el "portType".

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>

<binding type="glossaryTerms" name="b1">
  <soap:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http" />
  <operation>
    <soap:operation soapAction="http://example.com/getTerm"
    <input><soap:body use="literal"/></input>
    <output><soap:body use="literal"/></output>
  </operation>
</binding>
```

URI que identifica a una operación del servicio web en un "binding" determinado.

Imagen extraída de la web https://www.w3schools.com/xml/xml_wsdl.asp



OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo WSDL

```
<wsdl:service name="Services">
  <wsdl:documentation
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">Core
    by Altoro Mutual bank.</wsdl:documentation>
  ▼ <wsdl:port name="ServicesSoap" binding="tns:ServicesSoap">
    <soap:address location="http://www.testfire.net/bank/ws.asmx"/>
  </wsdl:port>
  ▼ <wsdl:port name="ServicesSoap12" bind
    <soap12:address location="http://www.
  </wsdl:port>
</wsdl:service>
```

Referencia a un "binding" definido previamente.

Ubicación del servicio web.

Imagen extraída de la web <http://www.testfire.net/bank/ws.asmx?WSDL>

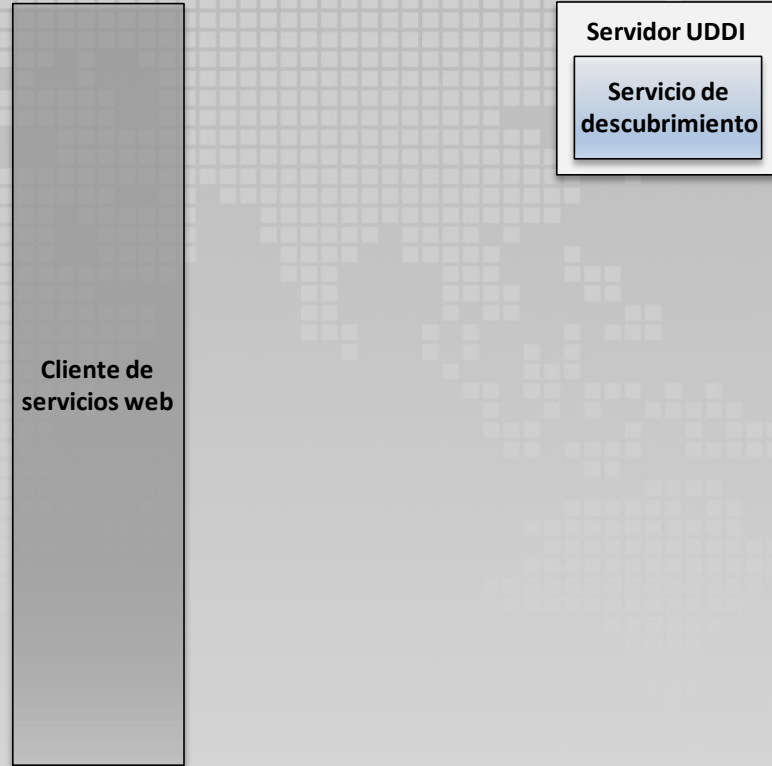


OWASP
Open Web Application
Security Project

¿Qué son los servicios web?

Entendiendo UDDI

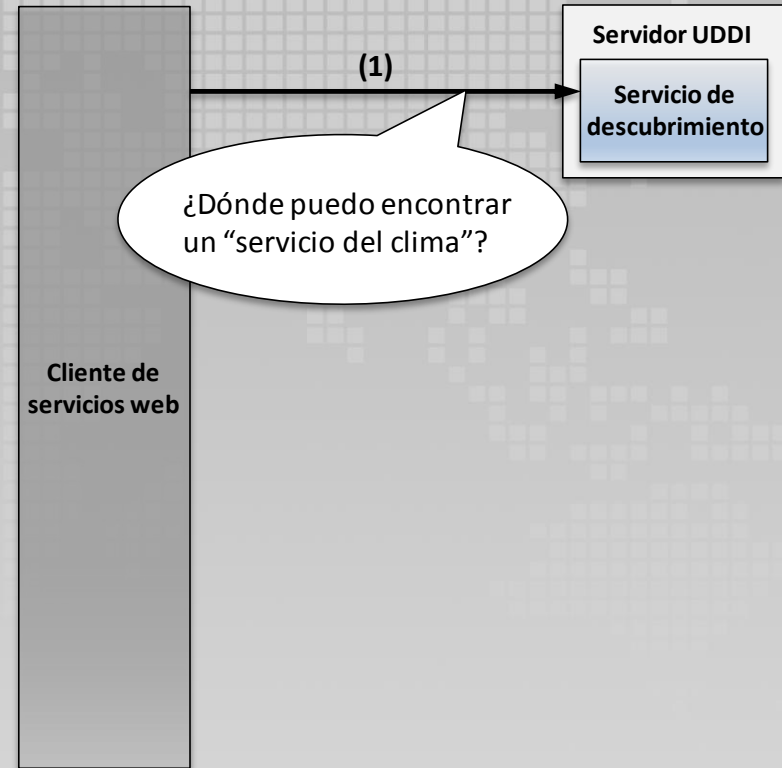
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

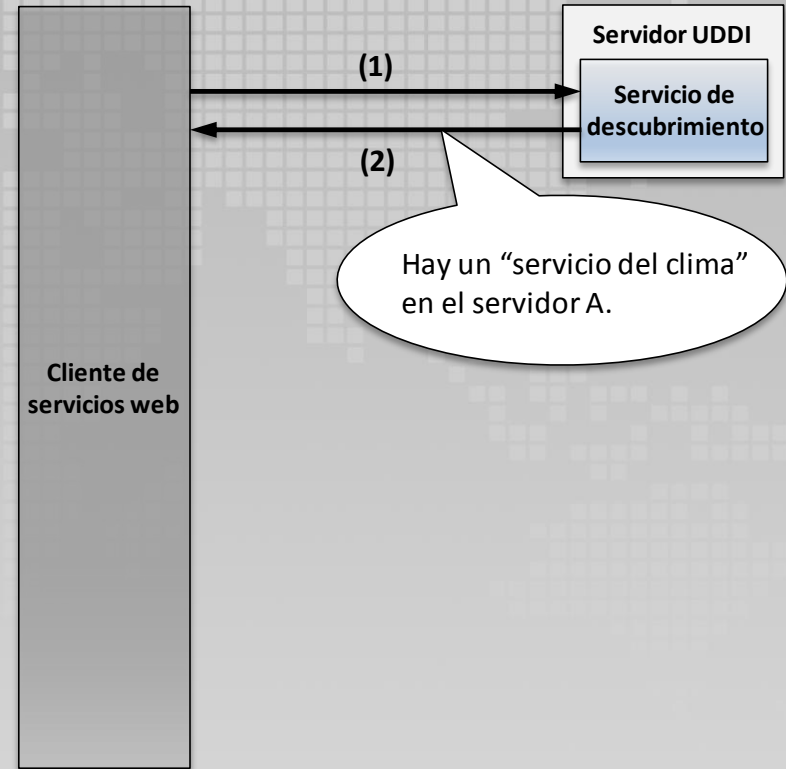
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

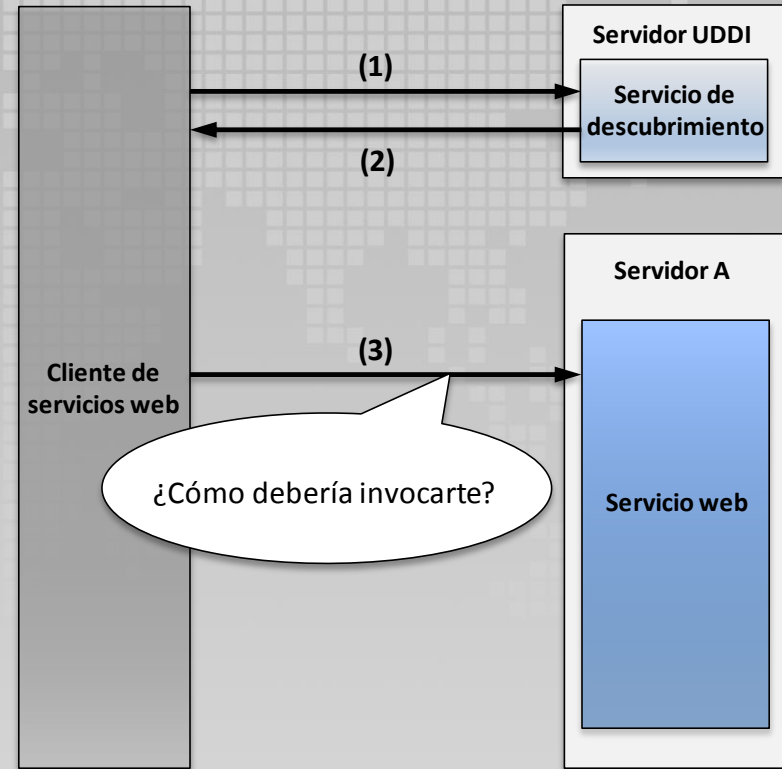
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

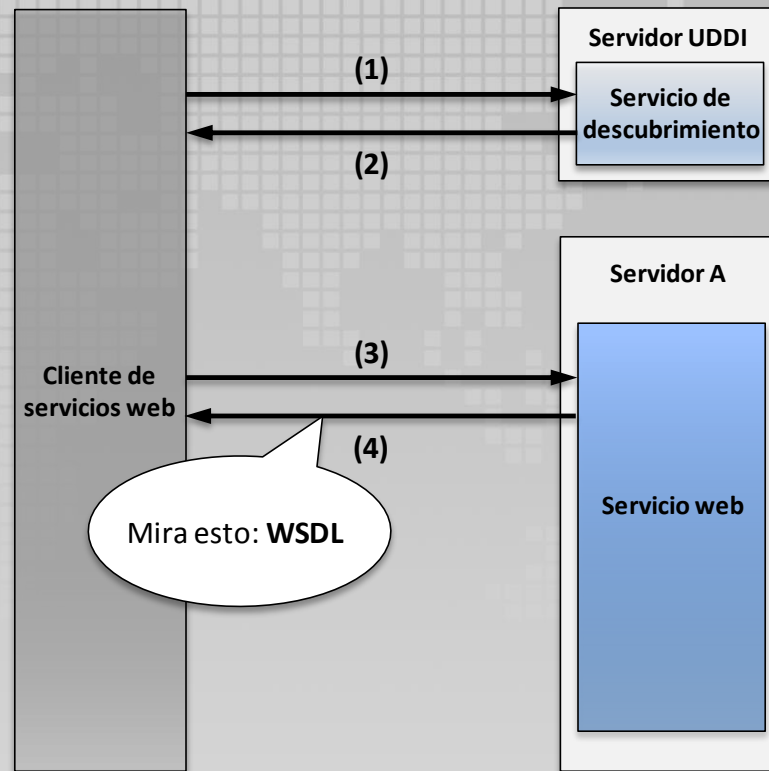
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

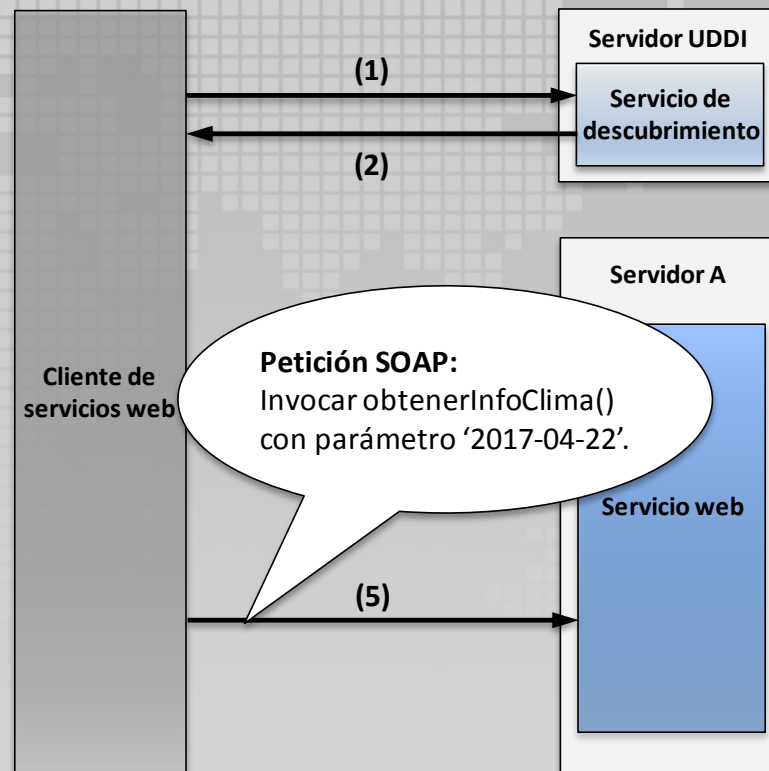
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

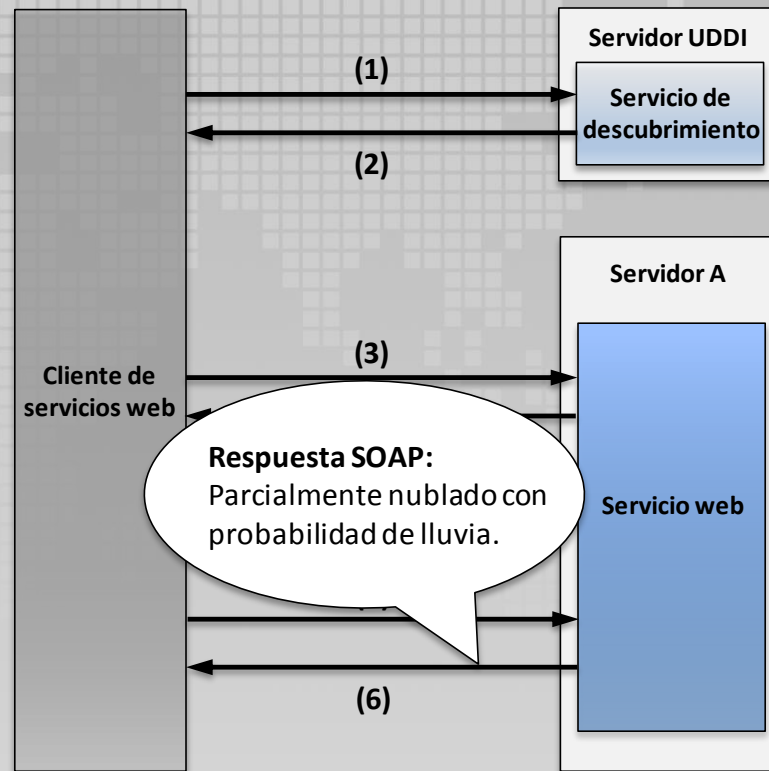
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

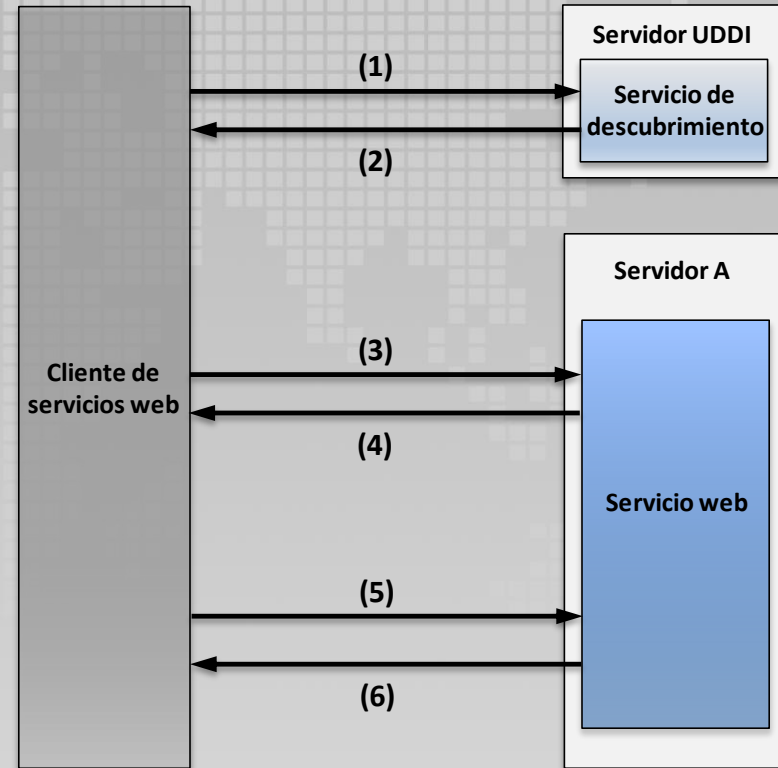
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.



¿Qué son los servicios web?

Entendiendo UDDI

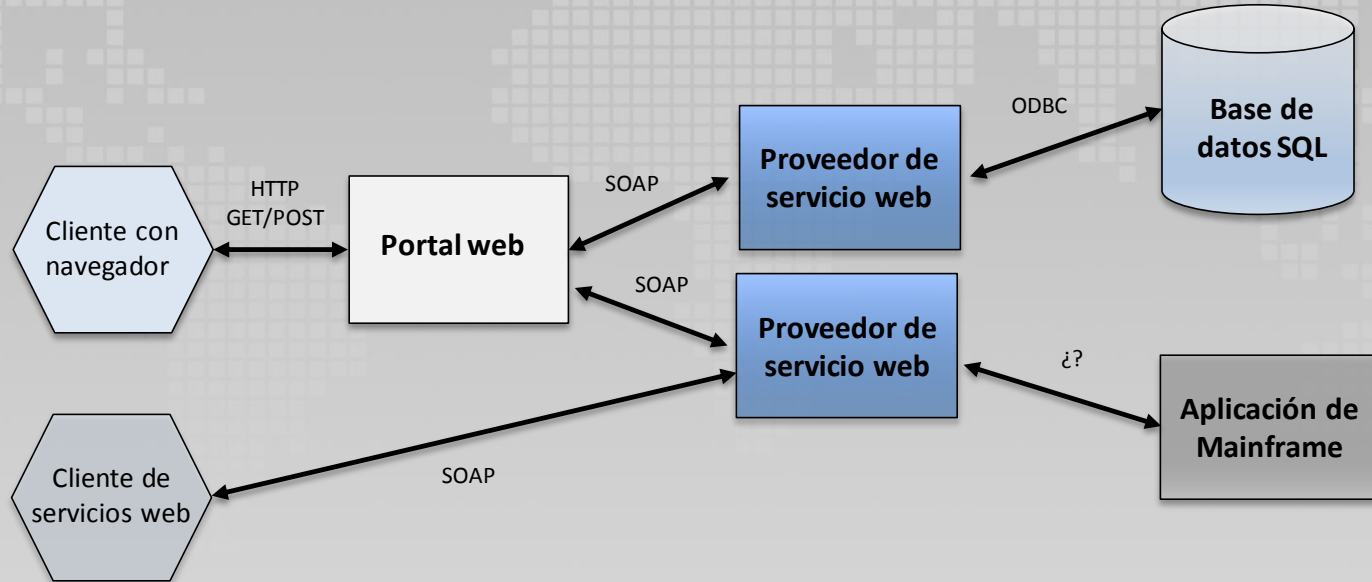
- Provee un catálogo de servicios web que están disponibles para las aplicaciones.
- Usado normalmente en organizaciones con gran cantidad de proveedores de servicios web.
- Componente opcional de los servicios web.



Arquitectura de los servicios web

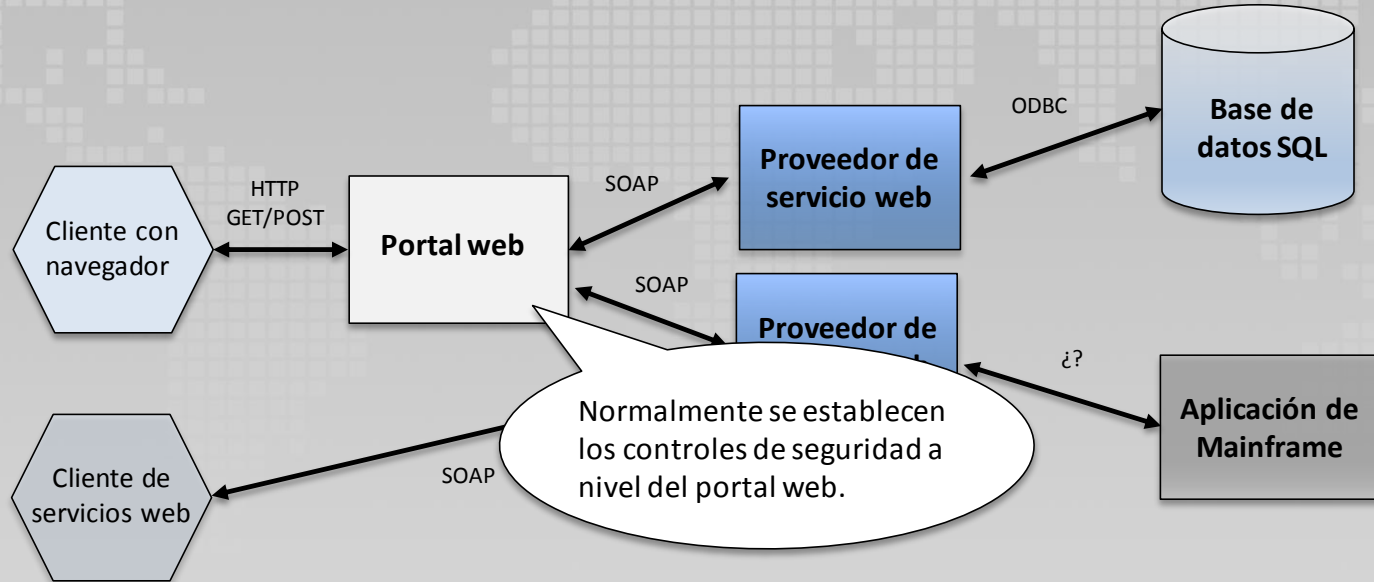
Arquitectura de los servicios web

Descripción general



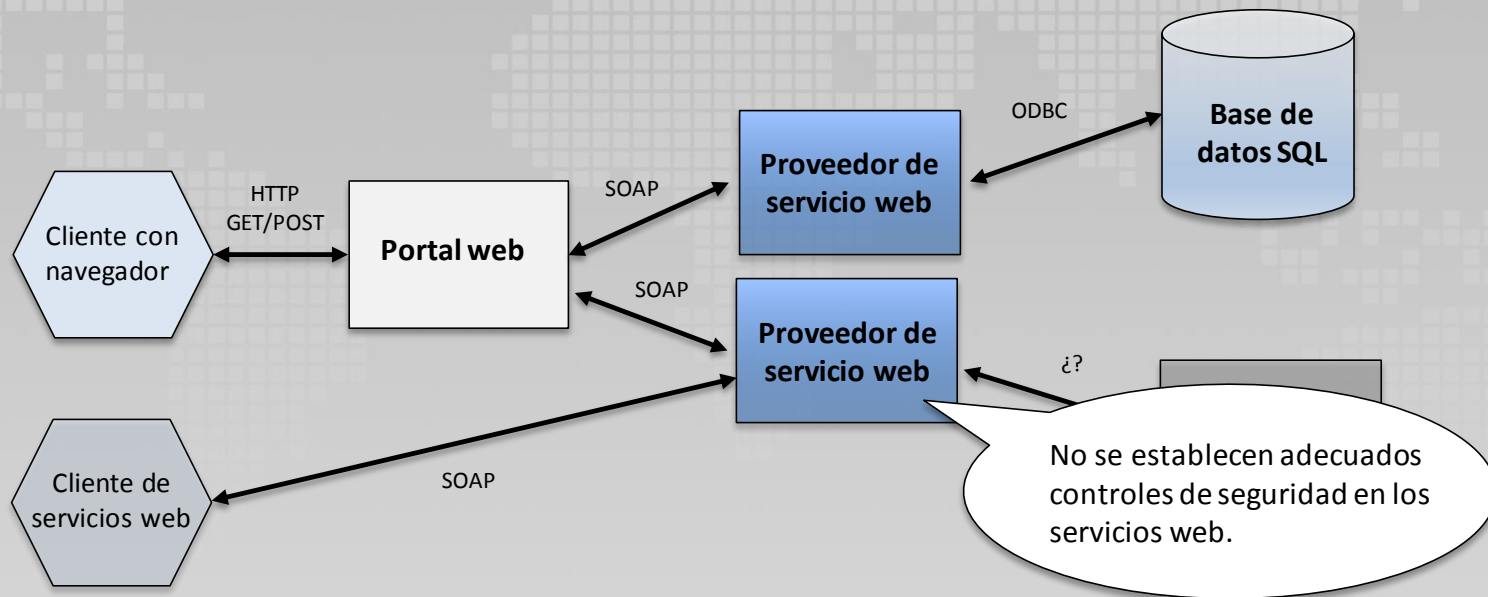
Arquitectura de los servicios web

Descripción general



Arquitectura de los servicios web

Descripción general



Ataques a servicios web

Ataques a servicios web

Ataque #1: Divulgación de WSDL

- Hoy en día, los servicios web son utilizados en escenarios B2B o backend. Deberían ser conocidos solo por un grupo de personas/empleados.
- Algunos de los servicios web “ocultos” realizan operaciones muy críticas: pagos, procesamientos de órdenes entre negocios, entre otros.
- Estos ataques apuntan a descubrir servicios web no públicos recuperando el archivo WSDL.

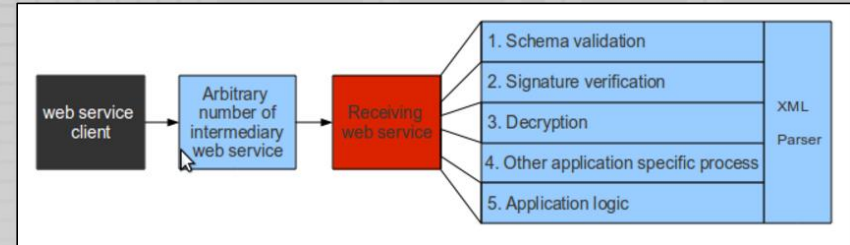


Imagen extraída de la web http://www.ws-attacks.org/WSDL_Disclosure

Ataques a servicios web

Ataque #1: Divulgación de WSDL - Subtipos

WSDL “Google” Hacking:

- Búsqueda de archivos WSDL expuestos a Internet mediante algún motor de búsqueda (Google, Bing, Shodan, etc.).

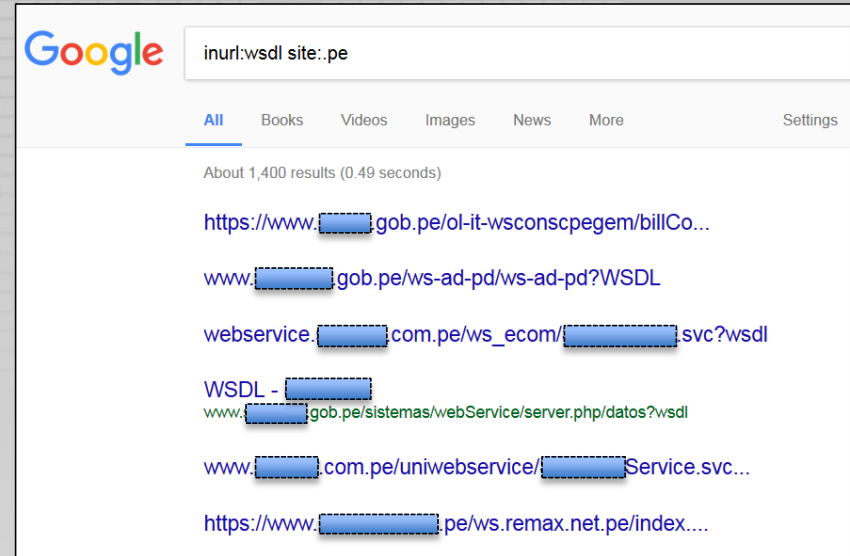


Ataques a servicios web

Ataque #1: Divulgación de WSDL - Subtipos

WSDL “Google” Hacking:

- Búsqueda de archivos WSDL expuestos a Internet mediante motores de búsqueda (Google, Bing, Shodan, etc.).
- Ejemplo: archivos WSDL en páginas con dominios de Perú en Google:
inurl:wSDL site:.pe



Ataques a servicios web

Ataque #1: Divulgación de WSDL - Subtipos

WSDL “Google” Hacking:

- Búsqueda de archivos WSDL expuestos a Internet mediante motores de búsqueda (Google, Bing, Shodan, etc.)
- Ejemplo: archivos WSDL en páginas con dominios de Perú en Google:
inurl:wSDL site:.pe
- Ejemplo anterior utilizando Shodan:
country:PE wSDL

The screenshot shows the Shodan search interface. The search bar contains 'country:PE wSDL'. The results page shows 909 total results. A map of Peru is displayed under 'TOP CITIES'. A list of cities and their result counts is shown:

City	Count
Lima	425
Cusco	13
Arequipa	13
Trujillo	10
Villa	7

Two sample WSDL snippets are shown, both from Peru. The first snippet is from a file named 'wSDL' and the second is from a file named 'wSDL1'. Both snippets show XML headers and namespaces.

Ataques a servicios web

Ataque #1: Divulgación de WSDL - Subtipos

Enumeración WSDL:

- Se asume que el atacante ya ha ganado acceso al archivo WSDL del proveedor de servicio web.
- A partir de esta información, el atacante puede descubrir métodos que se encontraban “ocultos” para las aplicaciones.

[Home](#)
[About](#)
[Setup instructions](#)
[PHP Information](#)
[Vulnerabilities](#)
[WSDL Enumeration](#)
[XML Bomb Denial-of-Service](#)
[XML External Entity Processing](#)
[XPath Injection](#)
[Command Injection](#)
[Cross Site Tracing \(XST\)](#)
[Server Side Request Forgery](#)
[REST API SQL Injection](#)

WSDL Enumeration

Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL file is not exposed to the public. However, if an attacker can access an application's WSDL file, he can try to enumerate and look for hidden services used by the web application.

WSDL enumeration aims to discover non-public web services by retrieving their WSDL file.

More Information

- [https://www.owasp.org/index.php/Testing_WSDL_\(OWASP-WS-002\)](https://www.owasp.org/index.php/Testing_WSDL_(OWASP-WS-002))
- http://www.ws-attacks.org/index.php/WSDL_Disclosure

The below form submits a value to be processed by the back-end SOAP service. Try to scan the WSDL file and look for other requests being processed by the SOAP service. To find the WSDL of the application, try spidering, directory bruteforcing and other enumeration methods.

Smartphone OS Market Share

☐ Android
☐ iOS
☐ Windows Phone
☐ Others

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



The screenshot shows a web browser window titled "WSDL Enumeration" with the address bar displaying "192.168.1.105/dvws/vulnerabilities/wsdlenum/". The page has a dark sidebar with navigation links: Home, About, Setup instructions, PHP Information, Vulnerabilities, WSDL Enumeration, XML Bomb Denial-of-Service, XML External Entity Processing, XPATH Injection, Command Injection, and Cross Site Tracing (XST). The main content area is titled "WSDL Enumeration" and contains the following text:

Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL file is not exposed to the public. However, if an attacker can access an application's WSDL file, he can try to enumerate and look for hidden services used by the web application.

WSDL enumeration aims to discover non-public web services.

More Information

- <https://www.owasp.org/index>
- <http://www.ws-attacks.org/>

The below form submits a value to the application, try spidering, directory listing, etc.

Smartphone OS Market Share

☐ Android

☐ iOS

☐ Windows Phone

☐ Others

requests being processed by the SOAP service. To find the WSDL of

A callout bubble points to the "Smartphone OS Market Share" form with the text: "Aplicación web sobre encuesta de cuota de mercado de los teléfonos inteligentes. Por el contexto de la prueba, se sabe que **esta aplicación consume un servicio web.**"

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado

Connecting... x +

192.168.1.105/dvws/vulnerabilities/wsdlenum/ x Search

Home

About

Setup Instructions

PHP Information

Vulnerabilities

WSDL Enumeration

XML Bomb Denial-of-Service

XML External Entity Processing

XPATH Injection

Command Injection

Cross Site Tracing (XST)

WSDL Enumeration

Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL file is not exposed to the public. However, if an attacker can access an application's WSDL file, he can try to enumerate and look for hidden services used by the web application.

WSDL enumeration aims to discover non-public web services by retrieving their WSDL file.

More Information

- <https://www.owasp.org/index.php/TenThingsOWASP>
- <http://www.ws-attacks.org/index.php>

The below form submits a value to the application, try spidering, direct

Smartphone OS Market Share

☒ Android

☐ iOS

☐ Windows Phone

☐ Others

Submit Query

Se selecciona la opción "Android" y se envía la encuesta.

WSDL file and look for other requests being processed by the SOAP service. To find the WSDL of

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado

Response from http://192.168.1.105:80/dvws/vulnerabilities/wsdlenum/

Forward Drop Intercept is on Action

Comment this item

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sat, 22 Apr 2017 01:34:25 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Content-Length: 4666
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>WSDL Enumeration</title>

    <!-- Bootstrap Core CSS -->
    <link href="/dvws/css/bootstrap.min.css" rel="stylesheet">
```

La respuesta del servidor muestra que la aplicación web está programada en PHP. Probablemente, el **servicio web** que consume también esté **programado en PHP**.

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado

WSDL Enumeration

Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL file is not exposed to the public. However, if an attacker can access an application's WSDL file, he can try to enumerate and look for hidden services used by the web application.

WSDL enumeration aims to discover non-public web services by retrieving their WSDL file.

More Information

- [https://www.owasp.org/index.php/Testing_WSDL_\(OWASP-WS-002\)](https://www.owasp.org/index.php/Testing_WSDL_(OWASP-WS-002))
- http://www.ws-attacks.org/index.php/WSDL_Disclosure

The below form submits a value to be processed by the back-end SOAP service. To find the WSDL file and look for other requests being processed by the SOAP service. To find the WSDL of the application, try spidering, directory bruteforcing and other enumeration techniques.

Smartphone OS Market Share

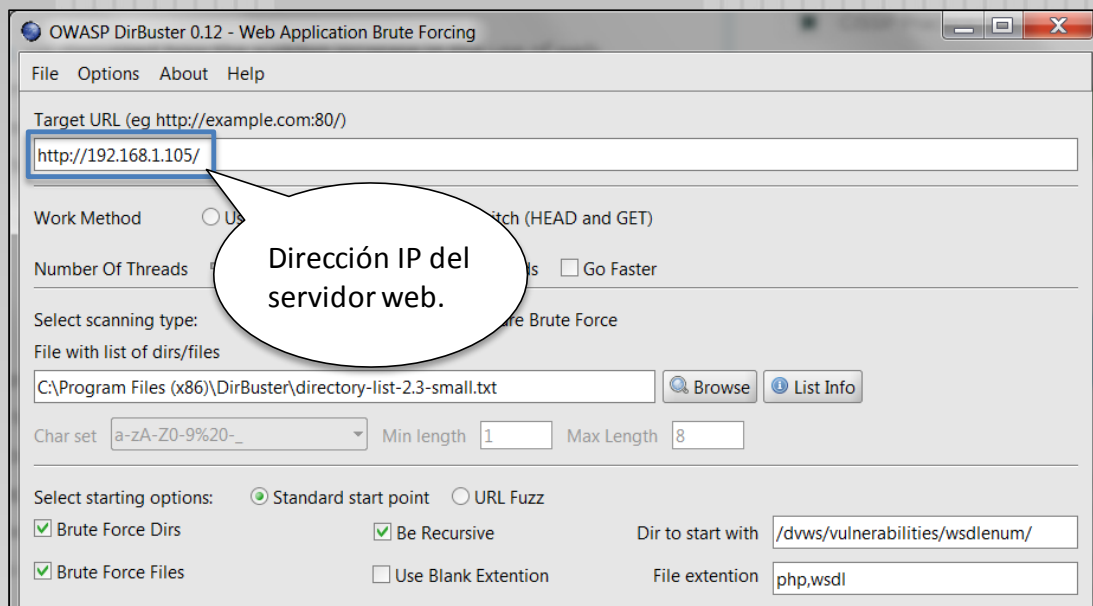
☒ Android
☐ iOS
☐ Windows Phone
☐ Others

The percentage of Android marketshare is 82.8%

El servidor nos responde que la cuota de mercado de los teléfonos Android es 82.8%.

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://192.168.1.105/

Work Method ☐ Use ☐ Switch (HEAD and GET)

Number Of Threads ☐ Go Faster

Select scanning type: ☐ Brute Force

File with list of dirs/files

C:\Program Files (x86)\DirBuster\directory-list-2.3-small.txt

Char set a-zA-Z0-9%20_ Min length 1 Max Length 8

Select starting options: ☒ Standard start point ☐ URL Fuzz

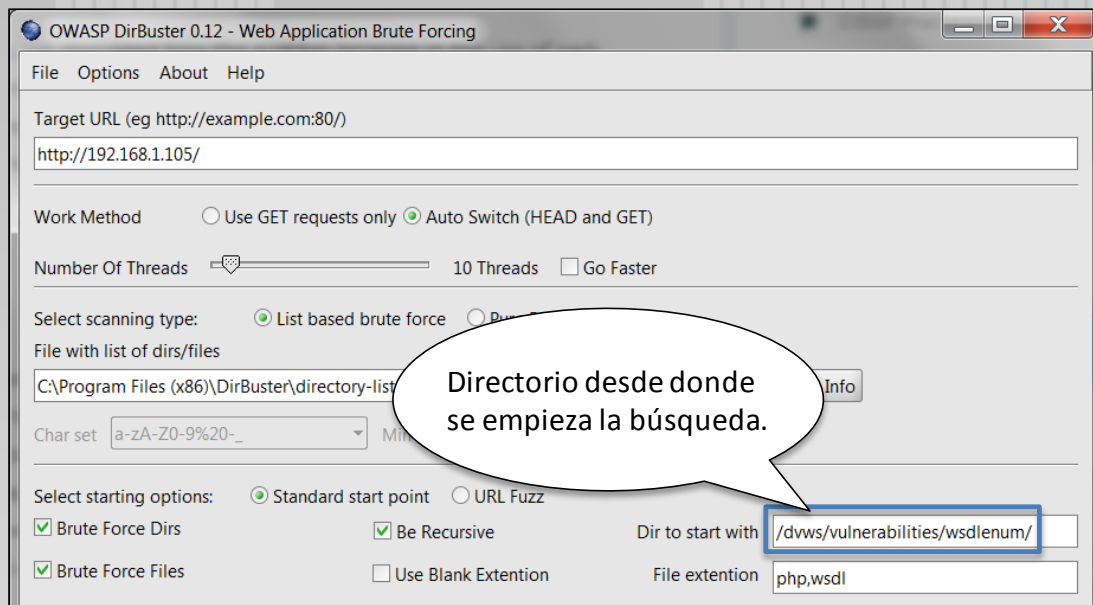
☒ Brute Force Dirs ☒ Be Recursive Dir to start with /dws/vulnerabilities/wsdlenum/

☒ Brute Force Files ☐ Use Blank Extension File extension php,wsdl

Dirección IP del servidor web.

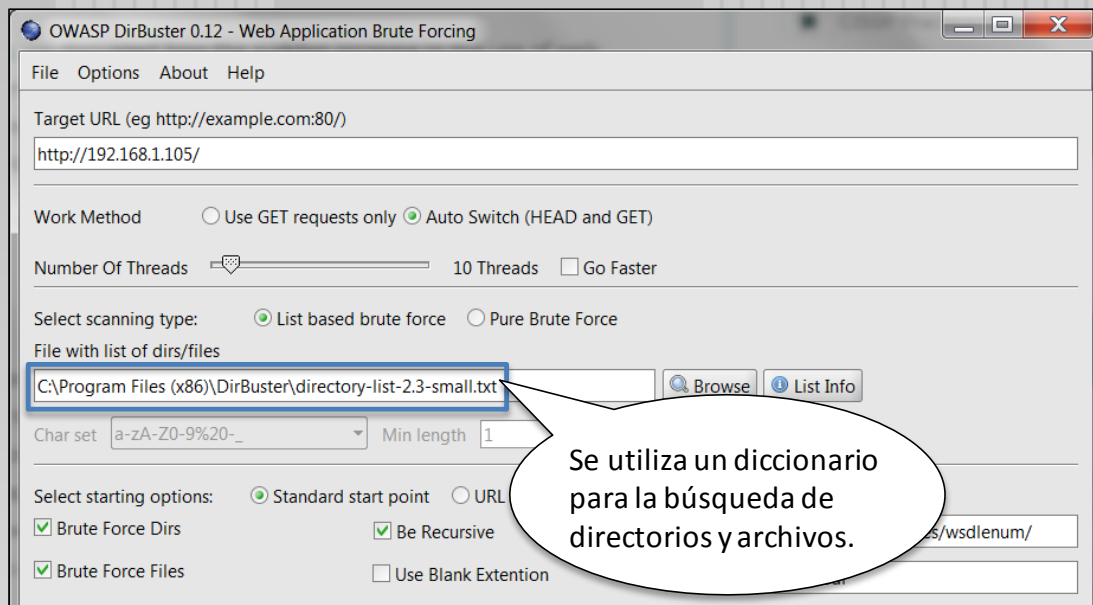
Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



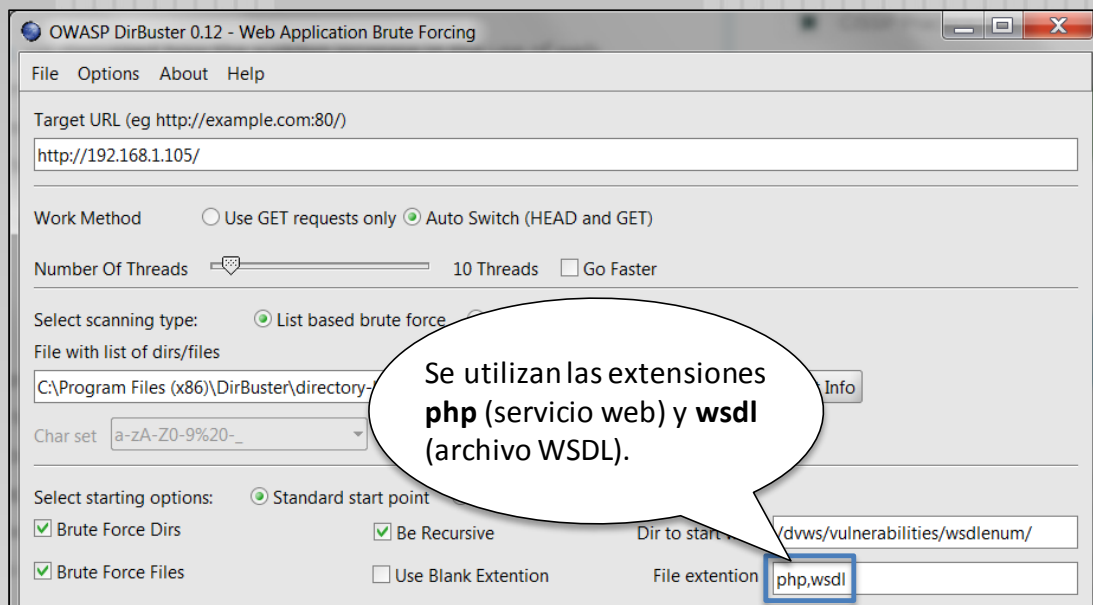
Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



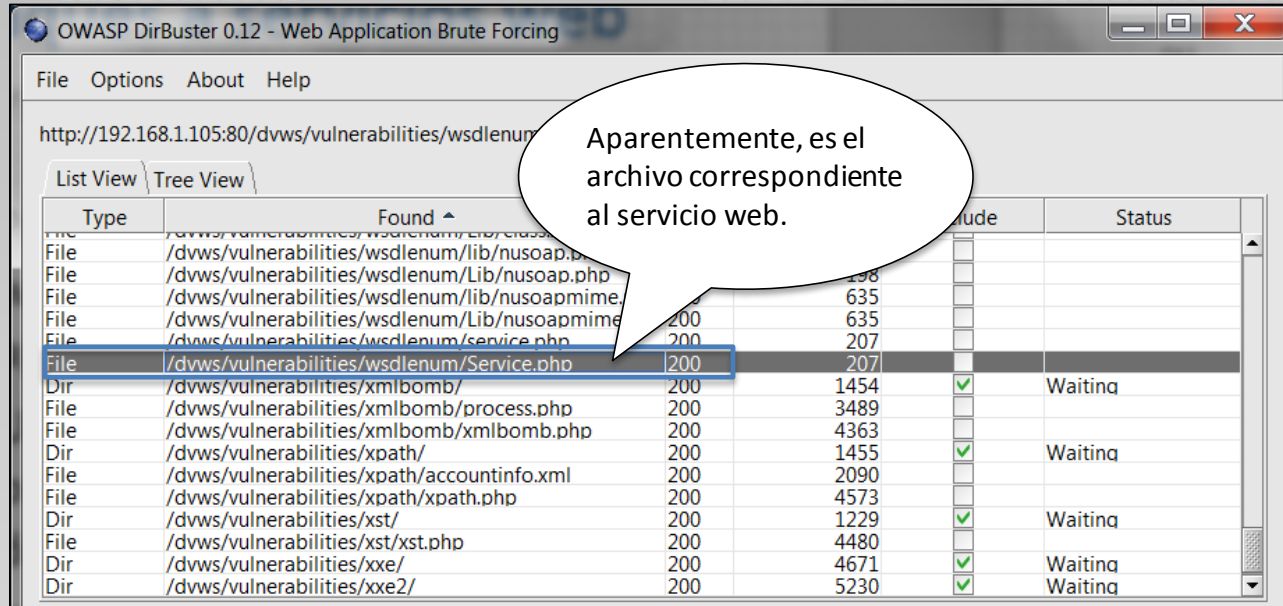
Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://192.168.1.105:80/dvws/vulnerabilities/wsdlenum

List View Tree View

Type	Found	Size	Include	Status
File	/dwvs/vulnerabilities/wsdlenum/lib/nusoap.php	198		
File	/dwvs/vulnerabilities/wsdlenum/Lib/nusoap.php	635		
File	/dwvs/vulnerabilities/wsdlenum/lib/nusoapmime.php	200		
File	/dwvs/vulnerabilities/wsdlenum/Lib/nusoapmime.php	635		
File	/dwvs/vulnerabilities/wsdlenum/service.php	200		
File	/dwvs/vulnerabilities/wsdlenum/Service.php	207		
Dir	/dwvs/vulnerabilities/xmlbomb/	200	✓	Waiting
File	/dwvs/vulnerabilities/xmlbomb/process.php	200		
File	/dwvs/vulnerabilities/xmlbomb/xmlbomb.php	200		
Dir	/dwvs/vulnerabilities/xpath/	200	✓	Waiting
File	/dwvs/vulnerabilities/xpath/accountinfo.xml	200		
File	/dwvs/vulnerabilities/xpath/xpath.php	200		
Dir	/dwvs/vulnerabilities/xst/	200	✓	Waiting
File	/dwvs/vulnerabilities/xst/xst.php	200		
Dir	/dwvs/vulnerabilities/xxe/	200	✓	Waiting
Dir	/dwvs/vulnerabilities/xxe2/	200	✓	Waiting

Aparentemente, es el archivo correspondiente al servicio web.

Ataques a servicios web

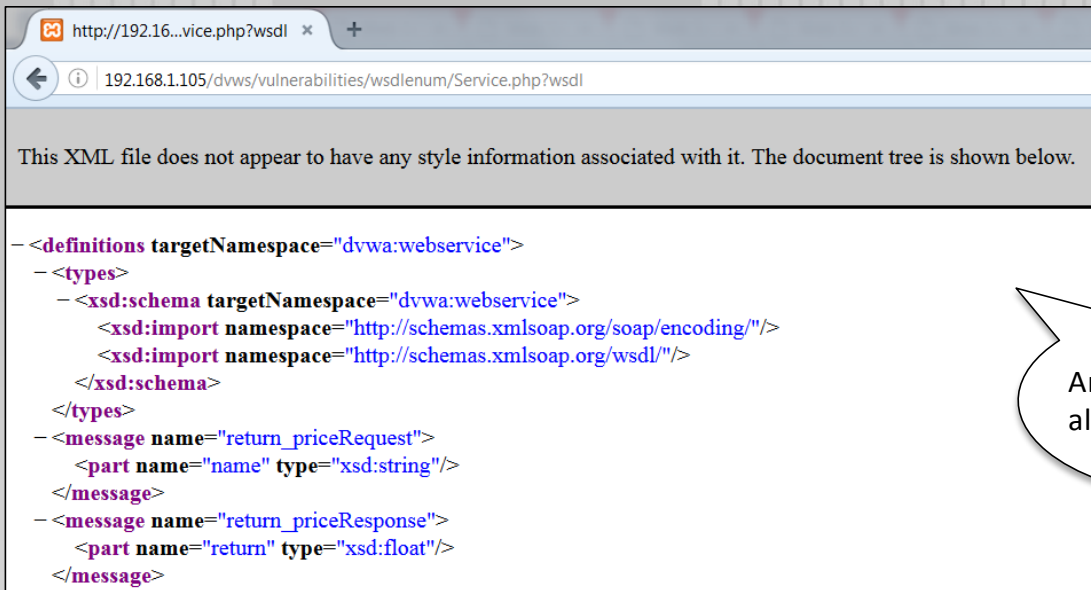
Ataque #1: Prueba en ambiente controlado



Nos muestra un enlace al archivo WSDL.

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



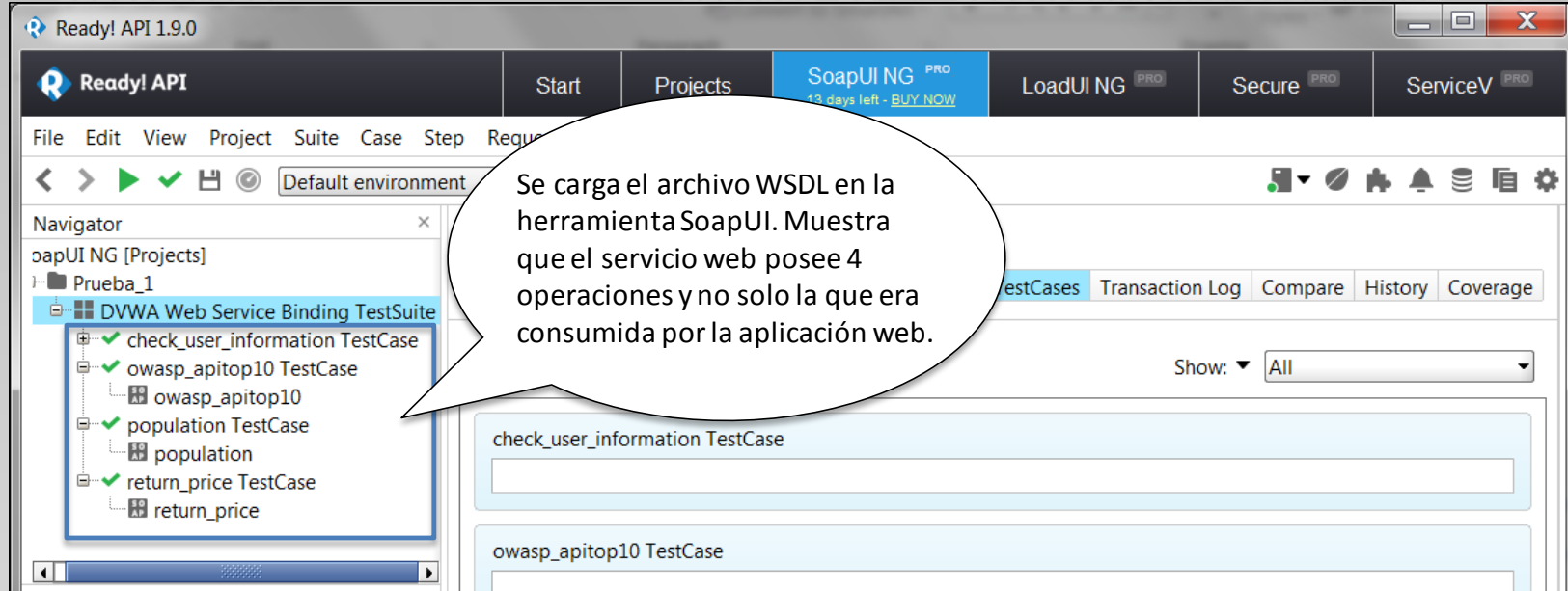
```
- <definitions targetNamespace="dvwa:webservice">
  - <types>
    - <xsd:schema targetNamespace="dvwa:webservice">
      <xsd:import namespace="http://schemas.xmlsoap.org/soap/encoding/" />
      <xsd:import namespace="http://schemas.xmlsoap.org/wsdl/" />
    </xsd:schema>
  </types>
  - <message name="return_priceRequest">
    <part name="name" type="xsd:string" />
  </message>
  - <message name="return_priceResponse">
    <part name="return" type="xsd:float" />
  </message>
```

Archivo WSDL asociado
al servicio web.



Ataques a servicios web

Ataque #1: Prueba en ambiente controlado



Ready! API 1.9.0

Ready! API Start Projects SoapUI NG PRO 43 days left - BUY NOW LoadUI NG PRO Secure PRO ServiceV PRO

File Edit View Project Suite Case Step Request

Default environment

Navigator

- SoapUI NG [Projects]
- Prueba_1
 - DVWA Web Service Binding TestSuite
 - check_user_information TestCase
 - owasp_apitop10 TestCase
 - owasp_apitop10
 - population TestCase
 - population
 - return_price TestCase
 - return_price

Se carga el archivo WSDL en la herramienta SoapUI. Muestra que el servicio web posee 4 operaciones y no solo la que era consumida por la aplicación web.

TestCases Transaction Log Compare History Coverage

Show: All

check_user_information TestCase

owasp_apitop10 TestCase

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado

The screenshot shows the SoapUI NG interface with the following components:

- Navigator:** A tree view on the left showing a project named 'Prueba_1' containing a test case 'return_price' which is currently selected and highlighted in blue.
- Request:** The central area shows the request configuration. The 'name' field is set to 'Android'.
- Response:** The right area shows the response in XML format. The response is a SOAP envelope containing a 'return_priceResponse' element with a 'return' field set to '82.8'.

Three callout boxes provide context for the actions shown:

- Callout 1:** "Probamos la operación 'return_price'." (We test the operation 'return_price').
- Callout 2:** "Enviamos como input el valor 'Android'." (We send the value 'Android' as input).
- Callout 3:** "Recibimos como resultado el valor 82.8." (We receive the value 82.8 as result).

Ataques a servicios web

Ataque #1: Prueba en ambiente controlado

The screenshot shows the SoapUI NG interface with the following components:

- Navigator:** A tree view on the left showing a project named 'owasp_apitop10' and a test case 'population TestCase'.
- Request:** A central area showing the request body with the parameter 'owaspid *' set to the value '5'.
- XML Node:** A right-hand pane showing the response XML structure, including a 'return' element with the value 'Sensitive Data Exposure'.

Three callout boxes provide context for the actions shown:

- Callout 1:** "Probamos la operación 'owasp_apitop10'." (We test the operation 'owasp_apitop10').
- Callout 2:** "Enviamos como input el valor '5'." (We send the value '5' as input).
- Callout 3:** "Recibimos como resultado el valor **Sensitive Data Exposure** (OWASP Top 10)." (We receive the value **Sensitive Data Exposure** (OWASP Top 10) as a result).

Ataques a servicios web

Ataque #1: Contramedidas

- La seguridad de los servicios web nunca deberían recaer en el secretismo del archivo WSDL.
- Deberían establecerse controles de integridad, confidencialidad y de acceso, a fin de asegurar los servicios web.
- Si las medidas planteadas son usadas correctamente, la divulgación del archivo WSDL no debería representar ningún problema.

Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

```
<?xml version="1.0"?>
<!DOCTYPE MaliciousDTD [
<!ENTITY ZERO "A">
<!ENTITY ONE "&ZERO;&ZERO;">
<!ENTITY TWO "&ONE;&ONE;">
...
<!ENTITY THIRTYTWO "&THIRTYONE;&THIRTYONE;">
]>
<data>&THIRTYTWO;</data>
```

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>



Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

La entidad es definida con el valor "A".

```
<?xml version="1.0"?>
<!DOCTYPE Malicious [
  <!ENTITY ZERO "A">
  <!ENTITY ONE "&ZERO;&ZERO;">
  <!ENTITY TWO "&ONE;&ONE;">
  ...
  <!ENTITY THIRTYTWO "&THIRTYONE;&THIRTYONE;">
]>
<data>&THIRTYTWO;</data>
```

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>

Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

```
<?xml version="1.0"?>
<!DOCTYPE MaliciousDTD [
<!ENTITY ZERO "A">
<!ENTITY ONE "&ZERO;&ZERO;">
<!ENTITY TWO "&ONE;&ONE;">
...
<!ENTITY THIRTYTWO "&THIRTYONE;&THIRTYONE;">
]>
<data>&THIRTYTWO;</data>
```

La entidad es definida con el valor "AA".

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>



OWASP
Open Web Application
Security Project

Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

```
<?xml version="1.0"?>
<!DOCTYPE MaliciousDTD [
<!ENTITY ZERO "A">
<!ENTITY ONE "&ZERO;&ZERO;">
<!ENTITY TWO "&ONE;&ONE;">
...
<!ENTITY THIRTYTWO "&THIRTYONE;&THIRTYONE;">
]>
<data>&THIRTYTWO;</data>
```

La entidad es definida con el valor "AAAA".

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>

Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

```
<?xml version="1.0"?>
<!DOCTYPE MaliciousD
<!ENTITY ZERO "A">
<!ENTITY ONE "&ZERO;&Z
<!ENTITY TWO "&ONE;&ON
...
<!ENTITY THIRTYTWO "&THIRTYONE;&THIRTYONE;">
]>
<data>&THIRTYTWO;</data>
```

La entidad es definida con el valor de 2^{32} veces "A".

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>

Ataques a servicios web

Ataque #2: Bomba XML

- Documento XML pequeño diseñado para expandirse a un tamaño gigantesco cuando es procesado por un parser XML desprotegido.
- Hace uso de sucesivas llamadas recursivas (permitidas por el DTD) para crecer de manera exponencial.
- Estos ataques apuntan causar una denegación de servicio en la aplicación web.

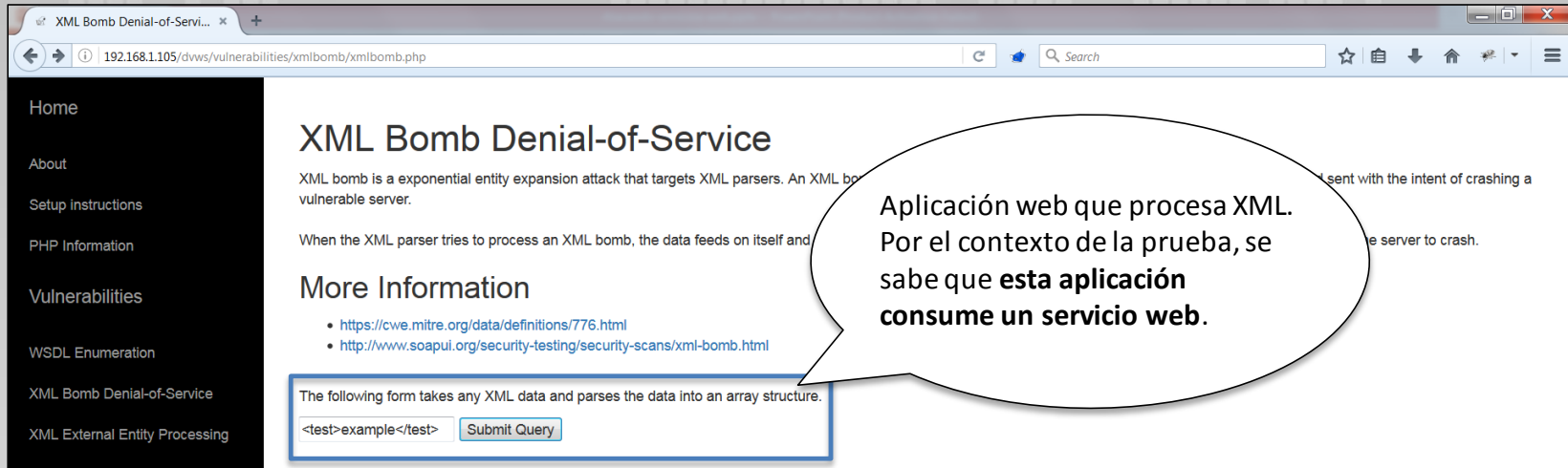
```
<?xml version="1.0" ?>
<!DOCTYPE Malicious [
  <!ENTITY ZERO "A" >
  <!ENTITY ONE "&ZERO;" >
  <!ENTITY TWO "&ONE;" >
  ...
  <!ENTITY THIRTYTWO "&THIRTYONE;" >
] >
<data>&THIRTYTWO;</data>
```

Cuando el parser XML procesa este documento, el valor 2^{32} veces "A" es cargado en la memoria del servidor web.

Imagen extraída de la web <https://cwe.mitre.org/data/definitions/776.html>

Ataques a servicios web

Ataque #2: Prueba en ambiente controlado



The screenshot shows a web browser window with the address bar displaying '192.168.1.105/dvws/vulnerabilities/xmlbomb/xmlbomb.php'. The page has a dark sidebar with navigation links: Home, About, Setup instructions, PHP Information, Vulnerabilities, WSDL Enumeration, XML Bomb Denial-of-Service, and XML External Entity Processing. The main content area is titled 'XML Bomb Denial-of-Service' and contains the following text:

XML bomb is a exponential entity expansion attack that targets XML parsers. An XML bomb is sent with the intent of crashing a vulnerable server.

When the XML parser tries to process an XML bomb, the data feeds on itself and the server to crash.

More Information

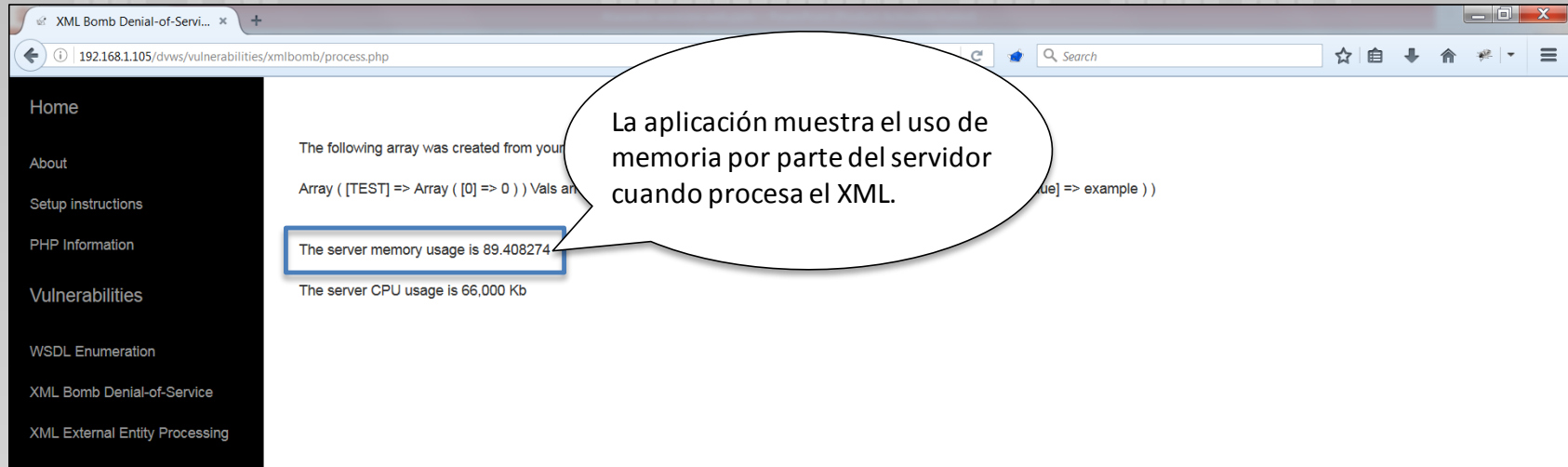
- <https://cwe.mitre.org/data/definitions/776.html>
- <http://www.soapui.org/security-testing/security-scans/xml-bomb.html>

The following form takes any XML data and parses the data into an array structure.

A speech bubble annotation points to the form and contains the text: 'Aplicación web que procesa XML. Por el contexto de la prueba, se sabe que **esta aplicación consume un servicio web.**'

Ataques a servicios web

Ataque #2: Prueba en ambiente controlado



The screenshot shows a web browser window with the address bar displaying `192.168.1.105/dvws/vulnerabilities/xmlbomb/process.php`. The page has a dark sidebar on the left with a menu containing: Home, About, Setup instructions, PHP Information, Vulnerabilities, WSDL Enumeration, XML Bomb Denial-of-Service, and XML External Entity Processing. The main content area displays the following text:

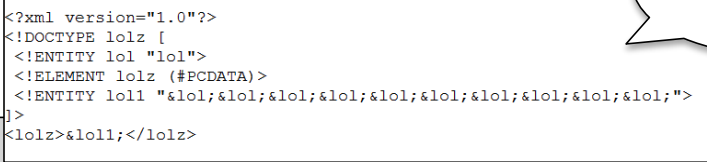
```
The following array was created from your  
Array ( [TEST] => Array ( [0] => 0 ) ) Vals an  
ue] => example ) )
```

Below this, a blue-bordered box highlights the text: `The server memory usage is 89.408274`. A speech bubble points to this box with the text: `La aplicación muestra el uso de memoria por parte del servidor cuando procesa el XML.`

Below the highlighted box, the text `The server CPU usage is 66,000 Kb` is visible.



Ataque #2: Prueba en ambiente controlado



Ataque #2: Prueba en ambiente controlado

The following array was created from your request:

```
Array ( [LOLZ] => Array ( [0] => 0 ) ) Vals are: LOLZ=0
```

The server memory usage is 93.56496 Mb

The server CPU usage is 65,792 Kb

La aplicación muestra el uso de memoria por parte del servidor cuando procesa el XML.

Mensaje enviado.

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
]>
<lolz>&lol2;</lolz>
```

Ataques a servicios web

Ataque #2: Contramedidas

- Si es posible, utilizar un parser XML sin soporte DTD.
- De ser necesario el soporte DTD, se deberían procesar las declaraciones de entidades hasta cierto nivel, y dejar de hacerlo en caso de identificar potencial contenido “explosivo”.



Ataques a servicios web

Ataque #3: Inyección XPath

- XPath es un lenguaje utilizado para consultar ciertas partes del documento XML.
- En algunos casos, los parámetros dentro del cuerpo del mensaje SOAP son usados directamente como input para la consulta XPath.
- Un atacante podría modificar la consulta XPath para obtener incluso todo el documento XML.

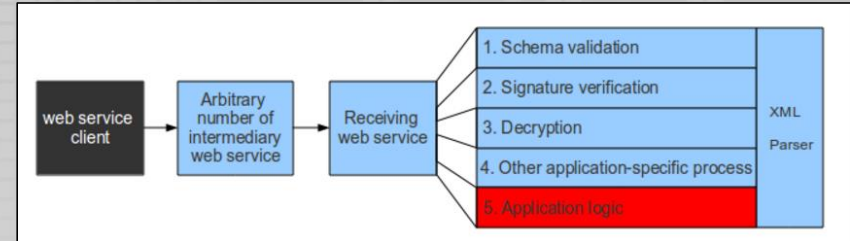
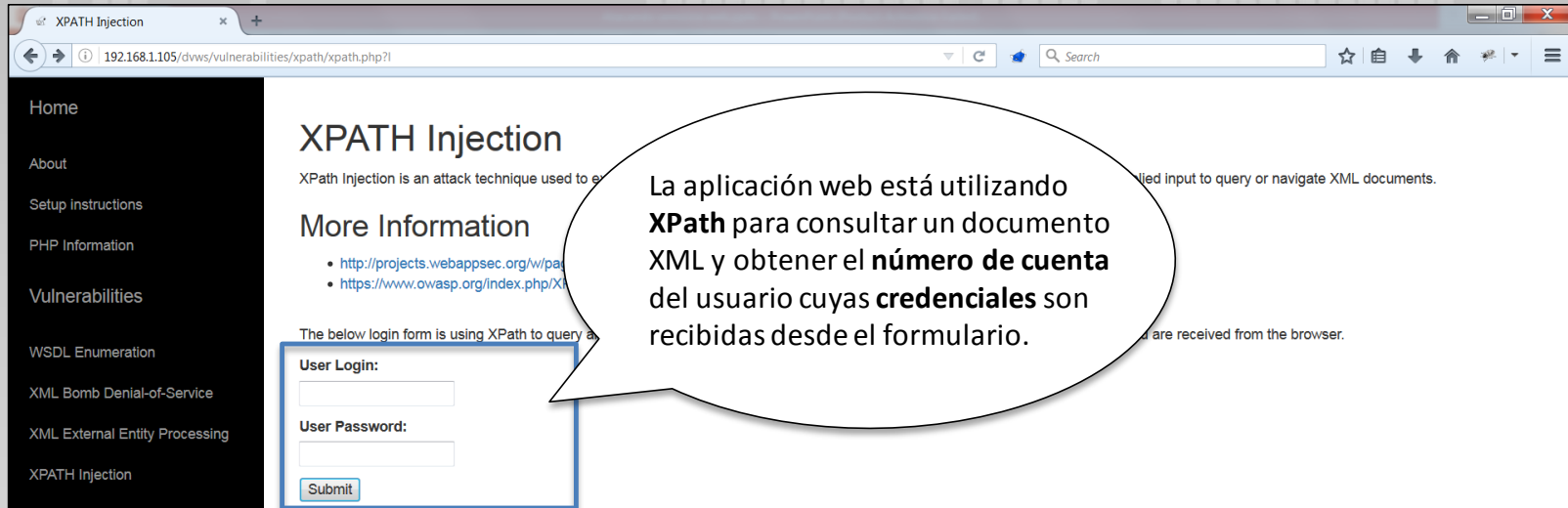


Imagen extraída de la web http://www.ws-attacks.org/Xpath_Injection

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado



The screenshot shows a web browser window with the address bar displaying `192.168.1.105/dvws/vulnerabilities/xpath/xpath.php?l`. The page has a dark sidebar with navigation links: Home, About, Setup instructions, PHP Information, Vulnerabilities, WSDL Enumeration, XML Bomb Denial-of-Service, XML External Entity Processing, and XPATH Injection. The main content area is titled "XPATH Injection" and contains the following text:

XPPath Injection is an attack technique used to exploit the application's ability to process user input to query or navigate XML documents.

More Information

- <http://projects.webappsec.org/w/p/secure-xml>
- https://www.owasp.org/index.php/XPath_Injection

The below login form is using XPath to query a database for user information. The results are received from the browser.

User Login:

User Password:

A callout bubble points to the login form with the text: "La aplicación web está utilizando **XPath** para consultar un documento XML y obtener el **número de cuenta** del usuario cuyas **credenciales** son recibidas desde el formulario."

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado

Home

About

Setup instructions

PHP Information

Vulnerabilities

WSDL Enumeration

XML Bomb Denial-of-Service

XML External Entity Processing

XPATH Injection

Command Injection

XPATH Injection

XPath Injection is an attack technique used to exploit applications that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

More Information

- <http://projects.webappsec.org/w/p/paths>
- https://www.owasp.org/index.php/XPath_Injection

The below login form is using XPath

User Login:

test

User Password:

••••

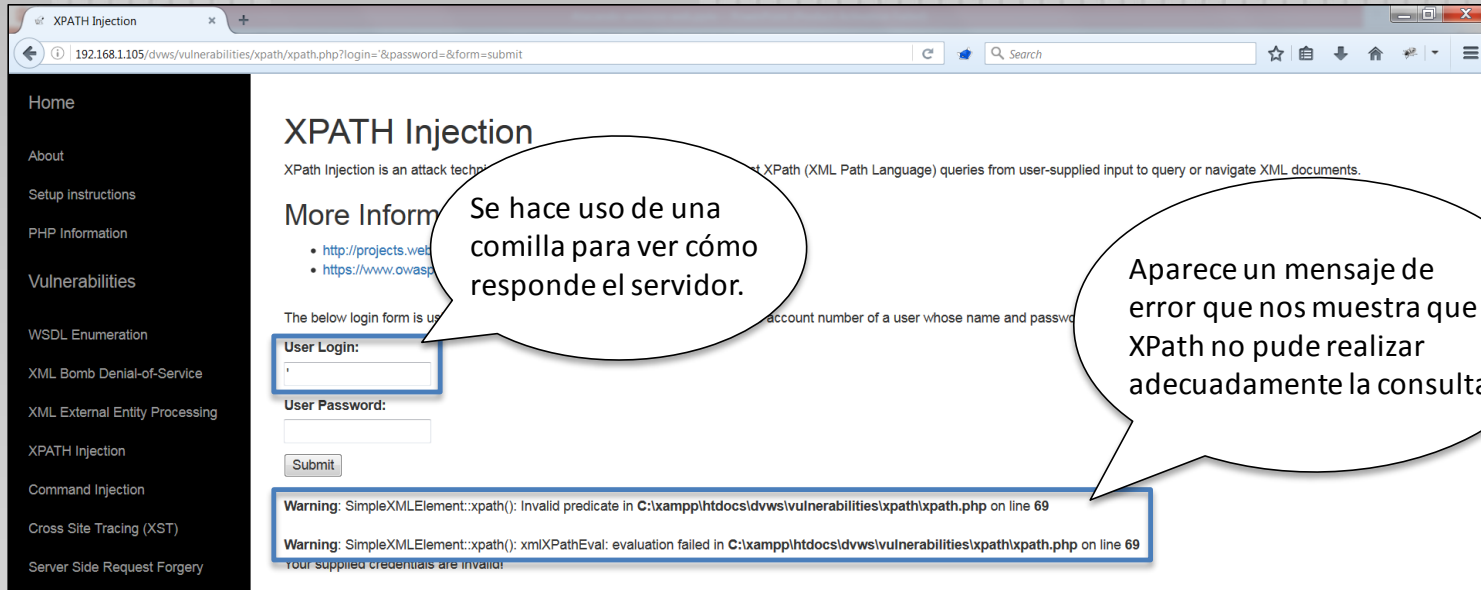
Submit

Your supplied credentials are invalid!

Mensaje de error cuando XPath procesa adecuadamente la información enviada y responde que las credenciales son inválidas.

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado



Home

About

Setup Instructions

PHP Information

Vulnerabilities

WSDL Enumeration

XML Bomb Denial-of-Service

XML External Entity Processing

XPATH Injection

Command Injection

Cross Site Tracing (XST)

Server Side Request Forgery

XPATH Injection

XPath Injection is an attack technique that uses XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

More Information

- <http://projects.web>
- <https://www.owasp>

The below login form is used to log in as an administrator. It requires the account number of a user whose name and password are known.

User Login:

User Password:

Warning: SimpleXMLElement::xpath(): Invalid predicate in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Warning: SimpleXMLElement::xpath(): xpathEval: evaluation failed in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Your supplied credentials are invalid!

Se hace uso de una comilla para ver cómo responde el servidor.

Aparece un mensaje de error que nos muestra que XPath no pudo realizar adecuadamente la consulta.

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado

Home

About

Setup Instructions

PHP Information

Vulnerabilities

WSDL Enumeration

XML Bomb Denial-of-Service

XML External Entity Processing

XPATH Injection

Command Injection

Cross Site Tracing (XST)

Server Side Request Forgery

XPATH Injection

XPath Injection is an attack technique that uses XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

More Information

- http://projects.wireshark.org/projects/wireshark/wiki/XPath_Injection
- https://www.owasp.org/index.php/XPath_Injection

The below login form is used to log in as a user whose name and password are received from the user.

User Login:

test' OR 'a'='a

User Password:

....

Warning: SimpleXMLElement::xpath(): Invalid predicate in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Warning: SimpleXMLElement::xpath(): xmlXPathEval: evaluation failed in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Your supplied credentials are invalid!

Se probó la siguiente inyección:
User: test' OR 'a'='a
Password: test

Primer intento no funcionó.

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado

Home

About

Setup Instructions

PHP Information

Vulnerabilities

WSDL Enumeration

XML Bomb Denial-of-Service

XML External Entity Processing

XPATH Injection

Command Injection

Cross Site Tracing (XST)

Server Side Request Forgery

XPATH Injection

XPath Injection is an attack technique that uses XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

More Information

- <http://projects.wisecoders.com/000001.php>
- https://www.owasp.org/index.php/XPath_Injection

The below login form is used to login a user whose name and password are received from the user.

User Login:
test' or 1=1 --

User Password:
.....

Warning: SimpleXMLElement::xpath(): Invalid predicate in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Warning: SimpleXMLElement::xpath(): xmlXPathEval: evaluation failed in C:\xampp\htdocs\dvws\vulnerabilities\xpath\xpath.php on line 69

Your supplied credentials are invalid!

Se probó la siguiente inyección:
User: test' OR 1=1 --
Password: test

Segundo intento no funcionó.

Ataques a servicios web

Ataque #3: Prueba en ambiente controlado

XPAT

Se probó la siguiente inyección:
User: test' OR 1=1 OR 'a'='a
Password: test

Se obtuvo el número de cuenta del usuario **Admin**.

Accepted User: Admin
Your Account Number: 06578368643

Ataques a servicios web

Ataque #3: Contramedidas

- Validar cada input utilizado en la consulta XPath.
- “Escapar” el input para hacerlo más seguro de incluir en las consultas XPath construida dinámicamente.
- Definir una lista blanca de caracteres a utilizar para los input. Dicha lista debería mantener la menor cantidad posible de caracteres especiales.

Ataques a servicios web

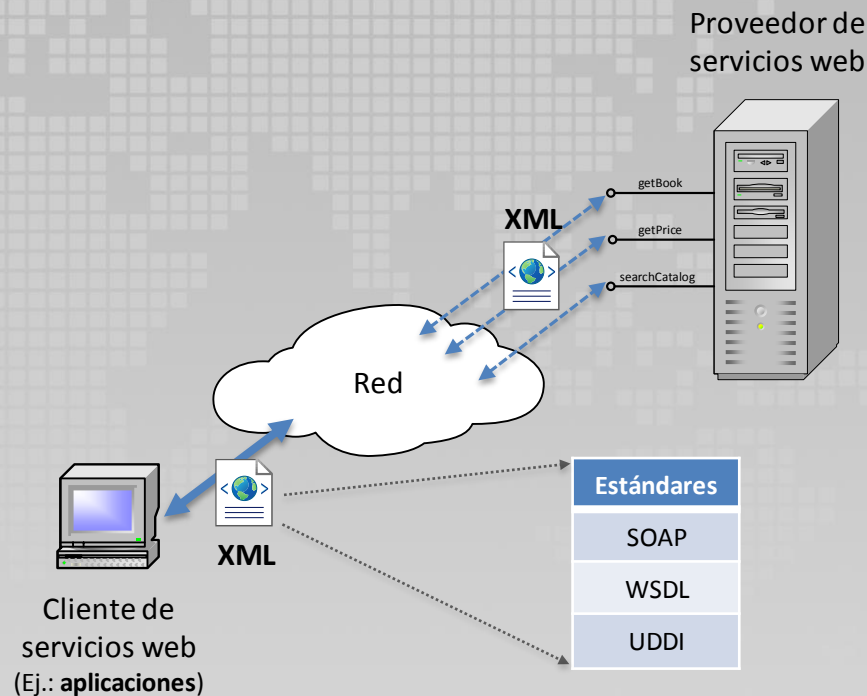
Otros ataques

- Ataques a la lógica de negocio.
- Envenenamiento de esquema de validación
- Expansión de entidad XML.
- Redirección de referencia
- XML flooding
- Reescritura de XML
- Y muchos, muchos más ataques en <http://www.ws-attacks.org/>, guía de pruebas de OWASP, etc.

Más por explorar

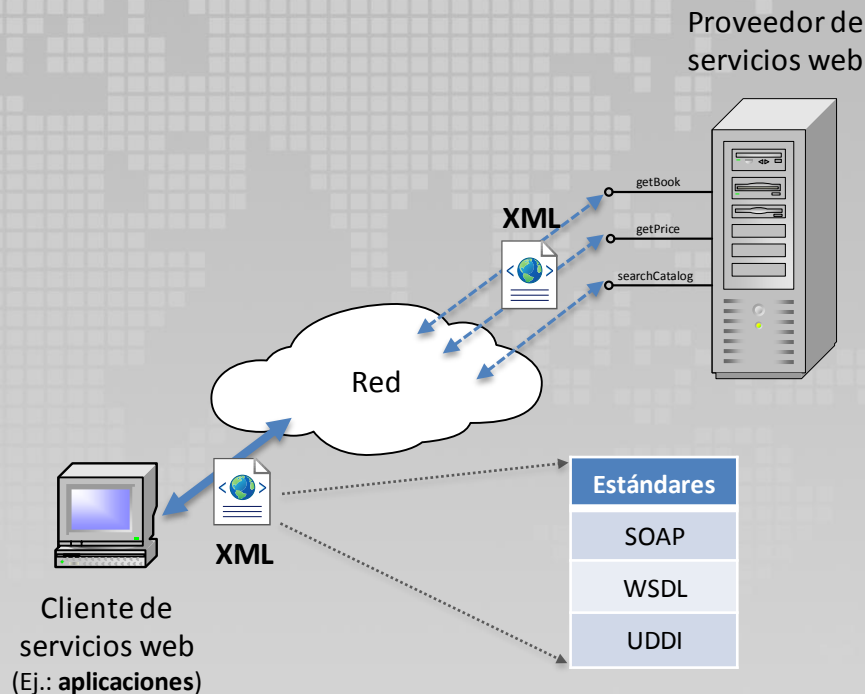
Más por explorar

Capas de los servicios web



Más por explorar

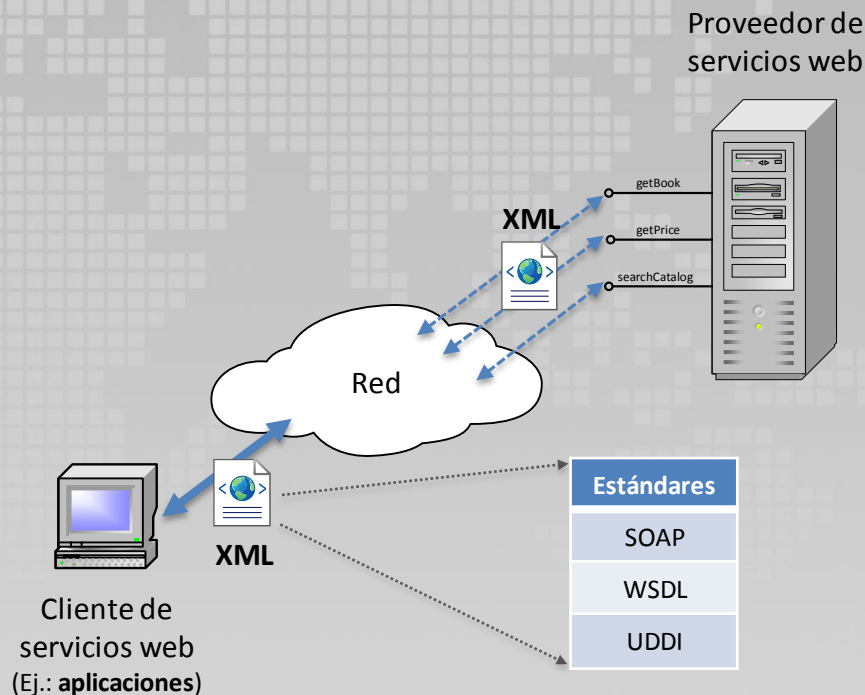
Capas de los servicios web



Más por explorar

Capas de los servicios web

Capas de servicios web
Capa de presentación XML, AJAX , JSON
Capa de descubrimiento UDDI, WSDL
Capa de acceso SOAP, REST , WCF
Capa de transporte HTTP, HTTPS, JMS



Más por explorar
Sección Q&A

¿Preguntas?



OWASP
Open Web Application
Security Project