



Extensión de módulos de pruebas de seguridad de
la herramienta Webgoat Proyecto OWASP



Daniel Cabezas Molina
Daniel Muñoz Marchante

CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. Prueba de Concepto I: Buffer Overflow
4. Prueba de Concepto II: Cifrado Débil
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones

CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. Prueba de Concepto I: Buffer Overflow
4. Prueba de Concepto II: Cifrado Débil
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones

INTRODUCCIÓN

- El servicio más difundido, **WWW**
- Según la consultora Gartner,
 - 75% ataques se realizan a aplicaciones web
 - 3 de 4 servidores son susceptibles a ataques web
- Según la empresa IBM,
 - Cada 1500 líneas de código hay una vulnerabilidad



INTRODUCCIÓN

- El escenario actual refuerza la necesidad de formación en seguridad
- Necesidad de desarrollo de aplicaciones con vulnerabilidades reales
- La comunidad OWASP proporciona WebGoat como herramienta para profesionales y docentes

OBJETIVOS

- Estudio y diseño de una plataforma de seguridad web en entorno Java
- Bases teorico-prácticas sobre seguridad en aplicaciones web
- Ampliación de conceptos y entendimiento de los protocolos en un marco práctico

CONTENIDOS

1. Introducción y objetivos
- 2. Herramientas utilizadas**
3. Prueba de Concepto I: Buffer Overflow
4. Prueba de Concepto II: Cifrado Débil
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones

WEBGOAT



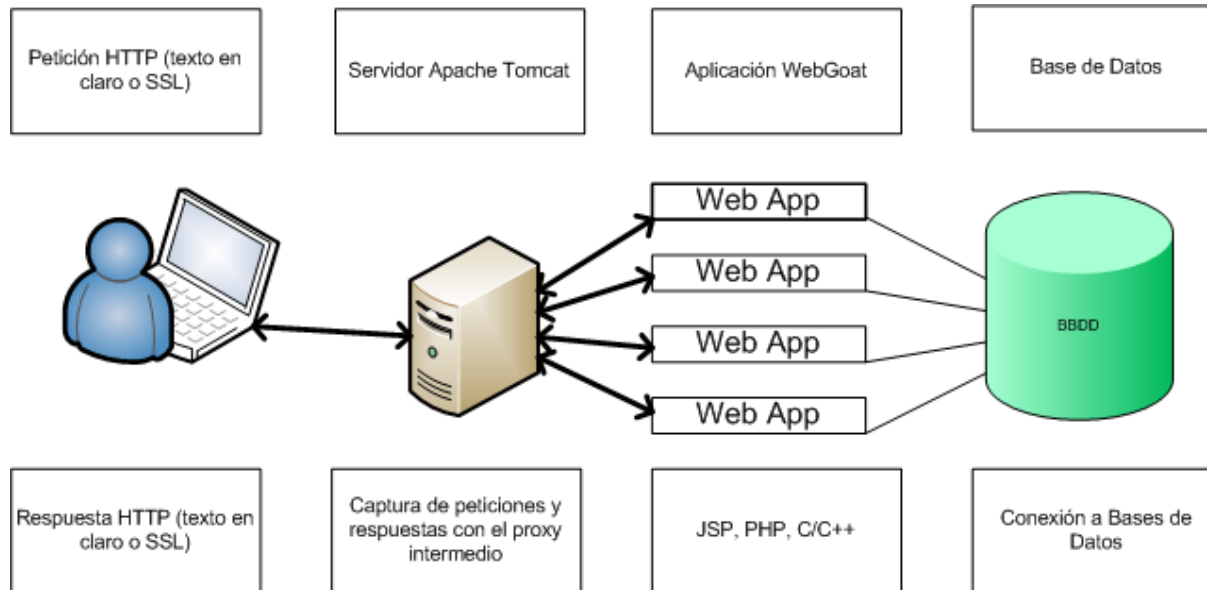
- **Open Web Application Security Project**
- **WebGoat**: Plataforma de seguridad web orientada a la formación y desarrollo
- Utilizada para la formación de nuevos profesionales en empresas:
 - Ernst & Young
 - Google



ENTORNO DE DESARROLLO

- Utilización del entorno de desarrollo integrado, **Eclipse**
- Aplicación realizada en lenguaje **Java (J2EE)**
- Servidor **Jakarta Tomcat**: Contenedor de servlets.
- Herramientas proxy y webspider
 - Paros Proxy
 - WebScarab

ESTRUCTURA DE LA APLICACIÓN



CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. **Prueba de Concepto I: Buffer Overflow**
4. Prueba de Concepto II: Cifrado Débil
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones y líneas futuras

BUFFER OVERFLOW

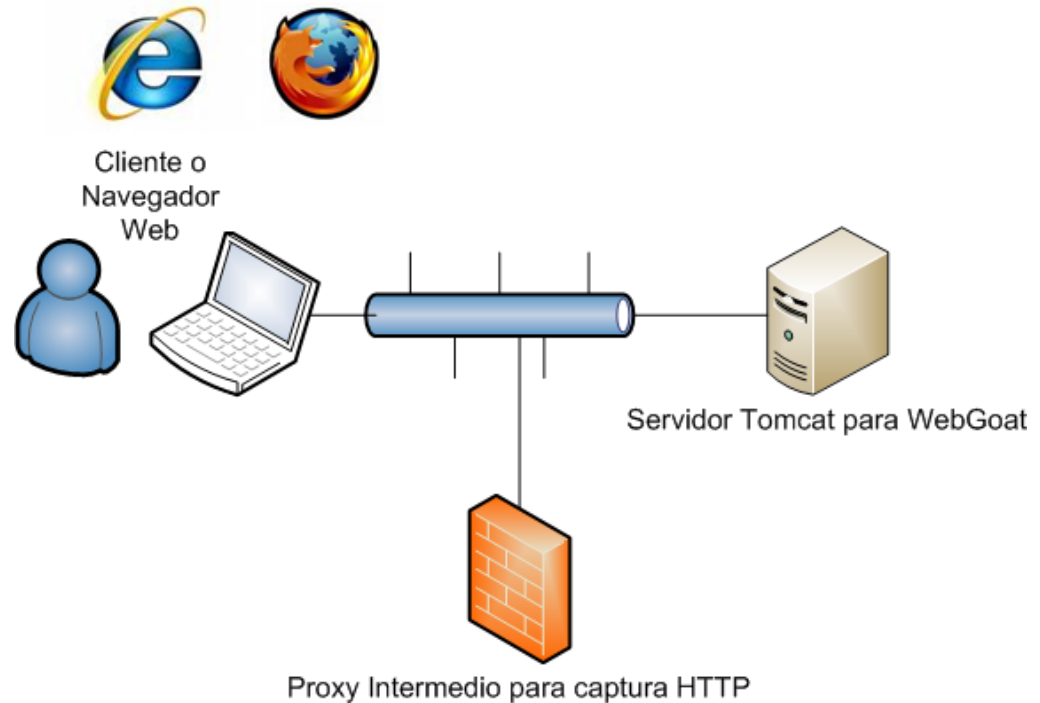
- Es una de las vulnerabilidades más conocidas y explotadas
- Debido a las siguientes causas principales:
 - Error en implementación de métodos de validación de datos de entrada
 - Error en la gestión de memoria

BUFFER OVERFLOW EN WEBGOAT

- Análisis de los métodos de validación de la aplicación
- Pruebas para determinar la validación:
 - Tipos de datos admitidos
 - Longitud de los datos
 - Lógica y flujo de la aplicación
- Objetivo: Provocar un buffer overflow en la aplicación

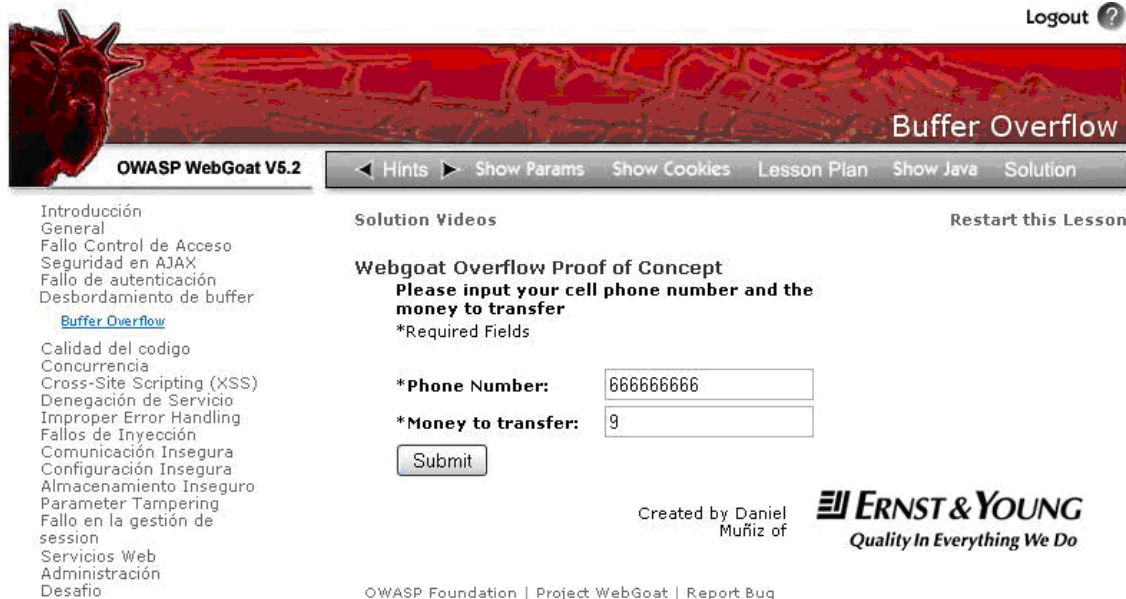
BUFFER OVERFLOW EN WEBGOAT

1. Envío peticiones HTTP al servidor
2. Estudio de los métodos de validación de datos de entrada y lógica de la aplicación
3. Forzar el error de la aplicación haciendo abuso de los métodos de validación



BUFFER OVERFLOW EN WEBGOAT

1. Envío peticiones



The screenshot shows the OWASP WebGoat V5.2 interface. At the top right is a "Logout ?" link. Below the navigation bar, there's a list of challenges on the left, including "Buffer Overflow" which is highlighted. The main content area displays the "Buffer Overflow" challenge details, including a "Solution Videos" section and a "Webgoat Overflow Proof of Concept" section. The challenge text reads: "Please input your cell phone number and the money to transfer". Below this, there are two input fields: "*Phone Number:" with the value "6666666666" and "*Money to transfer:" with the value "9". A "Submit" button is located below the input fields. At the bottom right, there's a logo for "ERNST & YOUNG" with the tagline "Quality In Everything We Do".

Logout ?

Buffer Overflow

OWASP WebGoat V5.2

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introducción
General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
[Buffer Overflow](#)
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura
Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos

Restart this Lesson

Webgoat Overflow Proof of Concept

Please input your cell phone number and the money to transfer

*Required Fields

*Phone Number: 6666666666

*Money to transfer: 9

Submit

Created by Daniel Muñiz of

ERNST & YOUNG
Quality In Everything We Do

OWASP Foundation | Project WebGoat | Report Bug

Variable asignada al número de teléfono

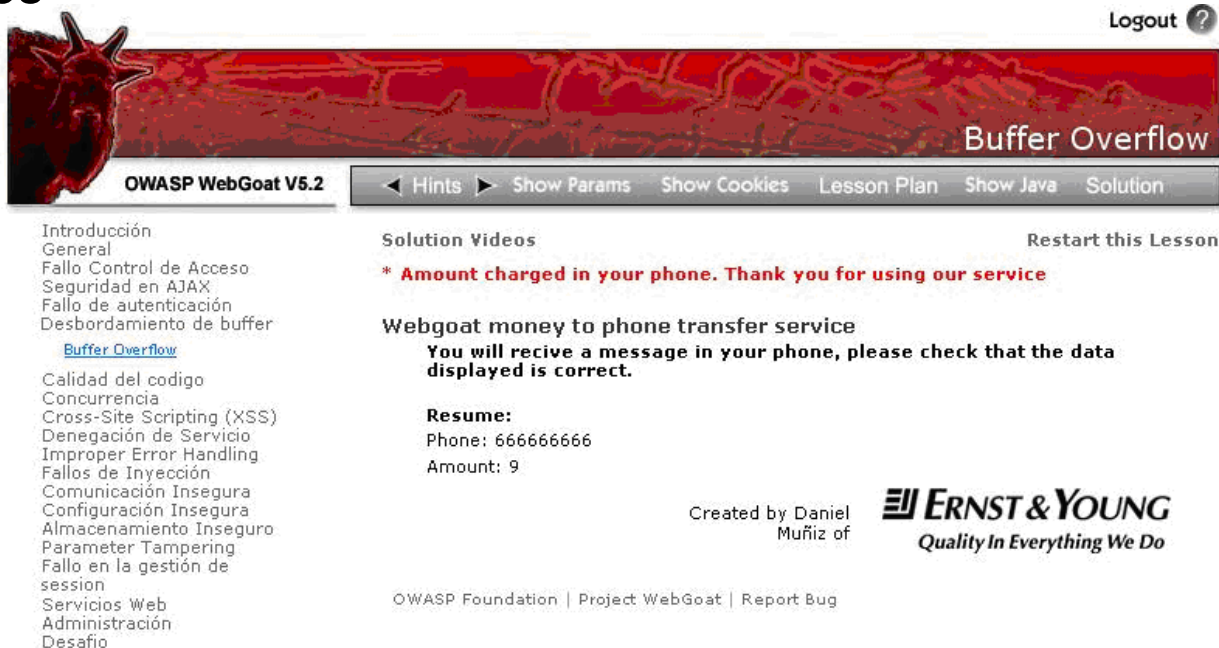
Variable asignada al saldo a cargar

.....

RET

BUFFER OVERFLOW EN WEBGOAT

1. Envío peticiones



The screenshot shows the OWASP WebGoat V5.2 interface. At the top right, there is a "Logout ?" link. The main header features a red banner with a goat head on the left and the text "Buffer Overflow" on the right. Below the banner is a navigation bar with links: "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution". The left sidebar contains a list of topics, with "Buffer Overflow" highlighted. The main content area displays the lesson title "Buffer Overflow" and a "Restart this Lesson" link. Below this, there is a red message: "* Amount charged in your phone. Thank you for using our service". The lesson content includes a "Webgoat money to phone transfer service" section with a "Resume:" link, a "Phone: 6666666666" field, and an "Amount: 9" field. At the bottom right, there is a logo for "ERNST & YOUNG" with the tagline "Quality In Everything We Do".

Logout ?

Buffer Overflow

OWASP WebGoat V5.2

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introducción
General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
[Buffer Overflow](#)
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura
Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos Restart this Lesson

* Amount charged in your phone. Thank you for using our service

Webgoat money to phone transfer service
You will receive a message in your phone, please check that the data displayed is correct.

Resume:
Phone: 6666666666
Amount: 9

Created by Daniel Mufiz of **ERNST & YOUNG**
Quality In Everything We Do

OWASP Foundation | Project: WebGoat | Report Bug

BUFFER OVERFLOW EN WEBGOAT

2. Estudio de los métodos de validación



The screenshot shows the OWASP WebGoat V5.2 interface. At the top, there's a red banner with a goat head on the left and the text "Buffer Overflow" on the right. Below the banner, a navigation bar contains links: "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution". To the right of the banner is a "Logout ?" link. Below the navigation bar, on the left, is a list of topics: "Introducción", "General", "Fallo Control de Acceso", "Seguridad en AJAX", "Fallo de autenticación", "Desbordamiento de buffer" (with "Buffer Overflow" as a sub-link), "Calidad del código", "Concurrencia", "Cross-Site Scripting (XSS)", "Denegación de Servicio", "Improper Error Handling", "Fallos de Inyección", "Comunicación Insegura", "Configuración Insegura", "Almacenamiento Inseguro", "Parameter Tampering", "Fallo en la gestión de session", "Servicios Web", "Administración", and "Desafío". To the right of this list, under "Solution Videos", is the "Webgoat Overflow Proof of Concept" section. It contains the text "Please input your cell phone number and the money to transfer" and "*Required Fields". Below this are two input fields: "*Phone Number:" with the value "no phone" and "*Money to transfer:" with the value "6". A "Submit" button is located below these fields. To the right of the input fields is a "Restart this Lesson" link. At the bottom right, it says "Created by Daniel Muñoz of ERNST & YOUNG Quality In Everything We Do". At the bottom center, it says "OWASP Foundation | Project WebGoat | Report Bug".

OWASP WebGoat V5.2

Logout ?

Buffer Overflow

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introducción
General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
[Buffer Overflow](#)
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura
Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos

Restart this Lesson

Webgoat Overflow Proof of Concept
Please input your cell phone number and the money to transfer
*Required Fields

*Phone Number: no phone

*Money to transfer: 6


Submit

Created by Daniel Muñoz of ERNST & YOUNG
Quality In Everything We Do

OWASP Foundation | Project WebGoat | Report Bug

BUFFER OVERFLOW EN WEBGOAT

2. Estudio de los métodos de validación



OWASP WebGoat V5.2

Logout ?

Buffer Overflow

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introducción
General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
[Buffer Overflow](#)
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura
Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos


Restart this Lesson

*** Not valid phone or amount. Please try again.**

Webgoat Overflow Proof of Concept
Please input your cell phone number and the money to transfer
*Required Fields


***Phone Number:**

***Money to transfer:**

Created by Daniel Muñiz of  **ERNST & YOUNG**
Quality In Everything We Do

BUFFER OVERFLOW EN WEBGOAT

2. Estudio de los métodos de validación



OWASP WebGoat V5.2

[Logout ?](#)

Buffer Overflow

[Hints](#) [Show Params](#) [Show Cookies](#) [Lesson Plan](#) [Show Java](#) [Solution](#)

- Introducción
- General
- Fallo Control de Acceso
- Seguridad en AJAX
- Fallo de autenticación
- Desbordamiento de buffer
- [Buffer Overflow](#)
- Calidad del código
- Concurrencia
- Cross-Site Scripting (XSS)
- Denegación de Servicio
- Improper Error Handling
- Fallos de Inyección
- Comunicación Insegura
- Configuración Insegura
- Almacenamiento Inseguro
- Parameter Tampering
- Fallo en la gestión de session
- Servicios Web
- Administración
- Desafío

Solution Videos

[Restart this Lesson](#)

Webgoat Overflow Proof of Concept


Please input your cell phone number and the money to transfer

*Required Fields

*Phone Number:

*Money to transfer:

Created by Daniel Mufiz of

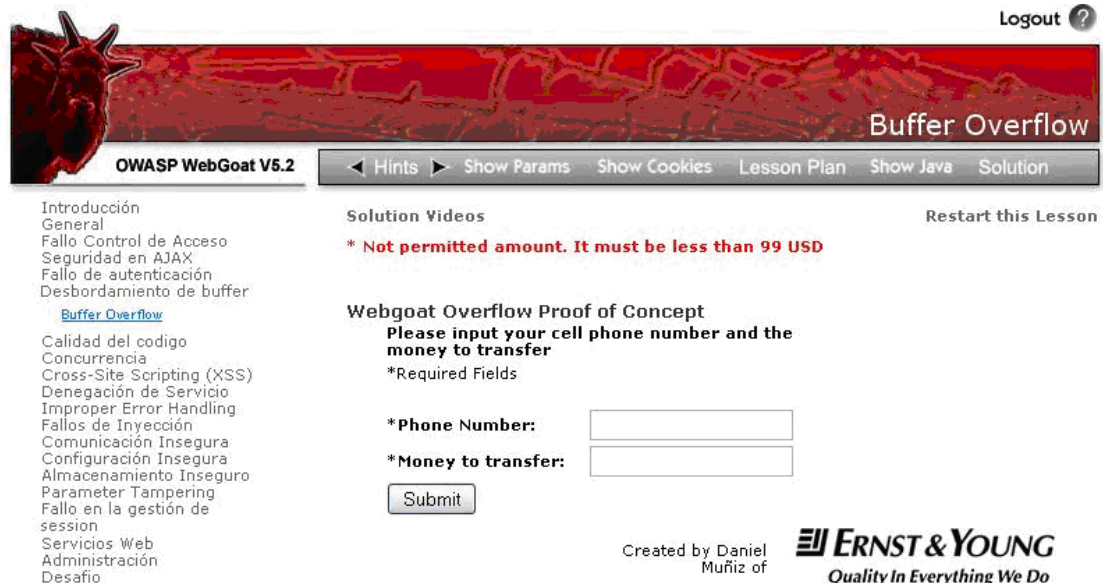


Quality In Everything We Do

OWASP Foundation | Project WebGoat | Report Bug

BUFFER OVERFLOW EN WEBGOAT

2. Estudio de los métodos de validación



The screenshot shows the OWASP WebGoat V5.2 interface. At the top right, there is a "Logout ?" link. Below the header, a navigation bar contains links: "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution". The main content area is titled "Buffer Overflow" and includes a "Restart this Lesson" link. A list of topics is on the left, with "Buffer Overflow" highlighted. The main text area contains the following content:

Solution Videos

*** Not permitted amount. It must be less than 99 USD**

Webgoat Overflow Proof of Concept
Please input your cell phone number and the money to transfer

***Required Fields**

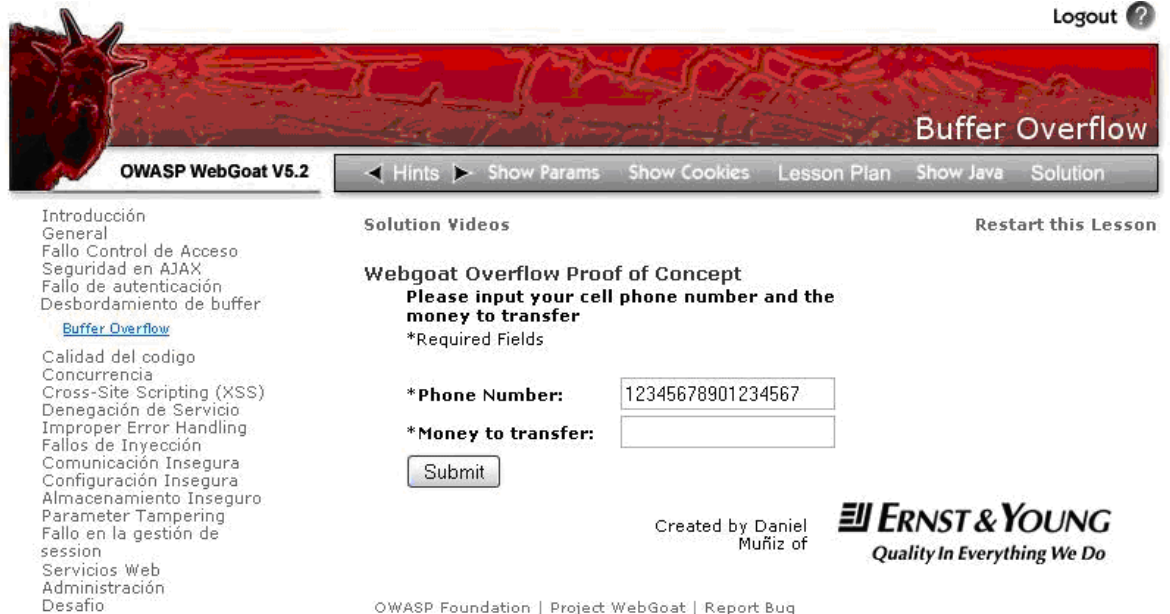
***Phone Number:**

***Money to transfer:**

Created by Daniel Mufiz of **ERNST & YOUNG**
Quality In Everything We Do

BUFFER OVERFLOW EN WEBGOAT

3. Forzar el error de la aplicación



The screenshot shows the OWASP WebGoat V5.2 web application interface. At the top right, there is a "Logout ?" link. The main header features a red banner with a goat head on the left and the text "Buffer Overflow" on the right. Below the banner is a navigation bar with links: "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution". The left sidebar contains a list of topics, with "Buffer Overflow" highlighted. The main content area is titled "Webgoat Overflow Proof of Concept" and includes a form for inputting a cell phone number and money to transfer. The form has two input fields, one for the phone number (containing "12345678901234567") and one for the money to transfer. A "Submit" button is located below the fields. The footer of the interface includes the OWASP Foundation logo, the text "OWASP Foundation | Project WebGoat | Report Bug", and the Ernst & Young logo with the tagline "Quality In Everything We Do".

Logout ?

Buffer Overflow

OWASP WebGoat V5.2

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introduction
General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
[Buffer Overflow](#)
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura
Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos

Restart this Lesson

Webgoat Overflow Proof of Concept
Please input your cell phone number and the money to transfer
*Required Fields

*Phone Number: 12345678901234567

*Money to transfer:

Submit

Created by Daniel Muñiz of

ERNST & YOUNG
Quality In Everything We Do

OWASP Foundation | Project WebGoat | Report Bug

BUFFER OVERFLOW EN WEBGOAT

3. Forzar el error de la aplicación

[illegible]

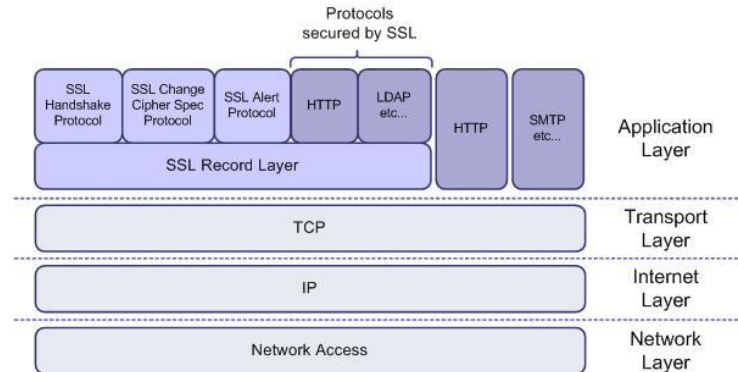
CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. Prueba de Concepto I: Buffer Overflow
- 4. Prueba de Concepto II: Cifrado Débil**
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones y líneas futuras

CIFRADO DÉBIL EN SSL



- **SSL**: **S**ecure **S**ocket **L**ayer
- Proporciona seguridad a las comunicaciones
- Aporta valores añadidos a la comunicación:
 - Integridad
 - Confidencialidad
 - Autenticidad



CIFRADO DÉBIL EN WEBGOAT

- Unsalted Hash
- Cifrado Débil RSA
 - Espacio de claves limitado
 - Longitud de claves bajo
- Certificados formados a partir de claves débiles
 - Ejemplo real

CIFRADO DÉBIL EN WEBGOAT

- No se envía la contraseña en claro, se utiliza el hash de la misma
- Existe el denominado unsalted hash o salted hash
- El uso de salted hash incrementa de forma exponencial la seguridad en el envío de información sensible
 - Unsalted Hash
 - **md5(admin)** = 21232f297a57a5a743894a0e4a801fc3 (128 bits)
 - Salted Hash
 - **Salt(md5(admin))** = 121232f297a57a5a743894a0e4a801fc3

CIFRADO DÉBIL EN WEBGOAT

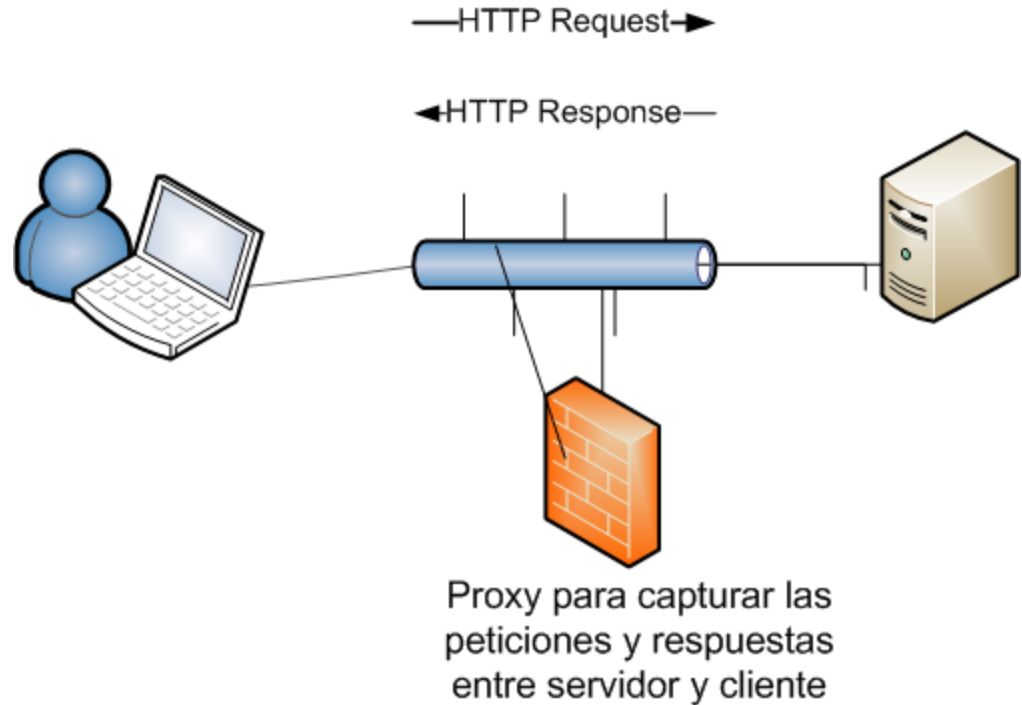
- Utilización de cifrado RSA de 16 bits
- Basa su fortaleza en la dificultad de factorizar números grandes
- Problemas del cifrado implementado:
 - Espacio de claves limitado
 - Longitud de claves baja

CIFRADO DÉBIL EN WEBGOAT

- Cifrado RSA con el generador de números aleatorios con una entropía baja
- Ejemplo: el generador utilizado en la distribución Linux, Debian
- Certificado creado a partir de clave débil de OpenSSL Debian

CIFRADO DÉBIL EN WEBGOAT

1. Mediante el proxy intermedio se capturan las credenciales cifradas para las pruebas 1 y 2.
2. En la tercera prueba se utiliza una conexión HTTPS. Se debe capturar y analizar el certificado del servidor



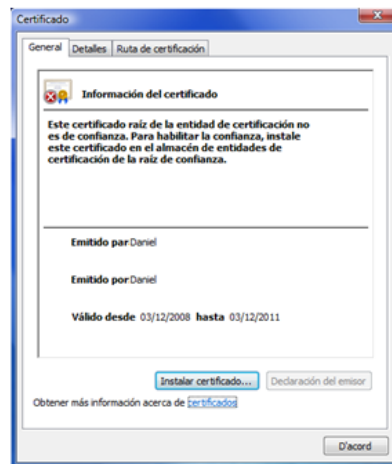
CIFRADO DÉBIL EN WEBGOAT

1. Captura de credenciales cifradas para las pruebas

```
openssl pkcs8 -topk8 -nocrypt -in bad_rsa.key -inform PEM -out bad_rsa.der -outform DER
```

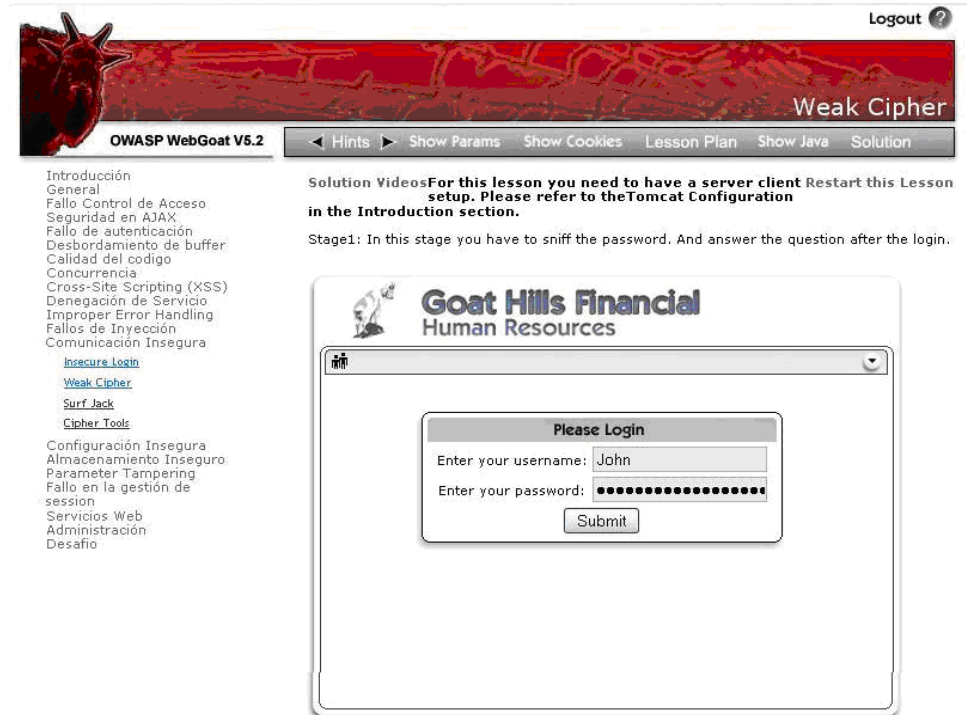
```
openssl x509 -in bad_ca.pem -inform PEM -out bad_ca.der -outform DER
```

Al ser un certificado firmado por el emisor del certificado los navegadores actuales lo detectan como un certificado no confiable y alertan al usuario de la utilización de un certificado no asociado a ningún CA de confianza y firma por el emisor del certificado. Si se visualiza el certificado bad_ca.der se obtiene el siguiente mensaje:



CIFRADO DÉBIL EN WEBGOAT

1. Captura de credenciales cifradas para las pruebas



The screenshot displays the OWASP WebGoat V5.2 interface. At the top, there is a red banner with a goat head on the left and the text "Weak Cipher" on the right. Below the banner, a navigation bar contains links: "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution".

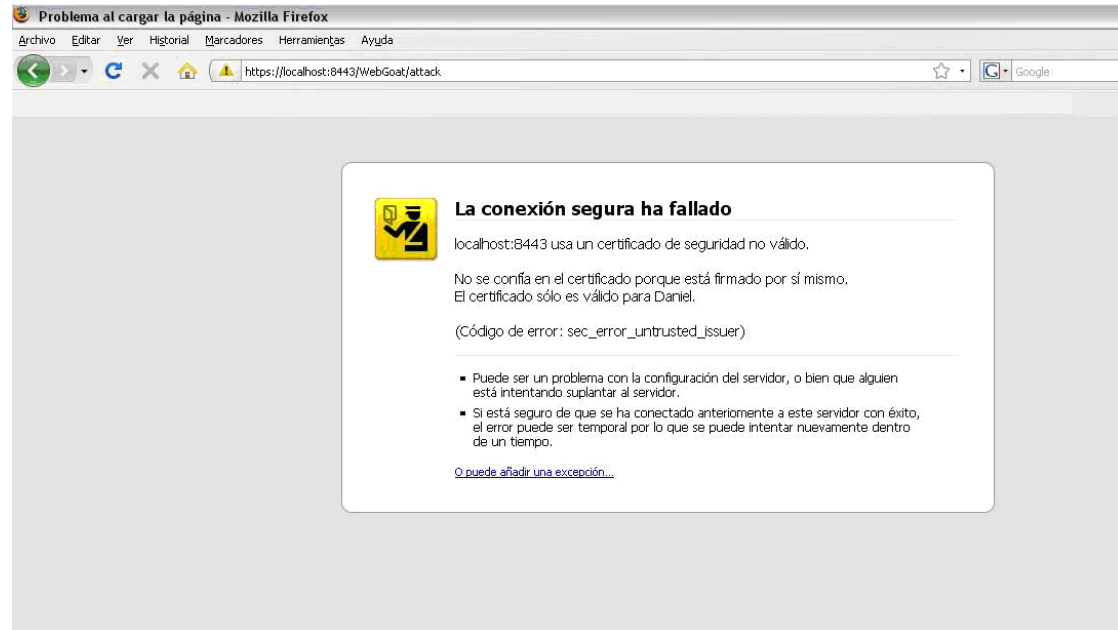
On the left side, a list of topics is shown, including "Introducción", "General", "Fallo Control de Acceso", "Seguridad en AJAX", "Fallo de autenticación", "Desbordamiento de buffer", "Calidad del código", "Concurrencia", "Cross-Site Scripting (XSS)", "Denegación de Servicio", "Improper Error Handling", "Fallos de Inyección", and "Comunicación Insegura". Below these, there are links for "Insecure Login", "Weak Cipher", "Surf Jack", and "Cipher Tools".

The main content area on the right features a "Solution Videos" section with the text: "For this lesson you need to have a server client Restart this Lesson setup. Please refer to the Tomcat Configuration in the Introduction section." Below this, it states: "Stage1: In this stage you have to sniff the password. And answer the question after the login."

At the bottom right, there is a simulated web application window titled "Goat Hills Financial Human Resources". It contains a login form with the heading "Please Login", fields for "Enter your username:" (containing "John") and "Enter your password:" (masked with dots), and a "Submit" button.

CIFRADO DÉBIL EN WEBGOAT

1. Captura de credenciales cifradas para las pruebas



CIFRADO DÉBIL EN WEBGOAT

1. Captura de credenciales cifradas para las pruebas

OWASP WebGoat V5.2

Logout ?

Weak Cipher

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introducción General
Fallo Control de Acceso
Seguridad en AJAX
Fallo de autenticación
Desbordamiento de buffer
Calidad del código
Concurrencia
Cross-Site Scripting (XSS)
Denegación de Servicio
Improper Error Handling
Fallos de Inyección
Comunicación Insegura

[Insecure Login](#)
[Weak Cipher](#)
[Surf Jack](#)
[Cipher Tools](#)

Configuración Insegura
Almacenamiento Inseguro
Parameter Tampering
Fallo en la gestión de session
Servicios Web
Administración
Desafío

Solution Videos For this lesson you need to have a server client Restart this Lesson setup. Please refer to the Tomcat Configuration in the Introduction section.

Stage3: Now you have to change to a secure connection. The URL should start with https:// If your browser is complaining about the certificate just ignore it. Sniff again the traffic and answer the questions. In example https://localhost:8443/... (If you the port 8443)

Goat Hills Financial
Human Resources

Firstname: John
Lastname: Wayne
Credit Card Type: AE
Credit Card Number: 934567890

Logout

What's the PID used to generate the RSA (1024 bits) private key. Try to sniff the conversation and decode the content:

CIFRADO DÉBIL EN WEBGOAT

1. Captura de credenciales cifradas para las pruebas

The screenshot displays the OWASP WebGoat V5.2 web application. The top navigation bar includes links for "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution". A "Weak Cipher" banner is visible on the right. The left sidebar contains a list of topics, including "Insecure Login", "Weak Cipher", "Surf Jack", and "Cipher Tools". A "Security Warning" dialog box is open, displaying the following information:

Security Warning

A weak SSL certificate has been detected.

Access to the following URL is not secure:

`https://localhost:8443/WebGoat/attack?Screen=15&menu=1300`

The server certificate has a known bad key.

It is recommended that you do not exchange sensitive data with this website.

Certificate Information

Display Name: Daniel

Certificate Fingerprint: 21F294F8AB712E66FE6873F91EC83F0795D87A8F

Key Generation Information

Bit count: 1024; Platform: x64, PID: 1234, .rnd: noreadrnd

Public Key Modulus SHA1 Hash: 58dce70acfd4dc1a9d28722fc62edb8d30110778

☐ Don't show this dialog for this certificate anymore

At the bottom of the dialog, there is a "Submit" button. Below the dialog, a diagram shows "Encrypted Data" being sent from a client to a server, with a note: "What's the PID used to generate the RSA (1024 bits) private key. Try to sniff the conversation and decode the content:".

CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. Prueba de Concepto I: Buffer Overflow
4. Prueba de Concepto II: Cifrado Débil
- 5. Prueba de Concepto III: HTTPS Inseguro**
6. Conclusiones y líneas futuras

HTTPS INSEGURO

- HTTPS, permite el uso de protocolo HTTP a través una conexión segura
- Utilización de cookies para mantener la sesión y preferencias del usuario
- Técnica de session hijacking o robo de sesión

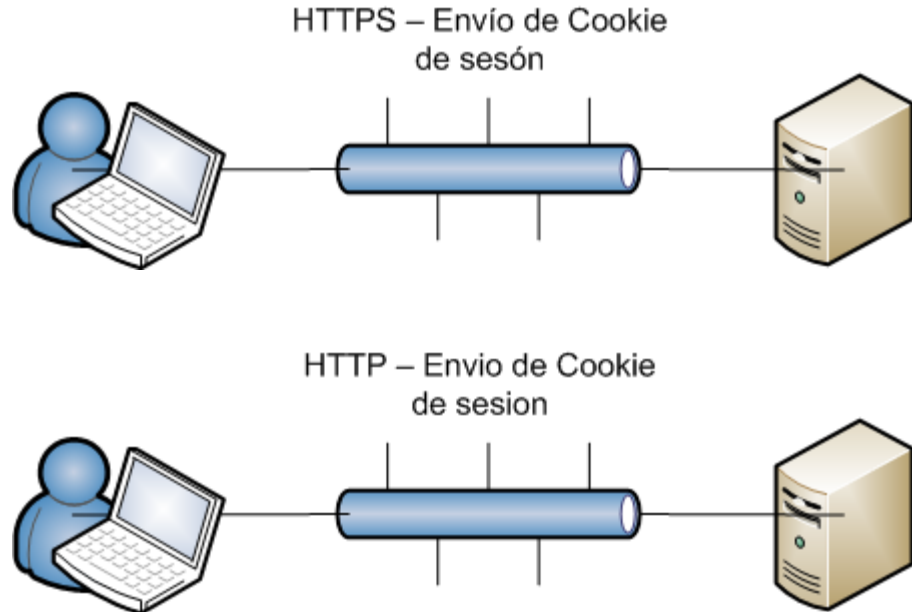


HTTPS INSEGURO

- Existen aplicaciones que permiten el envío de cookies de sesión a través de un canal no seguro
- El objetivo: cambiar el canal seguro (HTTPS) por un canal inseguro (HTTP) y capturar la cookie de sesión


HTTPS INSEGURO

1. Petición HTTPS para el envío de la cookie de sesión
2. Cambiar la conexión segura por HTTP y reenviar la cookie de sesión
3. Captura de la cookie de sesión



HTTPS INSEGURO

1. Petición HTTPS para el envío de la cookie de sesión



OWASP WebGoat V5.2

- Introducción
- General
- Fallo Control de Acceso
- Seguridad en AJAX
- Fallo de autenticación
- Desbordamiento de buffer
- Calidad del código
- Concurrencia
- Cross-Site Scripting (XSS)
- Denegación de Servicio
- Improper Error Handling
- Fallos de Inyección
- Comunicación Insegura
 - [Insecure Login](#)
 - [Weak Cipher](#)
 - [Surf Jack](#)
 - [Cipher Tools](#)
- Configuración Insegura
- Almacenamiento Inseguro
- Parameter Tampering
- Fallo en la gestión de session
- Servicios Web
- Administración
- Desafío


Logout ?

Surf Jack

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Solution Videos For this lesson you need to have a server client setup. Please refer to the Tomcat Configuration in the Introduction section. Restart this Lesson

Now you have to change to a secure connection. The URL should start with https:// If your browser is complaining about the certificate just ignore it. Sniff again the traffic and answer the questions



Goat Hills Financial
Human Resources

Please Login


Enter your name: WebGoat

Enter your password: ●●●●●●

Submit

HTTPS INSEGURO

2. Cambiar la conexión segura por HTTP y reenviar la cookie de sesión



OWASP WebGoat V5.2

[Logout ?](#)


[Hints](#) [Show Params](#) [Show Cookies](#) [Lesson Plan](#) [Show Java](#) [Solution](#)

[Introducción](#)
[General](#)
[Fallo Control de Acceso](#)
[Seguridad en AJAX](#)
[Fallo de autenticación](#)
[Desbordamiento de buffer](#)
[Calidad del código](#)
[Concurrencia](#)
[Cross-Site Scripting \(XSS\)](#)
[Denegación de Servicio](#)
[Improper Error Handling](#)
[Fallos de Inyección](#)
[Comunicación Insegura](#)
[Insecure Login](#)
[Weak Cipher](#)
[Surf Jack](#)
[Cipher Tools](#)
[Configuración Insegura](#)
[Almacenamiento Inseguro](#)
[Parameter Tampering](#)
[Fallo en la gestión de session](#)
[Servicios Web](#)
[Administración](#)
[Desafío](#)

Solution Videos For this lesson you need to have a server client Restart this Lesson setup. Please refer to the Tomcat Configuration in the Introduction section.

Now you have to change to a secure connection. The URL should start with https:// If your browser is complaining about the certificate just ignore it. Sniff again the traffic and answer the questions

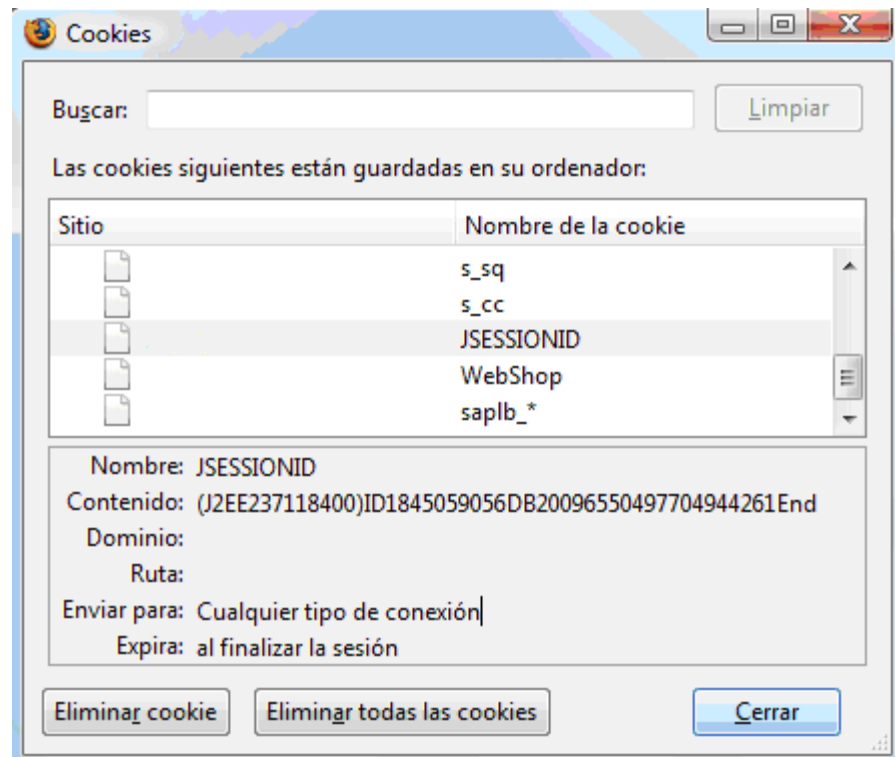
Press submit to send the session cookie

Created by Daniel Mufiz of  **ERNST & YOUNG**
Quality In Everything We Do

OWASP Foundation | Project WebGoat | Report Bug

HTTPS INSEGURO

3. Captura de la cookie



CONTENIDOS

1. Introducción y objetivos
2. Herramientas utilizadas
3. Prueba de Concepto I: Buffer Overflow
4. Prueba de Concepto II: Cifrado Débil
5. Prueba de Concepto III: HTTPS Inseguro
6. Conclusiones y líneas futuras

CONCLUSIONES Y LÍNEAS FUTURAS

- Tomar consciencia de la importancia de la seguridad en aplicaciones web
- WebGoat como herramienta docente para la formación en seguridad informática
- Base para la creación de un laboratorio de seguridad
- Participación en un proyecto abierto para la comunidad OWASP

GRACIAS POR SU ATENCIÓN

