

## Actividad | 1 | Pérdida de autenticación y gestión de sesiones.

### Auditoría Informática.

Ingeniería en Desarrollo de  
Software.



academiaglobal

TUTOR: Jessica Hernández Romero

ALUMNO: Carlos Ariel Nicolini

FECHA: 7/10/2025

## Índice

<b>Introducción .....</b>	<b>3</b>
<b>Descripción .....</b>	<b>4</b>
<b>Justificación .....</b>	<b>5</b>
<b>Desarrollo.....</b>	<b>6</b>
• <b>Descripción del sitio web .....</b>	<b>6</b>
• <b>Ataque al sitio web .....</b>	<b>8</b>
<b>Conclusión.....</b>	<b>13</b>
<b>Referencias.....</b>	<b>14</b>

# Introducción

Las vulnerabilidades relacionadas con la pérdida de autenticación y gestión de sesiones son críticas en la seguridad de aplicaciones y en especial de las aplicaciones WEB, ya que permiten a un atacante suplantar la información de un determinado usuario, pudiendo llegar a obtener una cuenta de administración que le permita sabotear los controles de autorización y registro de la aplicación. En esta situación podría ocasionar un acceso no autorizado a cualquier tipo de información que se encuentre almacenada en el servidor o los servicios que han sido comprometidos.

Existen multitud de situaciones en las que nos podemos encontrar ante una aplicación vulnerable a este tipo de ataque, pero la mayor parte de las veces se encuentra en la gestión de las contraseñas, la expiración de sesiones o el proceso de cierre de sesión. Además, debe prestarse especial atención a los procesos que permiten la recuperación de los valores del usuario de forma automática como pueden ser los servicios de pregunta secreta, de actualización de cuenta o de “Recordar contraseña”.

Existen diferentes formas de proteger la aplicación desarrollada de este tipo de vulnerabilidades, pero requieren decisiones a nivel de diseño. En primer lugar, la gestión de contraseñas nunca debe almacenarse en texto plano, aspecto que, aunque a ustedes les parezca obvio, es más común de lo que piensan. Además, deben utilizarse los servicios que utilicen información sensible a través de canales seguros, como puede ser una conexión sobre SSL, de forma que se evite la posibilidad de que un atacante se interponga en la comunicación de esta información entre nuestro cliente y el servidor de la aplicación de datos.

# Descripción

## **Contextualización:**

Una empresa de software solicita realizar varias pruebas de seguridad en páginas web que no cuentan con los candados de seguridad.

En esta primera etapa, realizar una prueba de la vulnerabilidad de la pérdida de autenticación y gestión de sesiones utilizando el programa WireShark. El objetivo de esta prueba es sacar las credenciales que se ingresaron y estas se puedan mostrar.

## **Actividad:**

Seleccionar un proyecto web realizado anteriormente que cuente con las siguientes características:

- Función de iniciar sesión y de registro de usuarios.
- Conexión con una base de datos.

Subir el proyecto a un servidor web con la base de datos incluida. Una vez que el proyecto este en internet, realizar la instalación de WireShark. Este programa permite realizar el ataque. Una vez echo esto, proceder a realizar el ataque al sitio web aprovechando la vulnerabilidad de falta de SSL o seguridad.

Para este ejercicio no utilizaremos un sitio creado en un proyecto anterior, ya que no se tenía un sitio publicado con las características necesarias, por tal motivo se utiliza una pagina de un sitio especializado en tener paginas vulnerables para estas pruebas de seguridad.

# Justificación

En esta actividad realizaremos un ataque de pérdida de autenticación y gestión de sesiones a una página donde nos mostrara, mediante esta prueba controlada, las consecuencias de una configuración de seguridad insuficiente en aplicaciones web que son más comunes de lo que creemos. Con ayuda de WireShark, capturaremos tráfico y se pretende demostrar de manera tangible como la ausencia de un cifrado de seguridad (SSL/TLS), además de una administración inadecuada de sesiones puede materializarse en la exposición de credenciales y otros datos sensibles de una manera tan fácil como se demostrará en el ejercicio.

El objetivo principal es observar, documentar y analizar las trazas de red que nos van a permitir la recuperación de credenciales en texto plano, con el objetivo de identificar fallos en la autenticación y en el manejo de sesiones. Con estos resultados desarrolladores y responsables de aplicaciones o paginas web, pueden ver de manera muy clara sobre la importancia de estos riesgos reales.

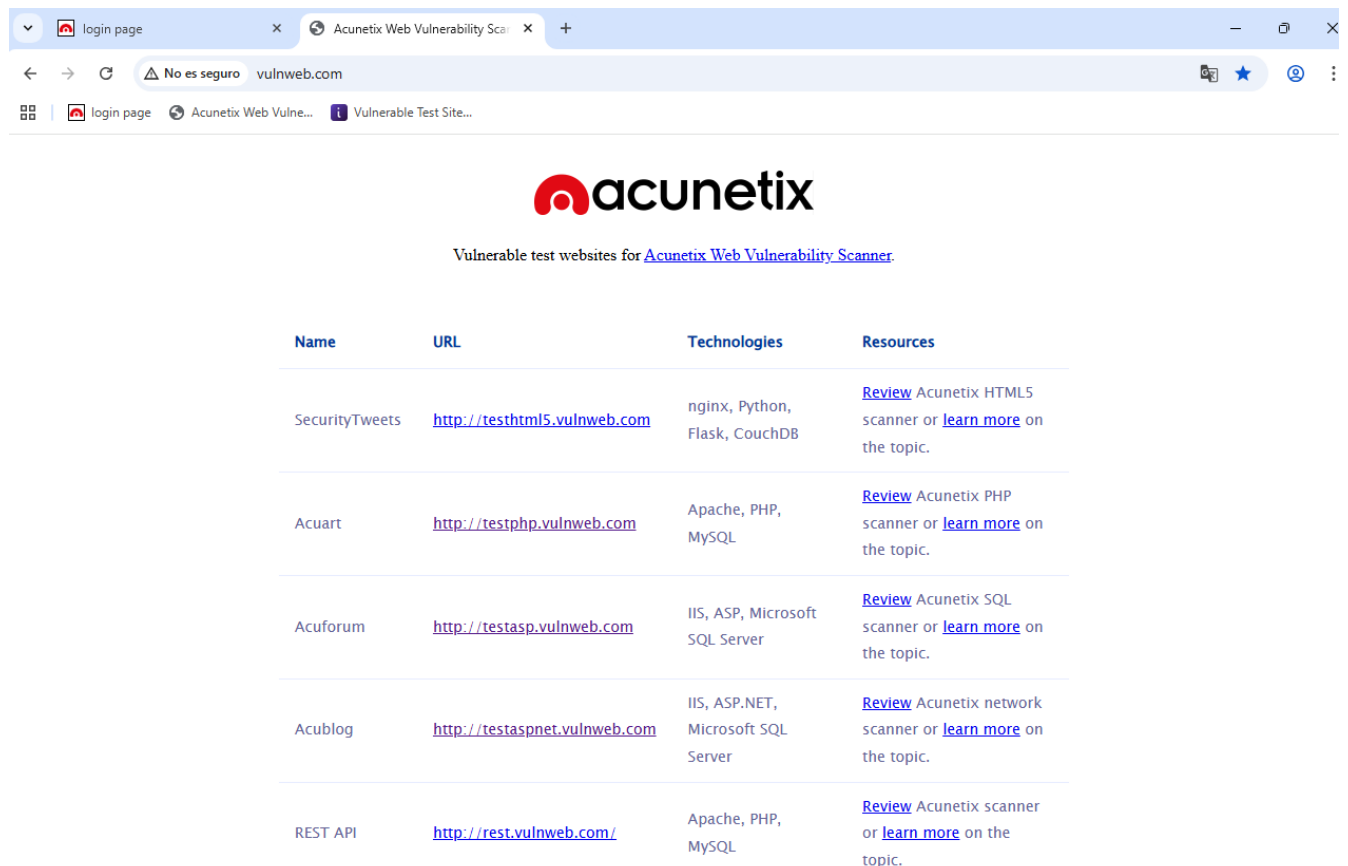
Este trabajo fue subido al siguiente enlace de GitHub

<https://github.com/CarlosNico/Auditor-a-Inform-tica>

# Desarrollo

## Descripción del sitio Web

Para el sitio Web no se utilizó un proyecto anterior, ya que no se contaba con un proyecto publicado con las características solicitadas. Por tal motivo, como se vio en clase se utilizó un sitio especial para realizar este tipo de pruebas de seguridad en una máquina virtual de Hyper-V. El sitio se llama Acuart, con la siguiente dirección <http://testphp.vulnweb.com>, el cual cuenta con apache, php y MySQL. La cual es proporcionada por Acunetix que es una web para escaneos de vulnerabilidades.



The screenshot shows a web browser window with the address bar displaying 'vulnweb.com'. The page content includes the Acunetix logo and a table titled 'Vulnerable test websites for Acunetix Web Vulnerability Scanner'. The table lists five test websites: SecurityTweets, Acuart, Acuforum, Acublog, and REST API, each with its URL, technologies, and resources for further information.

Name	URL	Technologies	Resources
SecurityTweets	<a href="http://testhtml5.vulnweb.com">http://testhtml5.vulnweb.com</a>	nginx, Python, Flask, CouchDB	<a href="#">Review</a> Acunetix HTML5 scanner or <a href="#">learn more</a> on the topic.
Acuart	<a href="http://testphp.vulnweb.com">http://testphp.vulnweb.com</a>	Apache, PHP, MySQL	<a href="#">Review</a> Acunetix PHP scanner or <a href="#">learn more</a> on the topic.
Acuforum	<a href="http://testasp.vulnweb.com">http://testasp.vulnweb.com</a>	IIS, ASP, Microsoft SQL Server	<a href="#">Review</a> Acunetix SQL scanner or <a href="#">learn more</a> on the topic.
Acublog	<a href="http://testaspnet.vulnweb.com">http://testaspnet.vulnweb.com</a>	IIS, ASP.NET, Microsoft SQL Server	<a href="#">Review</a> Acunetix network scanner or <a href="#">learn more</a> on the topic.
REST API	<a href="http://rest.vulnweb.com/">http://rest.vulnweb.com/</a>	Apache, PHP, MySQL	<a href="#">Review</a> Acunetix scanner or <a href="#">learn more</a> on the topic.

La página de prueba es <http://testphp.vulnweb.com>

login page x Acunetix Web Vulnerability Scanner x +

No es seguro testphp.vulnweb.com/login.php

login page Acunetix Web Vulnerability Scanner Vulnerable Test Site...

**acunetix** acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


**Links**

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

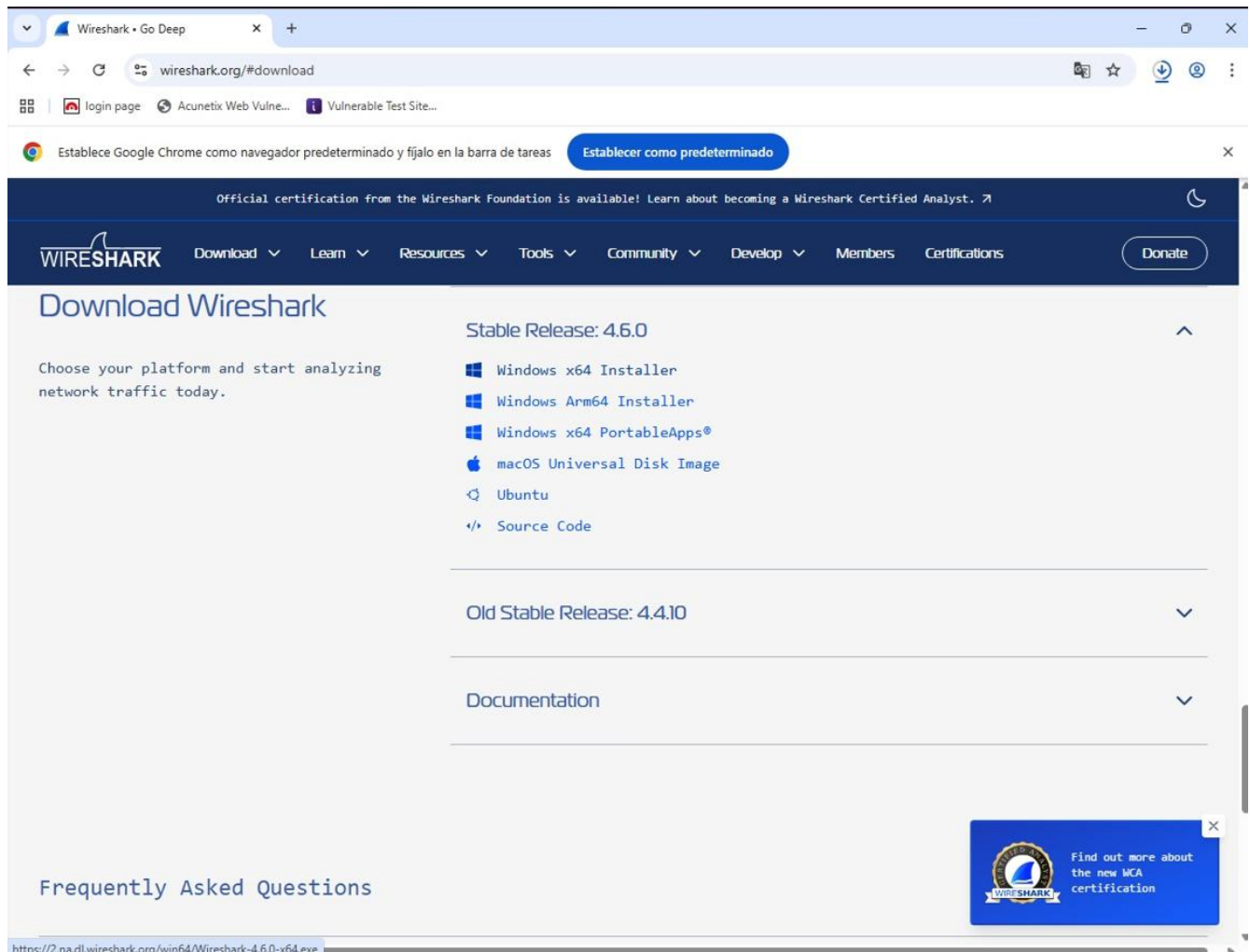
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

# Ataque al sitio

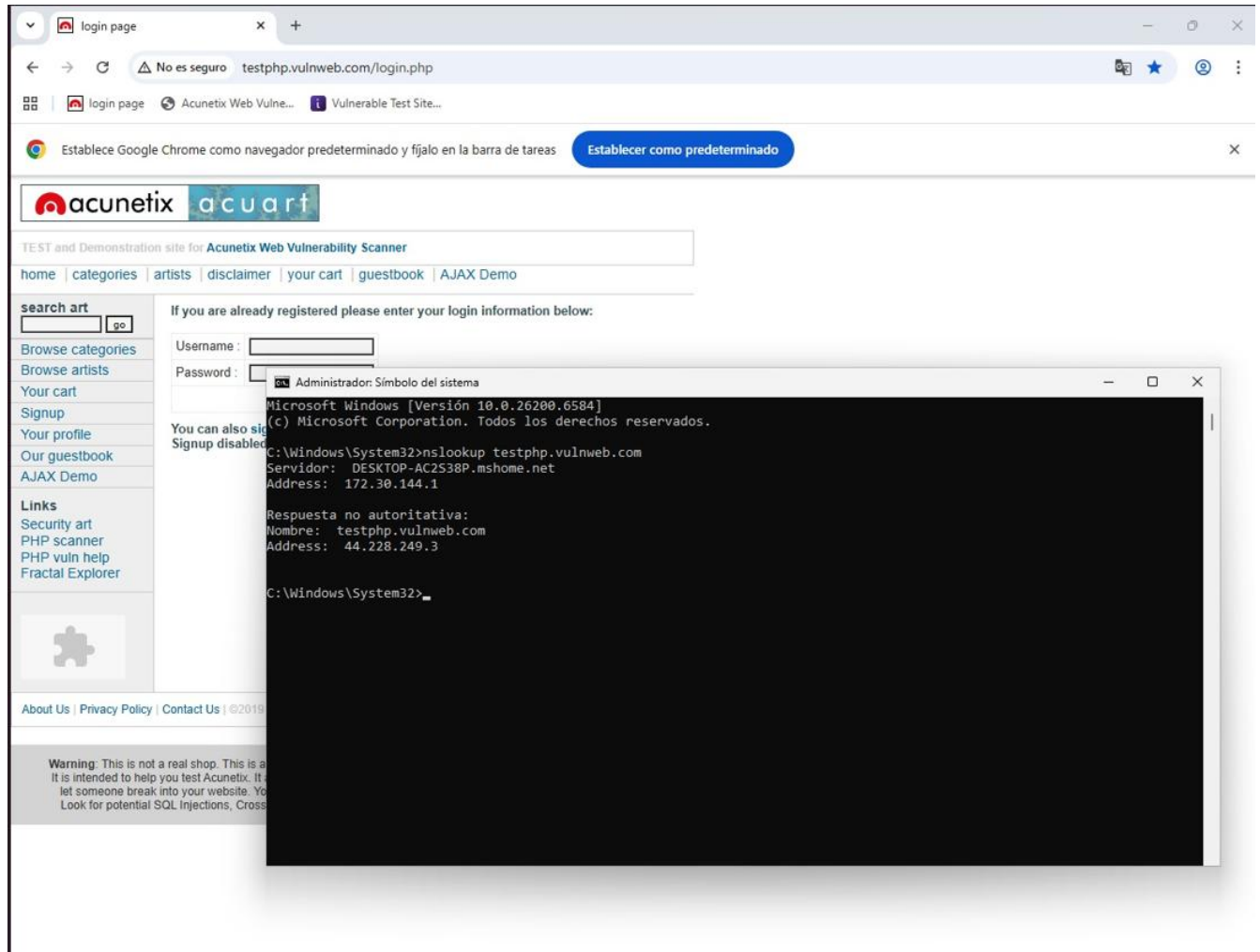
Para realizar el ataque al sitio como es solicitado, en la máquina virtual se instaló el programa Wireshark. El cual descargamos de la página <https://www.wireshark.org/> en la sección de download.



Una vez descargado lo instalamos.

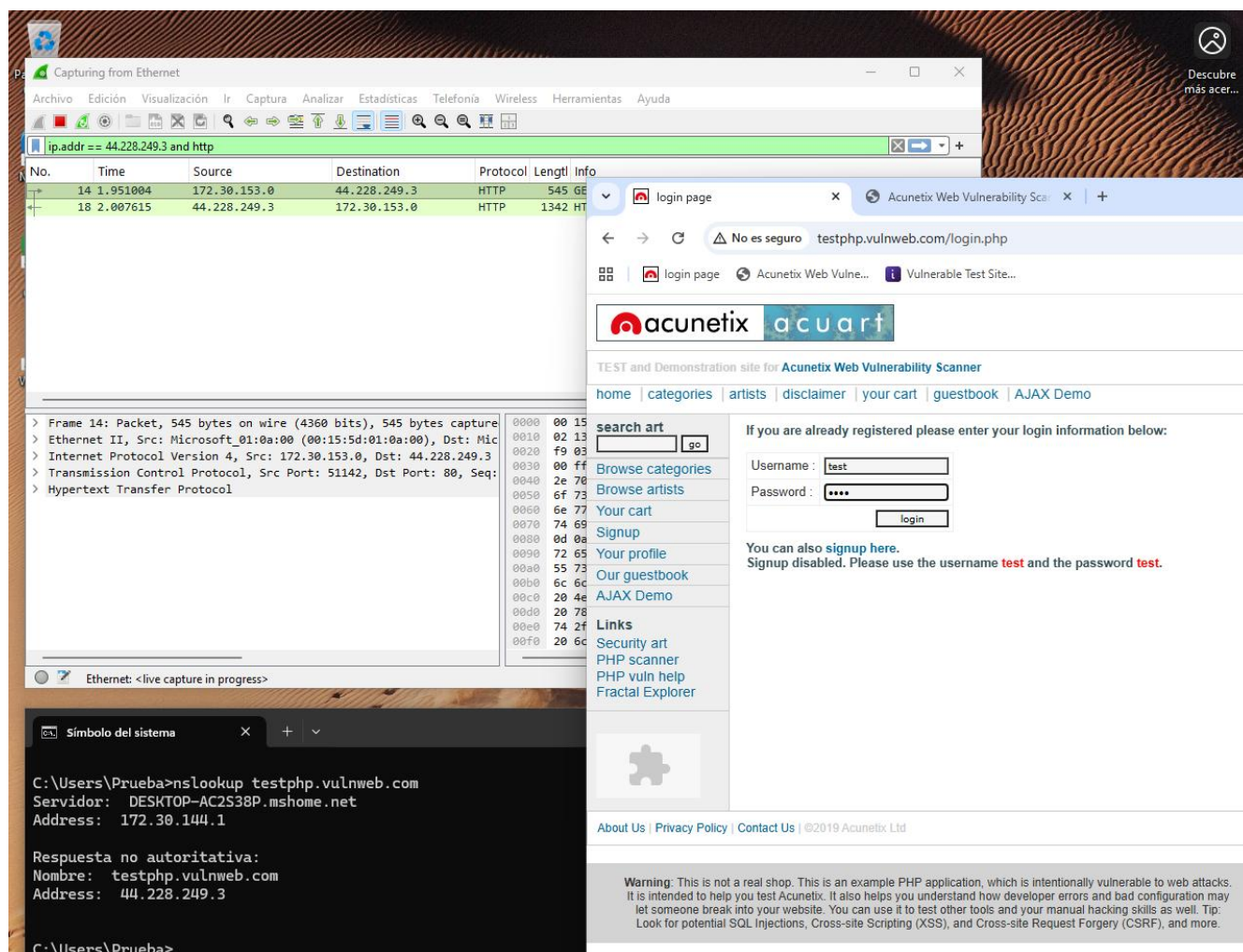


A continuación, ejecutamos en un cmd el comando nslookup para obtener la dirección ip del sitio que seleccionamos para realizar el ataque.



La cual nos da que la ip de la página es 44.228.249.3.

A continuación, abrimos el programa WireShark y como se nos explicó ponemos el filtro con la ip del sitio de la siguiente manera `ip.addr == 44.228.249.3 and http` y lo aplicamos con el icono de la flechita del lado derecho en el filtro. Activamos la captura de paquetes en el programa y ingresamos a la pagina



Los datos de la prueba en la página son los siguientes:

Usuario: test

Contraseña: test

Los ingresamos y dejamos que el programa realice la captura de datos.

En la siguiente captura se muestra cómo se realiza de manera correcta el robo de la autenticación en la página no protegida. En la captura de WireShark se ve que nos muestra la información del usuario test y el pass test.

The image displays a network traffic capture using Wireshark and a web browser window. The Wireshark interface shows a packet capture from Ethernet. The selected packet is a POST request to testphp.vulnweb.com/userinfo... with a body containing 'uname=test' and 'pass=test'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.153.0	44.228.249.3	HTTP	545	GET /log...
3	0.056892	44.228.249.3	172.30.153.0	HTTP	1342	HTTP/1.1
7	5.680529	172.30.153.0	44.228.249.3	HTTP	701	POST /us...
9	5.737923	44.228.249.3	172.30.153.0	HTTP	1509	HTTP/1.1

The browser window shows the 'user info' page for 'rehana (test)'. The form fields are filled with the following information:

- Name: rehana
- Credit card number: 5500-87600-456808
- E-Mail: rehana65@gmail.com
- Phone number: 644082537
- Address: karachi

The page also displays a warning message: 'Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.'

También se realizó un ingreso erróneo con usuario can y contraseña can el cual no puedo iniciar sesión, pero en WireShark salió también los datos mal ingresados y fueron capturados.

The image is a composite of three screenshots related to web security testing.

**Top Left (Wireshark):** A network packet capture showing an HTTP GET request from 172.30.153.0 to 44.228.249.3. The packet details pane shows the HTTP structure, including the request line and headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

**Top Right (Web Browser):** A screenshot of the Acunetix Web Vulnerability Scanner interface. The browser address bar shows the URL "testphp.vulnweb.com/login.php". The page content includes a login form with fields for "Username" and "Password", and a "login" button. There are also links for "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo".

**Bottom Left (Terminal):** A terminal window showing the command prompt "C:\Users\Prueba>nslookup testphp.vulnweb.com". The output shows the IP address "172.30.144.1". Below the command prompt, there is a response from the server: "Respuesta no autoritativa: Nombre: testphp.vulnweb.com Address: 44.228.249.3".

## Conclusión

En este ejercicio se nos mostró de manera clara la importancia de implementar de manera correcta las medidas de seguridad en las aplicaciones web. Se utilizó Wireshark para analizar el tráfico entre el cliente y el servidor, se evidencia como el no tener aplicados los controles de seguridad en el cifrado en la transmisión de datos puede exponer de manera muy fácil datos muy sensibles, como usuarios y contraseñas, poniendo en riesgo no solo a los sistemas sino a las personas que los utilizan.

En este ejercicio nos demostraron que estamos expuestos completamente, que la seguridad no es una opción, sino un requisito fundamental que debe ser encarado con esa seriedad desde las primeras etapas del desarrollo. Aprender sobre estas vulnerabilidades y cómo funcionan, nos permitirá reforzar las buenas prácticas de un buen uso de la seguridad, como unos de HTTPS, protección de cookies, la expiración de sesiones de manera adecuada y el cifrado de datos.

Además, también es un tema de maduración, el equipo debe ser lo bastante consciente de que estas brechas de seguridad son de suma importancia que sean cubiertas, pero muchas veces las personas son renuentes al cambio, lo que puede generar en una intromisión con pérdida de datos, lo que puede generar pérdidas económicas, demandas y hasta la pérdida de credibilidad por parte del cliente.

Este trabajo fue subido al siguiente enlace de GitHub

<https://github.com/CarlosNico/Auditor-a-Inform-tica>

## Referencias

Monteagudo, D. (2010, March 24). *OWASP TOP 10 (III): Pérdida de autenticación y Gestión de Sesiones*. Security Art Work. <https://www.securityartwork.es/2010/03/24/owasp-top-10-iii-perdida-de-autenticacion-y-gestion-de-sesiones/>

*Wireshark • undefined*. (n.d.). Wireshark. Retrieved October 24, 2025, from <https://www.wireshark.org/>

*A2-Pérdida autenticación y gestión sesiones :: PROYECTO SEGURIDAD INFORMÁTICA*. (n.d.). Webnode.es. Retrieved October 24, 2025, from <https://liliseguridadinformatica.webnode.es/guia-de-buenas-practicas/disenio/a2/>