

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

Auditoría Informática.

Ingeniería en Desarrollo de Software.



TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 23/10/2025.

Introducción.	3
Descripción.	3
Justificación.	4
Desarrollo.	4
Descripción del sitio web.	5
Ataque al sitio.	6
Conclusion.	9
Referencias.	10

Introducción.

En esta primera actividad de la materia Auditoría Informática, nos enfocamos en cómo la seguridad de las aplicaciones web es fundamental, y muchas empresas de software requieren pruebas de penetración para identificar y mitigar vulnerabilidades antes de un ataque real. En este contexto, se ha solicitado un análisis de seguridad en páginas web que carecen de mecanismos de cifrado y protección, un escenario común que expone datos sensibles. Esta primera fase se centrará en la vulnerabilidad de la pérdida de autenticación y gestión de sesiones, un fallo crítico que puede permitir a un atacante suplantar la identidad de un usuario. Para ello, se utilizará la herramienta de análisis de protocolos Wireshark.

El objetivo principal de esta prueba es interceptar el tráfico de red durante un intento de inicio de sesión para capturar y revelar las credenciales (nombre de usuario y contraseña) transmitidas en texto plano. La actividad práctica consistirá en la selección de un proyecto web propio en el caso de tener alguno, en el caso de no tenerlo utilizar algún sitio ya existente en internet, que debe incluir las funciones de registro e inicio de sesión y estar conectado a una base de datos, simulando un entorno real y vulnerable para la demostración.

Descripción.

Esta primera actividad de Auditoría Informática aborda un pilar crucial de la ciberseguridad: la protección de las aplicaciones web. Las empresas de software solicitan rutinariamente pruebas de penetración para adelantarse a los atacantes, y nuestro enfoque inicial es en sitios que carecen de cifrado adecuado. Este es un escenario de alto riesgo donde los datos sensibles se exponen fácilmente.

Nos centraremos en la vulnerabilidad de Pérdida de Autenticación y Gestión de Sesiones. Este fallo permite a un atacante, a través de la suplantación, tomar el control de la cuenta de un usuario. Para demostrar este riesgo, utilizaremos Wireshark, una poderosa herramienta de análisis de protocolos, para interceptar el tráfico de red.

El objetivo directo es iniciar sesión en un sitio web vulnerable y, mediante Wireshark, capturar las credenciales (usuario y contraseña) transmitidas en texto plano. Para la práctica, utilizaremos un proyecto web propio o uno existente en internet que cumpla con los requisitos de tener funciones de registro, inicio de sesión y conexión a una base de datos, simulando un entorno de producción para esta prueba crítica.

Justificación.

La realización de esta actividad se justifica plenamente por la necesidad imperante de comprender los riesgos de seguridad en el desarrollo web moderno. La Pérdida de Autenticación y Gestión de Sesiones es una vulnerabilidad persistente y catalogada como crítica por organizaciones como OWASP. Simular su explotación no es solo un ejercicio académico, sino una demostración práctica de las consecuencias de la falta de cifrado.

Utilizar Wireshark para capturar credenciales en texto plano subraya de manera contundente cómo la omisión de un simple certificado SSL/TLS convierte un sitio web en un riesgo de alto impacto para la privacidad del usuario. Esta prueba nos permite validar empíricamente la importancia de implementar protocolos de seguridad robustos desde las primeras fases del desarrollo.

En el contexto de la Auditoría Informática, esta práctica establece una base fundamental: la capacidad de identificar, replicar y documentar fallos de seguridad. Este conocimiento es esencial para cualquier auditor que aspire a proteger sistemas y recomendar mitigaciones efectivas que eviten la suplantación de identidad y el robo de datos.

Desarrollo.

En esta parte de la actividad nos enfocaremos a realizar la actividad de la materia que no indica el ataque a un sitio no seguro publicado en internet obteniendo el usuario de autenticación y su contraseña mediante el uso de la herramienta de Wireshark. En esta actividad utilizaremos un sitio web de test que


ya es un sitio existente en internet en el cual realizaremos la actividad de la materia.

Link: [GitHub](#).

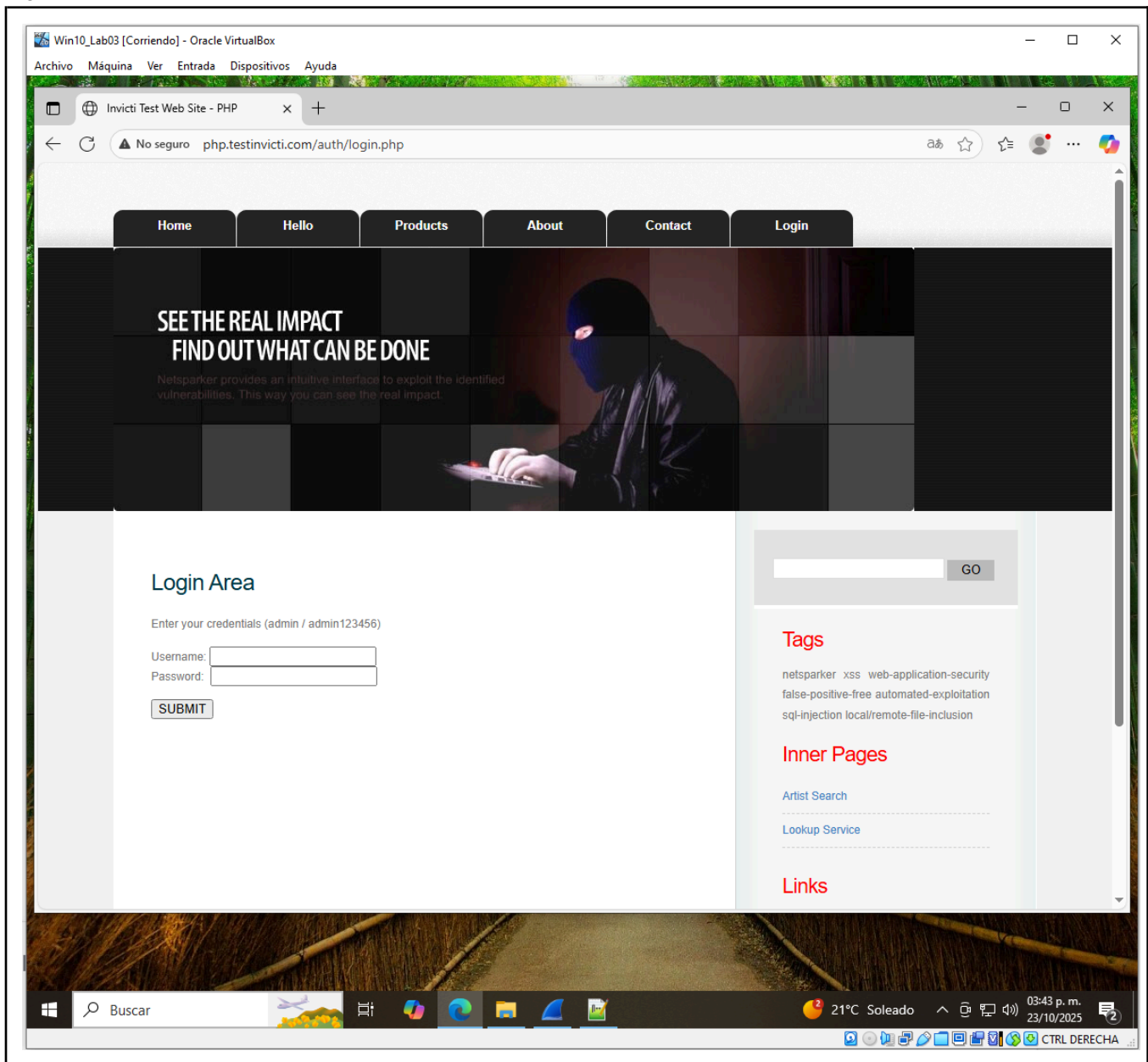
Descripción del sitio web.

Sitio web vulnerable

En este punto de la actividad, se utilizó una sitio vulnerable de un listado que mostro al ingresar a este sitio <http://testinvicti.com> del listado el sitio escogido contaba con las con lo siguiente estaba instalado en un equipo windows, con las herramientas web de apache/php y con una base de MySQL por lo cual fue seleccionado realizar el ataque con la herramienta de WireShark.

 Vulnerable Test Websites		
Name	URL	Technologies
ASP.Net - Testinvicti	aspnet.testinvicti.com	Windows, IIS, ASP.NET, MsSQL
PHP - Testinvicti	php.testinvicti.com	Windows, Apache, PHP, MySQL
SPA - Angular - Testinvicti	angular.testinvicti.com	Ubuntu, Apache, PHP, Angular 5, MySQL
API - REST - Testinvicti	rest.testinvicti.com	Ubuntu 18, Apache, PHP 7.1, MySQL
GraphQL - Testinvicti	graphql.testinvicti.com	Ubuntu 22.04, NodeJS, GraphQL
Python - Testinvicti	python.testinvicti.com	Ubuntu 22.04, Flask, CouchDB, Nginx
API - Vulnerable API	vulnapi.testinvicti.com	Ubuntu, NodeJS, Swagger, SQLite

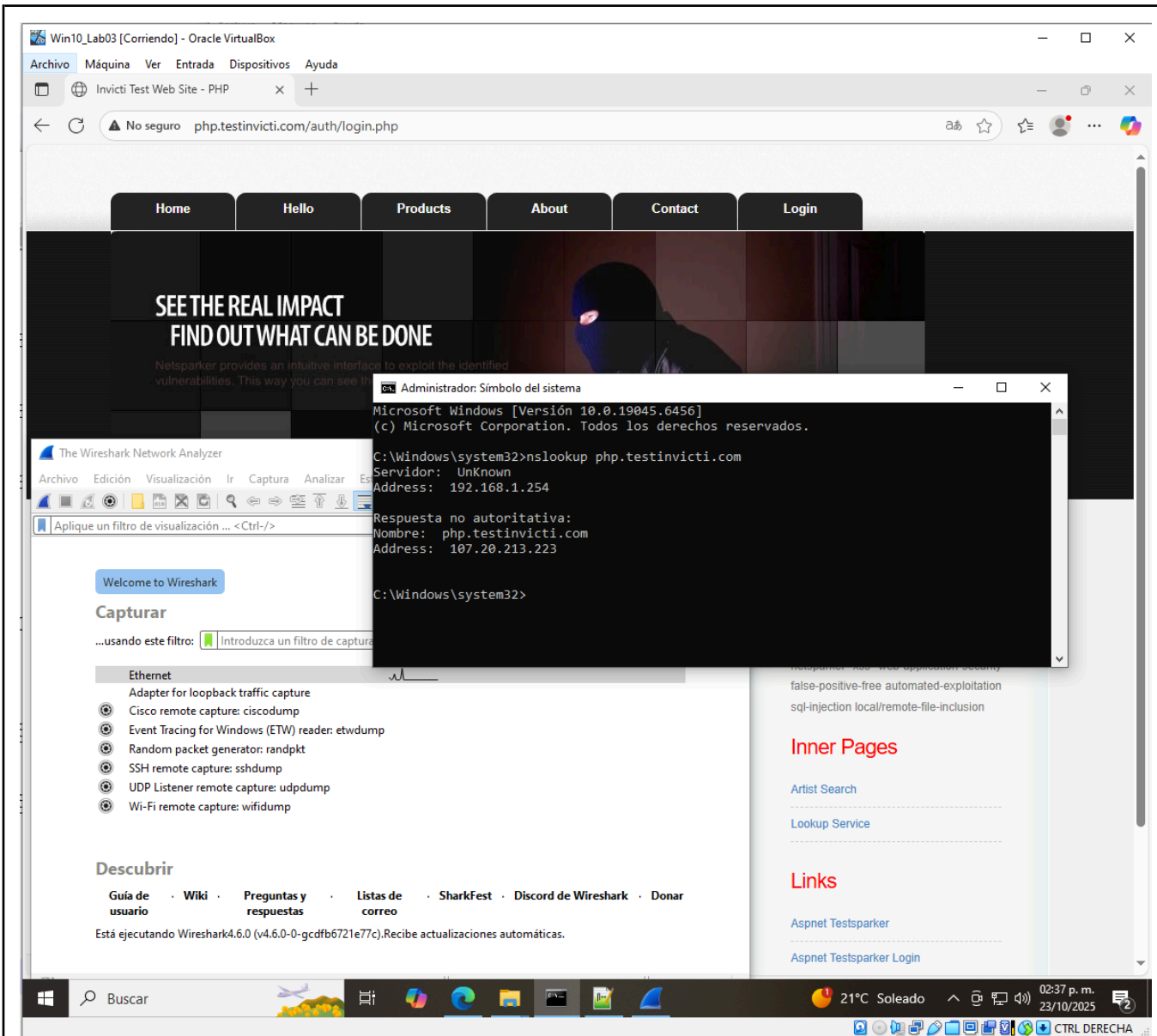
Este es un sitio de prueba y demostración de invicti que se utiliza para realizar escaneos de seguridad de aplicaciones web de última generación. Como sitio de pruebas los seleccione para la actividad anexando la imagen de evidencia del sitio <http://php.testinvicti.com/auth/login.php> a utilizar.



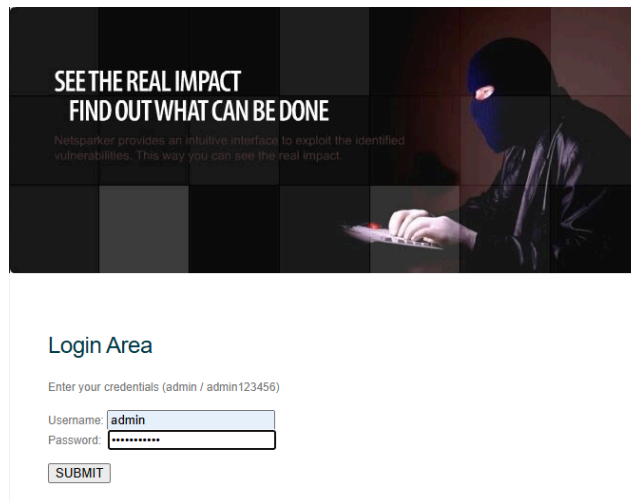
Ataque al sitio.

Ataque Web:

En este punto para realizar el ataque del sitio utilizaremos el comando nslookup para obtener la dirección ip del sitio al cual atacaremos, con la finalidad del robo de usuario y password, a continuación anexamos la imagen del uso de la línea de comando y se anexa como evidencia obteniendo la dirección p 107.20.213.223 del dominio: php.testinvicti.com.



Aquí en este punto ya con la instalación de la herramienta WireShark a utilizar y el filtro con la dirección ip del dominio y el del sitio no seguro (ip.addr == 107.20.213.223 and http) se aplica el filtro en la aplicación y se inicia la captura de paquetes, se ingresa al sitio al cual se va atacar.



**SEE THE REAL IMPACT
FIND OUT WHAT CAN BE DONE**

NetSparker provides an intuitive interface to exploit the identified vulnerabilities. This way you can see the real impact.

Login Area

Enter your credentials (admin / admin123456)

Username:

Password:

Se ingresa la cuenta de usuario y la contraseña, se valida que se haya capturado el ataque de robo de cuenta de autenticación y se detiene la captura. Anexo evidencia de la captura del robo de cuenta y credencial.

Win10_Lab03 [Corriendo] - Oracle VirtualBox

Actividad_1.pcapng

ip.addr == 107.20.213.223 and http

No.	Time	Source	Destination	Protocol	Length	Info
63	2.294901	10.0.2.15	107.20.213.223	HTTP	614	GET /auth/login.php HTTP/1.1
80	2.884383	107.20.213.223	10.0.2.15	HTTP	568	HTTP/1.1 200 OK (text/html)
105	14.430253	10.0.2.15	107.20.213.223	HTTP	846	POST /auth/control.php HTTP/1.1 (application/x-www-form-urlencoded)
112	14.544573	107.20.213.223	10.0.2.15	HTTP	436	HTTP/1.1 302 Found
113	14.551264	10.0.2.15	107.20.213.223	HTTP	692	GET /auth/login.php HTTP/1.1
121	14.756756	107.20.213.223	10.0.2.15	HTTP	570	HTTP/1.1 200 OK (text/html)

Frame 105: Packet, 846 bytes on wire (6768 bits), 846 bytes captured on interface 0

Ethernet II, Src: PCSSystemtec_c3:1f:a2 (08:00:27:c3:1f:a2), Dst: 10.0.2.15

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 107.20.213.223

Transmission Control Protocol, Src Port: 49774, Dst Port: 80, Seq: 1000000000, Win: 65535, Len: 846

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "username" = "admin"
 - Key: username
 - Value: admin
- Form item: "password" = "admin123456"
 - Key: password
 - Value: admin123456
- Form item: "token" = "450"
 - Key: token
 - Value: 450

Paquetes: 251 · Displayed: 6 (2.4%) · Perdido: 0 (0.0%) · Perfil: Default

Conclusion.

En conclusión: La gestión efectiva de la autenticación y las sesiones es fundamental, tanto en el campo laboral como en la vida cotidiana. La "Pérdida de autenticación y gestión de sesiones" (un riesgo crítico de ciberseguridad) significa que un atacante puede suplantar la identidad de un usuario, obteniendo acceso no autorizado a información confidencial, cuentas bancarias, o sistemas empresariales. En el ámbito laboral, esta vulnerabilidad pone en riesgo datos críticos de la empresa (propiedad intelectual, información de clientes) y puede causar graves daños financieros y de reputación, además de incumplimiento normativo.

En la vida cotidiana, una gestión de sesiones débil puede llevar al robo de identidad, fraude bancario o acceso a cuentas personales (correo, redes sociales). Por ello, implementar prácticas sólidas como la autenticación multifactor (MFA), el uso de contraseñas fuertes y la invalidación correcta de sesiones al cerrar, es esencial para proteger nuestros activos digitales y mantener la confianza en el entorno digital. Es una responsabilidad compartida para un entorno seguro.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved January 9, 2025, from <https://gemini.google.com/>

Neubert, J. (n.d.-a). *Vulnerable test sites to test your XSS skills: Hands-on AppSec.*

Invicti.com. Retrieved October 23, 2025, from <https://www.invicti.com/blog/web-security/test-xss-skills-vulnerable-sites/>

Vulnerable web apps - testinvicti. (n.d.). Testinvicti.com. Retrieved October 23, 2025, from <http://testinvicti.com>

Invicti Test Web Site - PHP. (n.d.). Testinvicti.com. Retrieved October 23, 2025, from <http://php.testinvicti.com/auth/login.php>