

Actividad 1 - Pérdida de Autenticación y Gestión de Sesiones Auditoría Informática Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero.

Alumno: Carlos Alberto Fuentes Mendoza

Fecha: 28-septiembre-2023

Índice

ntroducción
escripción4
ıstificación5
Pescripción del sitio web
taque al sitio
onclusión
eferencias

Introducción

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones y APIS que pueden ser confiables. Su proyecto de documentación más conocido es el TOP TEN, en el cual se listan las 10 vulnerabilidades (security risks) más habituales y cómo prevenirlas.



En su lista de TOP 10, se encuentra en segundo lugar A2-Perdida de autentificación y gestión de sesiones. En esta vulnerabilidad, las fallas generalmente conducen a la divulgación de información no autorizada, la modificación de todos los datos, la ejecución de una función de negocio fuera de los límites del usuario, suplantación de identidad, hackeo y pérdida de toda nuestra información, pérdida del control sobre documentos en los que hemos invertido gran parte de nuestro tiempo y esfuerzo, terceras personas pueden utilizar nuestra información con fines comerciales, nuestra privacidad deja de tener sentido, perdemos la autoridad sobre nuestra información confidencial, pérdida de la confianza de nuestros clientes, hasta el cierre del negocio.

Una de las recomendaciones para contrarrestar este riego, es el certificado SSL. Este es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web para mantener la privacidad de las interacciones en línea, esto garantiza a los usuarios que el sitio web es auténtico, que es seguro compartir información privada mediante él, evita que los atacantes creen una versión falsa del sitio y esto genera confianza a los usuarios.

Descripción

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

Para esta primera etapa, se debe de realizar una prueba de la vulnerabilidad de la perdida de autentificación y gestión de sesiones utilizando la aplicación WireShark, el objetivo de esta prueba es obtener las credenciales de autentificación que se ingresaron y que estas se puedan mostrar.

Para realizar esta actividad, se deberá elegir un proyecto web que se haya realizado con anterioridad, en caso de no contar con uno, se deberá elegir un sitio web que contenga las siguientes características:

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

En esta actividad vamos a aprender la manera de explotar una vulnerabilidad de un sitio web, en la cual, con la ayuda de la aplicación WirwShark, podremos observar la perdida de autentificación y gestión de sesiones, obteniendo las credenciales del Login, debido a la falta de certificación SSL.

.

Justificación

Los sitios web necesitan certificados SSL para mantener la seguridad de los datos del usuario, verificar la propiedad del sitio web, evitar que los atacantes creen una versión falsa del sitio y para transmitir confianza a los usuarios. Si un sitio web solicita a los usuarios que inicien sesión, ingresen datos personales, como sus números de tarjeta de crédito, o vean información confidencial, como los beneficios de salud o información financiera, entonces es esencial mantener la confidencialidad de los datos. Los certificados SSL ayudan a mantener la privacidad de las interacciones en línea y garantizan a los usuarios que el sitio web es auténtico y que es seguro compartir información privada mediante él.

Más relevante para las empresas es el hecho de que se necesita un certificado SSL para una dirección web HTTPS. El protocolo HTTPS es la versión segura del protocolo HTTP, lo que significa que los sitios web HTTPS tienen su tráfico cifrado mediante certificados SSL. La mayoría de los navegadores clasifican los sitios HTTP, aquellos sin certificados SSL, como "no seguros". Para los usuarios, esta es una clara señal de que el sitio puede no ser confiable, lo que incentiva a las empresas que no lo han hecho a migrar al protocolo HTTPS.

Un certificado SSL ayuda a proteger información como la siguiente:

- Credenciales de inicio de sesión
- Transacciones con tarjeta de crédito o información de la cuenta bancaria
- Información de identificación personal, como nombre completo, dirección, fecha de nacimiento o número de teléfono
- Documentos y contratos legales
- Historia clínica
- Información de propiedad

Descripción del sitio web

Las Páginas Verdes es el directorio impreso y en línea más completo de productos y servicios sustentables en México que genera un movimiento de consumo responsable.

Las Páginas Verdes, con siete años promoviendo el crecimiento de la economía sustentable en México, reúne más de 5,100 productos y servicios sustentables.

A continuación, se muestra la captura de pantalla del sitio web a atacar, el cual tiene la siguiente url:

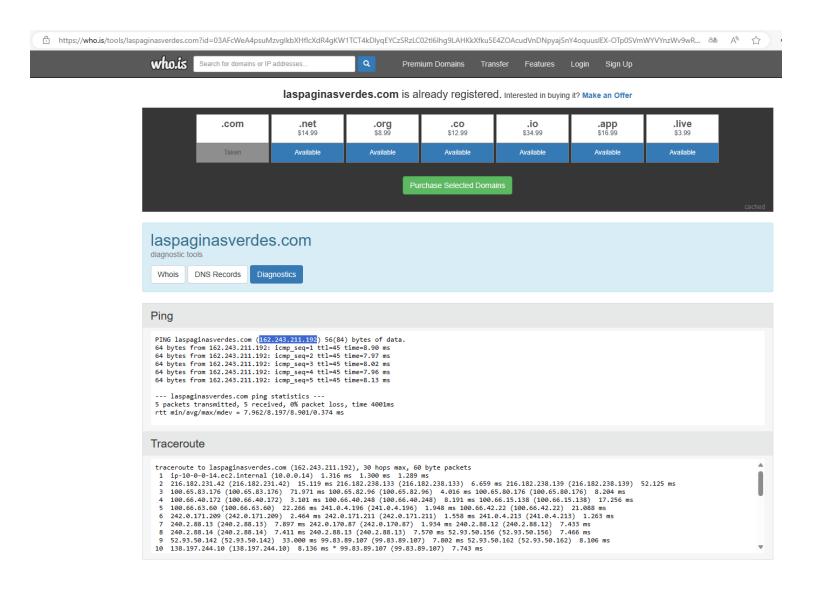
http://laspaginasverdes.com



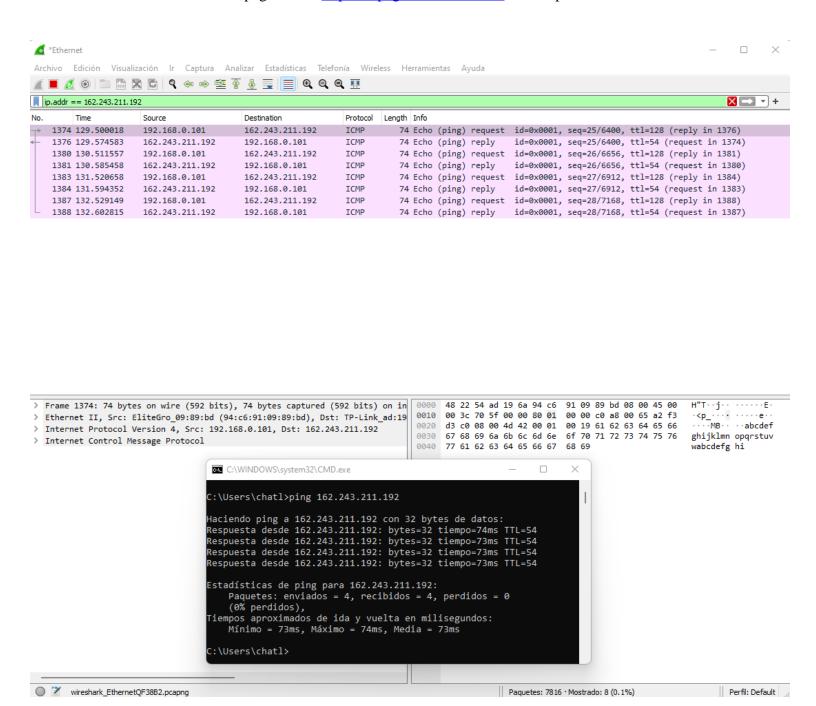
Ataques del sitio

Iniciamos obteniendo la ip de la página web que deseamos atacar con url http://laspaginasverdes.com/, para esto nos dirigimos al sitio web https://who.is y capturamos la url del sitio web.

Como se puede observar en la siguiente captura, el sitio web nos devuelve la información de dicha página, la cual la que más nos interesa es la ip 162.243.211.192.

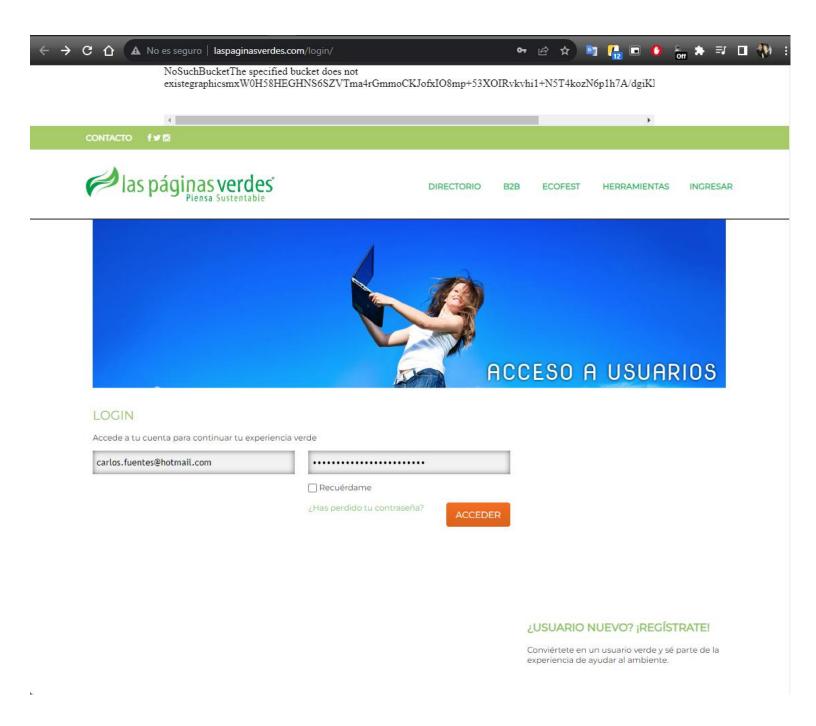


En la siguiente pantalla se observa la captura de paquetes de la aplicación wireshark al hacer ping desde la terminal de Windows en la página web http://laspaginasverdes.com/ con la ip 192.243.211.192.

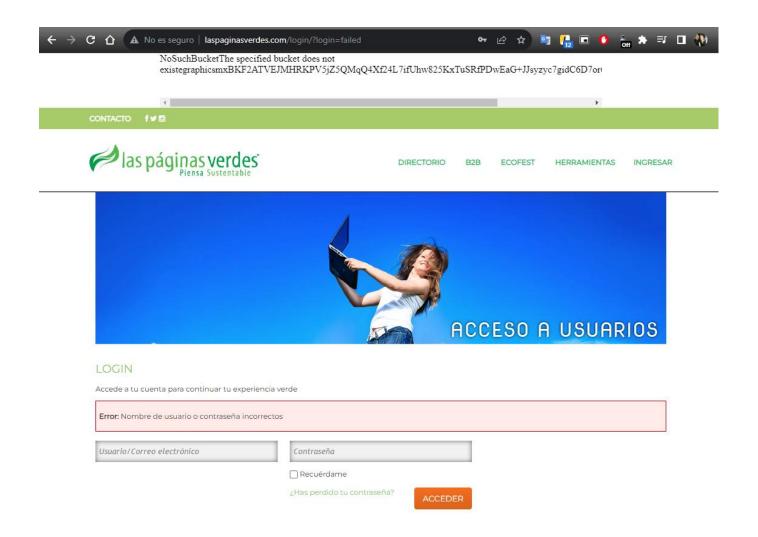


En la siguiente pantalla se observa la página del Login en la cual colocamos las siguientes credenciales:

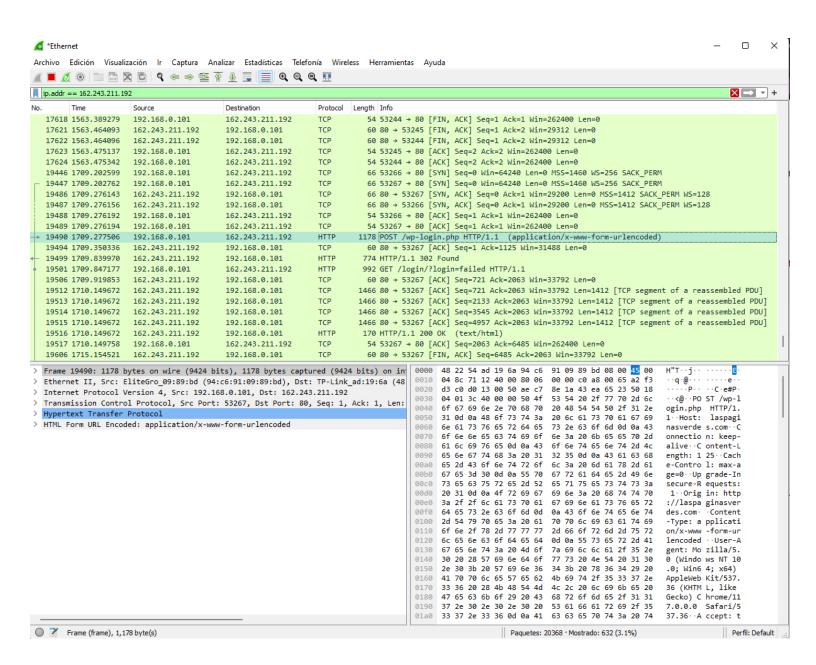
<u>Carlos.fuentes@hotmail.com</u> y en password= jessica hernandez romero



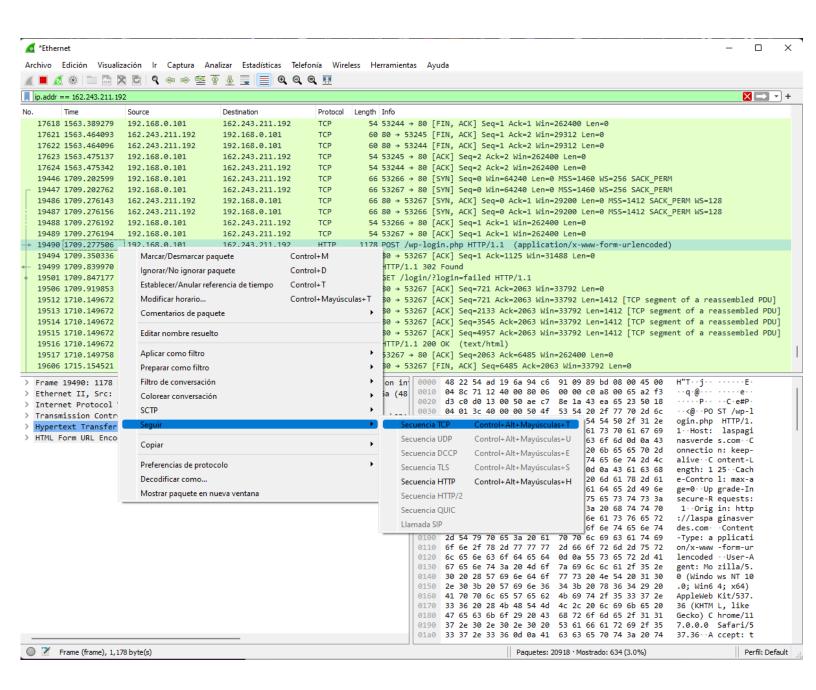
En la siguiente captura se puede observar que las credenciales son incorrectas debito a que no me encuentro registrado en este sitio web.



En la siguiente captura se observan los paquetes capturados por la aplicación, en los cuales encontramos el protocolo HTTP que es el que nos interesa.

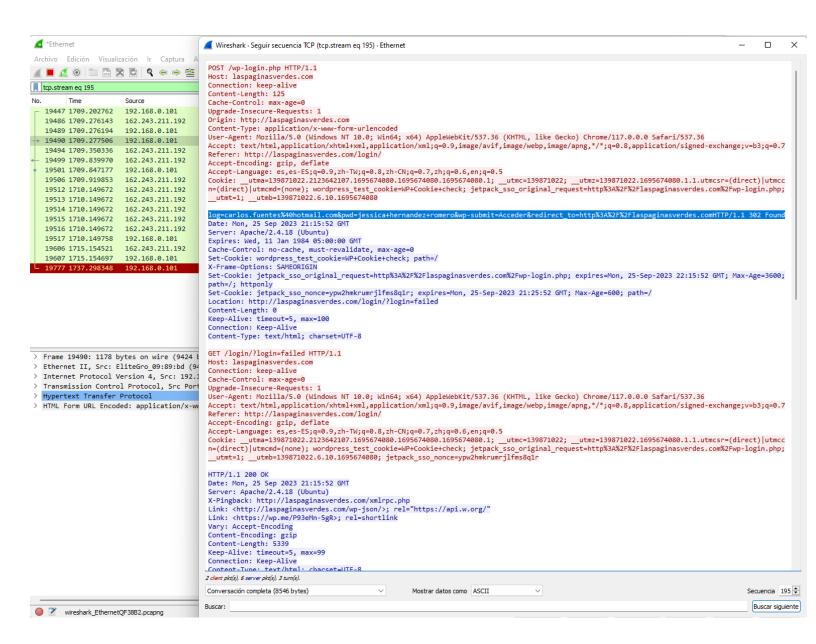


Después de haber localizado HTTP – POST que nos interesa, damos clic en la opción seguir y en secuencia TCP.



Por último, en la siguiente captura se puede observar que en el seguimiento a la secuencia TCP, nos proporciona las credenciales con las cuales intentamos realizar el logeo.

Log = carlos.fuentes@hotmail.com y en pwd: jessica+hernandez+romero



Conclusión

En esta actividad aprendí muchas cosas importantes, entre las cuales destacan que entendí que cuando las

claves o información sensible no son protegidas adecuadamente, el atacante aprovecha estas

vulnerabilidades que generalmente son aprovechadas en: el cierre de sesión, en la gestión de las contraseñas,

en el tiempo de desconexión y en la función de recordar contraseña, para robar la información sensible,

incluyendo un script en una página web que se ejecuta cuando el usuario la utiliza.

También conocí y aprendí que el certificado SSL mantiene seguras las conexiones a Internet y evita que los

delincuentes lean o modifiquen la información transferida entre dos sistemas. Ahora sé que cuando se ve

un ícono de candado junto a la URL en la barra de direcciones, significa que hay un certificado SSL que

protege el sitio web que se está visitando, francamente, solo sabía que era una página segura, ahora sé, él

porque es segura.

También conocí OWASP y su proyecto de documentación más conocido TOP TEN, en el cual se listan las

10 vulnerabilidades más habituales y lo principal, cómo prevenirlas.

También aprendí como aprovechar una vulnerabilidad por falta de certificado SSL con la ayuda del software

wireshark, en el cual obteniendo su ip del sitio web vulnerable y dando seguimiento a los paquetes TCP,

pude obtener las credenciales que se capturan para realizar login en esta página.

A continuación, se comparte el link de acceso a la actividad en GitHub

https://github.com/charlyfu/Auditoria_informatica

14

Referencias

A07 Fallas de Identificación y Autenticación - OWASP Top 10:2021. (s. f.)	.).
---	-----

https://owasp.org/Top10/es/A07_2021-Identification_and_Authentication_Failures/

Rivera, D. (2021, 29 noviembre). Riesgo A2 en OWASP - Pérdida de autenticación y gestión de sesiones. https://blog.pleets.org/article/es/owasp-a2-broken-authentication

Kaspersky. (2023, 29 agosto). Qué es un certificado SSL: definición y explicación. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

A2-Pérdida autenticación y gestión sesiones :: PROYECTO SEGURIDAD INFORMÁTICA. (s. f.). https://liliseguridadinformatica.webnode.es/guia-de-buenas-practicas/diseno/a2/

Da Silva, D. (2023, 18 septiembre). ¿Qué es SSL certificado y por qué tener en tu sitio web? Zendesk MX. https://www.zendesk.com.mx/blog/que-es-ssl-certificado/