Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad [#1] - [Perdida de autenticación y gestión de sesiones]

[Auditoria informática]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Gabriel German Verdugo Solís

Fecha: 07 de febrero del 2024

INDICE

INTRODUCCION

La pérdida de datos puede suponer un grave problema para las empresas y organizaciones, también para los usuarios particulares, aunque son las primeras las que pueden sufrir pérdidas económicas como daños a su reputación como consecuencia de una pérdida de datos. Una pérdida de datos o pérdida de información se produce, por lo tanto, cuando los datos ya no son accesibles o inteligibles tanto por los humanos como por las máquinas o cuando su eliminación es definitiva, es decir, son irrecuperables. En ese sentido, una pérdida de datos se diferencia en parte de lo que es una fuga de datos, ya que la primera suele producirse, habitualmente, de manera accidental o no intencionada, aunque hay excepciones y generalmente los datos perdidos no son vistos por terceros no autorizados, mientras que la segunda suele implicar intencionalidad para poder acceder a información confidencial para su filtración.

DESCRIPCION

En esta actividad se pretende aprender como realizar una prueba de vulnerabilidad de la perdida de autentificación 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. También se pretende a prender a utilizar el programa wireshark ya que wireshark es un analizador de red que le permite ver lo que sucede en su red. Le permite diseccionar sus paquetes de red a un nivel microscópico, brindándole información detallada sobre paquetes individuales.

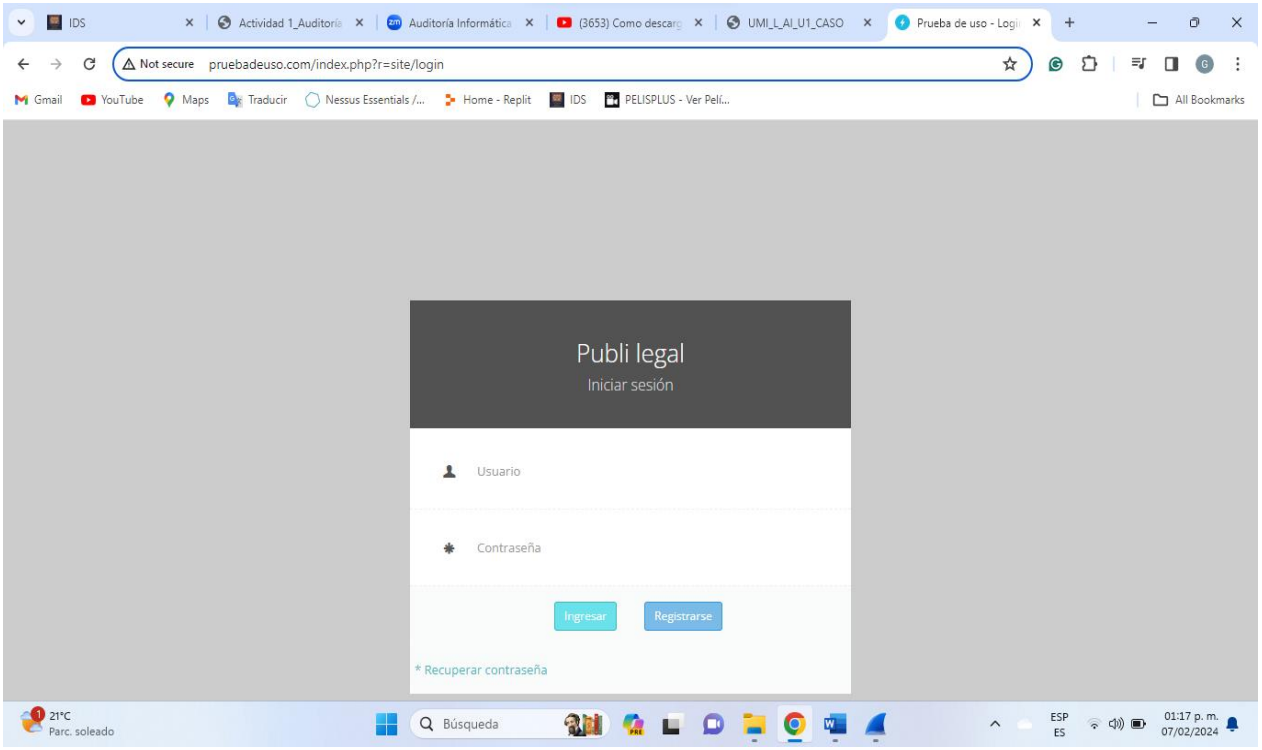
JUSTIFICACION

Es importante realizar este tipo de pruebas para saber el grado de vulnerabilidad que tenemos en nuestro sistema y así poder actuar de manera inmediata y poder proteger nuestros datos. Los ataques en los sistemas de autenticación se consideran como el segundo procedimiento más usado para vulnerar sistemas. La prevalencia de este tipo de ataque está muy extendida debido al diseño e implementación de la mayoría de los controles de identidad y acceso. La administración de sesiones es la base de los controles de autenticación y está presente en todas las aplicaciones. Los atacantes pueden detectar este tipo de vulnerabilidad utilizando medios manuales y explotarlos utilizando herramientas automatizadas con listas de contraseñas y ataques de diccionario. La mayoría de los ataques de autenticación se producen debido al uso continuo de contraseñas como único factor. Las políticas de rotación y los requisitos de complejidad en las contraseñas que no han sido bien diseñados son causantes de este tipo de vulnerabilidad.

DESCRIPCION DEL SITIO WEB

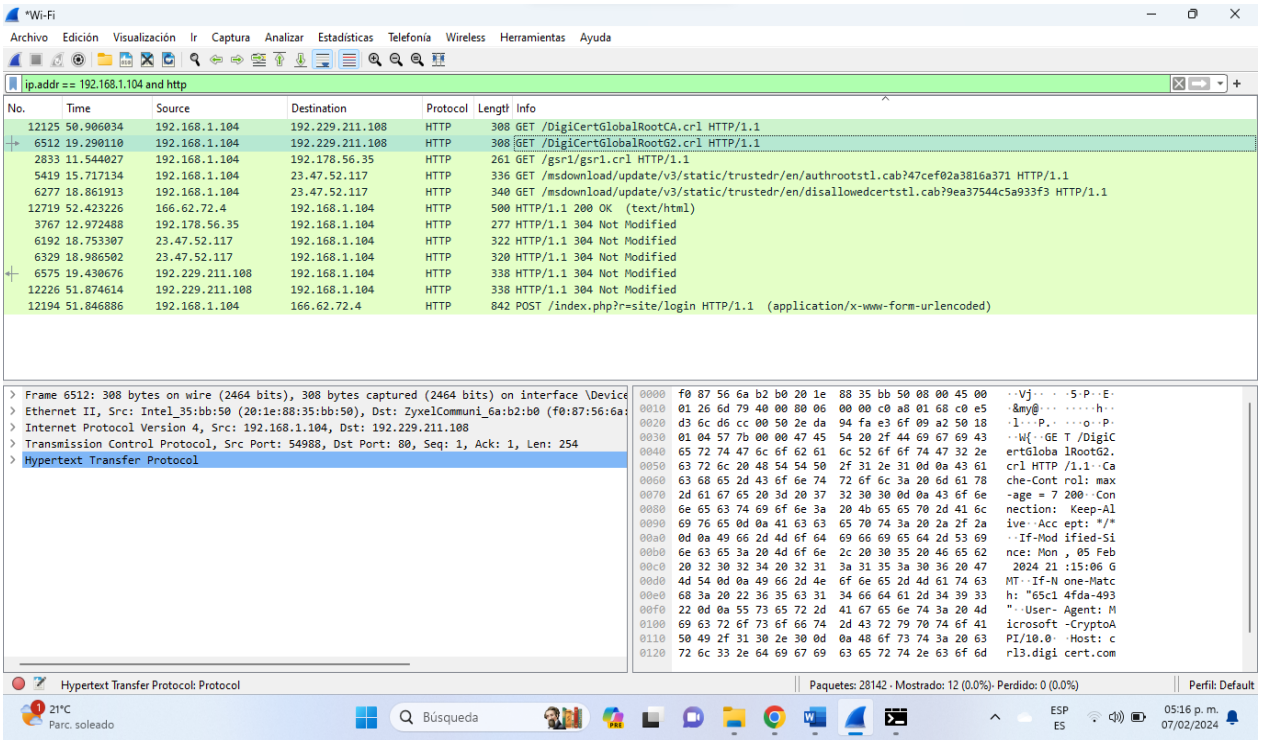
En esta actividad se utilizará una página web no segura para poder realizar la prueba de vulnerabilidad.

En este screenshot se muestra la pagina a utilizar

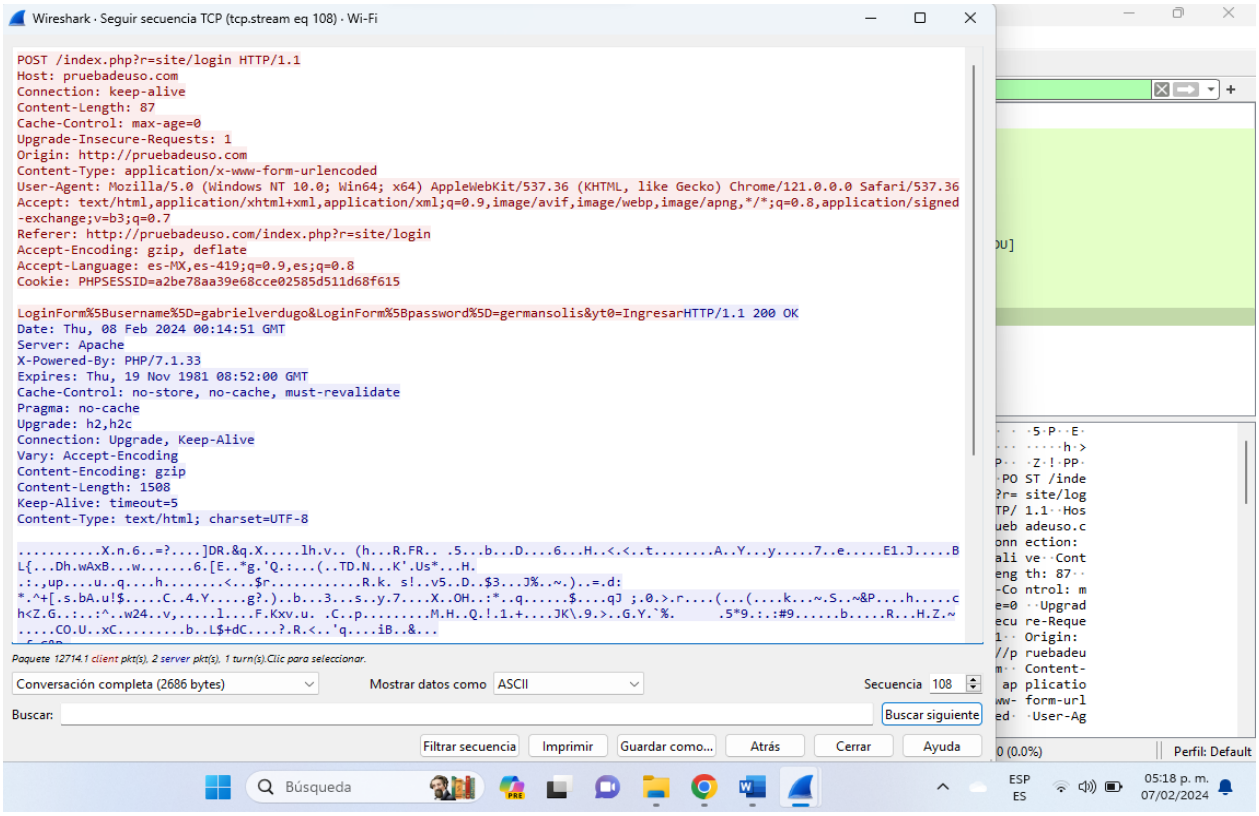


ATAQUE AL SITIO WEB

En esta imagen se muestra el funcionamiento de la prueba con wireshark



En esta imagen se muestra ya la contraseña y el usuario utilisado para querer ingresar ala pagina web donde se intento poner como usuario gabrielverdugo y en password germansolis



CONCLUSION

En conclusión, en esta actividad se aprende a interactuar con la herramienta wireshark que es una potente herramienta para monitorizar el tráfico de red y se puede utilizar para solucionar problemas. En la actualidad diferentes tipos de organizaciones utilizan Tecnologías de la Información y están es puetas a amenazas en constante evolución los programas de gestión de vulnerabilidades ahora son un requisito, ya no solo una opción, para las empresas que quieren cumplir con los marcos de gestión de riesgos. La gestión de vulnerabilidades debería ser la base de cualquier programa de Seguridad, ya que informa de todo lo que hay en una red. Con estos datos, el personal de Seguridad sabrá qué, cuándo y cómo protegerlo.

Las amenazas cibernéticas pueden interrumpir operaciones, generar multas y demandas, pérdidas de activos y negocios, causando impactos financieros y de reputación tan considerables que llegarían a afectar, incluso a la organización más estructurada para eso debemos de contar con una ciberseguridad que es implementar tecnologías y controles cibernéticos enfocados en las personas, controles de administración a los procesos, la infraestructura y las tecnologías, con el fin de reducir y controlar el riesgo de un ataque cibernético.

REFERENCIAS BIBLIOGRAFICAS

Ramírez, H. (2023a, abril 5). *Pérdida de datos ¿qué es y cómo prevenirla?* Grupo Atico34. https://protecciondatos-lopd.com/empresas/perdida-datos/

Salmerón, A., & Salmerón, A. (2023, 9 septiembre). *¿Qué es Wireshark y para qué?* Informática y Tecnología Digital. https://informatecdigital.com/redes/que-es-wireshark-y-para-que/

Toledo, R. (2023, 24 mayo). ¿Cómo funcionan los datos de autenticación y por qué son importantes? *cibernos grupo*. https://www.grupocibernos.com/blog/como-funcionan-los-datos-de-autenticacion-y-por-que-son-tan-importantes

A07 Fallas de identificación y autenticación - OWASP Top 10:2021. (s. f.). https://owasp.org/Top10/es/A07_2021-Identification_and_Authentication_Failures/