Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 2 | Deserialización

Insegura

Auditoría Informática

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Christian Ivan Ibarra Corrales

FECHA: 19 de junio de 2025

Introducción

En el contexto de la ciberseguridad, la deserialización insegura representa una grave amenaza para la integridad y confidencialidad de los sistemas web. Este tipo de vulnerabilidad ocurre cuando una aplicación acepta objetos serializados sin validación adecuada, permitiendo a un atacante modificar esos objetos para ejecutar código malicioso o escalar privilegios. En el caso de esta práctica, se simula un escenario real donde, a través de la manipulación de cookies, es posible pasar de un usuario estándar a un administrador. Esta situación afecta gravemente a los usuarios de internet, ya que su información personal, cuentas o sistemas pueden ser comprometidos sin que ellos lo adviertan. La actividad demuestra cómo fallas en la programación segura pueden abrir puertas a intrusiones no autorizadas. Mediante el uso de herramientas como Burp Suite, se evidencia la necesidad de implementar medidas de validación, cifrado y control de sesiones más robustas para proteger a los usuarios. Con este tipo de prácticas, se fomenta la conciencia sobre la importancia de aplicar seguridad desde el diseño.

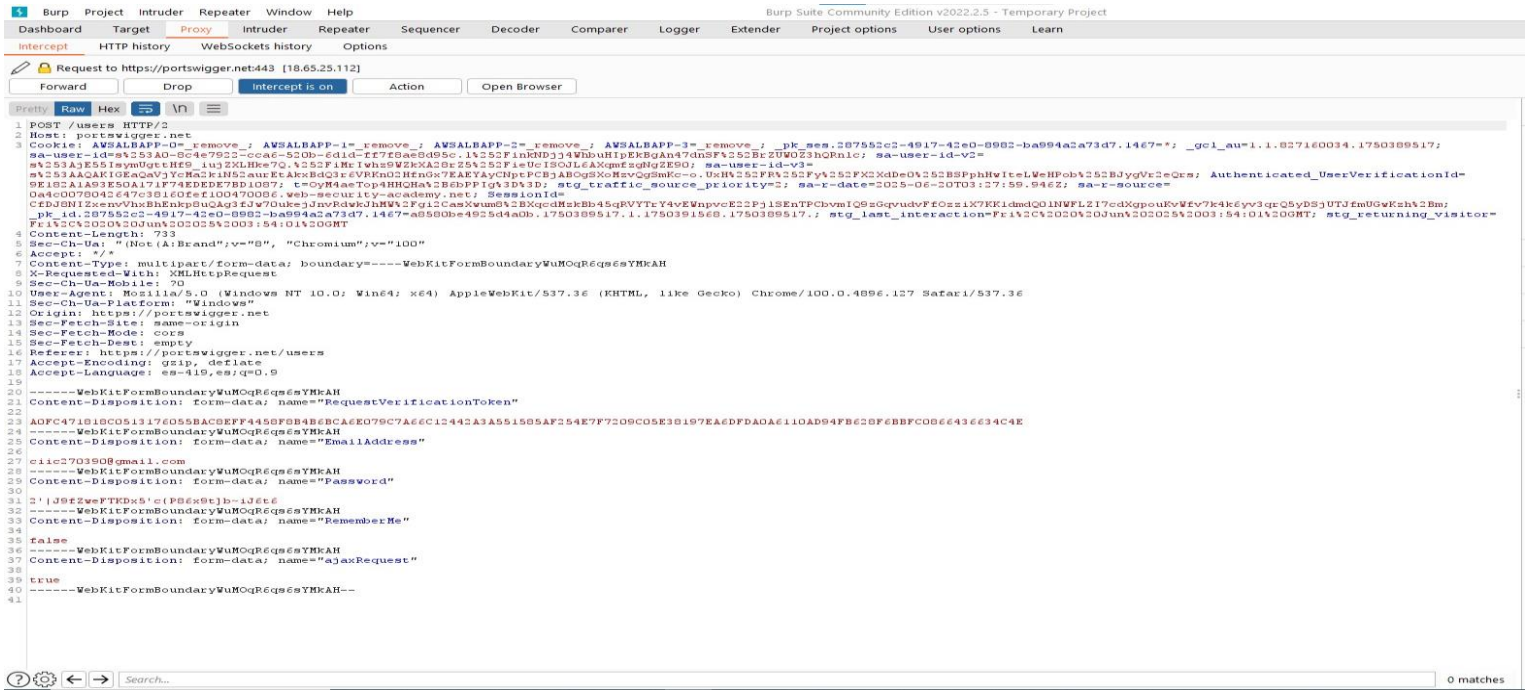
Descripción

La actividad tiene como propósito demostrar cómo una vulnerabilidad de deserialización insegura puede ser aprovechada para escalar privilegios en una aplicación web. Se espera que el alumno adquiera conocimientos prácticos sobre el funcionamiento de sesiones web, el uso de cookies y su potencial manipulación a través de herramientas de análisis como Burp Suite Community Edition. Durante la práctica, se simula un ataque controlado en un entorno proporcionado por PortSwigger, donde, con credenciales de un usuario común, se logra modificar una cookie serializada y obtener acceso al panel administrativo. Este tipo de simulaciones son fundamentales para entender la lógica de los ataques reales, evaluar los riesgos y formar competencias técnicas en auditoría informática. Además, se observarán los efectos que tiene una mala implementación del manejo de sesiones y la falta de validaciones en los objetos serializados. Esta experiencia permite fortalecer el pensamiento crítico frente a la seguridad en el desarrollo de software y preparar futuras estrategias defensivas.

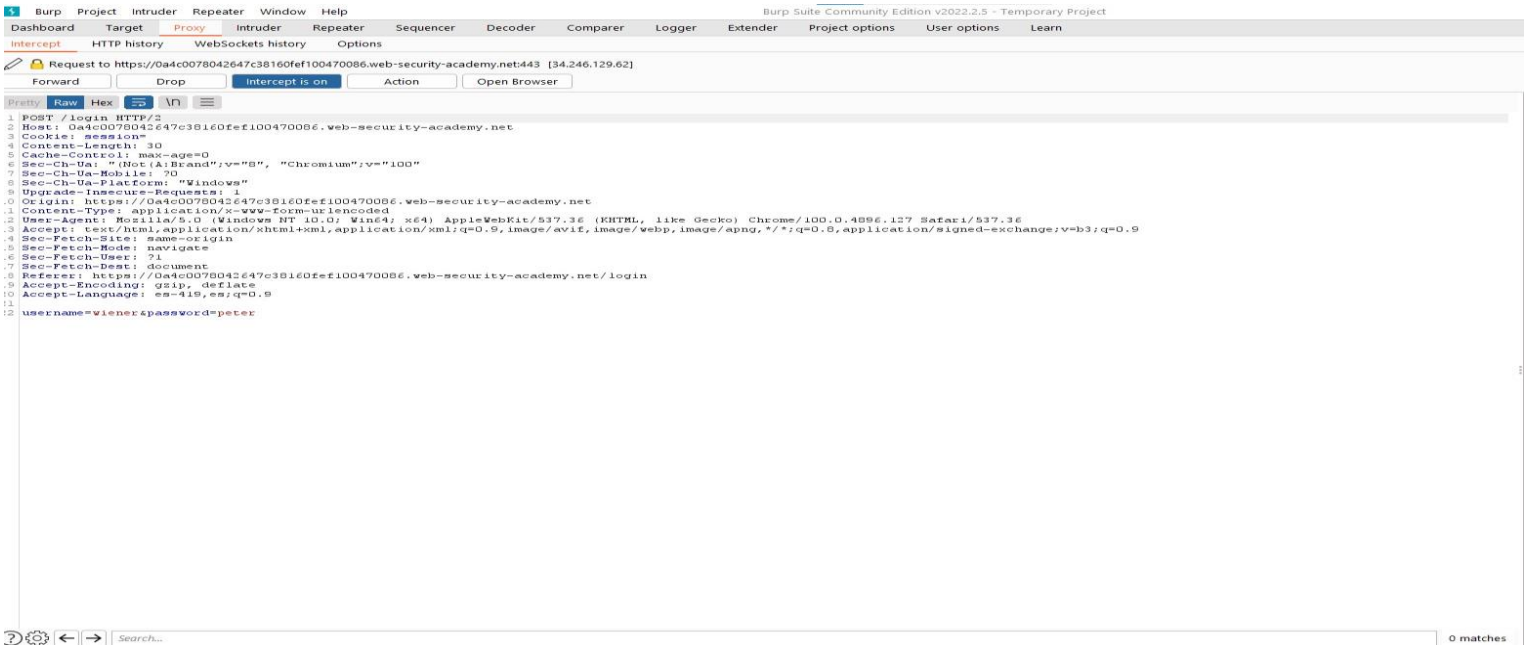
Justificación

Realizar pruebas de deserialización insegura es una necesidad crítica dentro de cualquier proceso de auditoría informática, ya que muchas aplicaciones actuales manejan objetos serializados para la gestión de sesiones o almacenamiento de datos temporales. Sin una validación adecuada, estos objetos pueden ser manipulados maliciosamente para alterar la lógica del sistema, lo cual representa un riesgo alto para la seguridad empresarial y del usuario final. Justificar esta práctica se fundamenta en la importancia de exponer fallos que suelen pasar desapercibidos en pruebas superficiales, pero que pueden comprometer la totalidad del sistema si son explotados. Esta actividad permite al estudiante entender cómo un atacante puede escalar privilegios de usuario, comprometer cuentas y alterar información confidencial mediante simples cambios en una cookie. Con esto, se promueve el desarrollo de competencias para detectar, reportar y mitigar este tipo de vulnerabilidades, así como la creación de aplicaciones más seguras desde su diseño. Además, proporciona habilidades que son directamente aplicables en escenarios laborales reales.

Ataque al sitio



Aquí pudimos realizar el ataque a cuando se nos están pidiendo el usuario de correo y contraseña que automáticamente te manda la misma web al iniciar sección para llegar a cabo el primer paso y a si obtener la información correspondiente que se muestra el correo y la contraseña que te da la web misma que tiene muchos caracteres y letras.



En este ataque es la información que se nos pide del usuario por default y contraseña para entrar al modo administrador y así encriptando lo que se nos pide la actividad.
Que este programa es para desencriptar dicha información para el momento que se necesita algún tipo de vulnerabilidad y que siempre no estamos protegidos.

Conclusión

La realización de esta actividad ha permitido evidenciar de forma práctica cómo una mala implementación en el manejo de objetos serializados dentro de una aplicación web puede derivar en serias vulnerabilidades, como el acceso no autorizado a funciones administrativas. El ejercicio realizado con Burp Suite y la plataforma PortSwigger ha sido clave para comprender los riesgos de la deserialización insegura y cómo un atacante puede manipular cookies para escalar privilegios. Esta experiencia resulta altamente relevante en el ámbito profesional, ya que permite identificar y mitigar fallos antes de que lleguen a ser explotados en un entorno real. Además, fomenta una cultura de desarrollo seguro y pensamiento crítico en torno a la protección de datos, sesiones y estructuras internas del software. En la vida cotidiana, ayuda a ser más consciente de los riesgos digitales y la importancia de medidas como el cifrado, validación de datos y actualizaciones constantes. Las lecciones aprendidas en esta actividad refuerzan la necesidad de una auditoría informática eficaz como defensa ante amenazas emergentes.

Referencias

Tutorías

https://academiaglobal-mx.zoom.us/rec/play/cjxZVN0HcWjImnqhjcKdc7xskm7T2lL2Vr5PSU4yq_QNms4Uamyd-5TkZ6ixbT4vWX78j7uMYQi19JQI.PVimx_GIZb0APX71?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FttXPXCms3IsVBrYr8Yg6AgSlXaNoSmvPa6GPT8b7wz5y-TIcgUxH2WuUwK5MvexG.LEJmiYEhLFDkc8Ty

PortSwigger

https://portswigger.net/burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform=

YouTube MX

https://www.youtube.com/watch?v=Aug94XHpMIQ

ciic2703 / Universidad-Coppel

https://github.com/ciic2703/Universidad-Coppel/tree/main/Auditor%C3%ADa%20Inform%C3%A1tica