

MÁSTER EN CIBERSEGURIDAD ONLINE

Identificación y Mitigación de Vulnerabilidades en Microservicios: Un Enfoque Práctico

TFM elaborado por: Andrew Steeve Ramirez Guzman

Tutor/a de TFM: Raimundo Alcázar Quesada

Bogotá, Colombia – 17/08/2024

Resumen

El presente Trabajo Fin de Máster se enfoca en la identificación y mitigación de vulnerabilidades dentro de arquitecturas de microservicios, un enfoque cada vez más popular en el desarrollo de software moderno. A través de un análisis exhaustivo de un sistema de microservicios, se han aplicado metodologías estándar para la detección de vulnerabilidades críticas que podrían comprometer la seguridad y la integridad de la información. El estudio incluye un análisis detallado de fases como el reconocimiento, escaneo, explotación y la redacción de un informe técnico con las medidas de mitigación sugeridas. Este enfoque práctico no solo identifica las debilidades en la infraestructura, sino que también propone soluciones viables y efectivas para fortalecer la seguridad del sistema.

Abstract

This master’s Thesis focuses on the identification and mitigation of vulnerabilities within microservices architectures, an increasingly popular approach in modern software development. Through an exhaustive analysis of a microservices system, standard methodologies have been applied to detect critical vulnerabilities that could compromise the security and integrity of information. The study includes a detailed analysis of phases such as reconnaissance, scanning, exploitation, and the drafting of a technical report with suggested mitigation measures. This practical approach not only identifies weaknesses in the infrastructure but also proposes viable and effective solutions to strengthen the system's security.

Índice

Lista de Figuras

Lista de Tablas

Introducción y Objetivos

Introducción

En la era digital actual, la ciberseguridad se ha convertido en una prioridad crítica para organizaciones de todo tipo y tamaño. Con el creciente uso de arquitecturas de microservicios, que permiten el desarrollo de aplicaciones modulares y escalables, también han surgido nuevos desafíos en términos de seguridad. Estas arquitecturas, si bien ofrecen ventajas significativas en términos de flexibilidad y despliegue, también presentan vulnerabilidades que pueden ser explotadas si no se gestionan adecuadamente.

La motivación para elegir el tema de este Trabajo Fin de Máster (TFM) radica en la necesidad imperiosa de comprender y abordar las vulnerabilidades inherentes a las arquitecturas de microservicios. A través de un enfoque práctico, este TFM busca no solo identificar estas vulnerabilidades, sino también proponer estrategias efectivas para su mitigación, contribuyendo así a la seguridad global de sistemas críticos en entornos empresariales.

La elección de este tema responde a un interés personal y profesional por las áreas de seguridad informática y desarrollo de software, donde la capacidad de proteger la integridad, confidencialidad y disponibilidad de los sistemas es esencial para el éxito de cualquier organización. Este trabajo pretende ser una contribución significativa al campo de la ciberseguridad, proporcionando un análisis detallado y soluciones prácticas aplicables a arquitecturas de microservicios.

Objetivos

Realizar un análisis exhaustivo de vulnerabilidades en sistemas basados en microservicios, identificando posibles amenazas y proponiendo soluciones efectivas para mitigar los riesgos asociados.

Objetivos Específicos

* **Identificación de Vulnerabilidades Críticas en Arquitecturas de Microservicios**
* Analizar un sistema de microservicios para identificar las principales vulnerabilidades que pueden comprometer la seguridad de este.  
  Utilizar herramientas y técnicas de análisis reconocidas para evaluar la seguridad del sistema.
* **Desarrollo de un Plan de Mitigación de Riesgos**
  + Proponer soluciones específicas para cada una de las vulnerabilidades identificadas, basadas en las mejores prácticas de la industria.
  + Desarrollar un plan de acción que detalle los pasos necesarios para implementar estas soluciones en un entorno real.
* **Evaluación de la Eficacia de las Medidas de Mitigación**
  + Medir el impacto de las soluciones propuestas en la seguridad del sistema, utilizando métricas y criterios de evaluación claros.
  + Ajustar las estrategias de mitigación según los resultados obtenidos, asegurando la máxima protección del sistema.

Desarrollo Del Contenido

1. Plantear el Escenario del Análisis
   1. Descripción de la Aplicación Web Vulnerable

La aplicación web vulnerable seleccionada para este análisis es un sistema de reservas en línea que permite a los usuarios gestionar reservas de hoteles y vuelos. Esta aplicación está diseñada utilizando una arquitectura de microservicios, que ofrece ventajas significativas en términos de escalabilidad y modularidad, pero también introduce varios desafíos de seguridad que necesitan ser abordados.

* + 1. Frontend de la Aplicación

El frontend de la aplicación está desarrollado utilizando tecnologías web estándar:

* **HTML**: Se utiliza para estructurar las páginas web, creando una interfaz de usuario intuitiva y fácil de navegar.
* **CSS**: Es utilizado para diseñar y estilizar la apariencia de la aplicación, asegurando una experiencia de usuario coherente y visualmente atractiva.
* **JavaScript**: Se emplea para agregar interactividad a la aplicación, permitiendo la manipulación dinámica de contenido y la gestión de eventos en el lado del cliente.

El frontend actúa como la interfaz principal a través de la cual los usuarios interactúan con el sistema, enviando solicitudes a los microservicios del backend y presentando la información de manera accesible.

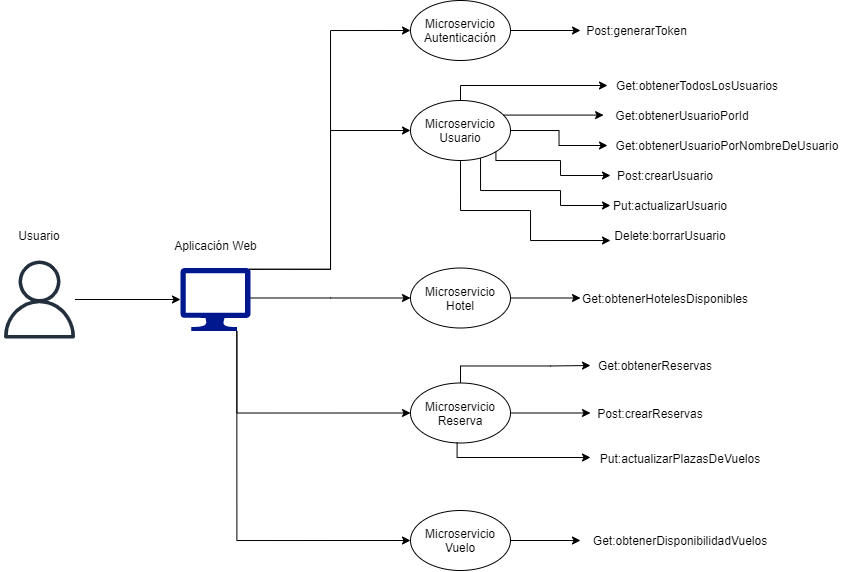
* + 1. Backend de la Aplicación

El backend de la aplicación está desarrollado utilizando **Spring Boot**, un marco de trabajo basado en Java que facilita la creación de aplicaciones robustas y escalables. El backend se conecta a una base de datos **MySQL** centralizada, donde se almacena toda la información relevante, como los detalles de usuarios, reservas, disponibilidad de hoteles y vuelos, entre otros.

* + 1. Arquitectura del Sistema

La aplicación sigue una arquitectura de microservicios, lo que significa que las diferentes funcionalidades están separadas en servicios independientes que se comunican entre sí. Esta arquitectura se ilustra en la siguiente figura:

**Figura 1**  
Esquema aplicación vulnerable



*Nota.* El esquema representa la interacción entre el usuario, la aplicación web y los microservicios.

En esta arquitectura:

Los usuarios interactúan con la **Aplicación Web**, que actúa como un intermediario entre ellos y los microservicios.

* Cada microservicio tiene una función específica, lo que permite la modularidad y escalabilidad del sistema.
* Los **Microservicios** están conectados a una base de datos MySQL que almacena toda la información relevante.
  1. Objetivo del Análisis

El objetivo principal de este análisis es identificar y mitigar las vulnerabilidades presentes en la arquitectura de microservicios de la aplicación. A través de este análisis, se pretende mejorar la seguridad general del sistema, asegurando que las vulnerabilidades críticas sean abordadas y que las medidas de mitigación sean efectivas en proteger los datos y la integridad del sistema.