Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de

Magister en Ciberseguridad

AUTORES:

FREIRE ORTIZ MARLON PAUL

PEÑAFIEL MIÑO RICARDO ANDRES

QUIÑONEZ APRAEZ DANIEL ADRIAN

REVELO BÁEZ MANOLO ALEJANDRO

TUTORES:

Iván Reyes Chacón

Paulina Vizcaíno

TEMA

Análisis comparativo de vulnerabilidades y mecanismos de mitigación en APIs de reserva hotelera con tecnologías REST y GraphQL

Junio-2026

Quito - Ecuador

REINVENTEMOS EL FUTURO

RESUMEN

Las APIs se han convertido en el pilar fundamental de la transformación digital del sector hotelero, permitiendo la integración entre sistemas de reserva, plataformas de distribución y aplicaciones móviles. Sin embargo, esta centralidad las convierte en objetivos prioritarios para ataques cibernéticos. El presente trabajo de investigación se centra en el análisis comparativo experimental entre dos arquitecturas de API ampliamente utilizadas en sistemas hoteleros: REST y GraphQL

Para llevar a cabo el estudio se implementaron dos prototipos funcionalmente equivalentes en un laboratorio controlado, compartiendo el mismo modelo de datos, lógica de negocio y mecanismos de autenticación, con el objetivo de evaluar su comportamiento frente a vulnerabilidades del OWASP API Security Top 10 como Broken Object Level Authorization, Broken Authentication, Broken Object Property Level Authorization, Security Misconfiguration y Unrestricted Resource Consumption.

Los resultados obtenidos revelan que GraphQL ofrece ventajas significativas en autenticación centralizada y control de exposición de datos, gracias a su contexto unificado y su sistema de schema que actúa como contrato de seguridad, mientras que REST presenta riesgos por la necesidad de implementar seguridad en cada endpoint de manera independiente. Sin embargo, GraphQL introduce un riesgo adicional crítico: la introspección activa, que permite a un atacante mapear toda la superficie de ataque si no se deshabilita en

producción. Ambas arquitecturas comparten vulnerabilidades fundamentales como BOLA y la ausencia de rate limiting, que deben ser mitigadas independientemente de la elección tecnológica. En términos de consumo de recursos, GraphQL demostró una gestión de memoria superior, aunque con menor rendimiento en solicitudes por segundo.

Palabras Clave: API Security, REST API, GraphQL API, OWASP API Security Top 10, Sector Hotelero, Vulnerabilidades, Mecanismos de Mitigación, Análisis Comparativo, Laboratorio Experimental, Seguridad de Datos.

ABSTRACT

APIs have become the cornerstone of the digital transformation of the hotel sector, enabling integration between reservation systems, distribution platforms, and mobile applications. However, this centrality makes them prime targets for cyberattacks. This research focuses on an experimental comparative analysis of two API architectures widely used in hotel systems: REST and GraphQL. To conduct the study, two functionally equivalent prototypes were implemented in a controlled laboratory, sharing the same data model, business logic, and authentication mechanisms, with the aim of evaluating their behavior against vulnerabilities from the OWASP API Security Top 10, such as Broken Object Level Authorization, Broken Authentication, Broken Object Property Level Authorization, Security Misconfiguration, and Unrestricted Resource Consumption. The results obtained reveal that GraphQL offers significant advantages in centralized authentication and data exposure control, thanks to its unified context and schema system that acts as a security contract, while REST presents risk due to the need to implement security independently at each endpoint. However, GraphQL introduces an additional critical risk: active introspection, which allows an attacker to map the entire attack surface if not disabled in production. Both architectures share fundamental vulnerabilities such as BOLA and the lack of rate limiting, which must be mitigated regardless of the technology chosen. In terms

of resource consumption, GraphQL demonstrated superior memory management, albeit with lower throughput in requests per second.

Keywords: API Security, REST API, GraphQL API, OWASP API Security Top 10, Hospitality Industry, Vulnerabilities, Mitigation Mechanisms, Comparative Analysis, Experimental Lab, Data Security.