Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

BASTIDAS SALTOS MARIO FABIAN

CEDEÑO BRAVO GUSTAVO ADOLFO

HERRERA PEREZ ERICK WILLIAM

PINTAG SANGA RAFAEL PINTAG

TUTORES:

Paulina Vizcaíno

TEMA

ANÁLISIS COMPARATIVO DE SEGURIDAD EN APIS REST (OWASP API TOP 10)

CASO DE ESTUDIO: CRAPI Y UNA API BASADA EN SPRING BOOT - BOILERPLATE

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Resumen

El presente Trabajo de Fin de Máster tuvo como objetivo evaluar comparativamente la seguridad de dos APIs REST mediante la ejecución de pruebas técnicas controladas, tomando como referencia el OWASP API Security Top 10 2023. Para ello, se analizó una API deliberadamente vulnerable, crAPI, y una API basada en Spring Boot Boilerplate con controles de seguridad implementados. La investigación se desarrolló en un entorno de laboratorio aislado, compuesto por máquinas virtuales, contenedores Docker y herramientas especializadas como Burp Suite, OWASP ZAP, Postman y utilidades de línea de comandos.

La metodología aplicada combinó pruebas manuales y automatizadas orientadas a identificar vulnerabilidades relacionadas con autenticación, autorización, control de acceso, exposición de datos, consumo de recursos, configuraciones inseguras, SSRF, gestión de inventario y consumo inseguro de APIs. Los hallazgos fueron documentados mediante evidencia técnica, descripción del riesgo, impacto potencial y valoración de severidad referencial basada en criterios CVSS v3.1.

Los resultados evidenciaron que crAPI presentó vulnerabilidades representativas en la mayoría de las categorías evaluadas, lo que confirmó su utilidad como entorno vulnerable para el análisis práctico de seguridad en APIs. En contraste, Spring Boot Boilerplate mostró una postura de seguridad más robusta, principalmente por la implementación de autenticación mediante JWT, validación de tokens, protección de endpoints, control de entradas y reducción de superficie expuesta.

En conclusión, el estudio demuestra que la aplicación sistemática de buenas prácticas de desarrollo seguro reduce significativamente el riesgo técnico en APIs REST.

Palabras Clave: APIs REST; OWASP API Security Top 10 2023; crAPI; Spring Boot Boilerplate; CVSS v3.1.

Abstract

This Master's Final Project aimed to comparatively evaluate the security of two REST APIs through controlled technical testing, using the OWASP API Security Top 10 2023 as the main reference framework. For this purpose, the study analyzed a deliberately vulnerable API, crAPI, and an API based on Spring Boot Boilerplate with implemented security controls. The research was conducted in an isolated laboratory environment composed of virtual machines, Docker containers, and specialized tools such as Burp Suite, OWASP ZAP, Postman, and command-line utilities.

The applied methodology combined manual and automated tests aimed at identifying vulnerabilities related to authentication, authorization, access control, data exposure, resource consumption, insecure configurations, SSRF, inventory management, and unsafe API consumption. The findings were documented through technical evidence, risk description, potential impact, and a referential severity assessment based on CVSS v3.1 criteria.

The results showed that crAPI presented representative vulnerabilities in most of the evaluated categories, confirming its usefulness as a vulnerable environment for practical API security analysis. In contrast, Spring Boot Boilerplate demonstrated a stronger security posture, mainly due to the implementation of JWT-based authentication, token validation, endpoint protection, input control, and reduction of the exposed attack surface.

In conclusion, the study demonstrates that the systematic application of secure development best practices significantly reduces technical risk in REST APIs.

Keywords: REST APIs; OWASP API Security Top 10 2023; crAPI; Spring Boot Boilerplate; CVSS v3.1.