Analisis Keamanan Web Application Sistem Pelacakan dan Pemantauan Aset dengan Pendekatan Uji Penetrasi menggunakan Kerangka Kerja OWASP = Security Analysis of a Web Application for Asset Tracking and Monitoring System using Penetration Testing Approach with OWASP Framework

Zana Niswah Awahita, author

Abstrak

Penggunaan internet terus meningkat dengan penggunaan untuk kepentingan yang makin beragam pula, termasuk dalam sebuah bisnis. Hal ini menyebabkan makin banyaknya pula data yang tersimpan dan terekspos di internet. Banyaknya data tersebut tidak diiringi dengan kesadaran terhadap seberapa penting kerahasiaan dan keamanannya. Ini menimbulkan potensi kejahatan yang biasa dikenal dengan cybercrime. Korban dari kejahatan siber dapat mengalami kerugian, mencakup rusaknya reputasi perusahaan atau organisasi hingga kerugian finansial. Untuk itu, penelitian ini bertujuan untuk mengidentifikasi kerentanan yang dimiliki oleh sebuah web application yang menjadi sistem pelacakan dan pemantauan aset. Penelitian ini dilakukan dengan pendekatan uji penetrasi menggunakan kerangka kerja dari OWASP (Open Worldwide Application Security Project). Framework ini berfokus pada keamanan dari web application sehingga sesuai dengan target pengujian dari penelitian ini. Penelitian ini mencakup information gathering dan 3 (tiga) metode pengujian mengacu pada OWASP WSTG, yaitu authentication testing, authorization testing, dan input validation testing dengan total 8 (delapan) metode pengujian yang dipilih. Dari hasil uji penetrasi yang dilakukan, ditemukan 4 kerentanan yang berhasil dieksploitasi. Keempat kerentanan tersebut kemudian dianalisis menggunakan OWASP Risk Rating Methodology dengan hasil akhir poin likelihood 6,5 (HIGH) dan impact 3,21 (MEDIUM). Hasil ini menunjukkan overall risk severity dari web application target yang diuji memiliki tingkat kerentanan tinggi.

.....The increasing use of the internet for a wide range of purposes, including business, has led to a significant growth in the amount of data stored and exposed online. However, this increase in data is not matched by an awareness of the importance of its confidentiality and security. This situation creates the potential for cybercrime, which can cause substantial harm, including damage to the reputation of a company or organization and financial losses. Therefore, this research aims to identify vulnerabilities in a web application used as an asset tracking and monitoring system. The study employs a penetration testing approach using the OWASP (Open Worldwide Application Security Project) framework. This framework focuses on web application security, making it suitable for the research's testing targets. The study involves information gathering and three testing methods from the OWASP WSTG: authentication testing, authorization testing, and input validation testing, using a total of eight selected testing methods. The penetration testing results revealed four exploitable vulnerabilities. These vulnerabilities were analyzed using the OWASP Risk Rating Methodology, resulting in a final likelihood score of 6.5 (HIGH) and an impact score of 3.21 (MEDIUM). These results indicate that the overall risk severity of the tested web application has a high level of vulnerability.