

**PENERAPAN METODE *INFORMATION SYSTEM SECURITY*
ASSESSMENT FRAMEWORK (ISSAF) UNTUK UJI
KUALITAS KEAMANAN *WEBSITE***

ROBLOX

ABSTRAK

Perkembangan teknologi informasi dan internet telah meningkatkan kebutuhan akan keamanan *website* untuk melindungi data serta aktivitas pengguna dari berbagai ancaman *siber*. Salah satu platform yang memiliki jumlah pengguna sangat besar adalah Roblox, yaitu platform game online berbasis web yang memungkinkan pengguna untuk bermain, berinteraksi, dan melakukan transaksi virtual. Tingginya jumlah pengguna menjadikan Roblox sebagai salah satu target potensial bagi berbagai ancaman keamanan. Oleh karena itu, diperlukan pengujian keamanan untuk mengidentifikasi potensi kerentanan yang dapat memengaruhi keamanan sistem. Penelitian ini bertujuan untuk menerapkan metode *Information Systems Security Assessment Framework* (ISSAF) pada proses *vulnerability assessment* website Roblox, mengidentifikasi kerentanan keamanan menggunakan Burp Suite dan Nessus, serta memberikan rekomendasi mitigasi berdasarkan hasil temuan pengujian. Metode penelitian yang digunakan adalah ISSAF yang difokuskan pada tahap *Information Gathering*, *Vulnerability Assessment*, *Analysis and Risk Assessment*, dan *Reporting*. Pengujian dilakukan menggunakan *Burp Suite* untuk menganalisis keamanan aplikasi web melalui pemeriksaan request, response, session management, dan security header. Selain itu, *Nessus* digunakan untuk melakukan pemindaian kerentanan pada sisi jaringan, layanan, dan konfigurasi server. Hasil pengujian kemudian dianalisis dan diklasifikasikan berdasarkan tingkat risiko yang ditemukan. Hasil penelitian menunjukkan bahwa website Roblox telah menerapkan berbagai mekanisme keamanan yang cukup baik, seperti penggunaan HTTPS, penerapan atribut *Secure* dan *HttpOnly* pada *cookie*, validasi autentikasi, serta penggunaan token keamanan pada beberapa layanan. Pengujian menggunakan *Burp Suite* menemukan dua temuan dengan tingkat risiko rendah (*Low*), yaitu tidak diterapkannya *Content Security Policy* (CSP) pada beberapa *response* dan belum diterapkannya *X-Frame-Options* secara menyeluruh. Sementara itu, hasil pemindaian menggunakan *Nessus* didominasi oleh temuan kategori *Informational* yang berkaitan dengan informasi konfigurasi server, layanan jaringan, dan *port* yang terdeteksi. Berdasarkan hasil analisis dan *risk assessment*, *website* Roblox dikategorikan memiliki tingkat risiko keamanan yang relatif rendah (*Low Risk*), namun tetap memerlukan peningkatan konfigurasi keamanan dan evaluasi secara berkala untuk meminimalkan potensi ancaman di masa mendatang.

Kata Kunci: *Vulnerability Assessment*, *ISSAF*, *Burp Suite*, *Nessus*, Roblox.

**PENERAPAN METODE *INFORMATION SYSTEM SECURITY*
ASSESSMENT FRAMEWORK (ISSAF) UNTUK UJI
KUALITAS KEAMANAN *WEBSITE*
ROBLOX**

ABSTRACT

The rapid growth of information technology and internet usage has increased the need for website security to protect user data and activities from various cyber threats. One of the platforms with a large number of active users is Roblox, a web-based online gaming platform that allows users to play games, interact with others, and conduct virtual transactions. Due to its popularity and extensive user base, Roblox has become a potential target for cyberattacks. Therefore, security testing is necessary to identify vulnerabilities that may affect the security of the system. This study aims to implement the Information Systems Security Assessment Framework (ISSAF) in the vulnerability assessment process of the Roblox website, identify security vulnerabilities using Burp Suite and Nessus, and provide mitigation recommendations based on the findings. The research method employed in this study is ISSAF, focusing on the stages of Information Gathering, Vulnerability Assessment, Analysis and Risk Assessment, and Reporting. Security testing was conducted using Burp Suite to analyze web application security through the examination of requests, responses, session management, and security headers. In addition, Nessus was utilized to perform vulnerability scanning on network services, server configurations, and system components. The results obtained from both tools were analyzed and classified according to their risk levels. The findings indicate that the Roblox website has implemented several security mechanisms effectively, including HTTPS communication, Secure and HttpOnly cookie attributes, authentication validation, and security token implementation across multiple services. Testing with Burp Suite identified two low-risk findings, namely the absence of Content Security Policy (CSP) in several responses and the incomplete implementation of X-Frame-Options. Meanwhile, the Nessus scan results were predominantly categorized as Informational, relating to server configuration details, network services, and detected ports. Based on the analysis and risk assessment, the Roblox website is classified as having a relatively low security risk (Low Risk). However, improvements in security configuration and periodic vulnerability assessments are still recommended to minimize potential threats and enhance overall system security.

Keywords: *Vulnerability Assessment, ISSAF, Burp Suite, Nessus, Roblox.*