RISK ASSESSMENT KEAMANAN INFORMASI PADA APLIKASI *E-COMMERCE* DI INDONESIA MENGGUNAKAN *FRAMEWORK* NIST SP 800-30 DAN OWASP MOBILE 2024

Nur Kholis[1], Alfirna Rizqi Lahitani[2]

INTISARI

Latar Belakang: Perkembangan *e-commerce* di Indonesia mendorong peningkatan jumlah pengguna, namun hal ini juga menimbulkan tantangan besar termasuk kebocoran data dan penyalahgunaan izin akses. Sebagian besar aplikasi *e-commerce* di Indonesia masih memiliki celah keamanan. Oleh karena itu, diperlukan upaya untuk mengidentifikasi dan menilai tingkat risiko keamanan informasi pada aplikasi *e-commerce* di Indonesia untuk meningkatkan perlindungan terhadap data pengguna.

Tujuan: Penelitian ini bertujuan untuk melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia dengan mengidentifikasi celah keamanan serta membandingkan tingkat keamanannya diantara beberapa platform, yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak dengan pendekatan analisis statis menggunakan *framework* NIST SP 800-30 dan OWASP Mobile 2024.

Metode Penelitian: Penelitian ini diawali dengan identifikasi aplikasi dan aset informasi, kemudian pemindaian kerentanan dengan MobSF. Temuan kerentanan dipetakan ke dalam kategori OWASP Mobile Top 10 2024. Selanjutnya, dilakukan analisis risiko berdasarkan NIST SP 800-30, evaluasi risiko dari setiap kerentanan yang ditemukan, rekomendasi mitigasi, dan pelaporan.

Hasil: Seluruh aplikasi teridentifikasi memiliki sejumlah kerentanan, diantaranya *hardcoded secrets*, kriptografi lemah, penyimpanan data tidak aman, izin akses berbahaya, dan kesalahan konfigurasi. Berdasarkan pemindaian dengan MobSF seluruh aplikasi memiliki skor keamanan 39-50. Berdasarkan pemetaan kerentanan ke OWASP Mobile Top 10 2024, kerentanan paling dominan masuk dalam kategori M10, M9, dan M8. Setelah dilakukan evaluasi risiko menggunakan *framework* NIST SP 800-30 seluruh aplikasi berada dalam kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan dan memerlukan perbaikan.

Kesimpulan: Hasil penelitian menunjukkan bahwa aplikasi *e-commerce* yang dianalisis masih memiliki kelemahan yang berpotensi membahayakan keamanan data pengguna. *Framework* NIST SP 800-30 dan OWASP Mobile Top 10 2024 dapat digunakan dalam mengidentifikasi, mengklasifikasi, dan *melakukan risk assessment* keamanan informasi aplikasi.

Kata-kunci: *E-commerce, Risk Assessment*, Keamanan Aplikasi, NIST SP 800-30, OWASP Mobile Top 10 2024

RISK ASSESSMENT OF INFORMATION SECURITY IN E-COMMERCE APPLICATIONS IN INDONESIA USING THE FRAMEWORK NIST SP 800-30 AND OWASP MOBILE 2024

Nur Kholis[1], Alfirna Rizqi Lahitani[2]

ABSTRACT

***Background**: The development of e-commerce in Indonesia has driven an increase in the number of users, but this also poses major challenges including data leaks and misuse of access permissions. Most e-commerce applications in Indonesia still have security gaps. Therefore, efforts are needed to identify and assess the level of information security risk in e-commerce applications in Indonesia to improve protection of user data.*

***Objective**: This research aims to conduct a risk assessment on e-commerce applications in Indonesia by identifying security gaps and comparing their security levels between several platforms, namely Shopee, Tokopedia, Lazada, Blibli, and Bukalapak with a static analysis approach using the NIST SP 800-30 framework and OWASP Mobile 2024.*

***Method**: This research began with the identification of applications and information assets, then vulnerability scanning with MobSF. Vulnerability findings were mapped into the OWASP Mobile Top 10 2024 category. Furthermore, a risk analysis was carried out based on NIST SP 800-30, risk evaluation of each vulnerability found, mitigation recommendations, and reporting.*

***Result**: All applications were identified as having a number of vulnerabilities, including hardcoded secrets, weak cryptography, insecure data storage, malicious access permissions, and misconfigurations. Based on scanning with MobSF, all applications had a security score of 39-50. Based on vulnerability mapping to the OWASP Mobile Top 10 2024, the most dominant vulnerabilities fall into categories M10, M9, and M8. After a risk evaluation using the NIST SP 800-30 framework, all applications were in the High category, meaning the applications still have many security holes and need to be fixed.*

***Conclusion**: The results of the research showed that the e-commerce applications analyzed still had weaknesses that could potentially endanger the security of user data. The NIST SP 800-30 and OWASP Mobile Top 10 2024 frameworks can be used to identifying, classifying, and conducting risk assessments of application information security.*

***Keywords**: E-commerce, Risk Assessment, Application Security, NIST SP 800-30, OWASP Mobile Top 10 2024*