

INTISARI

Serangan terhadap keamanan sistem komputer berupa ancaman dan kelemahan sistem dapat membahayakan operasi sistem komputer serta dapat menimbulkan celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk merusak atau menyerang sistem komputer. Untuk mencegah serangan yang berakibat rusaknya data dalam sistem, diperlukan usaha berupa evaluasi terhadap sistem secara berkala. Evaluasi dapat dilakukan dengan mencari lubang keamanan pada sistem komputer. Hasil evaluasi akan menghasilkan rekomendasi perbaikan keamanan sistem serta adanya rencana untuk melakukan evaluasi keamanan secara berkala. Evaluasi keamanan sistem perlu dilakukan secara berkala karena versi *software* yang digunakan pada sistem informasi berubah-ubah dengan cepat mengikuti perkembangan zaman. *Update software* ini terkadang menutup celah lama, namun seringkali juga mengandung lubang baru yang dapat dieksploitasi oleh pihak yang tidak bertanggungjawab.

Aplikasi web Monitoring dan Evaluasi Komisi Informasi Daerah Istimewa Yogyakarta dipilih sebagai obyek penelitian karena aplikasi ini merupakan salah satu komponen penting dalam penyelenggaraan keterbukaan informasi badan-badan publik di wilayah Daerah Istimewa Yogyakarta. Untuk melakukan evaluasi keamanan pada aplikasi web Monitoring dan Evaluasi Komisi Informasi Daerah Istimewa Yogyakarta, digunakan aplikasi *web scanner*. Open Web Application Security Project (OWASP) merupakan sebuah organisasi nonprofit yang bergerak di bidang keamanan sistem informasi yang menghasilkan beberapa produk, di antaranya adalah OWASP Top 10 2021 dan Zed Attack Proxy (ZAP).

Pada tugas akhir ini dilakukan pemindaian terhadap keamanan dari aplikasi web Monitoring dan Evaluasi Komisi Informasi Daerah Istimewa Yogyakarta. Dari hasil pemindaian ditemukan 30,8% celah berisiko menengah, 53,8% celah dengan risiko rendah, dan 15,4% celah yang bersifat informasional. Hasil pemindaian ini digunakan untuk menentukan rekomendasi perbaikan dan rencana evaluasi keamanan aplikasi web secara berkala demi mewujudkan aplikasi web yang handal.

Kata kunci: Keamanan aplikasi web, Rekayasa keamanan perangkat lunak, sistem deteksi gangguan.

ABSTRACT

In computer system security there are two important things namely the threats and weaknesses of the system. Threats are all forms of attack from outside the system that may occur and endanger the operation of the computer system, either system damage, disruption to acces, leakage of secrets or damage to data. The weaknesses of the system are gaps than can be exploited by irresponsible parties to damage and attack computer systems. To prevent the attack that can damage, efforts are nedded in the form of periodic evaluation of the system. System Security Evaluation can be done by looking for security holes in the computer system. The result of the evaluation will produce recommendations for improving system security as well as a plan for carry out regular security evaluations. System Security Evaluation needs to be done regularly because the software used in the information system changes rapidly following the times. This software update sometimes closes old gaps, but often contains new holes that cn be exploited by irresponsible parties.

Monitoring and Evaluation Komisi Informasi Daerah Istimewa Yogyakarta web application was chosen as the object of the research because this application is one of the important components in the implementation of public information disclosure in the Daerah Istimewa Yogyakarta Area. With this research, it is hoped that a reliable Monitoring and Evaluation Komisi Informasi Daerah Istimewa Yogyakarta web application will be realized.

This final assignment scanned the Monitoring and Evaluation Komisi Informasi Daerah Istimewa Yogyakarta. The scan resulted in 30,8% medium level risk, 53,8% low level risks, and 15,4% informational risks. These results are used to decide the steps necessary to patch the web application and routine evaluation of the web application security so that it will be a robust and dependable system.

Keywords: Web application security, Software security engineering, Intrusion detection systems.