PEMANFAATAN OPEN SOURCE INTELLIGENCE (OSINT) UNTUK MENENTUKAN RISK ASSESSMENT WEBSITE UPNVJ

Muhamad Wildan Akasyah

ABSTRAK

Website Universitas Pembangunan Nasional Veteran Jakarta (UPNVJ) menjadi salah satu aset digital penting yang berperan dalam mendukung kegiatan akademik dan administrasi. Namun, risiko keamanan siber terhadap *website* ini dapat mengancam data dan layanan yang disediakan. Penelitian ini bertujuan untuk melakukan evaluasi risiko pada website UPNVJ dengan memanfaatkan Open Source Intelligence (OSINT) sebagai pendekatan utama. Dengan menggunakan kerangka kerja NIST SP 800-30, penelitian ini mencakup identifikasi ancaman, kerentanan, dan dampak potensi serangan siber. Data dikumpulkan dari berbagai sumber OSINT seperti SecurityTrails, Pentest-Tools, Maltego, Whois Lookup, dan VirusTotal, untuk menganalisis aset digital dan mengevaluasi risiko. Hasil penelitian menunjukkan beberapa kerentanan pada konfigurasi server, termasuk potensi serangan seperti HTTP *Request Smuggling* yang ditemukan dalam laporan Pemindaian Kerentanan. Berdasarkan temuan tersebut, rekomendasi mitigasi seperti pembaruan perangkat lunak dan penguatan konfigurasi keamanan diberikan untuk meningkatkan keamanan *website* UPNVJ. Penelitian ini memberikan kontribusi pada pemahaman risiko siber berbasis OSINT serta langkah mitigasi yang relevan dalam konteks organisasi pendidikan.

Kata Kunci : Open Source Intelligence (OSINT), Risk Assessment, NIST SP 800-30, Website, UPN Veteran Jakarta (UPNVJ).

PEMANFAATAN OPEN SOURCE INTELLIGENCE (OSINT) UNTUK MENENTUKAN RISK ASSESSMENT WEBSITE UPNVJ

Muhamad Wildan Akasyah

ABSTRACT

The website of Universitas Pembangunan Nasional Veteran Jakarta (UPNVJ) is one of the important digital assets that plays a role in supporting academic and administrative activities. However, cybersecurity risks to this website can threaten the data and services provided. This study aims to conduct a risk evaluation on the UPNVJ website by utilizing Open Source Intelligence (OSINT) as the main approach. Using the NIST SP 800-30 Rev. 1 framework, this study includes identifying threats, vulnerabilities, and the impact of potential cyber attacks. Data was collected from various OSINT sources such as SecurityTrails, Pentest-Tools, Maltego, Whois Lookup, and VirusTotal, to analyze digital assets and evaluate risks. The results of the study showed several vulnerabilities in the server configuration, including potential attacks such as HTTP Request Smuggling found in the Vulnerability Scan report. Based on these findings, mitigation recommendations such as software updates and strengthening security configurations are provided to improve the security of the UPNVJ website. This study contributes to the understanding of OSINT-based cyber risks and relevant mitigation steps in the context of educational organizations.

Keywords : *Open Source Intelligence (OSINT), Risk Assessment, NIST SP 800-30, Website, UPN Veteran Jakarta (UPNVJ).*