ANALISIS KEAMANAN *WEBSITE* SIAKAD UPN "VETERAN" JAKARTA MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* BERDASARKAN OWASP *TOP TEN*

Alia Reviana Samosir

ABSTRAK

Transformasi digital di lingkungan pendidikan tinggi menghadirkan tantangan baru dalam aspek keamanan informasi. *Website* Sistem Informasi Akademik (SIAKAD) UPN "Veteran" Jakarta, sebagai pusat pengelolaan data akademik yang bersifat sensitif, menjadi target potensial serangan siber. Penelitian ini bertujuan untuk menganalisis keamanan *website* SIAKAD menggunakan metode *vulnerability assessment* berdasarkan *framework* OWASP *Top Ten* 2021. Pengujian dilakukan menggunakan OWASP ZAP dan enam tools tambahan, yaitu Nmap, Elastic Stack, Git Secrets, Gitleaks, OWASP Dependency-Check, dan OWASP Threat Dragon. Hasil analisis menunjukkan adanya kerentanan dalam kategori *Broken Access Control, Injection, Security Misconfiguration, Identification and Authentication Failures, Server-Side Request Forgery* (SSRF), *Cryptographic Failures, Software and Data Integrity Failures*, serta penggunaan komponen yang rentan dan usang. Beberapa kerentanan tidak dapat dianalisis lebih lanjut karena keterbatasan akses log keamanan dan arsitektur sistem. Penelitian ini merekomendasikan integrasi pengujian keamanan dalam SDLC dan penyediaan dokumentasi sistem yang memadai untuk mendukung proses threat modeling secara optimal.

Kata Kunci: siakad, owasp *top ten, vulnerability assessment*, keamanan informasi, *website*

SECURITY ANALYSIS OF THE SIAKAD WEBSITE OF UPN "VETERAN" JAKARTA *USING THE VULNERABILITY ASSESSMENT METHOD BASED ON* OWASP *TOP TEN*

Alia Reviana Samosir

ABSTRACT

The digital transformation within higher education institutions presents new challenges in information security. The Academic Information System (SIAKAD) *website of* UPN "Veteran" Jakarta*, as a central hub for sensitive academic data, is a potential target for cyberattacks. This study aims to analyze the security of the* SIAKAD *website using the vulnerability assessment method based on the* OWASP *Top Ten* 2021 *framework. The assessment was conducted using* OWASP ZAP *and six additional tools, namely* Nmap, Elastic Stack, Git Secrets, Gitleaks, OWASP Dependency-Check, *and* OWASP Threat Dragon. *The findings revealed vulnerabilities in the categories of Broken Access Control, Injection, Security Misconfiguration, Identification and Authentication Failures, Server-Side Request Forgery (SSRF), Cryptographic Failures, Software and Data Integrity Failures, and the use of vulnerable and outdated components. Certain vulnerabilities could not be fully analyzed due to limitations in access to system logs and architecture documentation. This research recommends the integration of security testing into the* SDLC *and the availability of comprehensive system documentation to support effective threat modeling.*

Keywords: siakad, owasp *top ten, vulnerability assessment, information security, website*