

ANALISIS KEAMANAN WEBSITE MENGGUNAKAN OWASP TOP 10 TAHUN 2021 DAN NIST SP 800-115 STUDI KASUS SISTEM INFORMASI CALON MAHASISWA BARU

Ahmad Nurhidayat, Chanief Budi Setiawan, Alfirna Rizqi Lahitani

INTISARI

Latar Belakang: Aplikasi web Sistem Informasi Calon Mahasiswa Baru (SICAMA) mengelola informasi krusial pengguna dan pemangku kepentingan di lingkungan universitas, sehingga menjadi target potensial serangan *cyber*. Dengan mempertimbangkan tiga komponen keamanan informasi: kerahasiaan (*confidentiality*), integritas (*integrity*), dan aksesibilitas (*availability*), aspek keamanan harus diterapkan pada Sistem Informasi Calon Mahasiswa Baru (SICAMA).

Tujuan: Penelitian ini bertujuan mengidentifikasi dan menganalisis kerentanan pada website SICAMA Universitas Jenderal Achmad Yani Yogyakarta. Dengan menggunakan metode NIST SP 800-115 dan panduan OWASP Top 10, penelitian ini menilai keamanan situs web dan memberikan rekomendasi untuk meningkatkan perlindungan data dan integritas sistem, serta menjaga kepercayaan pengguna.

Metode Penelitian: Penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) SP 800-115 untuk menganalisis kerentanan pada aplikasi web dan mengkategorikan kerentanan dengan acuan kerentanan *Open Web Application Security Project* (OWASP) TOP 10.

Hasil: Penelitian ini mengungkap berbagai kerentanan pada website SICAMA pada enam dari 10 kategori OWASP dengan presentase 60%, termasuk kebocoran informasi melalui *ETags header*, *cookies* tanpa *secure* dan *httponly flags*, ketidakhadiran token Anti-CSRF, kebijakan *Content-Security-Policy* (CSP) yang tidak memadai, dan *SQL Injection*.

Kesimpulan: Identifikasi kerentanan menggunakan metode NIST SP 800-115 menunjukkan bahwa SICAMA memiliki sejumlah kelemahan. Disarankan untuk menerapkan token Anti-CSRF, memperbarui *library* yang rentan, menambah *header* keamanan, dan memperketat kebijakan CSP untuk meningkatkan keamanan dan keandalan layanan informasi.

Kata-kunci: Keamanan Website, SICAMA, NIST SP 800-115, OWASP Top 10, Sistem Informasi Calon Mahasiswa Baru

ANALYZE WEBSITE SECURITY USES OWASP TOP 10 YEAR 2021 AND NIST SP 800-115 CASE STUDY OF PROSPECTIVE NEW STUDENT INFORMATION SYSTEMS

Ahmad Nurhidayat, Chanief Budi Setiawan, Alfirna Rizqi Lahitani

ABSTRACT

Background: The New Student Prospective Information System (SICAMA) web application manages crucial information for users and stakeholders in the university environment, making it a potential target for cyber attacks. By considering three components of information security: confidentiality, integrity and accessibility, security aspects must be applied to the Prospective New Student Information System (SICAMA).

Objective: This research aims to identify and analyze vulnerabilities on the SICAMA website of Jenderal Achmad Yani University, Yogyakarta. Using the NIST SP 800-115 method and the OWASP Top 10 guide, this research assesses website security and provides recommendations for improving data protection and system integrity, as well as maintaining user trust.

Method: This research uses the National Institute of Standards and Technology (NIST) SP 800-115 method to analyze vulnerabilities in web applications and categorize vulnerabilities with reference to the Open Web Application Security Project (OWASP) TOP 10 vulnerabilities.

Result: This research revealed various vulnerabilities on the SICAMA website in six of the 10 OWASP categories with a percentage of 60%, including information leaks via ETags headers, cookies without secure and httponly flags, absence of Anti-CSRF tokens, incomplete Content-Security-Policy (CSP) policies, adequate, and SQL Injection .

Conclusion: Vulnerability identification using the NIST SP 800-115 method shows that SICAMA has a number of weaknesses. It is recommended to implement Anti-CSRF tokens, update vulnerable libraries, add security headers, and tighten CSP policies to improve the security and reliability of information services.

Keywords: Website Security, SICAMA, NIST SP 800-115, OWASP Top 10, Information Systems for Prospective New Students