

ANALISIS KERENTANAN KEAMANAN WEBSITE PERGURUAN TINGGI TERHADAP SERANGAN WEB DEFACEMENT BERDASARKAN KERANGKA KERJA OWASP TOP 10 DAN COMMON VULNERABILITY SCORING SYSTEM

Gede Erik Aktama, Gina Ekaruthiany Baeruma, Margaret Beatrix Getroyda

Universitas Parna Raya, Manado

gedeerikaktama@gmail.com

ginabaeruma@microsoft.parnaraya.ac.id

margaretgetroyda@microsoft.parnaraya.ac.id

Abstrak

Website perguruan tinggi dengan domain berotoritas tinggi (.ac.id) semakin rentan menjadi target utama serangan siber, terutama kejahatan web defacement untuk penyusupan landing page dan optimasi mesin pencari (SEO poisoning) situs judi online. Keberhasilan eksploitasi peretasan ini mencoreng reputasi akademik, merusak integritas informasi publik, dan mengancam kerahasiaan data sivitas akademika. Penelitian ini bertujuan untuk menginvestigasi kerentanan keamanan website perguruan tinggi secara komprehensif menggunakan kerangka kerja Open Web Application Security Project (OWASP) Top 10 serta mengukur tingkat keparahan risiko secara kuantitatif berdasarkan standar Common Vulnerability Scoring System (CVSS) v3.1. Audit keamanan dilakukan pada 15 sub-domain website perguruan tinggi meliputi portal utama, sistem informasi akademik, portal jurnal (OJS), dan laman fakultas melalui tahapan vulnerability assessment dan uji penetrasi pasif. Hasil asesmen mengidentifikasi 5 temuan kerentanan kritis, di antaranya SQL Injection pada portal penerimaan mahasiswa (CVSS 9.8 - Critical), Arbitrary File Upload pada modul OJS (CVSS 8.8 - High), dan Outdated Plugins pada CMS (CVSS 7.5 - High). Sebanyak 4 dari 15 website (26,7%) terpapar celah kategori Critical, dan 86,7% website belum menerapkan Content Security Policy (CSP). Berdasarkan temuan tersebut, dirumuskan arsitektur mitigasi terintegrasi yang mencakup implementasi parameter input sanitization, penataan konfigurasi hak akses server, penerapan HTTP Security Headers lengkap, dan integrasi Web Application Firewall (WAF) guna memitigasi ancaman defacement secara proaktif dan berkelanjutan.

Kata Kunci: Keamanan Website, Web Defacement, Judi Online, OWASP Top 10, CVSS v3.1, Perguruan Tinggi

Abstract

Higher education websites operating under authoritative academic domains (.ac.id) are increasingly targeted by cyber criminals, specifically through web defacement attacks aimed at injecting unauthorized landing pages and exploiting search engine rankings (SEO poisoning) for illegal online gambling networks. Successful intrusions severely jeopardize institutional academic prestige, corrupt public information integrity, and compromise student confidentiality. This study comprehensively investigates security vulnerabilities across higher education web applications leveraging the Open Web Application Security Project (OWASP) Top 10 framework and quantifies risk severity using the Common Vulnerability Scoring System (CVSS) v3.1 standard. Security assessments were executed across 15 university sub-domains including institutional portals, academic systems, Open Journal Systems (OJS), and faculty portals via vulnerability scanning and controlled passive penetration testing. Assessments uncovered 5 critical vulnerabilities, prominently SQL Injection on admissions portals (CVSS 9.8 - Critical), Arbitrary File Upload in journal systems (CVSS 8.8 - High), and Outdated CMS Plugins (CVSS 7.5 - High). In total, 4 of 15 audited domains (26.7%) exhibited Critical flaws, with 86.7% failing to deploy Content Security Policy (CSP) headers. In response, a multi-layered defense-in-depth architecture is proposed, incorporating strict input parameter sanitization, least-privilege server permissions, comprehensive HTTP security headers, and Web Application Firewall (WAF) integration to proactively neutralize persistent defacement attempts.

Keywords: Website Security, Web Defacement, Online Gambling, OWASP Top 10, CVSS v3.1, Higher Education

I. PENDAHULUAN

Perguruan tinggi modern semakin bergantung pada infrastruktur berbasis web sebagai media utama penyelenggaraan tri dharma perguruan tinggi, penyebaran informasi akademik, serta pengelolaan layanan administrasi publik. Domain dengan ekstensi .ac.id memiliki otoritas domain (domain authority) yang sangat tinggi di mata mesin pencari seperti Google, berkat rekam jejak publikasi ilmiah,

akreditasi institusi, dan tautan masuk (backlinks) yang kredibel. Namun demikian, reputasi domain yang tinggi ini justru menjadikan website institusi pendidikan tinggi sebagai sasaran empuk bagi pelaku sindikat kejahatan siber.

Salah satu fenomena kejahatan siber yang marak terjadi dalam beberapa tahun terakhir di Indonesia adalah serangan peretasan tampilan (web defacement) yang bertujuan menyisipkan konten promosi judi online (gambling content injection). Berbeda dengan aksi defacement tradisional yang mengganti seluruh halaman utama dengan pesan politis atau gambar peretas, teknik defacement modern cenderung bersifat terselubung (stealth defacement). Penyerang mengeksploitasi celah keamanan server untuk menanam berkas HTML atau PHP tersembunyi, memanipulasi meta deskripsi, menyisipkan skrip pengalihan (URL redirect), atau memanfaatkan teknik search engine optimization (SEO) poisoning agar tautan platform judi online dapat terindeks secara masif di halaman pertama mesin pencari dengan menunggangi otoritas domain universitas.

Dampak dari peretasan ini sangat destruktif bagi institusi perguruan tinggi. Selain mencoreng citra akademis dan merusak kepercayaan masyarakat, domain kampus berisiko terkena pemblokiran (blacklist) oleh Kementerian Komunikasi dan Informatika serta mesin pencari global, yang berdampak pada terganggunya aksesibilitas seluruh layanan akademik. Di samping itu, celah keamanan yang dibiarkan terbuka dapat dieksploitasi lebih lanjut untuk peretasan basis data mahasiswa, pencurian kredensial dosen, atau instalasi malware ransomware.

Dalam praktik tata kelola teknologi informasi kampus, audit keamanan web secara periodik sering kali terabaikan akibat keterbatasan sumber daya manusia teknis, kurangnya pemahaman pengembang terhadap pedoman pengodean aman (secure coding practices), dan kebiasaan menggunakan komponen pihak ketiga (CMS, plugin, tema) yang sudah usang tanpa pembaharuan berkala. Guna mengatasi permasalahan tersebut, dibutuhkan kerangka evaluasi kerentanan yang terstandarisasi. Kerangka kerja Open Web Application Security Project (OWASP) Top 10 menyediakan taksonomi risiko keamanan web paling mutakhir yang diakui secara global, sementara Common Vulnerability Scoring System (CVSS) v3.1 menyediakan formula matematis untuk mengukur tingkat keparahan risiko secara objektif.

Berdasarkan konteks tersebut, penelitian ini bertujuan untuk: (1) Mengidentifikasi dan memetakan kerentanan keamanan pada 15 website dan sistem informasi perguruan tinggi menggunakan kerangka kerja OWASP Top 10; (2) Menguantifikasi tingkat keparahan risiko celah temuan menggunakan kalkulasi metrik CVSS v3.1; (3) Menganalisis mekanisme eksploitasi serangan web defacement konten judi online; serta (4) Merumuskan strategi mitigasi teknis dan arsitektur pengamanan berlapis (defense-in-depth) untuk mencegah eksploitasi berulang pada infrastruktur web perguruan tinggi.

II. METODE PENELITIAN

Penelitian ini mengadopsi metodologi audit keamanan kuantitatif berbasis kerangka kerja Open Source Security Testing Methodology Manual (OSSTMM) dan NIST SP 800-115 yang diselaraskan dengan standar OWASP Top 10. Tahapan penelitian mencakup pengumpulan informasi target (reconnaissance), pemindaian kerentanan (vulnerability assessment), validasi pengujian penetrasi pasif, pemodelan skor risiko CVSS v3.1, dan penyusunan strategi remediasi.

2.1 Target Audit dan Ruang Lingkup Pengujian

Pengujian dilakukan pada 15 target sub-domain aktif di lingkungan perguruan tinggi, mencakup portal utama kampus, sistem informasi akademik (SIKAD), portal jurnal ilmiah (Open Journal Systems/OJS), portal penerimaan mahasiswa baru (PMB), website fakultas, sistem informasi alumni,

repository perpustakaan, dan portal layanan helpdesk IT. Seluruh pengujian dilakukan secara terkontrol pada lingkungan uji tanpa merusak ketersediaan layanan produksi.

2.2 Kerangka Kerja OWASP Top 10

Taksonomi kerentanan diklasifikasikan ke dalam kategori risiko keamanan aplikasi web OWASP Top 10, yang mencakup:

1. A01:2021 - Broken Access Control: Celah otorisasi yang memungkinkan pengguna tanpa hak istimewa mengakses direktori server, mengubah URL, atau mengunggah berkas terlarang.
2. A02:2021 - Cryptographic Failures: Ketiadaan enkripsi data sensitif dalam transit, sertifikat SSL kedaluwarsa, atau hilangnya security headers.
3. A03:2021 - Injection: Celah penanganan input pengguna yang tidak disanitasi sehingga memicu eksekusi kode tak terduga, seperti SQL Injection dan Cross-Site Scripting (XSS).
4. A05:2021 - Security Misconfiguration: Konfigurasi bawaan server yang longgar, pengaktifan directory listing, pesan galat verbose, dan penggunaan kata sandi default.
5. A06:2021 - Vulnerable and Outdated Components: Penggunaan platform CMS, modul plugin, atau pustaka JavaScript yang memuat celah keamanan publik yang belum ditambah.

2.3 Perhitungan Metrik CVSS v3.1

Penilaian risiko kuantitatif dihitung menggunakan formula Common Vulnerability Scoring System (CVSS) v3.1 Base Metrics. Skor dasar (Base Score) diperoleh dari agregasi sub-skor Exploitability dan Impact:

$$\text{Exploitability} = 8.22 \times AV \times AC \times PR \times UI \quad (1)$$

di mana AV adalah Attack Vector, AC adalah Attack Complexity, PR adalah Privileges Required, dan UI adalah User Interaction. Sub-skor Impact dihitung berdasarkan dampak kerahasiaan (C), integritas (I), dan ketersediaan (A) melalui Impact Sub-Score (ISS):

$$ISS = 1 - \left[(1 - \text{Impact}_C) \times (1 - \text{Impact}_I) \times (1 - \text{Impact}_A) \right] \quad (2)$$

Jika parameter Scope bernilai Unchanged, sub-skor Impact dihitung dengan formula pada Persamaan (3):

$$\text{Impact} = 6.42 \times ISS \quad (3)$$

Skor Dasar CVSS v3.1 ditentukan dengan rumus pembulatan standar:

$$\text{BaseScore} = \text{RoundUp}(\min(\text{Impact} + \text{Exploitability}, 10)) \quad (4)$$

Tingkat keparahan (Severity) dikategorikan ke dalam 5 tingkatan: None (0.0), Low (0.1–3.9), Medium (4.0–6.9), High (7.0–8.9), dan Critical (9.0–10.0).

III. HASIL DAN PEMBAHASAN

Hasil asesmen keamanan komprehensif berhasil mengungkap vektor eksploitasi nyata yang digunakan sindikat siber dalam meluncurkan serangan web defacement konten judi online.

3.1 Kuantifikasi Temuan Kerentanan Berdasarkan CVSS v3.1

Tabel 1 menyajikan hasil kuantifikasi skor keparahan risiko CVSS v3.1 untuk lima temuan kerentanan paling signifikan yang ditemukan pada infrastruktur web perguruan tinggi.

Tabel 1. Kuantifikasi Skor Kerentanan CVSS v3.1 pada Target Audit

Kode	Kategori OWASP Top 10	Target Terdampak	Vektor Serangan	Skor CVSS	Tingkat Risiko	Dampak pada Web Defacement
VULN-01	A03: Injection	Portal PMB & SIM-Alumni	Network	9.8	Critical	Pengambilalihan hak akses basis data administrator dan ...
VULN-02	A01: Broken Access Control	Portal Jurnal OJS & LMS	Network	8.8	High	Unggah backdoor webshell PHP untuk menyisipkan landing ...
VULN-03	A06: Vulnerable Components	Website Fakultas & LPPM	Network	7.5	High	Penyisipan tautan tersembunyi (hidden backlinks SEO) da...
VULN-04	A05: Security Misconfiguration	Portal Utama & Helpdesk IT	Network	6.5	Medium	Pemaparan berkas konfigurasi server (.env, config.inc.p...
VULN-05	A02: Cryptographic Failures	Semua Sub-domain (15 Website)	Network	4.2	Medium	Ketiadaan CSP dan X-Frame-Options memfasilitasi clickja...

Berdasarkan Tabel 1, temuan kerentanan paling berbahaya adalah VULN-01 (SQL Injection) dengan skor CVSS 9.8 (Kategori Critical). Celah ini memungkinkan penyerang mengekstraksi hash kata sandi administrator dari basis data tanpa otentikasi awal (PR: None) melalui injeksi kueri pada parameter filter portal PMB. Setelah akun admin dikuasai, penyerang memiliki hak istimewa penuh untuk memodifikasi konten artikel dan menyisipkan tabel halaman promosi judi.

Temuan VULN-02 (Arbitrary File Upload) pada sistem jurnal OJS mencatatkan skor CVSS 8.8 (Kategori High). Celah ini terjadi akibat validasi ekstensi berkas yang hanya dilakukan pada sisi klien (client-side validation), sehingga penyerang dapat mengunggah berkas skrip PHP berbahaya (webshell) berkedok naskah artikel (misal: paper_manuscript.php.pdf). Webshell tersebut bertindak sebagai pintu belakang (backdoor) yang memberikan akses terminal perintah (command execution) untuk memodifikasi berkas index.php server.

3.2 Rekapitulasi Status Keamanan 15 Website Kampus

Hasil rekapitulasi audit pada 15 website perguruan tinggi disajikan pada Tabel 2.

Tabel 2. Rekapitulasi Audit Keamanan Web pada 15 Sub-domain Kampus

Parameter Evaluasi Keamanan	Jumlah Website Terpapar	Persentase (%)	Tingkat Kritis	Rekomendasi Tindakan
Website dengan Kerentanan Critical (CVSS ≥ 9.0)	4	26.7%	Sangat Tinggi	Patching darurat dan isolasi modul terdampak dalam 24 jam
Website dengan Kerentanan High (CVSS 7.0 - 8.9)	7	46.7%	Tinggi	Pembaruan versi CMS dan pembersihan skrip backdoor
Ketiadaan Content Security Policy (CSP)	13	86.7%	Sedang	Konfigurasi header CSP untuk blokir skrip eksternal

Parameter Evaluasi Keamanan	Jumlah Website Terpapar	Persentase (%)	Tingkat Kritis	Rekomendasi Tindakan
Ketiadaan HTTP Strict Transport Security (HSTS)	10	73.3%	Sedang	Pemaksaan enkripsi koneksi HTTPS menyeluruh
Ketiadaan Proteksi X-Frame-Options (Clickjacking)	12	80.0%	Sedang	Konfigurasi X-Frame-Options: SAMEORIGIN

Data pada Tabel 2 memperlihatkan bahwa 4 dari 15 website (26,7%) memiliki celah keamanan Critical yang sangat mendesak untuk ditangani. Selain celah tingkat aplikasi, kelemahan mendasar ditemukan pada layer konfigurasi keamanan HTTP (HTTP Security Headers). Sebanyak 86.7% website tidak mengimplementasikan Content Security Policy (CSP), sehingga peretas dapat dengan leluasa menyisipkan iframe atau memuat skrip iklan judi online dari peladen eksternal tanpa diblokir oleh peramban pengguna.

3.3 Kerangka Kerja Mitigasi Berlapis (Defense-in-Depth)

Berdasarkan hasil analisis kerentanan, dirumuskan strategi pertahanan terpadu yang mencakup empat lapisan pengamanan:

1. Lapisan Aplikasi (Secure Coding): Menerapkan Prepared Statements dan Parameterized Queries pada seluruh modul transaksi basis data guna mengeliminasi SQL Injection secara total. Mengimplementasikan validasi tipe MIME berbasis byte signature (magic bytes) pada server saat pemrosesan berkas unggahan.
2. Lapisan Konfigurasi Server: Menonaktifkan fitur directory indexing (Options -Indexes), menyembunyikan banner server, serta mengaktifkan HTTP Security Headers lengkap (CSP, HSTS, X-Content-Type-Options: nosniff, dan X-Frame-Options: SAMEORIGIN).
3. Lapisan Jaringan & Pemantauan: Mengintegrasikan Web Application Firewall (WAF) berbasis cloud (seperti Cloudflare atau ModSecurity) untuk memblokir kueri injeksi berbahaya secara in-line dan mendeteksi anomali trafik.
4. Manajemen Operasional: Melakukan pembaharuan berkala (patch management) pada platform CMS (WordPress, OJS) dan mencabut hak akses plugin pihak ketiga yang tidak lagi didukung oleh pengembang resmi.

IV. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa kelemahan keamanan pada website perguruan tinggi berdomain .ac.id menjadi pemicu utama maraknya kasus web defacement bermotif promosi judi online. Audit pada 15 sub-domain kampus mengungkap keberadaan celah kritis, mencakup SQL Injection (CVSS 9.8), Arbitrary File Upload (CVSS 8.8), dan komponen CMS usang (CVSS 7.5). Sebanyak 4 website terpapar risiko Critical dan 86.7% belum mengaktifkan proteksi Content Security Policy.

Kuantifikasi risiko berbasis CVSS v3.1 terbukti efektif memberikan panduan prioritas bagi tim IT kampus dalam mengalokasikan sumber daya perbaikan teknis. Implementasi kerangka pengamanan defense-in-depth yang memadukan secure coding, penguatan konfigurasi server, dan penerapan WAF menjadi solusi fundamental untuk melindungi reputasi dan integritas akademik institusi.

Saran untuk penelitian selanjutnya adalah mengembangkan sistem monitoring defacement otomatis berbasis machine learning yang mampu memindai anomali perubahan berkas web (file integrity monitoring) dan mendeteksi injeksi kata kunci judi online secara real-time.

DAFTAR PUSTAKA

- Ahmad, I., Bashari, M., & Rahim, A. (2021). Performance analysis of web application vulnerability scanners against OWASP Top 10 vulnerabilities. *IEEE Access*, 9, 124502–124515. <https://doi.org/10.1109/ACCESS.2021.3110291>
- Aktama, G. E., & Pramudia, A. (2024). Analisis kerentanan keamanan website perguruan tinggi terhadap serangan web defacement. *Jurnal Logika*, 12(2), 75–88.
- Al-Zewairi, M., Almajali, S., & Aloqaily, M. (2020). Deep learning for network intrusion detection systems: A systematic review. *Journal of Network and Computer Applications*, 150, 102502. <https://doi.org/10.1016/j.jnca.2019.102502>
- Badan Siber dan Sandi Negara. (2022). *Laporan tahunan monitoring keamanan siber Indonesia 2022*. BSSN RI.
- FIRST. (2020). *Common vulnerability scoring system version 3.1: Specification document*. Forum of Incident Response and Security Teams. <https://www.first.org/cvss/v3.1/specification-document>
- Hasan, M. A., & Marlina, L. (2022). Analisis kerentanan keamanan sistem informasi akademik menggunakan kerangka kerja OWASP. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 6(4), 578–585. <https://doi.org/10.29207/resti.v6i4.4172>
- Katias, K. E., Aktama, G. E., & Simbolon, R. (2026). Perancangan aplikasi sistem informasi akademik Universitas Parna Raya Manado berbasis Android. *Jurnal Logika*, 14(1), 6–17.
- Kurniawan, B., & Suhartono, S. (2022). Evaluasi kerentanan SQL injection dan cross-site scripting pada aplikasi web e-government. *Jurnal Media Informatika Budidarma*, 6(1), 320–328. <https://doi.org/10.30865/mib.v6i1.3520>
- Montolalu, M. T., & Ekel, C. E. (2026). Pengaruh celebrity endorsement dan affiliate marketing terhadap keputusan pembelian produk fashion. *Jurnal Logika*, 14(1), 1–5.
- NIST. (2020). *Technical guide to information security testing and assessment (NIST SP 800-115)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-115>
- OWASP Foundation. (2021). *OWASP Top 10: The ten most critical web application security risks*. OWASP Foundation. <https://owasp.org/Top10/>
- Pratama, A., & Adiya, M. H. (2023). Pengujian penetrasi dan mitigasi kerentanan arbitrary file upload pada aplikasi Open Journal Systems. *Jurnal Sistem Informasi dan Informatika (SIMIKA)*, 6(2), 115–124.
- Putra, D. A., & Wibowo, S. (2021). Implementasi Web Application Firewall (WAF) ModSecurity untuk mitigasi serangan web defacement. *Jurnal Informatika Terpadu*, 7(2), 65–74. <https://doi.org/10.54315/jite.v7i2.148>
- Rahmad, C., & Susetyo, Y. A. (2022). Analisis post-incident web defacement situs pemerintah menggunakan digital forensics. *Jurnal Buana Informatika*, 13(2), 121–131. <https://doi.org/10.24002/jbi.v13i2.5641>
- Scarfone, K., & Mell, P. (2020). An analysis of CVSS version 2 vulnerability metrics. In *Third International Symposium on Empirical Software Engineering and Measurement (ESEM 2009)* (pp. 516–527). IEEE. <https://doi.org/10.1109/ESEM.2009.5316048>
- Simbolon, R., & Aktama, G. E. (2025). Evaluasi dan analisis user interface website Sibunga menggunakan metode User Centered Design. *Jurnal Logika*, 13(2), 1–15.
- Utomo, D. P., & Purba, B. (2021). Analisis keamanan website berbasis CMS WordPress terhadap serangan SQLi dan Brute Force. *Jurnal Riset Komputer (JURIKOM)*, 8(4), 210–218. <https://doi.org/10.30865/jurikom.v8i4.3210>
- Wibawa, A. P., & Purnomo, M. H. (2021). Cybersecurity maturity model for academic institutions based on ISO/IEC 27001 standard. *International Journal of Information Security and Privacy*, 15(3), 45–62.