EVALUASI PENGUJIAN KERENTANAN *WEBSITE* UNIVERSITAS DI SURABAYA MENGGUNAKAN OWASP TOP 10 DENGAN PENDEKATAN BLACKBOX

Dimaz Aidil Firdaus[1)], Mochammad Hasnan Al Abiyyu[2)], Ahmad Ghozi Darmawan[3)], Yusuf Amrozi[4)]
[1,2,3,4]Prodi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sunan Ampel Surabaya

Correspondence author: D.A.Firdaus, didimvanlast@gmail.com, Surabaya, Indonesia

Abstract

Advances in web technology drive the need for digital system security, including academic websites that are vulnerable to cyberattacks. This study aims to analyze the vulnerabilities of a university website in Surabaya using the OWASP Top 10 standards and black-box penetration testing. Testing was conducted by analyzing HTTP configuration, SSL/TLS, malware, DNS, and email security. The results indicate dominant vulnerabilities in the Security misconfiguration and Security logging and monitoring failures categories, with an F grade for HTTP Security headers, support for legacy TLS protocols, and the absence of SPF and DMARC. Thirty-seven potential malware files were also identified. Key recommendations include system updates, enhanced security configurations, and the implementation of email authentication policies to improve the cyber resilience of academic websites.

Keywords: website, vulnerabilities, OWASP Top 10, blackbox, university

Abstrak

Kemajuan teknologi web mendorong kebutuhan akan keamanan sistem digital, termasuk pada *website* akademik yang rentan terhadap serangan siber. Penelitian ini bertujuan menganalisis kerentanan sebuah *website* universitas di Surabaya berdasarkan standar OWASP Top 10 menggunakan metode *black-box penetration testing*. Pengujian dilakukan melalui analisis konfigurasi HTTP, SSL/TLS, *malware*, serta keamanan DNS dan *email*. Hasil menunjukkan kerentanan dominan pada kategori *Security misconfiguration* dan *Security logging and monitoring failures*, dengan nilai F pada HTTP *Security headers*, dukungan protokol TLS lama, serta ketiadaan SPF dan DMARC. Ditemukan pula 37 file potensial *malware*. Rekomendasi utama meliputi pembaruan sistem, penguatan konfigurasi keamanan, dan penerapan kebijakan autentikasi *email* untuk meningkatkan ketahanan siber *website* akademik.

Kata Kunci: kerentanan, *website*, OWASP Top 10, blackbox, universitas

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 06 NOMOR 01 JANUARI 2026
ISSN 2774 – 5775 | eISSN 2774-5767

A. PENDAHULUAN

Kemajuan teknologi informasi telah menawarkan berbagai infrastruktur dan layanan, dengan internet sebagai salah satu contoh yang paling dominan pada saat ini. Kehadiran internet dan ragam teknologi informasi lainnya telah membawa kemudahan yang nyata bagi berbagai aspek aktivitas manusia (Paramitha et al., 2023). Dan kini, internet bukan lagi sekadar kemewahan, melainkan pondasi penting dalam keseharian, seiring dengan meroketnya inovasi teknologi digital (Alimuddin, 2021).

Salah satu dari kemajuan teknologi informasi dalam bentuk internet yang sering digunakan di kalangan masyarakat yaitu *website*. Kehadiran *website* telah menjadi fondasi utama bagi layanan digital, baik untuk dunia bisnis, pendidikan, maupun organisasi. Namun, tidak dapat dipungkiri, bahwa setiap inovasi dalam teknologi sistem informasi hampir selalu diikuti oleh munculnya bentuk-bentuk baru risiko keamanan yang perlu diwaspadai (Sutabri et al., 2024).

Website yang bersifat publik dan mudah diakses membuatnya rentan menjadi sasaran empuk bagi aksi peretasan oleh pihak yang tidak bertanggung jawab. Menurut lanskap keamanan siber indonesia tahun 2023, Ancaman yang muncul sangat beragam, termasuk kebocoran data, *defacement*, serangan DDoS, dan *ransomware*. Hal ini memaksa dilakukannya langkah-langkah pemantauan proaktif guna mengantisipasi dampak yang lebih luas (Bagaskara et al., 2025).

Oleh karena itu standar kepatuhan keamanan hadir untuk mencegah hal tersebut terjadi. Beberapa kerangka kerja yg berfungsi sebagai tolak ukur bagi para profesional seperti ISO, ISSAF, NIST CSF, dan OWASP. Di tengah perubahan yang terus-menerus di dunia keamanan siber, tetap mengikuti panduan yang sudah mapan saat melakukan uji penetrasi adalah cara terbaik untuk memastikan hasilnya efektif dan bisa diandalkan.

Urgensi untuk melakukan pengecekan keamanan *website* menjadi semakin tinggi karena ancaman siber bersifat dinamis. Kerentanan yang dianggap sepele dapat berkembang menjadi pintu masuk serangan serius ketika muncul metode eksploitasi baru. Oleh sebab itu, organisasi tidak bisa sekadar membangun *website*, tetapi harus melakukan evaluasi berkala melalui pengujian kerentanan (*vulnerability assessment*) dan pengujian penetrasi (*penetration testing*).

Beberapa penelitian di Indonesia membuktikan urgensi ini. Misalnya, analisis pada aplikasi web pemerintah daerah menunjukkan masih ditemukannya kerentanan *Broken Authentication* dan *Cross-Site Scripting* (XSS), meskipun *website* tersebut sudah digunakan secara publik (Armando & Rosalina, 2023). Hal serupa juga terungkap pada penelitian terhadap situs pemerintah di desa Curug, di mana kategori *Security misconfiguration* dan *Sensitive Data Exposure* mendominasi hasil evaluasi (Hilda et al., 2024). Fakta-fakta ini memperlihatkan bahwa tanpa adanya pengujian keamanan secara rutin, risiko serangan akan selalu terbuka. Karena hal tersebut penelitian ini dilakukan dengan tujuan untuk menganalisis potensi kerentanan dan menyusun langkah-langkah mitigasi bagi suatu *website* akademik di Surabaya berdasarkan OWASP TOP 10.

OWASP atau Open Web Application Security Project merupakan suatu komunitas global yang memfokuskan peningkatan keamanan suatu perangkat lunak (Sugara & Sriyasa, 2024). OWASP Top 10 merupakan salah satu hasil yang paling populer dan unggul. OWASP Top 10 menjadi standar yang unggul dalam keamanan aplikasi web karena sifatnya yang dinamis dan kolaboratif serta secara rutin diperbarui untuk mengantisipasi ancaman yang terus berubah, dengan pembaharuan terakhir dirilis pada tahun 2021. Sebagai proyek *open-source* yang dapat diakses secara gratis, OWASP Top 10 merupakan sumber daya yang sangat berharga, khususnya bagi organisasi yang beroperasi dengan anggaran terbatas (Arief et al., 2025). OWASP Top 10 pada dasarnya

adalah daftar yang terus diperbarui, memetakan sepuluh jenis kerentanan paling berisiko dalam aplikasi web. Panduan ini membantu developer dan tim keamanan untuk fokus pada celah-celah yang paling sering dieksploitasi oleh penyerang dan harus segera ditangani (Yusuf & Suharsono, 2023).

Dengan implementasi rekomendasi yang dihasilkan menggunakan OWASP Top 10, tingkat risiko keamanan dapat dikendalikan sehingga integritas dan keandalan *website* tersebut semakin meningkat. Upaya ini diharapkan mampu meningkatkan standar keamanan dalam setiap aktivitas penggunaan *website* tersebut.

B. METODE PENELITIAN

Penelitian ini menerapkan metodologi *penetration testing* melalui pendekatan *blackbox*. Pendekatan tersebut mensimulasikan sudut pandang seorang penyerang eksternal yang sama sekali tidak memiliki akses atau gambaran tentang struktur infrastruktur sistem target (Yunanri W. et al., 2021). Penelitian ini memiliki tiga keterbatasan utama: 1) fokusnya yang sempit pada kerentanan OWASP Top 10 berisiko melewatkan celah keamanan lainnya, 2) metode *black-box* tanpa akses kode sumber yang membatasi analisis, 3) dan ruang lingkup pengujian yang hanya mencakup domain xyz.ac.id dan bukan infrastruktur Universitas XYZ secara utuh.

Tahapan penelitian dapat dilihat pada gambar 1.

Gambar 1. Tahapan Metode Penelitian

Studi Literatur

Tahap awal penelitian ini yaitu melakukan pelaksanaan studi literatur. Penelitian ini bertujuan untuk membangun landasan teoritis dengan mengkaji berbagai referensi yang relevan. Sumber data diperoleh dari beragam materi, seperti publikasi ilmiah, jurnal, serta sumber daring terpercaya.

Identifikasi Kerentanan

Menurut OWASP Foundation (2021), terdapat sepuluh vulnerabilitas (kerentanan) paling umum terjadi pada web dan aplikasi diantaranya:

1. A01:2021 *Broken Access Control* – Kontrol akses yang tidak efektif memungkinkan pengguna mengakses data atau fungsi di luar izin mereka.
2. A02:2021 *Cryptographic Failures* – Kesalahan dalam penggunaan kriptografi, misalnya tidak mengenkripsi data sensitif atau menggunakan algoritma usang.
3. A03:2021 Injection – Serangan melalui input berbahaya (SQL, NoSQL, OS *command*, dll.) yang dieksekusi sistem.
4. A04:2021 *Insecure Design* – Kelemahan dari tahap desain aplikasi, kurangnya *threat modeling*, dan tidak adanya prinsip desain aman.
5. A05:2021 *Security misconfiguration* – Konfigurasi default, *error messages* berlebihan, atau setting tidak aman yang membuka celah serangan.
6. A06:2021 *Vulnerable and Outdated Components* – Penggunaan *library*, *framework*, atau *software* yang sudah usang/rentan.
7. A07:2021 *Identification and Authentication Failures* – Kegagalan mekanisme login, *session management*, atau otentikasi yang lemah.
8. A08:2021 *Software and data integrity failures* – Tidak adanya verifikasi integritas *software*/data, termasuk kesalahan dalam CI/CD atau *update software*.
9. A09:2021 *Security logging and monitoring failures* – Minimnya

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 06 NOMOR 01 JANUARI 2026
ISSN 2774 – 5775 | eISSN 2774-5767

logging/monitoring membuat serangan sulit terdeteksi dan direspons.

10. A10:2021 Server-Side Request Forgery (SSRF) – Aplikasi dimanipulasi untuk membuat request ke domain internal/eksternal yang berbahaya.

Pengujian Kerentanan

Pada fase ini pelaksanaan pengujian kerentanan adalah dengan menilai konfigurasi keamanan yang dapat diketahui dari luar (*black-box* testing), tanpa akses langsung ke *server*. Menggunakan beberapa tools untuk setiap kerentanan.

Tabel 1. Area dan Tools yang diterapkan

Area Testing	Tools/Metode yang Digunakan
Deteksi komponen dan framework website	Wappalyzer, WPScan, Wordfence
Pemeriksaan HTTP Security Headers	securityheaders.com
Testing sertifikat dan konfigurasi SSL/TLS	Qualys SSL Labs
Pemindaian konten terhadap malware	Quttera, Sucuri SiteCheck
Deteksi kerentanan umum	OWASP ZAP, HostedScan
Pemeriksaan DNS & keamanan email	ImmuniWeb, MXToolbox

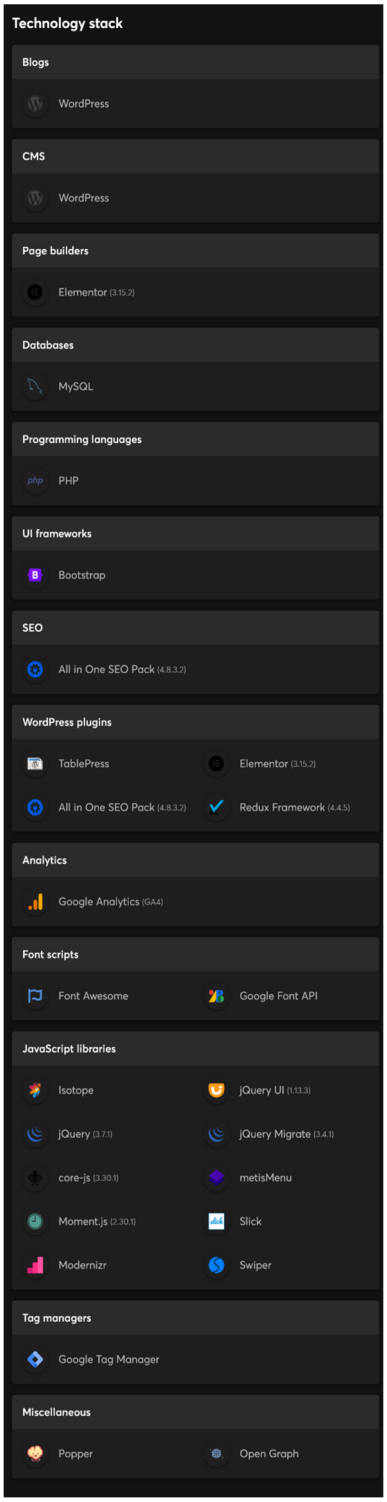
setiap kerentanan yang berhasil diungkap dengan merujuk pada standar kategorisasi dalam OWASP Top 10.

C. HASIL DAN PEMBAHASAN

Berdasarkan pengujian keamanan yang telah dilakukan pada salah satu *website* perguruan tinggi di Surabaya, dengan serangkaian tool dan metode, ditemukan beberapa aspek teknis dan kerentanan yang perlu menjadi perhatian penting. Berikut adalah beberapa hasil dan pembahasan mendetail untuk setiap bagian area pengujian.

Deteksi komponen dan *framework*

Pengujian ini dilakukan dengan menggunakan Wappalyzer untuk mengidentifikasi teknologi apa yang digunakan dalam *website*. Berdasarkan pemindaian, *website* xyz.ac.id ini dibangun menggunakan platform berikut:



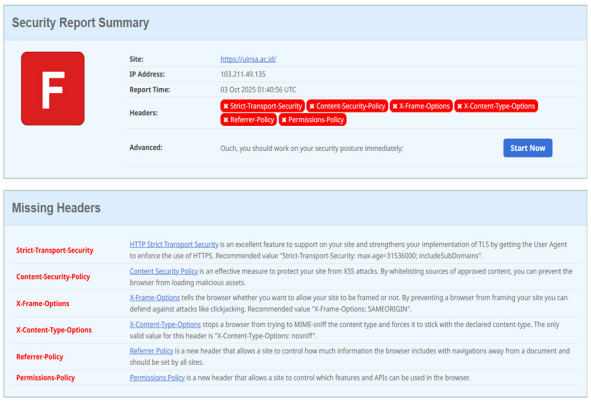
Gambar 2. Hasil Scan Wappalyzer

Pada gambar 2, diperlihatkan bahwa *website* akademik perguruan tinggi xyz.ac.id terdiri dari blogs yang berupa WordPress, CMS WordPress, Page builders berupa Elementor (3.15.2), Database MySQL, Bahasa pemrograman PHP, UI Framework Bootstrap, SEO All in One SEO Pack (4.8.3.2), Wordpress Plugin yang digunakan di antaranya (TablePress, All in One SEO Pack 4.8.3.2, Elementor 3.15.2, dan Redux Framework 4.4.5, kemudian untuk Analytics menggunakan Google Analytics GA4, Font Scripts yag digunakan adalah Font Awesome dan Google Font API, Library JavaScript yang digunakan antara lain (Isotop, jQuery 3.7.1, core-js 3.30.1, Moment.js 2.30.1, Modernizr, jQuery UI 1.13.3, jQuery Migrate 3.4.1, metisMenu, Slick, Swiper), Tag manager yang digunakan yaitu Google tag manager, dan Miscellaneous menggunakan Popper dan Open Graph.

Berdasarkan hasil penelusuran lebih lanjut menggunakan *website* WPScan dan Wordfence, tidak ditemukan informasi resmi yang menyebutkan adanya kerentanan spesifik pada versi-versi arsitektur yang teridentifikasi melalui pemindaian tersebut. Meskipun demikian, untuk menjaga keamanan dan stabilitas sistem, direkomendasikan agar pihak pengelola *website* senantiasa melakukan pembaruan (*update*) terhadap seluruh komponen, plugin, serta tema WordPress ke versi terbaru yang dirilis oleh pengembang resmi. Langkah tersebut penting sebagai bagian dari mitigasi proaktif terhadap potensi celah keamanan yang dapat muncul pada versi terdahulu.

Pemeriksaan HTTP *security headers*

Pemeriksaan ini dilakukan menggunakan securityheaders.com untuk menganalisis konfigurasi keamanan HTTP yang dikirim oleh *server*. Hasil pemeriksaan melalui layanan *Security headers* menunjukkan bahwa situs web menerima nilai F. Lebih detail hasil pemeriksaan dapat dilihat pada gambar 3.

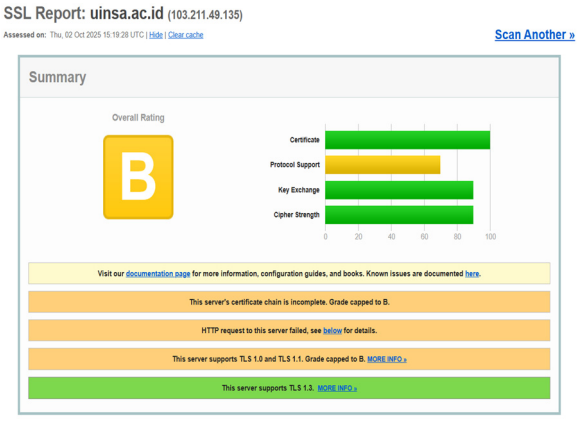


Gambar 3. Hasil Scan securityheaders

Hasil pemeriksaaan menunjukkan bahwa sejumlah besar HTTP Response Headers penting belum diterapkan. Strict-Transport-Security, Content-Security-Policy, X-FrameOptions, dan X-Content-Type-Options belum dikonfigurasi dengan benar. Serangan berbasis browser seperti cross-site scripting (XSS), *clickjacking*, dan MIME sniffing tidak dilindungi dengan baik oleh situs web dalam situasi ini. Hasil ini menunjukkan bahwa, dari perspektif implementasi keamanan, konfigurasi header keamanan harus diterapkan untuk mencegah ancaman di sisi klien.

Testing sertifikat dan konfigurasi SSL/TLS

Konfigurasi enkripsi *website* diuji dengan menggunakan Qualys SSL Labs untuk mengevaluasi kekuatan sertifikat SSL/TLS dan protokol yang didukung.



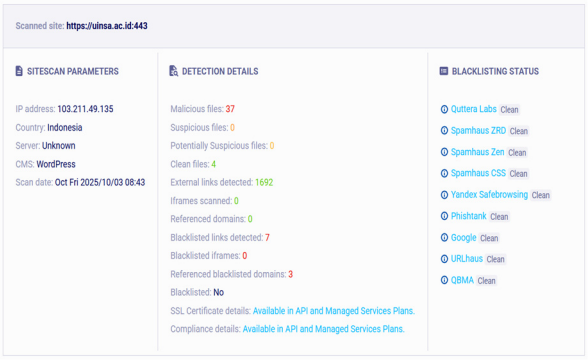
Gambar 4. Hasil Scan SSLLabs

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 06 NOMOR 01 JANUARI 2026
ISSN 2774 – 5775 | eISSN 2774-5767

Hasil uji Qualys SSL Labs menunjukkan bahwa situs tersebut menerima peringkat B. Sertifikat SSL dinyatakan valid, tetapi rantai sertifikat belum lengkap, dan dukungan untuk protokol lama seperti TLS 1.0 dan TLS 1.1 tidak disarankan saat ini. Meskipun TLS 1.3 telah digunakan dan suite cipher yang digunakan dianggap kuat, keberadaan protokol lama dapat menyebabkan serangan kriptografis menjadi lebih lemah. Hasil ini menunjukkan bahwa meskipun situs web memiliki sistem enkripsi yang cukup baik, konfigurasi masih perlu disesuaikan untuk mencapai tingkat keamanan terbaik sesuai dengan standar industri terbaru.

Pemindaian konten terhadap *malware*

Pemindaian dilakukan dengan Quttera untuk mendeteksi keberadaan file berbahaya, tautan mencurigakan, atau status blacklist pada domain.

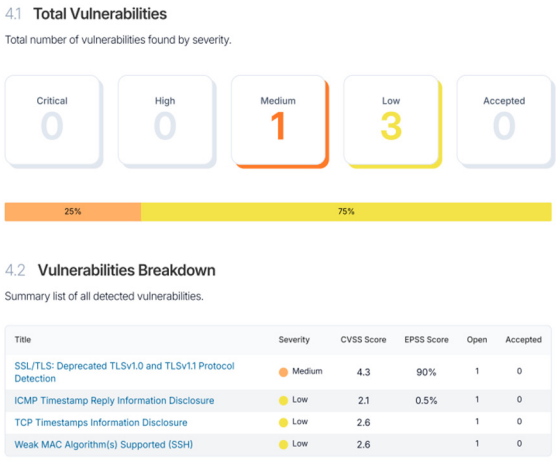


Gambar 5. Hasil Scan Quttera

Dengan menggunakan Quttera *Website Malware* Scanner, pemindaian situs menemukan 37 file yang mungkin berbahaya dan lebih dari 1.600 tautan eksternal. Platform yang digunakan berbasis WordPress biasanya memiliki banyak masalah jika tidak diperbarui secara berkala. Meskipun situs tersebut tidak tercantum dalam daftar hitam layanan keamanan terkemuka seperti Google Safe Browsing atau Phishtank, temuan ini menunjukkan bahwa ada kemungkinan bahwa skrip berbahaya atau aktivitas SEO spam injection telah dilakukan pada situs tersebut. Hasilnya menunjukkan bahwa audit keamanan internal harus dilakukan terhadap plugin, tema, dan file sistem untuk memastikan bahwa konten tetap murni dan mencegah eksploitasi lebih lanjut.

Deteksi kerentanan umum

Pemindaian kerentanan jaringan dan aplikasi dilakukan dengan menggunakan HostedScan untuk mengidentifikasi kelemahan umum.

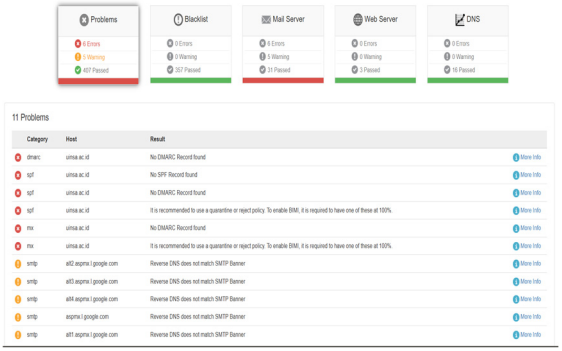


Gambar 6. Hasil Scan HostedScan

Ada satu kerentanan tingkat sedang dan tiga kerentanan tingkat rendah, menurut hasil evaluasi kerentanan melalui HostedScan. Hasilnya termasuk penggunaan protokol TLSv1.0/1.1 yang usang, penjelasan tentang timestamp ICMP dan TCP, dan penggunaan algoritma autentikasi lemah pada layanan SSH. Kerentanan-kerentanan ini mencakup kategori informasi sistem yang dapat digunakan oleh penyerang untuk melakukan fingerprinting atau serangan berbasis waktu (timing attack). Secara keseluruhan, temuan ini menunjukkan bahwa sistem telah relatif stabil, tetapi masih memungkinkan sejumlah vektor serangan yang perlu diperketat dengan mengubah konfigurasi *server*.

Pemeriksaan DNS dan keamanan *email*

Pemeriksaan ini menggunakan MXToolBox untuk menganalisis konfigurasi DNS dan rekam keamanan *email* seperti SPF, DKIM, dan DMARC. Hasil pemeriksaan dapat dilihat pada gambar 7.



Gambar 7. Hasil Scan MXToolbox

Terdapat enam kesalahan dan lima peringatan yang terkait dengan konfigurasi sistem surat elektronik domain, menurut pemeriksaan MX Toolbox. Ditunjukkan bahwa domain tidak memiliki catatan SPF, catatan DMARC, dan kesesuaian reverse DNS dengan identitas SMTP banner *server* pengirim *email*. Karena ketiadaan komponen tersebut, sistem *email* dapat digunakan untuk tindakan *spoofing* atau *phishing*, dan kemungkinan pesan masuk ke folder spam meningkat. Hasil ini menunjukkan bahwa elemen autentikasi *email* belum diterapkan dengan baik, dan penambahan kebijakan DNS diperlukan untuk meningkatkan reputasi dan keabsahan komunikasi elektronik domain.

Rekomendasi dan Mitigasi

Berdasarkan hasil pengujian dan pembahasan yang telah jelaskan, berikut rekomendasi dan mitigasi yang dapat diterapkan untuk meningkatkan keamanan *website* universitas tersebut:

1. Pembaruan dan Penguatan Komponen Arsitektur
   a. Perbarui semua plugin, tema, dan library (misalnya Elementor, Redux, All in One SEO Pack) ke versi terbaru untuk menutup celah keamanan yang sudah diketahui (Open Web Application Security Project (OWASP), 2021).
   b. Hapus atau nonaktifkan plugin atau tema yang tidak aktif untuk mengecilkan attack surface.
   c. Gunakan alat analisis dependensi atau software composition analysis untuk memantau kerentanan di dependensi luar.
2. Penguatan HTTP *Security headers*
   a. Terapkan Strict-Transport-Security (HSTS) agar browser selalu menggunakan HTTPS.
   b. Bangun dan aktifkan Content-Security-Policy (CSP) untuk membatasi sumber skrip dan mencegah injeksi skrip jahat.
   c. Gunakan X-Frame-Options (DENY atau SAMEORIGIN) untuk melindungi dari *clickjacking*.
   d. Tambahkan X-Content-Type-Options: nosniff untuk mencegah MIME sniffing (Allo & Widiasari, 2024).
3. Optimalisasi Konfigurasi SSL/TLS
   a. Nonaktifkan protokol lama seperti TLS 1.0 dan 1.1, hanya aktifkan TLS 1.2 atau 1.3.
   b. Pastikan rantai sertifikat (certificate chain) lengkap agar kepercayaan sertifikat tersambung penuh (Ali, 2021).
   c. Pilih cipher suites modern yang mendukung Perfect Forward Secrecy dan susun prioritas penggunaan cipher aman.
4. Pembersihan dan Audit Keamanan WordPress
   a. Gunakan plugin keamanan (misalnya Wordfence, Sucuri) untuk memindai dan membersihkan *malware*, skrip injeksi, atau backdoor.
   b. Verifikasi integritas file inti WordPress (misalnya dengan wp core verify-checksums) dan ganti kredensial akses (administrator, database, FTP).
   c. Audit tautan eksternal agar tidak mengarahkan ke sumber berbahaya atau digunakan untuk spam SEO.
5. Pengetatan Konfigurasi dan Layanan *Server*
   a. Tangani kerentanan yang ditemukan pada pengujian (misalnya ICMP timestamp disclosure, banner layanan yang membeberkan informasi)

dengan menonaktifkan layanan yang tidak perlu dan meminimalkan header informasi layanan (Putra & Santoso, 2025).

b. Untuk SSH, gunakan autentikasi berbasis kunci (key-based) dan menonaktifkan otentikasi berbasis kata sandi jika memungkinkan.
c. Terapkan firewall untuk membatasi akses hanya ke port yang diperlukan, serta sistem deteksi intrusi (IDS) atau fail2ban untuk mendeteksi upaya akses mencurigakan.

6. Implementasi Kebijakan Keamanan *Email*
   a. Tambahkan record SPF di DNS untuk menentukan *server* yang diizinkan mengirim *email* atas nama domain.
   b. Implementasikan DKIM dengan menandatangani *email* secara digital agar pesan dapat diverifikasi keasliannya.
   c. Konfigurasikan DMARC dengan kebijakan quarantine atau reject agar *email* yang gagal verifikasi tidak diterima begitu saja, serta memungkinkan pelaporan aktivitas mencurigakan.
   d. Pastikan reverse DNS (PTR record) sesuai dengan banner SMTP untuk meningkatkan reputasi pengiriman *email*.

D. PENUTUP

Berdasarkan pengujian *penetration testing black-box* berstandar OWASP Top 10, penelitian ini berhasil memetakan kerentanan pada sebuah *website* akademik suatu universitas di Surabaya. Dua kategori kerentanan paling menonjol adalah A05:2021 *Security misconfiguration* dan A09:2021 *Security logging and monitoring failures*. Temuan utamanya yaitu: (1) Gagal mengimplementasikan HTTP *Security headers* (skor 'F') yang berisiko terhadap serangan XSS dan *clickjacking*, (2) Konfigurasi SSL/TLS yang lemah karena masih mengizinkan protokol usang (TLS 1.0/1.1), serta (3) Tidak adanya kebijakan keamanan *email* (SPF dan DMARC) yang membuka celah untuk *spoofing* dan *phishing*. Selain itu, terdeteksi 37 file yang diduga *malware*, yang berpotensi diklasifikasikan sebagai A08:2021 *Software and data integrity failures*. Sebagai rekomendasi, diperlukan pembaruan arsitektur, pengetatan konfigurasi *server*, pembersihan *malware*, dan implementasi kebijakan keamanan *email* yang lebih *robust*.

Keberhasilan penelitian ini didukung oleh kerangka kerja OWASP Top 10 yang diakui secara global dan kemampuan untuk mendeteksi teknologi *website* target dari luar. Namun, metodologi *Black-box* menjadi penghambat karena keterbatasan akses ke kode sumber berpotensi menyebabkan beberapa kerentanan internal tidak dapat di identifikasi. Tantangan yang lain yaitu ancaman siber yang terus berkembang, sehingga pengujian keamanan harus dilakukan secara berkelanjutan, bukan insidental. Secara keseluruhan, temuan ini memberikan arahan yang jelas bagi mitra untuk melakukan perbaikan proaktif yang bertujuan untuk meningkatkan keamanan *website* akademiknya.

E. DAFTAR PUSTAKA

Alimuddin, A. (2021). Penggunaan Internet dan Peluang Berwirausaha di Indonesia. *JKB : Jurnal Kewirausahaan Dan Bisnis*, *26*(2), 112–121. https://doi.org/10.20961/jkb.v26i2.50913

Arief, M. I., Anwar, D. S., & Supriatman, A. (2025). Analisis Kerentanan Website Melalui Pendekatan Penetration Testing Berdasarkan Standar Owasp Top 10 Studi Kasus Simpelmas Universitas XYZ. *JEIS: Jurnal Elektro Dan Informatika Swadharma*, *5*(2), 93–104. https://doi.org/10.56486/jeis.vol5no2.798

Armando, Y., & Rosalina. (2023). Penetration Testing Tangerang City Web Application With Implementing OWASP Top 10 Web Security Risks Framework. *JISA : Jurnal*

Informatika Dan Sains, *6*(2), 105–109. https://doi.org/10.31326/jisa.v6i2.1656

Bagaskara, B. A., Idhom, M., & Wahanani, H. E. (2025). Pengujian Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing dan Owasp Top 10. *JIRE : Jurnal Informatika & Rekayasa Elektronika*, *8*(1), 40–50. https://doi.org/10.36595/jire.v8i1.1375

Hilda, S. D., Heryana, N., & Ridha, A. A. (2024). Website Security Analysis Curug Village Government Using Open Web Application Security Project (OWASP). *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3S1), 3951–3958. https://doi.org/10.23960/jitet.v12i3S1.5236

Paramitha, D. I., Farauqi, M. D. A. Al, & Tyas, I. K. D. (2023). Literasi Digital Pengguna Internet Indonesia Guna Mewujudkan Budaya Damai di Ruang Mayantara. *Jurnal Kewarganegaraan*, *7*(1), 292–304. https://doi.org/10.31316/jk.v7i1.5308

Sugara, V. I., & Sriyasa, I. W. (2024). Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP). *The Indonesian Journal of Computer Science*, *13*(2), 3315–3327. https://doi.org/10.33022/ijcs.v13i2.3736

Sutabri, T., Wijaya, A., Herdiansyah, M. I., & Negara, E. S. (2024). Evaluasi Risiko Celah Keamanan Aplikasi E-Office menggunakan Metode OWASP. *Edumatic: Jurnal Pendidikan Informatika*, *8*(1), 113–122. https://doi.org/10.29408/edumatic.v8i1.25463

Yunanri W., Anto, R., Yuwono, D. T., & Yuliadi. (2021). Deteksi Serangan Vulnerability Pada Open Journal System Menggunakan Metode Black-Box. *JIRE : Jurnal Informatika & Rekayasa Elektronika*, *4*(1), 68–77. https://doi.org/10.36595/jire.v4i1.365

Yusuf, R. R., & Suharsono, T. N. (2023). Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk. *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi Dan Teknik*, 402–413. https://doi.org/10.32897/sobat.2023.5.0.3132