ISSN: 2477-0078

Pengujian dan Analisis Kerentanan Keamanan Website Fakultas Teknik Universitas Islam Madura Menggunakan OWASP ZAP, Burp Suite, dan Nikto .

Moh. Khosiri [1], Hoiriyah [2], Anwari [3]
[1,2,3]Sistem Informasi, Fakultas Teknik, Universitas Islam Madura
[1]mkhosirir@gmail.com, [2]hoiriyah.file.uim@gmail.com, [3]anwari.uim@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada website Fakultas Teknik Universitas Islam Madura dengan menggunakan tiga tools pengujian keamanan web, yaitu OWASP ZAP, Burp Suite, dan Nikto. Proses dimulai dengan pengumpulan informasi target menggunakan teknik reconnaissance, kemudian dilanjutkan dengan pemindaian dan analisis kerentanan. OWASP ZAP digunakan untuk mendeteksi celah seperti XSS (Cross-Site Scripting) dan CSRF, Burp Suite digunakan untuk menganalisis lalu lintas HTTP/HTTPS dan menguji input form terhadap serangan injeksi, sementara Nikto berfungsi mendeteksi kerentanan server seperti konfigurasi yang tidak aman dan direktori tersembunyi. Hasil pengujian menunjukkan bahwa website masih memiliki beberapa celah keamanan, seperti open directory, informasi sensitif yang dapat diakses publik, serta potensi serangan XSS. Berdasarkan temuan tersebut, disusun rekomendasi peningkatan keamanan web, termasuk konfigurasi ulang server, pembaruan sistem, dan validasi input pada sisi pengguna. Penelitian ini diharapkan dapat menjadi acuan bagi pengelola sistem informasi di lingkungan pendidikan tinggi dalam meningkatkan ketahanan keamanan website dari potensi serangan siber.

Kata Kunci: Keamanan Web, OWASP ZAP, Burp Suite, Nikto, Website Fakultas Teknik, Kerentanan.

ABSTRACT

This study aims to identify and analyze security vulnerabilities on the website of the Faculty of Engineering at Universitas Islam Madura using three web security testing tools: OWASP ZAP, Burp Suite, and Nikto. The process begins with reconnaissance techniques to gather information about the target, followed by vulnerability scanning and analysis. OWASP ZAP is used to detect issues such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), Burp Suite is utilized to analyze HTTP/HTTPS traffic and test form inputs for injection attacks, while Nikto functions to detect server vulnerabilities such as insecure configurations and hidden directories. The testing results indicate that the website still contains several security gaps, including open directories, publicly accessible sensitive information, and potential XSS attack vectors. Based on these findings, recommendations were developed to improve web security, including server reconfiguration, system updates, and user-side input validation. This research is expected to serve as a reference for information system administrators in higher education institutions to enhance website security resilience against potential cyberattacks.

***Keywords**: Web Security, OWASP ZAP, Burp Suite, Nikto, Faculty Website, Vulnerability.*

.

ISSN: 2477-0078

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah menjadikan website sebagai salah satu media utama dalam penyebaran informasi, komunikasi, dan pelayanan publik, terutama di lingkungan perguruan tinggi. Website institusi pendidikan tinggi umumnya menyimpan dan mengelola data penting, baik untuk kebutuhan akademik, administrasi, maupun layanan mahasiswa. Oleh karena itu, keamanan website menjadi faktor krusial guna melindungi data dan menjaga reputasi institusi dari potensi ancaman siber.

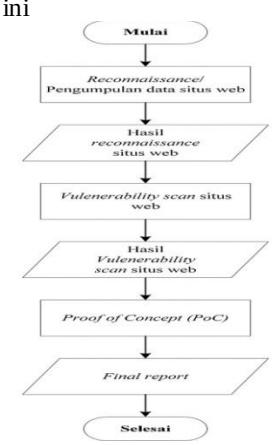
Namun demikian, banyak institusi pendidikan, termasuk perguruan tinggi di Indonesia, belum sepenuhnya menyadari pentingnya pengujian keamanan secara berkala. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), serangan siber di sektor pendidikan menunjukkan peningkatan signifikan dari tahun ke tahun, terutama melalui celah kerentanan aplikasi web (BSSN, 2023). Salah satu pendekatan untuk mengidentifikasi potensi celah keamanan tersebut adalah melalui *Penilaian kerentanan*, yaitu proses sistematis dalam mengevaluasi kerentanan yang ada pada suatu sistem.

Penelitian ini berfokus pada pengujian keamanan website Fakultas Teknik Universitas Islam Madura menggunakan tiga tools yang banyak digunakan dalam keamanan aplikasi web, yaitu OWASP ZAP, Burp Suite, dan Nikto. Ketiga tools ini mewakili metode pengujian yang berbeda namun saling melengkapi, seperti pemindaian otomatis (Nikto), *proxy interception* dan *manual testing* (Burp Suite), serta *passive-active scan* (OWASP ZAP) yang dapat mendeteksi celah umum seperti *Cross-Site Scripting (XSS)*, *SQL Injection*, dan *misconfiguration*.

Tujuan dari penelitian ini adalah untuk melakukan evaluasi terhadap tingkat keamanan website melalui tiga tools tersebut, mendokumentasikan jenis-jenis kerentanan yang ditemukan, serta memberikan rekomendasi yang tepat untuk meningkatkan keamanan sistem. Dengan adanya penelitian ini, diharapkan pengelola sistem informasi di institusi pendidikan dapat lebih proaktif dalam melakukan audit keamanan secara rutin sebagai langkah pencegahan terhadap serangan siber.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus, yaitu dengan melakukan pengujian terhadap website milik Instansi XYZ secara langsung untuk mengidentifikasi celah keamanan yang mungkin ada. Studi kasus ini bertujuan untuk menggambarkan penerapan *vulnerability assessment* secara nyata pada sebuah sistem website, sehingga hasil yang diperoleh dapat dijadikan dasar rekomendasi keamanan sistem informasi. Dengan diagram penelitian ini



Gambar 1.*Diagram Alur Penelitian*

2.1 Pengumpulan Data (Reconnaissance)

Pada tahap awal proses *Vulnerability Assessment*, dilakukan aktivitas reconnaissance, yaitu pengumpulan informasi awal terhadap target situs untuk memahami infrastruktur dan teknologi yang digunakan. Dalam penelitian ini, pengumpulan data dilakukan terhadap situs https://ft.uim.ac.id menggunakan tiga tools utama, yaitu Nmap, Wappalyzer, dan SSL Labs.

a. Pengumpulan Data dengan Nmap
   Nmap digunakan untuk melakukan pemindaian port, layanan yang berjalan, dan estimasi sistem operasi yang digunakan oleh server target.
b. Pengumpulan Data dengan Wappalyzer (Ekstensi Browser)
   Untuk mengetahui komponen teknologi pada sisi aplikasi, dilakukan profiling dengan Wappalyzer, yang memberikan informasi mendetail mengenai arsitektur sistem dan framework yang digunakan.
c. Pengumpulan Data dengan SSL Labs
   Untuk menilai keamanan koneksi HTTPS, dilakukan pengujian menggunakan Qualys

ISSN: 2477-0078

SSL Labs terhadap beberapa IP yang diasosiasikan dengan situs tersebut.

2.2 Tahap Vulnerability Scan

Setelah dilakukan pengumpulan data (*reconnaissance*), tahap selanjutnya dalam *vulnerability assessment* adalah pemindaian kerentanan (vulnerability scan). Tahap ini bertujuan untuk mengidentifikasi celah-celah keamanan yang terdapat pada sistem aplikasi web target. Dalam proses ini, tiga tools populer dan saling melengkapi digunakan, yaitu OWASP ZAP, Burp Suite, dan Nikto.

OWASP ZAP (Zed Attack Proxy)
OWASP ZAP digunakan untuk melakukan pemindaian otomatis terhadap aplikasi web berbasis WordPress yang digunakan situs ft.uim.ac.id.

a. *Burp Suite*
   Burp Suite digunakan dalam mode manual dan semi-otomatis untuk mengintersepsi lalu lintas dan menguji berbagai parameter input dari sisi klien (client-side testing).
b. *Nikto*
   Nikto digunakan sebagai scanner berbasis command-line yang fokus pada pemindaian direktori, file berbahaya, konfigurasi default, dan potensi kebocoran informasi.

2.3 Proof of Concept (PoC)

Setelah kerentanan berhasil diidentifikasi melalui proses *vulnerability scanning* menggunakan OWASP ZAP, Burp Suite, dan Nikto, langkah selanjutnya adalah melakukan Proof of Concept (PoC). Tahapan ini bertujuan untuk membuktikan bahwa kerentanan yang ditemukan benar-benar dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Pada penelitian ini, dilakukan PoC terhadap kerentanan Cross-Site Scripting (XSS), Clickjacking, dan uji template kerentanan otomatis dengan Nuclei.

2.4 Penyusunan Rekomendasi Perbaikan

Berdasarkan hasil analisis, disusun rekomendasi teknis sebagai panduan pengelola sistem untuk meningkatkan keamanan website.

3. HASIL DAN PEMBAHASAN

2.1 Hasil Reconnaissance

Hasil pengumpulan data dilakukan terhadap situs https://ft.uim.ac.id menggunakan tiga tools utama, yaitu Nmap, Wappalyzer, dan SSL Labs.

a. Pengumpulan Data dengan Nmap
   Nmap digunakan untuk melakukan pemindaian port, layanan yang berjalan, dan estimasi sistem operasi yang digunakan oleh server target. Dari hasil pemindaian, diketahui bahwa situs ft.uim.ac.id memiliki beberapa port yang terbuka, yaitu:

Tabel 1. ***Hasil Informasi Umum Website ft.uim.ac.id dari NMAP***

Keterangan	*Hasil*
Target	ft.uim.ac.id
IP yang discan	104.21.96.1
Host Status	Up (aktif), latency: 0.015s
Proteksi	Menggunakan Cloudflare Proxy
Jarak Jaringan	8 hop (berarti berada di luar jaringan lokal/publik)
Sertifikat SSL	Diterbitkan oleh Google Trust Services untuk *.uim.ac.id

Selain itu, server dilindungi oleh Cloudflare sebagai reverse proxy dan *content delivery network* (CDN). Estimasi sistem operasi menunjukkan kemungkinan besar menggunakan Linux Kernel versi 3.x, dan jenis perangkat teridentifikasi sebagai general-purpose server.

ISSN: 2477-0078

b. Pengumpulan Data dengan Wappalyzer (Ekstensi Browser)
Untuk mengetahui komponen teknologi pada sisi aplikasi, dilakukan profiling dengan Wappalyzer, yang memberikan informasi mendetail mengenai arsitektur sistem dan framework yang digunakan. Hasilnya sebagai berikut:

Tabel 2. Hasil Informasi Umum Website ft.uim.ac.id dari Wappalyzer

Kategori	Teknologi yang Digunakan
CMS (Platform)	WordPress
Tema WordPress	Hello Elementor
Plugin WordPress	Elementor, JetEngine
Bahasa Pemrograman	PHP
Basis Data	MySQL
CDN & Keamanan	Cloudflare (termasuk reverse proxy dan proteksi SSL/TLS)
SSL/TLS	Aktif, Sertifikat dari Google Trust Services
Analytics	Google Analytics
JavaScript Libraries	jQuery, jQuery Migrate, Underscore.js, Slick
UI Framework	Elementor (drag & drop builder)
HTTP Protocol	HTTP/3

Hasil ini menunjukkan bahwa sistem berbasis WordPress dengan banyak dependensi pada plugin pihak ketiga, yang dapat menjadi vektor serangan potensial jika tidak di-*update*.

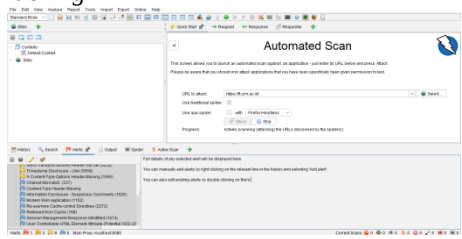
c. Pengumpulan Data dengan SSL Labs
Untuk menilai keamanan koneksi HTTPS, dilakukan pengujian menggunakan Qualys SSL Labs terhadap beberapa IP yang diasosiasikan dengan situs tersebut. Hasil pengujian menunjukkan bahwa semua IP mendapatkan grade B, yang berarti terdapat konfigurasi TLS yang belum maksimal.

Nilai "B" ini menunjukkan bahwa meskipun sertifikat valid dan terenkripsi, konfigurasi server belum memenuhi standar tinggi (A+), karena kemungkinan faktor seperti cipher suite lemah, tidak adanya HSTS, atau dukungan terhadap protokol lama.

2.2 Hasil Vulnerability Scan

Tahap ini bertujuan untuk mengidentifikasi celah-celah keamanan yang terdapat pada sistem aplikasi web target. Dalam proses ini, tiga tools populer dan saling melengkapi digunakan, yaitu OWASP ZAP, Burp Suite, dan Nikto.

a Hasil Pemindaian dengan OWASP ZAP
Pengujian dengan OWASP ZAP dilakukan menggunakan fitur *Automated Scan* serta *Spidering*.



Gambar 2. *Tampilan Pemindaian dengan OWASP ZAP*

Berdasarkan Gambar diatas hasil uji keamanan menggunakan OWASP ZAP, ditemukan beberapa kerentanan penting pada website yang perlu segera ditindaklanjuti untuk mencegah potensi penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Kerentanan pertama adalah Cross-Site Scripting (XSS) yang ditemukan pada halaman pencarian dan formulir kontak. Hal ini terjadi karena input dari pengguna tidak disaring atau disanitasi dengan baik sebelum ditampilkan kembali ke halaman web. Jika tidak diperbaiki, kerentanan ini dapat dimanfaatkan untuk menyisipkan skrip berbahaya, yang berisiko mencuri data pengguna atau mengarahkan pengguna ke situs palsu. Risiko ini tergolong sedang hingga tinggi.

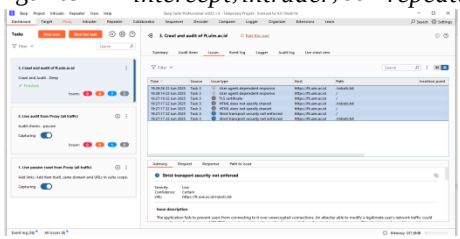
ISSN: 2477-0078

Selanjutnya, ditemukan bahwa website belum menerapkan header keamanan secara lengkap, seperti X-Content-Type-Options, X-Frame-Options, dan Content-Security-Policy. Header ini berfungsi untuk mencegah sejumlah serangan berbasis browser seperti sniffing konten atau clickjacking. Ketiadaan header ini tergolong risiko rendah, namun tetap penting untuk keamanan jangka panjang.

Kerentanan ketiga adalah tidak adanya CSRF token pada formulir login. Tanpa token ini, website rentan terhadap Cross-Site Request Forgery, yaitu serangan yang dapat menyebabkan tindakan tidak sah dilakukan oleh pengguna yang sedang login. Risiko dari celah ini tergolong sedang, karena berkaitan langsung dengan keamanan akun pengguna.

b Hasil Pemindaian dengan Burp Suite

Burp Suite digunakan untuk *manual testing* dengan teknik *intercept*, *intruder*, dan *repeater*.



Gambar 3 . ***tampilan Pemindaian dengan Burp Suite***

Dari Gambar diatas Hasil pemeriksaan terhadap website https://ft.uim.ac.id menunjukkan bahwa secara umum situs ini sudah menggunakan sertifikat HTTPS yang valid, namun masih ditemukan beberapa kelemahan pada sisi konfigurasi keamanan dasar. Pertama, server memberikan respon berbeda berdasarkan user-agent yang digunakan. Hal ini bisa dimanfaatkan oleh pihak tidak bertanggung jawab untuk menyembunyikan aktivitas berbahaya atau melewati deteksi keamanan. Kedua, halaman HTML pada situs ini tidak mendefinisikan jenis karakter (charset) seperti UTF-8. Tanpa charset yang jelas, browser dapat menebak sendiri encoding-nya, yang dapat membuka peluang terhadap serangan XSS, terutama di browser lama. Ketiga, situs belum menerapkan HTTP Strict Transport Security (HSTS). Tanpa HSTS, pengguna bisa saja diarahkan secara paksa ke versi HTTP yang tidak aman, sehingga rentan terhadap serangan man-in-the-middle.

c Hasil Pemindaian dengan Nikto

Gambar 4.*Tampilan Pemindaian dengan Nikto*

Berdasarkan Gambar diatas hasil pemindaian dengan tool Nikto, ditemukan bahwa website ft.uim.ac.id telah menggunakan SSL/TLS yang valid dan aman untuk komunikasi data terenkripsi. Namun, terdapat beberapa kelemahan dari sisi keamanan header HTTP yang belum diimplementasikan. Beberapa header penting seperti *Strict-Transport-Security*,*Content-Security-Policy, Permissions-Policy, X-Content-Type-Options, dan Referrer-Policy* belum tersedia. Ketiadaan header ini dapat menyebabkan risiko seperti serangan XSS, sniffing konten, hingga kebocoran informasi referrer.Selain itu, situs ini menggunakan kompresi deflate yang dapat membuka peluang terhadap serangan BREACH, yaitu serangan yang memanfaatkan ukuran respon data terenkripsi untuk menebak informasi sensitif. Pemindaian juga menunjukkan bahwa server berada di balik Cloudflare, dan menyebabkan beberapa koneksi diblokir, sehingga proses pemindaian tidak selesai 100%. Hal ini umum terjadi karena Cloudflare melindungi situs dari pemindaian otomatis.

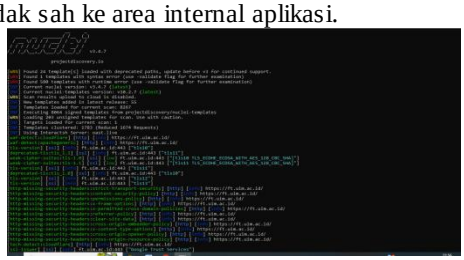
2.3 Hasil Proof of Concept (PoC)

Tahapan ini bertujuan untuk membuktikan bahwa kerentanan yang ditemukan benar-benar dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

Berdasarkan hasil pengujian serangan menggunakan *Nuclei* terhadap website ft.uim.ac.id, ditemukan beberapa indikasi kerentanan yang bersifat umum. Namun, dari seluruh skenario uji serang yang dilakukan, tidak ada satupun yang berhasil mendapatkan akses masuk ke dalam aplikasi web atau menembus autentikasi. Hal ini menunjukkan bahwa meskipun terdapat potensi celah

ISSN: 2477-0078

keamanan yang perlu diperbaiki, mekanisme proteksi saat ini masih mampu mencegah akses tidak sah ke area internal aplikasi.



Gambar 6. *Pengujian pakai Nuclei*

2.4 Rekomendasi Perbaikan

Berdasarkan hasil pengujian keamanan, terdapat beberapa langkah perbaikan penting yang perlu diterapkan untuk meningkatkan keamanan sistem. Pertama, aktifkan HSTS agar seluruh koneksi dipaksa melalui HTTPS dan mencegah *downgrade attack*. Kedua, gunakan versi TLS modern (minimal TLS 1.2) dan nonaktifkan versi lama. Ketiga, tambahkan header keamanan seperti *Content-Security-Policy*, *X-Frame-Options*, dan *Referrer-Policy* untuk mencegah XSS dan *clickjacking*.

Selain itu, perkuat keamanan cookie dengan atribut *Secure*, *HttpOnly*, dan *SameSite=Strict*. Terapkan pula perlindungan CSRF dengan token unik pada setiap form yang memodifikasi data. Hapus informasi **sensitif** dari header server seperti *X-Powered-By* dan gunakan pesan error generik. Terakhir, pastikan **semua** resource dimuat melalui HTTPS agar tidak terjadi *mixed content* yang dapat melemahkan enkripsi.

Penerapan rekomendasi ini secara keseluruhan akan memperkuat keamanan aplikasi web dan mengurangi risiko serangan siber yang umum terjadi.

4. KESIMPULAN

Pengujian keamanan pada website https://ft.uim.ac.id menggunakan OWASP ZAP, Burp Suite, Nikto, dan Nuclei berhasil mengidentifikasi sejumlah kerentanan seperti potensi serangan XSS, clickjacking, konfigurasi TLS yang belum optimal, serta ketiadaan beberapa header keamanan penting. Namun, hasil uji serangan (PoC) menunjukkan bahwa tidak ada skenario serangan yang berhasil mendapatkan akses ke dalam aplikasi web atau menembus autentikasi. Hal ini menandakan bahwa mekanisme proteksi yang ada masih mampu mencegah akses tidak sah, meskipun beberapa aspek teknis tetap memerlukan perbaikan segera. Dengan menerapkan rekomendasi seperti validasi input, penambahan header proteksi, penguatan konfigurasi TLS, dan manajemen sesi yang aman, keamanan website dapat ditingkatkan untuk meminimalkan risiko serangan siber di masa depan.

DAFTAR PUSTAKA

[1] S. Fitriani and A. Handayani, "Audit Keamanan Web Menggunakan Tools Burp Suite dan Nikto," *Jurnal Teknologi dan Sistem Komputer*, vol. 9, no. 3, pp. 214–221, 2021.

[2] A. Hidayat, "Penerapan Metode Vulnerability Assessment pada Website Menggunakan Nikto dan OpenVAS," *Skripsi*, Universitas Bina Sarana Informatika, 2021.

[3] R. D. Yuliani and A. Wibowo, "Evaluasi Keamanan Website Akademik dengan OWASP ZAP dan Metode Vulnerability Assessment," *Prosiding Seminar Nasional Sistem Informasi (SENASIF)*, vol. 2, no. 1, pp. 98–105, 2020.

[4] R. Alfian and M. A. Riyadi, "Analisis Keamanan Website Menggunakan OWASP ZAP (Studi Kasus: Website Universitas XYZ)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 6, no. 2, pp. 125–132, 2020.

[5] D. S. Nugroho, "Analisis Keamanan Web E-Commerce Menggunakan Burp Suite dan OWASP ZAP," *Skripsi*, Universitas AMIKOM Yogyakarta, 2019.

[6] A. R. Pratama, "Analisa Keamanan Situs Web Menggunakan OWASP Top 10," *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 16, no. 1, pp. 56–63, 2022.

[7] N. A. Rachmawati, "Penerapan Keamanan Aplikasi Web Berdasarkan Standar OWASP Top 10 Pada Website Sekolah," *Skripsi*, STMIK Nusa Mandiri, 2021. [8] L. Salsabila and I. Rahmat, "Analisis Keamanan Web dengan OWASP ZAP dan Nmap," *Jurnal Teknologi dan Informatika*, vol. 11, no. 1, pp. 90–98, 2022.

[9] M. A. Siregar, "Evaluasi Keamanan Web dengan Menggunakan Nikto dan SSL Labs

ISSN: 2477-0078

pada Website XYZ," *Tugas Akhir*, Politeknik Negeri Medan, 2023.

[10] M. R. Syahputra and H. Siregar, "Deteksi Kerentanan Website Menggunakan Metode Black Box dengan Tools Nikto dan Burp Suite," *Jurnal Mantik Penusa*, vol. 5, no. 2, pp. 240–248, 2021.