Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS

https://doi.org/10.35870/jimik.v6i1.1306

Analisis dan Rekomendasi Keamanan *Website* Kampus X Menggunakan ISSAF

Dio Wahyu Saputra [1*], Risqy Siwi Pradini [2], Mochammad Anshori [3]

[1*,2,3] Program Studi Informatika, Fakultas Teknologi dan Sains, Institut Teknologi, Sains, dan Kesehatan RS.DR. Soepraoen Kesdam V/BRW, Kota Malang, Provinsi Jawa Timur, Indonesia.

Corresponding Email: risqypradini@itsk-soepraoen.ac.id [1*]

Histori Artikel:
Dikirim 20 Desember 2024; *Diterima dalam bentuk revisi* 30 Desember 2024; *Diterima* 10 Januari 2025; *Diterbitkan* 20 Januari 2025.

Abstrak

Keamanan website institusi pendidikan menjadi isu kritis di era digital, terutama dengan meningkatnya ketergantungan pada layanan berbasis web. Penelitian ini mengevaluasi keamanan website Kampus X di Kota Malang menggunakan ISSAF (Information Systems Security Assessment Framework). Tahapan penelitian meliputi information gathering, network mapping, vulnerability identification, penetration testing. Pada tahap vulnerability identification, digunakan alat seperti OWASP ZAP dan Acunetix untuk mendeteksi celah keamanan aplikasi web. Hasil menunjukkan bahwa server telah menerapkan protokol TLS dengan konfigurasi keamanan dasar, namun terdapat sejumlah kerentanan, seperti port terbuka yang tidak diperlukan dan kekurangan dalam pengaturan header keamanan. Pemindaian menggunakan OWASP ZAP mengidentifikasi 24 alert keamanan, dengan 12,5% di antaranya masuk kategori risiko tinggi, termasuk SQL Injection dan kurangnya Content Security Policy (CSP). Selain itu, simulasi serangan DDoS menunjukkan ketahanan server, tetapi pengujian menunjukkan perlunya peningkatan keamanan pada aspek lain. Rekomendasi utama meliputi implementasi DNSSEC, penutupan port yang tidak digunakan, penambahan CSP header, dan peningkatan perlindungan terhadap serangan berbasis aplikasi web. Penelitian ini menegaskan pentingnya pendekatan holistik dan berkelanjutan dalam pengelolaan keamanan website, termasuk audit berkala dan pemantauan real-time. Dengan strategi ini, diharapkan institusi dapat memperkuat postur keamanan, melindungi aset digital, dan meminimalkan risiko serangan siber yang terus berkembang.

Kata Kunci: Evaluasi Keamanan; Website; ISSAF.

Abstract

The security of educational institution websites is critical in the digital era, especially with the increasing reliance on web-based services. This study evaluates the security of the Campus X website in Malang City using ISSAF (Information Systems Security Assessment Framework). The research stages include information gathering, network mapping, vulnerability identification, and penetration testing. At the vulnerability identification stage, tools such as OWASP ZAP and Acunetix detect security holes in web applications. The results show that the server has implemented the TLS protocol with basic security configuration. Still, several vulnerabilities exist, such as unnecessary open ports and deficiencies in the security header settings. Scanning using OWASP ZAP identified 24 security alerts, 12.5% of which were categorized as high risk, including SQL Injection and a lack of Content Security Policy (CSP). Additionally, DDoS attack simulations demonstrated server resilience, but testing showed the need for security improvements in other aspects. Key recommendations include implementing DNSSEC, closing unused ports, adding CSP headers, and improving protection against web application-based attacks. This research emphasizes the importance of a holistic and ongoing approach to website security management, including regular audits and real-time monitoring. With this strategy, institutions hope to strengthen their security posture, protect digital assets, and minimize the risk of ever-growing cyber attacks.

Keyword: Security Evaluation; Website; ISSAF.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

1. Pendahuluan

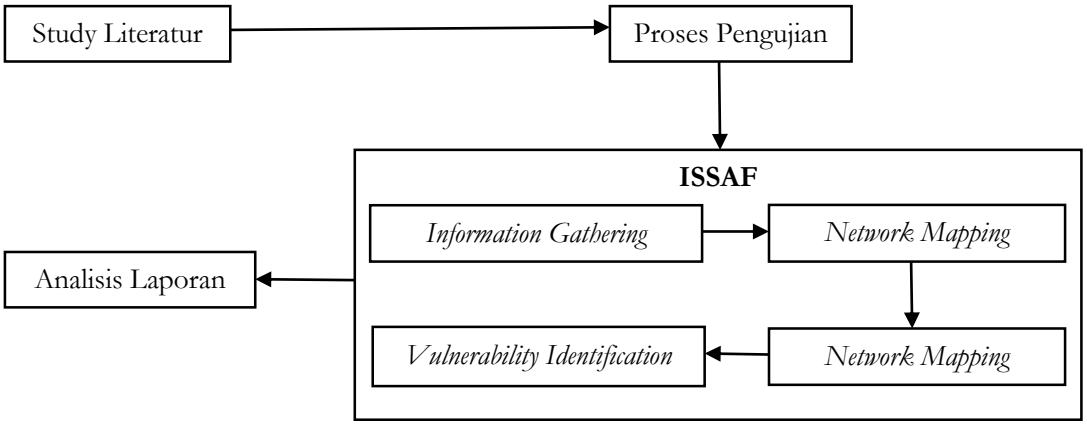
Di era digital saat ini, teknologi informasi telah menjadi elemen utama yang mendukung operasional dalam institusi pendidikan tinggi. Teknologi informasi telah mengubah secara fundamental cara pengelolaan dan penyediaan layanan akademik (Szymkowiak *et al.*, 2021). *Website* sebagai komponen vital dalam infrastruktur teknologi informasi kampus, memainkan peran krusial dalam mengelola berbagai layanan seperti sistem informasi akademik, perpustakaan digital, portal mahasiswa, dan sistem administrasi. Namun, seiring dengan peningkatan ketergantungan pada layanan berbasis *web*, ancaman keamanan siber terhadap institusi pendidikan juga mengalami eskalasi yang signifikan (Umar *et al.*, 2023)(Franchina *et al.*, 2021). Penelitian terdahulu mengungkapkan 78% institusi pendidikan telah mengalami setidaknya satu insiden keamanan siber dalam rentang waktu satu tahun terakhir, dengan *web server* menjadi target utama para penyerang (Nurelasari & Gumilang Al Farabi, 2024). Temuan ini diperkuat oleh studi yang mendemonstrasikan bahwa kerentanan pada *website* dapat mengakibatkan serangkaian konsekuensi serius, termasuk kebocoran data sensitif, gangguan layanan operasional, dan kerugian reputasi yang substansial bagi institusi pendidikan (Hariyadi & Nastiti, 2021)(Mishra *et al.*, 2021)(Eshetu *et al.*, 2024). Salah satu tantangan mendasar dalam keamanan *website* adalah kompleksitas sistem dan diversifikasi vektor serangan yang dapat dimanfaatkan oleh penyerang (Tara & W, 2023)(Singh *et al.*, 2021). Kondisi ini menjadi semakin mengkhawatirkan karena banyak institusi pendidikan belum sepenuhnya menerapkan konfigurasi keamanan yang optimal. Akibatnya, keamanan *website* menjadi isu yang sangat kritis, terutama mengingat tingginya sensitivitas data yang dikelola oleh institusi pendidikan (Asriyanik & Prajoko, 2018). Penelitian Silmina *et al.*, 2022 mengidentifikasi bahwa data akademik, informasi pribadi mahasiswa, dan data keuangan merupakan aset digital yang paling sering menjadi target serangan siber. Temuan ini didukung oleh penelitian Wijayanto & Firdonsyah (2024), yang mencatat peningkatan signifikan sebesar 40% dalam upaya peretasan yang secara spesifik menargetkan *website* institusi pendidikan dibandingkan dengan periode tahun sebelumnya.

Kampus X di Kota Malang merupakan institusi pendidikan yang mengelola data sensitif dari ribuan mahasiswa dan staf, sehingga memerlukan evaluasi keamanan *website* yang komprehensif dan berkelanjutan. Institusi pendidikan di Indonesia rata-rata mengalami peningkatan 50% dalam upaya serangan siber setiap tahunnya (Utomo & Rokhmah, 2022). Hal ini menekankan urgensi analisis keamanan berkala untuk mengidentifikasi dan memitigasi kerentanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab (Nadzirin & Nur, 2024)(Goni *et al.*, 2024). Untuk mengatasi tantangan keamanan yang semakin kompleks, ISSAF (*Information Systems Security Assessment Framework*) telah membuktikan efektivitasnya dalam mengidentifikasi dan mengevaluasi kerentanan keamanan *website* (Silmina *et al.*, 2022)(Sutabri *et al.*, 2024). Implementasi ISSAF dapat menghasilkan penilaian keamanan yang menyeluruh dan akurat (Rochman *et al.*, 2021). Efektivitas ISSAF untuk keamanan *website* telah divalidasi dan menunjukkan tingkat akurasi mencapai 85% dalam mengidentifikasi kerentanan kritis pada infrastruktur *web* (Herman *et al.*, 2023). Berdasarkan urgensitas permasalahan dan gap keamanan yang teridentifikasi, penelitian ini bertujuan untuk melakukan analisis keamanan *website* pada Kampus X Kota Malang dengan mengimplementasikan ISSAF secara mendalam. ISSAF digunakan untuk memberikan pendekatan terstruktur dan komprehensif dalam penilaian keamanan. Implementasi *framework* ini diharapkan dapat memberikan pemahaman mendalam tentang postur keamanan *website* institusi dan menghasilkan rekomendasi praktis yang dapat diimplementasikan untuk meningkatkan keamanan sistem. Penelitian ini menjadi semakin relevan mengingat peningkatan frekuensi dan kecanggihan serangan siber terhadap institusi pendidikan, serta kebutuhan untuk melindungi aset digital dan data sensitif yang dikelola oleh Kampus X Kota Malang. Diharapkan melalui penelitian ini dapat membantu Kampus X Kota Malang untuk lebih meningkatkan keamanan sistem *website* yang digunakan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

2. Metode Penelitian

Tahapan penelitian yang dilakukan pada penelitian ini adalah studi literatur, pengujian penetrasi menggunakan ISSAF serta analisis dan laporan. Adapun kerangka berpikir penelitian yang digunakan digambarkan pada Gambar 1.



Gambar 1. Kerangka Berpikir Penelitian

Tahap pertama yang dilakukan yaitu Studi Literatur. Pada tahap studi literatur, dilakukan kajian mendalam terhadap literatur yang relevan, termasuk jurnal, buku, dan sumber-sumber lain yang berhubungan dengan analisis keamanan *website* menggunakan ISSAF. Dari tahap ini didapatkan hasil bahwa ISSAF membuktikan efektivitasnya dalam mengidentifikasi dan mengevaluasi kerentanan keamanan *website*. Tahap kedua adalah Proses Pengujian, yang melibatkan penerapan ISSAF (*Information Systems Security Assessment Framework*). ISSAF adalah sebuah kerangka kerja terstruktur yang dirancang untuk menilai keamanan sistem informasi secara menyeluruh. Kerangka kerja ini menyediakan pendekatan yang sistematis untuk mengidentifikasi risiko keamanan, mengevaluasi efektivitas kontrol keamanan yang diterapkan, dan menyusun rencana perbaikan(Wijaya *et al.*, 2024). Dalam penelitian ini, ISSAF diterapkan untuk menganalisis kerentanan sistem secara langsung melalui praktik berbasis sistem operasi Kali Linux dan Windows. *Tools* dan teknik yang digunakan dalam implementasi metode ini dirangkum dalam Tabel 1.

Tabel 1. *Tools* yang Digunakan dalam Penelitian

No	Tahapan	*Source*	*Tools*
1.	*Information Gathering*	*Domain Info* SSL (*Source Socket Layer*)	Whois SSLscan
2.	*Network Mapping*	*Port Scanning, Service Detection,* dan *Network Info*	Nmap
3.	*Vulnerability Identification*	*Web Scanner Vulnerability* OWASP (*Security Scanning dan Analysis*)	Acunetix Owasp Zap Top 10
4.	*Penetration*	DDOS *Attack* Sql *Injection*	Low Orbit Ion Cannon(LOIC) Sqlmap

Tabel 1 diatas menunjukkan tahapan penelitian, penelitian ini menggunakan 4 tahapan mulai dari *infromation gathering, network mapping, vulnerability identification* dan yang terakhir yaitu *penetration testing.* Penelitian ini menggunakan berbagai *tools* keamanan siber yang diklasifikasikan berdasarkan tahapan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

dalam proses pengujian keamanan. Pada tahap *Information Gathering*, informasi terkait domain dan lapisan keamanan SSL (*Source Socket Layer*), diperoleh menggunakan *tool* seperti Whois untuk mendapatkan detail pendaftaran domain dan SSLscan untuk menganalisis konfigurasi SSL. Tahap selanjutnya adalah *Network Mapping*, yang bertujuan untuk memetakan layanan dan jaringan dengan melakukan *port scanning*, deteksi layanan (*service detection*), serta eksplorasi jaringan. *Tool* utama yang digunakan dalam tahap ini adalah Nmap, yang terkenal sebagai alat serbaguna untuk analisis jaringan. Tahap *Vulnerability Identification* bertujuan untuk mendeteksi kerentanan dalam aplikasi *web* dan infrastruktur jaringan. *Tools* yang digunakan meliputi Acunetix, yang merupakan pemindai kerentanan *web* otomatis, serta OWASP ZAP Top 10, yang memanfaatkan kerangka kerja OWASP (*Open Web Application Security Project*) untuk mengevaluasi potensi kerentanan berdasarkan standar keamanan aplikasi *web*. Acunetix dipilih karena kemampuannya sebagai pemindai otomatis yang dapat mendeteksi berbagai jenis kerentanan, termasuk *SQL Injection*, *Cross-Site Scripting* (XSS), dan kerentanan *konfigurasi server* (Shahid *et al.*, 2022). Acunetix juga dilengkapi dengan fitur pemetaan lengkap aplikasi *web*, deteksi kerentanan *zero-day*, serta laporan terperinci yang memudahkan prioritisasi perbaikan (Sarker *et al.*, 2023). OWASP ini menyediakan berbagai sumber daya, seperti panduan, alat, dan proyek, untuk membantu pengembang dan organisasi membangun aplikasi *web* yang aman (Idris *et al.*, 2022). Pemilihan alat seperti Acunetix dan OWASP ZAP dilakukan berdasarkan keunggulan spesifik yang dimiliki oleh masing-masing alat dalam mendukung identifikasi kerentanan aplikasi *web*. Meskipun alat lain seperti Nessus dan Nikto juga banyak digunakan dalam keamanan siber, keduanya memiliki fokus yang berbeda. Nessus lebih mengutamakan pemindaian kerentanan jaringan dan perangkat infrastruktur, sementara Nikto berfokus pada pengujian *server web*, seperti deteksi *file* atau konfigurasi yang tidak aman (Albalawi *et al.*, 2023). Dalam penelitian ini, yang menitikberatkan pada kerentanan aplikasi *web*, OWASP ZAP dan Acunetix dianggap lebih sesuai untuk mencapai tujuan penelitian. Pada tahap akhir, yaitu *Penetration*, berbagai serangan dilakukan untuk menguji sejauh mana kerentanan dapat dieksploitasi. Contohnya, serangan *Distributed Denial of Service* (DDOS *Attack*) dilakukan menggunakan *Low Orbit Ion Cannon* (LOIC), sementara kerentanan terhadap SQL *Injection* diuji menggunakan SQLmap, yang merupakan alat otomatis untuk eksploitasi *database* berbasis SQL. Tahap terakhir adalah Analisis Laporan, di mana hasil temuan dari implementasi ISSAF dianalisis secara mendalam. Proses ini mencakup evaluasi tingkat risiko serta penyusunan rekomendasi untuk perbaikan keamanan *website*. Diharapkan hasil analisis ini tidak hanya membantu meningkatkan keamanan *website* tetapi juga memberikan wawasan strategis untuk membangun sistem yang lebih tangguh terhadap ancaman siber di masa depan.

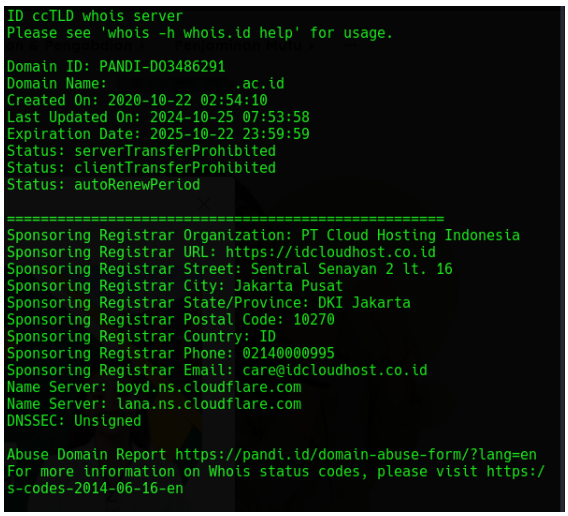
3. Hasil dan Pembahasan

3.1 Hasil

3.1.1 *Information Gathering*

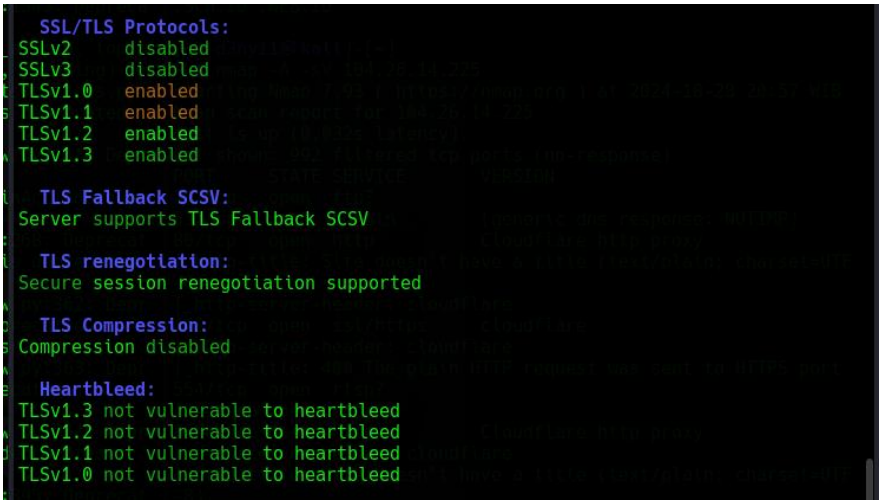
Pada tahap *information gathering*, peneliti melakukan pengumpulan informasi awal terkait *website* yang menjadi objek penelitian, yaitu domain *web* pada Kampus X. Pada tahap *information gathering* ini peneliti melakukan 2 tahapan yang pertama yaitu terkait *domain info* (pencarian informasi). Pada tahap ini bertujuan untuk mengidentifikasi detail teknis seperti informasi domain, status pendaftaran, alamat IP, serta konfigurasi dasar lainnya yang relevan untuk analisis keamanan. Tahap kedua yaitu *SSLscan* (memeriksa *protocol* keamanan) dalam tahap ini peneliti mencari informasi terkait penerapan protokol keamanan SSL pada domain yang menjadi objek penelitian. *Tools* yang digunakan dalam proses ini adalah whois dan SSlscan. Whois digunakan untuk mencari info terkait domain dari Kampus X, sedangkan SSLscan digunakan untuk mengetahui informasi terkait protokol keamanan dari *website* Kampus X. Hasil pencarian menggunakan Whois ditampilkan pada Gambar 2, sedangkan penerapan menggunakan SSLscan dapat ditampilkan pada Gambar 3. Hasil dari penerapan ini dapat digunakan sebagai bagian dari dokumentasi awal untuk mendukung langkah-langkah analisis berikutnya.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306



Gambar 2. Implementasi Whois

Berdasarkan Gambar 2, analisis Whois lookup dilakukan untuk memperoleh informasi terkait domain kampusX.ac.id. Hasil analisis menunjukkan beberapa informasi utama, yaitu: Domain ID: PANDI-D03486291, dengan *registrar* PT *Cloud Hosting* Indonesia, yang berlokasi di Sentral Senayan 2 Lt. 16, Jakarta Pusat, DKI Jakarta, Indonesia. *Registrar* ini menyediakan layanan melalui situs resmi https://idcloudhost.co.id, email care@idcloudhost.co.id, dan nomor telepon 02140000995. Domain kampusX.ac.id pertama kali terdaftar pada 22 Oktober 2020, pukul 02:54:10 WIB, dengan pembaruan terakhir dilakukan pada 22 Oktober 2024, pukul 07:53:58 WIB, dan masa kedaluwarsa hingga 22 Oktober 2025, pukul 23:59:59 WIB. Domain ini memiliki status *clientTransferProhibited*, yang menunjukkan bahwa domain dilindungi dari transfer tanpa izin, serta status *autoRenewPeriod*, yang menandakan domain berada dalam periode perpanjangan otomatis. Nama *server* yang digunakan adalah lana.ns.cloudflare.com dan boyd.ns.cloudflare.com, sementara mekanisme keamanan DNSSEC belum diterapkan dengan status *unsigned*. Informasi yang diperoleh dari Whois lookup ini sangat penting untuk memvalidasi kepemilikan domain, memastikan status aktif domain, dan mengevaluasi mekanisme keamanan yang diterapkan, seperti DNSSEC. Selain itu, proses ini juga berfungsi untuk mengidentifikasi *registrar* yang bertanggung jawab atas pengelolaan domain tersebut, yang merupakan elemen krusial dalam analisis keamanan domain secara komprehensif.



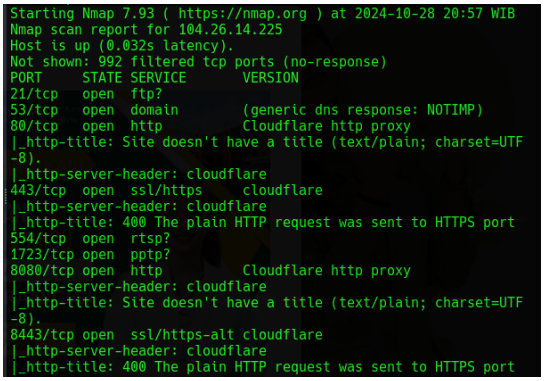
Gambar 3. Implementasi SSLscan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

Berdasarkan Gambar 3, dapat diidentifikasi bahwa hasil pemindaian menunjukkan domain *website* pada Kampus X telah menggunakan protokol TLS (*Transport Layer Security*) untuk meningkatkan keamanan komunikasi data. Implementasi TLS pada *server* ini mencakup berbagai versi protokol dengan status berikut: SSLv2 dan SSLv3 telah dinonaktifkan karena dianggap tidak lagi aman, sementara protokol TLSv1.0, TLSv1.1, TLSv1.2, dan TLSv1.3 masih diaktifkan. Dari semua versi yang diaktifkan, TLSv1.3 merupakan protokol terbaru dan paling aman, yang dirancang untuk mengatasi kelemahan pada versi sebelumnya. Selain itu, *server* mendukung mekanisme TLS *Fallback* SCSV (*Signaling Cipher Suite Value*) yang mencegah *downgrade attack* selama proses negosiasi protokol, memastikan hanya protokol yang aman digunakan. *Server* juga mengimplementasikan *secure session renegotiation*, yang menjamin keamanan selama sesi komunikasi yang diinisiasi ulang, sehingga terlindung dari serangan berbasis renegosiasi. Fitur TLS *Compression* telah dinonaktifkan untuk mencegah serangan seperti CRIME (*Compression Ratio Info-leak Made Easy*), yang memanfaatkan kelemahan kompresi data untuk mencuri informasi sensitif. Selanjutnya, analisis terhadap kerentanan *Heartbleed* menunjukkan bahwa *server* ini tidak rentan terhadap eksploitasi tersebut di semua versi TLS yang diaktifkan (1.0, 1.1, 1.2, dan 1.3). Hal ini menegaskan bahwa sistem telah diatur untuk mematuhi standar keamanan terkini, memastikan integritas, *autentikasi*, dan kerahasiaan komunikasi data yang dilakukan melalui *website* tersebut. Penerapan konfigurasi ini memberikan perlindungan yang signifikan terhadap ancaman keamanan siber sekaligus meningkatkan kepercayaan pengguna terhadap infrastruktur digital Kampus X.

3.1.2 *Network Mapping*

Tahap kedua adalah *network mapping* yang dilakukan menggunakan Nmap untuk mengidentifikasi *port* dan layanan aktif pada domain *website* dengan alamat IP 104.26.14.225. Rincian hasil pemindaian dapat dilihat pada Gambar 4.



Gambar 4. Implementasi Nmap

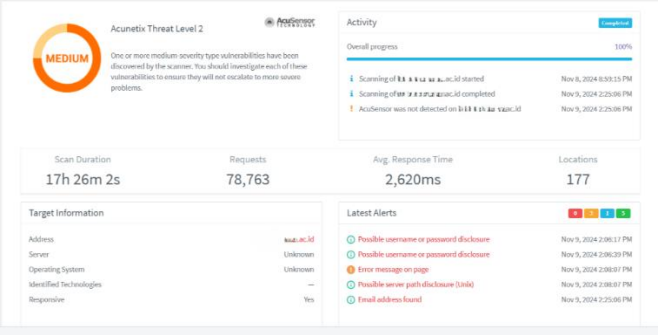
Berdasarkan hasil pemindaian pada Gambar 4 menunjukkan beberapa *port* terbuka pada *server* dengan alamat IP 104.26.14.225, yang mengindikasikan layanan tertentu. *Port* 21/tcp terdeteksi sebagai layanan FTP (*File Transfer Protocol*) yang aktif, menunjukkan dukungan *server* untuk *transfer file*. *Port* 53/tcp menunjukkan keberadaan layanan DNS (*Domain Name System*), yang digunakan untuk pengelolaan resolusi nama domain. Selanjutnya, *port* 80/tcp dan 8080/tcp mengindikasikan layanan HTTP yang berjalan melalui *proxy* Cloudflare, yang berfungsi untuk meningkatkan performa dan keamanan koneksi *web*. Selain itu, *port* 443/tcp dan 8443/tcp menunjukkan adanya layanan HTTPS (*Secure HTTP*) yang juga menggunakan Cloudflare sebagai *proxy*, memberikan enkripsi pada koneksi untuk melindungi data pengguna. *Port* lain yang terdeteksi adalah 554/tcp, yang menunjukkan layanan RTSP (*Real-Time Streaming Protocol*), kemungkinan digunakan untuk mendukung layanan *streaming* data secara *real-time*. Sementara itu, *port* 1723/tcp terdeteksi sebagai layanan PPTP (*Point-to-Point Tunneling Protocol*), yang biasanya digunakan untuk mendukung koneksi *Virtual Private Network* (VPN).

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

Hasil analisis ini menunjukkan bahwa *server* memiliki sejumlah layanan yang dikelola dengan dukungan Cloudflare untuk meningkatkan performa dan keamanan. Namun, keberadaan *port* terbuka, khususnya untuk FTP dan PPTP, dapat menjadi potensi risiko keamanan yang perlu dievaluasi lebih lanjut. Analisis ini memberikan gambaran komprehensif tentang layanan yang berjalan pada *server* dan menjadi dasar penting untuk pengelolaan keamanan jaringan secara menyeluruh

3.1.3 *Vulnerability Identification*

Tahap ketiga adalah *Vulnerability identification*. Pada tahap ini dilakukan 2 hal, yang pertama yaitu melakukan *Web Scanner Vulnerability* terhadap domain *website* pada Kampus X menggunakan Acunetix dan tahap kedua menerapkan penggunaan OWASP. Peneliti melakukan *scanning* terhadap *link website* Kampus X menggunakan OWASP ZAP Top 10. Proses *scanning acunetix* bertujuan untuk mengetahui tingkat kerentanan dari sistem *web* yang diuji. Adapun hasil dari *scanning acunetix* tersebut dapat dilihat pada Gambar 5.



Gambar 5. Implementasi pada Acunetix

Berdasarkan hasil pengujian yang telah dilakukan seperti pada gambar 5, domain *website* pada Kampus X berada pada level 2 (*Medium*). Hal ini menunjukkan adanya satu atau lebih kerentanan dengan tingkat risiko sedang. Sehingga perlu segera diperiksa agar tidak berkembang menjadi masalah yang lebih serius. Beberapa kerentanan yang teridentifikasi dalam laporan meliputi kemungkinan pengungkapan kredensial, seperti nama pengguna atau kata sandi, dengan dua kejadian yang terdeteksi. Selain itu, ditemukan pula pesan kesalahan yang terlihat pada halaman *web*, potensi pengungkapan jalur *server* pada sistem berbasis Unix, dan penemuan alamat *email* yang dapat dimanfaatkan oleh pihak tidak berwenang. Hasil pengujian ini menggarisbawahi bahwa meskipun sistem *web* pada domain tersebut menunjukkan *responsivitas* yang baik, masih terdapat potensi kerentanan yang membutuhkan langkah mitigasi lebih lanjut untuk meningkatkan tingkat keamanannya. Pada tahap pengujian OWASP peneliti melakukan *scanning* terhadap *link website* tujuan dengan menggunakan OWASP ZAP top10. Berikut adalah hasil dari *scanning* OWASP ZAP:

1) *Alert counts by risk and confidence*

Hasil dari *scanning* pada OWASP ZAP yang pertama adalah *alert counts by risk and confidence*. Berdasarkan hasil *scanning* hasil dari OWASP tentang "*Alert Counts by Risk and Confidence*," dapat dilihat pada Tabel 2.

Tabel 2. Hasil Scanning OWASP Zap *Alert Counts by Risk and Confidence*

		Confidence				
	Risiko	*User confirmed*	Tinggi	Sedang	Lemah	Total
1.	Tinggi	0(0,0%)	0(0,0%)	2(8,3%)	1(4,2%)	3(12,5%)
2.	Sedang	0(0,0%)	1(4,2%)	2(8,3%)	1(4,2%)	4(16,7%)
3.	Lemah	0(0,0%)	1(4,2%)	4(16,7%)	1(4,2%)	6(25,0%)
4.	Informasi	0(0,0%)	1(4,2%)	5(20,8%)	5(20,8%)	11(45,8%)
5.	Total	0(0,0%)	3(12,5%)	13(54,2%)	8(33,3%)	24(100%)

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

Tabel 2 di atas menunjukkan jumlah total *alert* sebanyak 24 *alert* yang terdeteksi. *Alert* diklasifikasikan berdasarkan tingkat risiko (*Risk*) dan tingkat keyakinan (*Confidence*). Tingkat risiko terbagi menjadi 4 kategori: Tinggi, Sedang, Lemah, dan Informasi. Tingkat keyakinan mencakup *User Confirmed*, Tinggi, Sedang, dan Lemah. Distribusi berdasarkan risiko menunjukkan bahwa kategori risiko ini memiliki jumlah *alert* tertinggi (11 *alert* atau 45,8% dari total). Mayoritas *alert* memiliki tingkat keyakinan "Sedang" dan "Lemah". Pada kategori Lemah didapatkan risiko 6 *alert* (25,0%), dan dominasi pada tingkat keyakinan "Sedang". Pada kategori Sedang didapatkan sebanyak 4 *alert* (16,7%) berada di kategori risiko ini, dengan distribusi keyakinan yang merata di setiap tingkatan. Pada kategori tinggi ini memiliki jumlah *alert* terendah, di dapatkan risiko sebanyak yaitu 3 *alert* (12,5%), dengan konsentrasi utama pada tingkat keyakinan "Sedang". Distribusi berdasarkan keyakinan dibuktikan dari frekuensi risiko, tingkat risiko sedang merupakan tingkat keyakinan tertinggi, dengan 13 *alert* (54,2% dari total), tingkat risiko lemah sebanyak 8 *alert* (33,3%) berada di tingkat keyakinan ini, tingkat risiko tinggi hanya 3 *alert* (12,5%) yang memiliki tingkat keyakinan tinggi. Untuk tingkat risiko u*ser confirmed*, tidak ditemukannya *alert* sehingga keyakinan ini (0 *alert*). Analisis khusus *alert* dengan risiko informasi dan keyakinan Sedang adalah yang paling banyak (20,8% dari total). Tidak ada *alert* dengan risiko Tinggi yang memiliki tingkat keyakinan Tinggi atau *user confirmed*, menunjukkan kemungkinan kesenjangan dalam validasi atau klasifikasi risiko. Kombinasi risiko Lemah dan keyakinan Sedang juga signifikan, mencerminkan kebutuhan untuk memvalidasi lebih lanjut kategori ini. Kesimpulan dan rekomendasi mayoritas *alert* berada pada risiko informasi, yang meskipun tidak mendesak, tetap memerlukan perhatian untuk memastikan bahwa potensi risiko rendah ini tidak terabaikan. *Alert* dengan risiko lebih tinggi seperti Tinggi atau Sedang memerlukan perhatian lebih besar, terutama untuk meningkatkan keyakinan validasi. Disarankan untuk melakukan tinjauan lebih lanjut pada *alert* dengan tingkat keyakinan "Lemah" untuk memvalidasi temuan dan mengurangi *false positives*.

2) *Alert counts by site and risk*
Hasil dari *scanning* pada OWASP ZAP yang kedua adalah *alert counts by side and risk*. Berdasarkan hasil *scanning* hasil dari OWASP tentang "*side and risk*," dapat dilihat pada tabel 3.

Tabel 3. Hasil *Scanning* OWASP Zap *Alert Counts by Site and Risk*

	Risk			
	Tinggi (= Tinggi)	Sedang (>= Sedang)	Lemah (> Lemah)	Informasi (>=informasi)
Site	3(3)	4(7)	6(13)	11(24)

Berdasarkan Tabel 3 di atas, hasilnya terbagi ke dalam beberapa kategori risiko berdasarkan tingkatannya, yaitu Tinggi yang diwakili dengan angka 3 (dengan total 3 risiko dalam kategori ini), Sedang yang diwakili dengan angka 4 (dengan total 7 risiko dalam kategori ini), Lemah yang diwakili dengan angka 6 (dengan total 13 risiko dalam kategori ini), dan Informasi yang diwakili dengan angka total 11 (dengan total 24 risiko/informasi terkait). Penilaian risiko ini dilakukan untuk menganalisis kerentanan keamanan informasi pada situs *web* tertentu, di mana setiap kategori memiliki ambang batas tertentu untuk mengevaluasi keparahan potensi risiko atau temuan. Pendekatan ini sering digunakan dalam keamanan siber untuk memprioritaskan langkah mitigasi yang sesuai.

3) *Alert counts by alert type*
Hasil dari *scanning* pada OWASP ZAP yang kedua adalah *alert counts by side and risk*. Berdasarkan hasil *scanning* dari metode OWASP tentang "*side and risk*", dapat di lihat pada Tabel 4.

Tabel 4. Hasil *Scanning* OWASP Zap Alert *Counts by Alert Type*

	Alert Type	*Risk*	*Count*
1.	Jalur Traversal	Tinggi	3 (12,5%)
2.	SQL Injection – Oracle- Time Based	Tinggi	3 (12,5)
3.	SQL Injection - SQLite	Tinggi	10 (41,7%)

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

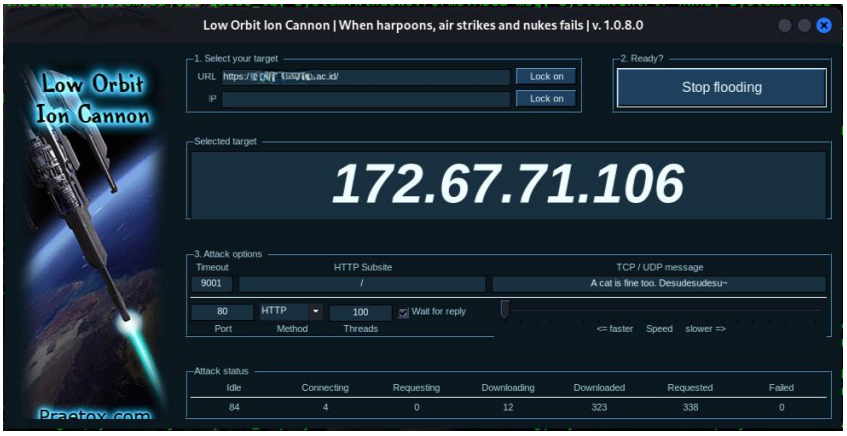
4.	Content Security Policy (CSP) Header Not Set	Sedang	418 (1.741,7%)
5.	Kesalahan konfigurasi lintas domain	Sedang	1 (4,2%)
6.	Missing Anti-clickjacking Header	Sedang	374 (1.558,3%)
7.	Tidak adanya Token Anti-CSRF	Sedang	14 (58,3%)
8.	Cookie with SameSite Attribute None	Lemah	8 (33,3%)
9.	Cross-Domain JavaScript Source File Inclusion	Lemah	420 (1.750,0%)
10.	Pengungkapan Timestamp - Unix	Lemah	37 (154,2%)
11.	Secure Pages Include Mixed Content	Lemah	60 (250,0%)
12.	Strict-Transport-Security Header Not Set	Lemah	2244 (9.350,0%)
13.	X-Content-Type-Options Header Missing	Lemah	1737 (7.237,5%)
14.	Authentication Request Identified	Informasi	4 (16,7%)
15.	Charset Mismatch	Informasi	126 (525,0%)
16.	Content-Type Header Missing	Informasi	1 (4,2%)
17.	GET for POST	Informasi	9 (37,5%)
18.	Keterbukaan Informasi - Komentar Mencurigakan	Informasi	881 (3.670,8%)
19.	Modern Web Application	Informasi	304 (1.266,7%)
20.	Re-examine Cache-control Directives	Informasi	919 (3.829,2%)
21.	Retrieved from Cache	Informasi	375 (1.562,5%)
22.	Session Management Response Identified	Informasi	16 (66,7%)
23.	User Agent Fuzzer	Informasi	12308 (51.283,3%)
24.	User Controllable HTML Element Attribute (Potential XSS)	Informasi	2 (8,3%)

Berdasarkan Tabel 4 di atas, terdapat beberapa risiko yang ditemui selama melakukan *scanning*. Diantaranya adalah risiko tinggi, sedang, lemah dan informasi. Merujuk pada Tabel 4 tersebut, pada tingkat risiko tinggi, ditemukan tiga jenis ancaman utama, yaitu Jalur *Traversal, SQL Injection* (*Oracle - Time-Based*), dan *SQL Injection* (*SQLite*), yang masing-masing menyumbang 12,5% dari total *alert*, dengan potensi serius terhadap eksploitasi sistem dan pengungkapan data sensitif. Pada tingkat risiko sedang, ancaman utama meliputi *Content Security Policy* (CSP) *Header Not Set*, dengan 418 temuan (1.741,7%), dan Kesalahan Konfigurasi Lintas Domain, dengan 374 temuan (1.558,3%). Selain itu, tidak adanya Token Anti-CSRF juga menjadi perhatian, dengan 14 temuan (58,3%), yang menunjukkan potensi kerentanan terhadap serangan CSRF (*Cross-Site Request Forgery*). Untuk tingkat risiko lemah, ditemukan beberapa kelemahan signifikan, seperti *Cookie* tanpa *SameSite Attribute* (8 temuan, 33,3%) dan *Cross-Domain JavaScript Source File Inclusion*, dengan jumlah temuan tertinggi mencapai 420 *alert* (1.750,0%). Ini menunjukkan kurangnya pengaturan keamanan yang dapat meningkatkan risiko serangan XSS (*Cross-Site Scripting*). Selain itu, ditemukan pula pengungkapan *Timestamp Unix*, dengan 37 *alert* (154,2%), yang berpotensi memberikan informasi tambahan bagi penyerang dalam melakukan eksploitasi sistem. Di sisi lain, temuan dengan kategori Informasi juga mencatat sejumlah besar *alert*. Contohnya, *Strict-Transport-Security Header Not Set* memiliki 2.244 temuan (9.350,0%), menunjukkan perlunya penguatan *header* keamanan untuk memastikan komunikasi data yang lebih aman. Selain itu, jumlah *alert* tinggi juga ditemukan pada *X-Content-Type-Options Header Missing* (1.737 temuan, 7.237,5%) dan Keterbukaan Informasi - Komentar Mencurigakan, dengan 881 temuan (3.670,8%). Temuan ini menunjukkan kelemahan yang dapat memberikan informasi tambahan kepada penyerang. Dengan tingginya jumlah *alert* pada berbagai jenis risiko, hasil ini menegaskan perlunya perhatian lebih terhadap implementasi mekanisme pengamanan tambahan untuk mengurangi celah keamanan, khususnya pada pengaturan *header*, pengelolaan *cookie*, dan mitigasi serangan berbasis SQL *Injection* maupun XSS. Strategi pengamanan yang terintegrasi dan berkelanjutan sangat dibutuhkan untuk meningkatkan postur keamanan *web* Kampus X.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

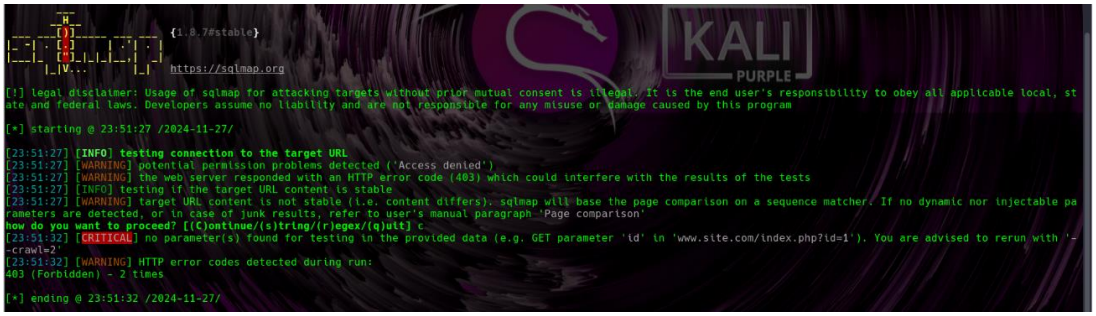
3.1.4 *Testing*

Pada tahap *testing* penguji melakukan 2 jenis serangan yaitu menggunakan DDOS *Attack* dengan LOIC (*Low Orbit Ion Cannon*) pada yang ditunjukkan pada Gambar 6 dan SQLInjection dengan SQLMap pada Gambar 7.



Gambar 6. Implementasi DDOS *Attack* Menggunakan *Low Orbit Ion Cannon* (LOIC)

Pada Gambar 6 ditampilkan hasil simulasi serangan terhadap situs *web* milik institusi X menggunakan LOIC (*Low Orbit Ion Cannon*). Dalam simulasi tersebut, peneliti menjalankan serangan dengan 100 *threads* aktif. Hasilnya, server target mengalami gangguan sementara (*server down*), namun tidak lama kemudian *server* berhasil memblokir serangan tersebut.



Gambar 7. Implementasi SQLInjection Menggunakan SQLMap

Selanjutnya, pada Gambar 7 ditunjukkan hasil simulasi serangan menggunakan *SQLMap*. Berdasarkan hasil pengujian, ditemukan beberapa peringatan yang mengindikasikan kendala selama proses evaluasi. Pertama, terdapat masalah izin umum yang menghasilkan pesan "*Access Denied*," mengindikasikan bahwa URL target tidak dapat diakses sepenuhnya. Selain itu, *server web* merespons dengan kode HTTP 403 (*Forbidden*), yang dapat memengaruhi akurasi hasil pengujian. SQLMap juga melaporkan bahwa *URL* target tidak stabil, kemungkinan karena adanya konten dinamis, sehingga perbandingan halaman dilakukan menggunakan pencocokan urutan. Tidak ditemukan parameter dinamis atau injeksi yang dapat diuji dalam data yang diberikan, termasuk parameter *GET* seperti "*id*". Sebagai hasilnya, alat memberikan peringatan kritis dan menyarankan pengguna untuk mengulang pengujian dengan parameter yang lebih spesifik. Hasil ini menunjukkan bahwa akses terbatas ke *URL* target dapat menghambat proses deteksi kerentanan, dan diperlukan penyesuaian konfigurasi atau parameter untuk mendapatkan hasil yang lebih komprehensif. Berdasarkan hasil penelitian, beberapa rekomendasi diajukan untuk meningkatkan keamanan *website* Kampus X. Langkah awal yang penting adalah meningkatkan keamanan dasar dengan mengimplementasikan DNSSEC untuk melindungi DNS dari serangan potensial. Penutupan *port* yang tidak diperlukan, seperti FTP dan PPTP, menjadi

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

prioritas guna mengurangi risiko eksploitasi. Selain itu, pembatasan akses pada layanan yang tidak kritis diperlukan untuk meminimalkan permukaan serangan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Manajemen kerentanan harus dilakukan secara menyeluruh melalui audit keamanan yang bertujuan untuk mengidentifikasi dan mengatasi celah pada kategori risiko sedang. Upaya ini perlu didukung dengan pembatasan pesan kesalahan yang dapat mengungkapkan informasi sistem kepada penyerang, serta penerapan mekanisme enkripsi dan penyamaran data guna melindungi informasi sensitif dari kebocoran.

Konfigurasi keamanan *web* juga memerlukan peningkatan signifikan. Langkah-langkah seperti penambahan *Content Security Policy* (CSP) *Header* untuk mencegah serangan injeksi skrip, penerapan Anti-CSRF Token untuk mencegah pemalsuan permintaan lintas situs, serta pengaturan ulang atribut *SameSite* pada *cookie* dan *aktivasi Strict-Transport-Security Header* untuk memperkuat koneksi HTTPS adalah tindakan penting untuk melindungi infrastruktur *website*. Pemantauan dan pengujian keamanan secara berkelanjutan juga menjadi bagian tak terpisahkan dari strategi keamanan. Penggunaan alat pemantauan secara *real-time* dan berkala diperlukan untuk deteksi dini potensi ancaman, sementara pelatihan keamanan rutin bagi tim teknologi informasi membantu meningkatkan kesadaran terhadap ancaman siber. Selain itu, pengujian penetrasi yang komprehensif dengan berbagai *framework* keamanan dan audit eksternal oleh pihak independen perlu dilakukan untuk memberikan evaluasi menyeluruh terhadap sistem. Kesimpulannya, keamanan *website* Kampus X adalah proses dinamis yang membutuhkan pendekatan holistik dalam mitigasi risiko. Implementasi rekomendasi yang diajukan diharapkan dapat memperkuat postur keamanan *website* secara signifikan dan mengurangi ancaman siber yang terus berkembang.

3.2 Pembahasan

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan website Kampus X di Kota Malang dengan menggunakan framework *ISSAF* (*Information Systems Security Assessment Framework*). Hasil penelitian menunjukkan bahwa meskipun website telah mengimplementasikan protokol *TLS* (*Transport Layer Security*) dengan pengaturan dasar yang aman, beberapa kerentanan masih ditemukan, seperti port terbuka yang tidak diperlukan. Hal ini sejalan dengan temuan yang dilaporkan oleh Herman *et al.* (2023), yang menyatakan bahwa pengelolaan port yang tidak tepat dapat membuka celah dalam sistem pertahanan keamanan web. Oleh karena itu, menutup port yang tidak terpakai dan memperketat kontrol akses akan mengurangi potensi ancaman. Selain itu, pemindaian menggunakan alat seperti *OWASP ZAP* dan *Acunetix* mengidentifikasi sejumlah celah, seperti *SQL Injection* dan ketidakadaan *Content Security Policy* (CSP). Temuan ini sejalan dengan penelitian Hariyadi dan Nastiti (2021), yang menekankan bahwa kurangnya penerapan *CSP* dapat meningkatkan risiko terhadap serangan aplikasi web. Albalawi *et al.* (2023) juga menunjukkan bahwa kerentanannya tidak hanya berasal dari aplikasi, tetapi juga dari layanan dan infrastruktur yang mendukungnya, sehingga membutuhkan pendekatan yang lebih luas dalam pengelolaan risiko. Dalam hal ketahanan terhadap serangan, simulasi *DDoS* menunjukkan bahwa server Kampus X dapat bertahan terhadap serangan ini, meskipun pengujian lebih lanjut menunjukkan perlunya penguatan pada aspek lainnya. Penelitian Nadzirin dan Nur (2024) mengungkapkan bahwa serangan *DDoS* dapat mengganggu kinerja sistem meskipun server dilindungi dengan pengaturan dasar yang baik, yang mengindikasikan perlunya penguatan mitigasi serangan *DDoS* yang lebih efisien. Oleh karena itu, langkah-langkah mitigasi berbasis perangkat keras dan teknik mitigasi lainnya disarankan untuk meningkatkan ketahanan server. Rekomendasi yang diperoleh dari penelitian ini mencakup penerapan *DNSSEC* (*Domain Name System Security Extensions*) untuk melindungi sistem *DNS* dari serangan spoofing, penutupan port yang tidak digunakan, serta penerapan header *CSP* untuk mengurangi potensi serangan *XSS* dan serangan lainnya. Rekomendasi tersebut sejalan dengan temuan Goni *et al.* (2024), yang menekankan pentingnya penerapan kebijakan perlindungan yang menyeluruh terhadap aplikasi web, serta penerapan standar keamanan yang ketat, seperti yang disarankan oleh Mishra *et al.* (2021) dalam *e-government*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

Penelitian ini menekankan pentingnya pendekatan berkelanjutan dalam pengelolaan keamanan website, terutama pada institusi pendidikan yang rawan terhadap ancaman dunia maya. Franchina *et al.* (2021) menekankan perlunya pelatihan aktif dan pasif untuk meningkatkan kewaspadaan dan respons terhadap serangan siber. Oleh karena itu, disarankan untuk menyelenggarakan program pelatihan yang rutin bagi staf IT dan pengguna di Kampus X agar mereka mampu mengidentifikasi dan mengatasi ancaman dengan lebih cepat. Meskipun website Kampus X sudah mengimplementasikan langkah-langkah dasar dalam pengelolaan keamanannya, banyak aspek yang masih perlu diperkuat guna mengurangi potensi risiko. Pengelolaan terhadap kerentanannya melalui penerapan kebijakan keamanan dan teknologi yang tepat sangat penting untuk menjaga integritas dan kerahasiaan data.

4. Kesimpulan

Penelitian ini mengkaji keamanan *website* Kampus X menggunakan ISSAF. Berdasarkan hasil analisis, penelitian ini menemukan bahwa domain kampusX.ac.id memiliki status aktif hingga Oktober 2025 dengan perlindungan dasar melalui fitur *clientTransferProhibited*, namun belum menerapkan mekanisme keamanan DNSSEC secara optimal. Hasil *SSLscan* menunjukkan penggunaan protokol TLS sebagai langkah awal pengamanan komunikasi data. *Network mapping* mengidentifikasi sejumlah *port* terbuka, termasuk *port* FTP dan PPTP, yang berpotensi menjadi titik kerentanan keamanan. Proses evaluasi kerentanan menunjukkan tingkat risiko sedang, dengan beberapa potensi celah keamanan seperti pengungkapan kredensial pengguna, informasi sistem, dan jalur *server*. Hasil simulasi serangan menunjukkan bahwa *server* mampu menahan serangan *DDoS*, namun terdapat beberapa area yang memerlukan perbaikan lebih lanjut, seperti pengelolaan pesan kesalahan dan perlindungan terhadap serangan berbasis SQL Injection. Pemindaian dengan OWASP ZAP mengidentifikasi 24 *alert* keamanan, dengan 12,5% di antaranya berada pada tingkat risiko tinggi.

Kesimpulan dari penelitian ini menegaskan bahwa meskipun telah ada upaya awal dalam melindungi *website*, masih terdapat banyak celah keamanan yang memerlukan perhatian lebih lanjut untuk meminimalkan risiko terhadap ancaman siber. Penelitian ini menyoroti pentingnya pendekatan yang komprehensif dan berkelanjutan dalam mengelola keamanan *website*. Untuk meningkatkan analisis keamanan pada penelitian selanjutnya, direkomendasikan penggunaan metode lanjutan seperti MITRE ATT&CK *Framework* untuk memetakan potensi ancaman dunia nyata secara sistematis, *Advanced Penetration Testing* yang melibatkan simulasi serangan oleh *tim red teaming*, serta penerapan analisis berbasis standar keamanan seperti NIST 800-115 atau *CIS Benchmarks*. Selain itu, pendekatan berbasis *Static Application Security Testing* (SAST) untuk analisis kode dan *Runtime Application Self-Protection* (RASP) untuk deteksi ancaman *runtime* dapat memberikan perlindungan lebih mendalam. Dengan integrasi metode yang telah disebutkan di atas, institusi pendidikan dapat mencapai pengelolaan keamanan *website* yang lebih kuat, berkelanjutan, dan adaptif terhadap ancaman siber yang terus berkembang, sehingga dapat meningkatkan postur keamanan siber di lingkungan pendidikan tinggi.

5. Daftar Pustaka

Albalawi, N., Alamrani, N., Aloufi, R., Albalawi, M., Aljaedi, A., & Alharbi, A. R. (2023). The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities. *Electronics*, *12*(12), 2664. https://doi.org/10.3390/electronics12122664.

Asriyanik, A., & Prajoko, P. (2018). Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005: 2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

(UMMI). *Jurnal Teknik Informatika dan Sistem Informasi*, *4*(2), 319-329. https://doi.org/http://dx.doi.org/10.28932/jutisi.v4i2.792.

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data*, *11*(1), 118.

Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G., & Roscioli, P. (2021). Passive and active training approaches for critical infrastructure protection. *International Journal of Disaster Risk Reduction*, *63*, 102461. https://doi.org/10.1016/j.ijdrr.2021.102461.

Goni, A., Jahangir, M. U. F., & Chowdhury, R. R. (2024). A Study on Cyber security: Analyzing Current Threats, Navigating Complexities, and Implementing Prevention Strategies. *International Journal of Research and Scientific Innovation*, *10*(12), 507-522.

Hariyadi, D., & Nastiti, F. E. (2021). Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi dan Informatika)*, *5*(1), 35-42. https://doi.org/10.31603/komtika.v5i1.5134.

Herman, H., Riadi, I., Kurniawan, Y., & Rafiq, I. A. (2023). Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF). *Jurnal Teknologi Informatika dan Komputer*, *9*(1), 126-136. https://doi.org/10.37012/jtik.v9i1.1439.

Idris, M., Syarif, I., & Winarno, I. (2022). Web application security education platform based on OWASP API security project. *EMITTER international journal of engineering technology*, 246-261. https://doi.org/10.24003/emitter.v10i2.705.

Maulana, S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz. *Jurnal Indonesia Sosial Teknologi*, *2*(04), 506-519. https://doi.org/https://doi.org/10.59141/jist.v2i04.124.

Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *Journal of Ambient Intelligence and Humanized Computing*, 1-12. https://doi.org/10.1007/s12652-020-02767-5.

Nur, M. N. A. (2024). cPanel Server Hosting Security Against Malware and DDoS Attacks on the Open Journal System Platform. *Scientific Journal of Informatics*, *11*(3), 761-772. https://doi.org/10.15294/sji.v11i3.11605.

Nurelasari, E., & Al Farabi, D. G. (2024). ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP. ID. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 3049-3054. https://doi.org/10.36040/jati.v8i3.9314.

Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. *Sustainability*, *15*(13), 10471. https://doi.org/10.3390/su151310471.

Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. *Sustainability*, *15*(13), 10471. https://doi.org/10.3390/app12084077.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1306

Silmina, E. P., Firdonsyah, A., & Amanda, R. A. A. (2022). Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf. *no*, *3*, 83-91. https://doi.org/10.14710/transmisi.24.3.83-91.

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *Ieee Access*, *9*, 13938-13959. https://doi.org/10.1109/ACCESS.2021.3051602.

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.

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. *Technology in Society*, *65*, 101565. https://doi.org/10.1016/j.techsoc.2021.101565.

Tara, T. R., & Yunanri, W. (2023). ANALISIS KEAMANAN WEBSITE SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN MENGGUNAKAN METODE VULNERABILITY ASSESMENT. *JURNAL TEKNOLOGI INFORMATIKA DAN KOMPUTER*, *1*(1), 1-9. https://doi.org/10.51401/jurtikom.v1i1.3172.

Umar, R., Riadi, I., Ihya, M., & Elfatiha, A. (2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. *JUTISI (Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi)*, *12*(1), 280–292. https://doi.org/10.35889/jutisi.v12i1.1191.

Utomo, I. C., & Rokhmah, S. (2022). Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *6*(2), 143. https://doi.org/10.30872/jurti.v6i2.8333.

Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web Application Penetration Testing on Udayana University's OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). *International Journal of Information Technology and Computer Science*, *16*(2), 45–56. https://doi.org/10.5815/ijitcs.2024.02.04.

Wijayanto, D., & Firdonsyah, A. (2024). Analisis Tingkat Resiko Pada Website Xyz Menggunakan Metode Owasp. *Digital Transformation Technology*, *4*(1), 644–651. https://doi.org/10.47709/digitech.v4i1.4485.