Jurnal Esensi Infokom Vol 8 No. 2 Oktober 2024
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infakom.v8i2.932

# Keamanan Siber dalam Era Digital: Tantangan dan Solusi

Ariawan Aryapranata[1], Yuliansyah Al Rasyid[2], Yogi Priya Agsena3, Sigit Hermanto[4]

*Program Studi Bisnis Digital Institut Pariwisata Trisakti*
*Jalan IKPN Tanah Kusir, Bintaro, South Jakarta, Jakarta Indonesia*

ariawan.aryapranata@iptrisakti.ac.id
yuliansyah@iptrisakti.ac.id
yogi.agsena@iptrisakti.ac.id
sigit.hermanto@iptrisakti.ac.id

*Intisari*— **Keamanan siber menjadi salah satu tantangan utama di era digital, seiring dengan meningkatnya ketergantungan terhadap teknologi informasi dan komunikasi. Makalah ini membahas berbagai jenis ancaman seperti serangan DDoS, malware, dan ransomware, serta solusi mitigasinya melalui penerapan Vulnerability Assessment and Penetration Testing (VAPT) menggunakan alat seperti Nmap dan Nikto. Penelitian ini bertujuan untuk memberikan wawasan tentang teknik terbaik dalam mitigasi ancaman siber dan menekankan pentingnya VAPT dalam menjaga integritas sistem. Hasil penelitian menunjukkan bahwa penerapan VAPT tidak hanya efektif dalam mengidentifikasi kerentanan, tetapi juga penting untuk meningkatkan kesiapan organisasi dalam menghadapi ancaman siber.**
*Kata kunci*— Keamanan siber, VAPT, Nmap, Nikto, Mitigasi Ancaman.

*Abstract*— **Cybersecurity is one of the main challenges in the digital era, along with the increasing dependence on information and communication technology. This paper discusses different types of threats such as DDoS, malware, and ransomware attacks, as well as mitigation solutions through the implementation of Vulnerability Assessment and Penetration Testing (VAPT) using tools such as Nmap and Nikto. This research aims to provide insight into the best techniques in cyber threat mitigation and emphasize the importance of VAPT in maintaining system integrity. The results of the study show that the implementation of VAPT is not only effective in identifying vulnerabilities, but also important for improving organizational readiness in dealing with cyber threats.**
Keywords-Cybersecurity, VAPT, Nmap, Nikto, Threat Mitigation.

## I. PENDAHULUAN

Perkembangan teknologi digital telah membawa banyak manfaat dan efisiensi dalam berbagai sektor, mulai dari pemerintahan, keuangan, hingga layanan kesehatan. Namun, di balik perkembangan ini, ancaman siber menjadi semakin kompleks dan terus berkembang. Organisasi tidak lagi hanya berhadapan dengan serangan sederhana seperti virus komputer, tetapi juga dengan serangan canggih seperti Distributed Denial of Service (DDoS), ransomware, Advanced Persistent Threat (APT), dan eksploitasi kerentanan zero-day.

Dalam beberapa tahun terakhir, peningkatan insiden keamanan siber menunjukkan betapa pentingnya upaya pencegahan dan mitigasi ancaman. Kebocoran data sensitif dan serangan ransomware yang mengenkripsi data organisasi telah menjadi ancaman nyata yang menimbulkan kerugian finansial, reputasi, dan operasional. Tidak hanya organisasi besar, perusahaan kecil dan menengah (UMKM) pun kini menjadi target karena sering kali memiliki sistem keamanan yang lemah.

Mengingat sifat dinamis dari ancaman siber, solusi keamanan siber tradisional seperti firewall dan antivirus tidak lagi cukup untuk memberikan perlindungan yang komprehensif. Diperlukan pendekatan yang lebih proaktif dan sistematis dalam mengidentifikasi dan memperbaiki potensi kerentanan sebelum dieksploitasi oleh pihak tidak bertanggung jawab. Salah satu teknik yang efektif dalam memastikan kesiapan sistem terhadap ancaman ini adalah Vulnerability Assessment and Penetration Testing (VAPT) [1].

VAPT adalah kombinasi dari dua pendekatan:

1. Vulnerability Assessment (VA), yang fokus pada identifikasi kerentanan dalam sistem dan aplikasi, dengan tujuan memberikan laporan komprehensif tentang celah keamanan yang ada.
2. Penetration Testing (PT), yang bertujuan untuk mensimulasikan serangan nyata guna menguji apakah kerentanan yang teridentifikasi dapat dieksploitasi oleh peretas.

VAPT memberikan wawasan yang lebih mendalam tentang titik lemah keamanan dan membantu organisasi dalam memperbaiki sistem secara lebih efektif [2]. Dengan memanfaatkan alat seperti Nmap dan Nikto, organisasi dapat memetakan layanan yang rentan dan mendeteksi kelemahan dalam aplikasi web secara proaktif. Alat ini sangat penting karena serangan terhadap port dan aplikasi web sering kali menjadi titik masuk pertama bagi peretas.

Dalam era di mana sistem semakin terhubung melalui Internet of Things (IoT) dan layanan berbasis cloud, keamanan siber tidak hanya menjadi tanggung jawab departemen IT tetapi juga merupakan prioritas strategis

e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infakom.v8i2.932

seluruh organisasi. Oleh karena itu, pendekatan seperti VAPT menjadi bagian integral dalam kerangka keamanan siber modern. Penelitian ini akan fokus pada penerapan VAPT pada domain 'cybersecurity.co.id', menggambarkan pentingnya langkah proaktif dalam mengidentifikasi dan mengatasi kerentanan sebelum serangan terjadi.

Penelitian ini diharapkan dapat memberikan wawasan tentang praktik terbaik dalam penerapan VAPT dan pentingnya integrasi langkah keamanan siber dalam strategi bisnis organisasi.

## II. BACKGROUNG/LATAR BELAKANG

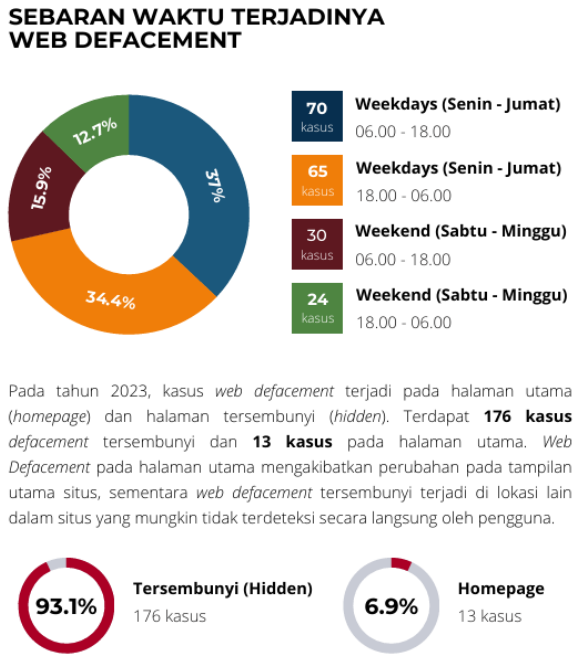
Ancaman siber semakin berkembang dan tidak hanya menyerang jaringan internal perusahaan besar, tetapi juga mempengaruhi organisasi kecil dan menengah. Dengan meningkatnya jumlah serangan yang menargetkan port terbuka dan aplikasi web, terdapat kebutuhan mendesak untuk memanfaatkan alat-alat keamanan yang mampu mengidentifikasi kerentanan secara efisien dan akurat. Salah satu metode yang terbukti efektif adalah Vulnerability Assessment and Penetration Testing (VAPT), sebuah pendekatan menyeluruh untuk memetakan kelemahan sistem dan menguji seberapa rentan sistem terhadap serangan.

### WEB DEFACEMENT

Serangan web defacement merupakan serangan yang dilakukan untuk mengeksploitasi situs web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem sehingga threat actor dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas.

Pelaku serangan web defacement disebut sebagai defacer. Terdapat 189 kasus web defacement yang dinotifikasi kepada pemilik sistem di situs-situs Indonesia dengan kasus terbanyak terjadi pada bulan Januari dengan jumlah kasus sebanyak 31 kasus web defacement [3].


Gambar 1. Sektor Terdampak Web Defacement




Gambar 2. Waktu Terjadinya Web Defacement

### Peran Nmap dan Nikto dalam VAPT

Dalam konteks VAPT, terdapat berbagai alat yang digunakan untuk melakukan pemindaian dan pengujian, namun Nmap dan Nikto adalah dua alat yang sering diandalkan untuk tugas ini:

**1. Nmap (Network Mapper):**

Nmap adalah alat pemindaian jaringan yang digunakan secara luas untuk mendeteksi port dan layanan terbuka dalam system. Fitur-fitur Nmap memungkinkan pemindaian berbagai jenis port dengan cepat dan mendeteksi aplikasi atau layanan yang berjalan di setiap port tersebut. Dengan kemampuan untuk mengidentifikasi versi aplikasi, Nmap memberikan wawasan tentang layanan yang rentan terhadap serangan atau sudah usang (outdated). Penggunaan alat seperti Nmap dan Nikto [4],[7], penting dalam fase awal pengujian keamanan, di mana pemetaan jaringan dan identifikasi titik akses menjadi langkah krusial untuk mencegah serangan yang memanfaatkan port terbuka.

**2. Nikto:**

Nikto adalah alat open-source yang difokuskan untuk mendeteksi kerentanan di aplikasi web [5]. Aplikasi web sering kali menjadi target utama karena aksesnya yang luas dan kerap kali berisi informasi sensitif. Nikto dapat mendeteksi kelemahan umum seperti:

a. Konfigurasi yang salah (misconfiguration)
b. Kehadiran file atau direktori sensitif yang tidak terlindungi
c. Versi software yang rentan terhadap eksploitasi

Dengan ribuan tes pra-konfigurasi, Nikto secara cepat dan efisien mengidentifikasi masalah yang dapat menyebabkan serangan seperti SQL Injection, Cross-Site Scripting (XSS), atau Remote Code Execution (RCE).

**Pentingnya VAPT dalam Strategi Keamanan**

Dalam lanskap ancaman yang dinamis, deteksi dan respons terhadap kerentanan tidak bisa lagi bersifat reaktif. Organisasi membutuhkan metode proaktif untuk mengidentifikasi kelemahan dan memperbaiki sistem sebelum diserang. Serangan zero-day dan APT (Advanced Persistent Threat) sering kali mengeksploitasi kerentanan yang tidak terdeteksi, sehingga VAPT menjadi langkah penting dalam mendeteksi dan mengatasi masalah keamanan yang mungkin luput dari pengawasan.

Implementasi Nmap dan Nikto dalam VAPT memungkinkan tim keamanan untuk mengidentifikasi:

a. Port dan layanan yang tidak diperlukan dan dapat ditutup untuk meminimalkan serangan.
b. Kerentanan aplikasi web yang dapat diperbaiki sebelum ditemukan oleh peretas.
c. Kesalahan konfigurasi sistem yang meningkatkan risiko serangan internal maupun eksternal.

**Dampak dan Manfaat VAPT bagi Organisasi**

Penelitian ini berfokus pada domain **'cybersecurity.co.id'**, yang berfungsi sebagai studi kasus untuk menunjukkan efektivitas alat-alat ini dalam memitigasi risiko siber. Dengan melakukan pemindaian menggunakan Nmap dan Nikto, Penelitian ini juga relevan dengan ISO 27001, yang memberikan kerangka kerja bagi organisasi untuk mengatur keamanan informasi secara efektif [6]. organisasi dapat mengurangi risiko operasional dan memastikan kepatuhan terhadap regulasi keamanan, seperti ISO 27001 [8] dan GDPR, yang semakin menekankan pentingnya perlindungan data dan sistem informasi.

Selain itu, hasil dari VAPT membantu organisasi untuk:

a. Membangun kebijakan keamanan yang lebih kuat berdasarkan analisis risiko yang teridentifikasi.
b. Memperkuat kesadaran dan kesiapan tim IT dalam menghadapi ancaman.

Mengurangi downtime dan potensi kerugian finansial akibat serangan siber.

## III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksploratif dengan pendekatan studi kasus pada domain 'cybersecurity.co.id'. Tujuan dari metodologi ini adalah untuk memperoleh pemahaman mendalam mengenai kerentanan yang ada dan bagaimana celah keamanan tersebut dapat dimitigasi. Fokus utama penelitian ini adalah penerapan Vulnerability Assessment and Penetration Testing (VAPT), yang terbagi ke dalam dua tahapan utama: pemindaian jaringan dan identifikasi kerentanan aplikasi web. Berikut adalah langkah-langkah yang diambil dalam penelitian ini.

A. Desain Penelitian

Studi kasus ini menggunakan teknik VAPT untuk mengidentifikasi celah keamanan yang mungkin ada di domain target. Pendekatan eksploratif dipilih karena sifat ancaman siber yang terus berkembang, sehingga penelitian perlu bersifat fleksibel untuk mengakomodasi berbagai skenario serangan.

B. Alur Pelaksanaan VAPT

Langkah-langkah VAPT dalam penelitian ini dilakukan melalui dua tahap penting, yaitu pemindaian jaringan menggunakan Nmap dan pengujian kerentanan aplikasi web dengan Nikto.

C. Tahap Pelaksanaan Pemindaian dan Pengujian

1. Pemindaian Port dan Layanan dengan Nmap

Alat: Nmap (Network Mapper)

Tujuan: Mengidentifikasi port dan layanan yang terbuka pada domain. Setiap port yang terbuka dapat menjadi pintu masuk bagi serangan.

2. Identifikasi Kerentanan Aplikasi Web dengan Nikto

Alat: Nikto Web Scanner

Tujuan: Mendeteksi kerentanan spesifik yang terdapat dalam aplikasi web di domain target.

D. Analisis dan Interpretasi Data

Setelah data dari Nmap dan Nikto terkumpul, dilakukan analisis mendalam untuk memahami implikasi keamanan dari hasil yang diperoleh. Langkah-langkah analisis meliputi:

a. Kategorisasi port dan layanan: Identifikasi port mana yang tidak diperlukan dan dapat ditutup untuk mengurangi permukaan serangan.
b. Evaluasi kerentanan aplikasi web: Menganalisis setiap temuan Nikto untuk menilai dampak dan risiko dari kerentanan yang ditemukan.
c. Pemetaan terhadap framework keamanan: Hasil pengujian disesuaikan dengan kerangka keamanan seperti ISO 27001 untuk memastikan bahwa praktik keamanan yang baik diterapkan.

E. Rekomendasi Mitigasi

Berdasarkan hasil pemindaian dan analisis, rekomendasi mitigasi disusun untuk mengurangi risiko siber. Contoh rekomendasi termasuk:

1. Menutup port yang tidak diperlukan untuk meminimalkan permukaan serangan.
2. Memperbarui aplikasi dan layanan ke versi terbaru untuk mengurangi risiko dari kerentanan yang teridentifikasi.
3. Mengimplementasikan header keamanan seperti Content-Security-Policy dan X-Frame-Options untuk melindungi aplikasi web.

Meningkatkan kebijakan firewall untuk mengontrol akses terhadap port terbuka.

## IV. HASIL DAN PEMBAHASAN

Berdasarkan hasil pemindaian Nmap dan pengujian menggunakan Nikto pada domain 'cybersecurity.co.id', ditemukan beberapa kerentanan dan konfigurasi layanan yang dapat dimanfaatkan oleh peretas. Bagian ini menyajikan analisis mendalam dari hasil VAPT, mengevaluasi setiap temuan dengan detail, dan memberikan rekomendasi mitigasi yang tepat.

A. Analisis Hasil Pemindaian Nmap

Ringkasan Temuan:

1. Port 80 (HTTP):
   Status: Tertutup

Implikasi: Meskipun port 80 tertutup, layanan ini biasanya digunakan untuk mengarahkan pengguna ke versi HTTPS. Tidak adanya layanan HTTP yang aktif mengurangi risiko serangan berbasis HTTP seperti man-in-the-middle (MitM) dan session hijacking.

2. Port 443 (HTTPS):
   Status: Terbuka
   Layanan: OpenResty web app server
   Detail Lainnya:
   Layanan web menggunakan TLS dengan cipher TLS_AES_256_GCM_SHA384, yang merupakan standar keamanan tinggi.

Analisis:

Port 443 yang terbuka mengindikasikan bahwa situs web menggunakan HTTPS untuk komunikasi aman. Namun, temuan ini juga menunjukkan bahwa server web yang digunakan adalah OpenResty, dan versi spesifik dari OpenResty tidak diidentifikasi. Jika layanan tidak diperbarui secara berkala, terdapat kemungkinan kerentanan eksploitasi pada server web tersebut.

Rekomendasi:

a. Lakukan pemantauan dan Perbarui Layanan Secara Rutin: Pastikan OpenResty dan semua dependensi terkait selalu diperbarui untuk menghindari risiko eksploitasi kerentanan yang diketahui.
b. Terapkan Kebijakan Firewall: Batasi akses berdasarkan lokasi atau IP jika memungkinkan, untuk meminimalkan serangan.

B. Analisis Hasil Pengujian Nikto

Temuan Utama:

1. Tidak Ada Header X-Frame-Options:
   a. Risiko: Rentan terhadap serangan clickjacking, di mana penyerang dapat menyematkan situs web dalam iframe dan mencuri data pengguna.
   b. Rekomendasi: Terapkan header `X-Frame-Options: DENY` atau `SAMEORIGIN` untuk mencegah serangan clickjacking.
2. Tidak Ada Header X-Content-Type-Options:
   a. Risiko: Rentan terhadap serangan berbasis MIME-sniffing, di mana browser dapat menampilkan konten dengan tipe yang salah.
   b. Rekomendasi: Terapkan header `X-Content-Type-Options: nosniff` untuk memastikan konten ditampilkan sesuai dengan tipe MIME yang benar.
3. Header Unik dari Hostinger:
   a. Header seperti `x-hostinger-datacenter` dan `x-hostinger-node` terdeteksi, menunjukkan bahwa situs ini di-host di infrastruktur milik Hostinger.
   b. Analisis: Meskipun tidak langsung berbahaya, informasi ini dapat digunakan oleh penyerang untuk merancang serangan yang lebih spesifik.
4. Sertifikat HTTPS Valid dengan Let's Encrypt:
   a. Status: Sertifikat dikeluarkan oleh Let's Encrypt dan valid pada saat pemindaian. Namun, sertifikat ini memiliki masa berlaku yang relatif singkat dan perlu diperbarui secara berkala.
   b. Rekomendasi: Pantau masa kedaluwarsa sertifikat dan gunakan otomatisasi untuk pembaruan agar tidak terjadi interupsi layanan.
5. Iklan HTTP/3 melalui Header alt-svc:
   a. Situs ini mengiklankan ketersediaan protokol HTTP/3. Namun, Nikto tidak dapat menguji protokol ini.
   b. Analisis: HTTP/3 memberikan performa yang lebih baik, tetapi memerlukan perhatian ekstra untuk memastikan bahwa implementasinya tidak menimbulkan celah keamanan.
6. Kesalahan SSL Negosiasi:
   a. Detail: Beberapa kesalahan SSL terjadi selama pemindaian, yang menunjukkan potensi masalah dalam konfigurasi atau stabilitas layanan SSL.
   b. Rekomendasi: Lakukan audit SSL untuk memastikan bahwa tidak ada konfigurasi yang salah dan semua cipher yang digunakan aman.

C. Implikasi dan Pembahasan

Hasil VAPT menunjukkan bahwa meskipun layanan HTTP ditutup dan situs web menggunakan HTTPS, terdapat beberapa celah konfigurasi yang dapat dimanfaatkan oleh peretas. Ketiadaan header keamanan seperti X-Frame-Options dan X-Content-Type-Options menunjukkan bahwa situs web masih rentan terhadap serangan berbasis web. Selain itu, kesalahan dalam negosiasi SSL menunjukkan potensi masalah pada koneksi aman, yang perlu segera diatasi.

D. Rekomendasi Mitigasi

Berdasarkan hasil analisis, berikut adalah rekomendasi yang dapat diterapkan:

1. Implementasi Header Keamanan:
   Terapkan `X-Frame-Options` dan `X-Content-Type-Options` untuk melindungi situs dari serangan clickjacking dan MIME-sniffing.
2. Perbarui dan Audit Layanan Web Secara Rutin:
   Pastikan bahwa server OpenResty dan semua aplikasi terkait selalu dalam kondisi terbaru untuk mengurangi risiko eksploitasi kerentanan.
3. Audit SSL dan Pantau Sertifikat:
   Periksa konfigurasi SSL untuk memastikan cipher dan protokol yang digunakan aman. Gunakan otomatisasi untuk pembaruan sertifikat Let's Encrypt.
4. Pembatasan Akses melalui Firewall:
   Batasi akses ke port 443 dengan kebijakan firewall berbasis IP untuk meminimalkan risiko serangan.

Tabel 1. Rangkuman VAPT

| Kategori | Temuan | Risiko | Rekomendasi |
|---|---|---|---|
| **Port dan Layanan** | **Port 80 (HTTP) tertutup** | Risiko eksploitasi jika OpenResty tidak diperbarui atau salah konfigurasi. | Perbarui OpenResty secara berkala dan terapkan patch keamanan terbaru. |
| | **Port 443 (HTTPS) terbuka dengan OpenResty** | | |
| **SSL/TLS** | Menggunakan **TLS_AES_256_GCM_SHA384** | Sertifikat valid tetapi memiliki masa berlaku singkat. | Gunakan otomatisasi pembaruan sertifikat untuk menghindari kedaluwarsa. |
| | Sertifikat HTTPS dari Let's Encrypt | | |
| **Header Keamanan** | - **X-Frame-Options** tidak diterapkan | Rentan terhadap **clickjacking** dan **MIME-sniffing**. | Terapkan header X-Frame-Options: DENY dan X-Content-Type-Options: nosniff. |
| | - **X-Content-Type-Options** tidak diterapkan | | |
| **Informasi Server** | - Menggunakan **OpenResty** | Memberikan informasi teknis yang dapat digunakan untuk serangan lebih spesifik. | Minimalkan pengungkapan informasi server dengan menonaktifkan header tidak perlu. |
| | - Header unik seperti x-hostinger-datacenter dan x-hostinger-node terdeteksi | | |
| **Protokol HTTP/3** | **Header alt-svc** menunjukkan layanan HTTP/3 | Potensi celah keamanan jika HTTP/3 tidak dikonfigurasi dengan benar. | Audit keamanan pada implementasi HTTP/3 dan lakukan uji penetrasi tambahan. |
| **SSL Negotiation Errors** | Kesalahan SSL selama pemindaian Nikto | Risiko ketidakstabilan koneksi atau konfigurasi SSL yang salah. | Audit SSL dan pastikan semua cipher serta protokol dikonfigurasi dengan benar. |

## V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan menggunakan VAPT (Vulnerability Assessment and Penetration Testing) dengan alat Nmap dan Nikto, terdapat beberapa poin penting dan rekomendasi yang dapat disimpulkan terkait keamanan domain yang diuji:

Temuan Utama:

1. Layanan Jaringan dan Port:

Port 80 (HTTP): Ditutup, mengurangi risiko serangan HTTP seperti Man-in-the-Middle (MitM).
Port 443 (HTTPS): Terbuka dan menggunakan server OpenResty dengan TLS standar tinggi (TLS_AES_256_GCM_SHA384). Namun, tidak ada informasi detail terkait pembaruan layanan tersebut, sehingga ada potensi kerentanan jika tidak diperbarui.

2. Kelemahan Aplikasi Web:

Header X-Frame-Options tidak diterapkan: Situs rentan terhadap serangan clickjacking.
Header X-Content-Type-Options tidak diterapkan: Berpotensi terkena MIME-sniffing, yang memungkinkan browser menafsirkan tipe konten secara keliru.
Header spesifik seperti x-hostinger-datacenter dan x-hostinger-node terdeteksi, memberikan informasi yang bisa dimanfaatkan penyerang untuk melakukan serangan lebih terarah.

3. Sertifikat HTTPS:

Menggunakan sertifikat dari Let's Encrypt dengan validitas singkat, yang memerlukan pemantauan dan pembaruan otomatis untuk mencegah downtime.

4. Implementasi HTTP/3:

Situs mengiklankan ketersediaan HTTP/3 melalui header `alt-svc`, namun ini memerlukan audit tambahan untuk memastikan konfigurasi yang aman.

5. Kesalahan SSL Negotiation:

Beberapa kesalahan SSL terdeteksi, menandakan potensi masalah konfigurasi atau stabilitas koneksi aman.

Rekomendasi Perbaikan:

1. Header Keamanan:

Terapkan `X-Frame-Options: DENY` atau `SAMEORIGIN` untuk mencegah clickjacking.
Tambahkan `X-Content-Type-Options: nosniff` untuk menghindari serangan MIME-sniffing.

2. Audit dan Pembaruan Layanan:

Perbarui OpenResty dan komponen terkait secara berkala untuk mencegah eksploitasi kerentanan yang sudah diketahui.
Minimalkan informasi yang diungkap melalui header yang tidak diperlukan, seperti `x-hostinger-datacenter`.

3. Pemantauan SSL dan Sertifikat:

Audit konfigurasi SSL secara berkala untuk memastikan tidak ada kesalahan yang berpotensi menurunkan keamanan.
Otomatisasi pembaruan sertifikat Let's Encrypt agar tidak terjadi interupsi layanan.

4. Penggunaan Firewall dan Pembatasan Akses:

Batasi akses ke port 443 dengan kebijakan firewall berbasis IP untuk meminimalkan risiko serangan eksternal.

5. Audit HTTP/3:

Lakukan uji penetrasi tambahan pada implementasi HTTP/3 untuk memastikan konfigurasi aman.

VAPT yang dilakukan menunjukkan bahwa meskipun layanan HTTPS telah diterapkan, masih terdapat beberapa konfigurasi keamanan yang kurang optimal yang perlu diperbaiki. Implementasi header keamanan, pembaruan layanan secara berkala, dan audit SSL sangat disarankan untuk memperkuat postur keamanan domain. Dengan mengatasi kelemahan ini, organisasi dapat mengurangi risiko

serangan dan memastikan kepatuhan terhadap standar keamanan seperti ISO 27001.

Langkah-langkah mitigasi yang direkomendasikan diharapkan dapat membantu menjaga integritas sistem dan melindungi aset digital dari potensi ancaman di masa mendatang.

## Ucapan Terima Kasih

Kami mengucapkan terima kasih kepada pengelola Jurnal Esensi Infokom Institut Bisnis Nusantara yang telah memberikan kesempatan untuk mempublikasi Tulisan ini.

## Referensi

[1] Gordon, L. A., et al. (2002). Computer Security: Managing Security Risks. ACM Press.
[2] Skoudis, E. & Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall.
[3] Lanskap Keamanan Siber Indonesia 2023 pada Lanskap-Keamanan-Siber-Indonesia-2023.pdf
[4] Nmap.org. (2023). "Nmap Reference Guide". [Online]. Tersedia di: https://nmap.org/
[5] Nikto.org. (2023). "Nikto Web Scanner Documentation". [Online]. Tersedia di: https://cirt.net/Nikto2
[6] Chen, J., & Bridges, R. A. (2017). *Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware.* Computers & Security, 81, 144-158.
[7] OWASP. (2023). "OWASP Testing Guide v4." [Online]. Tersedia di: https://owasp.org
[8] Calder, A. (2016). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* Kogan Page Publishers.