Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

ANALISIS SERANGAN SIBER DI WEBSITE UHAMKA DENGAN METODE *PENETRATION TESTING*

Rayhan Maulana[1], Ade Davy Wiranata[2*]
[1,2] Teknik Informatika, Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof. DR. HAMKA, Jakarta, Indonesia
Email: [1]rayhanmaulana@uhamka.ac.id, [2*]adedavy@uhamka.ac.id
(* : corresponding author)

Abstrak-Website perguruan tinggi menyimpan data penting sehingga rentan terhadap serangan siber apabila tidak dilindungi dengan baik. Permasalahan pada penelitian ini adalah belum diketahuinya tingkat keamanan website UHAMKA serta jenis kerentanan yang berpotensi dimanfaatkan oleh penyerang. Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan keamanan website UHAMKA melalui automated vulnerability assessment. Metode penelitian yang digunakan adalah kualitatif dengan tahapan pengintaian, pemindaian, dan pelaporan, menggunakan alat bantu OWASP ZAP dan Nmap berbasis pemindaian keamanan otomatis. Teridentifikasi 37 potensi kerentanan berdasarkan hasil pemindaian keamanan otomatis. terdiri dari empat kerentanan tingkat sedang dan lima kerentanan tingkat rendah, yang didominasi oleh konfigurasi keamanan *header* dan pengelolaan *plugin*. Kesimpulan penelitian ini menunjukkan bahwa metode pemindaian keamanan otomatis mampu mengidentifikasi potensi kelemahan konfigurasi keamanan pada website UHAMKA. Temuan ini memberikan gambaran awal mengenai kondisi keamanan website UHAMKA pada lingkungan perguruan tinggi berbasis layanan digital, serta dapat dijadikan dasar bagi pengelola sistem dalam merumuskan langkah mitigasi dan peningkatan konfigurasi keamanan. Selain itu, hasil penelitian ini diharapkan dapat menjadi referensi awal bagi penelitian selanjutnya yang mengkaji keamanan website perguruan tinggi dengan pendekatan pengujian yang lebih mendalam, termasuk validasi manual dan analisis dampak kerentanan secara komprehensif pada berbagai konteks institusi pendidikan tinggi. Dengan demikian, penelitian ini menegaskan pentingnya evaluasi keamanan berkala pada website perguruan tinggi institusi.

Kata Kunci: *Nmap, OWASP ZAP, Penetration Testing*, Penilaian Kerentanan, Serangan Siber

Abstract-*University websites store important data and are therefore vulnerable to cyberattacks if not properly protected. The problem in this study is the unknown security level of the UHAMKA website and the types of vulnerabilities that could potentially be exploited by attackers. This study aims to identify potential security vulnerabilities on the UHAMKA website through an automated vulnerability assessment. The research method used is qualitative with reconnaissance, scanning, and reporting stages, using OWASP ZAP and Nmap tools based on automated security scanning. Thirty-seven potential vulnerabilities were identified based on the automated security scan results, consisting of four moderate vulnerabilities and five low-level vulnerabilities, dominated by header security configuration and plugin management. The conclusion of this study shows that the automated security scanning method is able to identify potential security configuration weaknesses on the UHAMKA website. These findings provide an initial overview of the security condition of the UHAMKA website in a digital service-based higher education environment and can be used as a basis for system managers in formulating mitigation measures and improving security configurations. In addition, the results of this study are expected to serve as an initial reference for further research that examines university website security with a more in-depth testing approach, including manual validation and comprehensive vulnerability impact analysis in various contexts of higher education institutions. Thus, this study emphasizes the importance of periodic security evaluations on institutional college websites.*

Keywords*: Cyber Attacks, Nmap, OWASP ZAP, Penetration Testing, Vulnerability Assessment*

1. PENDAHULUAN

Keamanan informasi merupakan komponen penting dalam ekosistem digital saat ini. Perkembangan teknologi internet mendorong pemanfaatan website sebagai media utama penyampaian informasi dan layanan secara cepat dan luas, tidak hanya sebagai sarana pertukaran informasi, tetapi juga sebagai pendukung aktivitas operasional institusi secara daring[1]. Lemahnya regulasi dan rendahnya kesadaran terhadap keamanan siber tidak hanya terjadi pada tingkat masyarakat, tetapi juga pada instansi pemerintahan dan perusahaan besar

Keamanan siber bertujuan untuk mengidentifikasi, mencegah, dan meminimalkan dampak ancaman serta serangan siber terhadap data, perangkat keras, perangkat lunak, dan infrastruktur teknologi informasi[2]. Penerapan keamanan siber yang baik berperan penting dalam melindungi sistem digital dari berbagai bentuk serangan, menjaga privasi data pengguna, serta mencegah penyalahgunaan sistem seperti penyisipan konten ilegal pada website[3].

Website yang aman adalah website yang terlindungi dari serangan siber, termasuk penyisipan konten ilegal. Website UHAMKA (Universitas Muhammadiyah Prof. Dr. HAMKA) adalah portal digital yang berfungsi sebagai sarana informasi dan komunikasi resmi universitas. Website ini dirancang untuk memberikan berbagai layanan dan informasi yang relevan bagi mahasiswa, dosen, staf, alumni, calon mahasiswa, dan masyarakat umum. Sebagai situs

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

resmi yang mengelola data penting, Website UHAMKA berpotensi menjadi target serangan pada lapisan aplikasi web, khususnya yang berkaitan dengan konfigurasi *header* keamanan dan manajemen *plugin*. Kerentanan tersebut dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan peretasan maupun penyisipan konten ilegal[4].

Meskipun demikian, Website UHAMKA yang dikelola oleh BPTI UHAMKA (Badan Pengembangan Teknologi Informasi Universitas Muhammadiyah Prof. DR. HAMKA) masih menghadapi tantangan keamanan. Salah satu bentuk serangan yang pernah terjadi adalah penyisipan konten ilegal berupa iklan pada halaman website, yang menunjukkan adanya celah keamanan yang belum sepenuhnya tertangani[5]. Tujuan penelitian ini adalah menganalisis potensi kerentanan keamanan pada website UHAMKA dengan menggunakan metode *vulnerability assessment* berbasis *penetration testing tools*, serta memberikan rekomendasi perbaikan sebagai upaya peningkatan keamanan sistem[6].

Penelitian sebelumnya menunjukkan bahwa penggunaan *penetration testing* dan vulnerability assessment efektif dalam mengidentifikasi kerentanan keamanan website instansi pemerintahan dan pendidikan, terutama yang berkaitan dengan konfigurasi server dan kelemahan aplikasi web. Namun, sebagian besar penelitian tersebut masih berfokus pada aspek teknis hasil pemindaian tanpa mengaitkan temuan kerentanan dengan kondisi pengelolaan keamanan pada tingkat institusi. Hal ini menunjukkan adanya celah penelitian terkait analisis keamanan website yang mempertimbangkan konteks pengelolaan institusional.

Hal serupa juga ditunjukkan pada penelitian implementasi *penetration testing* pada website institusi pendidikan tinggi yang menemukan bahwa sebagian besar kerentanan berada pada tingkat risiko sedang, sehingga diperlukan rekomendasi perbaikan untuk meningkatkan keamanan aset informasi website secara menyeluruh[7]. Selain itu, salah satu jenis kerentanan yang sering ditemukan pada aplikasi web adalah *Cross-Site Scripting (XSS)*. Kerentanan ini terjadi akibat lemahnya validasi input dan pengelolaan output yang tidak aman, sehingga memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman website[8]. Penelitian sebelumnya menunjukkan bahwa metode *penetration testing* efektif dalam mengidentifikasi kerentanan *XSS* serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan aplikasi web[9].

Beberapa penelitian juga menemukan bahwa kerentanan aplikasi web umumnya berada pada tingkat risiko rendah hingga sedang, sehingga diperlukan rekomendasi perbaikan untuk meningkatkan keamanan aset informasi secara menyeluruh[10]. Salah satu jenis kerentanan yang sering ditemukan adalah *Cross-Site Scripting (XSS)*, yang terjadi akibat lemahnya validasi input dan pengelolaan output aplikasi web. Metode pengujian keamanan berbasis tools otomatis terbukti efektif dalam mendeteksi jenis kerentanan tersebut[11].

Selain itu, studi tentang metode *Penetration Testing Execution Standard (PTES)* untuk analisis kerentanan aplikasi web menunjukkan bahwa metode ini dapat secara sistematis menemukan celah keamanan melalui tahapan yang terstruktur, mulai dari pengumpulan informasi hingga analisis kerentanan. Kerangka kerja PTES memberikan panduan yang jelas dalam melakukan evaluasi keamanan aplikasi web sehingga hasil pengujian dapat dijadikan dasar rekomendasi perbaikan sistem keamanan[11]. Beberapa penelitian sebelumnya telah membahas pengembangan sistem berbasis web, namun belum secara khusus menyoroti aspek evaluasi keamanan sistem secara teknis. Kondisi ini membuka peluang penelitian lebih lanjut pada aspek pengujian keamanan website menggunakan pendekatan penetration testing[12].

Selain pengujian pada lapisan aplikasi web, analisis keamanan website juga dilakukan pada sisi jaringan dan layanan server. Pada tahap awal pengujian, digunakan *Nmap (Network Mapper)* sebagai *tools open-source* untuk melakukan pengintaian dan pemindaian jaringan, meliputi identifikasi host aktif, port terbuka, serta layanan yang berjalan pada server. Informasi yang dihasilkan dari Nmap memberikan gambaran awal mengenai konfigurasi jaringan dan potensi celah keamanan pada tingkat jaringan. Oleh karena itu, Nmap digunakan sebagai tools pendukung untuk melengkapi hasil pemindaian keamanan aplikasi web yang dilakukan menggunakan OWASP ZAP[13].

2. METODE PENELITIAN

2.1. Jenis Penelitian

Analisis dalam penelitian ini mencakup proses mengidentifikasi, mengklasifikasikan, dan mengevaluasi temuan kerentanan keamanan website berdasarkan kriteria tertentu[14]. Analisis dilakukan dengan memusatkan perhatian pada temuan hasil pemindaian keamanan untuk memecahnya ke dalam jenis kerentanan dan tingkat risikonya serta memahami hubungan antar temuan tersebut. Proses ini bertujuan untuk menyederhanakan informasi teknis hasil pengujian keamanan menjadi data yang lebih terstruktur dan mudah dipahami sebagai dasar penyusunan rekomendasi perbaikan[15].

Dalam konteks pengujian keamanan website, metode yang digunakan dalam penelitian ini lebih tepat dikategorikan sebagai vulnerability assessment berbasis *penetration testing* tools. Pengujian dilakukan menggunakan alat bantu otomatis, yaitu OWASP ZAP dan Nmap, untuk mengidentifikasi potensi kerentanan keamanan tanpa melakukan eksploitasi manual atau simulasi serangan secara penuh. Oleh karena itu, hasil penelitian difokuskan pada identifikasi dan klasifikasi potensi kerentanan sebagai dasar rekomendasi perbaikan keamanan sistem[16]. Subjek

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

penelitian merupakan sumber informasi yang dibutuhkan untuk pengumpulan data. Dua informan dari Institut Teknologi Indonesia (BPTI) berperan sebagai sumber atau subjek penelitian. Penelitian ini dilaksanakan dari tanggal 25 Desember 2024 hingga 6 Januari 2025 di BPTI UHAMKA. Pendekatan kualitatif digunakan untuk menafsirkan hasil pemindaian teknis ke dalam konteks pengelolaan keamanan website, sehingga data teknis yang dihasilkan tidak hanya disajikan secara numerik, tetapi dianalisis secara deskriptif untuk menghasilkan rekomendasi yang relevan.

2.2. Tahapan Penelitian

Gambar 1. Alur Tahapan Penelitian *Penetration Testing*

Gambar 1 menunjukkan alur tahapan penelitian yang digunakan dalam penelitian ini. Tahapan penelitian dimulai dari identifikasi masalah, yaitu penentuan objek penelitian dan perumusan permasalahan terkait keamanan website UHAMKA. Selanjutnya, dilakukan pengumpulan data melalui observasi, wawancara, dan dokumentasi untuk memperoleh informasi pendukung mengenai pengelolaan situs web dan sistem keamanannya. Tahap pengintaian dilakukan untuk mengumpulkan informasi awal mengenai domain, layanan, dan konfigurasi umum website yang menjadi objek penelitian. Setelah itu dilakukan tahap pemindaian, yang bertujuan untuk mengidentifikasi port terbuka serta potensi kerentanan keamanan menggunakan alat bantu pengujian. Hasil dari tahap pemindaian kemudian dianalisis pada tahap analisis kerentanan untuk menentukan jenis dan tingkat risiko kerentanan yang ditemukan. Tahap terakhir adalah pelaporan dan rekomendasi, yaitu penyusunan laporan hasil pengujian beserta saran perbaikan guna meningkatkan keamanan website. Alert hasil pemindaian OWASP ZAP difilter dengan menghilangkan temuan duplikat dan *informational alert* yang tidak berdampak langsung terhadap keamanan sistem. Selanjutnya, *alert* diklasifikasikan berdasarkan jenis kerentanan dan tingkat risiko *(low, medium, high)*. Penarikan kesimpulan dilakukan dengan mempertimbangkan frekuensi kemunculan dan potensi dampaknya terhadap sistem website.

2.3. Metode Pengumpulan Data

Metode pengumpulan data berikut digunakan dalam penelitian ini:

1. Observasi
   Teknik memantau perilaku manusia dan lingkungan fisik tempat perilaku itu terjadi secara sistematis dan terus menerus dari lokasi aktivitas alami untuk menghasilkan fakta disebut observasi. Kejadian-kejadian yang terjadi dijelaskan, dideskripsikan, dan dirinci melalui observasi. Penelitian ini dilakukan di kantor BPTI yang berlokasi di Jl. Tanah Merdeka No. 20, RT. 11/RW. 2, Rambutan, Kecamatan Ciracas, Kota Jakarta Timur, Daerah Khusus Ibu Kota Jakarta 13830. Periode penelitian selama dua minggu dimulai pada tanggal 25 Desember 2024 dan berakhir pada tanggal 6 Januari 2025.
2. Wawancara
   Wawancara adalah pertemuan di mana dua orang bertukar informasi dan pemikiran melalui pertanyaan dan jawaban untuk mendapatkan pemahaman yang lebih baik tentang suatu masalah tertentu. Wawancara digunakan untuk mengidentifikasi isu-isu yang memerlukan penyelidikan lebih lanjut serta untuk mempelajari informasi yang lebih mendalam dari responden.
3. Dokumentasi

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Dokumentasi merupakan catatan peristiwa yang sudah berlalu. Dokumentasi berfungsi untuk mengumpulkan data dari website UHAMKA dan data penting lainnya.

2.4. Metode Analisis Data

a. Metode *Penetration Testing*

Penetration testing adalah teknik yang mensimulasikan serangan peretasan terkontrol untuk menilai keamanan sistem komputer dan jaringan. Teknik ini digunakan untuk menemukan, memeriksa, dan menilai kemungkinan kelemahan keamanan pada sistem target. Dalam penelitian ini, *penetration testing* diterapkan sebagai metode analisis data untuk memperoleh gambaran tingkat keamanan website berdasarkan hasil temuan kerentanan yang teridentifikasi.

b. Tahapan *penetration testing* dalam penelitian ini meliputi:

1. Pengintaian
   Tahap pengintaian dilakukan untuk mengumpulkan informasi awal mengenai website UHAMKA, seperti nama domain, alamat IP, dan konfigurasi umum menggunakan *WHOIS*. Data ini digunakan untuk memetakan target dan mendukung proses pemindaian kerentanan.
2. Pemindaian
   Pada tahap pemindaian, peneliti menggunakan Nmap untuk memetakan port terbuka dan layanan yang berjalan pada server website UHAMKA. Hasil pemindaian divisualisasikan dengan Zenmap untuk mendukung identifikasi potensi kerentanan.
3. Analisis Kerentanan
   Tahap analisis kerentanan merupakan kelanjutan dari proses pengintaian dan pemindaian. Pada tahap ini, hasil pemindaian dari tools seperti Nmap dan OWASP ZAP dianalisis untuk mengidentifikasi potensi celah keamanan pada website yang diuji. Analisis dilakukan dengan mengelompokkan jenis kerentanan berdasarkan tingkat risiko dan dampaknya terhadap sistem. Temuan tersebut kemudian digunakan sebagai dasar penyusunan laporan serta rekomendasi perbaikan keamanan website.
   Hasil temuan pemindaian divalidasi dengan konfirmasi kepada pengelola sistem (wawancara) serta pengecekan terhadap dokumentasi untuk memastikan temuan bukan *false positive*.
4. Rekomendasi Pelaporan
   Hasilnya dikompilasi dalam laporan komprehensif setelah prosedur pengujian selesai[12]. Penelitian ini menyoroti efektivitas kedua alat dalam mendeteksi kerentanan dan menawarkan wawasan praktis tentang langkah-langkah mitigasi yang dapat diterapkan[15]. Hasil pelaporan ini diharapkan dapat menjadi acuan bagi pengelola sistem dalam meningkatkan keamanan website serta meminimalkan potensi serangan siber di masa mendatang.

3. HASIL DAN PEMBAHASAN

3.1. Dampak dari Serangan Siber terhadap Website dan Pengguna

Serangan siber terhadap website UHAMKA berpotensi menimbulkan dampak serius bagi institusi dan pengguna. Salah satu dampak utama dari serangan siber adalah risiko kehilangan atau kerusakan data institusional dan data pengguna akibat serangan seperti *malware, ransomware, atau DDoS.* Serangan siber juga berpotensi mengekspos data pribadi pengguna, seperti identitas dan informasi akademik, yang dapat disalahgunakan untuk tindakan penipuan atau pencurian identitas. Selain itu, serangan siber dapat menimbulkan kerugian finansial akibat biaya pemulihan sistem, perbaikan keamanan, dan potensi akses ilegal terhadap sumber daya institusi.

Dampak lain yang tidak kalah penting adalah penurunan kepercayaan pengguna terhadap website dan institusi pengelola. Gangguan keamanan seperti penyisipan konten ilegal atau perubahan tampilan akibat peretasan dapat merusak citra institusi di mata publik. Dalam lingkungan akademik, gangguan keamanan website berimplikasi pada terhambatnya akses informasi, layanan akademik, dan aktivitas administratif berbasis sistem digital. Oleh karena itu, keamanan website menjadi faktor krusial dalam menjaga keberlangsungan layanan informasi, stabilitas sistem, dan reputasi institusi pendidikan.

3.2. Penggunaan metode *Penetration Testing*

Penetration testing merupakan proses pengujian terhadap aset teknologi informasi yang bertujuan untuk mengidentifikasi celah keamanan yang berpotensi dieksploitasi oleh pihak tidak bertanggung jawab. Pengujian penetrasi dapat diotomatisasi dengan perangkat lunak atau dilakukan secara manual.

Penetration testing dikenal sebagai metode yang efektif untuk menilai tingkat keamanan suatu sistem informasi. Metode ini dilakukan melalui simulasi serangan nyata secara legal guna mengidentifikasi kerentanan yang berpotensi dimanfaatkan oleh peretas. Melalui *penetration testing*, pengelola sistem dapat mengetahui kelemahan keamanan sebelum dimanfaatkan oleh pihak eksternal yang berpotensi merugikan.

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Selain bertujuan untuk mengidentifikasi celah keamanan, *penetration testing* juga berperan dalam mengevaluasi efektivitas mekanisme pengamanan yang telah diterapkan pada sistem informasi. Hasil *penetration testing* umumnya berupa daftar kerentanan yang diklasifikasikan berdasarkan tingkat risiko untuk memudahkan pengelola sistem dalam menentukan prioritas perbaikan keamanan. Oleh karena itu, pengujian penetrasi berfungsi sebagai dasar pengambilan keputusan strategis dalam upaya peningkatan keamanan sistem secara berkelanjutan.

3.3. Celah Pada Website

Hasil laporan yang dihasilkan oleh aplikasi OWASP ZAP disajikan dalam format *HyperText Markup Language* (HTML) dan ditampilkan dalam bentuk tabel. Pada Tabel 1 ditampilkan tingkat risiko kerentanan keamanan beserta jumlah kerentanan yang terdeteksi. Selain itu, tabel tersebut juga memuat informasi mengenai tingkat risiko kerentanan, kategori atau jenis kerentanan, lokasi kerentanan, metode yang digunakan, parameter terkait, serta rekomendasi solusi untuk menangani kerentanan keamanan yang ditemukan. Penyajian data dalam bentuk tabel bertujuan untuk memudahkan proses analisis dan evaluasi terhadap celah keamanan yang teridentifikasi.

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (6.2%)	2 (12.5%)	1 (6.2%)	4 (25.0%)
	Low	0 (0.0%)	1 (6.2%)	4 (25.0%)	1 (6.2%)	6 (37.5%)
	Informational	0 (0.0%)	0 (0.0%)	4 (25.0%)	2 (12.5%)	6 (37.5%)
	Total	0 (0.0%)	2 (12.5%)	10 (62.5%)	4 (25.0%)	16 (100%)

Gambar 2. Ringkasan jumlah peringatan kerentanan berdasarkan tingkat risiko dan tingkat kepercayaan

Gambar 2 menunjukkan ringkasan hasil pemindaian keamanan website menggunakan OWASP ZAP berdasarkan tingkat risiko dan tingkat kepercayaan. Berdasarkan hasil pemindaian tersebut, ditemukan kerentanan dengan tingkat risiko menengah, rendah, dan informasional, serta tidak ditemukan kerentanan dengan tingkat risiko tinggi. Temuan ini mengindikasikan bahwa meskipun tidak terdapat kerentanan kritis yang secara langsung mengancam sistem, masih terdapat potensi kelemahan keamanan yang perlu diperhatikan. Kerentanan dengan tingkat risiko sedang dan rendah berpotensi dieksploitasi apabila tidak segera ditangani, sehingga diperlukan evaluasi dan perbaikan keamanan secara berkala untuk meningkatkan ketahanan website terhadap serangan siber.

http://uhamka.ac.id (1)

Content Security Policy (CSP) Header Not Set (1)

▼ GET http://uhamka.ac.id

Alert tags

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Request

▼ Request line and header section (224 bytes)

```
GET http://uhamka.ac.id HTTP/1.1
host: uhamka.ac.id
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Gambar 3. Temuan kerentanan *Content Security Policy* (CSP) *Header Not Set* pada website UHAMKA

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Gambar 3 menunjukkan hasil temuan kerentanan *Content Security Policy (CSP) Header Not Set* yang teridentifikasi oleh OWASP ZAP pada website UHAMKA. Kerentanan ini mengindikasikan bahwa website belum menerapkan kebijakan keamanan *CSP* yang berfungsi untuk membatasi sumber konten yang dapat dimuat oleh peramban pengguna. Kondisi tersebut berpotensi meningkatkan risiko serangan keamanan, seperti *cross-site scripting (XSS),* akibat tidak adanya pembatasan terhadap sumber skrip yang dijalankan pada halaman website. Oleh karena itu, penerapan dan konfigurasi *CSP* yang tepat diperlukan sebagai langkah mitigasi untuk meningkatkan perlindungan website terhadap potensi serangan siber.

Gambar 4. Respons server dan rekomendasi perbaikan kerentanan *Content Security Policy* (CSP)

Gambar 4 menunjukkan respons server website UHAMKA yang menampilkan informasi header HTTP serta rekomendasi perbaikan dari OWASP ZAP terkait kerentanan *Content Security Policy* (CSP). Informasi tersebut mengindikasikan bahwa server belum mengonfigurasi kebijakan CSP secara lengkap, sehingga diperlukan pengaturan tambahan pada sisi server atau aplikasi untuk membatasi sumber konten yang diizinkan. Rekomendasi yang diberikan oleh OWASP ZAP dapat dijadikan dasar dalam penyusunan saran perbaikan guna meningkatkan tingkat keamanan website.

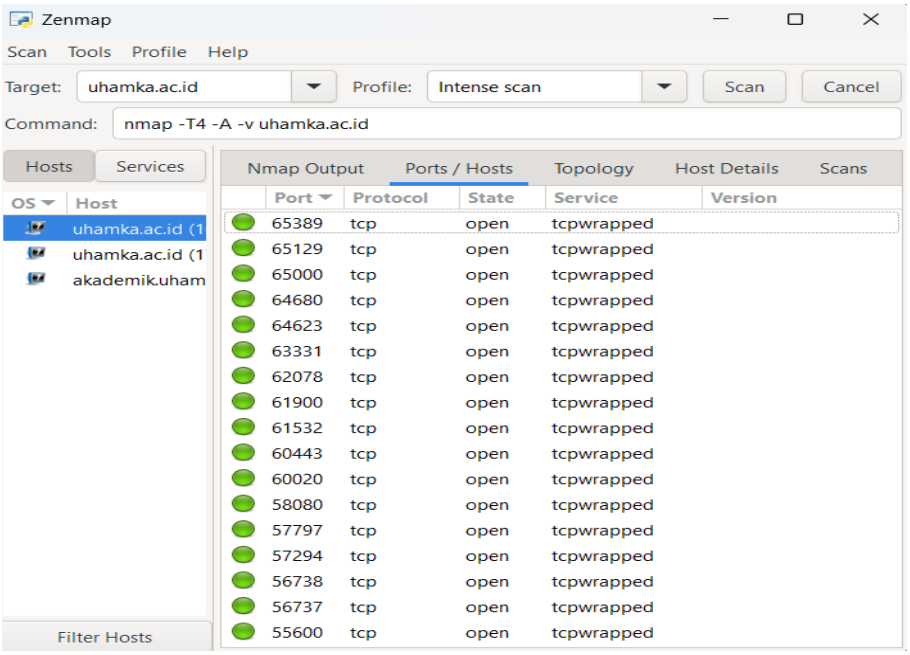
```
Domain ID: PANDI-DO151816
Domain Name: uhamka.ac.id
Created On: 2001-02-07 13:32:26
Last Updated On: 2024-11-03 02:17:18
Expiration Date: 2025-10-31 23:59:59
Status: clientUpdateProhibited
Status: clientDeleteProhibited
Status: serverTransferProhibited
Status: clientTransferProhibited

================================================
Sponsoring Registrar Organization: PT Web Commerce Communications
Sponsoring Registrar URL: www.merekmu.co.id
Sponsoring Registrar Street: Gedung Graha Raum Lt. 3 Ruang C  Jl. Tembus Kalimalang No. 1A-E   Ja
Sponsoring Registrar City: Kota Bekasi
Sponsoring Registrar State/Province: Jawa Barat
Sponsoring Registrar Postal Code: 17145
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 02189452129
Sponsoring Registrar Email: support@merekmu.co.id
Name Server: malcolm.ns.cloudflare.com
Name Server: romina.ns.cloudflare.com
DNSSEC: Unsigned
```

Gambar 5. Hasil pengumpulan informasi domain website UHAMKA menggunakan layanan WHOIS

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

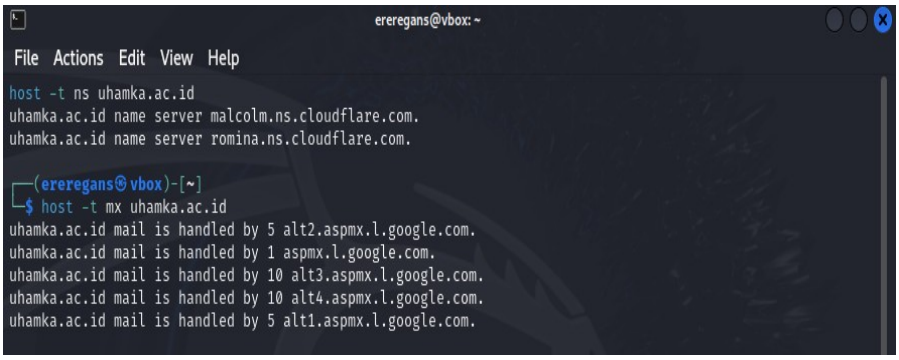
Gambar 5 menunjukkan hasil pengumpulan informasi *domain* website UHAMKA yang diperoleh melalui layanan *WHOIS*. Informasi yang ditampilkan meliputi identitas *domain*, status pengelolaan *domain*, *registrar*, serta *name server* yang digunakan. Data tersebut dimanfaatkan sebagai informasi pendukung pada tahap pengintaian untuk memahami konfigurasi awal domain sebelum dilakukan proses pemindaian dan analisis kerentanan.

Selain itu, informasi *WHOIS* membantu peneliti dalam mengidentifikasi pihak pengelola *domain* serta infrastruktur dasar yang digunakan, sehingga proses pemindaian dapat dilakukan secara lebih terarah dan sistematis.



Gambar 6. Hasil pemindaian port terbuka pada website UHAMKA menggunakan Zenmap

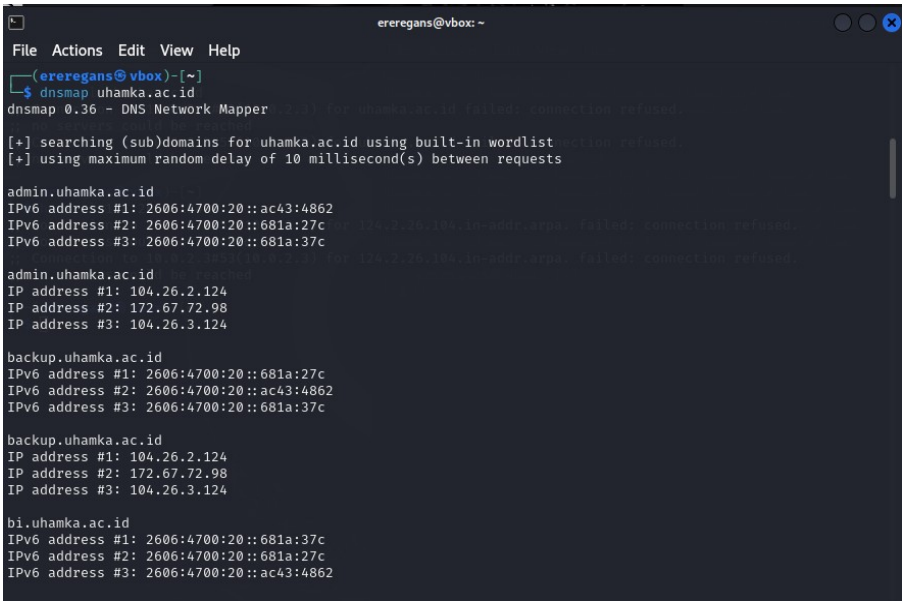
Gambar 6 menunjukkan hasil pemindaian *port* terhadap website UHAMKA menggunakan alat *Zenmap*. Hasil pemindaian menunjukkan adanya beberapa *port Transmission Control Protocol (TCP)* dalam kondisi terbuka yang menandakan layanan jaringan aktif pada server. Informasi ini digunakan sebagai dasar untuk mengidentifikasi potensi permukaan serangan sebelum dilakukan analisis kerentanan lebih lanjut.



Gambar 7. Hasil Analisis Kueri Rekaman DNS pada Domain Target

Gambar 7 menunjukkan data infrastruktur *DNS (Domain Name System)* yang digunakan oleh entitas target. Berdasarkan hasil pengujian, ditemukan bahwa manajemen resolusi nama domain dan layanan pertukaran surat elektronik telah didelegasikan kepada penyedia layanan komputasi awan. Analisis terhadap rekaman tersebut menunjukkan adanya implementasi sistem redundansi yang bertujuan untuk menjaga ketersediaan layanan dan meningkatkan keamanan pada lapisan jaringan. Temuan ini menjadi dasar dalam mengidentifikasi topologi logis sebelum dilakukan tahap evaluasi keamanan sistem lebih lanjut.

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index



Gambar 8. Hasil Pemetaan Subdomain dan Alamat Protokol Internet pada Domain Target

Gambar 8 menunjukkan hasil enumerasi subdomain melalui teknik *brute-force DNS*. Hasil analisis menunjukkan adanya beberapa sub-infrastruktur, seperti layanan administrasi dan sistem cadangan, yang telah mendukung teknologi *dual-stack*, yaitu penggunaan protokol IPv4 dan IPv6 secara bersamaan. Temuan ini mengindikasikan bahwa jaringan target memiliki kesiapan terhadap penerapan standar protokol internet terbaru. Namun demikian, keberadaan subdomain tersebut juga perlu mendapatkan perhatian khusus dari sisi keamanan, karena dapat berpotensi menjadi titik masuk serangan apabila tidak dikelola dan diamankan dengan konfigurasi yang tepat.

Gambar 9. Hasil Identifikasi Teknologi Web dan Metadata pada Domain Target

Gambar 9 menunjukkan profil teknologi yang digunakan oleh sistem target. Analisis menunjukkan penggunaan HTML5, server berbasis komputasi awan, dan penerapan kebijakan keamanan *Strict-Transport-Security (HSTS)*. Metadata ini mengonfirmasi bahwa platform telah mengintegrasikan protokol enkripsi untuk perlindungan data pengguna serta optimasi performa pada lapisan aplikasi.

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.googletagmanager.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://uhamka.ac.id	0 (0)	3 (3)	5 (8)	5 (13)
	http://uhamka.ac.id	0 (0)	1 (1)	0 (1)	1 (2)

Gambar 10. Ringkasan Tingkat Risiko Keamanan pada Infrastruktur Web

Gambar 10 menunjukkan statistik kerentanan yang terdeteksi melalui pemindaian dinamis. Hasil analisis menunjukkan dominasi temuan pada kategori Informational serta risiko rendah hingga menengah. Data ini

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

memberikan dasar evaluasi bagi pengelola sistem untuk melakukan penguatan keamanan pada aset digital yang memiliki skor risiko paling tinggi.

Tabel 1. Rekapitulasi Celah Keamanan pada Website Target

Tingkat Ancaman	Jenis Ancaman	Jumlah
Medium	*Content Security Policy (CSP) Header Not Set*	4
Medium	*Cross-Domain Misconfiguration*	2
Medium	*Hidden File Found*	4
Medium	*Missing Anti-clickjacking Header*	4
Low	*Cookie with SameSite Attribute None*	1
Low	*Cross-Domain JavaScript Source File Inclusion*	5
Low	*Private IP Disclosure*	1
Low	*Strict-Transport-Security Disabled*	11
Low	*Timestamp Disclosure - Unix*	3
Low	*X-Content-Type-Options Header Missing*	1

Pada Tabel 1 menampilkan rincian kerentanan yang ditemukan pada sistem melalui proses pemindaian keamanan otomatis. Berdasarkan data yang diperoleh, tidak ditemukan celah keamanan pada kategori kritis atau tinggi (*High*). Namun, teridentifikasi sejumlah ancaman pada kategori menengah (*Medium*) dan rendah (*Low*).

Analisis terhadap data tersebut menunjukkan bahwa kerentanan kategori menengah didominasi oleh masalah konfigurasi pada *header* keamanan, seperti belum diterapkannya *CSP* dan *Anti-clickjacking Header*. Sementara itu, pada kategori rendah, ditemukan ketidaksesuaian pada atribut cookie serta penonaktifan *Strict-Transport-Security* (HSTS) pada titik tertentu. Temuan ini mengindikasikan bahwa meskipun infrastruktur dasar memiliki pertahanan yang cukup, masih diperlukan optimalisasi konfigurasi pada lapisan aplikasi untuk memperkuat proteksi terhadap aktivitas intersepsi data dan serangan berbasis peramban.

3.4. Hasil Pengujian Metode *Penetration Testing* dan Celah yang Ditemukan

Situs web target memiliki beberapa celah keamanan yang dapat membahayakan keamanan situs web yang dikelola oleh BPTI, menurut hasil pemindaian yang dilakukan pada proses sebelumnya. Akibatnya, tindakan pencegahan dini harus segera dilakukan. Secara rata-rata, aplikasi otomatisasi OWASP ZAP mendeteksi celah keamanan pada plugin situs web tersebut. *Firewall* yang digunakan membantu situs web target, uhamka.ac.id, dengan memblokir dan segera mencegah serangan yang ditujukan pada celah keamanan yang teridentifikasi. Namun, sebagian besar plugin belum diperbarui oleh administrator, yang menyebabkan aplikasi pemindaian mengidentifikasi beberapa permintaan sebagai kerentanan. *False positive* dalam penelitian ini didefinisikan sebagai peringatan keamanan yang tidak dapat direproduksi atau divalidasi secara manual, atau peringatan keamanan yang tidak tervalidasi. Hal ini terjadi karena program mengidentifikasi kueri yang mungkin menunjukkan celah keamanan dan mengeluarkan peringatan. Selain itu, celah keamanan serius yang ditemukan di OWASP ZAP mengharuskan konfigurasi ulang pengaturan server untuk situs web target. Rekomendasi penulis, yang tercantum dalam Tabel 1, didasarkan pada semua tindakan yang dilakukan pada tahap sebelumnya.

3.5. Hasil Wawancara dan Saran Keamanan Website UHAMKA

Wawancara dilakukan secara semi-terstruktur dengan pihak BPTI untuk memperoleh informasi terkait kondisi keamanan website serta tanggapan terhadap hasil analisis kerentanan yang dilakukan. Hasil wawancara dicatat dan dianalisis secara kualitatif, yang menunjukkan bahwa penggunaan platform *WordPress* dan *framework* custom berbasis *NodeJS* serta *JavaScript* memberikan fleksibilitas dalam pengembangan web, namun juga meningkatkan potensi risiko terhadap serangan siber, sehingga diperlukan pengelolaan dan penguatan keamanan sistem yang lebih optimal.

Langkah-langkah yang telah diambil, seperti penggunaan *CDN*, firewall dari *Cloudflare*, cadangan rutin, dan pemantauan harian, menunjukkan komitmen BPTI dalam menjaga integritas dan keamanan sistem. Namun, fakta bahwa serangan seperti judi online terjadi setiap hari menunjukkan bahwa tantangan ini tidak bisa dianggap remeh. Sistem pemantauan dan respons yang telah diterapkan, dengan waktu respons rata-rata 1-2 jam, merupakan praktik yang baik, tetapi masih ada ruang untuk perbaikan, terutama dalam hal pencegahan.

Kendala utama yang dihadapi, seperti kekurangan SDM yang terampil dan anggaran terbatas untuk perangkat keras dan lunak keamanan, adalah masalah umum yang dihadapi oleh banyak institusi. Solusi yang diusulkan, seperti peningkatan keterampilan SDM dan pembentukan tim siber khusus, adalah langkah strategis yang sangat penting. Ini menunjukkan bahwa BPTI tidak hanya reaktif terhadap ancaman tetapi juga proaktif dalam merencanakan masa depan.

Idealis: Indonesia Journal Information System
Volume 9, Nomor 1, Januari 2026
ISSN 2684-7280 (*online*)
Halaman 113-123
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Untuk meningkatkan keamanan website UHAMKA, disarankan agar BPTI fokus pada peningkatan kapasitas SDM melalui pelatihan rutin dan program sertifikasi di bidang keamanan siber. Hal ini penting untuk meningkatkan keahlian tim dalam menangani insiden dengan lebih cepat dan efisien. Selain itu, penguatan infrastruktur keamanan dengan mengadopsi perangkat keras dan lunak tambahan seperti firewall canggih dan sistem deteksi intrusi akan memberikan lapisan perlindungan yang lebih kuat. Memperbarui dan menguji prosedur tanggap insiden secara berkala juga akan memastikan kesiapan tim dalam menghadapi ancaman terbaru.

4. KESIMPULAN DAN SARAN

Sebagai hasil analisis terhadap data yang diperoleh, BPTI UHAMKA telah menunjukkan upaya serius dalam menjaga keamanan website melalui penerapan berbagai teknologi pendukung, seperti penggunaan *Content Delivery Network* (CDN), firewall berbasis *Cloudflare*, serta mekanisme pemantauan sistem yang dilakukan secara berkala. Langkah-langkah tersebut berperan penting dalam meningkatkan ketersediaan layanan, melindungi website dari serangan dasar, serta meminimalkan dampak gangguan terhadap pengguna.

Namun demikian, hasil analisis juga menunjukkan bahwa intensitas serangan yang terjadi setiap hari, khususnya serangan berupa penyisipan konten dan promosi situs judi online, menegaskan bahwa tantangan keamanan siber yang dihadapi masih sangat kompleks dan dinamis. Serangan-serangan tersebut memanfaatkan celah keamanan aplikasi maupun konfigurasi sistem yang belum sepenuhnya optimal, sehingga berpotensi menurunkan kepercayaan pengguna serta merusak reputasi institusi.

Selain faktor teknis, kendala non-teknis seperti keterbatasan sumber daya manusia dan anggaran juga menjadi hambatan utama dalam upaya peningkatan keamanan sistem secara menyeluruh. Keterbatasan ini berdampak pada kemampuan pengelola dalam melakukan pemantauan lanjutan, pembaruan sistem secara rutin, serta penerapan mekanisme keamanan lanjutan yang membutuhkan keahlian khusus.

Oleh karena itu, peningkatan kapasitas sumber daya manusia melalui pelatihan berkelanjutan dan sertifikasi di bidang keamanan siber, serta penguatan infrastruktur teknologi informasi dengan perangkat keamanan yang lebih komprehensif, menjadi langkah strategis yang perlu diprioritaskan. Pendekatan yang lebih proaktif dan berkelanjutan ini diharapkan dapat meningkatkan kesiapan BPTI UHAMKA dalam menghadapi ancaman siber di masa mendatang, sekaligus memastikan keamanan, integritas, dan keandalan layanan website secara optimal.

DAFTAR PUSTAKA

[1] T. Anugrah, "PENETRATION TESTING KEAMANAN WEBSITE STIE SAMARINDA MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 1, Jan. 2024, doi: 10.23960/jitet.v12i1.3882.

[2] H. Irawan and M. N. I. Wicaksono, "MERANCANG BANGUN WEB E-COMMERCE MENGGUNAKAN WORDPRESS STUDI KASUS TOKO ARLEUIS," *IDEALIS: InDonEsiA journaL Information System*, vol. 5, no. 1, pp. 9–18, Jan. 2022, doi: 10.36080/idealis.v5i1.2882.

[3] F. Widianto, E. S. Wijaya, H. Harjono, and A. P. Wicaksono, "Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 1, pp. 155–166, Jan. 2025, doi: 10.52436/1.jpti.609.

[4] D. Rohmaniah, W. M. Ashari, L. Lukman, and A. D. Putra, "Enhancing Website Security Using Vulnerability Assessment and *Penetration Testing* (VAPT) Based on OWASP Top Ten," *Journal of Applied Informatics and Computing*, vol. 9, no. 2, pp. 404–411, Mar. 2025, doi: 10.30871/jaic.v9i2.9069.

[5] E. S. Alim, N. Nuroji, M. A. Rizkiawan, T. Anhari, and B. Sobari, "Monitoring dan Pencegahan Serangan Judi Online (Slot Gacor) pada Website," *Edumatic: Jurnal Pendidikan Informatika*, vol. 8, no. 1, pp. 75–83, Jun. 2024, doi: 10.29408/edumatic.v8i1.25267.

[6] R. Marta Dinata, M. Alzril, M. I. Yamin, H. Effendi, and M. Febriansyah, "Analisis Keamanan Situs Web Rumah Sakit Menggunakan Metode *Penetration Testing* OWASP," *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI*, vol. 35, no. 2, pp. 99–100, Jun. 2025, doi: 10.37277/stch.v35i2.2383.

[7] H. Sofyan, M. Sugiarto, and B. M. Akbar, "Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN 'Veteran' Yogyakarta", *Telematika*, vol. 20, no. 2, pp. 153–162, Jun. 2023., doi: 10.31315/telematika.v20i2.7757.

[8] Ade Gustiyonoo, E. Irawadi Alwi, and S. Mubarak Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode *Penetration Testing*," *Cyber Security dan Forensik Digital*, vol. 7, no. 1, pp. 25–33, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4432.

[9] Luthfi Arian Nugraha, "Website Penetration Analysis Against XSS Attacks using Payload Method," *Journal of Innovation Information Technology and Application (JINITA)*, vol. 6, no. 1, pp. 37–44, Jun. 2024, doi: 10.35970/jinita.v6i1.2225.

[10] B. A. Bagaskara, Mohammad Idhom, and Henni Endah Wahanani, "PENGUJIAN WEBSITE DINAS SOSIAL SURABAYA MENGGUNAKAN METODE PENETRATION TESTING DAN OWASP TOP 10," *Jurnal Informatika dan Rekayasa Elektronik*, vol. 8, no. 1, pp. 40–50, Apr. 2025, doi: 10.36595/jire.v8i1.1375.

[11] L. F. Burhani and D. Priyawati, "ANALISIS PENGUJIAN KEAMANAN WEBSITE PENGELOLAAN INTERNET DESA KRAGAN MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 1, pp. 307–319, Feb. 2024, doi: 10.29100/jipi.v9i1.4455.

[12] G. Y. Jayanto, J. P. P. Naibaho, and A. De Kweldju, "The Analisis Celah Keamanan Website Poltekkes Kemenkes Sorong Menggunakan Metode *Penetration Testing*," *SMATIKA JURNAL*, vol. 15, no. 01, pp. 136–150, Jun. 2025, doi: 10.32664/smatika.v15i01.1549.

[13] A. Agustinus and I. Sembiring, "WEBSITE VULNERABILITY TESTING USING THE PENETRATION TESTING METHOD REFERRING TO NIST SP 800 – 155 (CASE STUDY (Astonprinter.com Domain))," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 6, pp. 1651–1662, Dec. 2024, doi: 10.52436/1.jutif.2024.5.6.3859.

[14] T. Tan and Benfano Soewito, "Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity," *Journal of Information System, Applied, Management, Accounting and Research*, vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[15] F. Widianto, E. S. Wijaya, H. Harjono, and A. P. Wicaksono, "Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 1, pp. 155–166, Jan. 2025, doi: 10.52436/1.jpti.609.

[16] R. Pitriyani, G. Triyono, and S. Y. Nugroho, "PENGEMBANGAN MODEL SISTEM E-COMMERCE BERBASIS WEB DENGAN CONTENT MANAGEMENT SYSTEM (CMS)," *IDEALIS: InDonEsiA journaL Information System*, vol. 4, no. 1, pp. 37–46, Jan. 2021, doi: 10.36080/idealis.v4i1.2818.