



Analisis *Vulnerability Assessment* pada Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP

Aura Arnelia Zahrani ^{1*}, Dzihni Safwa Alifah², Yulia Cahyani³, Ilham Albana⁴

¹⁻⁴Program Studi Teknologi Informasi, Universitas Amikom Purwokerto, Indonesia

Alamat: Jalan Letjend Pol Soemarto, Watumas, Purwokerto Utara

Korespondensi penulis: auraarnelia123@gmail.com*

Abstract. Information system security is a crucial aspect in maintaining the confidentiality and integrity of user data. The IITC Intermedia website of Amikom Purwokerto University serves as an information system for national events and stores participants' personal data, necessitating a security evaluation. This study aims to analyze vulnerabilities on the website using the Vulnerability Assessment method with the OWASP ZAP tool. The research process involves data collection, vulnerability scanning, result analysis based on the OWASP Top 10 2021 categories, and providing technical recommendations. The scan results revealed 23 vulnerabilities, consisting of 1 high-risk, 4 medium-risk, 9 low-risk, and 9 informational findings. Among these, 15 vulnerabilities fall under the OWASP Top 10 classification. Key vulnerabilities identified include the use of outdated JavaScript libraries, security header misconfigurations, and weaknesses in session management and access control. Based on these findings, several mitigation measures are recommended to strengthen system security. This study emphasizes the importance of implementing OWASP standards in the development and management of web-based information systems.

Keywords: Information System, OWASP Top 10, OWASP ZAP, Vulnerability Assessment, Website Security.

Abstrak. Keamanan sistem informasi merupakan aspek penting dalam menjaga kerahasiaan dan integritas data pengguna. Website IITC Intermedia Universitas Amikom Purwokerto berfungsi sebagai sistem informasi event nasional dan menyimpan data pribadi peserta, sehingga memerlukan evaluasi keamanan. Penelitian ini bertujuan untuk menganalisis kerentanan pada website tersebut menggunakan metode Vulnerability Assessment dengan alat bantu OWASP ZAP. Proses penelitian dilakukan melalui tahapan pengumpulan data, pemindaian kerentanan, analisis hasil berdasarkan kategori OWASP Top 10 tahun 2021, serta pemberian rekomendasi teknis. Hasil pemindaian menunjukkan terdapat 23 kerentanan, terdiri dari 1 risiko tinggi (high), 4 risiko sedang (medium), 9 risiko rendah (low), dan 9 bersifat informasional (informational). Dari seluruh kerentanan yang ditemukan, 15 di antaranya termasuk dalam klasifikasi OWASP Top 10. Beberapa kerentanan utama yang ditemukan meliputi penggunaan pustaka JavaScript yang rentan, kesalahan konfigurasi header keamanan, serta kelemahan pada manajemen sesi dan kontrol akses. Berdasarkan hasil tersebut, direkomendasikan sejumlah tindakan mitigasi untuk memperkuat keamanan sistem. Penelitian ini menegaskan pentingnya penerapan standar OWASP dalam pengembangan dan pengelolaan sistem informasi berbasis web.

Kata kunci: Sistem Informasi, Vulnerability Assessment, OWASP ZAP, Website Security, OWASP Top 10

1. LATAR BELAKANG

Perkembangan teknologi informasi sudah cukup pesat yang sebagian besar kegiatan manusia pada era digital sekarang tidak lepas dari teknologi, contohnya dari berbagai jenis kegiatan yang berbasis teknologi seperti e-commerce, event kampus, e-government, e-bisnis dan sebagainya [1]. Masyarakat mulai memanfaatkan teknologi khususnya yaitu website untuk berbagai kegiatan. Pemanfaatan teknologi digital seperti website dapat meningkatkan kinerja, menghemat biaya dan sumber daya, serta memudahkan masyarakat dalam mengakses informasi yang akurat dan cepat, sekaligus memberikan pelayanan yang lebih efektif secara digital [2].

Adanya teknologi yang telah berkembang pesat, memiliki tantangan tersendiri yang menjadi ancaman serius yakni dari segi keamanan siber yang dapat menyerang kapan saja seiring meningkatnya ketergantungan masyarakat terhadap teknologi digital. Kejahatan siber merupakan bentuk aktivitas kriminal di ranah digital yang meliputi tindakan seperti peretasan sistem, penipuan daring, pencurian data pribadi, serta distribusi perangkat lunak berbahaya seperti malware dan virus [3]. Sementara jumlah pengguna internet di Indonesia menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2024 mencapai 221 juta orang, sehingga semakin mudah menimbulkan dampak positif dan negative tergantung bijak tidaknya dalam memanfaatkan internet [4]. Berdasarkan data oleh National Cyber Security Index (NCSI) menunjukkan bahwa kasus kejahatan siber di Indonesia sebesar 63.64 poin menempati posisi 49 dari 160 negara pada tahun 2023 [5].

Website IITC merupakan website event berupa lomba tingkat nasional yang diselenggarakan oleh UKM Intermedia Universitas Amikom Purwokerto. Website ini sebagai system informasi event yang mencakup ketentuan dan persyaratan lomba yang diselenggarakan, sebagai registrasi peserta dalam mengikuti event tersebut. Data yang diinputkan oleh peserta meliputi data pribadi yang cukup penting sehingga keamanan terhadap data memiliki kerahasiaan yang cukup tinggi, sehingga keamanan yang di terapkan juga harus cukup baik.

Keamanan informasi cukup penting karena keamanan siber merupakan suatu aktifitas pencegahan dan juga pengamanan suatu platform di era digital. Sehingga pengetahuan mengenai keamanan siber merupakan hal yang sangat penting untuk menciptakan sumber daya manusia yang paham terhadap kesadaran keamanan [6]. Mengetahui kerentanan website merupakan hal yang sangat penting untuk dapat dilakukan peningkatan keamanan agar tidak mudah di eksploitasi. Langkah untuk melakukan analisis celah keamanan pada sebuah website dapat menggunakan OWASP (Open Web Application Security Project) merupakan panduan utama dalam pengujian keamanan aplikasi website dengan salah satu metode yang cukup familiar digunakan dalam menganalisis keamanan aplikasi website adalah Vulnerability Assessment [7]. Namun terdapat standar kerentanan yaitu OWASP Top 10 yang merupakan dokumen standar yang memuat daftar sepuluh jenis kerentanan paling umum dan berisiko tinggi pada aplikasi web, yang sering dijumpai di berbagai organisasi. Fokus utama dokumen ini adalah membantu dalam mengidentifikasi dan memitigasi ancaman keamanan yang paling kritis [8]. Dibuktikan menurut penelitian oleh rohim dkk [9] yakni melakukan analisis celah

keamanan pada system website pembelajaran e-learning perguruan tinggi untuk mengetahui celah risiko kerentanan. Pada penelitian oleh Adha dkk [10] melakukan pengujian keamanan website universitas mataram menggunakan vulnerability assessment yang ditemukan beberapa kerentanan masuk pada level tinggi, sedang dan rendah sehingga dapat merekomendasikan perbaikan untuk meningkatkan keamanan layanan website. Kemudian pada penelitian oleh Saputra dkk [11] menganalisis assessment vulnerability pada (e-government) website dan aplikasi dinas komunikasi informatika dan statistic kota banda aceh yang bertujuan untuk mengidentifikasi, evaluasi dan mitigasi potensi kerentanan yang dapat muncul agar dapat diperbaiki kelemahan yang teridentifikasi. Pada penelitian oleh Gregorius [12] mengimplementasi OWASP ZAP untuk menguji keamanan system informasi akademik menemukan 19 kerentanan dan berdasarkan OWASP TOP 10 terdeteksi memiliki 4 kerentanan. Dengan demikian menunjukkan bahwa menganalisis celah keamanan website menggunakan metode Vulnerability Assessment dengan OWASP terbukti dapat dilakukan secara efektif.

Vulnerability assessment merupakan suatu tahapan sistematis dalam mengidentifikasi dan memprioritaskan kerentanan pada sistem informasi, aplikasi, dan infrastruktur jaringan. Proses ini berperan penting dalam memberikan wawasan menyeluruh kepada organisasi terkait potensi risiko keamanan yang dihadapi, sehingga memungkinkan pengambilan tindakan mitigasi yang tepat. Penilaian ini umumnya dilakukan dengan bantuan perangkat pemindai otomatis, yang hasilnya didokumentasikan dalam bentuk laporan sebagai dasar analisis lebih lanjut [9]. Oleh karena itu berdasarkan permasalahan diatas perlu dilakukan analisis keamanan untuk mengetahui ancaman dan risiko yang dapat terjadi pada website IITC. Proses analisis keamanan menggunakan teknik analisis kerentanan OWASP ZAP dengan metode vulnerability assessment yang bertujuan untuk melihat kerentanan yang dapat terjadi dan seberapa aman website yang digunakan.

2. KAJIAN TEORITIS

Keamanan Sistem Informasi

Keamanan sistem informasi merupakan aset penting yang wajib dijaga. Secara umum, keamanan dapat diartikan sebagai suatu kondisi atau kualitas yang menjamin perlindungan dari berbagai bentuk ancaman atau bahaya. Aspek-aspek keamanan informasi meliputi [13]:

- a. *Confidentiality* (Kerahasiaan) merupakan aspek untuk menjamin kerahasiaan suatu informasi memastikan bahwa informasi hanya dapat di akses oleh orang yang berwenang terhadap data yang di akses, dikirim atau di simpan.
- b. *Integrity* (Integritas) merupakan aspek untuk menjamin bahwa data tidak dirubah tanpa izin dari pihak yang memiliki wewenang untuk menjaga keutuhan dan keakuratan data informasi.
- c. *Availability* (Ketersediaan) merupakan aspek untuk menjamin bahwa data informasi dapat tersedia dengan baik saat dibutuhkan dan memastikan user berhak menggunakan informasi.

Vulnerability Assessment

Vulnerability adalah kerentanan yang dapat mengancam CIA (*Confidentiality, Integrity, Availability*). *Vulnerability Assessment* (VA) merupakan proses pemindaian terhadap sistem, perangkat lunak, dan jaringan untuk mengidentifikasi kelemahan atau celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab sebagai *backdoor* untuk melakukan serangan. Jenis kerentanan yang umum ditemukan antara lain mencakup *access control vulnerability, boundary condition vulnerability, input validation vulnerability, authentication vulnerabilities, configuration weakness vulnerabilities*, serta *exception handling vulnerabilities* [14].

Open Web Application Security (OWASP)

OWASP (*Open Web Application Security Project*) merupakan framework open source yang berfokus pada peningkatan keamanan perangkat lunak, khususnya aplikasi web. Organisasi ini bertujuan untuk mengidentifikasi dan mengatasi celah keamanan dalam aplikasi. Berdasarkan standar OWASP, terdapat sebelas tahapan utama dalam proses penilaian dan pengujian keamanan website, meliputi: *Information Gathering, Configuration Management, Secure Transmission, Authentication, Session Management, Authorization, Cryptography, Data Validation, Denial of Service*, dan *Error Handling* [15]. Menurut Priambodo [8] terdapat Top 10 2021 kerentanan yang paling berbahaya dan sering terjadi sebagai berikut :

Tabel 1. Top 10 2021 kerentanan yang paling berbahaya dan sering terjadi

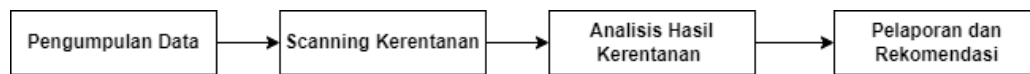
No	Nama Kerentanan	Kode OWASP	Deskripsi Singkat
1	Broken Access Control	A01:2021	Terjadi saat pembatasan hak akses tidak diterapkan dengan benar, memungkinkan akses tidak sah ke data atau fungsi aplikasi.
2	Cryptographic Failures	A02:2021	Gagalnya perlindungan terhadap data sensitif akibat penggunaan kriptografi yang lemah atau tidak memadai.
3	Injection	A03:2021	Kerentanan akibat input tidak terpercaya yang dikirim ke interpreter, memungkinkan eksekusi perintah berbahaya.
4	Insecure Design	A04:2021	Desain sistem yang tidak mempertimbangkan aspek keamanan sejak awal, akibat kurangnya analisis risiko.
5	Security Misconfiguration	A05:2021	Konfigurasi keamanan yang salah atau tidak optimal, termasuk penggunaan pengaturan default dan pembaruan sistem yang tidak rutin.
6	Vulnerable and Outdated Components	A06:2021	Penggunaan komponen yang sudah usang dan diketahui memiliki celah keamanan, yang dapat dieksploitasi penyerang.
7	Identification and Authentication Failures	A07:2021	Kegagalan dalam pengelolaan autentikasi dan sesi yang memungkinkan penyalahgunaan token atau kredensial pengguna.
8	Software and Data Integrity Failures	A08:2021	Ketergantungan pada komponen eksternal yang tidak terpercaya tanpa validasi integritas, yang berisiko menyebabkan manipulasi kode atau data.
9	Security Logging and Monitoring Failures	A09:2021	Lemahnya sistem pencatatan dan pemantauan membuat serangan tidak terdeteksi, memberi waktu bagi penyerang untuk mengeksploitasi sistem.
10	Server-Side Request Forgery (SSRF)	A10:2021	Terjadi saat aplikasi mengakses sumber eksternal tanpa validasi URL, memungkinkan penyerang mengakses sistem internal melalui celah permintaan.

OWASP ZAP

Zed Attack Proxy (ZAP) merupakan alat uji penetrasi bersifat *open-source* yang dikembangkan oleh OWASP, khusus untuk pengujian keamanan aplikasi web. Secara fungsional, ZAP bertindak sebagai *man-in-the-middle proxy*, yang memungkinkan penyadapan, analisis, dan modifikasi lalu lintas data antara browser dan aplikasi web sebelum diteruskan ke tujuan [15].

3. METODE PENELITIAN

Dalam melakukan analisis kerentanan website pertama penelitian ini melakukan pengumpulan data berupa wawancara singkat mengenai kerentanan yang pernah terjadi sebelumnya kemudian melakukan pengumpulan informasi keamanan siber dan risikonya melalui studi literatur. Proses analisis kerentanan menggunakan metode *Vulnerability Assesment* yang dilakukan dengan melakukan scanning pengujian pada website IITC untuk mengetahui kerentanan dan kualitas dengan *Vulnerablity Scanning Tools* OWASP ZAP. Dalam penelitian ini akan dilakukan melalui beberapa tahapan pengujian agar lebih terstruktur, seperti kerangka penelitian sebagai berikut:



Gambar 1. Tahapan penelitian

a. Pengumpulan Data

Pada tahapan ini dilakukan pengumpulan data mengenai target system informasi yang akan dilakukan pengujian keamanan dengan melakukan wawancara singkat mengenai keamanan sebelumnya dan pengumpulan informasi mengenai website, teknis kebutuhan aplikasi yang akan digunakan untuk melakukan *scanning* kerentanan (*vulnerability assesment*) suatu sistem informasi website melalui studi literatur.

b. *Scanning* Kerentanan

Melakukan tahapan proses *scanning* website menggunakan OWASP ZAP untuk menemukan kerentanan yang ada pada website

c. Analisis Hasil Kerentanan

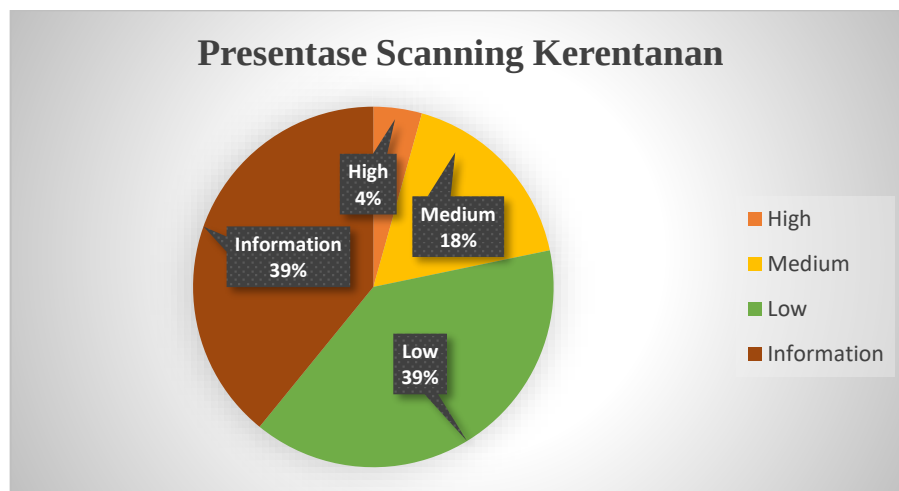
Mengidentifikasi kerentanan yang ditemukan untuk dikelompokkan dalam skala risiko yang tinggi, sedang ataupun rendah dan juga diidentifikasi untuk dikategorikan berdasarkan OWASP TOP 10.

d. Pelaporan dan Rekomendasi

Pada tahapan terakhir ini merupakan tahapan untuk melaporkan temuan temuan dari hasil *scanning* kerentanan website dengan mendokumentasikan kelompok kerentanan sesuai dengan skala risikonya dan memberikan rekomendasi perbaikan.

4. HASIL DAN PEMBAHASAN

Tahapan ini dilakukan analisis melalui scanning terhadap potensi kerentanan yang terdapat pada system informasi website IITC Intermedia Universitas Amikom Purwokerto. Proses scanning dilakukan dengan aplikasi OWASP ZAP untuk mengetahui kerentanan website. Berikut peresentase tingkatan risiko kerentanan dari hasil scanning menggunakan aplikasi OWASP ZAP:



Gambar 2. Presentasi daftar kerentanan

Berikut daftar kerentanan yang berhasil ditemukan berdasarkan hasil *scanning* menggunakan aplikasi OWASP ZAP:

Tabel 2. Hasil scanning kerentanan

No	Kerentanan	Risiko	Kategori OWASP Top 10
1	Vulnerable JS Library	High	A06:2021
2	Content Security Policy (CSP) Header Not Set	Medium	A05:2021
3	Cross-Domain Misconfiguration	Medium	-
4	Missing Anti-clickjacking Header	Medium	A05:2021
5	Session ID in URL Rewrite	Medium	A05:2021
6	Cookie No Http Only Flag	Low	A02:2021
7	Cookie Without Secure Flag	Low	A02:2021
8	Cookie without Same Site Attribute	Low	A02:2021
9	Cross-Domain JavaScript Source File Inclusion	Low	A05:2021
10	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	-

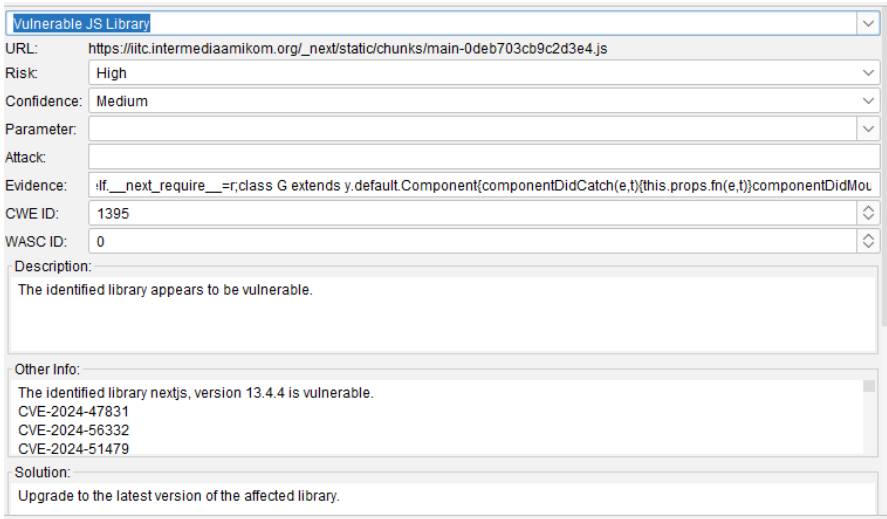
11	<i>Server Leaks Version Information via "Server" HTTP Response Header Field</i>	Low	-
12	<i>Strict-Transport-Security Header Not Set</i>	Low	A05:2021
13	<i>Timestamp Disclosure - Unix</i>	Low	-
14	<i>X-Content-Type-Options Header Missing</i>	Low	A05:2021
15	<i>Content-Type Header Missing</i>	Informational	A05:2021
16	<i>Information Disclosure - Information in Browser sessionStorage</i>	Informational	-
17	<i>Information Disclosure - Sensitive Information in URL</i>	Informational	-
18	<i>Information Disclosure - Suspicious Comments</i>	Informational	-
19	<i>Loosely Scoped Cookie</i>	Informational	A02:2021
20	<i>Modern Web Application</i>	Informational	A04:2021
21	<i>Re-examine Cache-control Directives</i>	Informational	A05:2021
22	<i>Retrieved from Cache</i>	Informational	-
23	<i>Session Management Response Identified</i>	Informational	A07:2021

Pada tabel 2 diatas menunjukkan hasil scanning kerentanan pada website IITC ditemukan sebanyak 23 kerentanan yang memiliki tingkatan risiko yang berbeda-beda mulai dari risiko yang *high*, *medium*, *low* dan *informational*. Pada 23 kerentanan yang terdeteksi, sebanyak 15 kerentanan dikategorikan ke dalam standar kerentanan OWASP Top 10 web application dimana standar kerentanan yang berbahaya dan sering banyak terjadi.

Tabel 3. Dampak dan rekomendasi kerentanan high

No.	Jenis Kerentanan	Dampak Potensial	Rekomendasi Teknis
1	<i>Vulnerable JavaScript Library</i>	Potensi eksploitasi melalui pustaka dengan kerentanan yang diketahui publik.	Memperbarui semua pustaka pihak ketiga ke versi terbaru yang aman dan lakukan audit rutin terhadap dependensi.

Risk = High, Confidence = Medium



Gambar 3. Detail *vulnerable js library*

Kerentanan yang ditemukan *Vulnerable JS Library* memiliki tingkat risiko yang tinggi dan masuk ke dalam kategori OWASP Top 10 A06:2021 sehingga ini yang perlu dilakukan perbaikan sesuai rekomendasi dengan memperbarui ke versi terbaru.

Tabel 4. Dampak dan rekomendasi kerentanan medium

No.	Jenis Kerentanan	Dampak Potensial	Rekomendasi Teknis
2	<i>Content Security Policy (CSP) Header Not Set</i>	Terbuka terhadap serangan Cross-Site Scripting (XSS) dan penyisipan konten tidak sah.	Implementasikan header CSP untuk mengontrol sumber daya eksternal yang dapat dimuat oleh browser.
3	<i>Cross-Domain Misconfiguration</i>	Akses lintas domain yang tidak dibatasi dapat dimanfaatkan untuk melakukan serangan origin spoofing.	Konfigurasikan header CORS (Access-Control-Allow-Origin) dengan lebih ketat dan sesuai kebutuhan.
4	<i>Missing Anti-clickjacking Header</i>	Rentan terhadap serangan clickjacking yang dapat mengecoh pengguna.	Tambahkan header X-Frame-Options atau Content-Security-Policy: frame-ancestors untuk membatasi framing.
5	<i>Session ID in URL Rewrite</i>	Session ID dapat terekspos dalam log, referer, atau dibagikan tidak sengaja.	Gunakan cookie aman untuk manajemen sesi dan hindari menempatkan session ID dalam URL.

Risk = Medium, Confidence = Medium (3,4)

Risk = Medium, Confidence = High (2,5)

Pada tingkat risiko medium termasuk ke dalam kategori OWASP Top 10 2013:2021 yaitu kerentanan *Content Security Policy (CSP) Header Not Set*, *Missing Anti-clickjacking Header*, *Session ID in URL Rewrite*. Kerentanan pada tingkat medium ini harus segera diperbaiki meskipun tidak secara langsung menyebabkan eksploitasi kritis, namun mereka dapat digunakan sebagai pintu masuk oleh penyerang yang memiliki pengalaman lebih atau sebagai serangan berlapis (*multi-stage attack*).

Tabel 5. Dampak dan rekomendasi kerentanan low

No.	Jenis Kerentanan	Dampak Potensial	Rekomendasi Teknis
6	<i>Cookie Without Http Only Flag</i>	Cookie dapat diakses melalui JavaScript dan dimanfaatkan oleh penyerang melalui XSS.	Aktifkan atribut HttpOnly untuk mencegah akses skrip ke cookie.
7	<i>Cookie Without Secure Flag</i>	Cookie dapat dikirim melalui koneksi HTTP tidak terenkripsi.	Aktifkan atribut Secure agar cookie hanya dikirim melalui HTTPS.
8	<i>Cookie Without Same Site Attribute</i>	Cookie rentan terhadap serangan Cross-Site Request Forgery (CSRF).	Tambahkan atribut SameSite (misalnya Strict atau Lax) untuk membatasi penggunaan lintas situs.
9	<i>Cross-Domain JavaScript Inclusion</i>	Menyertakan skrip dari domain luar berpotensi membuka pintu serangan jika sumber tidak terpercaya.	Gunakan skrip dari sumber terpercaya, dan implementasikan Subresource Integrity (SRI).
10	<i>Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</i>	Mengungkap teknologi backend dapat memudahkan penyerang melakukan fingerprinting.	Nonaktifkan atau ubah header X-Powered-By di konfigurasi server.
11	<i>Server Leaks Version Information via "Server" HTTP Response Header Field</i>	Menyediakan informasi spesifik tentang software server (misalnya Apache, Nginx).	Sembunyikan atau ubah konfigurasi header Server pada HTTP response.
12	<i>Strict-Transport-Security Header Not Set</i>	Pengguna dapat di-downgrade ke protokol HTTP, meningkatkan risiko MITM.	Tambahkan header Strict-Transport-Security (HSTS) untuk memaksa penggunaan HTTPS.
13	<i>Timestamp Disclosure (Unix)</i>	Informasi waktu sistem dapat digunakan untuk profiling dan perencanaan serangan.	Hindari menampilkan timestamp dalam format mentah di response atau sumber halaman.

14	<i>X-Content-Type-Options Header Missing</i>	Browser dapat menebak tipe MIME, memungkinkan XSS berbasis MIME sniffing.	Tambahkan X-Content-Type-Options: nosniff untuk memaksa validasi MIME.
-----------	--	---	--

Risk = Low, Confidence = Low (13)

Risk = Low, Confidence = Medium (6,7,8,9,10,14)

Risk = Low, Confidence = High (11,12)

Pada tingkat risiko low termasuk ke dalam kategori OWASP Top 10 202:2021 sebanyak 3 kerentanan, 205:2021 sebanyak 3 kerentanan juga dan 3 lagi tidak masuk kategori OWASP Top 10. Kerentanan pada Tingkat ini umumnya berdampak rendah terhadap system informasi, namun tetap berpotensi membuka celah keamanan tambahan jika dimanfaatkan dengan kerentanan yang lain. Maka dari itu, meskipun kerentanan ini bersifat minor, perlu dilakukan perbaikan untuk mencegah eskalasi risiko yang tidak terdeteksi sebelumnya.

Tabel 6. Dampak dan rekomendasi kerentanan informational

No.	Jenis Kerentanan	Dampak Potensial	Rekomendasi Teknis
15	<i>Content-Type Header Missing</i>	Browser dapat salah menafsirkan jenis konten dan memicu eksekusi yang tidak diinginkan.	Tetapkan secara eksplisit jenis konten melalui header Content-Type.
16	<i>Information Disclosure in sessionStorage</i>	Data di sessionStorage dapat diakses oleh skrip berbahaya pada halaman yang sama.	Hindari menyimpan informasi sensitif pada browser storage, terutama yang dapat diakses oleh JS.
17	<i>Sensitive Information in URL</i>	Informasi sensitif yang ditampilkan di URL dapat tersimpan di log, cache, atau histori.	Gunakan metode POST dan hindari menyisipkan data rahasia dalam parameter URL.
18	<i>Suspicious Comments</i>	Komentar dalam kode dapat memberikan informasi penting kepada penyerang.	Hapus atau sembunyikan komentar yang mengandung detail teknis atau jalur file.
19	<i>Loosely Scoped Cookie</i>	Cookie dapat dikirim ke subdomain yang tidak perlu, memperbesar permukaan serangan.	Batasi domain cookie sesuai kebutuhan menggunakan atribut Domain yang spesifik.
20	<i>Modern Web Application (Info)</i>	Menunjukkan penggunaan teknologi modern tanpa penilaian keamanan terperinci.	Lakukan audit keamanan menyeluruh terhadap fitur-fitur modern yang digunakan.
21	<i>Re-examine Cache-Control Directives</i>	Data sensitif dapat disimpan oleh browser atau proxy secara tidak tepat.	Gunakan Cache-Control: no-store dan Pragma: no-cache.

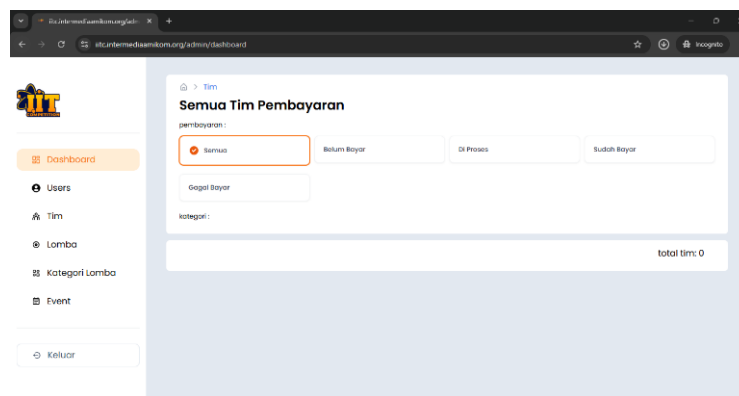
			cache untuk konten sensitif.
22	<i>Retrieved from Cache</i>	Halaman cache dapat dimuat ulang oleh pengguna yang berbeda (shared terminals).	Hindari cache pada konten personal atau dinamis, terutama di lingkungan publik.
23	<i>Session Management Response Identified</i>	Informasi tentang manajemen sesi dapat dimanfaatkan untuk serangan prediktif atau pencurian sesi.	Minimalkan informasi sesi dalam response dan amankan ID sesi dengan rotasi dan timeout.

Risk = Informational, Confidence = Low (18, 19,21)

Risk = Informational, Confidence = Medium (15,17,20,22,23)

Risk = Informational, Confidence = High (16)

Pada tingkat risiko informational termasuk ke dalam kategori OWASP Top 10 A02:2021 yaitu *Loosely Scoped Cookie*, A04:2021 yaitu *Modern Web Application*, A05:2021 yaitu *Content-Type Header Missing*, *Re-examine Cache-control Directives*, A07:2021 yaitu *Session Management Response Identified*. Kerentanan pada tingkat informational ini tidak langsung menimbulkan risiko eksploitasi namun tetap penting untuk diperhatikan karena dapat memberikan indikasi kelemahan konfigurasi atau praktik pengembangan yang kurang optimal, terutama karena beberapa di antaranya berhubungan dengan kerangka kerja OWASP Top 10, yang menandakan bahwa potensi risiko bisa meningkat jika dikombinasikan dengan kelemahan lainnya dalam sistem



Gambar 4. Kerentanan *broken access control* admin

Ketika dilakukan pengujian secara manual ditemukan kerentanan *Broken Access Control* pada website dikarenakan penyerang dapat masuk ke laman admin tanpa login, hanya dengan menambahkan route `/admin/dashboard` pada link website. Dengan hal itu penyerang dapat mengakses, menghapus data yang seharusnya tidak dapat mereka akses dan dapat melakukan modifikasi baik pada menu event, persyaratan dan data user.

5. KESIMPULAN DAN SARAN

Website IITC Intermedia Universitas Amikom Purwokerto merupakan sistem informasi yang memiliki tingkat akses berbeda-beda bagi setiap pengguna serta menyimpan data pengguna yang bersifat sensitif. Berdasarkan hasil pemindaian kerentanan menggunakan OWASP ZAP, ditemukan 23 jenis kerentanan pada website tersebut. Dari total kerentanan yang ditemukan 15 kerentanan termasuk ke dalam kategori OWASP Top 10 tahun 2021, yang merupakan daftar prioritas kerentanan paling berisiko dalam aplikasi web modern.

Berdasarkan tingkat risikonya:

- a. Terdapat 1 kerentanan diklasifikasikan dalam tingkat risiko tinggi (high).
- b. Terdapat 4 kerentanan tergolong risiko sedang (medium).
- c. Terdapat 9 kerentanan tergolong risiko rendah (low).
- d. Terdapat 9 kerentanan masuk dalam kategori informasi (informational).

Kerentanan-kerentanan tersebut mencakup berbagai aspek keamanan seperti kesalahan konfigurasi header HTTP, kebocoran informasi, pengelolaan sesi yang tidak aman, serta penggunaan pustaka JavaScript yang rentan. Hal ini menunjukkan bahwa sistem informasi IITC Intermedia masih memiliki celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, sehingga perlu segera dilakukan perbaikan dan penguatan keamanan sesuai dengan rekomendasi OWASP.

DAFTAR REFERENSI

- Adha, M., KWA, Z. D., & Muhammad, A. H. (2023). Website security test at the University of Mataram using vulnerability assessment. *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 8(2), 647–655. <https://doi.org/10.29100/jupi.v8i2.3830>
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (n.d.). *Jumlah pengguna internet Indonesia tembus 221 juta orang*. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).
- Faliandy, M. Y. L., & Sutabri, T. (2023). Analisis kesadaran keamanan siber pada pengguna aplikasi E-Court di lingkungan pengadilan. *Jurnal Ilmiah Binary STMIK Bina Nusantara Jaya Lubuklinggau*, 5(2), 101–107. <https://doi.org/10.52303/jb.v5i2.106>
- Hasibuan, A. F., Tommy, & Handoko, D. (2023). Analisis kerentanan website dengan aplikasi OWASP ZAP. *Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)*, 2(2), 141–154.
- Kusuma, G. H. A. (2022). Implementasi OWASP ZAP untuk pengujian keamanan sistem informasi akademik. *Jurnal Teknologi Informasi: Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika*, 16(2).

- NCSI. (n.d.). *National Cyber Security Index (NC SI): Indonesia*. National Cyber Security Index (NC SI).
- Noe'man, H., Hartanti, D., & Prayitno, H. (2021). Pelatihan pembuatan website dalam menghadapi perkembangan teknologi bagi siswa di SMK Galajuaa Bekasi. *Journals Journal of Computer Science Contributions*, 1(2), 111–118.
- Nurrahman, A., Dimas, M., Ma'sum, M. F., Ino, M. F., Institut, A., & Dalam Negeri, P. (2021). Pemanfaatan website sebagai bentuk digitalisasi pelayanan publik di Kabupaten Garut. *Jurnal Teknologi dan Komunikasi Pemerintahan*, 3(1), 78–93. <http://ejournal.ipdn.ac.id/JTKP>
- Pembuktian, T., Kasus, D., Siber-Nurul, K., Al, E., Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum*, 5. <https://doi.org/10.54209/judge.v5i02.566>
- Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration testing Web XYZ berdasarkan OWASP Risk Rating. *Teknika*, 12(1), 33–46. <https://doi.org/10.34148/teknika.v12i1.571>
- Rohim, A., & Setiyani, L. (2023). Analisis celah keamanan E-Learning perguruan tinggi menggunakan vulnerability assessment. *JIPAKIF*, 1(1), 1–10. <http://jurnal.edunovationresearch.org/>
- Saputra, R., Abdullah, D., Daud, M., Maulana, F. R., & Studi Magister Teknologi Informasi. (2024). Analisis assessment vulnerability pada website dan aplikasi publik di Dinas Komunikasi Informatika dan Statistik Kota Banda Aceh. *Jurnal Janitra Informatika dan Sistem Informasi*, 4(2), 87–91. <https://doi.org/10.59395/janitra.v4i2.205>
- Supriadi, D., Suryadi, E., Muslim, R., Samsumar, L. D., & Universitas Teknologi Mataram. (2024). Implementasi Vulnerability Assessment OWASP (Open Web Application Security Project) pada website Universitas Teknologi Mataram. *Journal of Data Analytics, Information, and Computer Science (JDAICS)*, 1(4), 3032–4696.
- Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, 6(1).
- Zirwan, A. (2022). Pengujian dan analisis kewanaman website menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi dan Teknologi*, 70–75. <https://doi.org/10.37034/jidt.v4i1.190>