Analisis Keamanan Sistem Informasi Menggunakan Owasp Untuk Menguji Kerentanan Website: Studi Kasus PT XYZ

1st Muhammad Ryan Vivaldi
Sistem Informasi
Telkom University
Surabaya, Indonesia
ryanvivaldi@student.telkomuniversity.ac.id

2nd Muhammad Nasrullah
Sistem Informasi
Telkom University
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Rizky Fenaldo M.
Teknik Informatika
Telkom University
Surabaya, Indonesia
rizkyfenaldo@telkomuniversity.ac.id

***Abstrak* — Keamanan sistem informasi menjadi tantangan utama dalam pengoperasian website, terutama bagi platform publik seperti situs berita PT XYZ yang memiliki hampir 300 ribu kunjungan bulanan. Tingginya lalu lintas pengguna meningkatkan risiko eksploitasi celah keamanan. Pada tahun sebelumnya, PT XYZ mengalami insiden siber yang menghapus seluruh *database* situs. Meskipun data berhasil dipulihkan, kejadian ini menyoroti lemahnya sistem keamanan yang berpotensi menurunkan kepercayaan pengguna. Untuk mencegah insiden serupa, dilakukan pengujian keamanan menggunakan *framework OWASP*, khususnya *OWASP Top 10 2021* dan *OWASP ZAP*. Pengujian dilakukan pada tiga *subdomain*: Situs XYZ, XYZ Jurnalis, dan XYZ Editor. Hasil menunjukkan terdapat 20 kerentanan, terdiri dari 4 risiko tinggi, 10 sedang, dan 6 rendah. Temuan utama meliputi potensi *SQL Injection*, absennya *header* keamanan, penggunaan komponen usang, serta kurangnya perlindungan terhadap *brute force*. Rekomendasi perbaikan mencakup penerapan *HTTPS*, penambahan *header* seperti *CSP* dan *HSTS*, pembaruan komponen, validasi *input*, serta implementasi mekanisme anti-*bot*. Langkah-langkah ini penting untuk meningkatkan ketahanan situs dari serangan siber dan menjaga kepercayaan pengguna.**

Kata kunci*— Keamanan Sistem Informasi, OWASP, *Vulnerability Test*, *Penetration Test

I. PENDAHULUAN

Perkembangan teknologi jaringan komputer dan internet telah mengubah cara bisnis beroperasi secara signifikan [1] Website, sebagai salah satu teknologi digital yang umum digunakan, memberikan aksesibilitas yang luas bagi pengguna untuk mengakses informasi dan layanan tanpa terkendala oleh batasan letak dan waktu [2]. Perkembangan teknologi digital telah mendorong meningkatnya penggunaan website sebagai media utama dalam penyebaran informasi, termasuk pada portal berita online [3]. Salah satu contoh media daring yang memanfaatkan teknologi tersebut adalah PT XYZ, yang didirikan pada tanggal 17 Agustus 2015 oleh PT XYZ. PT XYZ memiliki dua situs web utama, yaitu Situs XYZ dan XYZ Jurnalis dan XYZ Editor. Situs Situs XYZ berfungsi sebagai portal publik yang menyajikan berita kepada pembaca, sedangkan XYZ Jurnalis dan XYZ Editor digunakan sebagai sistem manajemen konten yang mendukung aktivitas internal jurnalis dan editor dalam mengelola, menulis, serta menerbitkan berita.

Saat ini, PT XYZ mencatat kunjungan bulanan yang hampir menyentuh angka 300 ribu, menunjukkan tingginya tingkat akses dan interaksi pengguna terhadap layanannya. Dengan tingginya tingkat kunjungan tersebut, aspek keamanan menjadi semakin krusial. Kebocoran data dan peretasan dapat memberikan dampak yang sangat merugikan terhadap reputasi sebuah media [4]. Tidak hanya itu, praktik spoofing atau peniruan website yang banyak digunakan untuk menyebarkan misinformasi juga dapat merusak citra media [5]. Ancaman siber tersebut memiliki dampak yang serius terhadap masyarakat. Rendahnya kepercayaan terhadap suatu media akibat banyaknya serangan membuat masyarakat menjadi semakin skeptis terhadap media tertentu [6].

Menurut hasil wawancara PT XYZ pernah mengalami insiden peretasan yang menyebabkan seluruh database terhapus akibat serangan siber, kejadian tersebut terjadi pada tahun 2022, tepatnya pada saat hari raya idul fitri. Meskipun data dapat dipulihkan dari cadangan, kejadian ini menunjukkan adanya celah keamanan yang dapat dieksploitasi. Kasus serupa juga terjadi di media outlet Indonesia lainnya. Pada tahun 2020, Konde.co mengalami serangan DDoS setelah merilis artikel sensitif terkait Kementerian Koperasi [7]. Project Multatuli, media online yang fokus melaporkan isu-isu perjuangan kaum marjinal, juga menjadi korban serangan siber. Pada tahun 2023, mereka menerima serangan DDoS jenis HTTP Flood, botnet, scraping data, hingga payload attack, setelah menerbitkan laporan investigatif terkait isu sensitif [8]. Selain itu, Tempo.co pernah mengalami serangan siber berupa DDoS pada tanggal 7 April 2025. Serangan tersebut melibatkan sekitar 120 juta payload yang menyerang antara pukul 17.50 hingga 19.20 WIB, menyebabkan gangguan akses layanan [9].

Penelitian ini akan menganalisis keamanan sistem informasi pada website portal berita online dengan menggunakan standar OWASP Top 10 2021 serta alat OWASP ZAP untuk menguji potensi kerentanan, dan

hasilnya diharapkan dapat memberikan rekomendasi strategis untuk meningkatkan keamanan website serta mengurangi risiko serangan siber yang dapat mengganggu operasional maupun kepercayaan pengguna.

Maka pada penelitian ini akan dilakukan analisis keamanan sistem informasi berupa uji penetrasi terhadap website Situs XYZ. Uji penetrasi bertujuan untuk mengidentifikasi dan memanfaatkan kelemahan yang mungkin ada dalam sistem, dengan tujuan akhir untuk meningkatkan tingkat keamanan secara keseluruhan. Uji penetrasi pada penelitian ini menggunakan kerangka kerja OWASP Top 10 2021. OWASP Top 10 2021 adalah daftar yang disusun oleh komunitas Open Web Application Security Project (OWASP) dunia yang mengidentifikasi sepuluh kerentanan keamanan perangkat lunak web yang paling umum. Penggunaan kerangka kerja ini dianggap penting karena telah diadopsi secara luas oleh organisasi dan ahli keamanan di seluruh dunia. Penelitian ini akan memberikan hasil berupa rekomendasi aksi sebagai langkah pencegahan. Diharapkan rekomendasi ini dapat memitigasi risiko yang teridentifikasi, memperkuat lapisan keamanan, dan secara keseluruhan melindungi website Situs XYZ dari potensi serangan siber.

II. KAJIAN TEORI

A. Sistem Informasi

Sistem informasi adalah kombinasi dari prosedur, perangkat lunak, perangkat keras, data, dan sumber daya manusia yang bekerja bersama untuk mengelola dan menyebarkan informasi guna mendukung operasi organisasi [10]. Tujuannya adalah mengubah data menjadi informasi yang berguna untuk pengambilan keputusan dan pengelolaan operasional. Website merupakan salah satu bentuk sistem informasi yang penting di era digital [2], berfungsi tidak hanya sebagai penyedia informasi, tetapi juga sebagai sarana interaksi, pengelolaan data, dan transaksi.

B. Keamanan Sistem Informasi

Keamanan sistem informasi bertujuan melindungi informasi yang diolah, disimpan, dan ditransmisikan oleh sistem, dengan menjaga kerahasiaan, keutuhan, dan ketersediaan data. Upaya ini mencakup penerapan kebijakan akses yang ketat agar hanya pengguna yang berwenang dapat mengakses data sensitif. Dalam era teknologi yang terus berkembang, keamanan informasi menjadi semakin penting bagi keberlangsungan operasional organisasi [11].

C. Penetration Testing

Pengujian penetrasi adalah metode untuk menilai keamanan sistem dengan mensimulasikan serangan eksternal guna menemukan celah yang dapat dieksploitasi [12]. Tujuannya untuk mengidentifikasi dan memperbaiki kerentanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Penelitian ini menggunakan metode *black-box testing*, yaitu pengujian tanpa pengetahuan tentang struktur internal sistem [13]. Penguji hanya berinteraksi melalui antarmuka, memberikan input tertentu, dan mengamati output yang dihasilkan.

D. Black Box Testing

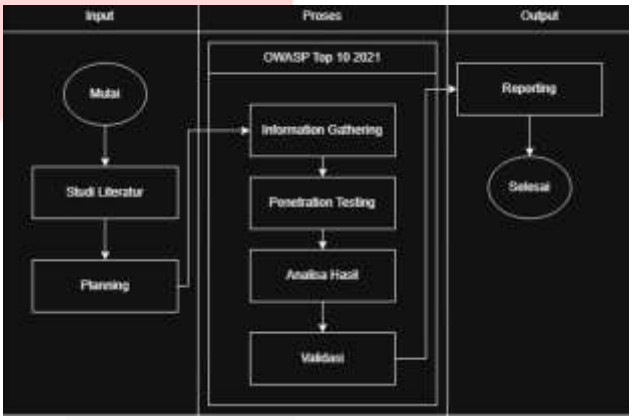
Black Box Testing adalah metode pengujian perangkat lunak yang mengevaluasi fungsionalitas sistem dari sudut pandang pengguna akhir, tanpa mengetahui struktur internal atau kode program. Pengujian dilakukan melalui antarmuka dengan memberikan input dan memverifikasi output, untuk memastikan sistem berfungsi sesuai harapan dan memenuhi persyaratan fungsional.

E. OWASP Top 10 2021

OWASP Top 10 2021 adalah daftar sepuluh kerentanan paling umum pada aplikasi web yang disusun oleh Open Web Application Security Project (OWASP) berdasarkan analisis industri dan penelitian terkini. Daftar ini menjadi acuan penting bagi pengembang dan profesional keamanan dalam mengenali ancaman utama selama siklus pengembangan aplikasi. Versi 2021 mencakup pembaruan signifikan, termasuk tiga kategori baru, perubahan nama dan cakupan empat kategori, serta beberapa penggabungan[14].

III. METODE

A. Alur Penelitian



GAMBAR 1
(ALUR PENELITIAN)

Proses penelitian terbagi menjadi tiga bagian utama: *Input, Proses,* dan *Output*. Bagian pertama, yakni *Input*, melibatkan studi literatur dan Planning. Pada bagian Proses, dilakukan *information gathering*, *vulnerability scan* dan *attacking* atau *penetration testing*. Sedangkan pada tahap terakhir, yakni bagian *Output*, terdapat analisis hasil, validasi, dan *reporting*. Bagian Proses dan *Output* mengacu pada OWASP TOP 10 2021 sebagai metode penelitian.

IV. HASIL DAN PEMBAHASAN

A. Information Gathering

Pada tahap ini, dilakukan pengujian menggunakan kombinasi aplikasi dan perintah pada sistem operasi dan Kali Linux. Aplikasi yang digunakan meliputi Wappalyzer dan OWASP ZAP, sedangkan perintah yang dijalankan melalui Kali Linux mencakup Nmap dan Whois.

1. Wappalyzer

Proses Information Gathering dimulai dengan menggunakan *Wappalyzer* untuk mengidentifikasi teknologi yang digunakan oleh situs web. *Wappalyzer* memberikan informasi yang komprehensif mengenai berbagai teknologi terkait website. Informasi ini sangat penting untuk memahami struktur dan potensi kerentanan situs web. Detail lengkap mengenai teknologi yang terdeteksi oleh *Wappalyzer* dapat dilihat pada Tabel 1 dan 2.

TABEL 1
(HASIL WAPPALYZER SITUS XYZ)

Teknologi	Keterangan	Versi
Teknologi	Keterangan	Versi
JavaScript Library	jQuery Flickity FancyBox	3.4.1 - 3.5.7
UI Frameworks	Bootstrap	4.3.1
FontScripts	Google Font API Font Awesome	- -
Misc	PWA Open Graph HTTP/3	- - -
CDN	cdnjs Cloudflare	- -
Performance	Cloudflare Rocket Loader	-

TABEL 2
(HASIL WAPPALYZER XYZ JURNALIS DAN EDITOR)

Teknologi	Keterangan	Versi
Web frameworks	Laravel	-
UI frameworks	Bootstrap	5.3.3
Programming Language	PHP	-
CDN	jsDelivr	
Cloudflare	-	
-		
Web frameworks	Laravel	-

2. Nmap

Tahap *network mapping* pada situs Situs XYZ.com dilakukan menggunakan perintah sudo nmap -sS -sV di Kali Linux untuk memindai domain utama dan dua *subdomain*. Pemindaian ini mengidentifikasi port terbuka, layanan yang aktif, dan versinya. Hasil menunjukkan bahwa port 80, 443, 8080, dan 8443 terbuka dan menggunakan layanan *Cloudflare HTTP Proxy*. Port 80 dan 8080 melayani HTTP, sementara 443 dan 8443 digunakan untuk HTTPS. Karena lalu lintas diarahkan melalui Cloudflare, informasi detail sistem asli tersembunyi, sehingga meningkatkan perlindungan dari potensi serangan langsung.

TABEL 3
(HASIL NMAP UNTUK 3 SITUS XYZ)

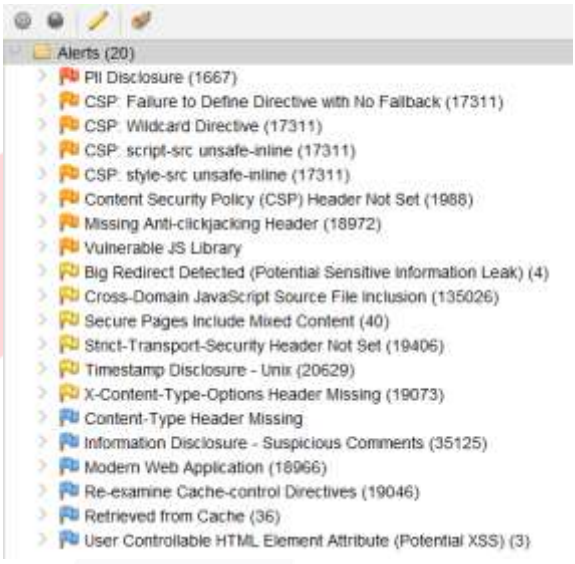
PORT	STATE	SERVICE	VERSION
80	Open	http	Cloudflare http proxy
443	Open	ssl/http	Cloudflare http proxy
8080	Open	http	Cloudflare http proxy
8443	Open	ssl/http	Cloudflare http proxy

3. Whois

Hasil WHOIS domain Situs XYZ memuat informasi seperti nama domain, ID registri, dan data registrar termasuk server WHOIS, URL, serta kontak penyalahgunaan. Tanggal penting seperti pendaftaran, pembaruan terakhir, dan masa berlaku juga ditampilkan. Status domain seperti *client Transfer Prohibited* menunjukkan perlindungan terhadap perubahan tanpa izin. Selain itu, dicantumkan *name server* yang digunakan untuk pengelolaan DNS dan status *DNSSEC* sebagai indikator apakah domain dilindungi oleh sistem keamanan DNS tambahan.

4. OWASP ZAP

Proses pemindaian kerentanan dilakukan pada website situs XYZ menggunakan OWASP ZAP. Hasil pemindaian menunjukkan bahwa website memiliki total 20 kerentanan



GAMBAR 2
(HASIL OWASP ZAP)

B. Penetration Testing

1. A02:2021 – *Cryptographic Failures*

Pengujian keamanan pada domain https://SitusXYZ/ mengungkap beberapa temuan penting. Melalui OWASP ZAP, ditemukan *mixed content* pada halaman artikel, serta ketiadaan pengaturan HSTS yang membuat browser tidak memaksa koneksi aman secara otomatis. Uji SSL Scan menunjukkan dukungan terhadap protokol usang TLSv1.0 dan TLSv1.1, yang rentan terhadap serangan seperti BEAST dan POODLE. Cipher suite yang digunakan (AES128-SHA dan AES256-SHA) juga sudah tidak aman karena tidak mendukung AEAD. Sementara itu, pengujian dengan curl menunjukkan bahwa meski HTTP dialihkan ke HTTPS, HSTS belum diaktifkan, sehingga koneksi awal tetap bisa melalui jalur tidak aman.

TABEL 4
(HASIL PENTEST A02)

Test	Parameter	Temuan	Keterangan
OWASP ZAP	Artikel berita pada https://Situs XYZ/	1. Secure Pages Include Mixed Content 2. HSTS not set	1. Konten gambar tidak dimuat melalui HTTPS 2. HSTS tidak disetel
SSL Scan	https://Situs XYZ/	1. Protokol TLS usang 2. Cipher Usang	1. TLSv1.0 dan TLSv1.1 sudah rentan terhadap sejumlah serangan kriptografi seperti BEAST dan POODLE 2. AES128-SHA dan AES256-SHA tidak

Test	Parameter	Temuan	Keterangan
			mendukung AEAD (Authenticated Encryption with Associated Data)
Curl	https://Situs XYZ/	*1. HSTS not set*	1. HTTP sudah dipindah permanen ke HTTPS namun HSTS masih belum disetel sehingga tidak semua akses wajib melewati HTTPS

2. A03:2021 – *Injection*

Pengujian lanjutan menggunakan OWASP ZAP dan Burp Suite pada berbagai endpoint seperti https://SitusXYZ/?target=amp, https://SitusXYZ/search?q=ZAP, serta domain XYZ Jurnalis dan XYZ Editor, menunjukkan potensi XSS namun tanpa eksekusi payload yang berhasil. Artinya, tidak terbukti adanya kerentanan XSS. Alat ParamSpider menemukan 646.762 URL valid pada Situs XYZ, namun tidak ada URL valid di dua domain lainnya. Tidak ditemukan parameter rentan terhadap injeksi SQL, sebagaimana dikonfirmasi oleh SQLMap dan pengujian manual menggunakan Burp Suite pada fitur login XYZ Editor dan search bar Situs XYZ. Seluruh request diproses server tanpa ada eksploitasi berhasil. Meskipun pada fitur pencarian ditemukan respon HTTP 301 terhadap input berbahaya—yang seharusnya tidak muncul dalam interaksi normal—hal ini hanya mengindikasikan potensi pengolahan input yang tidak aman, bukan bukti kerentanan SQLi.

TABEL 5
(HASIL PENTEST A03)

Test	Parameter	Temuan	Keterangan
OWASP ZAP & Burp Suite	https://Situs XYZ/?target=amp https://Situs XYZ/search?q=ZAP https://XYZ Jurnalis https://XYZ Editor	1. Potensi terjadinya XSS	1. Tidak ada XSS Injection yang berhasil
Param Spider	https://Situs XYZ/ https://XYZ Jurnalis https://XYZ Editor	1. Terdapat 646762 url valid hasil paramspider pada website XYZ 2. 0 url valid hasil paramspider pada website cmsnew dan netnew	1. Pada 646762 url yang dihasilkan paramspider tidak ada parameter yang terindikasi dapat diinjeksi dengan SQL
SQLMap & Burp Suite	https://Situs XYZ/ https://XYZ Jurnalis https://XYZ Editor	1. SQLMap tidak menemukan parameter yang dapat diinjeksi 2. Burp Suite mengirim dan mendapat respon dari server 3. *SQL Injection* situs XYZ memberi	1. Tidak ada indikasi kerentanan 2.Tidak ada hasil *SQL Injection* yang berhasil 3. Status code 301 tidak seharusnya muncul pada search bar, karena umumnya digunakan untuk pengalihan URL.

3. A04:2021 – Insecure Design

Pengujian manual pada https://XYZ Jurnalis dan https://XYZ Editor menunjukkan tidak adanya *rate limiting* pada proses login. Artinya, pengguna dapat mencoba login tanpa batasan waktu, tanpa peringatan atau pemblokiran setelah percobaan gagal. Kondisi ini membuka peluang terjadinya serangan *bruteforce*, di mana penyerang dapat menebak kredensial secara terus-menerus. Uji coba ini mengacu pada kategori OWASP A07 (*Broken Authentication*) untuk menguji kerentanan terhadap serangan login *bruteforce*

TABEL 6
(HASIL PENTEST A04)

Test	Parameter	Temuan	Keterangan
Manual	https://XYZ Jurnalis https://XYZ Editor	1. Tidak ada rate limit untuk login	1. Sistem tetap merespon gagal login tanpa adanya peringatan, jeda waktu atau pemblokiran

4. A05:2021 – *Security Misconfiguration*

Pengujian dengan OWASP ZAP pada Situs XYZ menemukan tidak adanya *Content-Security-Policy* (CSP), *CSP frame-ancestors*, serta pengaturan *X-Content-Type-Options: nosniff*. Ketiadaan CSP dan penggunaan wildcard (*) membuka potensi serangan seperti *clickjacking*, sementara pengaturan MIME sniffing yang tidak tepat meningkatkan risiko keamanan.

Uji coba dengan Burp Suite Clickandit menunjukkan ketiga situs (Situs XYZ, XYZ Jurnalis, dan XYZ Editor) rentan terhadap *clickjacking*, terbukti dari interaksi pengguna yang dapat dimanipulasi.

Pengujian menggunakan Nuclei juga menemukan bahwa Situs XYZ tidak menerapkan header keamanan penting dan tidak memiliki mekanisme *Subresource Integrity* (SRI), yang meningkatkan risiko terhadap serangan seperti XSS, *clickjacking*, dan modifikasi skrip dari CDN eksternal.

TABEL 7
(HASIL PENTEST A05)

Test	Parameter	Temuan	Keterangan
OWASP ZAP	https://Situs XYZ/	1. *Content-Security-Policy* tidak disetel 2. *CSP frame-ancestors* tidak diterapkan 3. *X-Content-Type-Options* tidak disetel ke nosniff	1. CSP tidak disetel serta menggunakan wildcard (*) 2. Terdapat potensi kerentanan untuk serangan clickjacking 3. Terdapat potensi terjadinya MIME Sniffing.
Burp Click Bandit	https://Situs XYZ/ https://XYZ Jurnalis https://XYZ Editor	1. Ditemukan kerentanan terhadap *clickjacking* pada ketiga website	1. Pengujian Clickjacking berhasil memanipulasi interaksi pengguna.

Test	Parameter	Temuan	Keterangan
Nuclei	https://Situs XYZ/	1. Tidak diterapkannya a header keamanan penting pada situs Situs XYZ 2. Tidak ada mekanisme *Subresource Integrity*	1. Ketiadaan header keamanan tersebut meningkatkan potensi serangan seperti clickjacking, XSS, dan sniffing MIME sniffing. 2. potensi modifikasi skrip dari sumber eksternal (seperti CDN) dapat mengekspos aplikasi terhadap risiko perubahan yang tidak sah

5. A06:2021 – *Vulnerable and Outdated Component*

Pengujian dengan OWASP ZAP dan *Wappalyzer* pada Situs XYZ menemukan penggunaan *Bootstrap* versi 4.3.1 yang sudah usang dan memiliki kerentanan *XSS* (*Cross-Site Scripting*). Kerentanan ini memungkinkan penyerang menyuntikkan skrip berbahaya ke halaman web. Sementara itu, XYZ Jurnalis dan XYZ Editor telah menggunakan versi *Bootstrap* terbaru, sehingga tidak ditemukan kerentanan serupa.

TABEL 8
(HASIL PENTEST A06)

Test	Parameter	Temuan	Keterangan
OWASP ZAP & Wappalyzer	https://Situs XYZ/	1. Versi Bootstrap yang usang	1. Bootstrap v4.3.1 memiliki banyak kerentanan XSS
Wappalyzer	https://XYZ Jurnalis https://XYZ Editor	1. Versi Bootstrap sudah diperbarui	1. Tidak ada indikasi kerentanan

6. A07:2021 – *Identification and Authentication Failures*

Pengujian manual pada https://XYZ Editor dengan login "admin" tidak berhasil dan tidak ditemukan indikasi kerentanan. Uji lanjutan menggunakan Burp Suite dengan 1000 kombinasi password umum juga gagal, meskipun seluruh permintaan mendapat respons dari server tanpa adanya mekanisme rate limiting. Variasi panjang respons (1606–1925 byte) disebabkan oleh header *Network Error Logging (NEL)* dan *Report-To* dari Cloudflare.

TABEL 9
(HASIL PENTEST A07)

Test	Parameter	Temuan	Keterangan
Manual	https://XYZ Editor	1. Uji coba username dan password admin gagal	1. Tidak ada indikasi adanya kerentanan
Burp Suite	https://XYZ Editor	1. *Bruteforcing* dengan payload 1000 password paling umum	1. Semua percobaan mendapat respon gagal, panjang respon bervariasi akibat adanya *Network Error Logging* dan *report to Cloudflare* yang berfungsi untuk memonitor jaringan. Namun semua percobaan *bruteforce* gagal.

7. A08:2021 – *Software and Data Integrity Failures*

Pengujian menggunakan OWASP ZAP dan curl menunjukkan bahwa Situs XYZ memuat JavaScript eksternal tanpa perlindungan SRI dan CSP, serta memiliki konfigurasi *access-control-allow-origin* wildcard (*) dan *x-xss-protection* yang dinonaktifkan. Kondisi ini meningkatkan risiko serangan Cross-Origin dan XSS. Disarankan untuk mengaktifkan CSP, menerapkan SRI, dan mengaktifkan perlindungan XSS untuk keamanan klien yang lebih baik.

TABEL 10
(HASIL PENTEST A08)

Test	Parameter	Temuan	Keterangan
OWASP ZAP	https://Situs XYZ/	1. file JavaScript dari domain eksternal	1. Perlindungan SRI dan CSP tidak ada untuk masuknya file js dari sumber luar
Curl	adsbygoogle.js	1.Konfigurasi *access-control-allow-origin* disetel ke *	Pengaturan access-control-allow-origin yang terbuka meningkatkan risiko serangan Cross-Origin. Menonaktifkan x-xss-protection meningkatkan potensi eksploitasi XSS

8. A09:2021 – *Security Logging and Monitoring*

Situs belum menerapkan *rate limiting*, sehingga rentan terhadap serangan brute force. Penyerang dapat mencoba kombinasi login tanpa batasan. Meski uji coba brute force tidak berhasil membobol akun, penerapan pembatasan tetap disarankan sebagai langkah mitigasi.

TABEL 11
(HASIL PENTEST A09)

Test	Parameter	Temuan	Keterangan
Burpsuite	https://XYZ Jurnalis https://XYZ Editor	1. 1000 payload menerima respon dari server	Ketiadaan rate limiting membuat sistem menjadi rentan terhadap serangan brute force dengan skala lebih besar

V. KESIMPULAN

Berdasarkan hasil uji keamanan terhadap Situs XYZ, XYZ Jurnalis, dan XYZ Editor, ditemukan total 20 kerentanan yang terbagi ke dalam tiga tingkat risiko. Sebanyak 4 temuan tergolong berisiko tinggi, yaitu *SQL Injection Potential*, *Missing Security Headers*, penggunaan *Bootstrap v4.3.1* yang rentan terhadap XSS, serta *bruteforce* login tanpa perlindungan pada sistem jurnalis dan editor. Risiko sedang mencakup 10 temuan, antara lain *HSTS not set*, *Deceprated TLS Protocol*, *Weak Cipher*, *CSP not set*, *CSP-frame-ancestors not set*, header *X-Content-Type-Options* yang tidak disetel ke *nosniff*, dua kasus *clickjacking*,

pengaturan *Access-Control-Allow-Origin* dan *X-XSS-Protection* yang tidak aman, serta tidak adanya *rate limiting* pada login. Sementara itu, terdapat 6 temuan berisiko rendah, seperti *mixed content* pada gambar, atribut HTML yang dapat dikendalikan pengguna, ketiadaan *Subresource Integrity (SRI)*, serta pemuatan file JavaScript lintas domain tanpa perlindungan.

REFERENSI

[1] I. F. Ashari, "Implementation of cyber-physical-social system based on service-oriented architecture in smart tourism," *J. Appl. Inform. Comput.*, vol. 4, no. 1, pp. 66–73, 2020.

[2] M. Awad, M. Ali, M. Takruri, and S. Ismail, "Security vulnerabilities related to web-based data," *TELKOMNIKA (Telecommun. Comput. Electron. Control)*, vol. 17, no. 2, pp. 852–856, 2019.

[3] Y. Devianto and S. Dwiasnati, "Rancang Bangun Web Portal Berita Sebagai Sumber Informasi Berita Tentang Pertanian," *JATISI (J. Tek. Inform. Sist. Informasi)*, vol. 8, no. 2, pp. 534–546, 2021.

[4] C. A. Makridis, "Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018," *J. Cybersecurity*, vol. 7, no. 1, Article tyab021, 2021.

[5] P. N. Petratos, "Misinformation, disinformation, and fake news: Cyber risks to business," *Bus. Horizons*, vol. 64, no. 6, pp. 763–774, 2021.

[6] R. Fletcher and S. Park, "The impact of trust in the news media on online news consumption and participation," *Digit. Journal.*, vol. 5, no. 10, pp. 1281–1299, 2017.

[7] International Federation of Journalists, "Indonesia: Cyber-attack targets independent media outlet," *ifj.org*, 2020. [Online]. Available: https://www.ifj.org/media-centre/news/detail/article/indonesia-cyber-attack-targets-independent-media-outlet. [Accessed: May 5, 2025].

[8] Cyberthreat.id, "Media online Project Multatuli kembali diteror serangan DDoS," *cyberthreat.id*, 2022. [Online]. Available: https://cyberthreat.id/read/15463/Media-Online-Project-Multatuli-Kembali-Diteror-Serangan-DDoS. [Accessed: May 5, 2025].

[9] Tempo.co, "Tempo kembali alami serangan siber DDoS, banyak berita tak bisa diakses publik," *tempo.co*, 2025. [Online]. Available: https://www.tempo.co/digital/tempo-kembali-alami-serangan-siber-ddos-banyak-berita-tak-bisa-diakses-publik-1228930. [Accessed: May 5, 2025].

[10] R. K. Rainer and B. Prince, *Introduction to Information Systems*. Hoboken, NJ: John Wiley & Sons, 2021.

[11] K. Arbanas and N. Ž. Hrustek, "Key success factors of information systems security," *J. Inf. Organ. Sci.*, vol. 43, no. 2, pp. 131–144, 2019.

[12] Cloudflare, "What is Penetration Testing." [Online]. Available: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/. [Accessed: May 1, 2025].

[13] Z. A. Hamza and M. Hammad, "Testing approaches for web and mobile applications: An overview," *Int. J. Comput. Digit. Syst.*, vol. 9, no. 4, pp. 657–665, 2020.

[14] Open Web Application Security Project, "About OWASP." [Online]. Available: https://owasp.org/about/. [Accessed: Nov. 23, 2023].