FORMAT: Jurnal Ilmiah Teknik Informatika
Vol. 15, No. 2, Juli 2026, pp. 130-141
Akreditasi Sinta 5 No. 156/C/C3/KPT/2026

DOI: format.2026.v15.i2.004
E-ISSN 2722-7162
P-ISSN 2089-5615

Analisis dan Evaluasi Risiko Kerentanan Aplikasi Web Berbasis OWASP *WSTG* dan *CVSS*

Eka Safari[1], Desi Ramayanti[2*]

[1,2]Fakultas Teknik dan Informatika, Universitas Dian Nusantara, Jakarta Barat

Email: [1]411221156@mahasiswa.undira.ac.id, [2]desi.ramayanti@undira.ac.id

*Penulis Korespondensi

ABSTRAK

Meningkatnya ancaman terhadap aplikasi berbasis web mendorong perlunya evaluasi yang terstruktur terhadap keamanan aplikasi web perusahaan. Penelitian ini bertujuan untuk mengidentifikasi kerentanan, menilai tingkat risiko, serta menyusun rekomendasi perbaikan pada aplikasi web *PT.XYZ*, sebuah perusahaan yang bergerak di bidang jasa maritim dan logistik yang menggunakan website sebagai profil perusahaan dan kanal informasi publik, menggunakan metodologi *Open Web Application Security Project Web Security Testing Guide (OWASP WSTG)* versi 4.2. Penelitian dilaksanakan menggunakan pendekatan *Black Box Testing* untuk menguji tiga kategori, yaitu *Information Gathering*, *Configuration and Deployment Management Testing*, dan *Error Handling Testing*, mengingat objek penelitian merupakan *static company profile website* tanpa form *input* maupun mekanisme otentikasi. Pengujian dilakukan menggunakan kombinasi *tools* seperti *Whatweb, DNS recon, Fierce, Nmap, Nikto, WAFW00F,* dan *curl,* dengan setiap temuan divalidasi secara manual untuk mengeliminasi *false positive*, sebelum dinilai tingkat risiko menggunakan *Common Vulnerability Scoring System (CVSS) versi 3.1*. Hasil pengujian dan validasi menunjukkan 12 kerentanan yang tervalidasi. Empat di antaranya berkategori *High* dengan skor 7,0–8,6, enam berkategori *Medium* dengan skor 4,0–5,9, dan dua berkategori *Low* dengan skor 2,6–3,1. Tidak ditemukan kerentanan berkategori *Critical*. Temuan dengan tingkat risiko tertinggi meliputi kondisi *Dangling DNS* pada subdomain yang mengarah ke infrastruktur pihak ketiga, penggunaan versi *PHP* yang telah mencapai status *End-of-Life* pada *subdomain*, serta eksposur layanan basis data yang dapat diakses dari jaringan publik. Sebanyak enam temuan berkorelasi dengan kategori *A05:2021-Security Misconfiguration* dan empat temuan dengan kategori *A06:2021-Vulnerable and Outdated Components* pada *OWASP Top 10:2021*, yang mengindikasikan bahwa kesalahan konfigurasi dan pemeliharaan komponen perangkat lunak merupakan sumber risiko dominan, dibandingkan dengan kerentanan pada logika aplikasi. Penelitian ini merekomendasikan pemutakhiran komponen perangkat lunak yang telah usang, pengetatan kontrol akses jaringan pada layanan basis data dan antarmuka administratif, serta pengelolaan siklus infrastruktur *DNS* secara berkala sebagai langkah mitigasi guna meningkatkan struktur keamanan aplikasi web secara berkelanjutan.

Article Info

Kata Kunci:
Black box testing
CVSS v3.1
Keamanan website
OWASP Top 10 2021
WSTG v4.2

Riwayat artikel:
Submit 14 Juli 2026
Revisi 18 Juli 2026
Diterima 22 Juli 2026

1. PENDAHULUAN

Perkembangan teknologi yang pesat telah mendorong berbagai sektor industri untuk mengadopsi sistem berbasis digital, termasuk pengelolaan operasional bisnis melalui aplikasi web. *Website* tidak hanya digunakan untuk branding bisnis, layanan konsumen, dan promosi, tetapi juga sebagai profil perusahaan dari suatu organisasi atau badan usaha agar memperoleh kepercayaan dari masyarakat luas [1]. Namun, dibalik manfaat yang ditawarkan, penggunaan *website* juga membuka peluang terhadap berbagai ancaman keamanan siber yang dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab.

E-ISSN 2722-7162
P-ISSN 2089-5615

Ancaman terhadap keamanan *website* terus mengalami peningkatan baik dari segi jumlah maupun kompleksitasnya. Kerentanan tersebut dapat berupa *Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection*, dan jenis serangan siber lainnya [2]. Badan Siber dan Sandi Negara (*BSSN*) melalui laporan Lanskap Keamanan Siber Indonesia 2024 mencatat sebanyak 5.780 kasus *web defacement* sepanjang tahun 2024, serta hasil pengujian *IT Security Assessment (ITSA)* terhadap 462 aplikasi yang mengungkap 1.931 kerentanan, terdiri dari 256 kerentanan kategori *Critical*, 405 *High*, 350 *Medium*, 621 *Low*, dan 299 bersifat informatif [3]. Sejalan dengan hal tersebut, laporan bulanan publik *Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center (ID-SIRTII/CC)* mencatat sebanyak 198 indikasi insiden siber sepanjang Agustus 2025, dengan jenis serangan yang paling sering terdeteksi meliputi *website* defacement, data breach, malicious software, serta *malicious activity* [4]. Lebih lanjut, laporan Kementerian Komunikasi dan Digital (*Komdigi*) menyatakan, kerugian akibat kejahatan siber pada periode November 2024 hingga Januari 2025 mencapai Rp476 miliar, yang menegaskan bahwa ancaman keamanan siber memiliki dampak ekonomi yang signifikan bagi organisasi, termasuk risiko gangguan operasional dan kebocoran data pada perusahaan penyedia layanan digital seperti PT.XYZ [5].

Untuk mengidentifikasi kerentanan secara sistematis, dibutuhkan suatu kerangka kerja pengujian yang terstandardisasi. *Open Web Application Security Project (OWASP*) menyediakan *Web Security Testing Guide (WSTG) v4.2*[6]. *WSTG* merupakan standar pengujian keamanan aplikasi web yang menyediakan prosedur sistematis untuk mengidentifikasi kelemahan keamanan. Melalui pendekatan analisis aktif, metode ini memungkinkan pengujian untuk mendeteksi berbagai kerentanan, baik akibat kesalahan teknis maupun celah keamanan yang berpotensi dieksploitasi oleh pihak yang tidak bertanggung jawab, serta dapat memberikan solusi mitigasi atau perbaikan yang tepat kepada pemilik sistem[7].

Beberapa penelitian terdahulu telah menerapkan kombinasi *WSTG* dan *CVSS* pada berbagai objek penelitian. Rafeli, dkk.[8], Melakukan pentesting terhadap *website XYZ* menggunakan *WSTG* untuk mengidentifikasi kerentanan pada data sensitif penggunanya, dan ditemukan 8 kerentanan pada kategori *Medium*. Yusuf dkk.[9] Melakukan pengujian keamanan pada *website XYZ* menggunakan metode *Information Systems Security Assessment Framework (ISSAF)* yang dipadukan dengan *OWASP WSTG v4.2* sebagai panduan validasi kerentanan, kemudian dinilai tingkat keparahannya menggunakan *OWASP Risk Rating*. Selanjutnya Priambodo dkk.[10], Melakukan *Penetration Testing* pada *website XYZ* menggunakan acuan *WSTG v4.2* untuk validasi kerentanan dan menghasilkan 9 kerentanan yang terdiri dari 2 kategori tinggi *High*, 1 kerentanan berkategori *Medium*, dan 6 kerentanan berkategori *Low*. Lalu, Setiawan dan Fachri[11] melakukan identifikasi kerentanan pada *website* sistem informasi akademik Universitas Ma'arif Nahdlatul Ulama Kebumen, menggunakan *framework WSTG*. Dalam penelitian tersebut, ditemukan 3 jenis kerentanan utama seperti *Content Security Policy (CSP) Header Not Set, HTTP to HTTPS Insecure Transition in Form Post*, dan *Missing Anti-clickjacking Header*. Selain itu, Widyaningrum dalam penelitiannya pada Sistem Informasi Manajemen Rumah Sakit (*SIMRS*) menggunakan *OWASP WSTG v4.2* yang dikombinasikan dengan *CVSS v3.1* untuk mengukur tingkat keparahan setiap kerentanan, sehingga prioritas mitigasi dapat ditentukan secara lebih objektif berdasarkan skor risiko [12]. Pendekatan berbasis standar keamanan aplikasi web untuk mendeteksi kerentanan pada website telah diterapkan pada berbagai penelitian sebelumnya [20]. Selain itu, metode pengujian penetrasi untuk memvalidasi kerentanan pada infrastruktur jaringan serta mengevaluasi keamanan sistem informasi juga telah banyak digunakan dalam penelitian terkait [21], [22].

Berdasarkan kajian terhadap penelitian-penelitian terdahulu tersebut, terdapat celah penelitian (*Gap Analysis*) yang menjadi dasar dilakukannya penelitian ini. Yang pertama, belum terdapat penelitian yang secara spesifik menerapkan kerangka kerja *OWASP WSTG v4.2* dengan penilaian risiko *CVSS v3.1* secara terintegrasi dan konsisten pada setiap temuan. Kedua, sebagian besar penelitian terdahulu mengasumsikan objek penelitian memiliki form input atau mekanisme otentikasi yang dapat diuji menggunakan kategori *Input Validation Testing*, sementara belum banyak penelitian yang membahas strategi pengujian pada aplikasi web yang tidak memiliki titik masukan data, sehingga memerlukan penyesuaian kategori pengujian yang relevan. Keterbatasan objek penelitian berupa static company profile website ini justru dijawab dengan mengoptimalkan kategori Information Gathering dan Configuration and Deployment Management Testing sebagai fokus utama pengujian, alih-alih Input Validation Testing yang umum digunakan pada penelitian sebelumnya. Ketiga, integrasi antara hasil pengujian *WSTG* dengan penilaian kuantitatif menggunakan *CVSS v3.1*, termasuk proses validasi manual untuk mengeliminasi *false positive* sebelum penilaian risiko dilakukan, secara konsisten masih jarang ditemukan pada penelitian dengan objek serupa.

Penelitian ini mengisi celah tersebut dengan menerapkan tiga kategori *WSTG v4.2* yang disesuaikan dengan karakteristik objek penelitian, yaitu *Information Gathering, Configuration and Deployment Testing,* dan *Error Handling Testing*, serta dilengkapi dengan penilaian risiko menggunakan *CVSS v3.1* pada setiap temuan yang divalidasi. Secara khusus, penelitian ini memberikan kontribusi dengan mengidentifikasi, mendokumentasikan, dan menilai tingkat risiko setiap kerentanan keamanan pada aplikasi web *xyz.com* secara terintegrasi dan konsisten. Selain itu, penelitian ini menyusun rekomendasi perbaikan yang spesifik untuk ditindaklanjuti berdasarkan prioritas

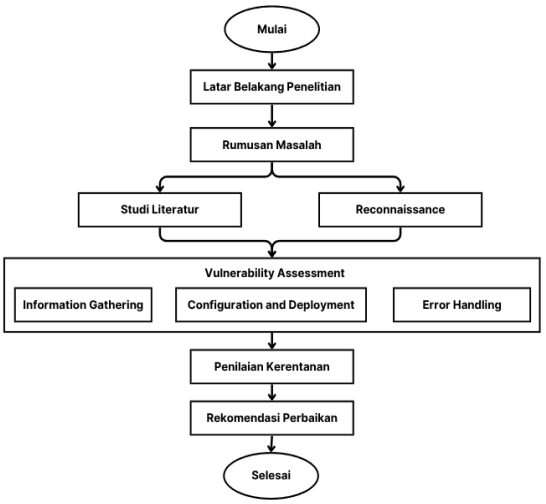
E-ISSN 2722-7162
P-ISSN 2089-5615

risiko yang telah dianalisis. Dengan demikian, hasil penelitian diharapkan dapat memberikan kontribusi praktis dalam peningkatan keamanan aplikasi *website xyz.com* bagi perusahaan, serta kontribusi akademis melalui penyediaan analisis empiris terkait kondisi keamanan aplikasi web pada sektor industri maritim yang masih terbatas pembahasannya dalam literatur keamanan siber di Indonesia.

2. METODE PENELITIAN

2.1. Tahapan Penelitian

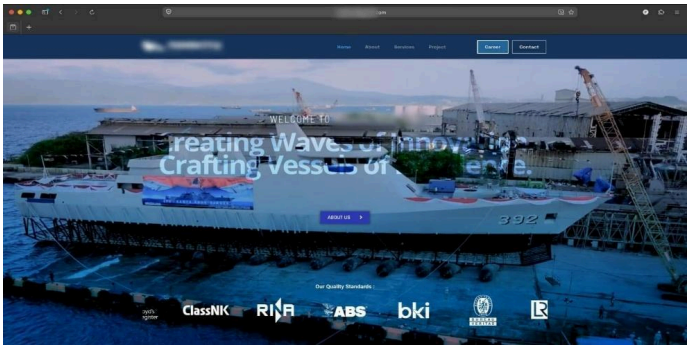
Penelitian ini menggunakan pendekatan *Black Box Testing* untuk menguji fungsionalitas sistem, tanpa mempertimbangkan struktur kode ataupun arsitektur internal[13], yang dilaksanakan melalui serangkaian pengujian teknis langsung terhadap aplikasi web yang menjadi objek penelitian, dan dikombinasikan dengan beberapa tahapan seperti pada Gambar 1.



Gambar 1. Tahapan Penelitian yang Terdiri atas Lima Tahap: Perencanaan, Pengumpulan Data, Pengujian, Validasi, dan Pelaporan

Sebagaimana ditunjukkan pada Gambar 1, penelitian ini dilaksanakan melalui lima tahapan. Tahap pertama adalah perencanaan, yaitu penetapan objek, ruang lingkup, serta kategori WSTG yang akan diujikan. Tahap kedua adalah pengumpulan data, mencakup studi dokumentasi terhadap standar WSTG v4.2 dan CVSS v3.1 serta reconnaissance awal terhadap objek penelitian. Tahap ketiga adalah pengujian teknis menggunakan kombinasi tools sebagaimana dijelaskan pada Tabel 1. Tahap keempat adalah validasi manual terhadap seluruh temuan untuk mengeliminasi false positive sekaligus menilai tingkat risiko menggunakan CVSS v3.1. Tahap kelima adalah pelaporan, yaitu penyusunan rekapitulasi temuan, klasifikasi OWASP Top 10, serta rekomendasi mitigasi yang dapat ditindaklanjuti oleh pemilik sistem.

2.2. Objek dan Ruang Lingkup Penelitian



Gambar 2. Objek Penelitian

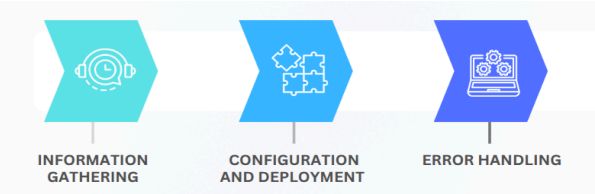
Objek pada penelitian ini adalah *website* milik *PT.XYZ* yang dapat diakses melalui jaringan internet dan digunakan sebagai media penyedia informasi serta layanan digital bagi pengguna. *Website xyz.com* dipilih sebagai

E-ISSN 2722-7162
P-ISSN 2089-5615

objek penelitian karena *website* tersebut berperan sebagai salah satu media utama interaksi antara organisasi dengan penggunanya.

Ruang lingkup pengujian dibatasi hanya pada area aplikasi web yang dapat diakses secara publik tanpa autentikasi. Tidak mencakup infrastruktur jaringan internal maupun basis data secara langsung dan tidak melibatkan eksploitasi penuh terhadap kerentanan yang ditemukan.

2.3. Kerangka Kerja Penelitian



Gambar 3. Kerangka Kerja Penelitian

Berdasarkan Gambar 3, penelitian ini menggunakan *WSTG v4.2* sebagai kerangka kerja utama yang memberikan panduan teknis untuk setiap jenis kerentanan[14], yang terdiri dari beberapa tahap pengujian yang dipilih sesuai dengan kondisi objek penelitian, seperti *Information Gathering* yang berfungsi untuk mengumpulkan informasi awal dan memetakan *attack surface* dan teknologi yang digunakan, *Configuration Testing* untuk mengidentifikasi kesalahan konfigurasi *server* dan *header*, lalu *Error Handling Testing* sebagai bahan evaluasi eksposur informasi.

2.4. Alat dan Teknik Pengumpulan Data

Pada Pengumpulan data dilaksanakan menggunakan kombinasi studi dokumentasi terhadap standar *WSTG v4.2* dan *CVSS v3.1, Reconnaissance*, pengujian teknis, serta dokumentasi bukti berupa tangkapan layar dan log aktivitas. Beberapa alat yang digunakan dalam penelitian ini ditunjukkan pada Tabel 1.

Tabel 1. Alat Pengujian

Alat	**Fungsi**
Nmap	pemindaian *Port* dan layanan
Wappalyzer	Identifikasi teknologi stack(*CMS, Server, OS*)
WAF W00F	Deteksi *Web Application Firewall*
DNS recon	Enumerasi *DNS*
Curl	Pengujian respon header dan metode *HTTP* manual

Pemilihan setiap alat didasarkan pada relevansinya dengan kategori pengujian yang dilakukan, fitur spesifik yang mendukung kebutuhan pengujian pada aplikasi web, serta statusnya sebagai perangkat *open source* yang telah divalidasi dan diadopsi secara luas dalam komunitas keamanan siber.

2.5. Teknik Analisis Data dan Penilaian Risiko

Pada setiap temuan yang diperoleh, divalidasi terlebih dahulu untuk menghilangkan *false positive* dan menghasilkan penilaian yang objektif, selanjutnya diklasifikasikan berdasarkan referensi *OWASP Top 10 2021*. Tingkat risiko setiap temuan dinilai menggunakan *Base Metrics CVSS* v3.1, yang dihitung berdasarkan delapan vektor[15]. *Base Metrics* merupakan bagian dari sistem *CVSS* yang dapat dipresentasikan ke dalam bentuk string vektor[16], seperti *Attack Vector* (Jarak serangan (jaringan, lokal, atau fisik), *Attack Complexity* (Tingkat kesulitan yang diperlukan), *Privileges Required* (Tingkat hak akses yang diperlukan), *User Interaction* (Apakah serangan memerlukan interaksi pengguna), dan *Scope* (Apakah kerentanan mempengaruhi komponen lain).
Setiap parameter digunakan untuk mengukur tingkat risiko kerentanan. Penilaian dilakukan dengan menentukan nilai dari masing-masing parameter sesuai kondisi aktual kerentanan, yang berfungsi sebagai matrik prioritas risiko yang paling relevan untuk pengambilan *keputusan*[17]. Hasilnya kemudian dihitung menjadi skor *CVSS* yang merepresentasikan tingkat risiko, seperti yang ditunjukkan pada Tabel 2.

E-ISSN 2722-7162
P-ISSN 2089-5615

Tabel 2. Klasifikasi Tingkat Kerentanan Berdasarkan CVSS v3.1

Tingkat Kerentanan	Skor
Critical	9.0-10
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9
Informational	0.0

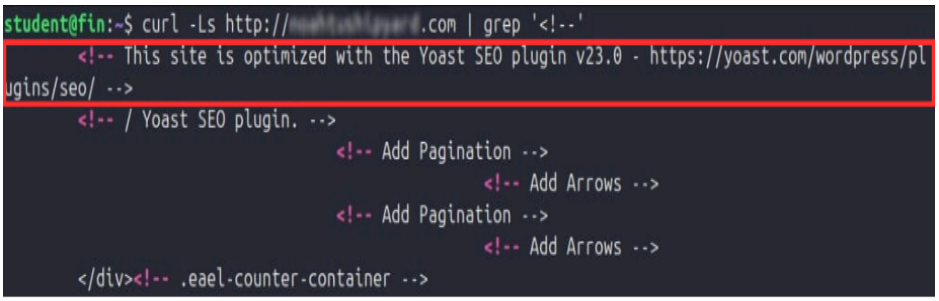
3. HASIL DAN DISKUSI

3.1. Hasil Pengujian Information Gathering (*WSTG-INFO*)

Tabel 3. Hasil Pengujian Information Gathering

Aspek	Temuan	Status
Conduct Search Engine Discovery/Reconnaissance for Information Leakage	File *robots.txt* (berisi entri sitemap, parameter *discount.php ?sitemap.xml*) bisa diakses	Ditemukan
Fingerprint server	*Zone transfer* ditolak, tidak ditemukan *wildcard DNS* pada domain	Tidak Ditemukan
Fingerprint Web Server	Domain dikelola *Niagahoster* berbasis *cPanel*, *DMARC* dengan *policyp=none*, beberapa *Port* terbuka, *Port MySQL* terbuka, subdomain *cPanel*, *cpcalendars* , dan *sea* (*IP* berbeda) ditemukan	Ditemukan
Fingerprint Web Application Framework	Teridentifikasi *WordPress* dengan *plugin Yoast SEO v23.0* dan Elementor + *Essential Addons for Elementor*	Ditemukan
Fingerprint Web Application	*Header x-powered-by* mengungkap penggunaan *PHP /7.4.33*, *Endpoint WP-JSON REST API* teridentifikasi	Ditemukan
Fingerprint Web Application	*Header X-Content-Type-OPTIONS*: *nosniff*, X-*XSS-Protection*, serta *cookie* sesi dengan atribut *HTTP Only* dan *secure* telah diterapkan	Terkonfirmasi
Map Application Architecture	Situs terlindungi oleh *Web Application Firewall (WAF) LiteSpeed Technologies*	Terkonfirmasi

Hasil dari beberapa pengujian tersebut di atas, terdapat dua kategori yang paling signifikan, yaitu terdeteksinya versi *PHP* 7.4.33 yang telah mencapai status *End of Life* sejak November 2022 dan tidak lagi menerima pembaruan keamanan resmi, dan juga eksposur versi *plugin Yoast SEO* pada komentar HTML yang bisa memudahkan pihak yang tidak bertanggung jawab untuk melakukan eksploitasi, seperti yang ditunjukkan pada Gambar 4.



Gambar 4. Pengujian terhadap konten HTML

3.2. Hasil Pengujian Configuration and Deployment Testing (*WSTG-CONF*)

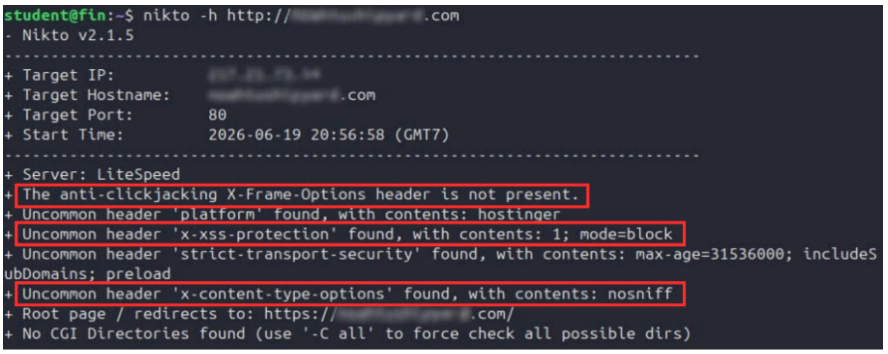
Tabel 4. Hasil Pengujian Configuration and Deployment Testing

Aspek	Temuan	Status
Network/Infrastructure Configuration	Versi *MariaDB* teridentifikasi, dengan beberapa *CVE* pada basis data, *Port* alternatif 8080/8443 terbuka (diduga Portal *hosting*)	Perlu Validasi Lanjutan

E-ISSN 2722-7162
P-ISSN 2089-5615

Aspek	Temuan	Status
	Path mencurigakan *(/jmx-console/, /wiki/, /j2ee/examples/*, dll.), tapi server merespons 404 untuk path tidak dikenal	False Positive
Application Platform Configuration	*Header X-Frame-OPTIONS* tidak ditemukan, *Endpoint/wp-admin/* bisa diakses publik tanpa pembatasan	Terkonfirmasi
	Header nosniff dan *x-xss-protection* terkonfirmasi diterapkan, termasuk respon halaman *error*	Terkonfirmasi
Metode HTTP	Pengujian metode *OPTIONS* dan *PUT* belum konklusif	Perlu Validasi Lanjutan
HTTP Strict Transport Security	*HSTS* diterapkan dengan max-age 1 tahun, *include SubDomains*, dan *preload*	Terkonfirmasi
Subdomain takeover	1 subdomain *IP* berbeda	Perlu Validasi Lanjutan

Berdasarkan Tabel 4 di atas, ditemukan bahwa sebagian besar mekanisme pertahanan dasar (*HSTS*, *redirect HTTPS*) telah diterapkan dengan baik, namun masih terdapat celah konfigurasi yang signifikan pada eksposur antarmuka administratif dan ketidaklengkapan header keamanan. Terdapat temuan subdomain *takeover* atau *dangling DNS* yang mengarahkan subdomain ke *IP* domain yang berbeda. Juga terdapat dua header keamanan lainnya yang tidak diterapkan, yaitu *X-Frame-OPTIONS* yang berpotensi rentan terhadap *clickjacking*[10], dan *CSP* yang berarti aplikasi tidak memiliki lapisan mitigasi terhadap potensi serangan *XSS*[18], seperti yang ditunjukkan pada Gambar 5.



Gambar 5. Pengujian terhadap konten HTML

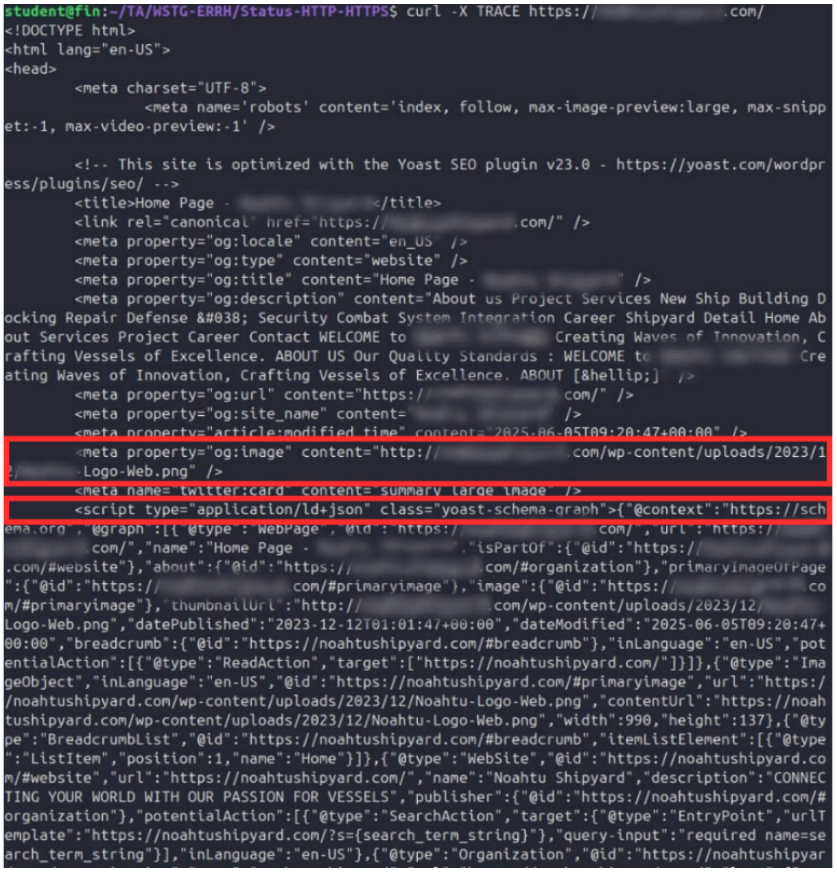
3.3. Hasil Pengujian *Error* Handling Testing (*WSTG-ERRH*)

Tabel 5. Hasil Pengujian Error Handling Testing

Aspek	Temuan	Status
Testing for Improper Error Handling	Server merespon 404 standar untuk halaman/parameter tidak valid tanpa membocorkan informasi *debug*, *payload* <*script*> pada parameter pencarian memicu respon 403 (*filtering* aktif)	Tidak Ditemukan
	Permintaan dengan metode *TRACE*, *PUT*, dan DELETE menghasilkan respon *body HTML*, namun *HTTP-methods* mengkonfirmasi metode yang didukung server hanya GET, HEAD, POST, dan *OPTIONS*	Tidak Ditemukan
	Path sensitif seperti /.git/ dan /admin/config/ tidak diproses *backend LiteSpeed*, melainkan dikembalikan dengan kode 415 *Unsupported Media Type* oleh layer terpisah yang teridentifikasi sebagai *openresty*	Ditemukan
	Tidak ditemukan eksposur informasi sensitif pada respon, pola penyaringan 415 oleh *openresty* konsisten dengan pengujian sebelumnya.	Tidak Ditemukan
	Semua *payload* yang memicu *error* aplikasi direspon 415 oleh *openresty* tanpa menampilkan stack *TRACE*, *query SQL*, maupun jalur direktori internal	Tidak Ditemukan

E-ISSN 2722-7162
P-ISSN 2089-5615

Pengujian menggunakan metode *HTTP* yang dianggap berisiko menunjukkan hasil yang signifikan. Salah satunya menggunakan metode *TRACE* terhadap *root* domain yang berhasil dieksekusi dengan respon 200 OK serta menampilkan seluruh halaman utama lengkap dengan metadata, judul, deskripsi, struktur data *JSON-LD*, juga tautan logo perusahaan, seperti pada Gambar 6.



Gambar 6. Pengujian Response Header HTTP

3.4. Validasi dan Rekapitulasi Temuan

Untuk memastikan akurasi dan menghindari kesimpulan berlebihan (overclaim) maupun bias akibat false positive, seluruh temuan pada *WSTG-INFO*, *WSTG-CONF*, dan *WSTG-ERRH* yang berstatus ditemukan atau perlu validasi lanjutan akan diuji ulang. Hasil keseluruhan proses validasi terhadap status temuan kemudian dirangkum ke dalam Tabel 6.

Tabel 6. Rekapitulasi Temuan Kerentanan

Temuan Awal	Hasil Validasi	Status Akhir
Sitemap acak & parameter *discount.php* pada *robots.txt*	File *discount.php* merespons normal (200, tanpa konten berbahaya), parameter sitemap tidak mengembalikan output	Ditemukan (indikasi historis, tidak terbukti aktif)
Port MySQL (3306) terbuka ke publik	*mySQL-info* berhasil melakukan *handshake* penuh dan memperoleh versi, *capabilities*, serta *salt autentikasi*	Ditemukan (terkonfirmasi)
Endpoint WP-JSON REST API dapat diakses	Permintaan daftar user *(/WP-JSON/wp/v2/users/)* ditolak dengan 401 Unauthorized	Tidak Ditemukan
Port 8080/8443 terbuka, *service* tidak teridentifikasi	Pemindaian versi tidak berhasil memastikan *service*, indikasi *filtering/throttling*	Perlu Validasi Lanjutan
Header *X-Frame-OPTIONS* tidak ditemukan pada situs	Header *X-Frame-OPTIONS* dan *Content-Security-Policy* ditemukan pada halaman */wp-login.php* , namun tidak pada halaman utama	Ditemukan (penerapan tidak konsisten)
Subdomain *sea* mengarah ke *IP* berbeda	*Whois* mengonfirmasi *IP* berada pada penyedia jaringan berbeda (Moratelindo), subdomain menjalankan *PHP* 5.6.3 (*EOL*) pada server *openresty*	Ditemukan (terkonfirmasi)

E-ISSN 2722-7162
P-ISSN 2089-5615

Berdasarkan Tabel di atas, dari enam temuan yang divalidasi ulang, empat temuan mengalami perubahan status. Satu temuan dieliminasi sebagai false positive (Endpoint WP-JSON REST API, karena permintaan daftar user ditolak dengan 401 Unauthorized), satu temuan diperjelas cakupan penerapannya (header X-Frame-OPTIONS, yang hanya ditemukan pada halaman /wp-login.php namun tidak pada halaman utama), dan dua temuan dinaikkan tingkat kepastiannya menjadi terkonfirmasi (Port MySQL dan subdomain sea). Proses validasi ini menegaskan pentingnya pengujian manual lanjutan terhadap hasil pemindaian otomatis sebelum suatu temuan disimpulkan sebagai kerentanan yang valid, sejalan dengan prinsip eliminasi false positive yang diterapkan secara konsisten dalam penelitian ini.

Validasi manual pada setiap temuan dilakukan dengan metode yang disesuaikan dengan karakteristik temuan guna menjaga transparansi dan reproduksibilitas hasil penelitian. Validasi terhadap pola sitemap acak dan discount.php dilakukan dengan pengujian ulang menggunakan curl -v untuk memeriksa kode respons HTTP dan konten yang dikembalikan. Validasi terhadap Port MySQL dilakukan dengan mencoba melakukan handshake langsung menggunakan mysql-info guna memastikan versi dan salt autentikasi benar-benar terekspos. Validasi terhadap Endpoint WP-JSON REST API dilakukan dengan pengujian ulang permintaan daftar pengguna untuk memeriksa kode respons HTTP. Validasi terhadap Port 8080/8443 dilakukan dengan pemindaian versi layanan menggunakan Nmap dengan opsi banner grabbing, namun hasilnya belum konklusif karena indikasi filtering/throttling pada Port tersebut. Meskipun demikian, penilaian CVSS dasar tetap diberikan pada temuan ini karena Port tersebut tetap terbuka dan dapat diakses dari jaringan publik, sehingga tetap merepresentasikan permukaan serangan (attack surface) yang perlu dimitigasi walau tingkat keparahannya belum dapat dipastikan secara pasti. Validasi terhadap header X-Frame-OPTIONS dan subdomain sea dilakukan dengan pengujian ulang pada beberapa halaman berbeda serta verifikasi kepemilikan IP melalui pengecekan WHOIS.

3.5. Klasifikasi OWASP Top 10

Tabel 7. Klasifikasi Temuan Berdasarkan OWASP Top 10:2021

Nama Temuan	**OWASP Top 10**
Port MySQL (3306) terbuka dan terkonfirmasi dapat diakses publik	A05:2021
Kebijakan *DMARC* dengan parameter *p=none*	A05:2021
Header *X-Frame-OPTIONS* tidak konsisten diterapkan antar halaman	A05:2021
Antarmuka */wp-admin/* dapat diakses publik tanpa pembatasan percobaan login	A05:2021
PHP 7.4.33 pada domain utama (*End-of-Life*)	A06:2021
MariaDB v10.11 dengan ratusan CVE yang terdaftar	A06:2021
PHP 5.6.3 pada subdomain *sea.xyz.com* (*End-of-Life*)	A06:2021
Disclosure versi *plugin Yoast SEO* v23.0 dan Elementor	A06:2021
Subdomain *cPanel* dan *cpcalendars* dapat di enumerasi publik	A01:2021
Subdomain *sea.xyz.com* mengarah ke infrastruktur pihak ketiga (dangling *DNS*)	A05:2021
Pola sitemap acak dan *discount.php* pada *robots.txt* (indikasi historis)	A06:2021
Port 8080/8443 terbuka, *service* belum teridentifikasi pasti	A05:2021

Berdasarkan Tabel 7, sebagian besar temuan terkonsentrasi pada kategori *Security Misconfiguration* dan *Vulnerable and Outdated Components*. Hal ini menunjukkan bahwa celah keamanan utama pada target penelitian disebabkan oleh kelalaian dalam proses pemeliharaan berkala, keterlambatan dalam pembaruan perangkat lunak, serta ketidaktepatan dalam penerapan konfigurasi sistem dan komponen infrastruktur. Rendahnya perhatian terhadap pembaruan versi perangkat lunak dan kurangnya implementasi praktik keamanan standar, misalnya pada penetapan header keamanan atau pembatasan akses pada layanan tertentu, secara langsung meningkatkan risiko eksploitasi oleh pihak tidak berwenang. Dengan demikian, permasalahan keamanan lebih dominan terjadi akibat faktor operasional dan administratif, bukan karena kelemahan mendasar pada logika aplikasi atau arsitektur perangkat lunak yang digunakan. Analisis ini menegaskan pentingnya pengelolaan infrastruktur yang proaktif dan sistematis sebagai langkah utama dalam mitigasi risiko keamanan aplikasi web.

E-ISSN 2722-7162
P-ISSN 2089-5615

3.6. Penilaian Risiko (CVSS)

Tahap selanjutnya adalah menghitung tingkat keparahan setiap temuan menggunakan *CVSS* v3.1, sesuai dengan metodologi yang telah dijelaskan. Hasil keseluruhan penilaian *CVSS* disajikan pada Tabel 8.

Tabel 8. Penilaian CVSS v3.1 terhadap Temuan

Nama Temuan	Vector String CVSS	Base Score	Tingkat Keparahan
Port MySQL (3306) terbuka dan terkonfirmasi dapat diakses publik	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3	*Medium*
Kebijakan *DMARC* dengan parameter *p=none*	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N	4.7	*Medium*
Header *X-Frame-OPTIONS* tidak konsisten diterapkan antar halaman	AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N	3.1	*Low*
Antarmuka */wp-admin/* dapat diakses publik tanpa pembatasan percobaan login	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3	*Medium*
PHP 7.4.33 pada domain utama (*End-of-Life*)	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	5.9	*Medium*
MariaDB 10.11.16 dengan ratusan CVE terdaftar	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0	*High*
PHP 5.6.3 pada subdomain *sea.xyz.com* (*End-of-Life*)	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L	7.9	*High*
Disclosure versi *plugin Yoast SEO* v23.0 dan Elementor	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3	*Medium*
Subdomain *cPanel* dan *cpcalendars* dapat di enumerasi publik	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	8.6	*High*
Subdomain sea.xyz.com mengarah ke infrastruktur pihak ketiga (dangling DNS)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	7.5	*High*
Pola sitemap acak dan *discount.php* pada *robots.txt*	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	4.0	*Medium*
Port 8080/8443 terbuka, *service* belum teridentifikasi	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N	2.6	*Low*

Tabel 8 di atas juga mencantumkan penilaian CVSS untuk temuan dangling DNS pada subdomain sea.xyz.com, yang sebelumnya belum disertakan pada revisi terdahulu. Dengan vector string AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N dan skor 7,5, temuan ini masuk kategori High, sejalan dengan degree of impact yang tinggi karena subdomain tersebut mengarah ke infrastruktur pihak ketiga yang tidak lagi berada di bawah kendali PT.XYZ, sehingga berpotensi disalahgunakan untuk hosting konten berbahaya, phishing, atau subdomain takeover yang mengatasnamakan domain resmi perusahaan. Dengan demikian, total kerentanan berkategori High pada penelitian ini adalah empat, yaitu subdomain sea.xyz.com (dangling DNS), subdomain cPanel/cpcalendars, PHP 5.6.3 pada subdomain sea, dan basis data MariaDB.

Untuk memperjelas signifikansi praktis setiap temuan, berikut disajikan skenario serangan ringkas pada beberapa temuan prioritas tinggi. Pada temuan Port MySQL (3306) yang terbuka ke publik, penyerang dapat mencoba koneksi secara brute-force dari internet; apabila berhasil, data sensitif seperti informasi pelanggan atau kredensial administratif dapat terekspos, yang berpotensi mengganggu ketersediaan layanan apabila basis data menjadi sasaran serangan ransomware. Pada temuan dangling DNS, penyerang dapat mengklaim infrastruktur pihak ketiga yang sudah tidak terpakai tersebut, kemudian menghosting halaman phishing atau malware yang tampak berasal dari domain resmi PT.XYZ, sehingga merusak reputasi dan kepercayaan pengguna. Pada temuan PHP End-of-Life, baik pada domain utama maupun subdomain sea, penyerang dapat memanfaatkan kerentanan publik yang telah terdokumentasi pada versi tersebut untuk melakukan remote code execution apabila tidak segera dimutakhirkan.

Meskipun temuan berkategori Low seperti ketidakkonsistenan header X-Frame-OPTIONS dan Port 8080/8443 yang belum teridentifikasi layanannya memiliki skor risiko individual yang rendah, kedua temuan tersebut tidak dapat diabaikan begitu saja. Header X-Frame-OPTIONS yang tidak diterapkan secara konsisten, apabila dikombinasikan dengan kerentanan lain seperti disclosure versi plugin yang rentan terhadap XSS, dapat

E-ISSN 2722-7162
P-ISSN 2089-5615

meningkatkan risiko serangan clickjacking secara signifikan melalui skema chained attack. Demikian pula, Port 8080/8443 yang terbuka meskipun layanannya belum teridentifikasi pasti tetap memperluas permukaan serangan (attack surface) aplikasi, sehingga apabila di kemudian hari teridentifikasi sebagai layanan administratif atau portal hosting yang tidak terlindungi, dapat menjadi titik masuk tambahan bagi penyerang. Oleh karena itu, kedua temuan Low ini tetap direkomendasikan untuk dimitigasi sebagai bagian dari upaya pengurangan permukaan serangan secara menyeluruh.

3.7. Rekomendasi Mitigasi

Berdasarkan hasil pengujian, validasi, klasifikasi OWASP Top 10, dan penilaian CVSS yang telah dipaparkan pada subbab sebelumnya, disusun rekomendasi perbaikan yang diprioritaskan berdasarkan tingkat keparahan masing-masing temuan, seperti yang ditunjukkan pada Tabel 9.

Tabel 9. Rekomendasi Mitigasi Berdasarkan Prioritas

Nama Temuan	Rekomendasi perbaikan	Prioritas
Subdomain sea.xyz.com mengarah ke infrastruktur pihak ketiga	Menghapus DNS record yang tidak lagi digunakan atau memverifikasi kepemilikan dan keabsahan infrastruktur tujuan secara berkala, menerapkan pemantauan rutin terhadap seluruh subdomain yang terdaftar untuk mendeteksi dangling DNS sedini mungkin	Tinggi
PHP 5.6.3 pada subdomain sea	Memutakhirkan versi PHP ke versi yang masih mendapat dukungan resmi, atau menonaktifkan subdomain tersebut apabila sudah tidak diperlukan	Tinggi
MariaDB dengan riwayat CVEprivilegeescalation	Memastikan versi MariaDB yang terpasang telah menerima seluruh backportpatch terkini dari penyedia distribusi, membatasi akses port 3306 hanya untuk koneksi localhost atau jaringan internal melalui konfigurasi firewall	Tinggi
PHP 7.4.33 pada domain utama	Memutakhirkan versi PHP ke versi LTS yang masih mendapat dukungan keamanan resmi (minimal PHP 8.1 ke atas)	Sedang
Port MySQL dapat diakses dan melakukan handshake dari publik	Mengkonfigurasi bind-address MySQL/MariaDB agar hanya menerima koneksi dari localhost, serta menerapkan pembatasan akses berbasis IP pada tingkat firewall	Sedang
Antarmuka /wp-admin/ dapat diakses tanpa pembatasan	Menerapkan pembatasan percobaan login (rate limiting), otentikasi dua faktor (2FA), serta pembatasan akses berbasis IP atau VPN untuk antarmuka administratif	Sedang
Disclosure versionplugin WordPress	Nonaktifkan tampilan versi plugin pada komentar HTML serta memutakhirkan seluruh plugin secara berkala	Sedang
Subdomain cpanel/cpcalendars dapat dienumerasi	Batasi akses ke subdomain manajemen hosting hanya untuk IP tertentu melalui konfigurasi firewall atau autentikasi tambahan pada tingkat web server	Sedang
Kebijakan DMARC p=none	Mengubah kebijakan DMARC secara bertahap menjadi p=quarantine, kemudian p=reject, setelah memastikan seluruh sumber pengiriman email yang sah telah terdaftar pada SPF dan DKIM	Sedang

Rekomendasi perbaikan pada penelitian ini dapat dikelompokkan ke dalam tiga area utama, yaitu pemutakhiran komponen perangkat lunak yang telah mencapai status End of Life, baik pada domain utama (PHP 7.4.33) maupun pada infrastruktur subdomain pihak ketiga (PHP 5.6.3), mengingat kedua versi tersebut tidak lagi menerima pembaruan keamanan resmi. Selanjutnya, pengetatan kontrol akses jaringan, khususnya pembatasan akses publik terhadap layanan basis data dan antarmuka manajemen hosting yang seharusnya hanya dapat diakses melalui jaringan internal atau dengan mekanisme autentikasi tambahan. Yang terakhir, pengelolaan siklus hidup infrastruktur DNS secara berkala, terutama untuk memastikan tidak ada subdomain yang mengarah ke layanan yang sudah tidak aktif atau berada di luar kendali pemilik domain, sebagaimana ditemukan pada kasus subdomain sea.xyz.com.
Penerapan rekomendasi tersebut secara konsisten diperkirakan dapat menurunkan tingkat keparahan keseluruhan temuan pada penelitian ini, khususnya pada keempat temuan berkategori High yang menjadi prioritas utama perbaikan.

E-ISSN 2722-7162
P-ISSN 2089-5615

4. KESIMPULAN

Penelitian ini telah berhasil mengidentifikasi dan memvalidasi kerentanan keamanan pada *website* xyz.com menggunakan metodologi *WSTG v4.2* dan penilaian risiko *CVSS* v3.1. Hasil pengujian menunjukkan bahwa *website* xyz.com tidak memiliki kerentanan kategori *Critical*, didukung oleh penerapan *HSTS*, *redirect HTTPS*, serta *WAF* berlapis (*LiteSpeed* dan *Openresty*) yang efektif mencegah eksposur informasi melalui pesan *error*.

Meskipun demikian, ditemukan empat kerentanan kategori High, yaitu kondisi dangling DNS pada subdomain sea.xyz.com yang mengarah ke infrastruktur pihak ketiga, enumerasi publik subdomain cPanel dan cpcalendars, penggunaan PHP 5.6.3 End-of-Life pada subdomain sea.xyz.com, serta eksposur basis data MariaDB yang dapat diakses publik. Proses validasi manual tidak hanya terbukti penting dalam memastikan akurasi hasil pengujian, tetapi juga berimplikasi signifikan terhadap kualitas data kerentanan yang dihasilkan. Melalui tahapan ini, satu temuan (Endpoint WP-JSON REST API) dieliminasi sebagai false positive, dua temuan (Port MySQL dan subdomain sea) dinaikkan statusnya menjadi terkonfirmasi, dan puluhan path mencurigakan lainnya turut dieliminasi sebagai false positive. Implikasi dari langkah validasi manual ini adalah meningkatnya keandalan hasil analisis serta meminimalkan risiko pengambilan keputusan yang didasarkan pada data yang tidak akurat atau berlebihan, sehingga prioritas mitigasi dapat ditetapkan secara lebih tepat sasaran.

Klasifikasi *OWASP Top 10* menunjukkan dominasi kategori *A05:2021-Security Misconfiguration* dan *A06:2021-Vulnerable and Outdated Components*, yang sejalan dengan temuan Widyaningrum et al. [12] dan Setiawan & Fachri [11], di mana mayoritas kerentanan juga disebabkan oleh kesalahan konfigurasi serta penggunaan komponen perangkat lunak yang tidak diperbarui. Hal ini mengindikasikan bahwa akar masalah lebih banyak berasal dari kelalaian dalam pemeliharaan infrastruktur dan pembaruan sistem, ketimbang dari kelemahan logika aplikasi sebagaimana juga ditekankan dalam standar *OWASP Top 10*:2021[19].

Agar keamanan aplikasi web dapat meningkat secara berkelanjutan, rekomendasi ini perlu diimplementasikan secara terukur dan spesifik. Pertama, lakukan pembaruan seluruh komponen perangkat lunak, khususnya versi-versi yang telah mencapai status End-of-Life, dengan memastikan seluruh modul PHP dan plugin pihak ketiga diganti dengan versi yang didukung secara resmi dan memiliki patch keamanan terbaru. Kedua, tetapkan dan terapkan kebijakan pembatasan akses jaringan melalui konfigurasi firewall serta whitelist untuk layanan basis data dan antarmuka administratif, memastikan hanya alamat IP terpercaya yang dapat mengakses layanan tersebut. Ketiga, susun prosedur audit dan pemantauan berkala pada infrastruktur DNS dengan melakukan inventarisasi seluruh subdomain, serta segera menonaktifkan atau memperbaiki konfigurasi yang memungkinkan subdomain takeover.

Penelitian ini merupakan salah satu upaya yang secara spesifik menerapkan kerangka kerja WSTG v4.2 dan penilaian risiko CVSS v3.1 secara terintegrasi dan konsisten pada aplikasi web profil perusahaan (static company profile website) di sektor industri maritim dan logistik, sekaligus mengisi celah pengujian pada objek penelitian yang tidak memiliki form input atau mekanisme otentikasi melalui optimalisasi kategori Information Gathering dan Configuration and Deployment Management Testing. Kontribusi ini diharapkan dapat menjadi rujukan bagi penelitian sejenis pada objek dengan karakteristik serupa.

Mengingat penelitian ini hanya mencakup tiga dari sepuluh kategori WSTG v4.2, penelitian selanjutnya dianjurkan untuk memasukkan kategori pengujian tambahan agar dapat memperoleh gambaran kerentanan yang lebih komprehensif. Secara lebih spesifik, penelitian selanjutnya dapat melakukan penetration testing pada subdomain sea.xyz.com untuk memverifikasi potensi eksploitasi dangling DNS secara lebih mendalam, melakukan verifikasi teknis lebih lanjut terhadap temuan pada Port 8080/8443 sehingga hasilnya dapat disimpulkan secara lebih pasti, serta mempertimbangkan penggunaan Environmental Metrics CVSS v3.1 apabila data kebutuhan bisnis PT.XYZ tersedia, agar skor risiko yang dihasilkan lebih merepresentasikan konteks dampak bisnis secara spesifik.

REFERENSI

[1] N. R. Jayanti, A. F. Sandy, and N. B. Anshary, "Pelatihan Desain dan Pengembangan *Website* Pada Yayasan Baitul Husna Harapan Indah," *Empowerment: J. Pengabdi. pada Masy.*, vol. 5, no. 1, pp. 41–48, 2025, [Online]. Available: *HTTPS*://www.journal.staidk.ac.id/index.*PHP* /pkm/article/view/972

[2] M. Fronita, "Analisis celah keamanan *website* Sitasi menggunakan vulnerability assessment," *J. Ilm. Rekayasa dan Manaj. Sist.* …, 2023, [Online]. Available: *HTTPS*://ejournal.uin-suska.ac.id/index.*PHP* /RMSI/article/view/21823

[3] BSSN, "LANSKAP KEAMANAN SIBER INDONESIA 2024," 2024, [Online]. Available: *HTTPS*://gate.bssn.go.id/ppid-document/Informasi-serta-merta/lanskap-keamanan-siber-indonesia/Lanskap Keamanan Siber Indonesia 2024.pdf

[4] idsirtii/cc, *Laporan Bulanan Publik - Hasil Monitoring Keamanan Siber*. 2025. [Online]. Available: *HTTPS*://drive.google.com/file/d/196vvBtvfyuz9rU-7CaZK0LSAi8B7vFRF/view

E-ISSN 2722-7162
P-ISSN 2089-5615

[5] Siaran Pers, "Kejahatan Siber Capai Kerugian Rp 476 M, AI Diperkuat untuk Cegah Ancaman di Ruang Digital," KOMDIGI. Accessed: Feb. 12, 2026. [Online]. Available: *HTTPS*://www.komdigi.go.id/berita/siaran-pers/detail/kejahatan-siber-capai-kerugian-rp-476-m-ai-diperkuat-untuk-cegah-ancaman-di-ruang-digital

[6] OWASP Foundation, "OWASP Web Security Testing Guide v4.2," OWASP *WSTG*. Accessed: Apr. 20, 2026. [Online]. Available: *HTTPS*://owasp.org/www-project-web-security-testing-guide/v42/2-Introduction/

[7] A. A. A. Setiawan, H. Farisi, and A. Suharsono, "Analisis Keamanan Aplikasi Web silapetro. ub. ac. id Menggunakan Metode VAPT dan *WSTG* 4.2," *… Teknol. Inf. dan Ilmu …*, 2025, [Online]. Available: *HTTPS*://j-ptiik.ub.ac.id/index.*PHP* /j-ptiik/article/view/14901

[8] A. I. Rafeli, H. B. Seta, and I. W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (*WSTG*) pada *Website* XYZ," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 97, 2022, doi: 10.52958/iftk.v18i2.4632.

[9] M. F. Yusuf, I. R. Hikmah, Amiruddin, and S. U. Sunaringtyas, "Security Testing of XYZ *Website* Application Using ISSAF and OWASP *WSTG v4.2* Methods," *Teknika*, vol. 14, no. 1, pp. 66–77, 2025, doi: 10.34148/teknika.v14i1.1156.

[10] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," *Teknika*, 2023, [Online]. Available: *HTTPS*://ejournal.ikado.ac.id/index.*PHP* /teknika/article/view/571

[11] E. Setiawan and F. Fachri, "Pengujian dan Mitigasi Kerentanan *Website* Sistem Informasi Akademik Universitas Ma'arif Nahdlatul Ulama Kebumen dengan OWASP ZAP," *Cyber Secur. dan Forensik Digit.*, vol. 8, no. 1, pp. 25–33, 2025, doi: 10.14421/csecurity.2025.8.1.5190.

[12] B. N. Widyaningrum, D. Maya Rani, and L. Kurnia Ramadhani, "Analysis of the OWASP V4.2 Method in Hospital Information System Security Testing," *MEDIKA TRADA*, vol. 5, no. 2, pp. 87–97, 2024, doi: 10.59485/jtemp.v5i2.99. [Online]. Available: *HTTPS*://journal.polbitrada.ac.id/index.*PHP* /Jtemp/article/view/99

[13] A. S. Lubis and M. P. A. Ginting, "Pengujian aplikasi berbasis web data SKA menggunakan metode *Black Box Testing*," *Cosm. J. Tek.*, 2024, [Online]. Available: *HTTPS*://journal.aira.or.id/cosmic/article/view/760

[14] I. UIN and A. S. P. Wijaya, "PROGRAM STUDI TEKNOLOGI INFORMASI FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI WALISONGO SEMARANG," *eprints.walisongo.ac.id*, [Online]. Available: *HTTPS*://eprints.walisongo.ac.id/29630/1/Skripsi_2008096010_Akbar_Sidiq_Putra_Wijaya.pdf

[15] FIRST, "Common Vulnerability Scoring System v3.1," 2026, [Online]. Available: *HTTPS*://www.first.org/*CVSS*/v3.1/user-guide

[16] NIST-NVD, "Vulnerability Metrics", [Online]. Available: *HTTPS*://nvd.nist.gov/vuln-metrics/*CVSS*

[17] M. A. Hakim, "Analisis Risiko Kerentanan Keamanan Aplikasi Gawai Layanan Masyarakat Pt. Xyz Menggunakan Parameter Owasp Mobile Security dan Pembobotan *CVSS*," *J. Sos. Teknol.*, 2025, [Online]. Available: *HTTP*://sostech.greenvest.co.id/index.*PHP* /sostech/article/view/32528

[18] D. Supriadi, E. Suryadi, R. Muslim, and ..., "Implementasi Vulnerability Assessment Owasp (Open Web Application Security Project) Pada *Website* Universitas Teknologi Mataram," *J. Data …*, 2024, [Online]. Available: *HTTPS*://journal.ppmi.web.id/index.*PHP* /jdaics/article/view/1368

[19] OWASP Foundation, "*OWASP Top 10*:2021," 2021, [Online]. Available: *HTTPS*://owasp.org/Top10/2021/id/

[20] I. M. A. Januraga, et al., "Mendeteksi Keamanan Website SMP Negeri 1 Blahbatuh Menggunakan Metode Open Web Application Security Project (OWASP) Versi 2.11: XSS & Rate Limiting," Format: J. Ilm. Tek. Inform., vol. 11, no. 2, pp. 137–144, 2022.

[21] Alfian, et al., "Pencegahan Kerentanan Keamanan Jaringan Komputer Mikrotik Menggunakan Metode Penetration Testing," J. Ilm. FIFO, vol. 16, no. 2, 2024, doi: 10.22441/fifo.2024.v16i2.003.

[22] Asih, et al., "Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review," J. Ilm. FIFO.