Penerapan Metode OWASP Top 10 2021 Pada Analisis Kerentanan Sistem Informasi Surabaya Single Window

1st Ahmad Difa Salsabila
Sistem Informasi
Universitas Telkom
Surabaya, Indonesia
ahmaddifa@student.telkomuniversity.ac.id

2nd Adzanil Rachmadhi Putra
Sistem Informasi
Universitas Telkom
Surabaya, Indonesia
adzrachmadhip@telkomuniversity.ac.id

3rd Fandisya Rahman
Informatika
Universitas Telkom
Surabaya, Indonesia
fandisya@telkomuniversity.ac.id

***Abstrak* — Dalam beberapa tahun terakhir, instansi pemerintah semakin mengandalkan pelayanan publik berbasis platform online, salah satunya melalui Surabaya Single Window yang dikelola oleh Instansi Pemerintah Kota Surabaya. Website ini digunakan oleh masyarakat untuk mengajukan hampir seluruh jenis permohonan perizinan secara terintegrasi. Tingginya penggunaan dan pengelolaan data penting membuat sistem ini rentan terhadap serangan siber, yang berpotensi merugikan pengguna dan menurunkan kepercayaan terhadap instansi pengelola.**

Penelitian ini bertujuan untuk menilai keamanan website Surabaya Single Window dengan menerapkan framework OWASP Top 10 2021 sebagai standar identifikasi kerentanan. Pengujian dilakukan untuk menemukan potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Hasil penelitian menunjukkan adanya 19 celah keamanan, meliputi konfigurasi sistem, pengelolaan cookie, penggunaan komponen usang, serta parameter yang rentan terhadap manipulasi input. Berdasarkan temuan tersebut, disusun rekomendasi perbaikan yang dapat digunakan oleh Instansi Pemerintah Kota Surabaya untuk meningkatkan keamanan website. Dengan demikian, penelitian ini memberikan kontribusi penting terhadap pengembangan infrastruktur teknologi informasi yang aman dalam mendukung pelayanan publik secara online.

***Kata kunci— OWASP Top 10, Surabaya Single Window*, Serangan Siber.**

I. PENDAHULUAN

Pemanfaatan website dalam pelayanan publik semakin meningkat seiring kebutuhan akan layanan yang cepat dan efisien. Digitalisasi layanan memberikan kemudahan akses bagi masyarakat, namun juga menimbulkan tantangan serius terkait keamanan data dan sistem. Keamanan siber dan privasi menjadi faktor penting dalam keberhasilan layanan digital, terutama pada sistem yang mengelola data sensitif dan informasi penting pengguna (Almeida et al., 2020). Seiring meningkatnya aktivitas digital, risiko kebocoran data turut meningkat, dan Indonesia tercatat sebagai salah satu negara dengan insiden kebocoran data yang tinggi secara global [1].

Surabaya Single Window (SSW) merupakan platform pelayanan perizinan milik Pemerintah Kota Surabaya yang mengelola berbagai layanan administratif dan data penting masyarakat, seperti data identitas pribadi dan dokumen perizinan. Berdasarkan hasil wawancara dengan pengelola sistem, diketahui bahwa hingga saat ini belum dilakukan pengujian keamanan aplikasi web secara terstruktur menggunakan framework OWASP Top 10, serta ditemukan kelemahan pada mekanisme validasi dokumen yang diunggah. Kondisi ini menunjukkan adanya potensi risiko terhadap keamanan sistem, penyalahgunaan fitur aplikasi, serta kebocoran data pengguna.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis keamanan website Surabaya Single Window menggunakan framework OWASP Top 10 guna mengidentifikasi potensi kerentanan dan menyusun rekomendasi perbaikan yang dapat meningkatkan keamanan sistem pelayanan publik berbasis web.

II. KAJIAN TEORI

A. *Penetration Testing*

Penetration testing adalah serangkaian proses berisi prosedur dan teknik mengevaluasi keamanan terhadap sistem komputer atau jaringan dengan melakukan simulasi penyerangan untuk mengetahui letak celah-celah kerawanan pada sistem agar kemudian celah tersebut ditutup atau diperbaiki [2]. Penetration Testing (disebut Pentest atau Ethical Hacking) merupakan serangan resmi pada sistem komputer yang dilakukan untuk mengevaluasi atau menilai keamanan sistem atau jaringan. Untuk mengidentifikasi kerentanan sebanyak-banyaknya dan risiko yang ditimbulkannya, serta membuat laporan dalam bentuk yang dapat diterima dan dipahami oleh klien [3].

B. *OWASP Top 10 2021*

Open Web Application Security Project (OWASP) Top 10 adalah dokumen standar yang berisi daftar kerentanan yang berfokus untuk mengidentifikasi risiko keamanan aplikasi web yang paling berbahaya dan yang paling sering

terjadi di organisasi [4]. Berikut Daftar OWASP Top 10 2021:

1. Broken Access Control [A01:2021]

Kerentanan ini secara khusus terjadi ketika sistem atau aplikasi gagal untuk memberlakukan aturan akses yang tepat, sehingga penyerang mendapatkan akses untuk mengubah akun pengguna, mendapatkan data sensitif, data pengguna, dan sebagainya [5].

2. Cryptographic Failures [A02:2021]

Kerentanan ini terjadi ketika web dan API gagal dalam melindungi data sensitif atau kunci enkripsi. Penyerang dapat melakukan pencurian, penipuan, dan tindak kejahatan yang lain. Untuk melindungi data sensitif memerlukan keamanan tambahan seperti menggunakan SSL/TLS yang terverifikasi [6].

3. Injection [A03:2021]

Ketika terdapat script yang tidak terpercaya disisipkan ke dalam perintah yang dieksekusi oleh sistem. Ini dapat menyebabkan sistem menjalankan perintah yang tidak diinginkan. Penyerang memasukkan kode yang tidak sah ke dalam input aplikasi web, yang dapat mengakibatkan akses tak terotorisasi ke basis data atau manipulasi data [7].

4. Insecure Design [A04:2021]

Ketika desain keamanan yang dikembangkan memiliki kekurangan sehingga menyebabkan kegagalan untuk menentukan tingkat desain keamanan yang dibutuhkan [8].

5. Security Misconfiguration [A05:2021]

Terjadi ketika konfigurasi keamanan tidak dilakukan konfigurasi atau menggunakan konfigurasi default, tanpa melakukan peningkatan pada sistem, dependensi, dan komponen secara berkala [9].

6. Vulnerable and Outdated Components [A06:2021]

Terjadi ketika aplikasi atau sistem menggunakan komponen perangkat lunak yang usang atau memiliki kerentanan keamanan yang diketahui. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk mengambil data sensitif yang ada hingga pengambilan alih server [10].

7. Identification and Authentication Failures [A07:2021]

Kurangnya perlindungan autentifikasi sehingga hal ini dapat menyebabkan penyerang melakukan manipulasi pada token session hingga manipulasi password sehingga penyerang mendapatkan akses ke dalam system [11].

8. Software and Data Integrity Failures [A08:2021]

Kerentanan ini terjadi karena sistem tidak memvalidasi data dengan benar, ini dapat menyebabkan data tidak valid dimasukkan ke dalam aplikasi dan mengancam integritas data seperti aplikasi bergantung pada plugin, libraries, atau modul dari sumber tidak terpercaya [12].

9. Security Logging and Monitoring Failures [A09:2021]

Terjadi ketika ada kegagalan dalam proses pencatatan keamanan dan pemantauan aktivitas yang terjadi pada sistem. Penyerang dapat menggunakan celah ini untuk merusak, mengekstrak, atau menghancur isi data sistem [13].

10. Server-Side Request Forgery [A10:2021]

Ketika penyerang dapat memanipulasi server untuk melakukan permintaan ke sumber daya atau sistem internal lainnya, dengan menggunakan server sebagai perantara. Serangan ini akan terjadi karena web menggunakan API atau layanan eksternal tanpa melakukan validasi. Serangan ini menggunakan perlindungan dari firewall, Virtual Private Network (VPN) dan sejenisnya [14].

C. Analisis Tingkat Resiko

Dalam manajemen risiko keamanan informasi, penilaian tingkat risiko merupakan tahapan penting yang digunakan untuk menentukan prioritas pengendalian terhadap temuan kerentanan yang telah diidentifikasi. Penilaian ini dilakukan dengan cara mengklasifikasikan dua komponen utama, yaitu *impact* dan *likelihood* berdasarkan rentang nilai tertentu. Nilai *impact* menggambarkan besarnya dampak yang mungkin timbul apabila suatu kerentanan dieksploitasi, sementara *likelihood* merepresentasikan kemungkinan terjadinya eksploitasi tersebut, baik secara kualitatif maupun semi-kuantitatif [15].

Perhitungan risiko dilakukan terhadap temuan yang memiliki dampak keamanan dengan menggunakan rumus:

$$Risk = Impact \times Likelihood \quad (1)$$

Kategori risiko dibagi menjadi tiga tingkat berdasarkan hasil perkalian antara *Impact* dan *Likelihood*. Risiko rendah (*Low*) ditandai dengan warna hijau, menunjukkan bahwa risiko tersebut relatif kecil dan cukup dipantau secara rutin tanpa memerlukan tindakan mitigasi khusus. Risiko sedang (*Medium*) ditandai dengan warna kuning, menandakan perlunya tindakan mitigasi sesuai prioritas untuk mengurangi kemungkinan atau dampak terhadap sistem. Sementara itu, risiko tinggi (*High*) ditandai dengan warna merah, yang mengindikasikan risiko signifikan dan membutuhkan penanganan segera agar dampak terhadap keamanan sistem dapat diminimalkan.

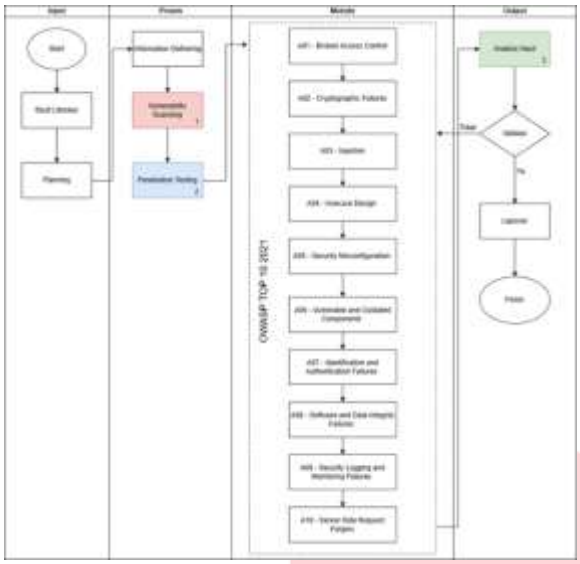
TABEL 1
(TINGKAT RESIKO)

Likelihood \ Impact	***Low Impact (1)***	***Medium Impact (2)***	***High Impact (3)***
High Likelihood (3)	*Medium (3)*	*High (6)*	*High (9)*
Medium Likelihood (2)	*Low (2)*	*Medium (4)*	*High (6)*
Low Likelihood (1)	*Low (1)*	*Low (2)*	*Medium (3)*

III. METODE

Penelitian dilaksanakan melalui 8 tahapan yang dimulai dengan studi literatur, planning, information gathering, vulnerability scanning, penetration testing sesuai dengan kategori OWASP Top 10 2021, analisis hasil, validasi, dan tahap terakhir laporan yang berisikan hasil analisis yang telah divalidasi sehingga memudahkan pengelola website untuk melakukan perbaikan.

A. Prosedur Penelitian



GAMBAR 1
(PROSEDUR PENELITIAN)

Seperti pada Gambar 1, penelitian ini diawali dengan tahap input yang meliputi studi literatur untuk memperoleh pemahaman mengenai konsep, metode, serta kerangka kerja keamanan aplikasi web, khususnya yang mengacu pada OWASP Top 10 2021. Tahap selanjutnya adalah perencanaan, yang mencakup pelaksanaan wawancara dengan pihak terkait, penentuan ruang lingkup dan arah penelitian, pemilihan metode pengujian yang digunakan, serta penetapan alat bantu yang mendukung proses pengujian keamanan. Setelah tahap perencanaan, penelitian memasuki tahap proses yang diawali dengan pengumpulan informasi (*information gathering*) untuk mengidentifikasi informasi teknis sistem, seperti domain, alamat IP, port yang terbuka, layanan aktif, dan teknologi yang digunakan. Informasi tersebut kemudian digunakan sebagai dasar dalam melakukan pemindaian kerentanan (*vulnerability scanning*) dan pengujian penetrasi (*penetration testing*) yang dilakukan dengan mengacu pada kategori kerentanan OWASP Top 10 2021, mulai dari A01 hingga A10, untuk mengidentifikasi dan menganalisis potensi celah keamanan pada sistem. Selanjutnya, hasil pengujian dianalisis untuk memperoleh gambaran kondisi keamanan sistem secara menyeluruh. Hasil analisis tersebut kemudian melalui tahap validasi oleh pihak yang berkompeten. Tahap akhir dari penelitian ini adalah penyusunan laporan yang memuat seluruh proses, hasil pengujian, analisis, dan kesimpulan penelitian.

IV. HASIL DAN PEMBAHASAN

A. Planning

Tahap awal adalah mendalami sistem Surabaya Single Window. Proses identifikasi ini penting untuk menentukan ruang lingkup pengujian keamanan. Karena tidak semua bagian website bisa diakses publik atau diuji secara bebas, maka analisis difokuskan pada halaman-halaman yang terbuka dan umum digunakan. Selain itu, pendekatan yang digunakan tetap mengikuti prinsip ethical hacking, yaitu tanpa merusak sistem atau mengambil data secara ilegal. Sebagai dasar pengujian, analisis akan mengacu pada standar OWASP Top 10, yang merupakan daftar sepuluh kerentanan paling umum dalam aplikasi web.

B. Information Gathering

Tahap kedua yaitu melakukan Information Gathering dimulai dari mencari tahu ip pada website menggunakan tools nslookup, dig (dns lookup), nmap. Lalu untuk mengetahui teknologi website menggunakan wappalyzer.

1. Nslookup

Pada saat dilakukan perintah “nslookup sswalfa.surabaya.go.id” menunjukkan bahwa permintaan nslookup dikirim ke server DNS lokal dengan alamat IP 10.0.2.3, yang juga merespons melalui port standar DNS yaitu port 53. Kemudian, sistem memberikan "non-authoritative answer", yang artinya informasi ini bukan berasal langsung dari server DNS utama (authoritative DNS server) untuk domain tersebut, melainkan dari DNS server lain. Sebagai hasilnya, nama domain sswalfa.surabaya.go.id dipetakan ke alamat IP publik 112.140.160.92.

2. Domain Information Groper

Pada saat dilakukan perintah “dig sswalfa.surabaya.go.id” menunjukkan bahwa permintaan DNS telah berhasil dijalankan tanpa error (status: NOERROR) dengan ID permintaan adalah 54904. Diketahui bahwa domain sswalfa.surabaya.go.id memiliki alamat IP yaitu 112.140.160.92. Informasi ini muncul di bagian ANSWER SECTION, yang merupakan bagian utama dari hasil query DNS.

Selanjutnya, di bagian AUTHORITY SECTION, ditampilkan daftar name server yang berwenang untuk domain induk surabaya.go.id. Beberapa di antaranya adalah:

1. dns2.surabaya.go.id,
2. nsa4.pusatdns.id,
3. nssec1.radnet-digital.id,
4. perseus.surabaya.go.id,
5. pluto.surabaya.go.id.

Server-server ini bertugas menjawab permintaan DNS yang berkaitan dengan domain surabaya.go.id.

Di bagian ADDITIONAL SECTION, sistem memberikan alamat IP dari beberapa name server yang telah disebutkan sebelumnya. Misalnya,

1. dns2.surabaya.go.id memiliki IP 112.140.160.9,
2. pluto.surabaya.go.id memiliki IP 203.14.183.8,
3. perseus.surabaya.go.id memiliki IP 36.95.133.214.

Informasi tambahan ini berguna untuk mempercepat proses resolusi DNS karena tidak perlu dilakukan query ulang terhadap IP dari name server tersebut.

3. Nmap

Hasil pemindaian menggunakan Nmap pada domain `sswalfa.surabaya.go.id` menunjukkan bahwa server tujuan dalam keadaan aktif dan merespons dengan sangat cepat, hanya memerlukan waktu sekitar 0.0023 detik (2.3 milidetik) untuk memberikan respons. Pemindaian ini menggunakan metode SYN scan (`-sS`) yang bersifat stealthy (tidak membuat koneksi penuh) dan juga melakukan deteksi versi

layanan (`-sV`). Dari total 1000 port TCP yang dipindai, sebanyak 998 port tidak memberikan respons dan terdeteksi sebagai "filtered", yang berarti sebagian besar diblokir oleh firewall atau sistem keamanan jaringan.

TABEL 2
(HASIL PORT TERBUKA NMAP)

Port	Status	Layanan	Versi
80	Open	http	nginx
443	Open	Ssl/http	nginx

Adapun dua port yang terdeteksi terbuka adalah port 80 dan port 443, yang masing-masing digunakan untuk layanan HTTP dan HTTPS. Kedua layanan ini dijalankan oleh web server nginx, yang cukup populer karena efisiensi dan performanya. Port 80 menunjukkan bahwa server menyediakan layanan web tanpa enkripsi, sedangkan port 443 menandakan layanan web yang menggunakan enkripsi SSL/TLS untuk koneksi aman.

4. Wappalyzer

Untuk mengetahui teknologi yang ada pada sebuah website membutuhkan extension dari web browser seperti wappalyzer, wappalyzer dapat memberikan informasi tentang teknologi seperti CMS (Content Management System), Framework hingga library pada website secara otomatis, hasilnya dapat dilihat pada tabel berikut:

TABEL 3
(HASIL SCAN WAPPALYZER)

Kategori	Teknologi	Versi
JavaScript Frameworks	toastr	2.1.4
	Handlebars	4.1.0
Font Scripts	Google Font API	
Web Frameworks	Laravel	-
Miscellaneous	Popper	-
CDN	Cloudflare	-
	Unpkg	-
	jQuery CDN	-
	cdnjs	-
JavaScript Libraries	Moment.js	2.24.0
	JSZip	3.2.0
	Dropzone	5.5.1
	SweetAlert2	-
Web Servers	Nginx	-
Rich Text Editors	Quill	-
	CKEditor	-
JavaScript Graphics	Raphael	2.3.0
	Chart.js	-
Programming Languages	PHP	-
Select Plugins	Select2	-
	OWL Carousel	-
	jQuery	1.14.15
	DataTables	1.10.20
	AOS	2.3.1
Reverse Proxies	Nginx	-
UI Frameworks	Bootstrap	4.4.1

C. Vulnerability Scanning

Pada tahap ini menggunakan aplikasi OWASPProses identifikasi kerentanan keamanan yang ada pada website dapat dilihat dari tabel dibawah dengan hasil sebagai berikut:

TABEL 4
(TABEL HASIL VULNERABILITY SCANNING)

Jenis Kerentanan	Tingkat Resiko
SQL Injection - SQLite	*High*
Absence of Anti-CSRF Tokens	*Medium*
CSP: script-src unsafe-eval	*Medium*
Cookie Without Secure Flag	*Medium*
Cookie No HttpOnly Flag	*Medium*
Strict-Transport-Security Header Not Set	*Medium*
Cross-Domain Misconfiguration	*Medium*
CSP: style-src unsafe-inline	*Low*
Timestamp Disclosure - Unix	*Informational*
X-Content-Type-Options Header Missing	*Informational*
Authentication Request Identified	*Informational*
Information Disclosure - localStorage	*Informational*
Information Disclosure - sessionStorage	*Informational*
Information Disclosure - URL	*Informational*
Information Disclosure - Suspicious Comments	*Informational*
Loosely Scoped Cookie	*Informational*
Modern Web Application	*Informational*
Re-examine Cache-Control Directives	*Informational*
Retrieved from Cache	*Informational*
Session Management Response Identified	*Informational*
Tech Detected (Laravel, PHP, jQuery, dll.)	*Informational*
User Agent Fuzzer	*Informational*
User Controllable HTML Element Attribute	*Informational*

Dari tabel diatas ditemukan 23 potensi kerentanan keamanan dengan tingkat risiko bervariasi mulai dari High, Medium, hingga Informational.

D. Penetration Testing

1. Broken Access Control [A01:2021]

TABEL 5
(TABEL HASIL A01 ZAP DAN DIRSEARCH)

Testing	Parameter	Temuan	Keterangan
OWASP ZAP	sswalfa.surabaya.go.id /cek	Tidak ada perlindungan token *anti-CSRF* pada formulir HTML.	Tidak memiliki mekanisme perlindungan anti-CSRF, yang dapat disalahgunakan.
OWASP ZAP	dist/aos.css	Konfigurasi Access-Control-Allow-Origin di setel dengan nilai *.	File css library AOS dari pihak ketiga sehingga scanner mendeteksi sebagai kerentanan, dan beresiko apabila pihak ketiga telah diretas.
OWASP ZAP	sswalfa.surabaya.go.id	*cookie XSRF-TOKEN* diatur tanpa *Attribute SameSite.*	*Cookie* dikirim sebagai bagian dari permintaan lintas situs, dapat dimanfaatkan oleh penyerang untuk melakukan serangan.
OWASP ZAP	datatables.bundle.js	*Timestamp Unix* terekspos di dalam kode JavaScript.	Dapat memberikan petunjuk mengenai usia *software* atau sistem saat dibuat.
Dirsearch	sswalfa.surabaya.go.id	Muncul Pesan *"Too many request errors"* kegagalan dalam mengakses server.	Terlalu banyak permintaan HTTP yang gagal server mendeteksi aktivitas pemindaian berlebihan. Hal ini disebabkan karena website memiliki WAF (*Web Application firewall*).

Setelah dilakukan pengetesan menggunakan OWASP ZAP dan Dirsearch, dilakukan juga pengetesan secara manual untuk mengetahui kerentanan yang ada. sesuai dengan kategori A01.

TABEL 6
(TABEL HASIL A01 MANUAL)

Testing	Parameter	Temuan	Keterangan
Manual	/info/daftar-perizinan	Setelah dilakukan pengetesan manual, tidak ada perlindungan token *anti-CSRF* pada formulir HTML.	Website tidak memiliki mekanisme perlindungan anti-CSRF, yang dapat disalahgunakan.
Manual	dist/aos.css	Setelah dilakukan pengetesan manual Konfigurasi Access-Control-Allow-Origin di setel dengan nilai *.	File css library AOS dari pihak ketiga sehingga scanner mendeteksi sebagai kerentanan, dan beresiko apabila pihak ketiga telah diretas.
Manual	sswalfa.surabaya.go.id	Setelah dilakukan pengetesan manual *cookie* dengan parameter *XSRF-TOKEN* diatur tanpa *Attribute SameSite*.	*cookie* tersebut dikirim sebagai bagian dari permintaan lintas situs, dapat dimanfaatkan oleh penyerang untuk melakukan serangan.
Manual	datatables.bundle.js	Setelah dilakukan pengetesan manual *Timestamp Unix* terekspos di dalam kode JavaScript.	Dapat memberikan petunjuk mengenai usia *software* atau sistem saat dibuat.

2. Cryptographic Failures [A02:2021]

TABEL 7
(TABEL HASIL A02 WIRESHARK)

Testing	Parameter	Temuan	Keterangan
Wire shark	sswalfa.surabaya.go.id	Telah menerapkan protokol TLS dan *cipher suit* untuk mengamankan jaringan	Tidak ditemukan celah kerentanan pada pengujian ini

Website telah menerapkan protokol jaringan yang aman antara server dan klien sehingga tidak ditemukan kerentanan sesuai dengan kategori A02.

3. Injection [A03:2021]

TABEL 8
(TABEL HASIL A03 OWASP ZAP, JSQL, MANUAL)

Testing	Parameter	Temuan	Keterangan
OWASP ZAP	simulasi_retribusi/ get_hari_penggunaan _gedung parameter id_kekda	Adanya kerentanan SQL Injection	Query dapat dikontrol menggunakan nilai parameter, yang menyebabkan waktu respons *server* meningkat secara signifikan saat *payload* dimasukkan.
JSQL	simulasi_retribusi/ get_hari_penggunaan _gedung parameter id_kekda	Test done dan tidak menemukan celah.	Tidak ditemukan kerentanan pada url tersebut sehingga aman
Manual	simulasi_retribusi/ get_hari_penggunaan _gedung parameter id_kekda	Setelah dilakukan pengetesan manual tidak ditemukan celah.	Tidak ditemukan kerentanan pada url tersebut sehingga aman

Setelah dilakukan pengetesan dengan OWASP ZAP, JSQL, dan Manual, dapat dipastikan apabila hasil dari OWASP ZAP termasuk kedalam false positive sehingga tidak ditemukan kerentanan dengan kategori A03.

4. Insecure Design [A04:2021]

TABEL 9
(TABEL HASIL A04 OWASP ZAP, MANUAL)

Testing	Parameter	Temuan	Keterangan
OWASP ZAP	sso-wargaku-auth	*Big Redirect* (Pengalihan Halaman) yang berlebihan atau tidak terkontrol.	*Redirect* ini berpotensi membocorkan informasi sensitif karena aplikasi mengarahkan pengguna kembali ke halaman tertentu sehingga bisa dimanipulasi.
Manual	sso-wargaku-auth	Temuan ini tidak menunjukkan indikasi kebocoran informasi sensitif pada url sehingga aman dari risiko kebocoran.	Aman tidak ditemukan kebocoran informasi sensitif pada URL.

Setelah dilakukan pengetesan dengan OWASP ZAP, dan Manual, dapat dipastikan apabila hasil dari OWASP ZAP termasuk kedalam false positive sehingga tidak ditemukan kerentanan dengan kategori A04.

5. Security Misconfiguration [A05:2021]

TABEL 10
(TABEL HASIL A05 OWASP ZAP)

Testing	Parameter	Temuan	Keterangan
OWASP ZAP	sswalfa.surabaya.go.id	Website tidak mengirimkan *header* CSP di respons HTTP-nya.	Rentan terhadap serangan XSS. Jika penyerang berhasil menyuntikkan skrip berbahaya, karena tidak ada kebijakan yang membatasi sumber skrip.
OWASP ZAP	sswalfa.surabaya.go.id	Tidak menggunakan header respon X-Frame-Options	Website mengizinkan situs web lain untuk memuat halaman ini di dalam frame tersendiri <iframe>
OWASP ZAP	simulasi_retribusi/simulasi	Server merespons dengan status kode HTTP/1.1 500 Internal Server Error	Ada kesalahan internal yang tidak terduga terjadi di sisi server
OWASP ZAP	sswalfa.surabaya.go.id	Tidak mengaktifkan `HttpOnly` pada cookie dengan parameter `XSFR-TOKEN`.	Jika atribut ini tidak diaktifkan, maka potensi serangan Cross-Site Scripting (XSS) dapat mengekspos data sensitif yang disimpan dalam cookie,
OWASP ZAP	sswalfa.surabaya.go.id	Cookie XSRF-TOKEN tidak memiliki *flag Secure*	*Cookie* dikirimkan melalui koneksi HTTP yang tidak terenkripsi meskipun situs diakses melalui https
OWASP ZAP	sswalfa.surabaya.go.id	Rentan SSL Stripping / Downgrade Attacks	Website tidak memaksa untuk *selalu* menggunakan HTTPS setelah kunjungan pertama
OWASP ZAP	sswalfa.surabaya.go.id	Tidak ada konfigurasi header X-Content-Type-Options	Rentan MIME Sniffing Penyerang bisa mengunggah file gambar, yang memungkinkan eksekusi kode jahat.

Setelah dilakukan pengetesan dengan OWASP ZAP, ditemukan 7 kerentanan dengan kategori A05.

TABEL 11
(TABEL HASIL A05 MANUAL)

Testing	Parameter	Temuan	Keterangan
Manual	sswalfa.surabaya.go.id	Website tidak mengirimkan *header* CSP di respons HTTP-nya.	Rentan terhadap serangan XSS. Jika penyerang berhasil menyuntikkan skrip berbahaya, karena tidak ada kebijakan yang membatasi sumber skrip.
Manual	sswalfa.surabaya.go.id	Tidak menggunakan header respon X-Frame-Options	Website mengizinkan situs web lain untuk memuat halaman ini di dalam frame tersendiri <iframe>
Manual	simulasi_retribusi/simulasi	Setelah dilakukan pengujian manual 405 Method Not Allowed website tidak bisa diakses. Bukan kesalahan server	Tidak terjadi kesalahan internal server namun server menolak request yang dikirm dari sisi client yang berarti aman.
Manual	sswalfa.surabaya.go.id	Tidak mengaktifkan `HttpOnly` pada cookie dengan parameter `XSFR-TOKEN`.	Jika atribut ini tidak diaktifkan, maka potensi serangan Cross-Site Scripting (XSS) dapat mengekspos data sensitif yang disimpan dalam cookie,
Manual	sswalfa.surabaya.go.id	Cookie XSRF-TOKEN tidak memiliki *flag Secure*	*Cookie* dikirimkan melalui koneksi HTTP yang tidak terenkripsi meskipun situs diakses melalui https
Manual	sswalfa.surabaya.go.id	Rentan SSL Stripping / Downgrade Attacks	Website tidak memaksa untuk *selalu* menggunakan HTTPS setelah kunjungan pertama
Manual	sswalfa.surabaya.go.id	Tidak ada konfigurasi header X-Content-Type-Options	Rentan MIME Sniffing Penyerang bisa mengunggah file gambar, yang memungkinkan eksekusi kode jahat.

Setelah dilakukan pengetesan secara manual dapat dipastikan beberapa kerentanan yang terdeteksi oleh OWASP ZAP dengan kategori A05 dipastikan valid kecuali HTTP/1.1 500 *Internal Server Error* karena hasil pengetesan manual menunjukan 405 *Method Not Allowed* yang berarti server menolak respon dan bukan kesalahan server.

6. Vulnerable and Outdated Components [A06:2021]

TABEL 12
(TABEL HASIL A06 WAPPALYZER)

Kategori	Teknologi	Versi saat ini	Versi Terbaru
JavaScript	*toastr*	2.1.4	17.0.0
Frameworks	*Handlebars*	4.1.0	4.7.7
JavaScript Libraries	*Moment.js*	2.24.0	2.29.1
JavaScript Libraries	*JSZip*	3.2.0	3.10.1
JavaScript Libraries	*Dropzone*	5.5.1	5.7.0
JavaScript Graphics	*Raphael*	2.3.0	2.3.0
Select Plugins	*jQuery*	1.14.15	3.6.0
Select Plugins	*DataTables*	1.10.20	1.11.5
Select Plugins	*AOS*	2.3.1	3.0.0
UI Frameworks	*Bootstrap*	4.4.1	5.2.3

Berdasarkan hasil analisis menggunakan Wappalyzer, ditemukan 10 komponen perangkat lunak yang sudah usang. Komponen yang tidak diperbarui berpotensi mengandung celah keamanan yang telah dan dapat dimanfaatkan oleh penyerang ini masuk dalam kategori A06.

7. Identification and Authentication Failures [A07:2021]

TABEL 13
(TABEL HASIL A07 BURPSUITE)

Testing	Parameter	Temuan	Keterangan
Burp Suite	sswalfa.surabaya.go.id/login	Setelah dilakukan simulasi percobaan autentikasi berulang, memberikan respon yang konsisten tanpa indikasi autentikasi berhasil maupun perbedaan respon yang dapat dimanfaatkan penyerang.	Hal ini menunjukkan bahwa mekanisme autentikasi tidak rentan terhadap serangan *brute force*.

Setelah dilakukan pengujian menggunakan burpsuite, tidak ditemukan celah dengan kategori A07.

8. Software and Data Integrity Failures [A08:2021]

TABEL 14
(TABEL HASIL A08 OWASP ZAP)

Testing	Parameter	Temuan	Keterangan
OWASP ZAP	dist/aos.js	Menggunakan file JavaScript dari domain pihak ketiga.	Aplikasi memuat file dari domain eksternal Hal berisiko apabila *third party* tersebut diretas.

Setelah dilakukan pengetesan dengan OWASP ZAP, ditemukan kerentanan dengan kategori A08.

TABEL 15
(TABEL HASIL A08 MANUAL)

Testing	Parameter	Temuan	Keterangan
Manual	dist/aos.js	Website menggunakan file JavaScript dari domain pihak ketiga.	Aplikasi memuat file dari domain eksternal Hal berisiko apabila *third party* tersebut diretas.

Setelah dilakukan pengetesan secara manual, dapat dipastikan bahwa hasil dari OWASP ZAP benar ditemukan javascript dari domain pihak ketiga termasuk kategori A08. disarankan untuk menerapkan Subresource Integrity (SRI) sebagai mekanisme verifikasi tambahan terhadap sumber daya eksternal atau memindahkan skrip tersebut ke server lokal.

9. Security Logging and Monitoring Failures [A09:2021]

TABEL 16
(TABEL HASIL A09 BURPSUITE)

Testing	Parameter	Temuan	Keterangan
Burp Suite	Sswalfa.surabaya.go.id/login	*Security logging dan monitoring* dapat merespon semua dengan status 200 OK	Semua proses direspon server dengan status 200 OK yang berarti tidak ada mekanisme pencegahan rate limiting atau pembatasan dalam percobaan login yang tidak sah.

Setelah dilakukan pengetesan menggunakan burpsuite ditemukan kesalahan dalam *logging* dan *monitoring* dari percobaa login yang tidak sah berulang yang direspon 200 OK tanpa adanya percobaan pembatasan atau *rate limiting* ini masuk kedalam kategori A09.

10. Server-Side Request Forgery [A10:2021]

TABEL 17
(TABEL HASIL A10 MANUAL)

Testing	Parameter	Temuan	Keterangan
Manual	127.0.0.1:8080	Page forbidden setelah ditambahkan parameter pada pencarian website http://127.0.0.1:8080	Server mendeteksi adanya akses oleh pengguna yang tidak sah dan server telah dilindungi dengan baik sehingga aman dari percobaan untuk SSRF.

Setelah dilakukan pengetesan manual, tidak ditemukan celah yang termasuk dalam kategori A10. Website aman dari percobaan SSRF.

11. Analisis Tingkat Resiko

Setelah seluruh proses analisis hasil pengujian selesai dilakukan, tahap berikutnya adalah penentuan tingkat resiko terhadap temuan kerentanan yang telah diidentifikasi, sebagai dasar dalam penyusunan rekomendasi perbaikan keamanan.

TABEL 18
(TABEL HASIL TINGKAT RESIKO)

ID	Kerentanan	Impact	Likelihood	Risk
A01	*Absence of Anti-CSRF Tokens*	–	–	*Informational*
A01	*Cross-Domain Misconfiguration*	1	1	*Low*
A01	*Cookie without SameSite Attribute*	–	–	*Informational*
A01	*Timestamp Disclosure (Unix)*	–	–	*Informational*
A02	Konfigurasi Keamanan Jaringan (TLS)	–	–	*Informational*
A03	*SQL Injection*	–	–	*Informational*
A04	*Open Redirect*	–	–	*Informational*
A05	*Content Security Policy (CSP) Header Not Set*	2	2	*Medium*
A05	*Missing Anti-clickjacking Header*	1	2	*Low*
A05	*Application Error Disclosure*	–	–	*Informational*
A05	*Cookie No HttpOnly Flag*	2	2	*Medium*
A05	*Cookie Without Secure Flag*	2	2	*Medium*
A05	*Strict-Transport-Security Header Not Set*	2	2	*Medium*
A05	*X-Content-Type-Options Header Missing*	1	2	*Low*
A06	*Outdated Components*	1	2	*Low*
A07	*Brute Force Authentication*	–	–	*Informational*
A08	*Cross-Domain JavaScript Inclusion*	–	–	*Informational*
A09	*Logging & Monitoring (Spam Login)*	2	2	*Medium*
A10	*Server-Side Request Forgery (SSRF)*	–	–	*Informational*

Berdasarkan hasil pada tabel, ditemukan total 19 kerentanan yang terdiri dari 10 temuan dengan kategori Informational, 4 temuan dengan tingkat Low, dan 5 temuan dengan tingkat Medium, serta tidak ditemukan kerentanan dengan tingkat High. Penilaian risiko pada

penelitian ini dilakukan dengan memisahkan temuan Informational dari temuan yang memiliki dampak keamanan. Temuan Informational tidak dihitung dalam perhitungan risiko karena tidak menimbulkan dampak langsung maupun potensi eksploitasi terhadap sistem, namun tetap dicatat sebagai informasi pendukung dalam upaya peningkatan keamanan aplikasi.

V. KESIMPULAN

Berdasarkan hasil pengujian penetrasi yang telah dilakukan terhadap website Surabaya Single Window (SSW) menggunakan metode OWASP Top 10 2021, dapat disimpulkan bahwa sistem masih memiliki sejumlah 19 potensi kerentanan keamanan. Kerentanan tersebut terutama ditemukan pada aspek Broken Access Control, Security Misconfiguration, Vulnerable and Outdated Components, serta Identification and Authentication Failures, yang berkaitan dengan konfigurasi keamanan, pengelolaan cookie, penggunaan komponen yang sudah usang, serta parameter tertentu yang rentan terhadap manipulasi input. Kerentanan yang teridentifikasi berpotensi menimbulkan berbagai dampak, seperti akses tidak sah, pengungkapan data sensitif, manipulasi permintaan, lemahnya mekanisme logging dan monitoring, serta risiko terhadap integritas data. Selain itu, penggunaan komponen yang tidak diperbarui meningkatkan kemungkinan terjadinya eksploitasi karena tidak lagi mendapatkan pembaruan keamanan. Secara keseluruhan, hasil analisis menunjukkan bahwa SSW memiliki total 19 kerentanan yang masuk ke dalam beberapa kategori OWASP Top 10 2021, khususnya pada aspek keamanan akses, konfigurasi sistem, serta pencatatan logging dan monitoring. Temuan ini mengindikasikan bahwa platform SSW memerlukan pembaruan komponen, perbaikan konfigurasi keamanan, serta penguatan mekanisme validasi dan proteksi agar selaras dengan standar keamanan aplikasi web modern.

REFERENSI

[1] Surfshark, “Data Breach Monitoring Quarterly Analysis.” [Online]. Available: https://surfshark.com/research/data-breach-monitoring/quarterly-analysis

[2] Mulyadi, “Bagaimana Melakukan ‘Penetration Test’?” [Online]. Available: https://www.kompasiana.com/moengil/5a4ae2655e13736b135dd7e3/bagaimana-melakukanpenetration-testing

[3] C. A. Indonesia, “Mengenal Tentang Penetration Testing.” [Online]. Available: https://www.cyberacademy.id/blog/mengenal-tentang-penetration-testing

[4] OWASP, “OWASP Top Ten.” [Online]. Available: https://owasp.org/Top10/

[5] OWASP, “Broken Access Control.” [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

[6] OWASP, “Cryptographic Failures.” [Online]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

[7] OWASP, “Injection.” [Online]. Available: https://owasp.org/Top10/A03_2021-Injection/

[8] OWASP, “Insecure Design.” [Online]. Available: https://owasp.org/Top10/A04_2021-Insecure_Design/

[9] OWASP, “Security Misconfiguration.” [Online]. Available: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

[10] OWASP, “Vulnerable And Outdated Components.” [Online]. Available: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

[11] OWASP, “Identification And Authentication Failures.” [Online]. Available: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

[12] OWASP, “Software And Data Integrity Failures.” [Online]. Available: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

[13] OWASP, “Security Logging And Monitoring Failures.” [Online]. Available: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/

[14] OWASP, “Server-side Request Forgery (SSRF).” [Online]. Available: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

[15] I. Kuzminykh, B. Ghita, V. Sokolov, and T. Bakhshi, “Information Security Risk Assessment,” *Encyclopedia*, vol. 1, no. 3, pp. 602–617, Jul. 2021, doi: 10.3390/encyclopedia1030050.