Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 2452-2460
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Kerentanan Keamanan Aplikasi SIGAP Sumsel Menggunakan Metode Open Web Application Security Project (OWASP)

Rama Antonius, Fenny Purwarni
Jurusan Sistem Informasi, Fakultas Sains Dan Teknologi, UIN Raden Fatah Palembang
ramaantonius14@gmail.com, fenny_purwani@radenfatah.ac.id

Abstrak

Di era digitalisasi layanan publik, aplikasi SIGAP Sumatera Selatan berperan krusial dalam proses administrasi magang, memfasilitasi pendaftaran, verifikasi, dan monitoring secara efisien. Namun, ketergantungan tinggi pada platform berbasis web menimbulkan risiko signifikan terhadap kerentanan keamanan cyber, seperti pelanggaran data sensitif mahasiswa dan pegawai, penyalahgunaan wewenang, hingga gangguan operasional pelayanan publik yang dapat berdampak luas pada kepercayaan masyarakat. Penelitian ini bertujuan menganalisis kerentanan keamanan aplikasi SIGAP Sumatera Selatan secara komprehensif menggunakan metodologi Open Web Application Security Project (OWASP), khususnya melalui pengujian otomatis dengan alat OWASP ZAP. Pendekatan bersifat deskriptif dengan teknik black-box non-intrusif, mencakup pemindaian pasif (spidering dan forced browsing) serta aktif (active scan) terhadap komponen utama seperti autentikasi pengguna, parameter input, dan konfigurasi server. Analisis difokuskan pada OWASP Top 10 risiko terkini, termasuk injection (SQLi), broken access control, konfigurasi keamanan tidak aman, serta cross-site scripting (XSS). Hasil pengujian mengungkap 15 kerentanan dengan tingkat risiko bervariasi (rendah hingga tinggi), seperti potensi eksploitasi SQL injection pada form login, CSRF pada endpoint approval magang, dan pengungkapan informasi sensitif via error message. Secara kolektif, temuan ini dapat menurunkan tingkat kepercayaan publik terhadap sistem. Rekomendasi mencakup penerapan enkripsi data end-to-end (AES-256), validasi input ketat dengan prepared statements, pembaruan patch keamanan berkala via automated tools, serta pelatihan rutin personel administrator mengenai best practices OWASP. Secara keseluruhan, penelitian ini berkontribusi pada penguatan ketahanan cyber aplikasi pemerintah daerah sekaligus menyediakan acuan metodologis bagi evaluasi keamanan sistem informasi serupa di Indonesia.

Kata kunci: *Analisis Keamanan, Aplikasi SIGAP Sumsel, Kerentanan Keamanan, Metode OWASP*

1. Latar Belakang

Magang merupakan bagian integral dari pendidikan tinggi yang dimaksudkan sebagai kesempatan bagi mahasiswa untuk mengembangkan kompetensi yang dibutuhkan dunia kerja, yaitu menerapkan pengetahuan, keterampilan, dan sikap (soft skill dan hard skill) dalam situasi nyata[1]. Dan memungkinkan mahasiswa mengaplikasikan ilmu teori ke dunia kerja nyata, mengasah keterampilan profesional, serta memahami dinamika lingkungan instansi pemerintahan.. Selama 40 hari magang di Kantor Wilayah Kementerian Hukum Sumatera Selatan, mahasiswa Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Raden Fatah Palembang, terlibat langsung dalam kegiatan digital seperti layanan administrasi hukum umum, kekayaan intelektual, dan pendaftaran magang/penelitian melalui aplikasi SIGAP Sumsel. Aplikasi ini, sebagai inovasi digital pemerintahan, memfasilitasi pendaftaran online dengan mengelola data pribadi sensitif seperti identitas mahasiswa, KTM, transkrip nilai, serta dokumen resmi, sehingga menuntut keamanan informasi yang ketat. Namun, transformasi digital di sektor publik rentan terhadap serangan siber seperti injection, broken access control, dan sensitive data exposure sebagaimana diidentifikasi OWASP Top 10 (2021). Metodologi OWASP, didukung alat OWASP ZAP untuk pengujian black-box non-intrusif (pemindaian pasif/aktif), efektif mengungkap kerentanan pada autentikasi, input parameter, dan konfigurasi server, sebagaimana dibahas [2], [3]. pengujian keamanan website menggunakan metode OWASP ZAP pada website 43.255.184.109. Dari hasil pengujian yang dilakukan melalui empat tahap, yaitu Information Gathering, Session Management Testing, Data Validation Testing, dan Webservices Testing, ditemukan berbagai celah keamanan pada website tersebut. Berdasarkan perhitungan OWASP Risk Rating, diperoleh skor Likelihood sebesar 5,5 dan skor Impact sebesar 2,6. Mengacu pada tabel Likelihood and Impact

Levels, website tersebut dikategorikan dalam Low severity risk dari sisi likelihood dan Medium severity risk dari sisi impact[4].

Kerentanan berisiko tinggi meliputi Stored Cross-Site Scripting (VULN-01, kategori A03:2021) pada fitur buku tamu yang memungkinkan penyerang menyimpan skrip berbahaya di basis data, serta penggunaan komponen CMS dan plugin yang usang (VULN-02, kategori A06:2021) yang berpotensi menyebabkan kompromi total server dan eksekusi kode jarak jauh. Sementara itu, kerentanan berisiko sedang mencakup Security Misconfiguration (VULN-03), Broken Access Control atau IDOR (VULN-04), dan kelemahan autentikasi tanpa proteksi brute-force (VULN-05)[5]. OWASP ZAP merupakan alat yang sangat berguna dalam mengidentifikasi dan menilai kerentanan keamanan pada website, dan merekomendasikan penerapan konfigurasi header keamanan seperti CSP, HSTS, dan X-Frame Options, serta perlindungan terhadap data sensitif sebagai langkah mitigasi utama untuk mencegah eksploitasi. Pengujian menggunakan OWASP ZAP pada website XYZ menemukan 11 kerentanan, yaitu Directory Browsing, Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Application Error Disclosure, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Timestamp Disclosure – Unix, X-Content-Type-Options Header Missing, dan Information Disclosure Suspicious Comments. Berdasarkan analisis OWASP Risk Rating, seluruh temuan memiliki tingkat likelihood sedang, sedangkan impact bervariasi antara sedang dan rendah[6]. Berdasarkan hasil penelitian evaluasi risiko celah keamanan pada aplikasi E-Office Pemerintah Kabupaten Ogan Ilir dilakukan menggunakan metode OWASP (Open Web Application Security Project) dengan pendekatan *standard risk model* (Risk = Likelihood * Impact). Proses pengujian mengidentifikasi berbagai celah keamanan berdasarkan standar OWASP Top 10 dengan menilai faktor kemungkinan (*likelihood*) dan dampak (*impact*). Hasil dari penilaian tersebut mengklasifikasikan tingkat risiko ke dalam kategori *Low*, *Medium*, atau *High*. Dari temuan identifikasi risiko ini, disusunlah rekomendasi perbaikan celah keamanan yang dapat digunakan oleh Pemerintah Kabupaten Ogan Ilir sebagai langkah antisipasi dan pencegahan terhadap kemungkinan kerugian sistem.[7]

Oleh karena itu, mengenai pentingnya magang dalam pendidikan tinggi dan kerentanan keamanan aplikasi SIGAP Sumsel yang mengelola data sensitif mahasiswa, penelitian ini merumuskan tiga masalah utama sebagai berikut: Apa saja kerentanan keamanan yang ditemukan pada aplikasi SIGAP Sumsel berdasarkan standar OWASP Top 10 tahun 2021, seperti injection, broken access control, dan sensitive data exposure, Bagaimana tingkat risiko dari setiap kerentanan yang teridentifikasi melalui proses penetration testing non-intrusif dengan OWASP ZAP, Apa rekomendasi teknis yang dapat diberikan untuk meningkatkan keamanan aplikasi SIGAP Sumsel berdasarkan hasil temuan kerentanan tersebut. Rumusan ini bertujuan mengarahkan analisis sistematis terhadap celah keamanan yang berpotensi mengancam integritas data pribadi dan kepercayaan publik terhadap layanan digital pemerintahan. Tujuan umumnya adalah menganalisis keamanan SIGAP Sumsel guna identifikasi kerentanan data pribadi menggunakan OWASP, sebagai acuan penguatan sistem pemerintahan digital. Secara khusus, penelitian menelaah mekanisme keamanan (data, autentikasi, transmisi), menganalisis OWASP Top 10 (injection dll.), mengidentifikasi penyebab celah teknis/prosedural, serta memberikan rekomendasi konseptual/teknis untuk menjaga integritas data., penelitian pada sistem informasi Universitas Duta Bangsa Surakarta melalui tahapan *Information Gathering*, *Network Mapping*, dan *Vulnerability Identification*. Penggunaan perangkat lunak Sudomy berhasil mengumpulkan dan memetakan aset digital instansi, menghasilkan daftar sub-domain beserta alamat IP yang aktif digunakan. penelusuran membuktikan adanya riwayat serangan *web defacement* pada situs tersebut. Hasil identifikasi kerentanan ini menunjukkan bahwa instansi perlu menindaklanjutinya dengan tahapan *Penetration Testing* untuk evaluasi yang lebih mendalam[8].

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif dengan pendekatan pengujian keamanan aplikasi (security testing). Pengujian dilakukan menggunakan standar Open Web Application Security Project Khususnya Owasp Top 10 untuk mengidentifikasi dan menganalisis kerentanan pada aplikasi SIGAP sumsel. data diperoleh melalui observasi, pengujian sistem, dan studi literatur, kemudian dianalisis berdasarkan tingkat risiko serta diberikan rekomendasi perbaikan. Metode OWASP ini berfungsi sebagai panduan standar internasional yang memuat kategori-kategori pengujian keamanan web, meliputi aspek autentikasi, otorisasi, validasi input, konfigurasi server, dan manajemen pembaruan sistem[9].

2.1. Observasi

Observasi merupakan pengamatan secara langsung ke objek penelitian untuk melihat secara detail kegiatan yang dilakukan oleh observee (pihak yang diamati)[10]. Observasi dilakukan melalui pengamatan langsung selama 40

DOI: https://doi.org/10.31004/riggs.v5i2.8553

hari pelaksanaan magang di Kantor Wilayah Kementerian Hukum Sumatera Selatan. Pengamatan difokuskan pada proses operasional aplikasi SIGAP Sumsel, meliputi monitoring alur pendaftaran magang dan penelitian, pengelolaan data sensitif mahasiswa (identitas, KTM, transkrip nilai, dokumen resmi), serta dokumentasi workflow lengkap mulai dari autentikasi pengguna, proses upload dokumen, hingga monitoring status permohonan secara real-time. Data observasi dicatat secara sistematis dalam log harian untuk mengidentifikasi pola penggunaan dan potensi titik lemah keamanan dari perspektif operasional.

2.2. Wawancara

Wawancara struktural dilakukan dengan pengguna akhir aplikasi SIGAP Sumsel, yaitu mahasiswa dan peneliti yang pernah menggunakan sistem untuk pendaftaran magang/penelitian. Wawancara adalah salah satu teknik pengumpulan data dalam penelitian kualitatif yang melibatkan interaksi langsung antara peneliti dan informan, dengan tujuan menggali pandangan, pengalaman, dan pengetahuan para informan secara mendalam[11]. Data wawancara dianalisis untuk melengkapi temuan teknis dari pengujian OWASP dengan perspektif pengguna, termasuk isu usability yang berpotensi memengaruhi kepatuhan keamanan seperti password management dan pengelolaan dokumen sensitif.

2.3. Studi Pustaka

Studi pustaka (*studi literatur*, *literature review*, atau *kajian pustaka*) adalah sebuah proses mencari, membaca, memahami, dan menganalisis berbagai literatur, hasil kajian (hasil penelitian) atau studi[10]. Dalam penelitian ini, studi pustaka digunakan untuk memperoleh landasan teoritis terkait keamanan aplikasi web, metode analisis kerentanan, serta pengujian yang digunakan. Penelitian ini mengacu padda standar yang dikembangkan oleh Open Web Application Security Project, yaitu sebuah organisasi internasional yang berfokus pada peningkatan keamanan perangkat lunak, khususnya aplikasi web. Salah satu panduan utama yang digunakan adalah OWASP Top 10, yang berisi daftar sepuluh kerantanan keamanan paling kritis pada aplikasi web.

3. Hasil dan Diskusi

Open Web Application Security merupakan organisasi internasional non-profit yang berdedikasi dibidang keamanan aplikasi website. OWAPS membuat sebuah website yang gratis dan mudah diakses, sehingga memudahkan pengguna untuk meningkatkan keamanan keamanan website mereka. Pedoman ini berfungsi untuk memberikan panduan kepada pengembang dan profesional keamanan mengenai kerentanan paling kritis yang umum ditemukan pada aplikasi web dan sangat mudah dieksploitasi. Memenuhi standar kepatuhan OWASP secara teoritis merupakan langkah pertama menuju penulisan kode yang aman[12]. OWASP Top 10 adalah daftar 10 standar keamanan website sehingga pengembang dapat memastikan apakah website tersebut aman atau tidak, dengan melakukan checklist berdasarkan standar ini [10], termasuk:

Tabel 1. OWASP Top 10

Code	Vulnerabilities
A01	Broken Access Control
A02	Cryptographic Failures
A03	Injection
A04	Insecure Design
A05	Security Misconfiguration
A06	Vulnerable and Outdated Components
A07	Identification and Authentication Failures
A08	Software and Data Integrity Failures
A09	Security Logging and Monitoring Failures
A10	Server-Side Request Forgery

DOI: https://doi.org/10.31004/riggs.v5i2.8553

a. Broken Access Control
Kerentanan di mana sistem tidak dapat mencegah pengguna yang tidak sah dari mengakses bagian-bagian tertentu dari aplikasi atau data website yang seharusnya tidak mereka akses. Menyebabkan pencurian data atau penggunaan aplikasi website secara tidak sah oleh pihak yang tidak bertanggung jawab

b. Cryptographic Failures
Kesalahan dalam penerapan teknik kriptografi, seperti penggunaan algoritma yang lemah atau pengaturan sandi yang buruk. Membuat data sensitif rentan terhadap pencurian atau dimanipulasi oleh penyerang.

c. Injection
Serangan di mana penyerang menyisipkan kode berbahaya, seperti SQL injection atau XSS, ke dalam input yang dieksekusi oleh aplikasi. Memungkinkan penyerang untuk mengambil alih kontrol atas aplikasi website atau mengakses data sensitive.

d. Insecure Design
Kelemahan yang muncul dari desain yang tidak aman atau rentan terhadap serangan. Dikarenakan keputusan desain yang buruk atau kurangnya pertimbangan keamanan selama proses pengembangan.

e. Security Misconfiguration
Kesalahan konfigurasi yang membuat sistem atau aplikasi website rentan terhadap serangan. Termasuk pengaturan default yang tidak aman, atau kegagalan dalam mengkonfigurasikan sistem keamanan dengan baik.

f. Vulnerable and Outdated Components
Kerentanan yang muncul dari penggunaan komponen atau perangkat lunak yang sudah lama atau rentan terhadap serangan yang diketahui. Termasuk kerentanan pada frameworkyang digunakan oleh aplikasi Website.

g. Identification and Authentication Failures
Kegagalan dalam proses identifikasi dan autotentikasi pengguna. Ini bisa termasuk kegagalan dalam menerapkan autotentikasi dua faktor, penggunaan kata sandi yang buruk, atau kegagalan dalam proses login pengguna.

h. Software and Data Integrity Failures
Kerentanan yang memungkinkan penyerang untuk mengubah atau merusak perangkat lunak atau data yang digunakan oleh aplikasi website. Hal ini dikarenakan kesalahan dalam proses validasi input atau kurangnya perlindungan pada manipulasi data.

i. Security Logging and Monitoring Failures
Kegagalan dalam memantau dan mencatat aktivitas keamanan aplikasi website. Menyebabkan keterlambatan untuk mendeteksi serangan atau kesulitan dalam menelusuri serangan yang terjadi.

j. Server-Side Request Forgery
Serangan di mana penyerang memanipulasi serveruntuk melakukan permintaan ke databaseyang tidak aman atau terlarang. Hal ini digunakan untuk mengakses data sensitif atau menyebabkan kerusakan pada sistem.

3.1. Perencanaan *(Planning)*

Perencanaan keseluruhan proses pemikiran dan penentuan secara matang tentang hal-hal yang akan dikerjakan selanjutnya[13]. Dalam perencanaan analisis kerantanan keamanan pada aplikasi SIGAP Sumsel menggunakan metode OWASP adapun hardware dan sofware yang di gunakan untuk proses pengujian.

DOI: https://doi.org/10.31004/riggs.v5i2.8553

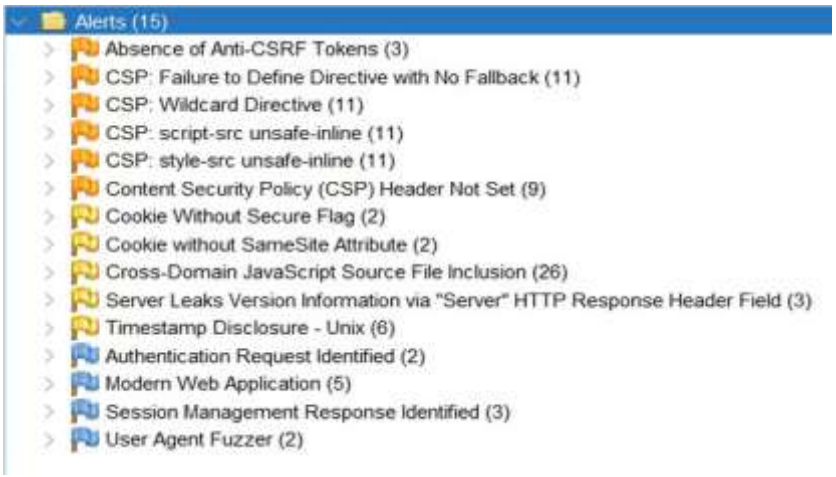
Tabel 2. Alat dan Bahan

Nama Alat dan Bahan	Spesifikasi
LAPTOP	OS: Windows 11 - 64 bit Processor : Intel(R) Core(TM) i3- 1005G1 CPU @ 1.20GHz 1.20 RAM: 12.0 GB (11.7 GB usable), DDR4 SSD 256 GB
OWASP (ZAP)	Version 2.16.1
Web Browser	Google Chrome

Setelah alat dan bahan di penuhi dilakukan analisis terhadap data yang telah dikumpulkan dengan mengacu pada pedoman OWASP TOP 10. OWASP TOP 10 sendiri merupakan panduan yang disusun dan dipublikasikan secara terbuka oleh OWASP, yang bertujuan untuk mengidentifikasi sepuluh jenis kerentanan keamanan paling umum dan sering ditemukan pada aplikasi berbasis web. Pada Tabel 2 disajikan daftar sepuluh kerentanan utama menurut standar OWASP TOP 10 versi terbaru.

3.2. Pemindaian *(Scanning)*

Scanning adalah proses atau tahap pengujian bertujuan untuk mencari celah kerentanan pada website menggunakan tool OWASP ZAP[14]. Lalu pengaturan browser agar terhubung dengan OWASP ZAP menggunakan metode intercepting proxy untuk menghasilkan data penetration testing. Pada Gambar 4 hasil penetration testing yang dilakukan pada aplikasi SIGAP SUMSEL menggunakan fitur pemindaian otomatis aplikasi ZAP.

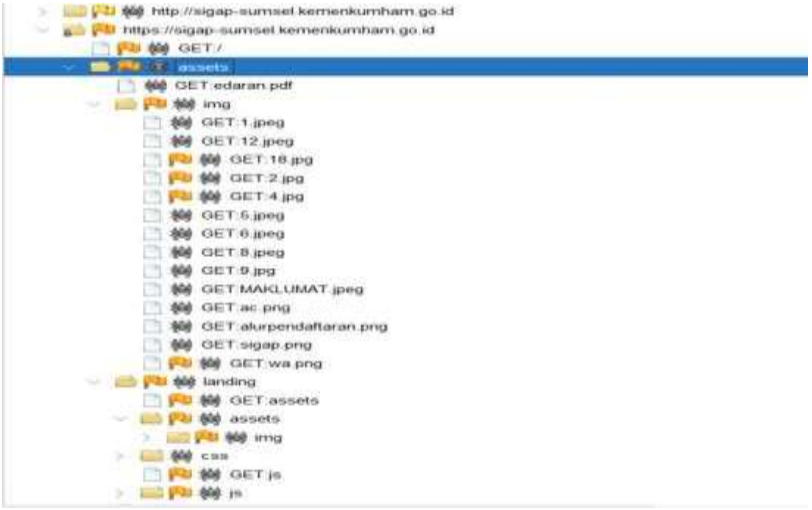


Gambar 1. Penetration testing

3.3 Mendapatkan *(Gaining)*

Setelah melakukan proses scanning beberapa kali maka akan mendapatkan hasil yang sama. Dari pengujian berupa source code yang bisa diakses oleh pelaku siber seperti pada gambar 2 dan 3 sehingga dapat disisipkan source code berbahaya seperti SQL injection.

DOI: https://doi.org/10.31004/riggs.v5i2.8553

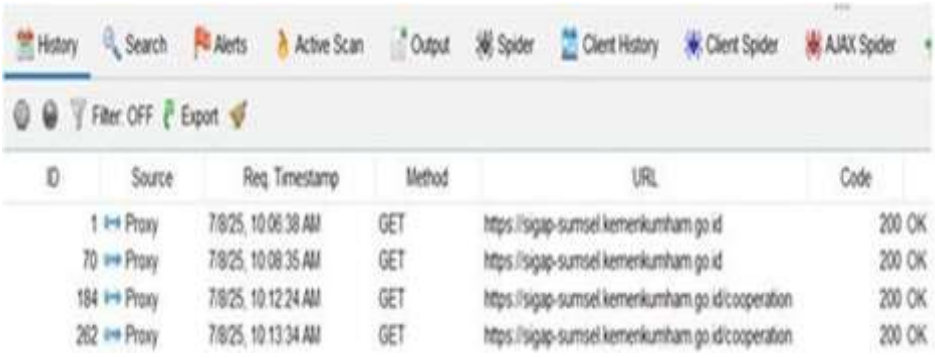


Gambar 2. Data Source code scanning

Gambar 3. Data Source code scanning

3.4 Mempertahankan Akses *(Maintaining Access)*

Proses pengujian apakah hak akses dari serangan sebelumnya dapat tetap terbuka atau tertutup. Maintaining Access, peneliti menguji ulang kerentanan dan mendapatkan akses menggunakan metode intercepting proxy sehingga peneliti dapat memantau aktivitas yang terjadi pada aplikasi SIGAP SUMSEL. Hasil metode intercepting proxy tampil pada gambar 4.

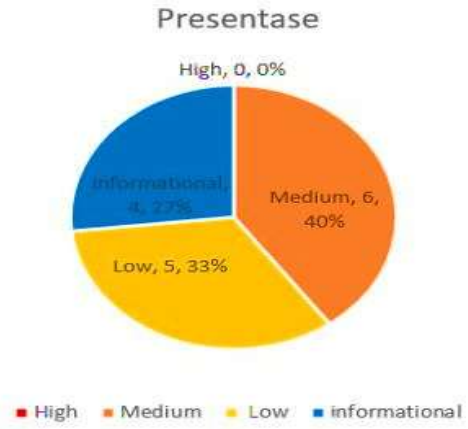


Gambar 4. Metode intercepting proxy

DOI: https://doi.org/10.31004/riggs.v5i2.8553

3.5 Analisis (*Analysis*)

Analisis adalah proses mengatur urutan data, mengorganisasikannya ke dalam suatu pola, kategori, dan satuan uraian dasar[15]. Merangkum hasil dari pengujian penetrasi terdiri dari celah keamanan yang dapat dimanfaatkan, juga data yang dapat dicuri dari sistem. Dengan presentase kerentanan seperti pada gambar 5 dan 6.



Gambar 5. Presentase tingkat risiko keamanan

Tingkat risiko keamanan disimbolkan dengan presentase dan Statistic pada gambar 7 dimana warna merah menandakan risiko tingkat tinggi, warna jingga untuk risiko tingkat sedang, warna kuning untuk risiko tingkat rendah, serta warna biru untuk jenis informasional. Grafik lingkaran yang diberikan mengkategorikan kerentanan yang teridentifikasi ke dalam empat tingkat risiko: Tinggi, Sedang, Rendah, dan Informasional. Setiap segmen grafik tersebut mewakili jumlah persentase dari total kerentanan yang terdeteksi. Berikut penjelasan tingkat resiko berdasarkan hasil grafik tersebut: High adalah cacat keamanan kritis dan berbahaya sehingga dapat dieksploitasi dengan mudah oleh perentas untuk menyebabkan kerusakan signifikan, sehingga dapat menggangu proses pada website menjadi tidak maksimal dan website tersebut menjadi tidak aman. Medium adalah masalah keamanan signifikan sehingga dapat dieksploitasi oleh penyerang untuk mendapatkan beberapa tingkat akses tertentu atau bahkan menyebabkan kerusakan terbatas. Hal ini mungkin memerlukan tingkat keterampilan yang lebih tinggi untuk dapat dieksploitasi oleh perentas dibandingkan dengan kerentanan risiko tinggi. Hal ini menunjukkan bahwa ada kerentanan penting yang perlu diatasi untuk mengurangi ancaman keamanan. Low adalah masalah yang kurang berbahaya yang dapat menimbulkan ancaman lebih rendah terhadap website. Hal ini mungkin lebih sulit untuk dieksploitasi oleh perentas sehingga memiliki dampak yang kurang parah jika dapat dieksploitasi. Informational adalah temuan masalah yang tidak dapat menimbul kanancaman keamanan secara langsung tetapi merupakan hal yang perlu ditingkatkan atau perbaikan.

Gambar 6. Statistic kerantanan keamanan setelah dilakukan Pengujian

Potensial yang dapat meningkatkan keamanan website, Kemudian berdasarkan hasil penetration testing tersebut, keterangan warna berdasarkan jenis tingkat risiko.

DOI: https://doi.org/10.31004/riggs.v5i2.8553

Gambar 7. Summary of alerts by OWASP ZAD

Berdasarkan hasil pengujian keamanan pada aplikasi SIGAP SUMSEL , terdapat 0 kerentanan pada tingkat risiko tinggi atau *high riskl level*, 6 kerentanan pada tingkat risiko sedang atau medium *risk level*, 5 kerentanan pada tingkat risiko rendah atau low *risk level,* dan 4 kerentanan yang bersifat informasional atau *informational risk level*. Kemudian jika dibuat lebih spesifik maka hasil tes kerentanan menggunakan OWASP ZAP seperti yang diperlihatkan pada Tabel 3.

Tabel 3. Specification alerts reports by OWAPS ZAP

Kerentanan yang Ditemukan	Jumlah	Tingkat Risiko
Absence of Anti-CSRF Tokens	3	Sedang
CSP: Failure to Define Directive with No Fallback	11	Sedang
Content Security Policy (CSP) Header Not Set	9	Sedang
Cookie Without SameSite Attribute	2	Rendah
Cross-Domain JavaScript Source File Inclusion	26	Sedang
Server Leaks Version Information via "Server" HTTP Header	3	Rendah
Timestamp Disclosure - Unix	6	Rendah
Authentication Request Identified	2	Sedang
Modern Web Application	5	Rendah
Session Management Response Identified	3	Sedang

4. Kesimpulan

Berdasarkan analisis keamanan aplikasi SIGAP Sumsel menggunakan OWASP Top 10 dan OWASP ZAP, tidak ditemukan kerentanan tingkat tinggi, dengan mayoritas temuan pada kategori sedang dan rendah seperti security misconfiguration (CSP header tidak ada, unsafe-inline JavaScript), authentication failures, serta software integrity issues (cookie tanpa Secure/SameSite, kebocoran server info). Aplikasi memiliki tingkat keamanan cukup baik namun memerlukan perbaikan konfigurasi untuk standar modern. Disarankan pengelola sistem menerapkan CSP header, atribut cookie Secure/SameSite, validasi skrip eksternal, dan sembunyikan metadata sensitif; lakukan evaluasi berkala via penetration testing serta perkuat logging/monitoring untuk deteksi dini ancaman, meningkatkan kepercayaan pengguna dan perlindungan data optimal.

Referensi

[1] E. Yanti, D. Anwar, S. Asrol, P. Perbankan, S. Uin, and R. F. Palembang, "PENGARUH PENGALAMAN MAGANG, SOFT SKILL DAN HARD SKILL TERHADAP KESIAPAN KERJA MAHASISWA PERBANKAN SYARIAH UIN RADEN FATAH PALEMBANG," 2025. [Online]. Available: https://ejournal.uniled.ac.id/index.php/Uniled-Ekonomia

[2] M. Amirul Mu'min, N. Tristanti, G. Pramuja, and I. Fanani, "Analisis dan Pengujian Kerentanan Website Menggunakan OWASP ZAP," *Jurnal Riset Sistem dan Teknologi Informasi (RESTIA*, vol. 3, no. 1, pp. 36–50, 2024.

[3] E. Nurelasari, D. Gumilang, and A. Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP.ID," 2024.

[4] H. Hermanto and H. Haeruddin, "Peningkatan Sistem Keamanan Website Menggunakan Metode OWASP," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 94–104, May 2022, doi: 10.47927/jikb.v13i1.277.

DOI: https://doi.org/10.31004/riggs.v5i2.8553

[5] H. Pahlawansah, Muh. F. Basmar, and M. Yusuf, "Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project)," *BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer*, vol. 6, no. 2, pp. 92–100, Sep. 2025, doi: 10.37148/bios.v6i2.180.
[6] D. Wijayanto and A. Firdonsyah, "Analisis Tingkat Resiko Pada Website Xyz Menggunakan Metode Owasp," *Digital Transformation Technology*, vol. 4, no. 1, pp. 644–651, Aug. 2024, doi: 10.47709/digitech.v4i1.4485.
[7] ADI WIJAYA, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," 2024.
[8] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 5, no. 1, pp. 35–42, Jul. 2021, doi: 10.31603/komtika.v5i1.5134.
[9] O. P. Agung, F. M. Faizal, I. Mascharenhas, S. Informasi, U. Pamulang, and T. Selatan, "Jurnal Riset Multidisiplin Edukasi Analisis Keamanan Sistem Informasi Website Pemerintah Menggunakan Metode OWASP WSTG (Study Kasus: Deface Situs Kemendagri)," 2025. [Online]. Available: https://journal.hasbaedukasi.co.id/index.php/jurmie
[10] S. Pt. , M. Pd. , M. S. Ns. I. L. M. S. Kep. M. Kep. Ns. E. F. S. Kep. M. | Dr. A. B. S. P. S. K. M. Kes. F. R. P. S. K. Ns. , M. K. Dr. Amruddin, "METODOLOGI PENELITIAN KUANTITATIF DAN KUALITATIF," 2022. [Online]. Available: www.medsan.co.id
[11] B. Arianto, M. Ak, and A. Rani, "TEKNIK WAWANCARA DALAM METODA PENELITIAN KUALITATIF," 2024.
[12] Abhishek Kashniyal, "OWASP TOP 10 VULNERABILITIES," 2019.
[13] H. Setiadi and S. Si, "Dasar-dasar Teori Perencanaan."
[14] Yunanri. W, "Analisis Keamanan Pada Web Aplikasi Open Journal System Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Metode Vulnerability Assessment," *Digital Transformation Technology*, vol. 3, no. 1, pp. 83–90, Jul. 2023, doi: 10.47709/digitech.v3i1.2476.
[15] Y. R. A. S. R. N. Dewi Kurniasih, "Teknik Analisa," 2021. [Online]. Available: www.cvalfabeta.com

DOI: https://doi.org/10.31004/riggs.v5i2.8553