e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 8 No. 1, Juni, 2024, **Hal. 113-122**
DOI: 10.29408/edumatic.v8i1.25463

Evaluasi Risiko Celah Keamanan Aplikasi E-Office menggunakan Metode OWASP

Tata Sutabri [1], Adi Wijaya [1,*], Muhammad Izman Herdiansyah [1], Edi Surya Negara [1]

[1] Program Studi Teknik Informatika, Universitas Bina Darma, Indonesia
[*] Correspondence: adiw1201@gmail.com

Received: 7 Maret 2024 | Revised: 17 Maret 2024 | Accepted: 24 April 2024 | Published: 20 Juni 2024

Abstrak
Berdasarkan data Badan Siber dan Sandi Negara (BSSN) pada tahun 2022 disebutkan bahwa ditemukan sebanyak 1.950 celah keamanan dari 457 sistem elektronik pada berbagai aplikasi yang digunakan oleh masyarakat secara luas. Tujuan Penelitian adalah untuk melakukan evaluasi risiko celah keamanan yang terdapat pada aplikasi E-Office Kabupaten Ogan Ilir agar supaya diketahui tingkat dan dampak yang dapat ditimbulkan oleh celah keamanan tersebut. Peneltian ini merupakan penelitan keamanan sistem informasi yang berfokus pada evaluasi risiko celah keamanan pada aplikasi E-Office Kabupaten Ogan Ilir. Penelitian dilakukan dengan menggunakan metode *Open Web Application Security Project* (OWASP) dengan penilaian *Risk Rating* dengan tahapan penelitian dimulai dari studi literatur dalam mencari sumber data dan informasi, menentukan ruang lingkup dan objek penelitian, pengujian, identifikasi celah keamanan, analisis celah keamanan, dan hasil analisis. Subjek penelitian adalah aplikasi E-Office Kabupaten Ogan Ilir dengan objek penelitian adalah celah keamanan yang terdapat pada aplikasi tersebut. OWASPZap digunakan sebagai alat untuk memperoleh data celah keamanan, dan dengan menggunakan OWASPZap ditemukan 38 celah keamanan dengan 18 diantara celah keamanan tersebut masuk dalam kriteria *OWASP Top 10*. Hasil temuan kami menunjukkan bahwa celah keamanan dalam aplikasi E-Office Kabupaten Ogan Ilir meliputi kerentanan pada tingkat otentifikasi, akses kontrol, konfigurasi, serta proses validasi data.

Kata kunci: e-office; owasp; celah keamanan; evaluasi; risiko

Abstract
Based on data from Badan Siber dan Sandi Negara (BSSN) in 2022, it was reported that a total of 1,950 security vulnerabilities were found in 457 electronic systems across various applications widely used by the public. The purpose of this research is to evaluate the risk of existing security vulnerabilities in the E-Office application and determine the level and impact that these vulnerabilities can cause. This research focuses on information system security, specifically evaluating the risk of security vulnerabilities in the E-Office application of the Ogan Ilir Regency. The research was conducted using the Open Web Application Security Project (OWASP) method with a risk rating assessment. The research process began with a literature review to gather data and information sources, determine the scope and research objectives, test, identify security vulnerabilities, analyze security vulnerabilities, and the results of the analysis. The research subject is the E-Office application of Ogan Ilir Regency, with the object of the research being the security vulnerabilities in that application. OWASPZap was used as a tool to obtain data on security vulnerabilities, and using OWASPZap, 38 security vulnerabilities were found, with 18 of them meeting the criteria of the OWASP Top 10. Our findings indicate that the security vulnerabilities in the E-Office application of Ogan Ilir Regency include vulnerabilities in authentication levels, access control, configuration, and data validation processes.

Keywords: *e-office; owasp; vulnerability; evaluation; risk*

PENDAHULUAN

Suatu sistem dapat didefenisikan sebagai suatu kesatuan yang terdiri dari dua atau lebih komponen atau subsistem yang berinteraksi untuk mencapai suatu tujuan (Rochaety, 2017). Sistem dalam organisasi memiliki sejumlah komponen (manusia, komputer, teknologi informasi, dan alur kerja), memiliki sesuatu yang diproses (data menjadi informasi), untuk mencapai tujuan dan sasaran (Andhika, 2021). Sehingga disimpulkan bahwa sistem informasi mencakup sejumlah komponen (manusia, komputer, teknologi informasi, dan prosedur kerja), ada sesuatu yang diproses (data menjadi informasi), dan dimaksudkan untuk mencapai suatu sasaran atau tujuan (Kadir, 2018). Dengan semakin berkembangnya teknologi sistem informasi tentunya akan diiringi pula dengan semakin tingginya risiko keamanan yang akan dihadapi. Ancaman terhadap sistem informasi terbagi menjadi dua jenis ancaman yaitu ancaman aktif (mencuri informasi, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi data) dan ancaman pasif (kesalahan sistem, kesalahan manusia, bencana alam) (Gustian, 2023).

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyebutkan dari hasil survei yang mereka buat bahwa pada periode tahun 2022-2023 pengguna internet di Indonesia mencapai 215,63 juta orang (Sadya, 2023). BSSN melalui "Lanskap Keamanan Siber Indonesia 2022" menyebutkan bahwa berdasarkan hasil *assessment* yang dilakukan pada tahun 2022 ditemukan sebanyak 1.950 celah keamanan dari 457 sistem elektronik pada berbagai aplikasi yang digunakan oleh masyarakat secara luas (Yusuf et al., 2022).

Di era digitalisasi pemerintahan saat ini tentunya penggunaan aplikasi E-Office telah menjadi kebutuhan dalam meningkatkan efisiensi serta efektivitas dalam proses layanan administrasi publik, namun aplikasi E-Office juga memiliki risiko keamanan yang perlu dievaluasi secara menyeluruh seperti peretasan akun pegawai, pencurian data informasi kepegawaian, dan data penting lainnya milik Pemerintah Kabupaten Ogan Ilir yang bukan untuk konsumsi publik. Didalam penggunaannya, Kabupaten Ogan Ilir tentunya menghadapi tantangan dalam memastikan keamanan aplikasi E-Office tersebut. Oleh karena itu, perlu dilakukan evaluasi terhadap risiko celah keamanan yang mungkin terdapat dalam aplikasi E-Office tersebut.

Keamanan sistem informasi adalah upaya untuk menghindari kejadian yang tidak diinginkan seperti hilangya kerahasiaan atau integritas data. Jika aset teknologi informasi mendapat ancaman dan serangan baik dari dalam maupun dari luar maka dapat menimbulkan risiko yang mengganggu dalam proses bisnis bahkan juga dapat menghentikan proses bisnis (Candra et al., 2019). Indikator keamanan informasi berbasis internet menjadi suatu keharusan untuk diperhatikan karena jaringan komputer internet bersifat publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lain di dalam internet, data ini akan melewati sejumlah komputer lain yang bisa memberi kesempatan kepada pengguna internet lain untuk menyadap atau mengubah data tersebut (Nurul et al., 2022). Salah satu bentuk pengendalian internal dalam mengantisipasi kemungkinan tersebut adalah dengan melakukan *risk assessment* (penilaian risiko). Dengan melakukan *risk assessment* organisasi atau perusahaan harus mengidentifikasi dan menganalisis serta mengevaluasi faktor-faktor yang menciptakan risiko dan harus menentukan bagaimana caranya mengelola risiko tersebut (Sayuthi, 2021). Setelah tingkat risiko *(risk severity*) telah ditentukan maka organisasi dapat menentukan daftar prioritas apa yang harus diperbaiki terlebih dahulu.

Penelitian yang dilakukan oleh (Ghozali et al., 2019) dalam mendeteksi kerentanan keamanan aplikasi website sistem informasi harga komoditas utama yang dibangun oleh PT. Gitsolution dengan metode OWASP serta menggunakan aplikasi Acunetix untuk mendeteksi celah keamanan yang ada. Dari hasil pengujiannya dinemukan 12 celah keamanan dengan 7 celah keamanan memiliki *risk severity high*, 3 celah keamanan *risk severity medium* dan 2 celah

keamanan *risk severity low*. Penelitian lain yang dilakukan oleh (Aryanti et al., 2021) menggunakan *tools Acunetix Web Vulnerability Scanner* dalam mengidentifikasi celah keamanan, ditemukan 7 celah keamanan dengan 3 celah keamanan memiliki *risk severity high*, 2 celah keamanan *risk severity medium* dan 2 celah keamanan *risk severity low*. Namun penelitian yang dilakukan oleh (Ghozali et al., 2019) serta (Aryanti et al., 2021) hanya sebatas penilaian tingkat risiko keparahan (*risk severity*) tanpa menggambarkan dampak serta rekomendasi perbaikan dari celah keamanan yang ditemukan, sehingga dalam penelitian ini juga akan memberikan kemungkinan dampak risiko yang ditimbulkan dan juga rekomendasi perbaikan dari tiap celah keamanan yang ada.

Tujuan dari penelitian ini adalah untuk mengevaluasi risiko celah keamanan yang ditemukan serta memberikan rekomendasi perbaikan untuk mengurangi risiko celah keamanan yang ditemukan guna meningkatkan keamanan aplikasi E-Office Kabupaten Ogan Ilir. Sehingga dengan dilakukan evaluasi ini dapat memberikan tingkat keamanan dalam melakukan aktifitas dengan menggunakan aplikasi E-Office Kabupaten Ogan Ilir.

METODE

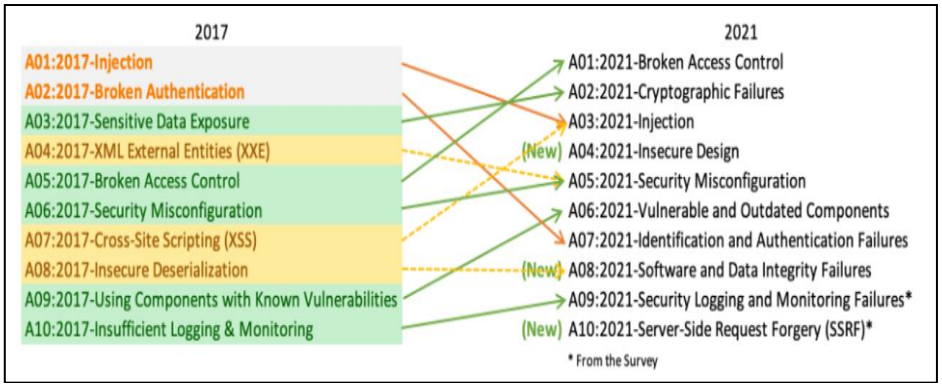
Metode OWASP dengan penilaian *Risk Rating* merupakan suatu pendekatan sederhana yang digunakan dalam menghitung serta menilai risiko celah keamanan. Dengan penilaian *Risk Rating* dapat membantu dalam menentukan tingkat risiko keparahan (risk serverity) yang ditemukan dalam aplikasi. Tahapan-tahapan penelitian yang dilakukan dimulai dari studi literatur, menentukan ruang lingkup dan objek penelitian, pengujian, identifikasi celah keamanan, serta analis dan penilaian terhadap celah keamanan.

Tahapan awal yang dilakukan dalam proses penelitian adalah dengan melakukan studi literatur yaitu mencari sumber data dan informasi yang sesuai dan relevan terhadap penelitian yang diperoleh, baik itu dari buku, jurnal publikasi, wawancara atau lainnya sebagai bahan penelitian. Dari data yang terkumpul tadi untuk selanjutnya menentukan ruang lingkup dan objek penelitian yaitu aplikasi E-Office Kabupaten Ogan ilir (Alamat URL (*Uniform Resource Locator*): https://e-office.oganilirkab.go.id/, IP (*Internet Protocol*): 103.162.35.77, *Web Server*: *Apache*, Bahasa Pemograman: PHP, Database MySQL). Kemudian dilanjutkan dengan proses pengujian untuk menemukan celah keamanan yang merupakan proses dari investigasi dari segi teknik untuk menyatakan kualitas aplikasi yang dikembangkan.

Proses pengujian dilakukan dengan menggunakan bantuan *tool* OWASPZap dengan satu metode yaitu *manual explore*. Pada proses *manual explore* dengan menggunakan OWASPZap, pengguna terlebih dahulu mengatur konfigurasi dan menentukan alamat atau *URL* aplikasi *web* yang akan di uji. Selama proses *manual explore* dijalankan, pengguna akan secara manual berinteraksi dengan aplikasi melalui peramban (*browser*) yang dipilih, baik itu melakukan input data, memiih tautan atau menjalankan perintah-perintah lainnya yang disediakan oleh aplikasi yang di uji tersebut. Selama proses atau aktivitas berlangsung, OWASPZap akan merekam dan menganalisis proses yang berlangsung guna mengidentifikasi celah keamanan yang ada. OWASPZap kemudian menghasilan report atau laporan yang berisikan daftar kerentanan yang ditemukan.

Kerentanan yang ditemukan tadi untuk selanjutnya diidentifikasi berdasarkan pendekatan *OWASP Top 10*. *OWASP Top 10* sendiri merupakan sebuah panduan bagi para *developers* dan *security team* untuk mengetahui informasi tentang kelemahan-kelemahan yang terdapat pada *web apps* yang paling sering diserang. Setiap kerentanan yang teridentifikasi atau ditemukan akan dinilai risiko dan keparahannya serta faktor-faktor lain seperti dampak potensial dan kemungkinan untuk di eksploitasi. Secara umum, berdasarkan dari hasil identifikasi celah keamanan yang ditemukan akan dinilai faktor *likelihood* untuk mengukur seberapa besar kemungkinan celah keamanan dapat di eksploitasi serta faktor i*mpact* untuk mengukur seberapa besar dampak yang ditimbulkan dari celah keamanan tersebut sehingga

dapat ditentukan risk severity dari masing-masing celah keamanan apakah berada pada level *risk severity high*, *risk severity medium* atau *risk severity low*.Untuk selanjutnya hasil yang diperoleh akan dijadikan rekomendasi dalam rangka antisipasi dan meningkatkan keamanan aplikasi.



Gambar 1. 10 Kerentanan keamanan aplikasi web tertinggi berdasarkan *owasp top 10*

Melakukan penilaian terhadap risiko celah keamanan, OWASP memberikan penilaian dengan pendekatan model risiko standar (*standard risk model*) yaitu:

Risk = Likelihood * Impact

Risk: Penilaian tingkat risiko yang terkait dengan faktor ancaman dan kerentanan (*likelihood*), serta dampak teknis dan bisnis yang ditimbulkan (*impact*); *Likelihood*: Kemungkinan kerentanan untuk dieksploitasi oleh penyerang (*threat agent factors, vulnerability factors); Impact*: Dampak yang ditimbulkan dari serangan tersebut (*technical impact factors, business impact factors).* Selanjutnya untuk perhitungan *likelihood* dan *impact factors* yang dapat dilihat pada persamaan 1.

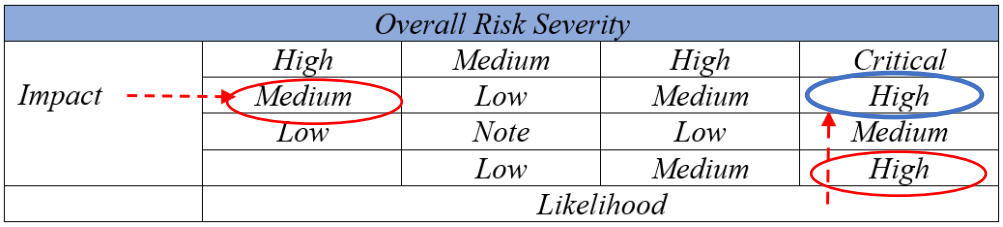
$$\bar{\chi} = \frac{\sum \chi}{n} \quad (1)$$

Keterangan:
$\bar{\chi}$= nilai rata-rata hitung, $\sum \chi$= nilai sampel (skor penilaian), n= jumlah sampel.

Tiap-tiap faktor *likelihood* dan *impact* dinilai, kemudian akan ditentukan skala level secara keseluruhan. Skala 0 sampai 9 dibagi menjadi tiga bagian seperti pada gambar 2. Setelah level untuk masing-masing faktor (*likelihood* dan *impact)* diperoleh, maka data keduanya digabungkan untuk mendapatkan tingkat risiko dari celah keamanan yang ditemukan. Seperti yang terlihat pada gambar 3, ketika faktor *likelihood* pada level *high* dan *impact* pada level *medium* maka setelah digabungkan perkiraan tingkat risiko (*risk severity*) berada pada level *high*.

Likelihood and Impact Levels	
0 to < 3	low
3 to < 6	medium
6 to 9	high

Gambar 2. Skala penilaian *likelihood and impact levels*



Gambar 3. Skala penentuan tingkat risiko keamanan

HASIL DAN PEMBAHASAN

Hasil

Berdasarkan hasil pengujian dengan menggunakan *OWASPZap*, ditemukan 38 celah keamanan yang terdapat pada aplikasi E-Office Kabupaten Ogan Ilir dengan 18 diantaranya masuk dalam kriteria *OWASP Top 10*. Selanjutnya 18 celah keamanan yang masuk dalam kriteria *OWASP Top 10* tersebut akan dinilai berdasarkan faktor-faktor yang telah ditentukan untuk mengetahui tingkat risikonyo (*Risk Severity*).

Tabel 1. Skor penilaian *threat agent factors* dan *vulnerability factors*

Celah Keamanan	**TAF**				***VF***			
	SL	***M***	***O***	***S***	***ED***	***EE***	***A***	***ID***
Absence of Anti-CSRF Tokens	9	9	7	6	7	5	9	3
Cross-Domain Misconfiguration	9	9	9	6	7	5	9	3
Cookie without SameSite Attribute	9	9	9	6	7	5	9	3
Information Disclosure - Debug Error Messages	6	4	9	2	7	5	9	9
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	6	4	9	9	7	3	9	9
Timestamp Disclosure - Unix	6	4	9	9	3	3	1	9
Information Disclosure - Suspicious Comments	6	4	9	2	7	3	6	9
Information Disclosure - Sensitive Information in URL	6	4	9	9	7	3	1	9
User Controllable HTML Element Attribute (Potential XSS)	9	9	9	6	7	5	1	9
User Controllable JavaScript Event (XSS)	9	9	9	6	7	5	1	9
PII Disclosure	6	4	9	6	7	5	9	3
Application Error Disclosure	6	4	9	6	7	5	9	3
Cookie Without Secure Flag	9	9	7	6	7	5	9	3
X-Content-Type-Options Header Missing	9	9	9	6	7	5	9	9
Cookie No HttpOnly Flag	6	4	7	6	7	5	9	3
X-AspNet-Version Response Header	6	4	9	9	7	3	4	9
Vulnerable JS Library	9	9	9	6	7	5	9	3
Cross-Domain JavaScript Source File Inclusion	9	9	7	6	3	5	4	3

Adapun kriteria serta nilai skor yang ditentukan dalam menentukan penilaian pada tabel.1 terdiri dari *Threat Agent Factors (TAF)* yaitu *Skill Level (SL) - network and programming skills (6), security penetration skills (9), Motive (M) - possible reward (4), high reward (9), Opportunity (O) - some access or resources required (7), no access or resources required (9), Size (S) - developers (2), system administrators (2), authenticated users (6), anonymous Internet users (9),* serta *Vulnerability Factors (VF)* yaitu *Ease of Discovery (ED) - difficult (3), easy (7), Ease of Exploit (EE) - difficult (3), easy (5), Awareness (A) - Unknown (1), hidden*

(4), obvious (6), public knowledge (9), Intrusion Detection (ID) - logged and reviewed (3), not logged (9).

Tabel 2. Skor penilaian *technical impact factors* dan *business impact factors*

	TIF				***BIF***			
Celah Keamanan	***LC***	***LI***	***LA***	***LAc***	***FD***	***RD***	***N***	***PV***
Absence of Anti-CSRF Tokens	2	7	9	9	1	1	2	7
Cross-Domain Misconfiguration	7	9	9	9	1	1	2	7
Cookie without SameSite Attribute	2	1	3	7	1	1	2	7
Information Disclosure - Debug Error Messages	6	1	1	7	1	1	2	7
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	2	1	1	7	1	1	2	7
Timestamp Disclosure - Unix	2	1	1	7	1	1	2	7
Information Disclosure - Suspicious Comments	2	1	1	7	1	1	2	7
Information Disclosure - Sensitive Information in URL	6	1	1	7	1	1	2	7
User Controllable HTML Element Attribute (Potential XSS)	6	7	1	7	1	1	2	7
User Controllable JavaScript Event (XSS)	7	9	5	7	1	1	2	7
PII Disclosure	7	9	5	1	1	1	2	7
Application Error Disclosure	2	1	1	1	1	1	2	7
Cookie Without Secure Flag	2	1	1	7	1	1	2	7
X-Content-Type-Options Header Missing	2	1	1	7	1	1	2	7
Cookie No HttpOnly Flag	2	1	1	1	1	1	2	7
X-AspNet-Version Response Header	2	1	1	9	1	1	2	7
Vulnerable JS Library	6	7	1	7	1	1	2	7
Cross-Domain JavaScript Source File Inclusion	7	9	7	9	1	1	2	7

Kriteria serta nilai skor yang ditentukan dalam menentukan penilaian pada tabel. 2 terdiri dari *Technical Impact Factors (TIF)* yaitu *Loss of Confidentiality (LC) - Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), Loss of Integrity (LI) - Minimal slightly corrupt data (1), extensive seriously corrupt data (7), all data totally corrupt (9), Loss of Availability (LA) - Minimal secondary services interrupted (1), minimal primary services interrupted (3), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9), Loss of Accountability (LAc) - Fully traceable (1), possibly traceable (7), completely anonymous (9)*, serta *Business Impact Factors (BIF)* yaitu *Financial Damage (FD) - Less than the cost to fix the vulnerability (1), Reputation Damage (RD) - Minimal damage (1), Non-compliance (N) - Minor violation (2), Privacy Violation (PV) - thousands of people (7).*

Setelah masing-masing faktor pada tabel 1 dan tabel 2 dinilai maka dari hasil dari penilaian tersebut akan digunakan dalam menentukan skala levelnya (*likelihood dan impact levels*) seperti terlihat pada tabel 3. Hasil dari penilaian skala level *likelihood* dan *impact factors* pada tabel 3 inilah yang selanjutnya di jadikan sebagai dasar dalam menentukan tingkat risiko (*risk severity*) dari celah keamanan yang ditemukan (tabel 4) dengan metode penilaian seperti pada gambar 3.

Tabel 3. *Factors for estimating likelihood (lk) and impact (im)*

Celah Keamanan	LK		Overall	Lv	IM		Overall	LV
	TAF	VF			TIF	BIF		
Absence of Anti-CSRF Tokens	7,75	6	6,875	*H*	6,75	2,75	4,75	*M*
Cross-Domain Misconfiguration	8,25	6	7,125	*H*	8,5	2,75	5,625	*M*
Cookie without SameSite Attribute	8,25	6	7,125	*H*	3,25	2,75	3	*M*
Information Disclosure - Debug Error Messages	5,25	7,5	6,375	*H*	3,75	2,75	3,25	*M*
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	7	7	7	*H*	2,75	2,75	2,75	*L*
Timestamp Disclosure - Unix	7	4	5,5	*M*	2,75	2,75	2,75	*L*
Information Disclosure - Suspicious Comments	5,25	6,25	5,75	*M*	2,75	2,75	2,75	*L*
Information Disclosure - Sensitive Information in URL	7	5	6	*H*	3,75	2,75	3,25	*M*
User Controllable HTML Element Attribute (Potential XSS)	8,25	5,5	6,875	*H*	5,25	2,75	4	*M*
User Controllable JavaScript Event (XSS)	8,25	5,5	6,875	*H*	7	2,75	4,875	*M*
PII Disclosure	6,25	6	6,125	*H*	5,5	2,75	4,125	*M*
Application Error Disclosure	6,25	6	6,125	*H*	1,25	2,75	2	*L*
Cookie Without Secure Flag	7,75	6	6,875	*H*	2,75	2,75	2,75	*L*
X-Content-Type-Options Header Missing	8,25	7,5	7,875	*H*	2,75	2,75	2,75	*L*
Cookie No HttpOnly Flag	5,75	6	5,875	*M*	1,25	2,75	2	*L*
X-AspNet-Version Response Header	7	5,75	6,375	*H*	3,25	2,75	3	*M*
Vulnerable JS Library	8,25	6	7,125	*H*	5,25	2,75	4	*M*
Cross-Domain JavaScript Source File Inclusion	7,75	3,75	5,75	*M*	8	2,75	5,375	*M*

Tabel 4. Tingkat risiko celah keamanan (*risk severity*)

Celah Keamanan	LK	IM	RS
Absence of Anti-CSRF Tokens	*H*	*M*	*High*
Cross-Domain Misconfiguration	*H*	*M*	*High*
Cookie without SameSite Attribute	*H*	*M*	*High*
Information Disclosure - Debug Error Messages	*H*	*M*	*High*
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	*H*	*L*	*Medium*
Timestamp Disclosure - Unix	*M*	*L*	*Low*
Information Disclosure - Suspicious Comments	*M*	*L*	*Low*
Information Disclosure - Sensitive Information in URL	*H*	*M*	*High*
User Controllable HTML Element Attribute (Potential XSS)	*H*	*M*	*High*
User Controllable JavaScript Event (XSS)	*H*	*M*	*High*
PII Disclosure	*H*	*M*	*High*
Application Error Disclosure	*H*	*L*	*Medium*
Cookie Without Secure Flag	*H*	*L*	*Medium*
X-Content-Type-Options Header Missing	*H*	*L*	*Medium*
Cookie No HttpOnly Flag	*M*	*L*	*Low*
X-AspNet-Version Response Header	*H*	*M*	*High*
Vulnerable JS Library	*H*	*M*	*High*
Cross-Domain JavaScript Source File Inclusion	*M*	*M*	*Medium*

Pada tabel 4 menunjukkan bahwa dari 18 celah keamanan yang masuk kriteria *OWASP Top 10* diketahui bahwa terdapat 10 (sepuluh) risiko celah keamanan dengan kategori *Risk Severity High*, 5 (lima) risiko celah keamanan dengan kategori *Risk Serverity Medium*, dan 3 (tiga) risiko celah keamanan dengan kategori *Risk Severity Low*.

Pembahasan

Berdasarkan kriteria yang terdapat pada OWASP Top 10, celah keamanan yang ditemukan akan dinilai dampak atau risiko serta dengan memberikan rekomendasi perbaikan yang harus dilakukan untuk mencegah kemungkinan kerusakan yang dapat ditimbulkan. *OWASP_2021_A01, Broken Access Control*; meliputi 8 celah keamanan yaitu *Absence of Anti-CSRF Tokens, Cross-Domain Misconfiguration, Cookie without SameSite Attribute, Information Disclosure - Debug Error Messages, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Timestamp Disclosure – Unix, Information Disclosure - Suspicious Comments, Information Disclosure- Sensitive Information in URL*. Dampak atau risiko yang ditimbulkan yaitu pengguna dapat mengakses ke data yang seharusnya tidak mereka lihat, mengedit data yang seharusnya hanya dapat diakses oleh orang lain, atau melakukan tindakan yang seharusnya hanya diizinkan untuk pengguna tertentu. Rekomendasi perbaikan adalah dengan menggunakan autentikasi dan otorisasi yang kuat, menerapkan kontrol akses berbasis peran (*Role-Based Access Control*) dan kendalikan akses dengan ketat, menerapkan validasi input pengguna sesuai hak aksesnya, serta memindahkan id query ke post body atau tempat lainnya dengan juga memanipulasi pemanggilan id nya.

OWASP_2021_A03, Injection; meliputi 2 celah keamanan yaitu *User Controllable HTML Element Attribute (Potential XSS), User Controllable JavaScript Event (XSS)*. Risiko yang ditimbulkan yaitu penyerang dapat menyisipkan skript berbahaya yang dapat mencuri informasi pengguna serta dapat menyusupkan iklan atau konten *phishing* ke dalam halaman web. Rekomendasi perbaikan adalah dengan melakukan validasi data input dari pengguna serta menggunakan koneksi *HTTPS* yang aman.

OWASP_2021_A04, Insecure Design; nama celah keamanan *PII (Personally Identifiable Information) Disclosure*. Dapat menyebabkan password yang disimpan pada database menjadi kurang aman karena memungkinkan penyerang untuk dapat melakukan dekripsi terhadap *hash* tersebut. Sehingga apabila berhasil, maka penyerang akan mendapatkan password akun pengguna dan terjadi pengambilalihan akun. Rekomendasi perbaikan adalah dengan menggunakan algoritma *hash* yang memadai untuk melakukan *hashing password* akun pengguna, misalnya *Bcrypt*.

OWASP_2021_A05, Security Misconfiguration; meliputi 5 celah keamanan yaitu *Application Error Disclosure, Cookie Without Secure Flag, X-Content-Type-Options Header Missing, Cookie No HttpOnly Flag, X-AspNet-Version Response Header*. Risiko yang ditimbulkan yaitu aplikasi menjadi lebih rentan terhadap serangan dasar dan serangan yang belum diketahui (*zero day attack*) akibat kurangnya perlindungan standar yang diperlukan dan bisa mengungkapkan informasi rahasia atau hingga pengambilan alih akun dari pengguna. Pada penelitian sebelumnya oleh (Ghozali et al., 2019) juga menemukan kerentanan yang masuk dalam kriteria *OWASP_2021_A05* dengan celah keamanan yang berbeda yaitu *Directoy Listing, Session Cookie Without HttpOnly Flag Set* dan *Slow Response Time*. Rekomendasi perbaikan adalah dengan menambahkan beberapa jenis konfigurasi atau pengaturan keamanan pada security headers sesuai kebutuhan aplikasi serta menggunakan WAF untuk memblokir iframes berbahaya dengan efektif.

OWASP_2021_A06, (Vulnerable and Outdated Components); nama celah keamanan *Vulnerable JS Library*. Penyerang dapat memanfaatkan kerentanan yang diketahui dalam versi komponen perpustakaan JavaScript yang sudah usang untuk meretas sistem, mencuri data rahasia, atau bahkan mengganggu operasional keseluruhan sistem. Rekomendasi perbaikan

adalah dengan melakukan pembaruan perpustakaan JavaScript secara teratur dengan versi terbaru. Pada penelitian yang dilakukan oleh (Ghozali et al., 2019) sebelumnya tidak ditemukan kerentanan yang masuk dalam kategori *OWASP_2021_A06* ataupun kerentanan yang berhubungan dengan perpustakaan *javascript*.

OWASP_2021_A08, Software and Data Integrity Failures; nama celah keamanan *Cross-Domain JavaScript Source File Inclusion*. Penyerang dapat menyisipkan skrip *JavaScript* yang berbahaya dari domain yang tidak dapat dipercaya yang dapat dieksekusi oleh browser pengguna, serangan *Cross-Site Scripting (XSS)* serta pencurian informasi pengguna. Serangan *Cross-Site Scripting* juga merupakan jenis ancaman yang ditemukan pula penelitian sebelumnya oleh (Ghozali et al., 2019) dan (Aryanti et al., 2021). Rekomendasi perbaikan adalah dengan melakukan proses validasi dan bersihkan input yang diterima dari pengguna untuk mencegah penyisipan skrip yang tidak aman dan memastikan perangkat lunak dan framework yang digunakan untuk membangun aplikasi selalu diperbarui dengan versi terbaru.

SIMPULAN

Hasil penelitian yang dilakukan dengan metode OWASP menunjukan bahwa terdapat 18 celah keamanan yang dapat dieksploitasi yang meliputi kerentanan pada tingkat otentifikasi, akses kontrol, konfigurasi serta pada input data yang tidak terfilter dengan baik, untuk itu perlu dilakukan perbaikan yang mencakup peningkatan kontrol akses, pembaruan sistem otentikasi, pembaruan perangkat lunak, konfigurasi pada sistem serta penerapan filterisasi data yang lebih tepat. Secara keseluruhan, penelitian ini diharapkan mampu memberikan kontribusi yang signifikan dalam meningkatkan keamanan aplikasi E-Office Kabupaten Ogan Ilir.

REFERENSI

Abdurrohim, I. (2019). Penetration Testing Sistem Keamanan Aplikasi Web Berbasis e-Commerce Pada Perusahaan Hptasik. *Jurnal Ilmu Komputer*, *1*, 125–131.

Andhika, D. A. (2021). Pengujian Ketahanan Website Menggunakan Model Penetration Testing Execution Standard (PTES). *Journal of Technology and Informatics Universitas Dinamika*, *3*, 55–61. https://doi.org/https://doi.org/10.37802/joti.v3i2.222

Ardiyasa, I. W., & Ndok, Theresia, A. (2023). Penetration Testing Keamanan Sistem Informasi Berbasis Web dengan Metode OSSTMM. *Seminar Nasional Corisindo*, 348–353.

Aryanti, D., Nurholis, & Utamajaya, J. N. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) pada Dinas Tenaga Kerja. *Jurnal Nasional Indonesia*, *1*, 15–25. https://doi.org/https://doi.org/10.54543/fusion.v1i03.53

Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (2019). Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018. *Jurnal CoreIT*, *5*(1), 19–28.

Dwiaranda, R. Y., Budiyono, A., & Widjajarto, A. (2020). Implementasi Dan Analisis Security Auditing Menggunakan Open Source Software ARE Dengan Framework Stride. *E-Proceeding of Engineering*, *7*(2), 7088–7095.

Fachrezi, M. I., Cahyono, A. D., & Tanaem, P. F. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(2), 764–773. https://doi.org/10.35957/jatisi.v8i2.789

Ghozali, B., Kusrini, & Sudarmawan. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*, 264–275. https://doi.org/10.24076/citec.2017v4i4.119

Guntoro, Costaner, L., & Musfawati. (2020). Analisis Keamanan Web Server Open Journal

System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45–55. https://doi.org/10.29100/jipi.v5i1.1565

Gustian, D. (Ed.). (2023). *Keamanan Sistem Informasi*. Bandung: Indie Press.

Kadir, A. (2018). *Buku Pengenalan Sistem Informasi* (Revisi). Yogyakarta; Andi.

Listartha, I. M. E., Mitha, I. M. A. P., Arta, M. W. A., & Arimika, I. K. W. Y. (2022). Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project). *Simkom*, *7*(1), 23–27. https://doi.org/10.51717/simkom.v7i1.63

Marzuki, M., Herdiansyah, M. I., Negara, E. S., & Sutabri, T. (2023). Analisis Layanan Digital SP4N LAPOR E-Government pada Pemerintahan Kota Pagaralam Menggunakan Model Delone And Mclean. *Jurnal Teknologi Informatika Dan Komputer*, *9*, 1189–1203. https://doi.org/10.37012/jtik.v9i2.1787

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat (Literature Review Sim). *Jurnal Ekonomi Manajemen Dan Sistem Informasi*, *3*(2), 520–529. https://doi.org/10.38035/jmpis.v3i2.1115

Rabbani, Athallariq, M., Budiyono, A., & Widjajarto, A. (2020). Implementasi dan Analisis Security Auditing Menggunakan Open Source Software Dengan Framework Mitre ATT&CK. *E-Proceeding of Engineering*, *7*(2), 7080–7087.

Rochaety, E. (2017). *Sistem Informasi Manajemen*. Jakarta: Mitra Wacana Media.

Rochman, A., Salam, R. R., & Maulana, S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di Rumah Sakit XYZ. *Jurnal Indonesia Sosial Teknologi: P–ISSN: 2723 - 6609*, *2*(4), 506–519. https://doi.org/10.36418/jist.v2i4.124

Sadya, S. (2023). *APJII: Pengguna Internet Indonesia 215,63 Juta pada 2022-2023*. https://dataindonesia.id/internet/detail/apjii-pengguna-internet-indonesia-21563-juta-pada-20222023

Sayuthi. (2021). Konsep Pengendalian Intern Untuk Keamanan Sistem Informasi. *Al-Buhuts*, *17*(2), 290–308. https://doi.org/10.30603/ab.v17i2.2370

Yusuf, A., Arianto, T., & Amanda, C. D. (Eds.). (2022). *Lanskap Keamanan Siber Indonesia 2022*. BSSN. Jakarta.