Analisis Keamanan Sistem Informasi *E-Government* XYZ Menggunakan Metode VAPT dan Rekomendasi Berbasis CWE

I Gede Putu Krisna Juliharta[1], I Dewa Gede Bhisma Deva Prasada[2], Made Adi Paramartha Putra[3]
[1,2]Fakultas Teknologi dan Desain, [3]Fakultas Ekonomi dan Bisnis
Universitas Primakara
Denpasar, Indonesia
e-mail: [1]krisna@primakara.ac.id, [2]bhismadeva11@gmail.com, [3]adi@primakara.ac.id

Diajukan: 22 Juli 2025; Direvisi: 24 Juli 2025; Diterima: 25 Juli 2025

Abstrak

Keamanan sistem informasi berbasis website merupakan aspek krusial dalam menjamin kelangsungan layanan publik, terutama dalam konteks implementasi e-government. Penelitian ini dilakukan untuk menganalisis keamanan tiga sistem informasi pada lingkungan pemerintahan Kabupaten XYZ, yaitu Sistem Perpustakaan, Sistem Pejabat Pengelola Informasi dan Dokumentasi (PPID), dan Sistem Mal Pelayanan Publik (MPP). Tujuan utama dari penelitian ini adalah mengidentifikasi potensi kerentanan yang ada serta memberikan rekomendasi teknis yang mengacu pada identifikasi jenis kelemahan sesuai standar Common Weakness Enumeration (CWE). Teknik pengumpulan data dilakukan melalui observasi langsung terhadap sistem serta studi literatur terkait aspek keamanan aplikasi web. Metode yang digunakan adalah Vulnerability Assessment and Penetration Testing (VAPT) dengan klasifikasi kerentanan berdasarkan CWE, sedangkan teknik analisis data dilakukan menggunakan skema Common Vulnerability Scoring System (CVSS) v3.1 untuk menentukan tingkat keparahan kerentanan. Hasil analisis menunjukkan bahwa ketiga sistem memiliki kerentanan dengan tingkat risiko tertinggi berada pada kategori High dengan nilai CVSS sebesar 8.6. Temuan ini mengindikasikan adanya celah keamanan yang cukup serius dan perlu segera diperbaiki untuk mencegah potensi penyalahgunaan. Setiap kerentanan yang ditemukan disertai rekomendasi mitigasi yang dirancang berdasarkan ID CWE yang relevan. Penelitian ini diharapkan dapat menjadi acuan dalam upaya peningkatan keamanan sistem e-government di tingkat daerah.

Kata kunci: *CVSS, CWE, E-Government, Keamanan Informasi, VAPT.*

Abstract

The security of web-based information systems is essential for maintaining public service continuity, particularly in the context of e-Government implementation. This study aims to evaluate the security of three government systems in XYZ Regency: the Library System, the Public Information and Documentation Management (PPID) System, and the Public Service Mall (MPP) System. The main objective is to identify potential vulnerabilities and provide technical recommendations based on the Common Weakness Enumeration (CWE) classification. Data were collected through direct observation and a literature review related to web application security. The assessment was conducted using the Vulnerability Assessment and Penetration Testing (VAPT) method, with severity levels analyzed using the Common Vulnerability Scoring System (CVSS) version 3.1. The results indicate that all three systems contain several vulnerabilities, with the highest severity categorized as High, having a CVSS score of 8.6. These findings highlight critical security issues that must be addressed promptly to prevent exploitation. Each identified vulnerability is accompanied by mitigation recommendations mapped to the corresponding CWE ID. This study is expected to serve as a reference for strengthening the security of regional e-Government systems.

Keywords*: CVSS, CWE, E-Government, Information Security, VAPT.*

1. Pendahuluan

Di era digital saat ini, situs web telah menjadi sarana utama dalam penyebaran informasi, termasuk dalam pelayanan publik oleh instansi pemerintah [1], [2]. Pemanfaatan teknologi informasi melalui sistem pemerintahan berbasis elektronik *(e-government)* memberikan kemudahan dalam akses informasi, efisiensi

birokrasi, serta meningkatkan transparansi layanan publik [3]. Pemerintah Indonesia secara aktif mendorong transformasi digital melalui kebijakan strategis, seperti Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang menuntut integrasi antar OPD, antar pemerintah daerah, dan antara pemerintah daerah dengan pusat [4].

Kinerja *e-government* Indonesia menunjukkan tren positif dalam *E-Government Development Index* (EGDI), di mana peringkat EGDI Indonesia meningkat dari peringkat 107 pada tahun 2018 menjadi peringkat 88 pada tahun 2020 [5]. Namun, seiring meningkatnya digitalisasi, risiko serangan siber terhadap aplikasi web pemerintah juga semakin kompleks. Berdasarkan laporan *Cybersecurity Landscape* 2023 oleh BSSN, sektor pemerintahan menjadi target utama serangan siber dengan persentase tertinggi dalam hal eksposur data, yaitu sebesar 39,78% dari total insiden yang tercatat [6]. Temuan ini menunjukkan bahwa sektor pemerintahan sangat rentan terhadap ancaman siber, termasuk kebocoran data dan pencurian kredensial, khususnya pada sistem informasi berbasis web [7].

Ancaman ini menuntut penerapan langkah-langkah pengamanan yang tepat. Salah satu pendekatan yang banyak digunakan adalah metode *Vulnerability Assessment and Penetration Testing* (VAPT), yang menggabungkan proses identifikasi kerentanan dan simulasi serangan untuk mengukur tingkat risiko keamanan [8]. Selain itu, pengelompokan kerentanan berdasarkan kerangka *Common Weakness Enumeration* (CWE) dapat membantu dalam memberikan rekomendasi mitigasi yang lebih terstruktur dan relevan [9].

Melalui pendekatan ini, penelitian dilakukan untuk mengevaluasi tingkat keamanan aplikasi web pada sistem informasi instansi publik, dengan tujuan mengidentifikasi potensi celah keamanan dan memberikan rekomendasi berbasis standar internasional guna meningkatkan ketahanan terhadap ancaman siber.

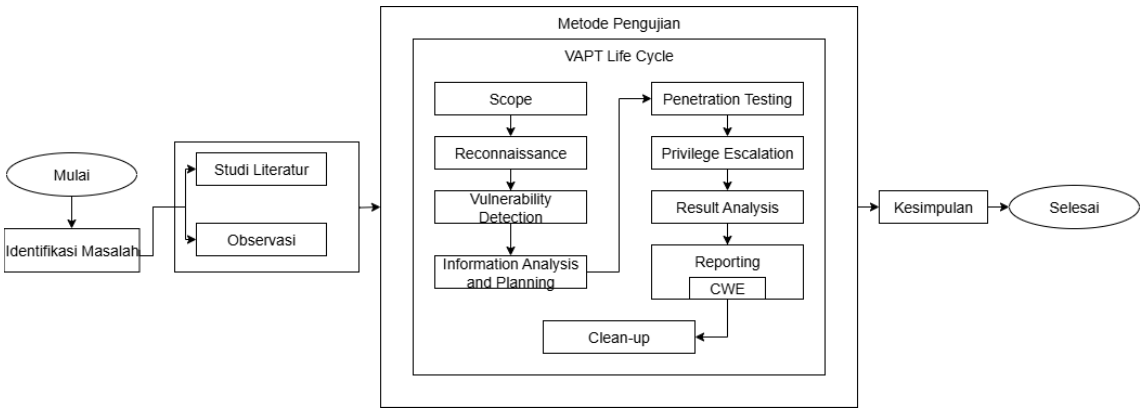
2. Metode Penelitian

Penelitian ini menggunakan pendekatan *Vulnerability Assessment and Penetration Testing* (VAPT) untuk mengevaluasi tingkat keamanan sistem informasi berbasis web pada layanan *e-government* Kabupaten XYZ. Pendekatan ini terdiri dari serangkaian tahapan yang mencakup penentuan ruang lingkup pengujian, pengumpulan informasi, deteksi kerentanan, perencanaan dan analisis, pengujian penetrasi, eskalasi hak akses, analisis hasil, pelaporan, hingga pembersihan sistem [10]. Pengujian dilakukan dengan pendekatan *black box*, di mana peneliti tidak memiliki akses terhadap struktur internal sistem sebelum proses pengujian dimulai.

Data dikumpulkan melalui observasi langsung terhadap sistem yang diuji dan studi literatur untuk mendukung kerangka analisis. Jenis data yang digunakan bersifat kualitatif, mencakup informasi terkait jenis kerentanan, tingkat keparahan, serta rekomendasi mitigasi berdasarkan referensi seperti *Common Weakness Enumeration* (CWE). Data primer diperoleh dari hasil pengujian aktual terhadap sistem, sedangkan data sekunder berasal dari referensi teoritis dan penelitian terdahulu. Seluruh temuan dianalisis secara deskriptif untuk menghasilkan evaluasi menyeluruh terhadap kondisi keamanan aplikasi yang diuji.

2.1. Alur Penelitian

Penulis memanfaatkan *flowchart* sebagai alat visualisasi untuk merinci alur penelitian secara sistematis. Berikut ini adalah *flowchart* yang mengilustrasikan setiap tahapan penelitian.



Gambar 1. Alur penelitian.

Berdasarkan Gambar 1 dapat dijelaskan sebagai berikut:

1. Identifikasi masalah: menentukan isu utama dan ruang lingkup penelitian.
2. Studi literatur: mengkaji referensi terkait keamanan informasi dan metode VAPT dari jurnal, dan dokumentasi CWE.
3. Observasi: melakukan pengamatan langsung terhadap sistem untuk memahami struktur dan potensi kerentanannya.
4. *Scope*: menetapkan area sistem dan pendekatan pengujian yang digunakan.
5. *Reconnaissance*: mengumpulkan data teknis sistem target menggunakan *tools* seperti WhatWeb dan Nmap.
6. *Vulnerability detection*: mengidentifikasi celah keamanan menggunakan OWASP ZAP.
7. Information analysis and planning: mengevaluasi hasil deteksi kerentanan dan merancang skenario pengujian lanjutan.
8. *Penetration testing*: melakukan eksploitasi celah dengan *tools* seperti Burp Suite dan SQLMap untuk menguji validitas kerentanan.
9. *Privilege escalation*: menganalisis potensi peningkatan hak akses berdasarkan hasil eksploitasi kerentanan.
10. *Result analysis*: mengukur tingkat keparahan setiap kerentanan menggunakan standar CVSS 3.1.
11. *Reporting*: menyusun laporan berisi hasil temuan dan rekomendasi perbaikan berbasis CWE.
12. *Clean-up*: mengembalikan sistem ke kondisi semula tanpa meninggalkan dampak negatif.
13. Rekomendasi (CWE): memberikan rekomendasi berbasis CWE untuk setiap kerentanan yang ditemukan pada tahap pengujian.
14. Kesimpulan: menyusun ringkasan hasil penelitian dan kesimpulan yang didapatkan.

3. Hasil dan Pembahasan

3.1. *Scope*

Pada tahap *Scope* dilakukan penentuan area-area yang akan diuji dan jenis penetrasi yang akan digunakan. Penelitian ini akan menganalisis keamanan Sistem Perpustakaan, Sistem PPID dan Sistem MPP. Selain itu, penelitian ini menggunakan penetrasi berjenis *black box testing*.

3.2. *Reconnaissance*

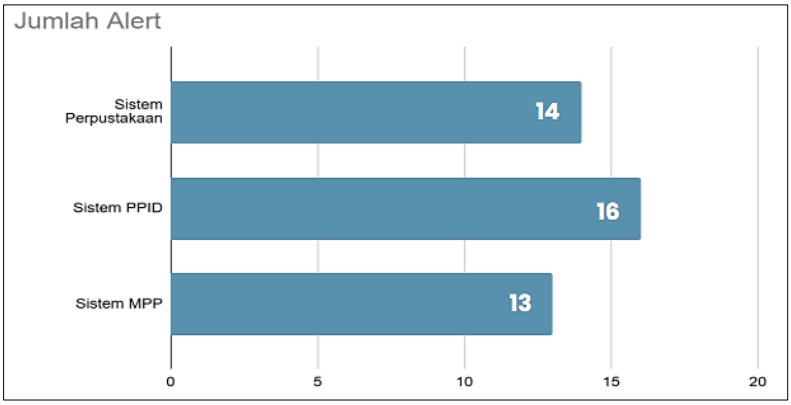
Pada tahap *Reconnaissance* dilakukan pengumpulan informasi menggunakan *tools* WhatWeb dan Nmap yang tersedia pada sistem operasi Kali Linux terhadap Sistem Perpustakaan, Sistem PPID, dan Sistem MPP. Hasil *information gathering* disajikan pada Tabel 1 berikut ini.

Tabel 1. Hasil *Information Gathering*.

Parameter	Sistem Perpustakaan	Sistem PPID	Sistem MPP
Server	*Cloudflare*	*Cloudflare*	*Cloudflare*
Framework	*CodeIgniter (PHP)*	*CodeIgniter (PHP)*	-
Web Technologies	-	*Lightbox, Open Graph Protocol*	*HTML5, JavaScript, iframe, Open Graph*
Cookies	*ci_session (HttpOnly)*	*ci_session (HttpOnly)*	*XSRF-TOKEN, mpp_kabupaten_xyz_session*
Security Headers	*report-to, nel, cf-ray, speculation-rules, alt-svc, server-timing*	*report-to, nel, cf-ray, speculation-rules, alt-svc, server-timing*	*report-to, nel, cf-ray, speculation-rules, alt-svc, server-timing*
Open Ports	80, 443, 8080	80, 443, 8080, 8443	80, 443, 8080, 8443
SSL Certificate	Valid hingga 15 Juli 2025	Valid hingga 16 April 2025	Valid hingga 4 Juni 2025
Redirects	*HTTP → HTTPS (301 Moved Permanently)*	*HTTP → HTTPS (301 Moved Permanently)*	*HTTP → HTTPS (301 Moved Permanently)*
Password Fields	*password*	*login_password*	-
Traceroute	Terhenti di node *Cloudflare* (104.26.7.158)	1 hop ke edge node *Cloudflare*	1 hop ke *edge* server *Cloudflare*

3.3. *Vulnerability Detection*

Pada tahap ini dilakukan pendeteksian kerentanan dengan memanfaatkan *tools* OWASP ZAP pada Sistem Perpustakaan, Sistem PPID, dan Sistem MPP. Pada Tabel 2 berikut ini disajikan jumlah peringatan kerentanan *(alert)* dan jumlah URL terdampak *(instance)* untuk setiap sistem.



Gambar 2. Perbandingan Jumlah Alert Per Sistem.

Gambar 2 menunjukkan jumlah *alert* atau temuan kerentanan pada tiga sistem yang diuji. Sistem PPID memiliki jumlah alert terbanyak dengan 16 temuan, disusul oleh Sistem Perpustakaan dengan 14 alert, dan Sistem MPP dengan 13 alert. Data ini mengindikasikan bahwa Sistem PPID memerlukan perhatian lebih dalam hal pengamanan dibandingkan dua sistem lainnya.

3.4. *Information Analysis and Planning*

Pada tahap ini dilakukan analisis terhadap *alerts* yang ditemukan pada tahap *vulnerability detection*, dilanjutkan dengan perencanaan *penetration testing* terhadap *alerts* yang telah dianalisis. Pada Tabel 3 berikut ini disajikan hasil *information analysis and planning* untuk setiap sistem.

Tabel 2. Hasil *Information Analysis and Planning.*

Alert	**Sistem**	**Rencana Pengujian**
Cross Site Scripting (Reflected)	Sistem Perpustakaan	Uji input dengan payload XSS dan cek eksekusi skrip di browser.
Public Exposure of .git Repository	Sistem Perpustakaan, PPID, dan MPP	Akses .git/HEAD, jika terbuka unduh repo dengan Git*Tools*.
Absence of Anti-CSRF Tokens	Sistem Perpustakaan	Cek keberadaan dan validasi token CSRF, lalu uji request tanpa token.
Path Traversal	Sistem PPID	Kirim payload dan cek apakah file luar direktori bisa diakses.
SQL Injection	Sistem PPID	Uji parameter dengan SQLMap atau *payload* manual dan amati respon.
Content Security Policy (CSP) Header Not Set	Sistem MPP	Periksa respons apakah mengandung header CSP.
Missing Anti-clickjacking Header	Sistem MPP	Cek header terkait, lalu muat situs dalam <iframe> dan lihat hasilnya.

3.5. *Penetration Testing*

Pada tahap ini dilakukan pengujian eksploitasi kerentanan berdasarkan hasil *Information Analysis and Planning* yang telah dilakukan pada Sistem Perpustakaan, Sistem PPID, dan Sistem MPP. Pada Tabel 4 berikut ini disajikan hasil *penetration testing* untuk setiap sistem.

Tabel 3. Hasil *Penetration Testing*.

Alert	Sistem	Hasil *Penetration Testing*
Cross Site Scripting (Reflected)	Sistem Perpustakaan	*Script* berhasil dieksekusi di *browser* tanpa penyaringan, membuktikan adanya kerentanan *XSS reflected*.
Public Exposure of .git Repository	Sistem Perpustakaan, PPID, dan MPP	Direktori .git dapat diakses publik dan file penting berhasil diunduh, menunjukkan konfigurasi keamanan yang tidak memadai.
Absence of Anti-CSRF Tokens	Sistem Perpustakaan	Tidak ditemukan *header* token CSRF dalam respons, menandakan tidak adanya perlindungan terhadap serangan CSRF.
Path Traversal	Sistem PPID	Tidak ditemukan bukti eksploitasi *path traversal* yang valid, dan hasil pemindaian dikategorikan sebagai *false positive*.
SQL Injection	Sistem PPID	Tidak ada *payload* injeksi SQL yang berhasil dieksekusi, menunjukkan parameter tidak rentan terhadap injeksi SQL.
Content Security Policy (CSP) Header Not Set	Sistem MPP	*Header Content-Security-Policy* tidak ditemukan pada respons, memperlihatkan tidak adanya perlindungan terhadap serangan berbasis *client-side*.
Missing Anti-clickjacking Header	Sistem MPP	Situs berhasil dimuat dalam elemen *iframe* tanpa pencegahan, menunjukkan tidak adanya proteksi terhadap serangan *clickjacking*.

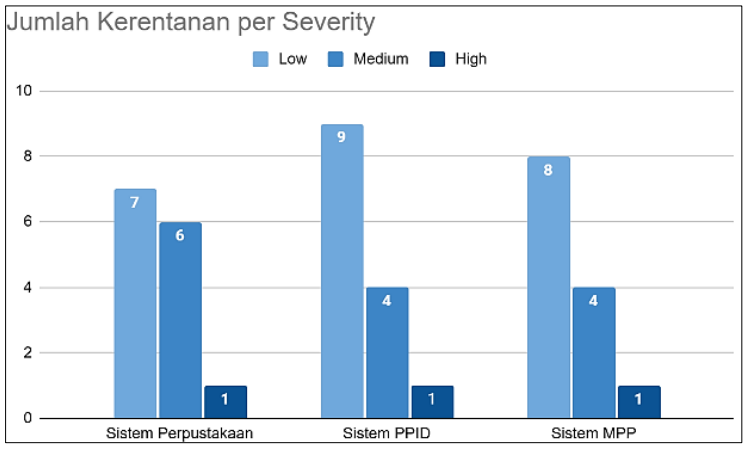
3.6. *Privilege Escalation*

Pada tahap ini, peneliti menganalisis potensi eskalasi hak akses berdasarkan hasil pengujian sebelumnya. Dari sembilan kerentanan yang ditemukan, dua di antaranya meliputi *Reflected Cross-Site Scripting* (pada Sistem Perpustakaan) dan *Missing Anti Clickjacking Header* (pada Sistem MPP) berpotensi dimanfaatkan untuk mengambil alih akun pengguna melalui pencurian sesi atau manipulasi interaksi pengguna.

Namun, karena kedua skenario ini memerlukan keterlibatan akun aktif dan interaksi nyata, pengujian tidak dilanjutkan ke tahap eksploitasi langsung. Untuk menjaga etika, integritas penelitian, dan mematuhi prinsip perlindungan data, analisis dibatasi pada tingkat teoretis sebagai *proof-of-concept* tanpa menyentuh akun maupun sistem produksi secara langsung.

3.7. *Result Analysis*

Pada tahap ini, dilakukan perhitungan skor kerentanan menggunakan CVSS 3.1 untuk membantu dalam mengkategorikan tingkat risiko dari masing-masing kerentanan, sehingga memudahkan prioritisasi dalam proses mitigasi.



Gambar 3. Rekap CVSS Per Sistem.

Berdasarkan Gambar 4.40, Sistem Perpustakaan memiliki total 14 kerentanan dengan rincian 7 berisiko rendah *(Low)*, 6 berisiko sedang *(Medium)*, dan 1 berisiko tinggi *(High)*. Sistem PPID memiliki total 14 kerentanan, terdiri dari 9 *Low*, 4 *Medium*, dan 1 *High*. Sementara itu, Sistem MPP mencatat 13 kerentanan dengan komposisi 8 *Low*, 4 *Medium*, dan 1 *High*. Secara umum, ketiga sistem menunjukkan pola serupa, dengan sebagian besar kerentanan berada pada tingkat risiko rendah hingga sedang.

3.8. *Reporting*

Tahap ini merupakan proses penyusunan laporan yang mencakup temuan kerentanan yang berhasil diidentifikasi. Untuk setiap kerentanan, diberikan rekomendasi perbaikan yang sesuai berdasarkan referensi *Common Weakness Enumeration* (CWE).

Tabel 4. Rekomendasi Berbasis CWE.

1	Kerentanan	*1. Public Exposure of .git Repository* *2. Hidden File Found*	2	Kerentanan	*(Reflected) Cross Site Scripting*
	Severity	*High*		*Severity*	*Medium*
	CWE ID	*CWE-200*		*CWE ID*	*CWE-79*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP		Sistem Terdampak	Sistem Perpustakaan
	Rekomendasi	Untuk mencegah kebocoran data, sistem harus memisahkan area aman dan tidak aman dengan tegas, serta menerapkan prinsip *least privilege* dengan memberikan akses seminimal mungkin dan hanya saat dibutuhkan.		Rekomendasi	Gunakan pustaka dengan output encoding otomatis (seperti OWASP ESAPI), lakukan validasi input ketat, dan pastikan *encoding* sesuai konteks. Tambahkan WAF dan *hardening server* sebagai pertahanan tambahan.
3	Kerentanan	*Absence of Anti-CSRF Tokens*	4	Kerentanan	*1. Content Security Policy (CSP) Header Not Set* *2. Missing Anti-clickjacking Header*
	Severity	*Medium*		*Severity*	*Medium*
	CWE ID	*CWE-352*		*CWE ID*	*CWE-693*
	Sistem Terdampak	Sistem Perpustakaan		Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Implementasikan token CSRF menggunakan pustaka seperti OWASP CSRFGuard, hindari metode GET untuk aksi sensitif, dan tambahkan validasi *header Referer* jika memungkinkan.		Rekomendasi	Untuk mencegah penyalahgunaan *frame*, gunakan *X-Frame-Options* atau CSP, dan tambahkan *frame-breaker* script untuk dukungan peramban lama.
5	Kerentanan	*Vulnerable JS Library*	6	Kerentanan	*Application Error Disclosure*
	Severity	*Medium*		*Severity*	*Low*
	CWE ID	*CWE-1395*		*CWE ID*	*CWE-209*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP		Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Rutin perbarui pustaka JavaScript. Gunakan *tools* seperti npm audit atau Snyk untuk mendeteksi dan memperbaiki kerentanan.		Rekomendasi	Tampilkan pesan kesalahan yang generik, simpan detail kesalahan dalam log internal yang aman, dan nonaktifkan error display pada produksi.
7	Kerentanan	1. *Cookie with SameSite Attribute None* 2. *Cookie without SameSite Attribute*	8	Kerentanan	*Cookie Without Secure Flag*
	Severity	*Low*		*Severity*	*Low*
	CWE ID	*CWE-1275*		*CWE ID*	*CWE-614*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP		Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID
	Rekomendasi	Setel atribut *SameSite* menjadi *Lax* atau *Strict* untuk *cookie* sensitif guna mencegah CSRF. Hindari nilai *None* kecuali benar-benar diperlukan.		Rekomendasi	Untuk menjaga keamanan, selalu tambahkan atribut *Secure* pada *cookie* agar hanya dikirim melalui koneksi HTTPS. Ini mencegah penyadapan *cookie* melalui jaringan yang tidak aman.
9	Kerentanan	*Cross-Domain JS Source File Inclusion*	10	Kerentanan	*Information Disclosure - Debug Error Messages*
	Severity	*(Low)*		*Severity*	*Low*

	CWE ID	*CWE-829*
	Sistem Terdampak	1. Sistem PPID 2. Sistem MPP
	Rekomendasi	Pastikan semua autentikasi dilakukan melalui koneksi HTTPS untuk mencegah pencurian data oleh pihak ketiga.
11	Kerentanan	*Strict-Transport-Security Header Not Set*
	Severity	*Low*
	CWE ID	*CWE-523*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Ganti kredensial default sebelum sistem digunakan, dan pastikan tidak ada akun dengan *username/password* bawaan.
12	*CWE ID*	*CWE-215*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Tambahkan atribut *Secure* pada *cookie* agar hanya dikirim melalui HTTPS.
	Kerentanan	*Timestamp Disclosure*
	Severity	*Low*
	CWE ID	*CWE-213*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Lengkapi sertifikat SSL/TLS dengan *intermediate certificate* agar *browser* dapat memverifikasi keabsahan sertifikat dengan benar.
13	Kerentanan	*X-Content-Type-Options Header Missing*
	Severity	*Low*
	CWE ID	*CWE-345*
	Sistem Terdampak	1. Sistem Perpustakaan 2. Sistem PPID 3. Sistem MPP
	Rekomendasi	Nonaktifkan pengungkapan versi *software* pada *header* HTTP (misalnya: *Server*, *X-Powered-By*) untuk mengurangi informasi bagi penyerang.

3.9. *Clean-up*

Tahap *clean-up* umumnya dilakukan untuk mengembalikan sistem ke kondisi semula setelah pengujian penetrasi. Namun, dalam penelitian ini, tahap *clean-up* tidak diperlukan karena selama proses *penetration testing* tidak dilakukan modifikasi, eksploitasi destruktif, atau perubahan konfigurasi pada Sistem Perpustakaan, Sistem PPID, maupun Sistem MPP. Semua aktivitas dilakukan secara pasif atau dalam batas aman yang tidak memengaruhi integritas sistem, sehingga sistem tetap berada dalam kondisi seperti semula.

4. Kesimpulan

Hasil analisis keamanan menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT) terhadap tiga sistem informasi *e-government* Kabupaten XYZ yaitu Sistem Perpustakaan, Sistem PPID, dan Sistem MPP menunjukkan adanya kerentanan dengan tingkat risiko tertinggi berada pada kategori *High*, dengan skor CVSS 3.1 mencapai 8.6. Setiap kerentanan telah diklasifikasikan berdasarkan standar *Common Weakness Enumeration* (CWE) dan disertai rekomendasi mitigasi teknis yang relevan. Temuan ini mengindikasikan adanya celah keamanan yang signifikan dan perlu segera diperbaiki untuk mencegah potensi penyalahgunaan. Selain menjadi perhatian di tingkat daerah, kondisi ini juga mencerminkan tantangan keamanan yang lebih luas dalam implementasi *e-government* secara nasional. Jika kerentanan serupa terjadi di berbagai wilayah, maka dapat menimbulkan risiko sistemik terhadap infrastruktur digital pemerintah, sehingga diperlukan strategi penguatan keamanan informasi yang terintegrasi dan berkelanjutan di tingkat nasional.

Daftar Pustaka

[1] A. Fatihah and P. Dinarto, "Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ," *INNOVATIVE: Journal Of Social Science Research*, vol. 4, pp. 4536–4549, 2024.

[2] F. N. S. Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," Online, Aug. 2023.

[3] M. Dewi Puspa Khairani, "Audit Web E-Government Dengan Acunetix Web Vulnerability Guna Menganalisis Dan Perbaikan Celah Keamanan Website," *Jurnal Riset Sistem Informasi Dan*

Teknik Informatika (JURASIK, vol. 9, no. 1, pp. 442–450, 2024, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[4] I. G. P. K. Juliharta, N. K. S. Febriani, and K. Q. Fredlina, "EVALUASI DAN REKOMENDASI PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) SPBE PADA INSTANSI XYZ," *Jurnal Teknologi Informasi dan Komputer*, vol. 9, no. 1, Jan. 2023, doi: 10.36002/jutik.v9i1.2348.

[5] I. D. Yazid and A. P. Karmila, "Menuju Pemerintahan Digital Unggul: Tantangan dan Transformasi Indeks E-Government di Indonesia," *Jurnal Ilmiah Wahana Pendidikan*, vol. 10, no. 13, pp. 387–396, 2024, doi: 10.5281/zenodo.12776465.

[6] M. F. Asyrofi and I. G. D. Nugraha, "Cybersecurity Of Work From Anywhere Model For Government : A Systematic Literature Review," *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 3, no. 1, May 2025, doi: 10.62146/ijecbe.v3i1.113.

[7] F. Novianto, "Analisa Keamanan Informasi Pada E-Government Menggunakan Cobit 5 Framework," 2023.

[8] D. Supriadi, E. Suryadi, R. Muslim, L. Delsi Samsumar, and U. Teknologi Mataram, "Implementasi Vulnerability Assessment OWASP (Open Web Application Security Project) Pada Website Universitas Teknologi Mataram," Oct. 2024.

[9] P. Mell and A. Gueye, "A Suite of Metrics for Calculating the Most Significant Security Relevant Software Flaw Types," 2020. doi: 10.48550/arXiv.2006.08524.

[10] V. Varma Vegesna, "Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," Jul. 2022. [Online]. Available: https://ssrn.com/abstract=4612524