Analisis Keamanan Sistem Informasi Berbasis *Website* Menggunakan *Network Security Assessment* Studi Kasus *E-Government* Kota Xyz

I Gede Putu Krisna Juliharta[1], I Kadek Adithya Deva Supariyoga[2], Anak Agung Gede Adi Mega Putra[3]
Fakultas Teknologi dan Desain
Universitas Primakara
Denpasar, Indonesia
e-mail: [1]krisna@primakara.ac.id, [2]adityadeva515@gmail.com, [3]gungde@primakara.ac.id

Diajukan: 22 Juli 2025; Direvisi: 23 Juli 2025; Diterima: 25 Juli 2025

Abstrak

Pemerintah Kota XYZ telah mengembangkan berbagai layanan e-government berbasis web seperti Sistem A, Sistem B, Sistem C, dan Sistem D. Meskipun layanan tersebut memberikan kemudahan dalam akses informasi dan pelayanan publik, aspek keamanannya masih perlu dievaluasi lebih lanjut, terutama karena pada Sistem C sebelumnya pernah terjadi insiden kebocoran data. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan sistem informasi pada keempat layanan tersebut berdasarkan prinsip Confidentiality, Integrity, dan Availability (CIA). Metode yang digunakan adalah Network Security Assessment (NSA) dengan pendekatan penetration testing, serta dibantu dengan alat seperti Nmap, WhatWeb, OWASP ZAP, dan Acunetix. Teknik pengumpulan data dilakukan melalui observasi langsung terhadap sistem dan studi literatur terhadap standar dan kerangka kerja keamanan informasi. Hasil pengujian yang dianalisis menggunakan Common Vulnerability Scoring System (CVSS) menunjukkan adanya sejumlah kerentanan dengan tingkat risiko sedang hingga tinggi. Penelitian ini juga memberikan rekomendasi teknis sebagai langkah mitigasi terhadap temuan kerentanan tersebut.

Kata kunci: *E-Government, Keamanan Sistem Informasi, Network Security Assessment.*

Abstract

XYZ City Government has developed various web-based e-Government services such as System A, System B, System C, and System D. Although these services provide easy access to information and public services, their security aspects still need to be further evaluated, especially because System C has previously experienced data leakage incidents. This research aims to analyze information system security vulnerabilities in the four services based on the principles of Confidentiality, Integrity, and Availability (CIA). The method used is Network Security Assessment (NSA) with a penetration testing approach, and assisted by tools such as Nmap, WhatWeb, OWASP ZAP, and Acunetix. Data collection techniques are carried out through direct observation of the system and literature study of information security standards and frameworks. The test results analyzed using the Common Vulnerability Scoring System (CVSS) show the existence of a number of vulnerabilities with moderate to high risk levels. This research also provides technical recommendations as mitigation measures against the vulnerability findings.

Keywords*: E-Government, Information System Security, Network Security Assessment.*

1. Pendahuluan

Dalam era digital saat ini, pemerintah dituntut untuk mengadopsi teknologi informasi guna meningkatkan efektivitas, efisiensi, dan transparansi layanan publik [1]. Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagaimana tertuang dalam Peraturan Presiden No. 95 Tahun 2018, bertujuan untuk menyelaraskan proses administrasi pemerintahan dengan kemajuan teknologi informasi demi mendukung tata kelola pemerintahan yang lebih baik [2].

Pemerintah Kota Xyz merupakan salah satu daerah yang aktif mengembangkan layanan *e-government* melalui beberapa sistem informasi berbasis *website*, seperti Sistem A, Sistem B, Sistem C, dan Sistem D. Sistem-sistem ini dirancang untuk mempermudah akses masyarakat terhadap informasi dan pelayanan publik. Namun, meskipun sistem tersebut memberikan kemudahan akses dan interaksi, aspek

keamanannya masih menjadi tantangan tersendiri [3]. Insiden kebocoran data pada Sistem DPMPTSP Kota Xyz yang terjadi pada pertengahan tahun 2024, yang menyebabkan informasi sensitif seperti data perusahaan dan kontak proyek tersebar di *dark* web, menjadi bukti nyata masih lemahnya keamanan sistem informasi pemerintah daerah[4].

Ancaman terhadap sistem *e-government* terus meningkat seiring dengan kompleksitas serangan siber. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 tercatat sebanyak 403.990.813 trafik anomali dan 347 insiden serangan siber yang terdeteksi di Indonesia, di mana 71 insiden di antaranya terjadi di sektor administrasi publik[5]. Kondisi ini menunjukkan pentingnya evaluasi keamanan sistem informasi secara berkala, guna memastikan keberlangsungan dan kepercayaan publik terhadap sistem digital pemerintah.

Untuk menjawab tantangan tersebut, diperlukan metode analisis yang komprehensif dan sistematis. Salah satu pendekatan yang banyak digunakan adalah metode *Network Security Assessment* (NSA). NSA merupakan serangkaian tahapan pengujian keamanan yang meliputi *reconnaissance*, *vulnerability scanning*, investigasi kerentanan, eksploitasi, dan pelaporan[6]. Pendekatan ini mampu memberikan gambaran mendalam terhadap tingkat kerentanan sistem informasi berdasarkan prinsip *Confidentiality, Integrity, dan Availability* (CIA).

Penelitian-penelitian sebelumnya telah menunjukkan efektivitas metode NSA dalam mengidentifikasi dan mengukur risiko keamanan pada sistem pemerintah daerah. Setiawan et al. [7] berhasil mengungkap berbagai celah keamanan pada situs Pemerintah Kota Surabaya melalui pendekatan *penetration testing*. Sementara itu, Juliharta et al. [8] menggunakan NSA untuk menganalisis sistem milik Kominfo Kabupaten Gianyar dan menemukan sejumlah kerentanan pada konfigurasi server dan aplikasi.

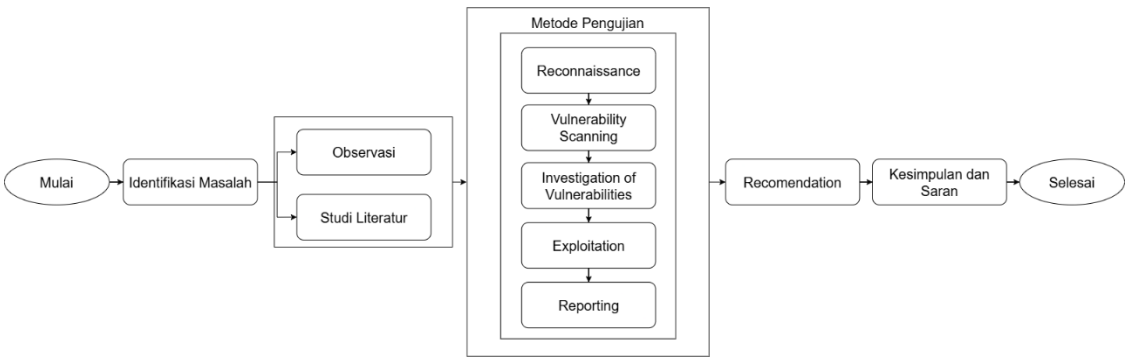
Namun demikian, kajian spesifik terhadap sistem informasi milik Pemerintah Kota Xyz masih terbatas. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis keamanan terhadap empat sistem *e-government* berbasis *website* milik Pemerintah Kota Xyz menggunakan metode *Network Security Assessment*, serta memberikan rekomendasi teknis sebagai mitigasi terhadap temuan kerentanan yang teridentifikasi.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan *Network Security Assessment* (NSA) dalam bentuk *black-box testing* untuk menganalisis tingkat keamanan pada empat sistem layanan *e-government* milik Pemerintah Kota Xyz. NSA merupakan pendekatan sistematis yang mencakup pengumpulan informasi, pemindaian kerentanan, investigasi, eksploitasi terbatas, dan pelaporan. Metode ini banyak diterapkan dalam evaluasi keamanan karena memberikan hasil yang praktis dan dapat disesuaikan dengan kebutuhan organisasi pemerintah [9] Selain itu, penerapan metode NSA sangat relevan mengingat tren serangan terhadap sektor publik terus meningkat, khususnya pada layanan berbasis web[8]. Penelitian sebelumnya juga menunjukkan bahwa metode ini efektif dalam mengidentifikasi konfigurasi server yang rentan dan logika aplikasi yang keliru dalam sistem informasi pemerintahan daerah (Juliharta et al., 2021). Seluruh proses penelitian mengacu pada prinsip *Confidentiality, Integrity, dan Availability* (CIA) serta klasifikasi kerentanan menggunakan Common Weakness Enumeration (CWE) dan pengukuran risiko melalui Common Vulnerability Scoring System (CVSS) versi 3.1[6] [10].

2.1. Alur Penelitian

Tahapan penelitian digambarkan secara sistematis dalam diagram alur seperti pada Gambar 1.



Gambar 1. Alur Penelitian Evaluasi Keamanan Sistem Website Pemerintah Kota Xyz.

Berikut tahapan-tahapan penelitian secara ringkas:

1. Identifikasi masalah: mendefinisikan isu utama terkait keamanan sistem informasi *e-government* Kota Xyz.
2. Observasi: pengamatan langsung terhadap sistem untuk memahami struktur dan potensi risikonya.
3. Studi literatur: penelaahan referensi terkait metodologi pengujian keamanan dan alat pemindaian.
4. *Reconnaissance*: mengumpulkan informasi sistem seperti layanan, *software*, dan konfigurasi.
5. *Vulnerability* scanning: pemindaian kerentanan menggunakan Acunetix.
6. *Investigation of vulnerabilities*: evaluasi dan klasifikasi dampak kerentanan menggunakan CWE dan *CVSS*.
7. *Exploitation*: uji terbatas terhadap kerentanan untuk mengukur dampak eksploitasi.
8. *Reporting*: penyusunan laporan analisis dan rekomendasi perbaikan.
9. *Recommendation*: penyusunan saran mitigasi teknis berdasarkan CWE.
10. Kesimpulan dan saran: penarikan kesimpulan dan rekomendasi lanjutan kepada pihak terkait.

3. Hasil dan Pembahasan

3.1. *Reconnaissance*

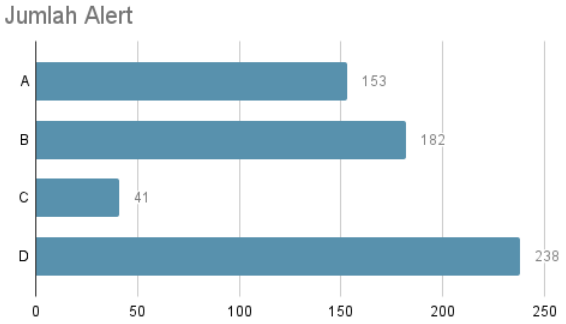
Pada tahapan *Reconnaissance*, dilakukan proses pengumpulan informasi awal terhadap *website* A,B,C, dan D menggunakan Nmap dan WhatWeb sebagai *tools* utama.

Tabel 1. Hasil *Information Gathering*.

Parameter	Sistem A	Sistem B	Sistem C	Sistem D
Server	Nginx (OpenResty 1.27.1.1)	Nginx	Apache	Nginx (OpenResty 1.27.1.1)
Framework / Engine	OpenResty berbasis NGINX dan LuaJIT	Bootstrap, JQuery 1.11.0	Bootstrap, PHPCake, JQuery	OpenResty (berbasis NGINX dan LuaJIT)
Web Technologies	-	HTML5, Script (text/javascript), Strict-Transport-Security, CSP	HTML5, Script (text/javascript), Frame/iFrame, Lightbox, YouTube, Modernizr 2.8.3.min	-
Cookies / Session Management	-	PHPSESSID (cookie HttpOnly, Secure, SameSite)	CAKEPHP (cookie HttpOnly, Secure)	-
Security Headers	-	X-Frame-Options, X-Content-Type-Options, X-UA-Compatible	X-Frame-Options, X-Content-Type-Options, X-UA-Compatible	-
Open Ports	80 (HTTP - OpenResty), 443 (HTTPS - OpenResty)	80 (HTTP - Nginx), 443 (HTTPS - Nginx), 2022 (SSH - OpenSSH 8.9p1), 8083 (HTTP - Nginx)	80 (HTTP - Apache), 443 (HTTPS - Apache), 10000 (HTTPS - MiniServ/Webmin)	80 (HTTP - OpenResty), 443 (HTTPS - OpenResty)
SSL Certificate	CN: *.Xyz.go.id; Valid 2025-04-16 s.d. 2026-04-16	CN: *.Xyz.go.id; Valid 2025-04-16 s.d. 2026-04-16	CN: *.Xyz.go.id; Valid 2025-04-16 s.d. 2026-04-16	CN: *.Xyz.go.id; Valid 2025-04-16 s.d. 2026-04-16
Redirects / HTTP Status	415 Unsupported Media Type	200 OK (setelah redirect 301)	200 OK (setelah redirect bertingkat 301 → 302 → 301)	415 Unsupported Media Type
Operating System (OS)	Oracle VirtualBox Slirp NAT Bridge	Oracle VirtualBox / Slirp NAT Bridge	Oracle VirtualBox / Slirp / QEMU	Oracle VirtualBox / Slirp / QEMU
Header HTTP	Server: openresty/1.27.1.1, Content-Type: text/html	Server: Nginx, Content-Type: text/html	Server: Apache, Content-Type: text/html	Server: openresty/1.27.1.1, Content-Type: text/html

3.2. *Vulnerability Scanning*

Pada tahap ini dilakukan pendeteksian kerentanan dengan memanfaatkan *tools* Acunetix pada Sistem A,B,C dan D.



Gambar 2. Perbandingan Jumlah *Alert* Per Sistem.

Gambar 2 menunjukkan jumlah *alert* atau temuan untuk empat kategori yang diuji (A, B, C, dan D). Kategori D memiliki jumlah *alert* terbanyak dengan 238 temuan. Disusul oleh kategori B dengan 182 *alert*, kategori A dengan 153 *alert*, dan kategori C dengan jumlah *alert* paling sedikit yaitu 41 temuan. Data ini mengindikasikan bahwa kategori D memerlukan perhatian paling besar dalam hal penanganan kerentanan dibandingkan kategori lainnya.

3.3. *Investigation of Vulnerabilities*

Pada tahap ini, *alert* dari *vulnerability scanning* dianalisis mendalam untuk perencanaan proses exploitasi dan pemberian *CWE ID*. Tabel 3 menyajikan hasil analisis informasi dan perencanaan untuk setiap sistem.

Tabel 2. Hasil *Investigation of Vulnerabilities*.

Jenis Kerentanan	Dampak Kerentanan	CWE-ID
SQL Injection	Potensi pengungkapan atau manipulasi data pada basis data	89
Cross Site Scripting (XSS)	Dapat digunakan untuk mencuri sesi pengguna atau menyisipkan skrip berbahaya	79
Directory Traversal	Akses ke file sistem di luar direktori yang diizinkan	35
HTML Injection	Dapat digunakan untuk manipulasi tampilan antarmuka dan rekayasa sosial	80
Application Error Messages	Memberikan informasi teknis yang dapat digunakan untuk merancang serangan lanjutan	209
Host Header Attack	Dapat dimanfaatkan untuk cache poisoning atau pengambilalihan token otentikasi	1388

3.4. *Exploitation*

Pada tahap ini, dilakukan pengujian eksploitasi kerentanan yang teridentifikasi dan teranalisis sebelumnya dalam fase *Investigation of Vulnerabilities*. Pengujian ini secara spesifik diterapkan pada Sistem A, Sistem B, Sistem C, dan Sistem D untuk memvalidasi keberadaan dan tingkat keparahan kerentanan yang ada. Hasil dari *exploitation* ini, yang mencakup detail mengenai kerentanan yang berhasil dieksploitasi dan potensi dampaknya, disajikan secara rinci dalam Tabel 3 untuk setiap sistem yang diuji.

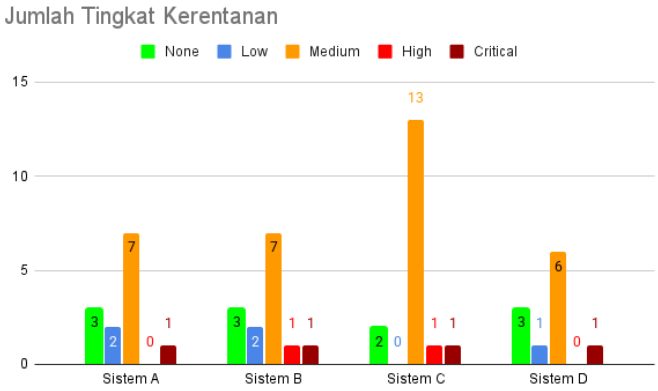
Tabel 3. Hasil *Exploitation*.

Alert	Sistem	Hasil
SQL Injection	A,B,C,D	1. Sistem A,C,D: Tidak berhasil dieksploitasi penuh. Terdeteksi *WAF/IPS.* 2. Sistem B: Berhasil dieksploitasi penuh. *SQLMap* berhasil mendapatkan basis data dari sistem melalui kerentanan pada parameter 'uname'.
Cross Site Scripting (XSS)	A,B,D	*Script XSS* yang disisipkan berhasil dieksekusi di browser tanpa adanya penyaringan yang efektif dan membuktikan adanya kerentanan *Cross-Site Scripting (XSS) reflected* pada situs web yang diuji.

Directory Traversal	A,D	Dengan payload khusus, kerentanan Directory Traversal berhasil dieksploitasi pada sistem A dan D. Penyerang dapat mengakses file di luar direktori web root, termasuk informasi sensitif seperti akun pengguna server.
HTML Injection	C	Penyisipan kode *HTML* ke dalam input tahun pada sistem C berhasil dieksekusi dan ditampilkan di halaman web tanpa penyaringan.
Application Error Messages	C	Kerentanan "Application Error Message" berhasil di ekploitasi
Host Header Attack	C	Kerentanan Host Header Attack berhasil ditemukan dan dapat dieksploitasi.

3.5. *Reporting*

Pada tahap ini, evaluasi terhadap setiap kerentanan dilakukan dengan menggunakan *Common Vulnerability Scoring System* (CVSS) versi 3.1. Penilaian ini menghasilkan skor numerik yang merepresentasikan tingkat keparahan (*severity*) kerentanan, yang kemudian dikategorikan berdasarkan skala risiko standar.



Gambar 3. Jumlah Tingkat Kerentanan pada Sistem.

Berdasarkan grafik "Jumlah Tingkat Kerentanan", Sistem A memiliki total 13 kerentanan dengan rincian 3 tidak ada risiko (*None*), 2 berisiko rendah (*Low*), 7 berisiko sedang (*Medium*), dan 1 berisiko tinggi (*High*). Sistem B memiliki total 14 kerentanan, terdiri dari 3 None, 2 Low, 7 Medium, 1 High, dan 1 Kritikal. Sementara itu, Sistem C mencatat 17 kerentanan dengan komposisi 2 Low, 13 Medium, 1 High, dan 1 Kritikal. Sistem D memiliki 11 kerentanan yang terdiri dari 3 None, 1 Low, 6 Medium, dan 1 Kritikal. Secara umum, keempat sistem menunjukkan pola di mana kerentanan berisiko sedang mendominasi, dengan beberapa kerentanan berisiko tinggi dan kritikal yang memerlukan perhatian khusus.

3.6. *Recomendation*

Tahap Rekomendasi adalah penyusunan saran perbaikan berdasarkan hasil pemindaian kerentanan. Rekomendasi ini disusun dengan merujuk pada standar Common Weakness Enumeration (CWE).

Tabel 4. Hasil Rekomendasi.

	Kerentanan	*SQL Injection*		Kerentanan	*Cross-site Scripting*
	CWE ID	89		*CWE ID*	79
	Sistem Terdampak	Sistem A,B,C,D		Sistem Terdampak	Sistem A,B,C
1	Rekomendasi	Validasi input harus ganda (klien-server) dengan *whitelist* dan filter karakter berbahaya. Pesan *error* tidak boleh menampilkan detail *query* SQL. Implementasikan WAF untuk memblokir SQL Injection, terutama pada sistem lama.	2	Rekomendasi	Mengidentifikasi dan meminimalkan semua input yang tidak tepercaya. Validasi input harus ganda (klien dan *server*) menggunakan *whitelist* (cek panjang, jenis, sintaks, nilai), bukan hanya filter karakter berbahaya. Pastikan *output encoding* UTF-8. Implementasikan WAF untuk filter serangan, terutama pada sistem lama.

3	Kerentanan	*Directory Traversal*	4	Kerentanan	*HTML Injection*
	CWE ID	35		*CWE ID*	80
	Sistem Terdampak	Sisem A,D		Sistem Terdampak	Sistem C
	Rekomendasi	Minimalisir input tidak tepercaya. Validasi input harus ganda (klien-server) dengan *whitelist* dan *output encoding* UTF-8. Pasang WAF, terutama untuk sistem lama.		Rekomendasi	Terapkan *escaping* atau *encoding* (misal: *HTML entity encoding*) pada output pengguna, atau gunakan *framework* / *library* yang otomatis menangani *escaping*. Monitor log untuk input mencurigakan dan segera perbaiki celah atau *library* rentan.
5	Kerentanan	*Application Error Messages*	6	Kerentanan	*Host Header Attack*
	CWE ID	209		*CWE ID*	1388
	Sistem Terdampak	Sistem A,B,C		Sistem Terdampak	Sistem C
	Rekomendasi	Konfigurasi *server* untuk menyembunyikan *error* langsung (misal: display_errors = Off), terapkan kontrol akses pada *log file*, dan gunakan halaman *error* kustom (misal: 404, 500) yang tidak membocorkan info internal.		Rekomendasi	Aplikasi harus memvalidasi *Host header* dengan *whitelist* nama *host* yang sah. Konfigurasikan *server* dan *middleware* untuk menolak (status 400) permintaan jika *Host header* tidak sesuai domain yang diharapkan. Pastikan aplikasi hanya mengizinkan *host* sah dan mempercayai *Host header* dari sumber tepercaya. Implementasikan pemantauan aktif pada *log server* untuk mendeteksi nilai *Host header* yang mencurigakan.

4. Kesimpulan

Berdasarkan hasil analisis keamanan yang dilakukan menggunakan metode *Network Security Assessment* (NSA), diketahui bahwa keempat sistem informasi *e-government* Kota Xyz, yaitu Sistem A, Sistem B, Sistem C, dan Sistem D, masing-masing memiliki kerentanan dengan tingkat risiko tertinggi berada pada kategori *Critical* berdasarkan perhitungan *Common Vulnerability Scoring System* (CVSS). Temuan ini menunjukkan bahwa sistem-sistem tersebut masih memiliki celah keamanan yang signifikan dan berpotensi dieksploitasi oleh pihak tidak bertanggung jawab. Untuk setiap kerentanan yang ditemukan, telah disusun rekomendasi perbaikan yang mengacu pada standar *Common Weakness Enumeration* (CWE). Rekomendasi ini dapat dijadikan pedoman teknis dalam proses perbaikan serta peningkatan keamanan sistem informasi yang bersangkutan secara berkelanjutan.

Daftar Pustaka

[1] Anak Agung Gede Adi Mega Putra, Helmy Syakh Alam, Surya Adi Prayoga, Gusti Ngurah Fajar Aditya Darma Putra, and Christian Junior Lenggu, "Pentingnya Keamanan Digital dan Internet Sehat di SMP Negeri 3 Bangli," *Joong-Ki : Jurnal Pengabdian Masyarakat*, vol. 4, no. 3, pp. 1115–1120, May 2025, doi: 10.56799/joongki.v4i3.9693.

[2] R. M. Iman, R. Rusdy, and S. Flambonita, "PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) DI PEMERINTAH DAERAH UNTUK MEWUJUDKAN GOOD GOVERNANCE," *Lex LATA*, vol. 5, no. 2, Jun. 2023, doi: 10.28946/lexl.v5i2.2351.

[3] I. G. P. K. Juliharta, K. T. Werthi, and N. L. P. N. S. P. Astawa, "PENILAIAN KEAMANAN INFORMASI E-GOVERNMENT MENGGUNAKAN INDEX KEAMANAN INFORMASI (KAMI) 4.0," *Jurnal Teknologi Informasi dan Komputer*, vol. 6, no. 2, Feb. 2020, doi: 10.36002/jutik.v6i2.1052.

[4] Akila Nuranisa and Diana Lukitasari, "Tindak Pidana Pencurian Data Dan Privasi Pengguna Dalam Transaksi E-Commerce," *Amandemen: Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia*, vol. 1, no. 2, pp. 115–126, Mar. 2024, doi: 10.62383/amandemen.v1i2.145.

[5] "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 6, no. 2, Dec. 2023, doi: 10.7454/jkskn.v6i2.10082.

[6] Chris. McNab, *Network security assessment : know your network*. O'Reilly Media, Inc., 2017. Accessed: Nov. 14, 2024. [Online]. Available: https://dokumen.pub/qdownload/network-security-assessment-know-your-network-3rdnbsped-978-1-491-91095-5.html

[7] B. Setiawan, F. Samopa, I. A. Akbar, N. A. Sani, B. C. Hidayanto, and Y. S. Dharmawan, "Pendampingan Analisis Vulnerability dan Hardening pada *Website* Pemerintah Kota Surabaya," *Sewagati*, vol. 7, no. 6, pp. 897–906, Oct. 2023, doi: 10.12962/j26139960.v7i6.624.

[8] I. G. P. K. Juliharta, I. N. Yudi Anggara Wijaya, and A. S. Laksana, "PENGUKURAN TINGKAT KEAMANAN SISTEM INFORMASI MENGGUNAKAN INDEKS KAMI VERSI 3.1, DAN MENGUKUR TINGKAT KERENTANAN SERVER MENGGUNAKAN NETWORK SECURITY ASSESSMENT STUDI KASUS KOMINFO KABUPATEN GIANYAR," *Jurnal Teknologi Informasi dan Komputer*, vol. 7, no. 3, Oct. 2021, doi: 10.36002/jutik.v7i3.1524.

[9] H. Setiawan, L. E. Erlangga, S. Siddiq, and Y. A. Gunawan, "Analisis Kerawanan Pada Aplikasi *Website* Menggunakan Standar OWASP Top 10 Untuk Penilaian Risk Rating," *Info Kripto*, vol. 17, no. 1, pp. 15–21, May 2023, doi: 10.56706/ik.v17i1.64.

[10] L. Muliawaty and S. Hendryawan, "PERANAN E-GOVERNMENT DALAM PELAYANAN PUBLIK (STUDI KASUS: MAL PELAYANAN PUBLIK KABUPATEN SUMEDANG)," *Kebijakan : Jurnal Ilmu Administrasi*, vol. 11, no. 2, pp. 45–57, Jul. 2020, doi: 10.23969/KEBIJAKAN.V11I2.2898.