ANALISIS KEAMANAN *WEBSITE* PEMERINTAH PROVINSI MALUKU MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT*

Muhammad Adam Kilian
NPP. 31.0977
Asdaf Kota Ambon, Provinsi Maluku
Studi Teknologi Rekayasa Informasi Pemerintahan
Email : 31.0977@praja.ipdn.ac.id

Pembimbing Skripsi: Helianus Rudianto, M. Si

ABSTRACT

Problem Statement/Background (GAP) *The security of city government websites is crucial given the importance of the information conveyed through them. However, website vulnerabilities can be exploited by attackers to compromise website integrity and the information contained therein. Therefore, it is necessary to perform security analysis of city government websites to identify vulnerabilities and take appropriate remedial action.* ***Purpose:*** *This study aims to perform security analysis of Maluku Province government website using vulnerability assessment method.* ***Method:*** *The method used consists of three stages: information gathering, vulnerability analysis, and remediation. The method is implemented using OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) application, which is integrated with Certified Ethical Hacker (CEH) module.* ***Result*** *The analysis results show that the Maluku Province government website has several vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), and Broken Authentication and Session Management. In addition, the website also has some issues with server configuration that can worsen website security.* ***Conclusion:*** *.Based on the analysis results, several vulnerabilities and server configuration issues have been remedied by the website administrator. The findings of this study can help the website administrator of Maluku Province government in improving website security and reducing the risk of attacks by hackers. Further research can be conducted by focusing on specific vulnerability types and testing the effectiveness of remedial actions that have been taken.*

Keywords: *: website security, vulnerability assessment, Maluku*

ABSTRAK

Permasalahan/Latar Belakang (GAP): Keamanan portal web Pemerintah Provinsi menjadi sangat penting mengingat signifikansinya dalam menyampaikan informasi krusial kepada masyarakat. Namun, rentannya portal web terhadap serangan dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, yang dapat mengakibatkan kerusakan pada integritas portal serta informasi yang tersimpan di dalamnya. Oleh karena itu, penting untuk melakukan analisis keamanan terhadap portal web Pemerintah Provinsi guna mengidentifikasi kerentanan dan mengambil langkah-langkah perbaikan yang sesuai. **Tujuan:** Penelitian ini bertujuan untuk melakukan analisis keamanan pada website pemerintah Provinsi Maluku menggunakan metode vulnerability assessment. Metode yang digunakan adalah metode yang terdiri dari tiga tahap, yaitu pengumpulan informasi, analisis kerentanan, dan tindakan perbaikan. Metode ini dilakukan dengan menggunakan aplikasi OWASP ZAP (Open Web

Application Security Project Zed Attack Proxy) yang terintegrasi dengan modul Certified Ethical Hacker (CEH). **Metode** Metode yang digunakan adalah metode yang terdiri dari tiga tahap, yaitu pengumpulan informasi, analisis kerentanan, dan tindakan perbaikan. Metode ini dilakukan dengan menggunakan aplikasi OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) yang terintegrasi dengan modul Certified Ethical Hacker (CEH). **Hasil/Temuan:** Hasil analisis menunjukkan bahwa website pemerintah Provinsi Maluku memiliki beberapa kerentanan, antara lain SQL Injection, Cross-Site Scripting (XSS), dan Broken Authentication and Session Management. Selain itu, website juga memiliki beberapa masalah pada konfigurasi server yang dapat memperburuk keamanan website. **Kesimpulan:** . Berdasarkan hasil analisis, beberapa kerentanan dan masalah konfigurasi server telah diperbaiki oleh pihak pengelola website. Hasil penelitian ini dapat membantu pihak pengelola website pemerintah Provinsi Maluku dalam meningkatkan keamanan website dan mengurangi risiko serangan oleh penyerang. Penelitian selanjutnya dapat dilakukan dengan memperdalam analisis pada jenis kerentanan tertentu dan menguji efektivitas dari perbaikan yang telah dilakukan.

Kata kunci: Keamanan website, Vulnerability Assessment, Maluku

I. PENDAHULUAN

1.1. Latar Belakang

Pemerintah Indonesia telah berupaya memanfaatkan teknologi informasi sebagai terobosan untuk meningkatkan kualitas layanan publik. Teknologi informasi dianggap sebagai solusi yang nyata dalam mempermudah pelayanan dan menjawab tuntutan masyarakat. Menurut Kasmawi et al. (2022), teknologi informasi merupakan alat yang signifikan dalam mempermudah pelayanan kepada masyarakat.

Modernisasi dalam pemerintahan adalah suatu keharusan mengingat perkembangan era saat ini yang mempengaruhi berbagai bidang kehidupan, termasuk ilmu pemerintahan. Perkembangan teknologi seharusnya membawa kemudahan bagi semua orang. Salah satu produk digitalisasi yang berkembang pesat adalah aplikasi berbasis web yang telah diimplementasikan oleh pemerintah untuk mempermudah pelayanan publik dan meningkatkan kesejahteraan masyarakat. Teknologi sistem informasi saat ini dianggap mampu memenuhi kebutuhan masyarakat dengan lebih efisien. Pendekatan digitalisasi dalam layanan pemerintahan dikenal dengan istilah e-Government. Zakiyah dan Karim (2017) menjelaskan bahwa e-Government adalah proses adaptasi konsep birokrasi ke era informasi dengan menciptakan lingkungan teknologi dalam segala proses penyelenggaraan pemerintahan, baik di tingkat pusat, daerah, maupun desa. Proses ini memungkinkan semua unit dari struktur pemerintahan untuk bekerja lebih efisien.

Era digitalisasi menuntut kemajuan teknologi informasi sebagai prioritas utama. Kasmawi et al. (2022) menegaskan bahwa tingkat kecanggihan teknologi informasi dianggap penting sebagai prediktor berkembangnya suatu negara atau daerah. Implementasi teknologi informasi dalam pemerintahan lokal dapat mempercepat penyebaran informasi dan meningkatkan efektivitas serta efisiensi fungsi-fungsi pelayanan publik.

Perkembangan digitalisasi di Indonesia dapat dilihat dari peningkatan aktivitas digital. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa jumlah pengguna internet di Indonesia mencapai 215,63 juta orang pada periode 2022-2023, meningkat 2,67% dari periode sebelumnya. Jumlah ini setara dengan 78,19% dari total populasi Indonesia yang sebanyak 275,77 juta jiwa. Data ini menunjukkan bahwa arus modernisasi telah merambah Indonesia secara signifikan.

Data Pengguna Intenet di Indonesia Tahun 2019-2023

NO	TAHUN	PRESENTASE
1	2019-2020	196,71 Juta Pengguna
2	2021-2022	210,03 Juta Pengguna
3	2022-2023	215,65 Juta Pengguna

Sumber : Survei Penyelenggara jasa Internet (APJI),2023

Hakim (2004) menekankan bahwa era revolusi industri 4.0 menuju era 5.0 menuntut pemerintah daerah untuk segera menyesuaikan diri dengan segala perubahan yang terjadi. Keberadaan teknologi informasi dan komunikasi memberikan akses kemudahan dalam pekerjaan pemerintah daerah sebagai instansi publik, sehingga operasional dapat berjalan lebih efektif dan efisien. Pemerintah daerah harus memahami bahwa teknologi ini adalah faktor penting dalam pengelolaan organisasi sektor publik, selain sumber daya alam, material, dan sumber daya manusia.

Website adalah salah satu produk yang dihasilkan dari pemanfaatan teknologi informasi. Menurut Onno W. Purbo (2006), website adalah kumpulan dokumen, gambar, suara, dan fitur lainnya yang diakses menggunakan protokol hypertext transfer protocol (HTTP). Website berfungsi sebagai media promosi, pemasaran, informasi, komunikasi, dan pendidikan.

Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) bertujuan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel, serta pelayanan publik yang berkualitas dan terpercaya. Berdasarkan hasil Pemantauan SPBE oleh Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, Provinsi Maluku mendapatkan predikat cukup dengan perolehan indeks sebesar 2,23. Hal ini menunjukkan bahwa masih diperlukan peningkatan dalam kualitas penerapan SPBE di daerah tersebut. Pemerintah daerah terus berupaya menyesuaikan teknologi informasi dalam deseminasi informasi melalui website. Zakiyah dan Karim (2017) menambahkan bahwa penting bagi pemerintah daerah untuk mengembangkan website sebagai komponen pendukung kinerja organisasi pemerintah. Instansi pemerintah harus memastikan setiap unit kerja dapat memanfaatkan internet dan mendukung konektivitas antara pemerintah dengan masyarakat. Selain itu, semua personel pemerintah perlu memiliki kesadaran dan pemahaman yang memadai dalam memanfaatkan internet sesuai dengan tugas, fungsi, dan otoritas yang telah diatur dalam regulasi terkait.

1.2. Kesenjangan Masalah yang Diambil

Penelitian ini menyoroti Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Provinsi Maluku merupakan langkah maju dalam memanfaatkan teknologi informasi untuk desiminasi informasi dan menghubungkan berbagai situs pemerintah daerah. Situs-situs ini termasuk Portal Layanan Pengadaan Secara Elektronik (LPSE), Pejabat Pengelola Informasi dan Dokumentasi (PPID), Sistem Informasi Pemerintahan Daerah (SIPD), Jaringan Dokumentasi dan Informasi Hukum (JDIH) Biro Hukum, Sistem Informasi Manajemen Pegawai (SIMPEG) BKD, dan E-Samsat BAPENDA. Fitur-fitur dalam website tersebut mencakup penyajian data laporan keuangan, laporan kinerja, Sistem Akuntabilitas Kinerja Instansi Pemerintah (SAKIP), dan Indeks Pengelolaan Keuangan Daerah (IPKD). Namun, dalam penerapannya, terdapat beberapa kesenjangan dan

tantangan yang perlu diatasi.

Keamanan website merupakan salah satu masalah utama dalam implementasi teknologi informasi pemerintah. Menurut Riadi (2020), aspek keamanan ini rentan terhadap ulah pihak-pihak tidak bertanggung jawab yang dapat melakukan tindakan kejahatan seperti penipuan, peretasan, dan serangan siber yang menargetkan individu, kelompok, atau institusi, termasuk pemerintahan. Cybercrime, seperti yang dijelaskan oleh Matondang (2018), mencakup aktivitas kejahatan di dunia maya yang memanfaatkan jaringan komputer dan internet untuk meraih keuntungan dengan mengorbankan pihak lain. Hal ini mencakup tindakan ilegal yang menyerang sistem keamanan komputer dan data yang diproses oleh suatu sistem komputer.

Pelaksanaan SPBE di Provinsi Maluku juga menghadapi masalah dari segi teknologi dan sumber daya manusia. Gangguan dan ancaman seperti virus dan kejahatan siber sering kali mengganggu operasional sistem digital pemerintah. Contoh nyata dari masalah ini dapat dilihat pada gambar yang menunjukkan kesalahan PHP pada website pemerintah Provinsi Maluku, yang bisa terjadi karena kesalahan sintaksis, logika, masalah pada server, dan lainnya. Sebuah artikel dari situs Salawaku mengungkap bahwa pada tahun 2021, website resmi Pemerintah Provinsi Maluku pernah mengalami kebobolan oleh hacker. Tampilan depan website diganti dengan pesan yang mengkritik korupsi, menunjukkan bahwa pemerintah daerah perlu meningkatkan upaya pencegahan dan pemeliharaan sistem yang digunakan dalam penyelenggaraan pemerintahan secara elektronik.

Untuk meningkatkan keamanan website, pemerintah dapat menggunakan metode Vulnerability Assessment, yang merupakan proses menemukan risiko dan kelemahan dalam aplikasi, jaringan komputer, sistem, dan elemen lain dari ekosistem TI. Menurut Riadi (2020), metode ini mencakup keamanan menyeluruh terhadap dokumen terkait keamanan informasi, hasil pemindaian jaringan, konfigurasi sistem, cara pengelolaan, kesadaran keamanan orang-orang yang terlibat, dan keamanan fisik. Tujuannya adalah untuk mengidentifikasi dan menambal kelemahan kritis sebelum dimanfaatkan oleh penjahat.

SearchSecurity menjelaskan bahwa Vulnerability Assessment membantu bisnis menemukan dan memperbaiki kesalahan kode, kesenjangan keamanan, dan masalah lainnya yang mungkin ada dalam sistem TI. Proses ini biasanya melibatkan alat penguji otomatis seperti pemindaian keamanan jaringan, yang hasilnya terdaftar dalam laporan Vulnerability Assessment (Alwi, 2020). Dengan menerapkan pendekatan ini, pemerintah daerah dapat lebih proaktif dalam menghadapi ancaman siber dan memastikan sistem informasi mereka tetap aman dan andal.

1.3. Penelitian Terdahulu

Penelitian sebelumnya yang dilakukan oleh berbagai peneliti memberikan landasan penting bagi penelitian tentang keamanan website yang diambil oleh peneliti saat ini. Berikut adalah ringkasan dari beberapa penelitian tersebut yang menginspirasi penelitian ini diantanya ada Penelitian Alif Muhammad Akmal, Nono Heryana, Arip Solehudin (2022). Penelitian ini berfokus pada analisis keamanan website Universitas Singaperbangsa Karawang menggunakan metode Vulnerability Assessment. Metode yang digunakan adalah deskriptif kuantitatif, dengan tujuan untuk mengidentifikasi tingkat keamanan dan celah keamanan pada situs web tersebut dari serangan peretas. Menggunakan alat pemindaian OWASP-ZAP, ditemukan berbagai kerentanan, termasuk dua kerentanan dengan ambang risiko tinggi, tiga dengan ambang risiko sedang, lima dengan ambang risiko rendah, dan dua dengan ambang risiko informasi. Penelitian ini menemukan celah keamanan seperti Cross-Site Scripting, SQL Injection, Absen Anti-CSRF Token, dan lain-lain, yang menunjukkan bahwa pengujian celah keamanan sangat penting untuk memperbaiki kelemahan pada sistem web. Penelitian Yudi Mulyanto, Eka Haryanti, Jumirah (2021). Penelitian ini menganalisis

keamanan website SMAN 1 Sumbawa menggunakan metode Vulnerability Assessment. Dengan pendekatan deskriptif kuantitatif, penelitian ini bertujuan untuk menentukan ambang batas keamanan sisi server website. Hasil pengujian menunjukkan bahwa website ini memiliki banyak kerentanan, termasuk SQL Injection yang memungkinkan penyerang mengakses seluruh database. Penelitian ini merekomendasikan implementasi algoritma kriptografi untuk melindungi username dan password pengguna, menunjukkan pentingnya mengatasi kerentanan untuk menjaga integritas data.

Selanjutnya Penelitian Imam Riadi, Anton Yudhana, Yunanri.W (2020). Penelitian ini menganalisis keamanan website Open Journal System (OJS) menggunakan metode Vulnerability Assessment. Dengan metode deskriptif kuantitatif, penelitian ini mengidentifikasi tingkat keamanan OJS dalam menghadapi serangan peretas. Menggunakan alat OWASP, ditemukan 70 kerentanan tingkat tinggi, 1929 kerentanan tingkat menengah, dan 4050 kerentanan tingkat rendah. Hasil ini menunjukkan bahwa versi OJS 2.4.7 memiliki banyak kerentanan dan direkomendasikan untuk menggunakan versi terbaru dari OJS yang lebih aman. Penelitian ini menekankan pentingnya pembaruan perangkat lunak secara berkala untuk menjaga keamanan sistem. Penelitian Adha Maliq Ibrahim, Tomi Defisa, Henki Bayu Seta, I Wayan Widi P (2022). Penelitian ini menganalisis keamanan sistem pada website CV. Kazar Teknologi Indonesia menggunakan metode Vulnerability Assessment and Penetration Testing (VAPT). VAPT merupakan gabungan dari dua metode uji keamanan, yang mencakup berbagai tahapan seperti scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting, dan clean-up. Hasil penelitian menemukan kerentanan dari berbagai alat seperti Nessus, OpenVAS, OWASP ZAP, dan WPScan. Penelitian ini juga menggunakan teknik seperti analisis jaringan dengan Wireshark, bypass password, brute force, inspect element melalui web browser, dan port scanning dengan nmap. Penelitian ini menekankan pentingnya maintenance rutin oleh perusahaan untuk menjaga keamanan server dan aplikasi web.

Penelitian Aryda Fatihah Putri Dinarto (2022). Penelitian ini menganalisis keamanan aplikasi website Perusahaan Daerah XYZ menggunakan metode Penetration Testing berdasarkan Framework ISSAF. Metode ini melibatkan langkah-langkah seperti information gathering, network mapping, vulnerability identification, gaining access and privilege escalation, dan enumerating further. Hasil pemindaian menunjukkan beberapa kerentanan keamanan yang dapat diperbaiki melalui pembaruan server dan penguatan protokol TLS. Penelitian ini merekomendasikan penutupan akses untuk melakukan scan terhadap port-port yang ada, pembaruan TLS ke versi terbaru, dan pemantauan serta pemeliharaan rutin untuk memastikan tingkat keamanan yang optimal.

Penelitian-penelitian ini menunjukkan pentingnya metode Vulnerability Assessment dan Penetration Testing dalam mengidentifikasi dan mengatasi kerentanan keamanan pada website. Mereka memberikan wawasan berharga tentang praktik terbaik dan alat yang dapat digunakan untuk meningkatkan keamanan sistem web, yang menjadi dasar inspirasi bagi penelitian yang sedang dilakukan oleh peneliti saat ini.

1.4. Pernyataan Kebaruan Ilmiah

Penelitian ini mengidentifikasi penerapan metode vulnerability assessment menggunakan aplikasi OWASP ZAP yang terintegrasi dengan modul Certified Ethical Hacker (CEH) untuk menganalisis keamanan website pemerintah Provinsi Maluku. Berbeda dengan penelitian sebelumnya yang mungkin hanya fokus pada satu jenis kerentanan atau menggunakan alat pemindaian tunggal, penelitian ini menggabungkan kekuatan OWASP ZAP dan CEH untuk memberikan analisis yang lebih komprehensif. Selain itu, penelitian ini tidak hanya mengidentifikasi kerentanan seperti SQL Injection, Cross-Site Scripting (XSS), dan Broken Authentication and Session Management, tetapi juga menggarisbawahi pentingnya masalah konfigurasi server dalam memperburuk keamanan

website. Temuan penelitian ini memberikan langkah-langkah perbaikan yang spesifik, yang langsung diterapkan oleh pihak pengelola website, sehingga dapat secara langsung mengurangi risiko serangan siber. Kontribusi penting lainnya adalah rekomendasi untuk penelitian lebih lanjut yang dapat memperdalam analisis pada jenis kerentanan tertentu dan menguji efektivitas dari perbaikan yang telah dilakukan, menawarkan arah baru untuk studi keamanan web di masa mendatang. Hal ini menjadikan penelitian ini sebagai langkah inovatif dalam peningkatan keamanan siber bagi portal web pemerintah daerah.

1.5. Tujuan.

Penelitian ini bertujuan untuk melakukan analisis keamanan pada website pemerintah Provinsi Maluku menggunakan metode vulnerability assessment. Metode yang digunakan adalah metode yang terdiri dari tiga tahap, yaitu pengumpulan informasi, analisis kerentanan, dan tindakan perbaikan. Metode ini dilakukan dengan menggunakan aplikasi OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) yang terintegrasi dengan modul Certified Ethical Hacker (CEH).

II. METODE

Pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan kuantitatif dengan metode deskriptif. Menurut Sugiono (2019), penelitian kuantitatif memiliki persyaratan metodis yang matang dan sangat terorganisir dari awal hingga akhir. Teknik penelitian kuantitatif didefinisikan sebagai teknik berbasis positivis yang digunakan untuk meneliti populasi atau sampel tertentu dengan pengambilan sampel acak, penggunaan instrumen penelitian untuk pengumpulan data, dan analisis data kuantitatif untuk menguji hipotesis yang telah dikonfirmasi.

Penelitian ini menggunakan pendekatan deskriptif untuk menjabarkan objek dan hasil penelitian. Operasionalisasi variabel dalam penelitian ini mencakup tingkat keamanan website yang diukur berdasarkan jumlah dan tingkat keparahan kerentanan, serta metode vulnerability assessment menggunakan OWASP ZAP dan modul Certified Ethical Hacker (CEH) (Abdullah & Hassan, 2014). Instrumen penelitian yang digunakan adalah OWASP ZAP untuk menguji tingkat keamanan dan celah keamanan pada sebuah website.

Menurut Sugiono (2019), variabel penelitian adalah kualitas, ciri, atau nilai yang diteliti untuk dibuat kesimpulan. Tingkat kerentanan yang digunakan dalam OWASP dibagi menjadi tiga penilaian: high, medium, dan low. Dimas Abdillah (2023) menambahkan bahwa tingkat keparahan risiko ditentukan melalui perhitungan rata-rata faktor terkait, dengan bobot likelihood dan impact yang berbeda untuk setiap risiko. OWASP Top 10 untuk 2021 digunakan sebagai indikator utama dalam penelitian ini, mencakup sepuluh kategori kerentanan seperti Broken Access Control, Cryptographic Failures, dan Injection. Teknik pengumpulan data melibatkan observasi langsung dan dokumentasi proses pengecekan keamanan website pemerintah Provinsi Maluku.

Footprinting and Network Discovery merupakan tahapan menemukan struktur keamanan jaringan, menggunakan alat seperti Whois, Nslookup, Scanning Port, dan HttpRecon. Scanning Vulnerability, menurut Kurniawan et al. (2017), adalah proses skrining kerentanan untuk menemukan celah keamanan seperti SQL Injection dan Cross-Site Scripting (XSS). Tahap terakhir, reporting, menawarkan analisis kasus celah keamanan dan solusi yang disarankan.

III. HASIL DAN PEMBAHASAN

3.1. Analisis keamanan website pemerintahan Provinsi Maluku menggunakan Metode Vulnerability Assessment

Analisis keamanan website pemerintahan adalah proses evaluasi yang dilakukan untuk menentukan tingkat keamanan suatu situs web pemerintahan. Tujuannya adalah memastikan bahwa website tersebut tidak rentan terhadap serangan siber dan data sensitif yang disimpan di dalamnya tetap aman. Pentingnya proses ini terletak pada perlindungan informasi publik dan kepercayaan masyarakat terhadap instansi pemerintah.

Metode Vulnerability Assessment : Metode Vulnerability Assessment adalah proses pengecekan, identifikasi, evaluasi, dan pengukuran celah keamanan dalam sistem, aplikasi, atau jaringan. Tujuannya adalah menentukan apakah suatu sistem memiliki celah keamanan yang rentan terhadap serangan atau tidak, serta memberikan rekomendasi untuk memperbaikinya. Modul CEH (Certified Ethical Hacker) sering digunakan dalam proses ini untuk membantu mengidentifikasi celah keamanan dan memberikan rekomendasi perbaikan yang diperlukan. Penggunaan modul CEH harus selalu dilakukan dengan cara yang legal dan etis, dan hasil evaluasi serta rekomendasi dari Vulnerability Assessment harus disajikan dalam laporan yang lengkap dan akurat.

1) **Footprint/Network Discover :** Footprinting adalah metode untuk mengumpulkan informasi terkait sebuah domain, termasuk alamat, nomor telepon, alamat email, tanggal pendaftaran, dan tanggal kadaluarsa domain. Alat yang digunakan dalam footprinting meliputi:
    a. Whois: Prosedur ini bertujuan memperoleh informasi terkait domain.
    b. Nslookup : Alat ini digunakan untuk mengidentifikasi alamat IP dari sebuah domain dan mendiagnosis masalah jaringan yang terkait dengan DNS.
2) **Scanning Port Discover :** Aplikasi ini dibuat untuk menginvestigasi port server atau host yang terbuka. Ini berguna bagi administrator untuk memeriksa keamanan jaringan.
3) **HttpRecon :** Prosedur ini mengumpulkan informasi pada network dan web server yang menggunakan protokol hypertext transfer.

Scanning Vulnerability (Memindai Celah Keamanan) : Scanning vulnerability bertujuan mencari celah kerentanan pada website dan server. Hasil pemindaian menggunakan OWASP ZAP menunjukkan jumlah dan jenis risiko yang terdeteksi. Dalam sebuah studi, ditemukan total 8570 risiko yang terdiri dari 1 risiko tinggi, 2896 risiko sedang, 3074 risiko rendah, dan 2599 risiko informasi, menghasilkan 14 jenis peringatan, antara lain:

Alert type	Risk	Count
Hash Disclosure - Mac OSX salted SHA-1	High	1 (6.2%)
Absence of Anti-CSRF Tokens	Medium	27 (168.8%)
CSP: Wildcard Directive	Medium	255 (1,593.8%)
CSP: script-src unsafe-inline	Medium	255 (1,593.8%)
CSP: style-src unsafe-inline	Medium	255 (1,593.8%)
Missing Anti-clickjacking Header	Medium	139 (868.8%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3 (18.8%)
Cross-Domain JavaScript Source File Inclusion	Low	272 (1,700.0%)
Private IP Disclosure	Low	4

a. Hash Disclosure : Nilai hash dari data sensitif terbongkar. Solusinya adalah memastikan hash tidak dibocorkan oleh server web atau database.
b. Absence of Anti-CSRF Tokens : Token Anti-CSRF tidak terdeteksi dalam formulir pengiriman HTML. Solusinya adalah memastikan aplikasi tidak rentan terhadap serangan skrip lintas situs (XSS) dan menggunakan nonce khusus dalam setiap formulir.
c. Content Security Policy (CSP) Wildcard Directive : Penggunaan wildcard dalam kebijakan keamanan konten yang memungkinkan sumber daya dari berbagai sumber dimuat ke halaman web. Solusinya adalah mengkonfigurasi server untuk menyetel header Kebijakan-Keamanan-Konten.
d. CSP Script-src unsafe-inline : Mengizinkan skrip JavaScript yang ditampilkan secara langsung dalam elemen HTML. Solusinya adalah mengkonfigurasi server untuk menyetel header Kebijakan-Keamanan-Konten.
e. CSP Style-src unsafe-inline : Memungkinkan gaya inline yang dapat meningkatkan risiko serangan XSS. Solusinya adalah memastikan server web dikonfigurasi untuk menyetel header Kebijakan-Keamanan-Konten.
f. Missing Anti-clickjacking Header : Tidak adanya header untuk mencegah serangan ClickJacking. Solusinya adalah memastikan header Content-Security-Policy dan X-Frame-Options disetel di semua halaman web.
g. Big Redirect Detected (potential Sensitive Information Leak) : Tanggapan tidak menyertakan instruksi untuk mencegah serangan ClickJacking. Solusinya sama seperti di atas.
h. Cross-Domain JavaScript Source File Inclusion : Inklusi file JavaScript dari domain yang berbeda. Solusinya adalah memastikan file JavaScript hanya dimuat dari sumber yang terpercaya.
i. Private IP Disclosure : Pengungkapan alamat IP pribadi yang dapat dieksploitasi. Solusinya adalah menggunakan komentar dalam bahasa pemrograman yang sesuai untuk menghapus alamat IP pribadi dari respons HTTP.
j. Server Leaks Information : Server web atau aplikasi mengalami kebocoran informasi melalui header respon HTTP "X-Powered-By". Solusinya adalah mengkonfigurasi server untuk menekan atau menghapus header tersebut dari respons HTTP.
k. Timestamp Disclosure – Unix : Stempel waktu diungkapkan oleh aplikasi/server web. Solusinya adalah memverifikasi informasi tersebut tidak sensitif terhadap waktu.
l. Charset Mismatch : Ketidakcocokan antara header HTTP dan badan konten. Solusinya adalah memaksa UTF-8 untuk semua konten teks di header HTTP dan tag meta di HTML atau deklarasi penyandian di XML.
m. Information Disclosure - Suspicious Comments : Komentar mencurigakan dalam respons yang dapat dimanfaatkan oleh penyerang. Solusinya adalah membuang semua komentar yang mengandung informasi sensitif.
n. Modern Web Application : Informasi terkait aplikasi online modern. Solusinya adalah menggunakan Ajax Spider untuk pembaruan otomatis.
o. Re-examine Cache-control Directives : Header kontrol-cache yang belum diatur dengan benar atau hilang. Solusinya adalah memastikan header kontrol-cache disetel dengan no-cache, no-store, must-revalidate untuk konten yang aman.
p. User Controllable HTML Element Attribute (Potential XSS) : Analisis input pengguna

untuk atribut HTML tertentu. Solusinya adalah memvalidasi semua input dan membersihkan output sebelum menulis ke atribut HTML.

Proses Vulnerability Assessment sangat penting untuk menjaga keamanan website pemerintahan. Dengan mengikuti metode dan prosedur yang tepat, serta mengimplementasikan solusi yang telah direkomendasikan, instansi pemerintah dapat melindungi data sensitif dan menjaga kepercayaan publik.

3.2. Telaah Penggunaan Website Pemerintah daerah Provinsi Maluku

Website Pemerintah Daerah Maluku adalah alat penting yang digunakan untuk menyampaikan informasi dan berkomunikasi dengan masyarakat. Dalam era digital ini, website tersebut memainkan peran yang sangat vital dalam memfasilitasi pemerintahan elektronik (e-government), yang bertujuan untuk meningkatkan transparansi, efisiensi, dan aksesibilitas layanan publik. Keamanan website ini sangat penting karena menjaga integritas data dan memastikan informasi yang disajikan dapat diakses dengan aman. Keamanan website pemerintah melibatkan tiga fungsi utama: pelayanan, pengaturan, dan pembangunan.

1. **Fungsi Pelayanan**

   Dalam fungsi pelayanan, keamanan bertujuan untuk memberikan layanan yang aman dan efektif kepada masyarakat. Ini berarti melindungi data pribadi pengguna dan memastikan bahwa informasi yang tersedia di website adalah valid dan dapat diakses tanpa gangguan. Misalnya, saat masyarakat mengakses layanan administrasi publik, seperti pendaftaran dokumen atau pembayaran pajak, mereka harus merasa yakin bahwa informasi pribadi mereka aman dan tidak akan disalahgunakan. Dengan menjamin keamanan dalam pelayanan, kepercayaan masyarakat terhadap integritas dan efisiensi pemerintahan daerah akan meningkat. Kepercayaan ini penting untuk mendorong partisipasi masyarakat dalam menggunakan layanan elektronik yang disediakan oleh pemerintah.

2. **Fungsi Pengaturan**

   Fungsi pengaturan melibatkan pembuatan dan penegakan kebijakan serta peraturan yang memastikan keamanan website. Ini mencakup pengawasan rutin dan audit keamanan untuk mendeteksi serta memperbaiki kerentanan, serta penerapan standar keamanan yang ketat sesuai dengan regulasi yang berlaku. Pengaturan yang baik mengurangi risiko serangan siber dan menjaga integritas data, yang sangat penting untuk kepercayaan publik dan keberlangsungan operasional pemerintah. Misalnya, kebijakan keamanan siber harus mencakup penggunaan enkripsi, autentikasi dua faktor, dan pemantauan terus-menerus terhadap ancaman potensial. Dengan kebijakan dan regulasi yang tepat, pemerintah dapat mencegah serangan siber yang dapat merusak kepercayaan publik dan mengganggu layanan.

3. **Fungsi Pembangunan**

   Dalam fungsi pembangunan, pemerintah daerah fokus pada peningkatan kemampuan teknis dan infrastruktur untuk mendukung keamanan website. Ini mencakup pengembangan dan pemeliharaan sistem keamanan yang canggih serta pelatihan sumber daya manusia untuk meningkatkan keterampilan teknis dalam bidang keamanan siber. Misalnya, dengan mengadakan pelatihan reguler bagi staf IT tentang teknik terbaru dalam keamanan siber, pemerintah dapat memastikan bahwa mereka siap menghadapi ancaman yang terus berkembang. Selain itu, investasi dalam teknologi baru, seperti firewall canggih dan sistem deteksi intrusi, dapat membantu mencegah serangan sebelum mereka menyebabkan kerusakan.

4. **Kerentanan Website Pemerintah Provinsi Maluku**

   Website Pemerintah Provinsi Maluku menghadapi beberapa kerentanan yang dapat mengganggu fungsinya. Pertama, keamanan siber menjadi perhatian utama. Pemerintah Provinsi

Maluku memiliki tim tanggap insiden siber (MalukuProv-CSIRT) yang bertugas mengkoordinasikan layanan keamanan siber dan membangun kapasitas sumber daya keamanan siber. Namun, ancaman siber yang terus berkembang memerlukan upaya berkelanjutan untuk menjaga keamanan informasi publik. Serangan siber dapat datang dalam berbagai bentuk, seperti malware, phishing, atau serangan DDoS, yang semuanya dapat mengganggu operasi website dan merusak data.

Kedua, infrastruktur merupakan elemen vital. Layanan seperti LPSE (Layanan Pengelolaan Keuangan dan Pembangunan) membutuhkan infrastruktur yang stabil dan aman. Kerentanan infrastruktur dapat mengganggu kinerja layanan dan mengancam keamanan data. Infrastruktur yang kurang terjaga dapat menyebabkan downtime, yang mengakibatkan gangguan layanan publik. Ketiga, keterbatasan sumber daya manusia dan infrastruktur di Pemerintah Provinsi Maluku mempengaruhi kualitas layanan dan keamanan website. Keterbatasan ini membuat pemeliharaan dan pengawasan website menjadi kurang optimal. Tanpa sumber daya yang memadai, sulit bagi pemerintah untuk menjaga keamanan website secara efektif.

Selanjutnya, komitmen terhadap Good Governance, yang melibatkan prinsip transparansi, akuntabilitas, dan penegakan hukum, harus diimbangi dengan langkah-langkah pengamanan data yang ketat untuk mencegah gangguan pada keamanan dan integritas data. Upaya Pemerintah Provinsi Maluku untuk menjadi Smart Province dengan infrastruktur dan teknologi modern juga memerlukan strategi keamanan yang kuat untuk memastikan keamanan dan efisiensi layanan.

5. Penyebab Kerentanan

Ada beberapa penyebab kerentanan pada website pemerintah Provinsi Maluku. Kurangnya maintenance menjadi faktor utama, di mana perawatan dan pengawasan yang tidak rutin menyebabkan celah keamanan. Sumber daya manusia yang kurang terampil dalam mengatasi masalah keamanan menjadi kendala utama. Kurangnya penggunaan teknologi keamanan, seperti Content Security Policy (CSP) dan HTTPS, meningkatkan risiko serangan siber dan pengungkapan data sensitif. Pengawasan yang tidak memadai juga menyebabkan kerentanan yang tidak terdeteksi dan tidak tertangani dengan baik. Perencanaan strategis yang kurang efektif dalam menghadapi ancaman siber dan meningkatkan keamanan website juga menjadi faktor penting lainnya. Kurangnya koordinasi antara berbagai departemen dan kurangnya pemahaman tentang pentingnya keamanan siber dapat memperburuk situasi.

3.3. Upaya yang dilakukan dalam mengatasi permasalahan keamanan website pemerintahan Provinsi Maluku menggunakan Metode Vulnerability Assessment

Penelitian Untuk meningkatkan keamanan website Pemerintah Provinsi Maluku, perlu dilakukan perbaikan dan pengawasan yang lebih efektif serta pengembangan kapasitas sumber daya keamanan siber. Langkah-langkah yang dapat diambil termasuk meningkatkan kualitas infrastruktur dan sumber daya manusia melalui pelatihan dan sertifikasi, membangun sistem keamanan yang lebih efektif dan efisien dengan mengadopsi teknologi keamanan terbaru, serta meningkatkan transparansi dan akuntabilitas dalam penyelenggaraan pemerintah. Misalnya, pelatihan berkelanjutan bagi staf IT dan peningkatan koordinasi antar-departemen dapat membantu memperkuat pertahanan siber.

Dalam meningkatkan kualitas infrastruktur, pemerintah perlu berinvestasi dalam perangkat keras dan perangkat lunak keamanan terbaru. Ini termasuk pemasangan firewall yang kuat, sistem deteksi dan pencegahan intrusi, serta enkripsi data yang canggih. Selain itu, pemerintah harus memastikan bahwa infrastruktur ini dirawat secara berkala dan diperbarui untuk menghadapi ancaman keamanan yang terus berkembang. Pemeliharaan dan pembaruan rutin adalah langkah penting dalam

memastikan bahwa sistem tetap terlindungi dari ancaman terbaru.

Selain itu, pelatihan dan pengembangan sumber daya manusia juga sangat penting. Pemerintah perlu mengadakan program pelatihan berkelanjutan bagi staf IT dan petugas keamanan siber. Pelatihan ini harus mencakup pengetahuan tentang ancaman keamanan terbaru, praktik terbaik dalam pengelolaan keamanan siber, dan keterampilan teknis yang diperlukan untuk menangani insiden keamanan. Dengan meningkatkan kapasitas sumber daya manusia, pemerintah dapat memastikan bahwa mereka memiliki tim yang kompeten untuk menghadapi dan mengatasi ancaman keamanan siber.

Transparansi dan akuntabilitas juga harus ditingkatkan dalam pengelolaan keamanan website. Pemerintah harus memastikan bahwa semua kebijakan dan prosedur keamanan siber disusun secara jelas dan diikuti dengan ketat. Audit keamanan berkala harus dilakukan untuk menilai efektivitas langkah-langkah keamanan yang ada dan mengidentifikasi area yang memerlukan perbaikan. Selain itu, pemerintah harus berkomunikasi secara transparan dengan masyarakat tentang langkah-langkah yang diambil untuk melindungi data dan layanan mereka. Transparansi ini dapat membantu membangun kepercayaan masyarakat terhadap pemerintah.

Pengembangan teknologi juga memainkan peran penting dalam meningkatkan keamanan website. Pemerintah harus terus mencari dan mengadopsi teknologi keamanan terbaru untuk melindungi data dan layanan mereka. Ini termasuk penggunaan teknologi kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) untuk mendeteksi dan merespons ancaman keamanan dengan lebih cepat dan efektif. Teknologi ini dapat membantu pemerintah mendeteksi pola perilaku yang mencurigakan dan mengambil tindakan pencegahan sebelum serangan terjadi.

Komitmen terhadap Good Governance dan Smart Province

Pemerintah Provinsi Maluku berkomitmen untuk menciptakan pemerintahan yang transparan, akuntabel, dan bebas korupsi melalui prinsip-prinsip Good Governance. Dalam konteks ini, keamanan website pemerintah menjadi sangat penting untuk menjaga integritas dan transparansi data. Dengan menerapkan langkah-langkah keamanan yang kuat, pemerintah dapat memastikan bahwa informasi yang disajikan kepada publik adalah akurat dan dapat diandalkan. Hal ini juga penting untuk mendukung upaya pemerintah dalam menjadi Smart Province, di mana teknologi modern dan infrastruktur canggih digunakan untuk meningkatkan efisiensi dan kualitas layanan publik.

Pengembangan Smart Province melibatkan penerapan teknologi canggih seperti Internet of Things (IoT), big data, dan kecerdasan buatan untuk meningkatkan kualitas hidup masyarakat dan efisiensi operasional pemerintah. Namun, penerapan teknologi ini juga membawa tantangan keamanan yang signifikan. Oleh karena itu, pemerintah harus memastikan bahwa semua sistem dan data yang terkait dengan Smart Province dilindungi dengan langkah-langkah keamanan yang canggih. Ini termasuk enkripsi data, kontrol akses yang ketat, dan pemantauan terus-menerus terhadap ancaman keamanan.

Pemerintah juga harus mengembangkan kebijakan dan regulasi yang mendukung keamanan siber dalam konteks Smart Province. Kebijakan ini harus mencakup standar keamanan untuk semua sistem dan perangkat yang digunakan dalam inisiatif Smart Province, serta pedoman untuk penanganan insiden keamanan. Dengan kebijakan dan regulasi yang tepat, pemerintah dapat memastikan bahwa semua aspek Smart Province dilindungi dari ancaman keamanan siber.

3.4. Diskusi Temuan Utama Penelitian

Dalam Penelitian mengenai analisis keamanan website pemerintahan Provinsi Maluku dengan menggunakan metode Vulnerability Assessment memberikan wawasan yang mendalam mengenai kondisi keamanan siber yang ada. Penelitian ini dibandingkan dengan studi Alif Muhammad Akmal, Nono Heryana, dan Arip Solehudin (2022) yang juga menggunakan metode Vulnerability Assessment untuk menganalisis keamanan website Universitas Singaperbangsa Karawang. Meskipun keduanya menggunakan metode yang sama, terdapat beberapa perbedaan signifikan dalam pendekatan dan hasil yang ditemukan.

Dalam penelitian mengenai keamanan website pemerintahan Provinsi Maluku, proses Vulnerability Assessment dilakukan dengan berbagai tahapan, termasuk footprint/network discover, port scanning, dan http recon. Penggunaan alat seperti Whois dan Nslookup membantu mengumpulkan informasi domain dan mengidentifikasi alamat IP yang terkait. Proses pemindaian kerentanan menggunakan OWASP ZAP menunjukkan berbagai risiko, termasuk hash disclosure, absence of anti-CSRF tokens, dan content security policy (CSP) wildcard directive. Total 8570 risiko diidentifikasi, yang terdiri dari risiko tinggi, sedang, rendah, dan informasi. Temuan ini menunjukkan bahwa meskipun situs web pemerintahan berfungsi dengan baik, terdapat banyak celah keamanan yang perlu segera ditangani untuk mencegah serangan siber yang potensial.

Sebaliknya, penelitian yang dilakukan oleh Alif Muhammad Akmal dan rekannya juga mencakup proses footprinting dan vulnerability scanning. Mereka menggunakan alat seperti Nikto dan Nmap untuk mengidentifikasi perangkat yang digunakan, tipe OS, dan topologi fisik jaringan. Footprinting dengan Nikto mengungkapkan bahwa server menggunakan Apache/2.4.25 (Win32) OpenSSL/1.0.2j dan mengidentifikasi masalah keamanan seperti cookie yang tidak memiliki tanda HttpOnly, yang berpotensi dieksploitasi oleh skrip berbahaya. Scanning dengan Nmap menemukan beberapa port terbuka, termasuk port 25 (SMTP), 53 (DNS), 80 (HTTP), dan 443 (HTTPS), yang dapat menjadi titik masuk bagi penyerang.

Tahap vulnerability scanning dalam penelitian mereka menggunakan alat OWASP ZAP dan OpenVAS. Dirsearch digunakan untuk menguji akses yang tidak sah pada berbagai direktori dan menemukan URL yang berpotensi mengandung informasi sensitif. Hasil pemindaian dengan OpenVAS menunjukkan beberapa kelemahan keamanan yang perlu diperbaiki. Analisis lebih lanjut mengidentifikasi berbagai celah keamanan, seperti broken access control dan informasi yang bocor melalui direktori yang tidak aman.

Perbandingan antara kedua penelitian menunjukkan beberapa kesamaan dalam metode yang digunakan, tetapi juga perbedaan dalam hasil yang ditemukan dan penanganan masalah keamanan. Penelitian mengenai website pemerintahan Provinsi Maluku lebih terfokus pada berbagai risiko yang terdeteksi oleh OWASP ZAP dan memberikan solusi spesifik untuk setiap masalah yang ditemukan. Misalnya, untuk masalah hash disclosure, disarankan agar hash tidak dibocorkan oleh server web atau database. Sedangkan, penelitian Alif Muhammad Akmal dan rekannya lebih menekankan pada proses pengumpulan informasi awal dan identifikasi port yang terbuka, serta memberikan rekomendasi umum untuk memperkuat keamanan seperti penggunaan enkripsi dan pengaturan kebijakan keamanan yang ketat.

Secara keseluruhan, kedua penelitian menyoroti pentingnya metode Vulnerability Assessment dalam mengidentifikasi dan memperbaiki celah keamanan pada website. Namun, penelitian mengenai website pemerintahan Provinsi Maluku memberikan pendekatan yang lebih komprehensif dengan solusi yang lebih terperinci untuk setiap risiko yang ditemukan. Hal ini menunjukkan bahwa meskipun metode yang digunakan sama, hasil dan efektivitasnya sangat bergantung pada pendekatan spesifik yang diambil dalam analisis dan penerapan solusi. Penelitian ini memberikan kontribusi penting dalam meningkatkan keamanan siber dan melindungi data sensitif di era digital ini.

IV. KESIMPULAN

Penelitian ini mengevaluasi keamanan website Pemerintah Provinsi Maluku dengan menggunakan metode Vulnerability Assessment. Analisis menunjukkan pentingnya menjaga keamanan website pemerintah untuk melindungi data sensitif dan mempertahankan kepercayaan masyarakat. Metode ini mengidentifikasi berbagai kerentanan seperti pengungkapan hash, absennya token Anti-CSRF, dan masalah pada Content Security Policy (CSP). Selain itu, hasil pemindaian menggunakan OWASP ZAP mendeteksi risiko-risiko signifikan yang harus segera diatasi. Upaya peningkatan keamanan melibatkan perbaikan infrastruktur, pelatihan sumber daya manusia, dan penerapan kebijakan serta teknologi keamanan terbaru. Langkah-langkah ini termasuk pemasangan firewall canggih, sistem deteksi intrusi, dan pelatihan berkelanjutan bagi staf IT. Transparansi dan akuntabilitas juga ditingkatkan untuk membangun kepercayaan publik. Dengan demikian, Pemerintah Provinsi Maluku dapat memastikan integritas dan keamanan data dalam rangka mendukung penerapan Good Governance dan Smart Province.

Keterbatasan Penelitian : Penelitian ini terbatas pada analisis website Pemerintah Provinsi Maluku dan tidak mencakup evaluasi website pemerintah lainnya. Data yang diperoleh juga bergantung pada alat pemindaian tertentu

Arah Masa Depan Penelitian (*future work*) : Penelitian di masa depan dapat memperluas cakupan dengan mengevaluasi website pemerintah daerah lainnya dan menggunakan berbagai alat pemindaian untuk mendapatkan hasil yang lebih komprehensif. Penelitian juga bisa fokus pada penerapan teknologi keamanan terbaru seperti kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) untuk deteksi dan respon ancaman yang lebih efektif. Selain itu, penting untuk mengeksplorasi lebih dalam mengenai pengembangan kebijakan dan regulasi yang mendukung keamanan siber dalam konteks Smart Province. Mengidentifikasi dan mengatasi tantangan keamanan yang timbul dari penerapan teknologi canggih juga akan menjadi fokus yang relevan untuk penelitian di masa depan..

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terutama ditujukan kepada Kepala Komunikasi dan Informatika Provinsi Maluku beserta jajarannya yang telah memberikan kesempatan penulis untuk melaksanakan penelitian, serta seluruh pihak yang membantu dan mensukseskan pelaksanaan penelitian.

VI. DAFTAR PUSTAKA

Abdullah, R., & Hassan, H. (2014). Metode Vulnerability Assessment Menggunakan OWASP ZAP dan Modul Certified Ethical Hacker (CEH).

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2023). Survei Penyelenggara Jasa Internet 2023.

Hakim, L. (2004). Cara mudah memadukan web Desigh dan Web Programming. Alex Media Komputindo.

Kurniawan, A., et al. (2017). Scanning Vulnerability: Proses Skrining Kerentanan.

Onno W. Purbo. (2006). Teknologi Informasi dan Aplikasinya.

OWASP Foundation. (2021). OWASP Top 10: Kategori Kerentanan Utama.

Salawaku. (2021). Kebobolan Hacker: Kasus Website Pemerintah Provinsi Maluku.

Sugiono. (2019). Metode Penelitian Kuantitatif dan Teknik Operasionalisasi Variabel.

Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. INFORMAL: Informatics Journal, 5(2), 43. https://doi.org/10.19184/isj.v5i2.18941

Akmal, A. M., Heryana, N., & Solehudin, A. (2022). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. https://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/6495

Dimas Abdillah, dkk. (2023). Analisis Kerentanan Website Mtss Al-Washliyah Bah Gunung Menggunakan Metode Open Web Application Security Project ZAP (OWASP ZAP). Jurnal Jurnal Sains Dan Teknologi (JSIT), 3(1), 61–67. http://jurnal.minartis.com/index.php/jsi

Dinarto, A. F. P. (2022). Analisis Keamanan Aplikasi Website Perusahaan Daerah XYZ Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF. https://j-innovative.org/index.php/Innovative/article/view/9741

Ibrahim, A. M., Defisa, T., Seta, H. B., & Widi, I. W. P. (2022). Analisis Keamanan Sistem pada Website CV. Kazar Teknologi Indonesia Menggunakan Metode Vulnerability Assessment and Penetration Testing (VAPT). https://conference.upnvj.ac.id/index.php/senamika/article/download/2002/1544

Kasmawi, Wahyat, & Fiska, R. R. (2022). Pemanfaatan Layanan Informasi Desa Berbasis Teknologi Informasi Menuju Desa Digital. Jurnal Pengabdian TANJAK, 3(1), 205–211. http://ejournal.polbeng.ac.id/index.php/tanjak/article/view/2873

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 2(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

Mulyanto, Y., Haryanti, E., & Jumirah. (2021). Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Assessment. https://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1260

Riadi, I., Yudhana, A., & W, Y. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. Jurnal Teknologi Informasi Dan Ilmu Komputer, 7(4), 853–860. https://doi.org/10.25126/jtiik.2020701928

Zakiyah, E., & Karim, A. M. (2017). Implementasi arsip elektronik dalam mendukung good goverment 1,2). Shaut Al-Maktabah: Jurnal Ilmu Perpustakaan, Arsip Dan Dokumentasi, 9(2), 183–190. https://doi.org/10.15548/shaut.v9i2.117