Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Audit Web E-Government Dengan Acunetix Web Vulnerability Guna Menganalisis Dan Perbaikan Celah Keamanan Website

Maisan Dewi Puspa Khairani[1], Yuhandri[2], Sumijan[3]
[1,2,3]Universitas Putra Indonesia "YPTK" Padang, Indonesia
Email: [1]khairanii2017@gmail.com, [2]yuyu@upiyptk.ac.id, [3]sumijan@upiyptk.ac.id

Abstract

The use of the internet in government to encourage the realization of e-Government can provide benefits in increasing the power of society by increasing access to information, improving government services to the community, strengthening interaction between government and the private sector in related industries, and increasing the ease and openness of government management. One tool used to identify vulnerabilities in web applications is Acunetix Web Vulnerability. This tool is a security scanner that can automatically detect common vulnerabilities in web applications, including SQL injection attacks, Cross-Site Scripting (XSS), and others. The purpose of this research is to conduct an e-Government web audit, steps for e-Government security analysis and provide recommendations for improvements from the results of security analysis using Acunetix web vulnerabilities on the Padang City DPMPTSP website. Data was obtained using the Acunetix web Vulnerability tool to obtain a report from the penetration test process which contains information about security vulnerabilities found on the SINOPEN website https://nonperizinan.web.dpmptsp.padang.go.id/sinopen. The vulnerability findings of 148 data were at a high level, 107 data were at a medium level, 16 data were at a low level. Some of the attacks found were 11 attacks, namely Blind SQL injection, Cross site scripting (XSS), SQL injection, Application error message, HTML form without CSRF protection, Clickjacking: X-Frame-Option Header Missing, Cookie Without Secure Flag Set, File Upload, Login Page Password Guessing Attack, Broken Link, Password Type Input With AutoComplete Enabled. The Acunetix web vulnerability tool is used as a basis for analyzing improvements made after scanning the website. The results after an e-gov security audit was carried out to analyze and improve the level of vulnerabilities found on the SINOPEN website were at a low level, thereby increasing the level of security from attacks and the status of the website can be said to be safe from attack vulnerabilities.

Keywords*: Audit, e-Government, Acunetix Web Vulnerability, Vulnerability Assessment, SINOPEN*

Abstrak

Penggunaan internet di pemerintahan untuk mendorong realisasi e-government dapat memberikan manfaat peningkatan kekuatan masyarakat dengan meningkatkan akses informasi, meningkatkan pelayanan pemerintah kepada masyarakat, memperkuat interaksi antara pemerintah dan swasta di industri terkait, serta meningkatkan kemudahan dan keterbukaan pengelolaan pemerintahan. Salah satu alat yang digunakan untuk mengidentifikasi kerentanan dalam aplikasi web adalah Acunetix Web Vulnerability. Alat ini adalah sebuah scanner keamanan yang dapat secara otomatis mendeteksi kerentanan umum dalam aplikasi web, termasuk serangan SQL injection, Cross-Site Scripting (XSS), dan lainnya. Tujuan dilakukannya penelitian ini adalah melakukan audit web e-government, langkah- langkah analisis keamanan e-government dan memberikan rekomendasi perbaikan dari hasil analaisis keamanan menggunakan acunetix web vulnerability pada website DPMPTSP Kota Padang. Data diperoleh dengan menggunakan tools acunetix web vulnerability memperoleh laporan dari proses uji penetrasi yang berisi informasi tentang kerentanan keamanan yang ditemukan pada website SINOPEN https://nonperizinan.web.dpmptsp.padang.go.id/sinopen. Temuan kerentanan sebanyak 148 data berada pada level high, 107 data berada pada level medium, 16 data berada pada level low. Beberapa diantaranya serangan yang ditemukan sebanyak 11 serangan yaitu Blind sql injection, Cross site scripting (xss), Sql injection,Application error message, HTML form without CSRF protection, Clickjacking:X-Frame-Option Header Missing, Cookie Without

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Secure Flag Set, File Upload, Login Page Password-Guessing Attack, Broken Links, Password Type Input With Auto-Complete Enabled. Tools acunetix web vulnerability digunakan sebagai dasar menganalisis perbaikan yang dilakukan setelah melakukan scanning pada website tersebut. Hasil setelah dilakukan audit keamanan e-government guna melakukan analisis dan perbaikan level kerentanan yang ditemukan pada website SINOPEN berada pada level low, sehingga meningkatkan level keamanan dari serangan dan status website dapat dikatakan aman dari kerentanan serangan.

***Kata kunci**: Audit, e-government, Acunetix Web Vulnerability, Vulnerability Assessment, SINOPEN*

1. PENDAHULUAN

Pesatnya perkembangan dunia internet saat ini mengakibatkan ada usaha maksimal dari suatu organisasi dan individu untuk membuat sebuah keamanan dalam sistem dan jaringan karena sangat memungkinkan datangnya sebuah serangan. *Hacker* merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan komputer. Indonesia tercatat sebagai Negara peringkat 5 yang paling banyak terinfeksi *ransomware* di Asia Tenggara dengan jumlah rata-rata 14 kasus terjadi setiap hari, menurut riset yang dilakukan perusahaan peranti lunak antivirus *Symantec.* Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari resiko organisasi yang mungkin di hadapi. Upaya memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi [1].

Aplikasi web digunakan oleh hampir semua organisasi di semua sektor untuk berbagai tujuan, termasuk *e-commerce, e-banking, e-learning,* dan jejaring sosial. Organisasi yang gagal melindungi aplikasi web mereka berisiko menjadi sasaran penyerang. Ini dapat mengakibatkan pengungkapan informasi, kehilangan pendapatan, hubungan klien yang rusak, dan banyak lagi [2]. Penggunaan internet di pemerintahan untuk mendorong realisasi *e-government* dapat memberikan manfaat peningkatan kekuatan masyarakat dengan meningkatkan akses informasi, meningkatkan pelayanan pemerintah kepada masyarakat, memperkuat interaksi antara pemerintah dan swasta di industri terkait, serta meningkatkan kemudahan dan keterbukaan pengelolaan pemerintahan *E-government* merupakan sebuah mekanisme baru dari interaksi antara pemerintah dengan masyarakat memanfaatkan teknologi komunikasi sehingga dapat meningkatkan kualitas layanan publik. Sistem Pemerintahan Berbasis Elektronik (SPBE) atau selanjutnya disebut *e-government* adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna[3][4]. Salah satu strategi efektif *e-government* adalah menyederhanakan pelayanan kepada masyarakat, menghilangkan jenjang pada birokrasi pemerintah dan memfasilitasi apa yang sebelumnya dilakukan oleh masyarakat, kalangan bisnis, dan pemerintah yang sebelumnya dianggap sulit menjadi mudah [5].

Keamanan pada sektor publik terutama dalam penerapan sistem *e-government* merupakan hal yang perlu diperhatikan pemerintah karena merupakan hal sensitif sebab rentan disalahgunakan oleh pihak yang tidak berhak

dan akan berpengaruh pada kepercayaan publik pada pelaksanaannya [6]. Salah satu alat yang digunakan untuk mengidentifikasi kerentanan dalam aplikasi web adalah *Acunetix Web Vulnerability*. Alat ini adalah sebuah *scanner* keamanan yang dapat secara otomatis mendeteksi kerentanan umum dalam aplikasi web, termasuk serangan *SQL injection*, *Cross-Site Scripting (XSS)*, dan lainnya. Dalam studi kasus ini, fokus penelitian difokuskan pada penerapan *Acunetix Web Vulnerability* untuk menganalisis dan perbaikan keamanan situs web yang digunakan oleh Pemerintah Kota Padang khususnya Dinas Penaman Modal dan Pelayanan Satu Pintu (DPMPTSP) Kota Padang.

DPMPTSP Kota Padang telah menerapkan sistem *e-government* untuk memberikan pelayanan publik yang lebih efisien dan transparan kepada warganya. Namun, semakin kompleksnya ancaman keamanan *cyber* yang ada saat ini membuat perlindungan terhadap sistem *e-government* menjadi sangat penting. Salah satu formasi pemerintahan Kota Padang yang menggunakan *e-government* sebagai sistem pelayanan publik berbasis elektronik yaitu DPMPTSP Kota Padang yang bertugas menyelenggarakan pelayanan administrasi di bidang perizinan. Layanan pada website DPMPTSP salah satunya adalah kemudahan dalam mengurus perizinan berbasis online.

Penelitian terdahulu yang dilakukan oleh J. I. Dan dkk tentang analisis keamanan website menggunakan metode *Vulnerability Assessment* dan perhitungan *security matriks*. Data yang digunakan adalah website New Kuta Golf menghasilkan pengujian keamanan website menggunakan *acunetix web vulnerability* menghasilkan hasil yang detail. Dapat menentukan keamanan website menggunakan *security matriks*. Hasil *vulnerabily* pada new kuta golf adalah bernilai *high* [7].

Selanjutnya penelitian yang dilakukan oleh A. M. Akmal dkk tentang analisis keamanan website dengan metode *Vulnerability Assessment*. Data yang digunakan yaitu website Universitas Singaperbangsa Karawang. Hasil penelitian yaitu ditemukan 2 kerentanan dengan tingkat risiko *high*, 3 kerentanan dengan tingkat risiko *medium*, 5 kerentanan dengan tingkat risiko *low*, dan 2 kerentanan dengan tingkat risiko *informational* [8].

Penelitian yang dilakukan oleh S. Sandy dkk tentang audit keamanan dan manajemen resiko *e-learning* menggunakan framework NIST, serta aplikasi *acunetix vulnerability* sebagai alat pengujian keamanan sistem, menghasilkan nilai rata–rata 76,09% atau pada level 3 (*Implemented Procedures and Controls*). Sementara itu level yang hendak dicapai adalah level 4 (*Tested and Review Procedures and Controls*). Untuk dapat mencapai level tersebut, berdasarkan *framework NIST* SP 800-26 sebaiknya dilakukan beberapa aktivitas rekomendasi [9].

Penelitian yang dilakukan oleh F. G. Putra dkk tentang pengukuran kinerja sistem keamanan pada website kepegawaian di pemerintahan, menggunakan metode *scanning vulnerability assessment.* Data yang digunakan yaitu website sistem informasi kepegawaian di lingkungan Pemerintahan. Hasil analisis penelitian ini menjelaskan bahwa website pemerintah mempunyai 8 celah

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

keamanan. Berdasarkan hasil perhitungan menunjukan perbaikan guna meningkatkan keamanan website [10].

Tujuan penelitian ini adalah untuk melakukan audit web *e-government* pada website DPMPTSP Kota Padang menggunakan tools *Acunetix Web Vulnerability Scanner* sebagai tools untuk menganalisis dan perbaikan celah keamanan pada website DPMPTSP Kota Padang serta memberikan rekomendasi perbaikan memperbaiki kerentanan pada website.

2. METODOLOGI PENELITIAN

Metodologi penelitian mengidentifikasi semua tahapan yang digunakan dalam pembuatan struktur kerja atau biasa dikenal dengan kerangka kerja. Kerangka kerja digunakan untuk membuat tahapan – tahapan yang akan diselesaikan dalam penelitian, sehingga tahapan tersebut mempengaruhi setiap tahapan dalam mencapai tujuan penelitian.

Analisa yang dilakukan pada penelitian ini adalah menjelaskan celah keamanan yang ditemukan, darimana celah keamanan tersebut, dan bagaimana penenaganan perbaikan yang harus dilakukan agar celah dapat tertutup. Gamabar 1 menunjukan proses yang akan dilakukan dalam audit *web e-government* dengan *acunetix web vulnerability scanner* .

Gambar 1. Kerangka Penelitian

2.1. *Screening* Sistem Informasi Target

Sistem informasi target yang digunakan dalam penelitian ini adalah website SINOPEN. Pemilihan sistem informasi non perizinan untuk memberikan kemudahan pelayanan prima dan cepat serta gratis kepada masyarakat dalam mengurus perizinan khususnya di Kota Padang.

Tahapan *screening* sistem informasi target dilakukan untuk mengetahui lingkungan teknologi yang digunakan pada sistem informasi. Informasi terkait akan membantu dalam pengambilan keputusan terkait rekomendasi perbaikan yang akan diimplementasikan dalam mengetasi *web alert* yang ditemukan dari proses *scanning vulnerability.*

2.2. *Scanning Vulnerability*

Scanning vulnerability atau tahap *Assessment Vunerability* adalah proses pengumpulan berbagai informasi terkait kerentanan yang ditemukan pada website SINOPEN. Langkah ini mencari berbagai kemungkinan terkait kerentanan dapat digunakan oleh penyerang untuk merusak dan memanipulasi data pada website SINOPEN. Proses pemindaian menggunakan *tools Acunetix Web Vulnerability* versi 10.5

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

2.3. Analisis Hasil *Vulnerability Assessment*

Setelah proses *scanning* selesai langkah selanjutnya adalah melakukakan analisis pada setiap kerentanan yang ditemukan. Setiap kerentanan akan diidentifikasi sesuai dengan tingkat keparahan, peringkat risiko, sumber masalah dan saran tentang cara memperbaiki kerentanan tersebut.

3. HASIL DAN PEMBAHASAN

Identifikasi kebutuhan untuk perbaikan sistem. Dilakukan berdasarkan hasil analisis *vulnerability assessment* menggunakan *acunetix web vulnerability scanner.* Dilakukan dalam dua teknik yaitu perbaikan konfigurasi pada sistem informasi atau *review source code.* Pemilihan jenis perbaikan berdasarkan *web alert* dan teknologi yang digunakan pada aplikasi.

3.1. *Screening* Sistem Informasi Target

Gambar 2 memperlihatkan halaman utama pada website SINOPEN yang akan di uji menggunakan *tools acunetix web vulnerability scanner.*

Gambar 2. Halaman Utama Website SINOPEN

Berikut ini adalah Raw Whois Data tentang website yang akan diteliti sebagai sumber informasi yang dapat memberikan wawasan tambahan tentang domain dan informasi terkait dengan website SINOPEN dijelaskan pada Gambar 3 berikut ini

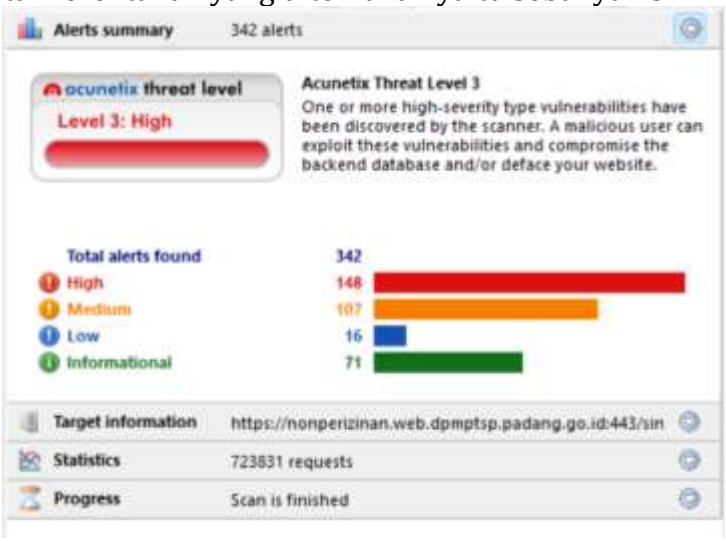
Gambar 3. Hasil Whois Website SINOPEN

Hasil yang ditampilkan pada Gambar 3 adalah hasil pemindaian menggunakan www.whois.com/whois/padang.go.id yang menunjukan nonperizinan.web.dpmptsp.padang.go.id/sinopen menggunakan domain ID PANDI-DO200361. Domain ini berasal dari layanan Pengelola Nama Domain

Internet Indonesia (PANDI) yang dibuat pada 2 Februari 2022 dan kadaluarsa pada 31 Maret 2024.

3.2. *Scanning Vulnerability*

Gambar 4 menjelaskan data hasil *scanning* website SINOPEN yang menjelaskan total kerentanan yang ditemukan yaitu sebanyak 342 kerentanan.



Gambar 4. *Scan Details* Website SINOPEN

3.3. Analisis Hasil *Vulnerability Assessment*

Data berikut ini merupakan jenis kerentanan yang ditemukan serta level kerentanan dari masing - masing kerentanan diurutkan berdasarkan level kerentanan tertinggi ke kerentanan terendah. Tabel 1 menjelaskan data kerentanan dari hasil *scanning* yang dilakukan pada website SINOPEN.

Tabel 1. Data *Scanning Vulnerability Assessment Website* SINOPEN

Level Kerentanan	Jenis Kerentanan	Jumlah Kerentanan
High	*Blind sql injection*	13
	Cross site scripting (xss)	84
	Sql injection	51
Medium	*Application error message*	97
	HTML *form without* CSRF *protection*	10
Low	*Clickjacking:X-Frame-Option Header Missing*	1
	Cookie Without Secure Flag Set	1
	File Upload	13
	Login Page Password-Guessing Attack	1
Informational	*Broken Links*	63
	Password Type Input With Auto-Complete Enabled	8
Total		342

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Data *vulnerability assessment* website SINOPEN terdapat 148 *web alert* berada pada *level security high* yang terdeteksi. *Web alert* ini nantinya akan dilakukan perbaikan dengan tujuan agar dilakukan *scanning* pada uji coba perbaikan iterasi kedua *web alert* tidak terdeteksi atau berada pada level *informational.* Pada penelitian ini dilakukan perbaikan pada level *high* hingga *medium.*

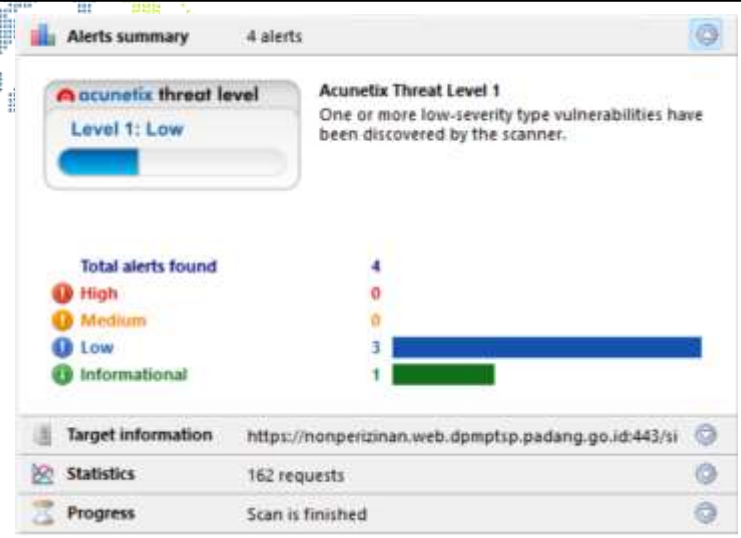
Tabel 2 menunjukan perbaikan yang akan dilakukan dalam melakukan audit web *e-government* pada website DPMPTSP Kota Padang menggunakan tools *Acunetix Web Vulnerability Scanner* sebagai tools untuk menganalisis dan perbaikan celah keamanan pada website DPMPTSP Kota Padang serta memberikan rekomendasi perbaikan memperbaiki kerentanan pada website:

Tabel 2. Perbaikan Kerentanan

No.	Jenis *Web Alert*	*Level*	Perbaikan
1	*Blind Sql Injection*	*High*	Implementasi validasi input yang digunakan adalah menggunakan *rules* panjang karakter, membatasi jenis karakter, penggunaan pada masing-masing form input
2	*Cross Site Scripting (XSS)*	*High*	Penerapan XSS *filtering* dapat membantu mencegah eksekusi skrip berbahaya yang mungkin disisipkan oleh penyerang.
3	*Sql Injection*	*High*	Melakukan pemberian validasi pada pesan kesalahan guna memastikan bahwa data yang dimasukkan oleh pengguna sesuai dengan yang diharapkan.
4	*Application error message*	*Medium*	Perbaikan *vulnerability application error message* dapat diatasi dengan memodifikasi *handling multiple environments* pada sistem agar tidak menampilkan informasi sensitif tentang sistem.
5	HTML *form without* CSRF *protection*	*Medium*	Teknik perbaikan web alert ini dapat dilakukan dengan membertikan perlindungan CSRF *protection* pada *file config* pada aplikasi. Memodifikasi konfigurasi yang ada pada konfigurasi *general website.*

Gambar 5 meunjukan hasil *scanning* iterasi kedua setelah dilakukan perbaikan. Hasil scan Iterasi 2 menggunakan *tools acunetix web vulnerability scanner* pada *website* SINOPEN menunjukan adanya penurunan jumlah *web alert* setelah dilakukannya perbaikan.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 1, Februari 2024, pp 442-450
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 5. *Scan Details* Website SINOPEN Setelah dilakukan perbaikan

Berdasarkan *scanning* iterasi kedua diperoleh hasil bahwa baik pada *scanning* pertama maupun pada *scanning* yang kedua, total *web alert website* SINOPEN mengalami penurunan jika dibandingkan dengan total *web alert* pada *scanning* iterasi pertama.

4. SIMPULAN

Hasil audit untuk menganalisis dan memperbaiki celah kerentanan yang ditemukan menggunakan *tools acunetix web vulnerability scanner* menunjukan kerentanan awal menunjukan bahwa *website* SINOPEN terkena ancaman kerentanan pada level 3 *high.* Perbaikan dilakukan pada *website* SINOPEN dihasilkan berada pada level 1 *low. Tools Acunetix Web Vulnerability Scanner* membantu dalam *vulnerability assessment* dan melakukan perbaikan untuk mengurangi tingkat kerentanan pada *website* SINOPEN.

DAFTAR PUSTAKA

[1] Y. W, R. Anto, D. Teguh Yuwono, and Y. Yuliadi, "Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box," *J. Inform. dan Rekayasa Elektron.*, vol. 4, no. 1, pp. 68–77, 2021, doi: 10.36595/jire.v4i1.365.

[2] M. Althunayyan, N. Saxena, S. Li, and P. Gope, "Evaluation of Black-Box Web Application Security Scanners in Detecting Injection Vulnerabilities," *Electron.*, vol. 11, no. 13, pp. 1–20, 2022, doi: 10.3390/electronics11132049.

[3] Elsa Prisanda and Rury Febrina, "Penerapan Teknologi Informasi dan Komunikasi Berbasis Aplikasi SISPEDAL Dalam Rangka Mewujudkan Good Village Governance," *J. Gov. Innov.*, vol. 3, no. 2, pp. 155–171, 2021, doi: 10.36636/jogiv.v3i2.723.

[4] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.

[5] T. H. Taufik, S. W. Sarah, and Y. A. Yusuf, "Analisis Strategi Keberhasilan E-Government di Kabupaten Bojonegoro," *J. Gov. Innov.*, vol. 4, no. 1, pp. 14–26, 2022, doi: 10.36636/jogiv.v4i1.1116.

[6] B. A. Iswandari, "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance," *J. Huk. Ius Quia Iustum*, vol. 28, no. 1, pp. 115–138, 2021, doi: 10.20885/iustum.vol28.iss1.art6.

[7] J. I. Dan, "Analisis Keamanan Web New Kuta Golf Menggunakan Metode," vol. 2, no. 3, pp. 256–265, 2022.

[8] A. M. Akmal, N. Heryana, and A. Solehudin, "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment," *Al-Irsyad*, vol. 105, no. 2, p. 79, 2017.

[9] S. Sandy and H. H. Solihin, "Audit Keamanan dan Manajemen Risiko pada e-Learning Universitas Sangga Buana," *J. Manaj. Inform.*, vol. 11, no. 1, pp. 1–14, 2021, doi: 10.34010/jamika.v11i1.3641.

[10] F. G. Putra and B. Soewito, "Measurement of Security System Performance on Websites of Personnel Information Systems in Government Using Common Vulnerability Scoring System," *J. Pendidik. Tambusai*, vol. 6, pp. 2949–2957, 2022.