Vol. 4, No. 2 - October 2024, Hal. 87-91
DOI: 10.59395/janitra.v4i2.205

Analisis *Assesment Vulnerability* pada *Website* dan Aplikasi Publik di Dinas Komunikasi Informatika dan Statistik Kota Banda Aceh

Rizwan Saputra[1], Dahlan Abdullah[2], Muhammad Daud*[3], Fatur Rahman Maulana[4]
[1,2,3]Program Studi Magister Teknologi Informasi, Fakultas Teknik, Universitas Malikussaleh
[4]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Malikussaleh
*e-mail: rizwansaputra@gmail.com[1], dahlan@unimal.ac.id[2], mdaud@unimal.ac.id[3], fatur.2001500075@mhs.unimal.ac.id[4]

Received:	Revised:	Accepted:	Available online:
21.08.2024	11.09.2024	19.10.2024	30.10.2024

Abstrak: Penelitian ini bertujuan untuk melakukan analisis asesmen kerentanan pada website dan aplikasi publik yang dikelola oleh Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik) Kota Banda Aceh. Kerentanan dalam sistem informasi dapat membuka peluang bagi serangan siber yang dapat merugikan integritas dan kerahasiaan data, serta ketersediaan layanan. Oleh karena itu, penelitian ini fokus pada identifikasi, evaluasi, dan mitigasi potensi kerentanan yang dapat muncul pada infrastruktur digital tersebut. Metode penelitian melibatkan analisis keamanan yang holistik, mencakup uji penetrasi, analisis kode, dan pemeriksaan konfigurasi sistem. Data yang diperoleh dari asesmen ini akan membantu Diskominfotik dalam meningkatkan keamanan sistem mereka dan melindungi informasi yang dikelola. Hasil penelitian diharapkan dapat memberikan wawasan mendalam tentang tingkat kerentanan yang ada, serta rekomendasi konkret untuk memperbaiki kelemahan yang teridentifikasi. Dengan demikian, Diskominfotik Kota Banda Aceh dapat mengambil langkah-langkah proaktif untuk mengamankan website dan aplikasi publik mereka, meningkatkan kepercayaan pengguna, dan memastikan kelangsungan operasional layanan digital.
Kata kunci: Asesmen Kerentanan, Keamanan Informasi, Uji Penetrasi, Website Publik, Aplikasi Publik.

Abstract: *This study aims to conduct a vulnerability assessment and analysis of websites and public applications managed by the Communication, Informatics, and Statistics Agency (Diskominfotik) of Banda Aceh City. Vulnerabilities in information systems can create opportunities for cyberattacks, potentially compromising the integrity, confidentiality, and availability of data and services. Therefore, this study focuses on identifying, evaluating, and mitigating potential vulnerabilities within the digital infrastructure. The research methodology includes a comprehensive security analysis, encompassing penetration testing, code review, and system configuration checks. The data obtained from this assessment will assist Diskominfotik in enhancing the security of their systems and safeguarding the information they manage. The study's results are expected to provide valuable insights into existing vulnerabilities and offer actionable recommendations for addressing identified weaknesses. By implementing these recommendations, Diskominfotik of Banda Aceh City can take proactive measures to secure their websites and public applications, increase user trust, and ensure the continuity of digital service operations.*
Keywords*: Vulnerability Assessment, Information Security, Penetration Testing, Public Website, Public Application.*

1. PENDAHULUAN

Pada era digital saat ini, pemanfaatan teknologi informasi dan komunikasi telah mengubah cara pemerintah berinteraksi dengan masyarakat [1]. Salah satu bentuk implementasinya adalah melalui pengembangan sistem *e-government*, di mana pemerintah memanfaatkan teknologi untuk memberikan pelayanan publik yang lebih efisien, transparan, dan partisipatif kepada masyarakat [2]. Dalam lingkup *e-government*, *website*, dan aplikasi publik menjadi sarana utama dalam memberikan informasi, menerima permohonan, serta menyediakan layanan publik kepada masyarakat [3].

Namun, seiring dengan kemajuan teknologi, resiko keamanan pada *website* dan aplikasi publik juga semakin meningkat [4]. Keberadaan kerentanan atau celah keamanan dapat memberikan peluang bagi pihak yang tidak bertanggung jawab untuk melakukan serangan, mengakses data sensitif, atau merusak sistem [5]. Pada saat yang sama, pemerintah dituntut untuk menjaga keamanan dan privasi data masyarakat yang diakses melalui website dan aplikasi publik, serta memastikan bahwa layanan yang disediakan dapat diandalkan dan terjamin keamanannya [6] [7].

Dalam konteks ini, penting untuk melakukan analisis dan evaluasi terhadap kerentanan dan tingkat kematangan keamanan pada *website* dan aplikasi publik dalam lingkungan *e-government* [8]. Dengan melakukan penilaian terhadap kerentanan yang ada dan mengukur tingkat kematangan keamanan, pemerintah dapat mengidentifikasi risiko yang mungkin terjadi, mengambil langkah-langkah yang tepat untuk mengurangi risiko tersebut, serta meningkatkan keamanan secara keseluruhan [9][10].

Studi kasus yang dilakukan pada Dinas Komunikasi Informatika dan Statistik yang selanjutnya disebut dengan Diskominfotik Kota Banda Aceh menjadi relevan dalam konteks ini. Kota

Vol. 4, No. 2 - October 2024, Hal. 87-91
DOI: 10.59395/janitra.v4i2.205

Banda Aceh telah mengimplementasikan berbagai sistem *e-government* untuk meningkatkan pelayanan publik kepada masyarakatnya. Namun, dalam pengoperasiannya, kemungkinan terdapat kerentanan keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang, serta perlu dilakukan evaluasi terhadap tingkat kematangan keamanan yang ada. Oleh karena itu, analisis *assessment* mengenai kerentanan dan tingkat kematangan keamanan pada website dan aplikasi publik dalam lingkungan *e-government* Kota Banda Aceh menjadi penting untuk dilakukan [11].

Dalam penelitian ini, dilakukan analisis dan evaluasi kerentanan serta tingkat kematangan keamanan pada website dan aplikasi publik di lingkungan e-government Kota Banda Aceh. Diharapkan hasil dari penelitian ini dapat memberikan wawasan yang mendalam tentang keamanan dalam konteks *e-government*, serta memberikan rekomendasi perbaikan dan langkah-langkah yang dapat diambil untuk meningkatkan keamanan pada *website* dan aplikasi publik di Kota Banda Aceh. Dengan demikian, pelayanan publik dapat dilakukan secara efektif, aman, dan dapat dipercaya oleh masyarakat

Analisis *assesment vulnerability* dan *maturity model* pada website dan aplikasi publik di Diskominfotik Kota Banda Aceh adalah untuk mengevaluasi tingkat keamanan *website* dan aplikasi publik yang digunakan oleh pemerintah Kota Banda Aceh dalam menyediakan layanan *e-government*. Analisis ini akan menggunakan model Vulnerability dan Maturity untuk mengevaluasi tingkat kerentanan (*vulnerability*) dan tingkat kematangan (*maturity*) dari *website* dan aplikasi tersebut. Studi kasus ini akan fokus pada layanan *e-government* yang disediakan oleh pemerintah Kota Banda Aceh, yang diharapkan dapat memberikan gambaran mengenai tingkat keamanan dari layanan *e-government* secara umum.

2. METODE

Dalam melakukan penelitian ini peneliti melakukan tahapan-tahapan kegiatan dengan mengikuti rencana kegiatan yang tertuang dalam tahapan pelaksanaan penelitian meliputi metode pengujian analisis yang dapat dilihat pada Gambar 1. Penelitian ini dirancang sebagai tahapan sistematis untuk mendeteksi, menganalisis, dan mendokumentasikan kerentanan keamanan siber pada sistem berbasis web, Web portal Kota Band Aceh atau sistem PPID (Pejabat Pengelola Informasi dan Dokumentasi). Proses penelitian dimulai dengan tahap Reconnaissance, yaitu pengumpulan informasi awal untuk memahami karakteristik sistem target. Pada tahap ini, informasi penting yang dikumpulkan mencakup domain, framework yang digunakan, versi perangkat lunak yang mungkin rentan, dan hasil eksplorasi menggunakan teknik dorking. Tujuannya adalah untuk mengidentifikasi potensi celah keamanan dan membangun fondasi awal untuk analisis lebih lanjut.

Selanjutnya, tahap Scanning dilakukan untuk melakukan analisis teknis terhadap target. Proses ini melibatkan pemeriksaan terhadap konektivitas jaringan (ping), analisis port untuk melihat layanan yang terbuka, serta identifikasi kerentanan yang mungkin dapat dimanfaatkan. Jika hasil scanning menunjukkan adanya potensi celah keamanan, penelitian dilanjutkan ke tahap Exploitation, di mana celah keamanan tersebut dimanfaatkan untuk mendapatkan akses ke sistem secara tidak sah. Tahap ini melibatkan teknik eksploitasi berbasis web yang dirancang untuk mengevaluasi dampak nyata dari kerentanan tersebut.

Tahap berikutnya adalah Exploitation and Maintaining Access, yang berfokus pada eksploitasi lanjutan untuk menjaga keberlanjutan akses ke sistem target. Proses ini juga mencakup dokumentasi rinci dari hasil eksploitasi untuk digunakan sebagai bahan analisis dan evaluasi keamanan. Penelitian ini diakhiri dengan penyusunan laporan akhir yang mencakup seluruh proses dari awal hingga akhir, mulai dari pengumpulan data, identifikasi kerentanan, eksploitasi, hingga langkah-langkah mitigasi yang dapat dilakukan.

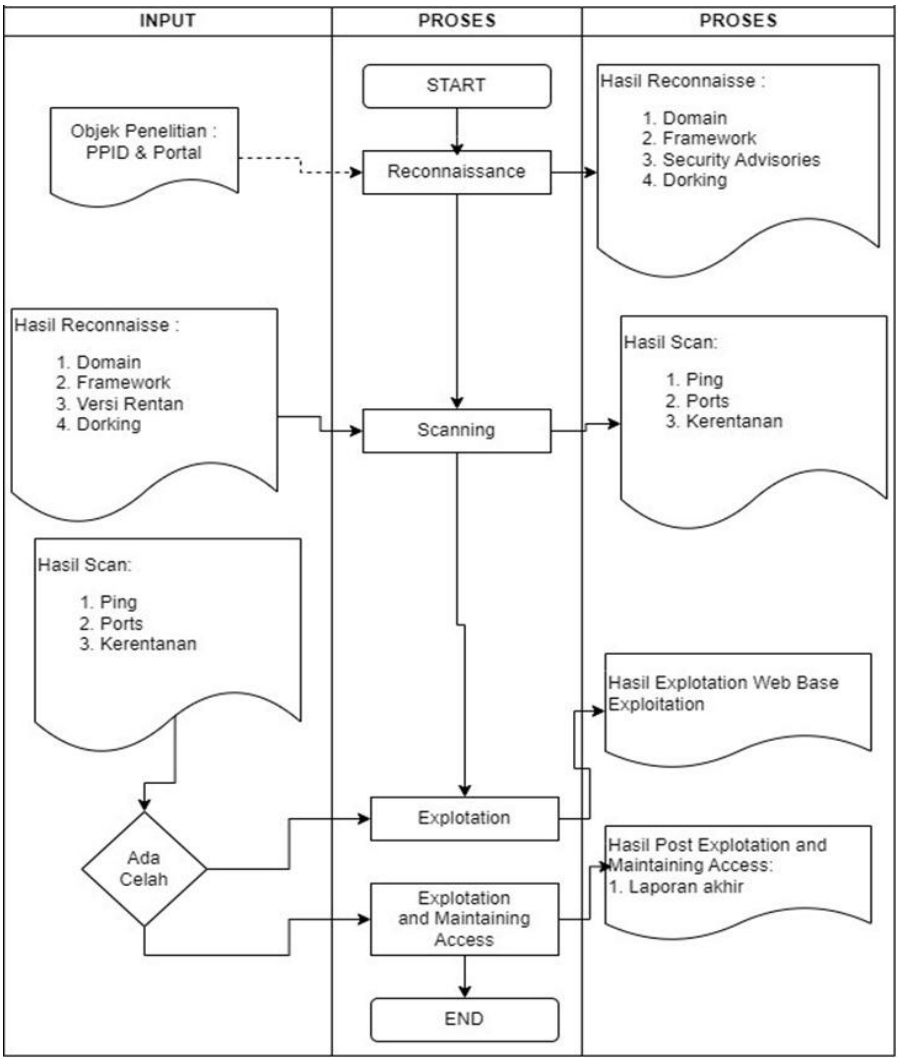
Tahapan akhir adalah penulisan laporan dan artikel publikasi. Laporan akhir ini menjadi kontribusi penting dalam penelitian akademik karena memberikan panduan kepada para pemangku kepentingan untuk meningkatkan keamanan sistem, menutup kerentanan, dan mencegah serangan serupa di masa depan. Penelitian ini juga menekankan pentingnya pendekatan etis dalam pengujian keamanan dengan tujuan meningkatkan keandalan dan integritas sistem berbasis web.

Variabel-variabel yang diteliti pada penelitian untuk analisis *assesment vulnerability* pada *website* dan aplikasi publik di Diskominfotik Kota Banda Aceh ini adalah sebagai berikut:

A. Variabel Independen:

Vol. 4, No. 2 - October 2024, Hal. 87-91
DOI: 10.59395/janitra.v4i2.205

1. Penggunaan Alat Pemindaian Keamanan: Variabel ini dapat diukur dengan frekuensi penggunaan alat pemindaian keamanan seperti Nessus atau Skipfish untuk melakukan skrining dan deteksi kerentanan pada website dan aplikasi publik yang dikelola oleh Diskominfotik Kota Banda Aceh. Contoh pertanyaan penelitian terkait variabel ini adalah: "Sejauh mana Diskominfotik Kota Banda Aceh menggunakan alat pemindaian keamanan untuk menilai kerentanan pada website dan aplikasi publik mereka?"



Gambar 1. Tahapan Penelitian

2. Penerapan Kebijakan Keamanan: Variabel ini dapat diukur dengan mengevaluasi kepatuhan Diskominfotik Kota Banda Aceh terhadap kebijakan keamanan yang telah ditetapkan dalam mengelola website dan aplikasi publik. Contoh pertanyaan penelitian terkait variabel ini adalah: "Apakah kebijakan keamanan yang telah ditetapkan oleh Diskominfotik Kota Banda Aceh diterapkan secara konsisten pada website dan aplikasi publik mereka?"
3. Pelaksanaan Model Kematangan Keamanan: Variabel ini dapat diukur dengan mengidentifikasi penerapan langkah-langkah dan praktik-praktik keamanan yang dianalisis berdasarkan model kematangan keamanan tertentu seperti CMMI, ISO/IEC 27001, atau kerangka kerja keamanan lainnya. Contoh pertanyaan penelitian terkait variabel ini adalah: "Sejauh mana Diskominfotik Kota Banda Aceh telah menerapkan model kematangan keamanan dalam mengelola website dan aplikasi publik mereka?"

B. Variabel Dependen:

1. Tingkat Kerentanan Keamanan: Variabel ini dapat diukur dengan melakukan pemindaian keamanan dan pengujian penetrasi untuk mengidentifikasi kerentanan dan celah keamanan yang ada pada website dan aplikasi publik di Diskominfotik Kota Banda Aceh. Contoh pertanyaan

Vol. 4, No. 2 - October 2024, Hal. 87-91
DOI: 10.59395/janitra.v4i2.205

penelitian terkait variabel ini adalah: "Berapa tingkat kerentanan keamanan yang ditemukan pada website dan aplikasi publik di Diskominfotik Kota Banda Aceh?"

2. Tingkat Kematangan Keamanan: Variabel ini dapat diukur dengan menerapkan model kematangan keamanan tertentu dan menilai sejauh mana website dan aplikasi publik di Diskominfotik Kota Banda Aceh sesuai dengan tingkat kematangan yang diinginkan. Contoh pertanyaan penelitian terkait variabel ini adalah: "Bagaimana tingkat kematangan keamanan secara keseluruhan pada website dan aplikasi publik di Diskominfotik Kota Banda Aceh berdasarkan model kematangan yang digunakan?"

C. Variabel Kontrol:

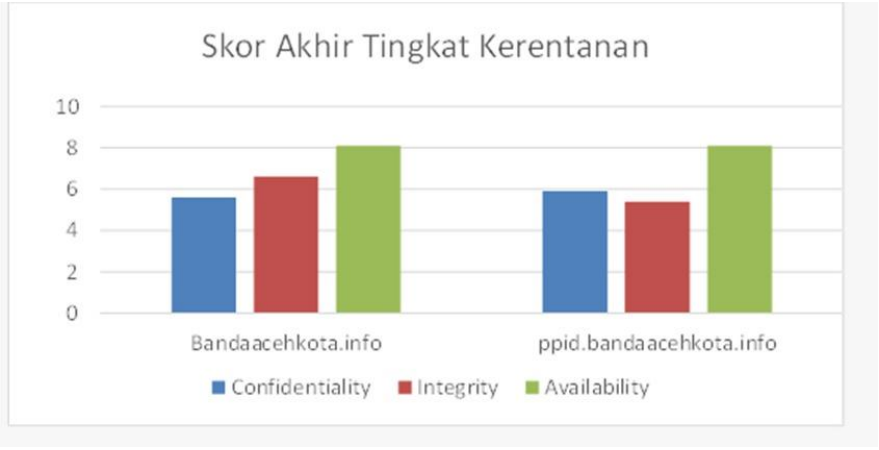
1. Ukuran Aplikasi: Variabel ini dapat diukur berdasarkan kompleksitas dan jumlah halaman serta fitur-fitur yang ada pada website dan aplikasi publik di Diskominfotik Kota Banda Aceh. Contoh pertanyaan penelitian terkait variabel ini adalah: "Apakah ukuran dan kompleksitas website dan aplikasi publik berpengaruh pada tingkat kerentanan dan kematangan keamanan?"
2. Jenis Aplikasi: Variabel ini dapat diukur berdasarkan jenis-jenis aplikasi publik yang dikelola oleh Diskominfotik Kota Banda Aceh, misalnya aplikasi e-government, aplikasi informasi publik, atau aplikasi layanan publik lainnya. Contoh pertanyaan penelitian terkait variabel ini adalah: "Apakah jenis aplikasi publik berpengaruh pada tingkat kerentanan dan kematangan keamanan?"

3. HASIL DAN PEMBAHASAN

Hasil penelitian pada masing-masing Aplikasi Portal Kota Banda Aceh Bandaacehkota.info dan ppidv2.bandaacehkota.info di Dinas Komunikasi Informatika dan Statistik kota Banda Aceh mendapatkan hasil pengujian kerentanan diketahui rata-ratanya, maka perlu dilakukan penghitungan Confidentility, Integrity dan Availability secara keseluruhan, adapun hasil akhirnya sebagai berikut yang dapat dilihat pada Tabel 1, dan skor akhir Tingkat kerentanan dapat dilihat pada Gambar 2.

Tabel 1. Skor Akhir Tingkat Kerentanan

No.	Web	Confidentiality	Integrity	Availability	Rata-Rata	Peringkat Kualitatif
1	Aplikasi I	5.6	6.6	8.1	6.8	Medium
2	Aplikasi II	5.9	5.4	8.1	6.5	Medium
Level Kerentanan		5.8	6	8.1	6.6	Medium



Gambar 2. Skor Akhir Tingkat Kerentanan

4. KESIMPULAN

Setelah melakukan pengujian kerentanan terhadap website Dinas Komunikasi Informatika dan Statistik Kota Banda Aceh, dapat disimpulkan bahwa: Kerentanan Sistem Informasi pada web aplikasi dapat diketahui dengan menggunakan metode VAPT Life Cycle dengan tahapan Identyfing Scope, Information Gathering, Vulnerability Scanning, False Positive Analysis, Vulnerability Exploitation,

Vol. 4, No. 2 - October 2024, Hal. 87-91
DOI: 10.59395/janitra.v4i2.205

dan Generating Report. Kemudian untuk mengukur tingkat kerentanannya menggunakan Common Vulnerability Scoring System (CVSS) sehingga dapat dipetakan tingkat kerentanannya ke dalam kategori critical, high, medium, low, dan none. Setelah dilakukan pengujian kerentanan terhadap Web Aplikasi di Dinas Komuninakasi Informatika dan Statistik Kota Banda Aceh memiliki 4 kerentanan. Dari 4 kerentanan tersebut 1 yang masuk kategori high dan 3 yang masuk kategori medium sehingga perlu segera diperbaiki. Adapun kerentanan tersebut ialah DNS Server Spoofed Request Amplification DDoS, SSL Certificate Cannot BeTrusted, DNS Server Cache Snooping Remote Information Disclosure, dan DNS Server Recursive Query Cache Poisoning Weakness.

DAFTAR PUSTAKA

[1] I. G. N. Mantra, M. S. Hartawan, H. Saragih, dan A. A. Rahman, "Web vulnerability assessment and maturity model analysis on Indonesia higher education," *Procedia Comput. Sci.*, vol. 161, hal. 1165–1172, 2019, doi: 10.1016/j.procs.2019.11.229.

[2] E. A. Sosiawan, "Evaluasi implementasi e-government pada situs web pemerintahan daerah di indonesia : prespektif content dan manajemen," *Semin. Nas. Inform.*, vol. 1, no. 5, hal. 88–98, 2008, [Daring]. Tersedia pada: http://edwi.dosen.upnyk.ac.id

[3] M. N. N. Sitokdana, "Evaluasi Implementasi eGovernment Pada Situs Web Pemerintah Kota Surabaya, Medan, Banjarmasin, Makassar dan Jayapura," *J. Buana Inform.*, vol. 6, no. 4, hal. 289–300, 2015, doi: 10.24002/jbi.v6i4.461.

[4] U. Ravindran dan R. V. Potukuchi, "A Review on Web Application Vulnerability Assessment and Penetration Testing," *Rev. Comput. Eng. Stud.*, vol. 9, no. 1, hal. 1–22, 2022, doi: 10.18280/rces.090101.

[5] H. N. Prasetyo, "a Review of Data Governance Maturity Level in Higher Education," *J. Ilm. Teknol. Infomasi Terap.*, vol. 3, no. 1, 2016, doi: 10.33197/jitter.vol3.iss1.2016.115.

[6] M. A. A. Hammoudeh, A. Alobaid, A. Alwabli, dan F. Alabdulmunim, "The Study on Assessment of Security Web Applications," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 23, hal. 120–135, 2021, doi: 10.3991/ijim.v15i23.27357.

[7] E. B. Setiawan dan A. Setiyadi, "Web vulnerability analysis and implementation," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 407, no. 1, 2018, doi: 10.1088/1757-899X/407/1/012081.

[8] S. Nagpure dan S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2017*, hal. 1–6, 2017, doi: 10.1109/ICCUBEA.2017.8463920.

[9] I. Mantra, A. Abd. Rahman, dan H. Saragih, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," *Int. J. Eng. Technol.*, vol. 9, no. 2, hal. 429–436, 2020, doi: 10.14419/ijet.v9i2.30581.

[10] W. V. Siregar, A. Hasibuan, dan M. D. Nurdin, "Pemanfaatan Aplikasi Pembelajaran Daring untuk Membangun Generasi Hebat," vol. 5, no. 2, hal. 86–90, 2021.

[11] M. Fathurrahman, Zulhelman, dan A. Aziz, "Vulnerability Assessment dan Penetration Test Pada Website MA/MTS Husnul Khatimah Kuningan," *ISAS Publ.*, vol. 8, no. 3, hal. 138–145, 2022.