Contents list avaliable at Directory of Open Access Journals (DOAJ)

JUTIN : Jurnal Teknik Industri Terintegrasi

Volume 8 Issue 4 2025, Page 3862-3874

ISSN: 2620-8962 (Online)

Journal Homepage: https://journal.universitaspahlawan.ac.id/index.php/jutin/index

Analisis Kerentanan Website Desa Sekecamatan Bengkalis Menggunakan *Vulnerability Assessment*

Muhammad Sani[1]✉, Muhammad Asep Subandri[1]

(1) Program Studi Keamanan Sistem Informasi, Jurusan Teknik Informatika, Politeknik Negeri Bengkalis, Riau, Indonesia

DOI: 10.31004/jutin.v8i4.48851

✉ Corresponding author:
[sanisans342@gmail.com]

Article Info

Kata kunci:
Keamanan Website;
Vulnerability Assessment;
OWASP ZAP;
Nmap;
Website Desa

Abstrak

Website desa digunakan sebagai sarana utama untuk memberikan layanan dan menyebarkan informasi kepada masyarakat. Namun, tanpa keamanan yang baik, website ini rentan terhadap serangan siber. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan website desa di Kecamatan Bengkalis menggunakan metode Vulnerability Assessment. Dalam penelitian ini delapan website desa diuji menggunakan alat Nmap dan OWASP ZAP untuk menemukan celah keamanan. Hasil pengujian menunjukkan adanya beberapa kelemahan dengan tingkat risiko yang berbeda, mulai dari High, Medium, Low, hingga Informational. Beberapa masalah yang ditemukan antara lain penggunaan pustaka JavaScript yang rentan, pengaturan keamanan yang kurang, serta risiko serangan seperti Clickjacking dan Cross-Site Scripting (XSS). Agar website lebih aman, penelitian ini menyarankan beberapa perbaikan, seperti memperbarui sistem keamanan, menambahkan perlindungan terhadap serangan, serta meningkatkan pengaturan keamanan website. Dengan adanya penelitian ini, diharapkan pemerintah desa dapat lebih memahami dan meningkatkan keamanan website mereka agar lebih terlindungi dari ancaman siber.

Keywords:
Website Security;
Vulnerability Assessment;
OWASP ZAP;
Nmap;
Village Website

Abstract

The village website is used as the main means of providing services and disseminating information to the community. However, without good security, these websites are vulnerable to cyber attacks. This research aims to analyze the level of vulnerability of village websites in Bengkalis District using the Vulnerability Assessment method. In this research, eight village websites were tested using the Nmap and OWASP ZAP tools to find security gaps. The test results show that there are several weaknesses with different risk levels, ranging from High, Medium, Low, to Informational. Some of the problems found include the use of vulnerable JavaScript libraries, inadequate security settings, and the risk of attacks such as Clickjacking and Cross-Site Scripting (XSS). To make websites safer, this research suggests several improvements, such as updating the security system, adding

Received 21 July 2025; Received in revised form 28 July 2025 year; Accepted 16 August 2025
Available online 2 October 2025 /

protection against attacks, and improving website security settings. With this research, it is hoped that village governments can better understand and improve the security of their websites so that they are better protected from cyber threats.

1. PENDAHULUAN

Perkembangan teknologi website telah membawa perubahan besar dalam cara lembaga daerah dan pemerintah di Indonesia menyampaikan serta mengelola informasi. Website kini menjadi media utama dalam menyebarluaskan informasi, menjadikannya alat penting bagi lembaga pemerintah, termasuk desa-desa di Kecamatan Bengkalis, untuk memberikan pelayanan kepada masyarakat. Namun, sejalan dengan kemajuan teknologi, ancaman serangan siber yang semakin kompleks juga meningkat, menjadikan keamanan aplikasi website sebagai aspek krusial. Keamanan ini tidak hanya bertujuan untuk melindungi integritas, kerahasiaan, dan ketersediaan data di dunia digital, tetapi juga untuk menghadapi tantangan dari beragam serangan siber yang semakin canggih(Dinarto 2024).

Ancaman utama terhadap sistem digital adalah serangan siber, yang dapat berupa gangguan terhadap sistem elektronik, seperti serangan virus, pencurian data, penyalahgunaan informasi pribadi, pelanggaran hak kekayaan intelektual, perusakan tampilan web (web defacement), serta gangguan akses layanan elektronik[2]. Pengguna dalam bidang keamanan siber berkembang pesat seiring dengan kemajuan teknologi. Jumlah penelitian terkait keamanan siber juga terus meningkat. Salah satu studi terkait penilaian kerentanan mengevaluasi keamanan situs web dengan menggunakan metode Vulnerability Assessment(Sari et al. 2024).

Modernisasi dalam pemerintahan menjadi suatu keharusan seiring perkembangan zaman yang memengaruhi berbagai aspek kehidupan, termasuk bidang ilmu pemerintahan. Teknologi yang terus berkembang diharapkan dapat memberikan kemudahan bagi semua kalangan. Salah satu hasil dari digitalisasi yang kini banyak digunakan adalah aplikasi berbasis web yang telah diterapkan pemerintah untuk meningkatkan kualitas pelayanan publik sekaligus mendukung kesejahteraan masyarakat. Sistem informasi berbasis teknologi saat ini dianggap mampu memenuhi kebutuhan masyarakat secara lebih efektif dan efisien. Transformasi digital dalam layanan pemerintahan ini dikenal dengan istilah e-Government. Menurut Zakiyah dan Karim (2017), e-Government adalah proses pengadaptasian konsep birokrasi ke era digital dengan menciptakan lingkungan berbasis teknologi dalam seluruh aktivitas pemerintahan, baik di tingkat pusat, daerah, maupun desa. Proses ini memungkinkan setiap unit dalam struktur pemerintahan bekerja secara lebih optimal(Sari et al. 2024).

Namun, tidak sedikit individu yang menyalahgunakan kemajuan teknologi dengan melakukan peretasan, penipuan, dan kejahatan siber yang menyasar individu, bisnis, perusahaan, hingga organisasi pemerintah. Ancaman terhadap keamanan sistem informasi perlu diwaspadai, baik yang berasal dari dalam maupun luar sistem, karena dapat menyebabkan ketidakstabilan. Berbagai faktor seperti mekanisme, perusahaan, kelompok, hingga individu bisa menjadi penyebab yang mengganggu sistem dan merusak data. Karena setiap serangan pasti melibatkan ancaman, maka langkah-langkah keamanan sistem informasi harus berfokus pada identifikasi dan prediksi ancaman tersebut guna mengurangi ketidakstabilan sistem yang disebabkan oleh serangan. Hal ini dapat dilakukan dengan memprediksi ancaman sebelum serangan terjadi(Firman Syech 2023)

Kerentanan pada aplikasi web dapat bervariasi, tergantung pada modul, pustaka, CMS, dan basis data yang digunakan. Hal ini membuat aplikasi web memiliki banyak titik lemah yang berpotensi menjadi sasaran serangan. Penilaian kerentanan merupakan metode untuk mengidentifikasi kelemahan dalam infrastruktur. Dalam konteks sistem TI, kerentanan dapat diartikan sebagai potensi kelemahan yang, jika dieksploitasi, dapat memicu serangan terhadap sistem. Oleh karena itu, diperlukan evaluasi terhadap celah keamanan pada situs web di Kecamatan Bengkalis agar sistem lebih efisien dan terlindungi dari serangan pihak yang tidak bertanggung jawab(Budiman, Ahdan, and Aziz 2021).

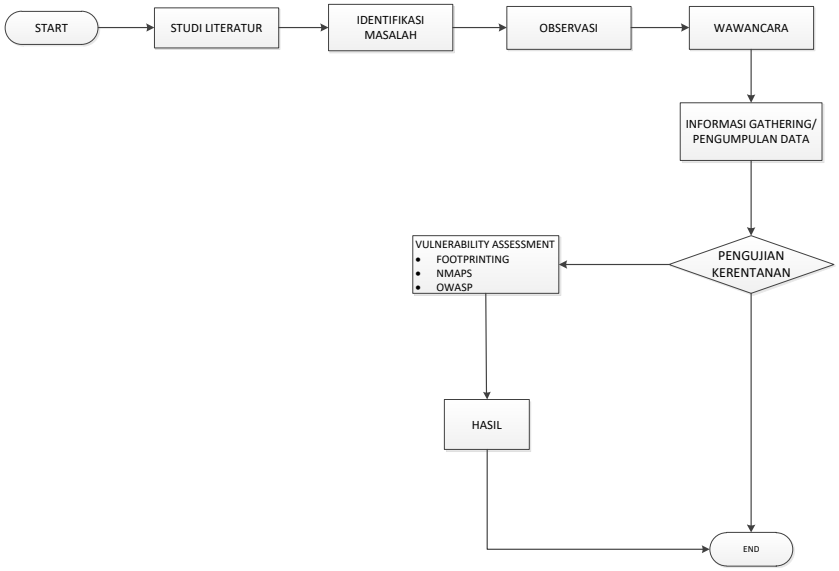
Metode Vulnerability Assessment digunakan untuk memindai situs web guna mendeteksi kerentanannya terhadap serangan siber, termasuk teknik peretasan yang mengeksploitasi celah keamanan pada aplikasi atau situs web. Celah ini sering muncul akibat input yang tidak difilter dengan baik selama pengembangan, sehingga memudahkan terjadinya penyalahgunaan.Vulnerability Assessment adalah proses yang bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi potensi kelemahan dalam sistem, jaringan, atau aplikasi. Proses ini dilakukan untuk menemukan celah yang mungkin dimanfaatkan oleh pihak yang tidak berwenang, seperti peretas, guna melakukan serangan. Langkah ini penting untuk meningkatkan keamanan dan melindungi sistem dari ancaman(Sari et al. 2024).

Untuk meningkatkan keamanan situs web desa-desa di Kecamatan Bengkalis, metode Vulnerability Assessment dapat diterapkan. Metode ini merupakan proses identifikasi risiko dan kelemahan dalam aplikasi, jaringan komputer, sistem, serta komponen lain dari ekosistem teknologi. Proses ini mencakup evaluasi menyeluruh terhadap keamanan informasi, hasil pemindaian jaringan, konfigurasi sistem, tata kelola, kesadaran keamanan dari semua pihak yang terlibat, serta keamanan fisik. Tujuan utamanya adalah untuk menemukan dan menutup kelemahan kritis sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab(Adam Kilian 2023)

Penelitian ini akan menganalisis kerentanan website desa Sekecamatan Bengkalis menggunakan metode Vulnerability Assessment. Fokus utamanya adalah mengidentifikasi potensi celah keamanan, menilai tingkat keparahan serta kemungkinan eksploitasi, dan memberikan rekomendasi perbaikan untuk meningkatkan keamanan situs web tersebut. Diharapkan, langkah ini dapat memberikan kontribusi positif dalam menjaga keberlanjutan informasi dan layanan desa di Kecamatan Bengkalis serta melindungi data yang ada. Oleh karena itu, diperlukan penyelidikan menyeluruh terhadap kemungkinan celah keamanan pada web desa di Kecamatan Bengkalis untuk mengurangi risiko serangan siber di masa mendatang.

2. METODE

Penelitian ini menganalisis kerentanan situs web desa di Kecamatan Bengkalis dengan menggunakan metode vulnerability assessment. Tahapan penelitian dilakukan secara sistematis untuk memperoleh informasi yang diperlukan dalam menganalisis keamanan situs web.



Gambar 1. Tahapan Peneltian

Tahapan-tahapan yang diterapkan dalam penelitian ini adalah sebagai berikut:

1) Studi literatur: Tahap penelitian ini melakukan pengumpulan berbagai informasi. Tujuan dari pengumpulan sumber literatur ini adalah untuk mendapatkan informasi yang relevan dan mendalam tentang serangan celah keamanan ini, serta memperoleh dasar teoritis yang kuat dalam penelitian.
2) Identifikasi Masalah: Tahap ini dilakukan untuk menemukan dan merumuskan permasalahan. Masalah utama dalam penelitian ini adalah belum pernah dilakukan vulnerability assessment pada situs web desa di Kecamatan Bengkalis. Kondisi ini menyebabkan potensi celah keamanan yang dapat dimanfaatkan pihak tidak bertanggung jawab.
3) Observasi: Peneliti melakukan observasi lapangan untuk memperoleh gambaran umum kondisi website desa. Observasi dilakukan secara langsung dengan tujuan agar hasil yang diperoleh lebih valid dan menjadi dasar untuk tahap berikutnya.
4) Wawancara: Pengumpulan data juga dilakukan melalui wawancara langsung dengan pengelola situs web desa di Kecamatan Bengkalis. Pertanyaan yang diajukan berfokus pada proses pengelolaan situs.
5) Pengumpulan data: Tahap ini meliputi pengumpulan informasi mengenai daftar desa di Kecamatan Bengkalis beserta alamat situs web resmi yang digunakan oleh masing-masing desa. Data tersebut digunakan sebagai dasar pelaksanaan vulnerability assessment.

6) Metode *vulnerability assessment* digunakan untuk mengidentifikasi, mengevaluasi, dan mengukur potensi celah keamanan. Tujuannya adalah mengetahui apakah sistem memiliki kerentanan dan memberikan rekomendasi perbaikan. Proses pengujian meliputi beberapa teknik berikut:
   a. Footprinting Teknik ini bertujuan mengumpulkan informasi publik terkait situs web seperti nama domain, alamat IP, kontak admin, masa berlaku domain, dan informasi teknis lainnya. Pengujian dilakukan menggunakan layanan who.is.
   b. Nmap digunakan untuk mendeteksi port yang terbuka pada server. Hasil pemindaian menunjukkan status port yang berpotensi menjadi jalur masuk serangan.
   c. Tool OWASP Zed Attack Proxy digunakan untuk melakukan pengujian keamanan aplikasi web secara otomatis. Tool ini memindai celah umum seperti XSS, SQL injection, dan konfigurasi yang tidak aman.
7) Analisa Hasil: Tahap terakhir adalah menganalisis hasil pemindaian kerentanan yang diperoleh. Kerentanan yang teridentifikasi dinilai berdasarkan tingkat keparahan dan potensi dampak. Hasil analisis digunakan untuk menyusun rekomendasi perbaikan agar situs web desa lebih aman dari ancaman serangan siber.

3. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil penelitian mengenai kerentanan website desa di Kecamatan Bengkalis. Pemaparan dilakukan mulai dari proses pengumpulan data, hasil pemindaian, hingga analisis kerentanan berdasarkan standar OWASP Top 10 (2021).

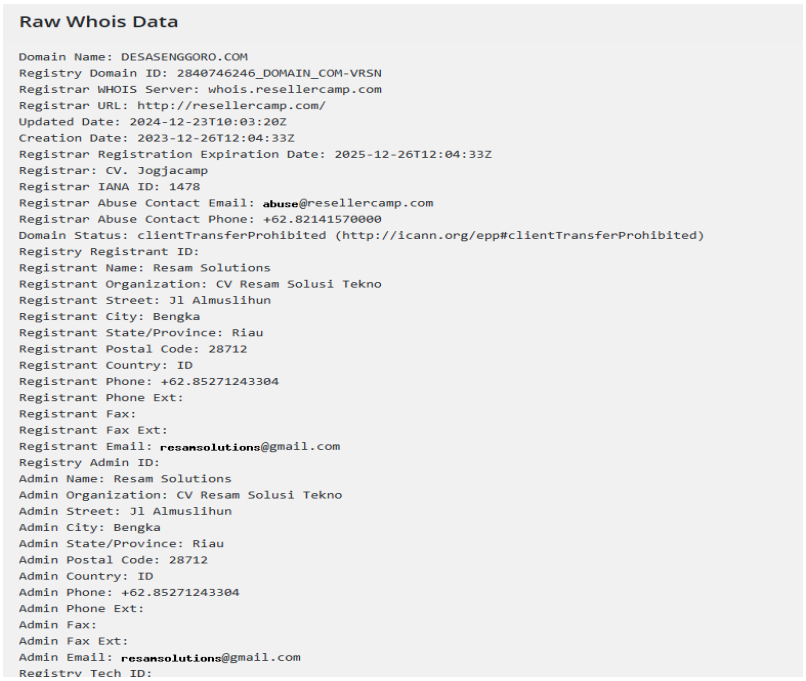
Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan untuk memperoleh daftar website desa di Kecamatan Bengkalis yang menjadi objek analisis. Data diperoleh melalui observasi langsung dan penelusuran daring terhadap portal resmi desa yang aktif. Dari hasil pengumpulan data, diperoleh delapan website desa yang memenuhi kriteria penelitian, yaitu dapat diakses, memiliki domain aktif, dan digunakan sebagai sarana penyebaran informasi publik. Pada tahap ini juga dikumpulkan informasi awal mengenai setiap website, meliputi alamat domain, status aktif, teknologi yang digunakan, serta hasil penelusuran data WHOIS. Informasi tersebut digunakan sebagai dasar untuk proses pemindaian kerentanan pada tahap berikutnya.

Tabel 1. Domain Website Kecamatan Bengkalis

Nama Desa	Domain Website
Kelurahan Bengkalis Kota	https://kelurahankota.bengkaliskab.go.id/
Kelurahan Damon	https://kelurahandamon.bengkaliskab.go.id/
Kelurahan Rimbas Sekampung	https://www.kelurahanrimbasekampung.com/
Desa Senggoro	https://www.desasenggoro.com/
Desa Pematang Duku	https://pematangduku.desa.id/
Desa Pematang Duku Timur	https://pematangdukutimur.id/
Desa Prapat Tunggal	https://prapattunggaldesa.id/
Desa Pangkalan Batang Barat	https://desapangkalanbatangbarat.com/

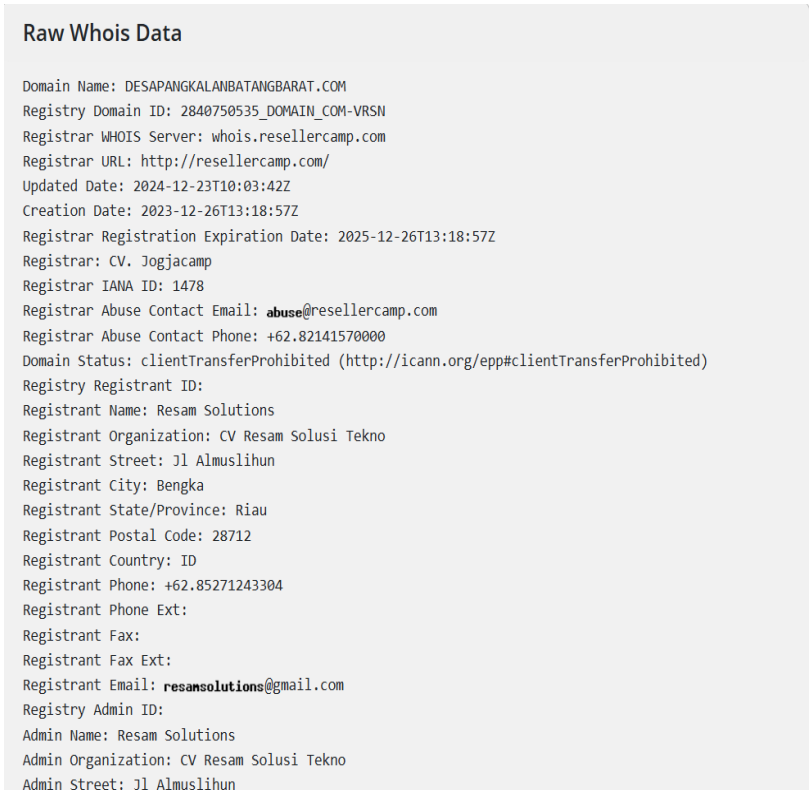
Sebagai contoh, Gambar 2 menampilkan hasil penelusuran data WHOIS untuk domain desasenggoro.com. Informasi WHOIS ini memuat registrar, tanggal pendaftaran, alamat IP, serta detail teknis lainnya yang digunakan untuk tahap awal identifikasi keamanan. Data WHOIS yang ditampilkan hanya mewakili dua domain dengan tingkat kerentanan paling tinggi.



Raw Whois Data

```
Domain Name: DESASENGGORO.COM
Registry Domain ID: 2840746246_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.resellercamp.com
Registrar URL: http://resellercamp.com/
Updated Date: 2024-12-23T10:03:20Z
Creation Date: 2023-12-26T12:04:33Z
Registrar Registration Expiration Date: 2025-12-26T12:04:33Z
Registrar: CV. Jogjacamp
Registrar IANA ID: 1478
Registrar Abuse Contact Email: abuse@resellercamp.com
Registrar Abuse Contact Phone: +62.82141570000
Domain Status: clientTransferProhibited (http://icann.org/epp#clientTransferProhibited)
Registry Registrant ID:
Registrant Name: Resam Solutions
Registrant Organization: CV Resam Solusi Tekno
Registrant Street: Jl Almuslihun
Registrant City: Bengka
Registrant State/Province: Riau
Registrant Postal Code: 28712
Registrant Country: ID
Registrant Phone: +62.85271243304
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: resansolutions@gmail.com
Registry Admin ID:
Admin Name: Resam Solutions
Admin Organization: CV Resam Solusi Tekno
Admin Street: Jl Almuslihun
Admin City: Bengka
Admin State/Province: Riau
Admin Postal Code: 28712
Admin Country: ID
Admin Phone: +62.85271243304
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: resansolutions@gmail.com
Registry Tech ID:
```

Gambar 2. Hasil Pemindaian WHOIS untuk domain desa Senggoro



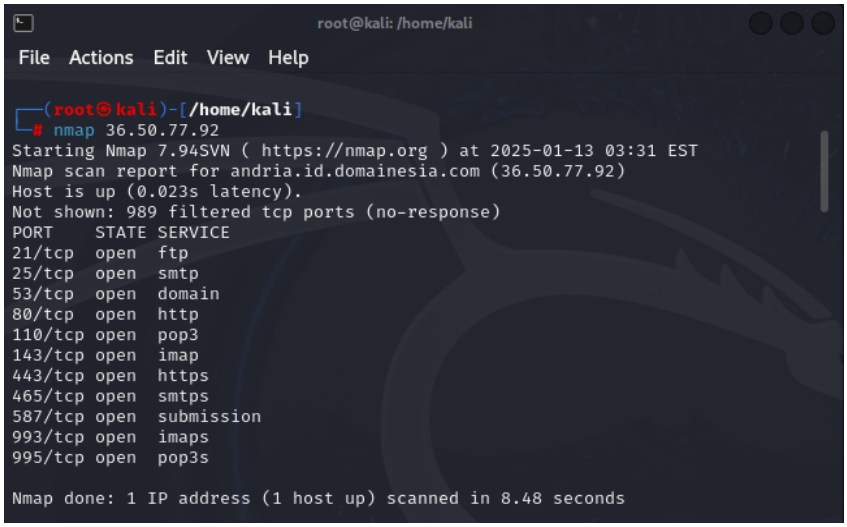
Raw Whois Data

```
Domain Name: DESAPANGKALANBATANGBARAT.COM
Registry Domain ID: 2840750535_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.resellercamp.com
Registrar URL: http://resellercamp.com/
Updated Date: 2024-12-23T10:03:42Z
Creation Date: 2023-12-26T13:18:57Z
Registrar Registration Expiration Date: 2025-12-26T13:18:57Z
Registrar: CV. Jogjacamp
Registrar IANA ID: 1478
Registrar Abuse Contact Email: abuse@resellercamp.com
Registrar Abuse Contact Phone: +62.82141570000
Domain Status: clientTransferProhibited (http://icann.org/epp#clientTransferProhibited)
Registry Registrant ID:
Registrant Name: Resam Solutions
Registrant Organization: CV Resam Solusi Tekno
Registrant Street: Jl Almuslihun
Registrant City: Bengka
Registrant State/Province: Riau
Registrant Postal Code: 28712
Registrant Country: ID
Registrant Phone: +62.85271243304
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: resansolutions@gmail.com
Registry Admin ID:
Admin Name: Resam Solutions
Admin Organization: CV Resam Solusi Tekno
Admin Street: Jl Almuslihun
```

Gambar 3. Hasil pemindaian WHOIS untuk domain desa senggoro

Berdasarkan hasil penelusuran WHOIS terhadap delapan website desa di Kecamatan Bengkalis, dua domain yaitu desasenggoro.com dan desapangkalanbatangbarat.com ditemukan memiliki kelemahan yang perlu diperbaiki. Informasi pemilik domain seperti nama, alamat, dan email masih terlihat jelas di data WHOIS. Kondisi ini dapat dimanfaatkan penyerang untuk melakukan serangan sosial, termasuk pengiriman email palsu (phishing) dan pencurian data. Selain itu, kedua domain tersebut belum menggunakan mekanisme Domain Name System Security Extensions (DNSSEC) yang berfungsi melindungi integritas catatan DNS agar tidak dimanipulasi. Hal ini membuat website berisiko diarahkan ke situs palsu. Untuk meningkatkan keamanan, pemilik domain disarankan menyembunyikan informasi pribadi pada WHOIS, mengaktifkan DNSSEC, dan melakukan pemeriksaan keamanan secara rutin.

Selain data WHOIS, proses pengumpulan data juga mencakup pemindaian port menggunakan Nmap pada delapan website desa. Pemindaian ini bertujuan untuk mengidentifikasi port yang terbuka sebagai bahan awal untuk analisis tahap berikutnya. Gambar 4 menampilkan hasil pemindaian Nmap pada salah satu server yang menunjukkan daftar port terbuka.



Gambar 4. Contoh Hasil pemindaian awal port menggunakan Nmap

Pemindaian kerentanan System

Tahap pemindaian ini dilakukan untuk mengidentifikasi celah keamanan pada delapan website desa di Kecamatan Bengkalis menggunakan *tools* OWASP ZAP versi 2.16.0. Pemindaian dilakukan dengan metode *Automated Scan* dengan cara memasukkan alamat URL masing-masing website desa. Hasil pemindaian menunjukkan adanya berbagai kerentanan dengan tingkat risiko yang berbeda. Ringkasan hasil pemindaian berdasarkan jenis kerentanan, tingkat risiko, jumlah kasus, dan website yang terdampak disajikan pada Tabel 2.

Tabel 2. Jumlah Jenis kerentanan pada website desa sekecamatan bengkalis

No	Jenis kerentanan	Risk	Count	Website
1	Vulnerable JS Library	High	1	Kotabengkaliskab.go.id
2	Cloud Metadata Potentially Exposed	High	4	Kotabengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Desapangkalanbatangbarat.com.
3	Content Security Policy (CSP) Header Not Set	Medium	8	Kotabengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, Pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
4	Hidden File Found	Medium	4	bengkaliskab.go.id, kelurahanrimbasekampung.com, Pematangduku.desa.id, Desapangkalanbatangbarat.com
5	Missing Anti-clickjacking Header	Medium	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
6	Absence of Anti-CSRF Tokens	Medium		Pematangduku.desa.id,
7	Vulnerable JS Library	Medium	2	Pematangduku.desa.id, pematangdukutimur.id,
8	Big Redirect Detected (Potential Sensitive Information Leak)	Low	2	bengkaliskab.go.id, Damonbengkaliskab.go.id,
9	Cookie No HttpOnly Flag	Low	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com

No	Jenis kerentanan	Risk	Count	Website
10	Cookie Without Secure Flag	Low	7	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
11	Cross-Domain JavaScript Source File Inclusion	Low	5	bengkaliskab.go.id, Damonbengkaliskab.go.id, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id,
12	Strict-Transport-Security Header Not Set	Low	7	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id,
13	X-Content-Type-Options Header Missing	Low	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
14	Application Error Disclosure	Low	1	Pematangduku.desa.id,
15	Cookie without SameSite Attribute	Low	1	Pematangduku.desa.id,
16	Server Leaks Information via "X-Powered-By" HTTP Response Header	Low	1	Pematangduku.desa.id,
17	Timestamp Disclosure - Unix	Low	4	Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Desapangkalanbatangbarat.com
18	Secure Pages Include Mixed Content	Low	1	Desapangkalanbatangbarat.com
19	Information Disclosure - Suspicious Comments	Informational	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
20	Modern Web Application	Informational	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
21	Re-examine Cache-control Directives	Informational	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
22	Retrieved from Cache	Informational	2	bengkaliskab.go.id, Pematangduku.desa.id
23	Session Management Response Identified	Informational	8	bengkaliskab.go.id, Damonbengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, pematangdukutimur.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
24	User Agent Fuzzer	Informational	6	bengkaliskab.go.id, kelurahanrimbasekampung.com, Desasenggoro.com, Pematangduku.desa.id, prapattunggaldesa.id, Desapangkalanbatangbarat.com
25	User Controllable HTML Element Attribute (Potential XSS)	Informational	3	bengkaliskab.go.id, Damonbengkaliskab.go.id, Prapattunggaldesa.id
	Total			117

Berdasarkan hasil pemindaian, total 25 jenis kerentanan berhasil diidentifikasi dengan tingkat risiko yang bervariasi. Rinciannya adalah:

a. Tingkat Risiko Tinggi (High): Satu kasus kerentanan berupa Vulnerable JS Library ditemukan. Kerentanan ini berpotensi memungkinkan eksekusi kode berbahaya melalui pustaka JavaScript yang tidak aman.
b. Tingkat Risiko Sedang (Medium): Sebanyak 23 temuan termasuk Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, dan Absence of Anti-CSRF Tokens. Kerentanan ini dapat meningkatkan risiko serangan seperti clickjacking dan CSRF.
c. Tingkat Risiko Rendah (Low): Sebanyak 45 temuan termasuk Cookie No HttpOnly Flag dan Strict-Transport-Security Header Not Set. Kerentanan ini berpotensi menyebabkan kebocoran informasi dan serangan man-in-the-middle.
d. Tingkat Informasi (Informational): Sebanyak 43 temuan bersifat informasional seperti Suspicious Comments, Modern Web Application, dan Session Management Response Identified. Temuan ini tidak langsung berbahaya, namun menunjukkan area yang memerlukan perbaikan.

Untuk memberikan gambaran yang lebih jelas mengenai karakteristik setiap temuan, berikut adalah penjelasan singkat dari masing-masing jenis kerentanan yang teridentifikasi:

a. Vulnerable JS Library
   Website masih menggunakan pustaka JavaScript versi lama yang memiliki kelemahan keamanan sehingga berpotensi dimanfaatkan untuk mengambil alih sistem atau mencuri data pengguna.
b. Cloud Metadata Potentially Exposed
   Metadata server yang sensitif dapat diakses secara publik dan berpotensi digunakan penyerang untuk mendapatkan akses tidak sah.
c. Content Security Policy (CSP) Header Not Set
   Tidak adanya CSP memungkinkan eksekusi script berbahaya (XSS) dari sumber luar.
d. Hidden File Found
   Ditemukannya file atau direktori tersembunyi yang dapat diakses dari luar dan berpotensi mengandung data atau konfigurasi sensitif.
e. Missing Anti-clickjacking Header
   Website tidak melindungi diri dari teknik clickjacking yang dapat menipu pengguna agar mengklik elemen yang tidak disadari.
f. Absence of Anti-CSRF Tokens
   Tidak adanya token anti-CSRF memungkinkan serangan yang memaksa pengguna melakukan tindakan tertentu tanpa sepengetahuan mereka.
g. Big Redirect Detected (Sensitive Information Leak)
   Pengalihan (redirect) berulang dapat menyebabkan data sensitif terbawa saat berpindah halaman.
h. Cookie No HttpOnly Flag
   Cookie tidak diberi atribut HttpOnly sehingga dapat diakses oleh JavaScript, yang berpotensi dicuri melalui serangan XSS.
i. Cookie Without Secure Flag
   Cookie dapat terkirim melalui koneksi HTTP yang tidak aman, sehingga rentan disadap.
j. Cross-Domain JavaScript Source File Inclusion
   Website memuat JavaScript dari domain eksternal, yang dapat disalahgunakan jika domain sumber disusupi.
k. Strict-Transport-Security Header Not Set
   Website tidak memaksa penggunaan HTTPS, sehingga data pengguna dapat disadap.
l. X-Content-Type-Options Header Missing
   Tidak adanya pengaturan ini dapat menyebabkan browser menjalankan file dengan tipe yang salah dan membuka peluang eksekusi kode berbahaya.
m. Application Error Disclosure
   Pesan kesalahan menampilkan detail teknis yang dapat dimanfaatkan penyerang.
n. Cookie Without SameSite Attribute
   Cookie dapat digunakan lintas domain, sehingga meningkatkan risiko serangan CSRF.
o. Server Leaks Information via "X-Powered-By" Header
   Website menampilkan informasi teknologi yang digunakan, yang memudahkan penyerang mencari kerentanan spesifik.

p. Timestamp Disclosure - Unix
Informasi waktu sistem yang terbuka dapat dimanfaatkan untuk menganalisis pola aktivitas server.
q. Secure Pages Include Mixed Content
Halaman HTTPS memuat elemen dari sumber HTTP yang tidak aman, membuka peluang injeksi konten berbahaya.
r. Information Disclosure - Suspicious Comments
Komentar pada kode website mengandung catatan atau informasi yang seharusnya tidak terlihat publik.
s. Modern Web Application
Struktur aplikasi web modern yang kompleks memerlukan pengamanan tambahan.
t. Re-examine Cache-control Directives
Konfigurasi cache yang tidak tepat memungkinkan penyimpanan data sensitif secara lokal.
u. Retrieved from Cache
Halaman yang seharusnya tidak disimpan bisa dimuat ulang dari cache, membuka akses tidak sah ke data.
v. Session Management Response Identified
Mekanisme manajemen sesi terdeteksi, berpotensi menjadi target pembajakan sesi.
w. User Agent Fuzzer
Respon berbeda terhadap user-agent palsu dapat mengungkap informasi tambahan tentang struktur sistem.
x. User Controllable HTML Element Attribute (Potential XSS)
Atribut HTML yang dapat diubah pengguna memungkinkan eksekusi script berbahaya.

Penjelasan di atas menunjukkan bahwa sebagian besar kelemahan terjadi pada konfigurasi keamanan dasar yang belum diterapkan dengan baik, seperti header keamanan, pengaturan cookie, dan perlindungan anti-CSRF. Hasil ini akan menjadi dasar untuk pembahasan klasifikasi kerentanan terhadap standar OWASP Top 10 pada bagian selanjutnya.

Analisis Hasil Scan Map

Berdasarkan hasil scan Nmap dari delapan website desa yang ada di kecamatan bengkalis yaitu terdapat tiga website dengan ip yang sama (kelurahanrimbasekampung, desasenggoro, dan desapangkalanbatangbarat) dengan IP 36.50.77.92 memiliki lebih banyak port terbuka, sehingga lebih rentan terhadap serangan hacker, terutama jika konfigurasi layanan seperti FTP, SMTP, DNS, atau layanan email tidak aman.

Tabel 3. Analisa hasil Scan Nmap

No	Jenis dan Analisa	Rekomendasi
1	Port 21 (FTP) FTP (File Transfer Protocol) digunakan untuk transfer file antara komputer dan server. FTP tidak mengenkripsi data yang ditransfer, sehingga data seperti nama pengguna dan kata sandi dapat dengan mudah dilihat oleh pihak ketiga jika tidak diamankan. Selain itu, serangan seperti brute force (usaha menebak kata sandi) juga sering menargetkan FTP.	Nonaktifkan FTP dan gunakan SFTP (Secure File Transfer Protocol) atau FTPS (FTP Secure) yang menggunakan enkripsi untuk melindungi data saat ditransfer.
2	Port 25 (SMTP) SMTP (Simple Mail Transfer Protocol) digunakan untuk pengiriman email. Port ini sering disalahgunakan oleh spammer untuk mengirimkan email spam beberapa server memblokir port ini untuk mencegah spam.	Jika tidak digunakan untuk kirim email langsung dari server nonaktifkan port 25 gunakan port yang lebih aman seperti 465 atau 587 untuk mengirim email dan aktifkan autentikasi email artinya pengguna harus login sebelum bisa mengirim email dan terapkan pelindung email seperti SPF (Sender Policy Framework).

No	Jenis dan Analisa	Rekomendasi
3	Port 53 (DNS) DNS (Domain Name System) mengubah alamat IP menjadi nama domain (misalnya, 36.50.77.92 menjadi andria.id.domainesia.com). DNS bisa diserang dengan rekayasa DNS atau serangan DDoS (Distributed Denial of Service), yang mengarah pada ketidakstabilan layanan atau manipulasi DNS untuk redirect ke situs berbahaya.	Aktifkan DNSSEC (Domain Name System Security Extensions) untuk memverifikasi integritas data DNS dan mencegah serangan *cache poisoning*.
4	Port 80 (HTTP) HTTP (Hypertext Transfer Protocol) adalah protokol dasar untuk website yang digunakan untuk menampilkan halaman web. Karena tidak dienkripsi, HTTP rentan terhadap serangan seperti man-in-the-middle (MITM), di mana data yang dikirim bisa diambil oleh pihak yang tidak berwenang. Selain itu, aplikasi web yang berjalan di atas HTTP bisa terkena serangan seperti SQL injection atau Cross-Site Scripting (XSS).	Jangan gunakan HTTP karena data bisa dilihat siapa pun yang menyadap jaringan agar lebih aman alihkan semua pengunjung ke HTTPS secara otomatis menggunakan redirect (misalnya lewat .htaccess atau pengaturan server).
5	Port 443 (HTTPS) HTTPS adalah versi aman dari HTTP yang menggunakan enkripsi SSL/TLS untuk melindungi data yang dikirim. Meskipun dienkripsi, port ini tetap dapat diserang melalui kerentanan pada aplikasi web atau bug dalam sistem yang berjalan di atasnya.	Pastikan sertifikat SSL Anda valid dan tidak kadaluarsa terus gunakan HTTPS di seluruh halaman dan aktifkan TLS versi terbaru agar tidak ada bug pada website tersebut.
6	Port 110 (POP3) dan Port 995 (POP3S) POP3 (Post Office Protocol 3) digunakan untuk mengambil email dari server email, sementara POP3S adalah versi aman dengan enkripsi SSL. Serangan seperti man-in-the-middle (MITM) dan brute force sering menargetkan protokol ini, terutama yang tanpa enkripsi.	Jika pengguna email hanya pakai webmail atau IMAP, nonaktifkan POP3 (port 110) gunakan hanya POP3S (port 995) yang lebih aman karena sudah menggunakan enkripsi SSL dan gunakan password yang rumit agar tidak mudah ditebak.
7	Port 143 (IMAP) dan Port 993 (IMAPS) IMAP (Internet Message Access Protocol) digunakan untuk membaca email dari server email, sedangkan IMAPS adalah versi aman dengan enkripsi SSL. Sama seperti POP3, IMAP juga bisa diserang dengan serangan serupa seperti MITM dan brute force.	Nonaktifkan IMAP tanpa enkripsi (port 143) jika tidak di perlukan gunakan IMAPS (port 993) untuk memastikan koneksi email terenkripsi.
8	Port 465 (SMTPS) dan Port 587 (Submission) SMTPS (Simple Mail Transfer Protocol Secure) dan Submission digunakan untuk mengirim email dengan enkripsi. Port ini rentan terhadap penyalahgunaan spam dan eksploitasi kerentanan pada protokol pengiriman email yang aman.	Gunakan port 587 untuk pengiriman email oleh pengguna akhir, dan port 465 untuk SMTP dengan terenkripsi dan pastikan seluruh pengiriman email mewajibkan proses login agar tidak disalahgunakan.
9	Port 8080 (http-proxy) Port 8080 umumnya digunakan untuk layanan proxy web atau sebagai alternatif dari HTTP. Jika tidak dijaga dengan baik, port ini bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses halaman admin atau layanan sensitif lainnya.	Tutup port ini jika memang tidak sedang dipakai jika digunakan, pastikan halaman admin atau aplikasi web di balik port ini memiliki sistem login yang kuat dan batasi akses hanya untuk alamat IP tertentu melalui firewall jika ingin aman gunakan protokol HTTPS agar data yang dikirim aman.
10	Port 22 (SSH) Port 22 digunakan untuk mengakses server dari jarak jauh melalui SSH. Namun, jika tidak dilindungi dengan baik, port ini bisa menjadi sasaran serangan brute force, yaitu serangan untuk menebak kata sandi secara terus-menerus.	Ganti port SSH ke nomor lain yang tidak umum agar lebih sulit ditebak dan gunakan metode autentikasi dengan SSH key, bukan hanya password teru nonaktifkan akses langsung sebagai root atur firewall agar hanya IP tertentu yang bisa mengakses port ini gunakan tools seperti fail2ban untuk memblokir IP yang melakukan percobaan login berulang.
11	Port 3306 (MySQL) Port ini dipakai untuk mengakses layanan database MySQL. Jika terbuka ke jaringan luar tanpa pengamanan, maka data penting bisa dicuri atau diserang.	Jangan izinkan akses MySQL dari luar, cukup dari server lokal saja, bila memang harus diakses dari luar batasi hanya untuk IP tertentu dan gunakan koneksi yang terenkripsi seperti password yang kuat untuk semua pengguna database. pastikan MySQL selalu diperbarui ke versi terbaru agar aman dari celah keamanan.

Analisis Hasil Kerenteanan Sistem

Berdasarkan hasil scan menggunakan tools OWASP ZAP pada delapan website desa di kecamatan bengkalis sejumlah kerentanan telah teridentifikasi dan akan diuraikan sebagai berikut:

Tabel 4. Analisa hasil Kerentanan Sistem

No	Jenis dan Analisa	Rekomendasi
1	*Vulnerable JS Library* *Vulnerable JS Library* menemukan bahwa salah satu pustaka *JavaScript* yang digunakan website bengkaliskota memiliki kerentanan yang dikenal (High).	Pastikan pustaka JavaScript yang di pakai selalu diperbarui ke versi terbaru.
2	*Cloud Metadata Potentially Exposed* Informasi penting dari server cloud bisa diakses oleh orang yang tidak punya izin. Informasi ini bisa berupa nama server, alamat ip, atau kunci akses rahasia. Jika informasi ini jatuh ke tangan yang salah, server bisa diretas, data bisa dicuri, dan sistem bisa dirusak**.**	penting untuk membatasi dan mengamankan akses ke metadata service cloud dengan cara melindungi endpoint metadata (misalnya menggunakan IMDSv2 di AWS), mencegah serangan SSRF melalui validasi input dan pembatasan URL, serta memblokir akses jaringan yang tidak perlu ke metadata service.
3	Content Security Policy (CSP) Header Not Set kerentanan terhadap Header CSP yang tidak diatur. CSP merupakan lapisan keamanan tambahan untuk membantu mendeteksi dan mengurangi jenis serangan tertentu, termasuk Cross Site Scripting (XSS) dan Data Injection.	Pastikan pengaturan header CSP telah diterapkan pada server web, server aplikasi, dan komponen lain yang terlibat.
4	Missing Anti-clickjacking Header Tidak ada Content Security Policy (CSP) dan X-Frame-Options untuk melindungi dari serangan 'ClickJacking'. Ketika header keamanan konten seperti X-Frame Options tidak diatur, situs dapat menjadi rentan terhadap serangan Clickjacking, serangan yang memanfaatkan penyisipan halaman web.	Pastikan semua halaman website yang ditampilkan di situs atau aplikasi menggunakan header CSP atau X-Frame-Options.
5	Absence of Anti-CSRF Tokens token anti-CSRF yang tidak ditemukan dalam formulir pengiriman HTML. Token Anti-CSRF pada formulir pengiriman HTML untuk melindungi terhadap serangan CSRF.	Gunakan library yang atau framework yang tidak memnungkinkan kerentanan terjadi, misalnya memanfaatkan paket anti CSRF seperti OWASP CSRFGuard, untuk membantu melindungi aplikasi web dari serangan CSRF.
6	*Hidden File Found* Saat memeriksa direktori, menemukan file tersembunyi yang seharusnya tidak dapat diakses secara publik. File ini berpotensi mengungkapkan informasi sensitif atau konfigurasi internal yang bisa dimanfaatkan oleh penyerang.	Pastikan file-file penting seperti konfigurasi dan log yang tidak perlu diakses publik, disembunyikan atau dilindungi di server. Jangan biarkan orang luar mengaksesnya karena bisa berisi informasi yang sangat sensitif.

Berdasarkan hasil analisis dari Tabel 2, yang memuat jumlah dan jenis kerentanan pada delapan website desa di Kecamatan Bengkalis, ditemukan sebanyak 117 kerentanan dengan tingkat risiko yang beragam, mulai dari risiko tinggi (High), sedang (Medium), rendah (Low), hingga bersifat informatif (Informational). Jenis-jenis kerentanan yang paling sering ditemukan di antaranya adalah tidak diterapkannya header keamanan seperti Content Security Policy (CSP) dan Anti-clickjacking, penggunaan pustaka JavaScript yang rentan, terbukanya metadata server cloud, serta konfigurasi cookie yang tidak aman. Temuan-temuan tersebut kemudian dianalisis lebih lanjut dalam Tabel 4, yang memberikan uraian detail dan rekomendasi terhadap masing-masing jenis kerentanan. Website Pematangduku.desa.id tercatat sebagai website dengan tingkat risiko tertinggi, diikuti oleh Desapangkalanbatangbarat.com dan bengkaliskab.go.id. Meskipun Kotabengkaliskab.go.id hanya memiliki sedikit temuan, domain ini tetap dikategorikan berisiko tinggi karena mengandung kerentanan dalam kategori High. Secara umum, seluruh website yang dianalisis masih membutuhkan peningkatan aspek keamanan untuk mengurangi risiko serangan siber serta menjaga perlindungan data pemerintahan desa.

4. KESIMPULAN

Penelitian ini menemukan 117 kerentanan pada delapan website desa di Kecamatan Bengkalis melalui metode *vulnerability assessment*. Celah keamanan yang teridentifikasi meliputi pustaka JavaScript usang, tidak adanya header keamanan seperti CSP dan anti-clickjacking, terbukanya metadata server, serta port terbuka (FTP, SMTP, HTTP). Tingkat kerentanan bervariasi dari tinggi hingga informatif. Rekomendasi perbaikan meliputi penerapan HTTPS, aktivasi DNSSEC, pembaruan pustaka, dan konfigurasi keamanan server. Hasil ini menegaskan pentingnya pengujian berkala dan peningkatan keamanan siber untuk melindungi layanan publik digital dan data pemerintahan desa.

5. REFERENSI

Adam Kilian, Muhammad. 2023. "ANALISIS KEAMANAN WEBSITE PEMERINTAH PROVINSI MALUKU MENGGUNAKAN METODE VULNERABILITY ASSESSMENT." *Etika Jurnalisme Pada Koran Kuning : Sebuah Studi Mengenai Koran Lampu Hijau* 16(2):39–55.

Budiman, Arief, Syaiful Ahdan, and Muhammad Aziz. 2021. "Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment." *Jurnal Komputasi* 9(2):1–10. doi:10.23960/komputasi.v9i2.2800.

Dinarto, Aryda Fatihah Putri. 2024. "Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ." *INNOVATIVE: Journal Of Social Science Research* 4:4536–49.

Firman Syech, I. 2023. "ANALISIS KEAMANAN WEBSITE PEMERINTAH KOTA TIDORE KEPULAUANMENGGUNAKAN METODE VULNERABILITY ASSESSMENT Asdaf KOTA Tidore Kepulauan Provinsi Maluku Utara."

Sari, Nova Christina, Achmad Solichan, Basirudin Ansor, Aditya Putra Ramdani, Muhammad Zainudin Al Amin, Mulil Khaira, and Auliya Rohman Riquelm Al Ubaidah. 2024. "Deteksi Kerentanan SQL Injection Pada Website Menggunakan Vulnerability Assessment." *Journal of Data Insights* 2(1):9–17. http://journalnew.unimus.ac.id/index.php/jodi.