ANALISIS KEAMANAN WEBSITE PEMERINTAH KOTA TIDORE KEPULAUANMENGGUNAKAN METODE *VULNERABILITY ASSESSMENT*

DA'I FIRMAN SYECH
NPP 30.1410
Asdaf KOTA Tidore Kepulauan Provinsi Maluku Utara

Program Studi Teknologi Rekayasa Informasi Pemerintaha

E-mail: daifirman1@gmail.com

ABSTRACT

Problems/Background (GAP): *The security of government websites is crucial considering the information conveyed through these websites. However, vulnerabilities in websites can be exploited by attackers to launch attacks and compromise the integrity of the website and the information stored within. Therefore, there is a need for a security analysis of the Tidore Kepulauan City government website to identify vulnerabilities and take appropriate corrective actions.* ***Purpose:*** *This research aims to perform a security analysis on the Tidore Kepulauan City government website using the vulnerability assessment method. The objective of this study is to identify vulnerabilities in the website and implement suitable corrective measures.* ***Method:*** *The vulnerability assessment method, consisting of three stages - information gathering, vulnerability analysis, and corrective actions, is employed in this study. The OWASP ZAP application integrated with the Certified Ethical Hacker (CEH) module is used to conduct the analysis.* ***Results/Findings:*** *The analysis results reveal that the Tidore Kepulauan City government website has several vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), and Broken Authentication and Session Management. Additionally, there are server configuration issues that worsen the website's security. Some vulnerabilities and server configuration issues have been addressed by the website administrators.* ***Conclusion:*** *Based on the analysis findings, it can be concluded that the security analysis of the Tidore Kepulauan City government website using the vulnerability assessment method can identify vulnerabilities and provide necessary corrective measures. The implemented corrective actions contribute to enhancing the website's security and reducing the risk of attacks by adversaries.*

Keywords: Website security, vulnerability assessment, government website, OWASP ZAP, Tidore Kepulauan

ABSTRAK

Permasalahan/Latar Belakang (GAP): Keamanan website pemerintah kota menjadi hal yang penting mengingat informasi yang disampaikan melalui website tersebut. Namun, kerentanan pada website dapat dimanfaatkan oleh penyerang untuk melakukan serangan dan merusak integritas website serta informasi yang tersimpan di dalamnya. Oleh karena itu, diperlukan analisis keamanan pada website pemerintah kota Tidore Kepulauan untuk mengidentifikasi kerentanan dan mengambil tindakan perbaikan yang sesuai.. **Tujuan:** Penelitian ini bertujuan untuk melakukan analisis keamanan pada website pemerintah kota Tidore Kepulauan menggunakan metode vulnerability assessment. Tujuan penelitian ini adalah untuk mengidentifikasi kerentanan yang ada pada website tersebut dan mengambil langkah-langkah perbaikan yang tepat. **Metode:** Metode yang digunakan dalam penelitian ini adalah metode vulnerability assessment yang terdiri dari tiga tahap, yaitu pengumpulan informasi, analisis kerentanan, dan tindakan perbaikan. Metode ini dilakukan dengan menggunakan aplikasi OWASP ZAP yang terintegrasi dengan modul Certified Ethical Hacker (CEH). **Hasil/Temuan:** Hasil analisis menunjukkan bahwa website pemerintah kota Tidore Kepulauan memiliki beberapa kerentanan, antara lain SQL Injection, Cross-Site Scripting (XSS), dan Broken Authentication and Session Management. Selain itu, terdapat beberapa masalah konfigurasi server yang memperburuk keamanan website. Beberapa kerentanan dan masalah konfigurasi server tersebut telah diperbaiki oleh pihak pengelola website. **Kesimpulan:** Berdasarkan hasil analisis, dapat disimpulkan bahwa analisis keamanan website pemerintah kota Tidore Kepulauan menggunakan metode vulnerability assessment dapat mengidentifikasi kerentanan dan memberikan langkah-langkah perbaikan yang diperlukan. Langkah-langkah perbaikan yang telah dilakukan dapat membantu meningkatkan keamanan website dan mengurangi risiko serangan oleh penyerang.

Kata kunci: Keamanan website, vulnerability assessment, website pemerintah, OWASP ZAP, Tidore Kepulauan

I. PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi dan komunikasi (TIK) adalah kata umum yang mencakup semua peralatan teknologi yang digunakan untuk memproses dan mengirimkan data. Pemerintah Kota Kepulauan Tidore adalah salah satu organisasi pemerintahan kota yang menggunakan internet untuk menangani data dan menyebarkan informasi kepada masyarakat umum. Penerapan Situs Web Pemerintah Daerah merupakan sebuah langkah strategis dalam mengembangkan e-government secara bertahap dan terukur.

Namun, tidak sedikit orang yang sembarangan mengeksploitasi kemajuan teknologi. dimulai dengan contoh peretasan, penipuan, dan bahkan kejahatan dunia maya yang menargetkan tidak hanya orang tetapi juga bisnis, perusahaan, dan organisasi pemerintah. Serangan *Virus, Worm, Dorm*, *Web Deface*, isu pencurian data diri, pinjaman online, dan penipuan kartu kredit merupakan kejahatan lazim yang terjadi melalui jaringan internet di Indonesia.

Ancaman terhadap keamanan sistem informasi harus diwaspadai baik di dalam maupun di luar sistem, termasuk yang dapat menyebabkan ketidakstabilan di dalam sistem. Mekanisme, perusahaan, kelompok, dan individu semuanya dapat bertindak sebagai pemicu keamanan sistem informasi untuk mengganggu sistem dan merusak data. Karena tidak ada serangan sebelum ada ancaman, upaya keamanan sistem informasi harus terlebih dahulu mengidentifikasi dan meramalkan ancaman ini untuk mengurangi ketidakstabilan sistem sebagai akibat dari serangan yang sebenarnya. Ini dapat dilakukan dengan meramalkan ancaman sebelum serangan terjadi

Kutipan dari searchsecurity.techtarget.com bahwa *Vulnerability Assessment* yaitu proses menemukan risiko dan kelemahan dalam aplikasi, jaringan komputer, sistem, dan elemen lain dari ekosistem TI. Bisnis dapat menggunakan kemampuan ini untuk menunjukkan kelemahan sistem TI seperti kesalahan kode, kesenjangan keamanan, dan masalah lainnya. Dengan melakukan ini, bisnis dapat dengan cepat menambal kerentanan paling berbahaya sebelum penjahat menggunakannya.

Berdasarkan dari uraian-uraian di atas maka penulis tertarik untuk meneliti permasalahan yang akan dijadikan bahan penelitian guna menyusun Skripsi. Adapun judul yang dipilih yaitu "**ANALISIS KEAMANAN WEBSITE PEMERINTAH KOTA TIDORE KEPULAUAN MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT***"

1.2. Kesenjangan Masalah yang Diambil (GAP Penelitian)

Jumlah individu yang berinteraksi secara online mungkin didukung oleh tiga elemen, menurut jejak pendapat MarkPlus Insight (dailysocial.net) yang dilakukan pada 13 November 2012, tentang pengguna internet di Indonesia. Sekitar 24,2 juta orang Indonesia, atau 39,62% dari pengguna Internet di negara ini, menggunakannya setiap hari selama lebih dari tiga jam. Sebagian besar pengguna Internet di Indonesia juga berusia antara 15 dan 35 tahun. Selain itu, 56,4% individu, bahkan pencari barang murah, memiliki akses ke Internet dan dapat menemukan semua yang mereka butuhkan untuk waktu yang sangat lama.

Kejahatan dunia maya (*Cybercrime*), sering dikenal sebagai kejahatan komputer, kejahatan dunia maya, atau hanya kejahatan dunia maya, adalah jenis kejahatan di mana

kegiatan ilegal dilakukan melalui komputer dan internet. Peretasan, pelanggaran hak cipta, pornografi anak, dan eksploitasi anak adalah masalah yang terkait dengan kejahatan semacam ini. Ketika informasi pribadi diambil atau hilang, itu juga merupakan pelanggaran privasi.

Pemerintah Kota Kepulauan Tidore adalah salah satu organisasi pemerintahan kota yang menggunakan internet untuk menangani data dan menyebarkan informasi kepada masyarakat umum. Penerapan Situs Web Pemerintah Daerah merupakan sebuah langkah strategis dalam mengembangkan e-government secara bertahap dan terukur. Hal ini didasarkan pada jenis transaksi informasi dan layanan publik yang disediakan oleh pemerintah melalui jaringan informasi. Salah satu metode yang digunakan dalam menjaga keamanan situs tersebut adalah evaluasi kerentanan (vulnerability assessment) yang bertujuan untuk mengidentifikasi, menentukan tingkat kerentanan, dan memberikan peringkat terhadap sistem komputer, aplikasi, serta infrastruktur jaringan. Dengan melakukan evaluasi kerentanan, organisasi dapat memahami potensi ancaman terhadap lingkungannya dan merespons dengan tepat.. Teknik pengujian otomatis, termasuk pemindaian keamanan jaringan, sering digunakan dalam prosedur penilaian kerentanan untuk menggambarkan ancaman dan risiko yang mereka berikan. Temuan tes ini disajikan dalam laporan penilaian kerentanan.

1.3. Penelitian Terdahulu

Penelitian sebelumnya adalah hasil dari peneliti terdahulu yang dijadikan sebagai tolak ukur atau pedoman bagi penulis untuk melakukan penelitian, sehingga dari penelitian sebelumnya akan menambah pengetahuan dan wawasan tentang penelitian yang akan dilakukan penulis. Dari beberapa penelitian sebelumnya yang telah didapatkan, tidak ada satupun judul penelitian yang sama persis dengan judul penelitian penulis. Ada beberapa judul yang diangkat penulis untuk dijadikan sebagai acuan atau pedoman dan referensi dalam menambah bahan kajian penulis. Berikut adalah beberapa penelitian terdahulu yang berhubungan dengan judul penelitian yang akan diteliti penulis.

Penelitian Imam Riadi, Anton Yudhana, Yunanri.W (2020), berjudul "Analisis Keamanan *Website Open Journal System* Menggunakan Metode *Vulnerability Assessment* ". Penelitian ini menggunakan metode deskriptif kuantitatif pada penelitiannya. Penelitian ini bertujuan untuk menganalisis tingkat keamanan pada Website Open Jurnal dalam menghadapi serangan peretas website.

Penelitian Yudi Mulyanto, Eka Haryanti, dan Jumirah (2021), berjudul Analisis Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Assessment. Metodologi penelitian ini adalah Deskriptif, Kuantitatif untuk analisisnya. Tujuan dari penelitian ini adalah untuk menentukan ambang batas keamanan sisi server website SMAN 1 Sumbawa.

Penelitian Alif Muhammad Akmal, Nono Heryana, Arip Solehudin (2022), berjudul Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode *Vulnerability Assessment.* Penelitian ini menggunakan Metode Deskriptif, Kuantitatif pada penelitiannya. Penelitian ini bertujuan untuk mengetahui Tingkat keamanan dan celah keamanan pada *Website* Universitas Singaperbangsa Karawang dari serangan peretas.

1.4. Pernyataan Kebaruan Ilmiah

Pembaharuan yang dilakukan oleh peneliti pada penelitian ini yaitu dengan mengangkat masalah sistem keamanan website pemerintah Kota Tidore Kepulauan diteliti dengan menggunakan metode vulnerability assessment yang terdiri dari tiga tahap, yaitu pengumpulan informasi, analisis kerentanan, dan tindakan perbaikan. Metode ini dilakukan dengan menggunakan aplikasi OWASP ZAP yang terintegrasi dengan modul Certified Ethical Hacker (CEH). Serta masalah yang diangkat berdasarkan lokasi ini belum pernah diteliti oleh penelitian-penelitian sebelumnya. Penelitian ini juga dilakukan berdasarkan kondisi terbaru yang ditemukan di lapangan selama peneliti yaitu dengan melakukan penelitian langsung dilapangan pada bulan januari tahun 2023.

1.5. Tujuan.

Tujuan dari penelitian ini sesuai dengan rurmusan masalah diatas adalah Untuk mengetahui seberapa banyak kerentanan yang terdapat pada *website* Pemerintah Kota Tidore Kepulauan (https://tidorekota.go.id).

II. METODE

Metode: yang digunakan dalam penelitian ini adalah Pada penelitian ini juga menggunakan pendekatan deskriptif yang bertujuan yaitu menjabarkan objek penelitian dan hasil dari penelitian tersebut.

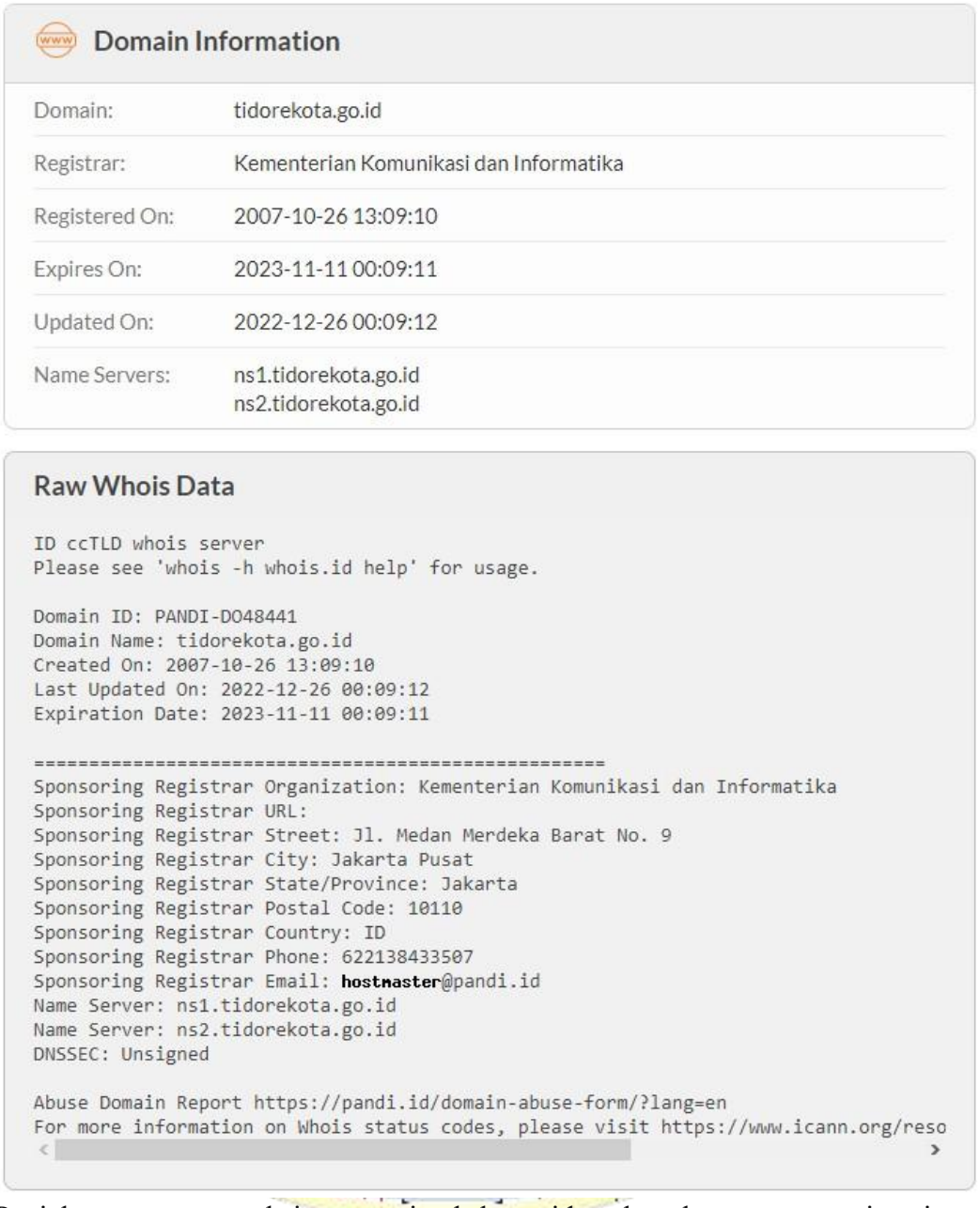
. . Instrumen yang dipergunakan dalam penelitian ini yaitu aplikasi *OWASP ZAP* (*The OWASP Foundation, 2018)* untuk menguji tingkat keamanan dan celah keamanan yang terdapat pada sebuah website. Untuk menetapkan tingkat keparahan dari setiap risiko yang ditemukan, dilakukan perhitungan rata-rata faktor yang terkait. Setelah itu, tingkat risiko ditentukan melalui tingkat likelihood dan impact. Dalam hal ini, setiap risiko memiliki bobot likelihood dan impact yang berbeda, dimulai dari rendah (low), sedang (medium), hingga yang tertinggi adalah tinggi (high), semua perhitungan tersebut akan diolah secara otomatis pada aplikasi *OWASP ZAP*.

Setelah data dan perlengkapan telah terkumpul maka langkah selanjutnya adalah menganalisis data tersebut. Analisis pada penelitian ini untuk mendapatkan data/informasi dari website pemerintah kota tidore kepulauan untuk melakukan analisis keamanan website. Tahapan yang dilakukan dalam mendapatkan dan mengelola informasi menggunakan modul CEH (*Certified Ethical Hacker*) (Elizabeth dan Jimenez, 2016).

III. HASIL DAN PEMBAHASAN

3.1 Vulnerability Assessment

A. Footprint / Network Discover



Domain Information

Domain:	tidorekota.go.id
Registrar:	Kementerian Komunikasi dan Informatika
Registered On:	2007-10-26 13:09:10
Expires On:	2023-11-11 00:09:11
Updated On:	2022-12-26 00:09:12
Name Servers:	ns1.tidorekota.go.id ns2.tidorekota.go.id

Raw Whois Data

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PANDI-DO48441
Domain Name: tidorekota.go.id
Created On: 2007-10-26 13:09:10
Last Updated On: 2022-12-26 00:09:12
Expiration Date: 2023-11-11 00:09:11

================================================
Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar URL:
Sponsoring Registrar Street: Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City: Jakarta Pusat
Sponsoring Registrar State/Province: Jakarta
Sponsoring Registrar Postal Code: 10110
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 622138433507
Sponsoring Registrar Email: hostmaster@pandi.id
Name Server: ns1.tidorekota.go.id
Name Server: ns2.tidorekota.go.id
DNSSEC: Unsigned

Abuse Domain Report https://pandi.id/domain-abuse-form/?lang=en
For more information on Whois status codes, please visit https://www.icann.org/reso
```

Penjelasan tentang website pemerintah kota tidore kepulauan mengenai registrar, tanggal register, expired,update, dan nama server.

A records

IPv4 address	Revalidate in
103.78.208.148	4h

Alamat IP dari website pemerintah kota tidore kepulauan

Port	Name	Status
21	FTP	closed, incoming traffic denied
22	SSH	closed, incoming traffic denied
25	SMTP	open (243ms), incoming traffic allowed
26	SMTP	closed, incoming traffic denied
2525	SMTP	closed, incoming traffic denied
587	SMTP SSL	open (240ms), incoming traffic allowed
80	HTTP	open (242ms), incoming traffic allowed
443	HTTPS	open (241ms), incoming traffic allowed
110	POP3	open (238ms), incoming traffic allowed
995	POP3 SSL	open (241ms), incoming traffic allowed
143	IMAP	open (241ms), incoming traffic allowed
993	IMAP SSL	open (242ms), incoming traffic allowed
3306	MySQL	closed, incoming traffic denied

Port yang dapat digunakan untuk mengakses website pemerintah kota tidorekepulauan.

```
HTTP/1.1 200 OK
Date: Mon, 20 Jan 2023 03:21:12 GMT
Server: Apache
X-DNS-Prefetch-Control: on
Link: <https://tidorekota.go.id/wp-json/>; rel="https://api.w.org/",
<https://tidorekota.go.id/wp-json/wp/v2/pages/22>; rel="alternate"; type="application/json",
<https://tidorekota.go.id/>; rel=shortlink
X-LiteSpeed-Tag:
7a6_HTTP.200,7a6_front,7a6_URL.6666cd76f96956469e7be39d750cc7d9,7a6_F,7a6_Po.22,7a6_PGS,7a6_
guest,7a6_,7a6_MIN.eb50f946c9802c4c8ed4b934d58c04c2.css,7a6_MIN.703b6b9cc4005dcc8671343b754c
b897.js
Vary: Accept-Encoding,User-Agent
Content-Length: 170593
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Hypertext transfer protokol ketika mengakses website pemerintah kota tidore kepulauan.

B. *Scanning Vulneraility* (Memindai Celah Keamanan)

Alert type	Risk	Count
PII Disclosure	High	1 (7.1%)
Absence of Anti-CSRF Tokens	Medium	1156 (8,257.1%)
Content Security Policy (CSP) Header Not Set	Medium	861 (6,150.0%)
HTTP to HTTPS Insecure Transition in Form Post	Medium	21 (150.0%)
Missing Anti-clickjacking Header	Medium	858 (6,128.6%)
Secure Pages Include Mixed Content	Low	18 (128.6%)
Strict-Transport-Security Header Not Set	Low	1641 (11,721.4%)
Timestamp Disclosure - Unix	Low	17 (121.4%)
X-Content-Type-Options Header Missing	Low	1398 (9,985.7%)
Charset Mismatch	Informational	99 (707.1%)
Information Disclosure - Suspicious Comments	Informational	974 (6,957.1%)
Modern Web Application	Informational	270 (1,928.6%)
Re-examine Cache-control Directives	Informational	1229 (8,778.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	27 (192.9%)
Total		14

Hasil scanning vulnerability pada website pemerintah kota tidore kepulauan.

C. *Reporting*/ Laporan

		Confidence					
		User Confirmed	High	Medium	Low	False Positive	Total
Risk	High	0 (0.0%)	1 (7.1%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (7.1%)
	Medium	0 (0.0%)	1 (7.1%)	2 (14.3%)	1 (7.1%)	0 (0.0%)	4 (28.6%)
	Low	0 (0.0%)	1 (7.1%)	2 (14.3%)	1 (7.1%)	0 (0.0%)	4 (28.6%)
	Informational	0 (0.0%)	0 (0.0%)	1 (7.1%)	4 (28.6%)	0 (0.0%)	5 (35.7%)
	Total	0 (0.0%)	3 (21.4%)	5 (35.7%)	6 (42.9%)	0 (0.0%)	14 (100%)

Dari 3 tingkatan Alert ditamah Informational meghasilkan total 8570 risk yang terdiri dari 1 high risk, 2896 medium risk, 3074 low risk, dan 2599 informtionalrisk menghasilkan 14 Alert type.

3.2. Diskusi Temuan Utama Penelitian

Apabila penelktian ini dikatkan dengan Penelitian terdahulu menurut Penelitian Imam Riadi, Anton Yudhana, Yunanri.W (2020), berjudul "Analisis Keamanan *Website Open Journal System* Menggunakan Metode *Vulnerability Assessment* ". Penelitian ini menggunakan metode deskriptif kuantitatif pada penelitiannya. Penelitian ini bertujuan untuk menganalisis tingkat keamanan pada Website Open Jurnal dalam menghadapi serangan peretas website. Dan juga Penelitian sebelumnya menurut Penelitian Yudi Mulyanto, Eka Haryanti, dan Jumirah (2021), berjudul Analisis Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Assessment. Metodologi penelitian ini adalah Deskriptif, Kuantitatif untuk analisisnya. Tujuan dari penelitian ini adalah untuk menentukan ambang batas keamanan sisi server website SMAN 1 Sumbawa. Kemudian Penelitian Alif Muhammad Akmal, Nono Heryana, Arip Solehudin (2022), berjudul Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode *Vulnerability Assessment.* Penelitian ini menggunakan Metode Deskriptif, Kuantitatif pada penelitiannya. Penelitian ini bertujuan untuk mengetahui Tingkat keamanan dan celah keamanan pada *Website* Universitas Singaperbangsa Karawang dari serangan peretas.

Apabila ketiga penelitan tersebut dikaitkan dengan temuan yang ditemukan pada penelitian ini, maka pada penelitian ini juga terdapat beberapa kesamaan temuan

dimana masalah mengneai keamanan website srig terjadi diakibatkan kurangnya maintanance terhadap sistem yang dimiliki website pemerintahan itu sendiri serta kurangnya kemampuan sumber daya manusia yang mampu untuk megatasi hal tersebut dalam lingkungan pemerintah kota tidore kepulauan. Ternyata permasalahan tentang kurangnya maintanance atau pengawasan website secara berkala kurang dilakukan sehingga munculnya celah celah atau kerentanan pada website tersebut. Sehingga perlunya aparatur sipil negara yang berkompeten pada bidang keamanan siber ini.

IV. KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan terhadap keamanan website Pemerintah Kota Tidore Kepulauan, dapat diambil kesimpulan sebagai berikut:

Terdapat 14 kerentanan pada website Pemerintah Kota Tidore Kepulauan yang dapat mempengaruhi keamanan data yang terdapat pada website tersebut. Beberapa kerentanan tersebut antara lain PII Disclosure, Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, HTTP to HTTPS Insecure Transition in Form Post, Missing Anti-clickjacking Header, Secure Pages Include Mixed Content, Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix, X-Content-Type-Options Header Missing, Charset Mismatch, Information Disclosure - Suspicious Comments, Modern Web Application, Re-examine Cache-control Directives, dan User Controllable HTML Element Attribute (Potential XSS).

Berdasarkan hasil tersebut, dapat disimpulkan bahwa website pemerintah kota Tidore Kepulauan memiliki kerentanan yang cukup signifikan pada berbagai aspek, termasuk keamanan dan privasi pengguna

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan pada pelaksanaannya yakni waktu penelitian yang relatif singkat sehinngga pada kondisi di lapangan dimana beberapa pengujian yang dapat menguji tingkat keamanan website lebih dalam hingga sub-domain pada website tidak dapat dilakukan. Penelitian juga hanyadapat melakukan pengujian menggunakan metode dan modul yang sudah direncanakan pada domain utama saja

Arah Masa Depan Penelitian (*future work*). Penulis menyadari masih awalnya temuan penelitian ini merupakan titik awal kepedulian terhadam keamanan data digital pada sistem pemerintahan terutama pada pemerintah daerah kota tidore kepulauan. Maka dari hal

tersebut diharapkan bahwa dengan upaya yang dilakukan analisis keamanan pada website pemerintah daerah tersebut, maupun memberikan pemahaman kepada pemerintah dan masyarakat bahwa pentingnya mengetahui betapa pentingnya data digital agar tidak disalahgunakan dalam tindak kejahatan. Dan dapat meningkatkan kemampuan serta kemauan pemerintah untuk terus meningkatkan keamanan serta kenyamanan pada pelayanan kepada masyarakat kedepannya.

V . Ucapan Terima Kasih

Ucapan terima kasih terutama ditujukan kepada Pemerintah Kota Tidore Kepulauan terutama kepada bidang protokol dan informasi pimpinan Kota Tidore Kepulauan beserta jajarannya yang telah memberikan kesempatan penulis untuk melaksanakan penelitian, serta seluruh pihak yang membantu dan mensukseskan pelaksanaan penelitian ini.

V. DAFTAR PUSTAKA

Mulyanto, Y., Haryanti, E., & Jumirah (2021). SUMBAWA MENGGUNAKAN METODE VULNERABILITY ASESEMENT. *JINTEKS*, *3*(3). https://doi.org/10.51401

Riadi, I., Yudhana, A., & Korspondensi, P. (2020). *ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT*. *7*(4). https://doi.org/10.25126/jtiik.202071928

Akmal, A. M. ., Heryana, N. ., & Solehudin, A. . (2022). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. *Jurnal Pendidikan Dan Konseling (JPDK)*, *4*(4), 6298–6308. https://doi.org/10.31004/jpdk.v4i4.6495

Rina, Elizabeth, Lopez, de, Jimenez. (2016). Pentesting on web applications using ethical - hacking. 1-6. doi: 10.1109/CONCAPAN.2016.7942364