JURNAL TEKNOLOGI INFORMATIKA DAN KOMPUTER
Vol. 1, no.1, Desember 2023
Hal. 1-9
https://jurnal.uts.ac.id/index.php/jurtikom
e-issn : xxxx-xxxx
Doi Prefix : 10.xxxxx

ANALISIS KEAMANAN WEBSITE SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN MENGGUNAKAN METODE VULNERABILITY ASSESMENT

Tara Rizkayanti, Yunanri. W[2]
[1,2]Informatika, Universitas Teknologi Sumbawa
email: tararizkayanti05@gmail.com

Abstrak: *Website* adalah suatu halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama aktivitas internet pada suatu *device* tersambung. Keamanan informasi pada suatu *website* adalah terpenting saat ini, tidak terkecuali pada *website* lembaga kementrian daam negeri dibidang kependudukan dan pencatatan sipil yang menyajikan informasi tentang suatu data data pribadi kemasyarakatan. Masalah tersebut sangat penting jika diakses oleh orang yang tidak bertanggung jawab. Metode yang digunakan dalam penelitian ini adalah metode *Vulnerability Assesment*. Penelitian ini telah menemukan hasil informasi terkait *website* target dan beberapa peringatan kerentanan seteah dilakukan pengujian pemindai kerentanan dengan tingkat resiko tinggi sehingga penelitian merekomendasikan perbaikan kerentanan untuk meminimalkan lubang keamanan yang dimanfaatkan oleh peretas. Pengujian dilakukan menggunakan *kali linux* dan *OWASP ZAP*.

Kata Kunci : *Keamanan, Website, Dukcapil, kali Linux, OWAPS ZAP*.

Abstract: *Website is an information page that is provided via the internet so that it can be accessed throughout the world as long as internet activity on a device is connected. Information security on a website is the most important at this time, including the website of the Ministry of Home Affairs in the field of population and civil registration which provides information about community personal data. This problem is very important if it is accessed by irresponsible people. The method used in this study is the Vulnerability Assessment method. This research has found information related to the target website and several vulnerability warnings after testing a vulnerability scanner with a high level of risk so that the research recommends fixing the vulnerability to minimize security holes exploited by hackers. Testing was carried out using Kali Linux and OWASP ZAP.*

Keywords: *Security, Website, Dukcapil, Kali Linux, OWAPS ZAP*

PENDAHULUAN

Pada era internet saat ini, perkembangan sistem informasi berkembang sangat pesat, sama halnya seperti aplikasi. Aplikasi merupakan salah satu layananmedia informasi atau kumpulan halaman yang menampilkan informasi data *teks*, data gambar, data animasi, suara, *video* dan atau gabungan dari semuanya, baik yang bersifat *statis* maupun *dinamis* yang membentuk satu rangkaian bangunan yang saling terkait, dimana masing-masing dihubungkan dengan jaringan-jaringanhalaman. Melalui aplikasi, informasi sangat mudah diperoleh dan disebarluaskan. Oleh karena itu, informasi menjadi aset yang sangat berharga baik bagi perseorangan, instansi maupun perusahaan [24]

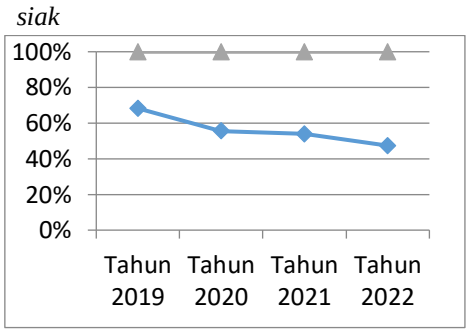
Sistem informasi administrasi kependudukan (SIAK) adalah sistem informasi dengan pemanfaatan teknologi informasi dan komunikasi untuk memfasilitasi pengolaan informasi administrasi kependudukan ditingkat penyelenggara dan instansi pelaksana sebagai satu kesatuan [23] . Dengan tersedianya informasi dan data yang mudah di akses maka potensi masyarkat untuk berperan serta dalam membangun desa dapat meningkat. Masyarakat atau warga akan mengetahui kegiatan apa saja yang sedang di rancang dan yang sedang berlangsung. Sehingga dapat ikut mengawasi kegiatan tersebut atau dapat juga memberikan masukan terkait pembangunan desa.

Keamanan informasi merupakan bagian terpenting dari sebuah instansi atau perusahaan. Kebutuhan akan keamanan informasi timbul dari kebutuhan dalam melindungi data. Informasi sangat berharga karena jika informasi tersebut berada di tangan orang yang salah seorang tersebut mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat merusak dan menjadikannya suatu keuntungan. Sebagai contoh : Virus, Pencurian Kartu Kredit, Pembobolan Rekening Bank, Pencurian *Password Email*/*Web Server*. *Hacker* mengambil data-data penting pada suatu sistem informasi dan bahkan pula mengacak-acak tampilan *web* tersebut di aplikasi disebuah pemerintahan ataupun swasta.

Kantor Dinas Kependudukan Dan Pencatatan Sipil adalah salah satu kantor yang beralamat di Jalan Garuda No.07, Lempeh, Kec. Sumbawa, Kabupaten Sumbawa, NTB. Kantor yang sudah memanfaatkan aplikasi SIAK dalam

JURNAL TEKNOLOGI INFORMATIKA DAN KOMPUTER
Vol. 1, no.1, Desember 2023
Hal. 1-9
https://jurnal.uts.ac.id/index.php/jurtikom
e-issn : xxxx-xxxx
Doi Prefix : 10.xxxxx

menyampaikan informasi ke masyarakatnya. Dapat di *accses* melalui *web* dengan domain *https://www.siak.co.id*. Kantor Dukcapil menyediakan informasi dalam sebuah aplikasi, baik informasi tentang data penduduk. Siak merupakan salah satu aplikasi yang banyak digunakan. Pengguna siak dari tahun 2019 pada masa covid-19 sampai pada tahun 2022 mengalami peningkatan penggunaan. Penggunaan siak yang semakin banyak , tidak menutup kemungkinan akan adanya serangan *hacker* yang dapat mengganggu performa siak, bahkan dapat diambil alih oleh *hacker*. Keamanan sistem Siak diperlukan untuk melindungi informasi yang terdapat didalamnya. Keamanan yang dimaksud mengacu pada kerahasiaan data, integritas dan ketersediaan layanan pada sistem yang diterapkan.



Gambar 1.1 Menunjukkan penggunaan siak dari tahun 2019 sampai tahun 2022.

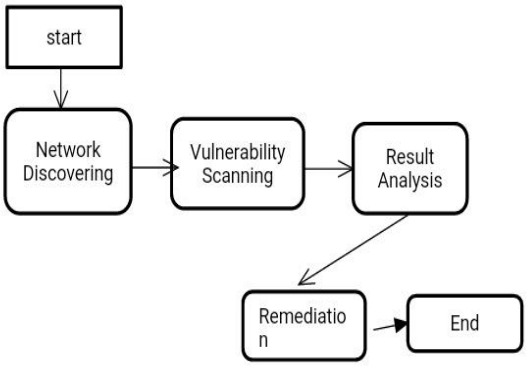
Dilihat dari banyaknya ancaman dilakukan oleh orang yang tidak bertanggung jawab (*hacker*) di dunia internet saat ini khusunya di bidang keamanan aplikasi yang sudah banyak terbukti kejadiannya seperti *SQL Injection, Phising, DoS, Brute Force,* dan lain-lain [19] Dapat mengakibatkan kehilangan informasi yang sangat penting bagi masyarakat.

Masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data ,transaksi, dan komunikasi. Minimnya penelitian yang membahas tentang keamanan aplikasi SIAK tersebut, Sehingga penelitian berinisiatif untuk menganalisis tingkat keamanan pada aplikasi tersebut.Untuk mengetahui tingkat ketahanan keamanan dari aplikasi SIAK, agar tidak terjadinya berbagai hal yang tidak diinginkan.

Perumusan masalah dari latar belakang diatas, penulis menarik garis besar bahwa dalam menganalisis tingkat ketahanan keamanan dan mencari celah pada aplikasi SIAK merupakan tindakan yang cukup membawa pengaruh besar di dalam menjaga kualitas dari aplikasi. Jadi penulis memberikan sebuah solusi yaitu dengan menganalisa tingkat keamanan dan mencari celah pada keamanan aplikasi sistem informasi administrasi kependudukan (SIAK) pada Kantor Dukcapil menggunakan tool *Open Web Application Security Project* (OWASP) dengan metode *Vurnerability Assessment*. Jika hasil dari aplikasi ini masih memiliki kelemahan pada sistem keamanan diharapkan dapat menjadi rekomendasi bagi pihak Kantor Dukcapil agar dapat meningkatkan keamanan aplikasi.

2. METODE PENELITIAN

Metode Vunerabiity assessment (Penilaian Kerentanan) digunakan untuk melakukan pengujian pada point-point yang berpotensi masuknya serangan. Selain itu juga port-port yang terbuka. Mengidentifikasi masa berlakunya versi sebuah software dan dapat juga mengidentifikasi aplikasi apa saja yang sedang berjalan. Vulnaerability assessment digunakan untuk mendeteksi kelemahan dalam sebuah system (Orisa & Ardita, 2021).



3.2 Alur Pengujiian Sistem vulnerability Assesment pada *Website.*

Berdasarkan Gambar 3.2. langkah awal pengujian penelitian perlu dilakukan pengumpulan informasi mengenai fisik server, jenis jaringan yang digunakan dan berbagai informasi yang berkaitan dengan webserver pada aplikasi antara Lain:

a. *Network discovery/ Information*
Bertujuan menemukan struktur rancang dari keamanan jaringan pada target sasaran yang dituju. Dalam penelitian ini penulis menggunakan beberapa tools diantaranya : *whois, Nslookup,*dan *Scanning port,*

JURNAL TEKNOLOGI INFORMATIKA DAN KOMPUTER
Vol. 1, no.1, Desember 2023
Hal. 1-9
https://jurnal.uts.ac.id/index.php/jurtikom
e-issn : xxxx-xxxx
Doi Prefix : 10.xxxxx

b. Vulnerability scanning
Bertujuan mencari Celah kerentanan atau vulnerability pada website dengan menggunakan tools OWASP ZAP untuk melakukan pengujian kerentanan.

c. Result Analysis
Kesimpulan akhir ,berupa tabel dari jumlah nilai dari sebuah penelitian yang dilakukan.

d. Remediation
Bertujuan untuk merekomendasikan perbaikan yang tepat untuk mengurangi/menghilangkan resiko kerentanan dalam website siak pada tools OWASP ZAP.

2.1 Sistem Analisis

Analisis system dilakukan untuk maemperoleh informasi dari system yang bertujuan untuk meakukan analisis kelemahan system. Beberapa alat yang diimplementasikan, yaitu:

a. Information gethring
Fase ini adalah untuk menemukan struktur rancang bangun dari keamanan jaringan pada website siak tersebut:

Nslookup Adalah suatu *tools* yang digunakan untuk mengetahui IP address dari domain Sistem Informasi Administrasi Kependudukan.

Scanning Port Discover Merupakan sebuah prosedur aplikasi yang dirancang untuk menyelidiki *server* atau *port host* yang terbuka dengan cara ketik *nmap* dan IP dari sebuah domain, lalu tekan *enter*.

b. Vulnerability Detection
Bertujuan untuk mencari celah pada aplikasi website. Pada tahap ini penguji menggunakan apikasi OWASP ZAP. Penguji menggunakan profile attack mode (serangan) pada saat pemindaian.

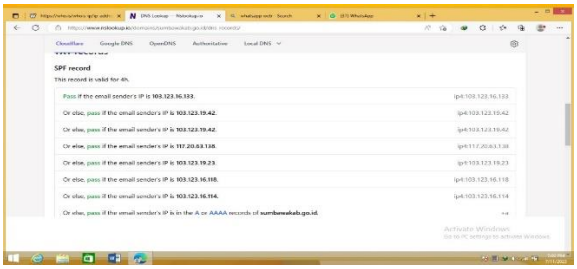
3. HASIL DAN PEMBAHASAN

3. 1 Informasi gethring

Fase ini adalah untuk menemukan struktur rancang bangun dari keamanan jaringan pada website tersebut:

1.Nslookup

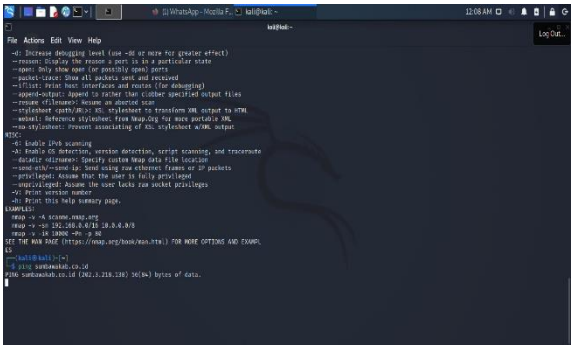
Adalah suatu tools yang digunakan untuk mengetahui IP address dari domain Sistem Informasi Administrasi Kependudukan.



Gambar4.1 hasil scanning tools nslookup

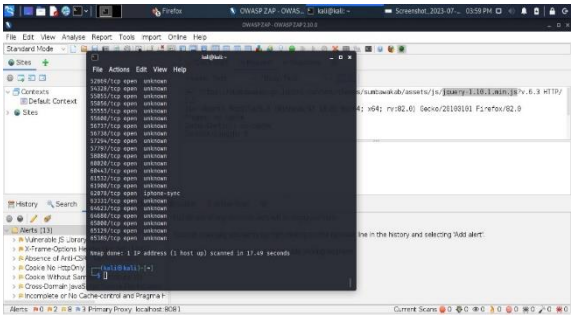
Untuk melakukan pencarian pada tools ini dengan cara memasukan domain dari apikasi adapun Ip Addres yang di temukan yaitu 103.123.16.133, 103.123.19.42, 117.20.63.138, 103.123.19.23,103.123.16.118,dan103.123.16.114

2. Scanning Port Discover
Merupakan sebuah prosedur aplikasi yang dirancang untuk menyelidiki server atau port host yang terbuka dengan cara ketik nmap dan IP dari sebuah domain, lalu tekan enter.



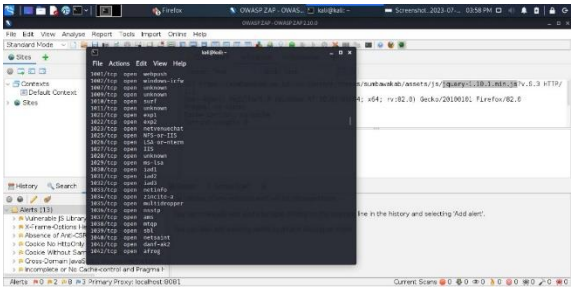
Gambar 4.2 Hasil Scaning NMAP

Adapun hasil pengujian menggunakan NMAP didapatkan informasi penting mengenai port apa saja yang statusnya aktif atau open. Adapuan Port yang berstatus open pada website nya antara lain**:**



Gambar 4.3 Hasil scanning Port Discover

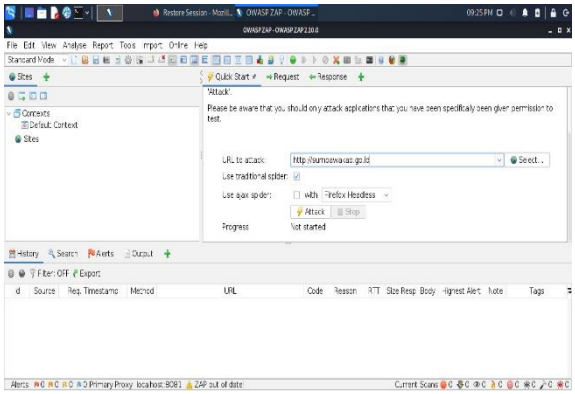
JURNAL TEKNOLOGI INFORMATIKA DAN KOMPUTER
Vol. 1, no.1, Desember 2023
Hal. 1-9
https://jurnal.uts.ac.id/index.php/jurtikom
e-issn : xxxx-xxxx
Doi Prefix : 10.xxxxx



Gambar 4.4 Hasil scanning Port Discover

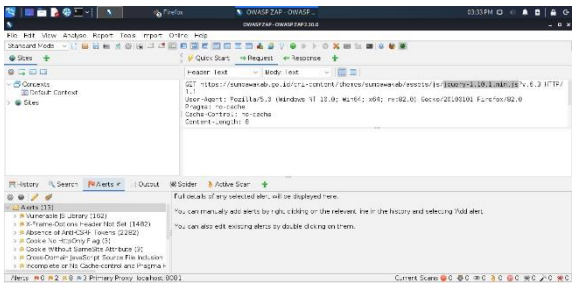
3.2 Vulnerability Detection

Bertujuan untuk mencari celah pada aplikasi website. Pada tahap ini penguji menggunakan apikasi OWASP ZAP. Penguji menggunakan profile attack mode (serangan) pada saat pemindaian. Hasil pemindaian pada ZAP dapat diihat pada gambar :



Gambar 4.6 Awal- awal melakukan penyerangan terhadap website.

Setelah melakukan pengujian terhadap alamat website tersebut, terbukti bahwa alamat website http://sumbawakab.go.id rentan terhadap serangan.



Gambar 4.7 Hasil Scanning Setelah melakukan serangan

Berdasarkan hasil pengujian kerentanan pada apikasi website menampikan adanya kerentanan. Berdasarkan Hasil pengujian kerentanan pada website tersebut ditemukan adanya 14 kerentsnsn atau celah diantaranya : *3 Medium risk dan 11 low Risk*, Dan menghasilkan alert diantaranya*: Vunerability Library, X-Frame-Option HeaderNot Set, Absence of anti- CSRF Token, Cookie Without Samesite Atributte, Cookie Withoute HttpOnly flag, Cross-Domain java Scrip Source File inclution, Incomplete or no cache and pragma HTTP Header Set, Secure pages Mixed Content, Server leaks Information Via, X-content-Type-Options Header Missing, Charset mismate, Information Discosure, Timetamp Discover-Unix.* Dan ada 4 level Kerentanan yaitu : *medium, low, high, informational.*

3.3 Hasil Analisis atau *Result Analysis*

Adapun hasi yang di dapatkan dari hasi pengujian tersebut, mendeteksi 14 sub file vulnerability diantaranya **:**

Setelah Melakukan pencarian celah menggunakan tool OWASP didapatkanhasil celah yang di tentukan oleh peneliti untuk dilakukan pengujian antara lain:

Tabel 4.8 Pengujian yang teah diakukan pada Website dan mendeteksi 14 sub file Vunerability : High, Medium, low.

N0	Alert	Risk	Keterangan
	High low	medium	
1.Directory Browsing (3)	Medium		
2. Vulnerability JS Library *(162)*	Medium		Pada medium Risk pada Website ini, Berada pada tahap menghawatirkan, Oleh karena itu harus segera diperbaiki oeh admin pengelola website kantor

		Disdukcapil Sumbawa Besar.
3.*X-Frame-option Header Not Set (3490)*	Medium	
4. *Absence of anti-CSRF Token (5170)*	Low	
5.Cokie Without Samesite Atributte (3)	Low	Sementara pada Low Risk masih berada pada keadaan kerusakan Ringan.
6.Cookie withoute httponly flag (3)	Low	
7.Cross-Domain javaScrip Source file inclution (2)	Low	
8. Incomplete or no cache and pragma HTTP Header Set (893)	Low	
9.Secure pages include Mixed content (1313)	Low	
10. X-content-Type-Options Header Missing (5752)	Low	
11.Server leaks Information via (3492)	Low	
12.Charset mismate (3490)	Low	
13.Informationd iscosure (486)	Low	
14. Timestamp Discosure-Unix(1673)	Low	

Source: Fictitious data, for illustration purposes only

3.4 Rekomendasi (*Remediation*) atau *countermeasure*

Countermeasure merupakan sebuah saran yang direkomendasi oleh tools owasp yang memiliki standar dan kualitas yang tinggi pada bidang IT. Rekomendasi perbaikan kerentanan dari website Siak predator dibuat dalam bentuk report (laporan) detail terkait vulnerability, jumlah vulnerability dan rekomendasi perbaikan vulnerability yang ditemukan

N0	Alert	Deskripsi	Rekomendas
1.	Vulnerability JS Library *(162)*	Jquery perpustakaan yang diidentifikasi versi 1.10.1. rentan	Perlu ditingkatkan ke versi Jquery terbaru
2.	*.X-Frame-option Header Not Set (3490)*	Header X-Frame-Option tidak disertakan dalam respons HTTP untuk melindungi dari serangan.	
3.	*Absence of anti-CSRF Token (5170)*	Risiko pengungkapan informasi secara dramatis meningkat ketika target situs tersebut	

	rentan terhadap XSS,	
4.Cokie Without Samesite Atributte (3)	Cookie telah ditetapkan tanpa atribut SameSite, yang berarti bahwa cookie dapat dikirim sebagai hasil dari permintaan “lintas situs”. Atribut SameSite adalah tindakan balasan yang efektif untuk pemalsuan permintaan lintas situs, penyertaan skrip lintas situs, dan serangan waktu.	Pastikan atribut SameSite diatur ke ‘lax’ atau idealnya strict’ untuk semua cookie.
5.Cookie withoute httponly flag (3)	Cookie telah disetel tanpa bendera HttpOnly, yang berarti cookie dapat diakses oleh JavaScript. Jika skrip jahat dapat dijalankan di laman ini, maka kuki akan dapat diaks es dan dapat dikirimkan ke situs lain. Jika ini adalah cookie sesi, maka pembajakan sesi dapat dilakukan	Pastikan bendera HttpOnly disetel untuk semua cookie
6.Cross-Domain javaScrip Source file inclution (2)	Halaman berisi satu atau beberapa file skrip dari domain pihak ketiga.	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi
7. Incomplete or no cache and pragma HTTP Header Set (893)	kontrol cache dan header HTTP pragma belum disetel dengan benar atau tidak ada sehingga browser dan proxy dapat menyimpan konten dalam cache.	Bila memungkinkan pastikan header HTTP cache-control disetel dengan no-cache, nostore, must-revalidate, dan bahwa program HTTP header disetel dengan no-cache.
8. Secure pages include Mixed content (1313)	Halaman tersebut	Halaman yang

	mencakup konten campuran, yaitu konten yang diakses melalui HTTP, bukan HTTPS.	tersedia melalui SSL/TLS harus terdiri dari konten yang dikirimkan melalui SSL/TLS. halaman tersebut tidak boleh berisi konten apapun yang dikirimkan melalui HTTP yang tidak terenkripsi.
9.X-content-Type-Options Header Missing (5752)	Server web / aplikasi membocorkan informasi melalui satu atau lebih header respons HTTP 'X Powered-By'	Pastikan server web anda, server aplikasi, penyeimbang beban, dll. Dikonfigurasi untuk menekan header "x-p ewered-by".
10..Server leaks Information via (3492)	Header Anti-MIMESniffing X-Content-TypeOptions tidak disetel ke 'nonsiff. Ini memungkinkan versi internet Explorer dan Chrome yang lebih lama	Pastikan aplikasi / server web menyetel header X-ContentType-Option dengan tepat, dan mengatur header-control ke 'nonsif' dan diatur untuk semua halaman web.
11.Charset mismate (3490)	Seorang penyerang dapat memanipulasi konten pada halaman untuk ditafsirkan dalam penyandian pilihan mereka.	Paksa untuk semua konten teks di header HTTP dan tag meta di HTML atau deklarasi penyandian di XML
12.Informationd iscosure (486)	Respons tampaknya berisi komentar mencurigakan yang dapat membantu penyerang.	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.
13. Timestamp Discosure-Unix(1673)	Stempel waktu diungkapkan oleh aplikasi/server web – Unix	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungk

	an untuk mengungkap pola yang dapat dieksploitasi.

Sumber: Real-time oleh Open web application security project (OWASP)

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dalam melakukan pengujian celah keamanan/kerentanan pada website system informasi dministrasi kependudukan (Siak) Menggunakan metode Vulneraility Assesment pada Domain http://sumbawakab.go.id atau https://siak.co.id maka dapat di ambil kesimpulan:

1) Dari penelitian ini di audit, diawali dengan langkah information gethring, scanning vulnerability assessment, reporting analisys dan remediation.
2) Kelebihan dari tools owasps adalah dapat melihat source code yang ditandai kkhusus oleh tools owasp. Tools owasp berhasil menguji kerentanan system pada website tersebut.
3) Pengujian yang telah dilakukan berhasil mengidentifikasi 4 kerentanan, high, medium, low, dan informational. Tingkat kerentanan diproleh dari notifikasi alert

5.2 Saran

Berdasarkan penelitian yang telah dilakukan terdapat beberapa saran yang dapat diterapkan pada penelitian berikutnya:

1. Perlu dilakukan pengecekan secara berkala guna menghindari serangan yang berasal dari luar dengan memanfaatkan kelemahan yang ada pada sistem.

2. Untuk pengembangan penelitian kedepanya bisa dengan menggunakan metode lain yang dapat melakukan perbaikan langsung ke dalam sistemnya. Dan dapat menggunakan berbagai macam tools untuk dapat membantu dalam melakukan pengujian keamanan.

3. Menerapkan rekomendasi yang disarankan dalam penelitian ini untuk menutup kerentanan.

4. Dapat melakukan serangan dengan cara lain yang lebih detail, guna mendapatkan kerentanan cross site scripting

DAFTAR PUSTAKA

[1] Adha Maliq Ibrahim. (2022) *analisis keamanan sistem pada website perusahaan cv. kazar teknologi indonesia dengan metode vulnerability assesment. skripsi thesis, universitas pembangunan nasional veteran* Jakarta.

[2] Anggi Elanda (2020) Analisis Keamanan Sistem Informasi Berbasis *website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. Jurnal of Computer Engineering, System an Science,* Vol 5, No 02 (2020)

[3] Agus Rochman (2021). analisis *keamanan website dengan information system security assessment framework (issaf) danopen web application security project (owasp)di rumah sakit xyz.* Jurnal Indonesia Sosial Teknologi:p–ISSN: 2723 -6609e-ISSN : 2745-5254Vol. 2, No.4 April2021

[4] Easttom, C. (2020). Vulnerability Assessment and Management. *The NICE Cyber Security Framework*, *4*(2), 241–258.

[5] Edy Susanto. (2019). *Mengenal Vulnerability Analysis*. Kompasiana.

[6] Chayadi oktomy noto susanto (2020). *Security assessment using nessus tool to determine security gaps on the repository web application in educational institutions. Emerging information science and technology* vol. 1, no. 2, (2020), pp. 58-62.

[7] Eko prasetyo, s., & hassanah, n. (2021). Analisis keamanan website universitas internasional batam menggunakan metode issaf. *Jurnal ilmiah informatika*, *9*(02), 82–86.

[8] Feradhita. (2019). *Metode Pentest: Black-Box, Grey-Box, dan White-Box Testing*. Logique.

[9] Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45.

[10] Hafizulhaq, F. (2021). *Brute Force: Pengertian, Metode, dan Cara Mencegahnya*. Exabytes.

[11] Hidayanto, B. C. (2018). *Mahasiswa menggunakan framework vapt (studi kasus : sister universitas jember) evaluation of student information system application security using vapt framework (case study : sister universitas jember) mahasiswa menggunakan framework vapt*.

[12] IT Governance Indonesia. (2021). *Mengenal VAPT Testing*. ITG.ID.

[13]Julismail.(2020). *Penetration Testing*. ITG.ID.

[14] Kerentanan, P., Penetrasi, D. A. N., Listartha, I. M. E., Arna, G., Saskara, J., & Santyadiputra, [1 5] S. (2021). *KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications*. *4*(2), 1–14.

[16] M. Askari Zakariah, Vivi Afriani, K. M. Z. (2020). *Metodologi Penelitian Kualitatif, Kuantitatif, Action Research, Research And Development (R n D)*.Google Books.

[17] M. Prawiro. (2019). *Pengertian Aplikasi: Arti, Fungsi, Klasifikasi, dan Contoh Aplikasi*. MAxmanroe.

[18] M. Prawiro. (2019). *Pengertian Aplikasi: Arti, Fungsi, Klasifikasi, dan Contoh Aplikasi*. MAxmanroe.

[19] Mahardika, F. (2017). *Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)*.*02*(02), 1–8.

[20] Muhamad Alfin Mubarok. (2018). *Mengenal OpenSID*. Putra Kudus

[21] Muhammad Bakri. (2022). *Vulnerabality*. Edmodo.Id.

[22] Mykhel David. (2017). *Jenis Serangan Yang Menyerang Website*. Dumetschool. Prasetia, T. (2019). *OWASP*. IDwebhost.

[23] Ratna Patria. (2022). *Penjelasan Who.Is*. DomainNesia.

[24] Sahtyawan, R. (2019). Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment). *Journal of Information System Management (JOISM)*, *1*(1), 18–22.

[25]Soehartono,Hendrastuti,Sri.(2019) *Administrasi kependudukan berbasis registrasi*

[26] Slamet JP (2021) *Sistem informasi pada Aplikasi Website.*

[27] Widyatama, S. (2018). Bab II Landasan Teori. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.