Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales

Wahyudin[1], Heri Kuswara[2*], Resti[3], Sopiyan Dalis[4]

[1,2,3,4]Universitas Bina Sarana Informatika
Jl. Kramat Raya No 98, RT 2/RW 9, Kwitang, Kec Senen, Kota Jakarta Pusat, Indonesia

e-mail: [1]wahyudin.whd@bsi.ac.id, [2] heri.hrk@bsi.ac.id, [3]17190655@bsi.ac.id, [4]sopiyan.spd@bsi.ac.id

(*) Corresponding Author

Artikel Info : Diterima : 27-11-2023 | Direvisi : 18-01-2024 | Disetujui : 29-01-2024

Abstrak - Perkembangan perdagangan elektronik melalui website berbasis point of sales terkait erat dengan tingkat pertumbuhan internet, karena perdagangan elektronik berjalan melalui jaringan dan koneksi Internet. Namun, semakin banyaknya website berbasis point of sale yang dibangun, semakin besar pula kemungkinan terjadinya serangan cyber yang dapat merugikan website tersebut. Oleh karena itu, keamanan website menjadi sangat penting untuk diperhatikan. Salah satu metode yang dapat dilakukan untuk menjaga keamanan website adalah dengan melakukan Vulnerability Assessment. Vulnerability Assessment adalah sebuah proses pencarian celah keamanan pada sistem informasi atau jaringan computer dengan tujuan untuk mengidentifikasi potensi kerentanan keamanan dan mengambil langkah pencegahan sebelum serangan terjadi. Teknik vulnerability assesment yang digunakan adalah menggunakan aplikasi pemindai kelemahan untuk mengidentifikasi celah keamanan pada sistem dan aplikasi seperti nikto, nmap, zenmap dan owasp ZAP. Berdasarkan pengujian dengan tool Owasp ZAP, hasil dari scanning yang telah dilakukan pada website sakupos.com yang merupakan website berbasis points of sales bahwa terdapat kerentanan pada website tersebut. Hasil pengujian menunjukkan Level Kerentanan (Risk Assessment) serta Rekomendasi solusi yang bisa digunakan untuk mencegahnya. Terdapat ada 10 kerentanan yang terdeteksi, ditemukan 7 kerentanan dengan level/tingkat resiko Medium, 2 kerentanan dengan tingkat resiko Low, Serta 1 kerentanan lainnya di tingkat resiko Informational.

Kata Kunci : Keamanan website, Vulnerability Assesment, Website

Abstracts *- The development of electronic commerce through point of sales based websites is closely related to the growth rate of the internet, because electronic commerce runs through networks and Internet connections. However, the more point of sale based websites that are built, the greater the possibility of cyber attacks that could harm the website. Therefore, website security is very important to pay attention to. One method that can be used to maintain website security is to carry out a Vulnerability Assessment. Vulnerability Assessment is a process of searching for security gaps in an information system or computer network with the aim of identifying potential security vulnerabilities and taking preventative steps before an attack occurs. The vulnerability assessment technique used is using a weakness scanner application to identify security gaps in systems and applications such as Nikto, Nmap, Zenmap and Owasp ZAP. Based on testing with the Owasp ZAP tool, the results of scanning carried out on the sakupos.com website, which is a points of sales based website, show that there is a vulnerability on the website. The test results show the Level of Vulnerability (Risk Assessment) as well as recommended solutions that can be used to prevent it. There were 10 vulnerabilities detected, 7 vulnerabilities were found with a Medium risk level, 2 vulnerabilities with a Low risk level, and 1 other vulnerabilities at the Informational risk level.*

Keywords : Website Security, Vulnerability Assesment, Website

PENDAHULUAN

Website berbasis Point Of Sales(POS) merupakan website yang sistemnya dirancang khusus untuk mempermudah dan mempercepat proses transaksi dalam operasional bisnis pada umumnya. Biasanya POS terdiri dari software dan hardware yang sudah dirancang agar sesuai dengan kebutuhan bisnis yang diinginkan. Menurut (ukmindonesia.id, 2024) sistem POS sudah banyak sekali digunakan oleh beragam jenis usaha saat ini, seperti

restoran, coffee shop (kedai kopi), barbershop, hingga laundry kiloan Saat ini penggunaan website berbasis POS semakin marak di internet seiring dengan perkembangan teknologi internet saat ini.

Dengan kecanggihan Internet saat ini yang bisa mengirimkan berbagai bentuk data seperti teks, grafik, gambar, animasi, bahkan video, menyebabkan banyak kalangan bisnis yang memanfaatkan teknologi ini dengan membuat hompage untuk mempromosikan usahanya dan dengan adanya Internet proses pemasaran dan penjualan dapat dilakukan kapan saja dan dimana saja tanpa terikat ruang dan waktu(Kusbandono & Rosyad, 2019). Namun, seiring berkembangnya teknologi khususnya internet, maka banyak sekali kejahatan yang disebut dengan *cyber crime* berkembang di dunia internet. Kejahatan dunia maya ini termasuk dalam kategori pemalsuan data, peretasan, sabotase, dan pemerasan(S. Ghobadi, 2020). *Cybersecurity is a subset of Information Technology It is basically used to ensure both programming and equipment parts. Along these lines, in the coming years, this innovation assumes an essential part. There are a few things identified with Cybersecurity like Physical security, Network security, Application security, Information security, these are to be ensured in the right manner for any fruitful working of any organization*.(Kumar, 2021). Menjamurnya aplikasi berbasis web menjadi tantangan sendiri bagi para pengembang aplikasi berbasis web dalam mengembangkan aspek keamanan. Vulnerability Assesment terhadap web aplikasi E-Learning bertujuan untuk mendeteksi kerentanan, mendeskripsikan kerentanan(Aziz, 2021)

Kerentanan pada aplikasi berbasis web dapat bervariasi tergantung pada modul, perpustakaan (library), CMS, dan database yang digunakan. Oleh karena itu, aplikasi berbasis web memiliki banyak titik potensial yang dapat menjadi target serangan(Budiman et al., 2021). *The rapid increase of the machinery whether its mobile or computer systems have brought more advance and efficient Windows, Web and Mobile applications but it also increases the complexity in systems which ultimately leads to vulnerabilities that attackers use to exploit the victim systems. In decades, the uses of web applications and web hacking activities have been amplified swiftly*(Khera et al., 2019). Semakin banyaknya website yang dibangun, semakin besar pula kemungkinan terjadinya serangan *cyber* yang merugikan website tersebut. Oleh karena itu, keamanan website menjadi sangat penting untuk diperhatikan. Salah satu metode yang dapat dilakukan untuk menjaga keamanan website adalah dengan melakukan *Vulnerability Assessment. Vulnerability Assessment* adalah suatu proses untuk mengidentifikasi kerentanan yang mungkin ada dalam sistem keamanan yang terdapat dalam informasi ekosistem teknologi. Kerentanan dalam konteks informasi teknologi merujuk pada kelemahan atau potensi celah keamanan yang jika dieksploitasi, dapat mengakibatkan terjadinya serangan atau gangguan pada system. Metode ini meliputi proses pengumpulan data, identifikasi celah keamanan, dan memberikan rekomendasi penyelesaian celah keamanan. Tujuan dari penelitian ini adalah untuk memberikan gambaran mengenai pentingnya menjaga keamanan website dan bagaimana *Vulnerability Assessnment* dapat diaplikasikan pada website. Diharapkan, dengan penelitian ini dapat membantu pengguna website untuk meningkatkan keamanan website mereka dan mengurangi resiko serangan *cyber*(Raazi Irfan Murti et al., 2023).

Untuk mencegah serangan tersebut, pengembang web perlu melakukan penilaian kerentanan (vulnerability assessment). Penilaian kerentanan ini bertujuan untuk mengidentifikasi, mendefinisikan, mengelompokkan, dan memberikan prioritas terhadap kerentanan dalam sistem web(Mira Orisa and M. Ardita, 2021)

Vulnerability Assessment (VA) adalah evaluasi komprehensif dan mendalam terhadap aspek-aspek keamanan, termasuk keamanan informasi, hasil pemindaian jaringan, pengelolaan sistem, konfigurasi, kesadaran keamanan dari pihak yang terlibat, serta aspek keamanan fisik, dengan tujuan untuk mengidentifikasi semua potensi kerentananankritis yang mungkin ada(Darojat et al., 2022).

Vulnerability assessment is a process that defines, identifies, classifies security gaps (vulnerabilities) on computers, networks, or communication infrastructure. In addition, vulnerability analysis can estimate the effectiveness of the proposed preventive actions and evaluate their actual effectiveness after they are implemented(Mantra et al., 2019). Kelemahan (vulnerability) dalam sebuah sistem informasi dapat disebabkan oleh faktor internal maupun faktor eksternal. Vulnerability Assessment (VA) juga dapat dianggap sebagai salah satu bentuk kontrol preventif, mirip dengan perangkat antivirus yang bertujuan untuk mencegah terjadinya kejadian pada sistem(Wibowo et al., 2019). Vulnerability Assesment dalam melakukan scannin terhadap sistem, untuk dapat mengetahui kekelemahan-kelemahan terhadap sistem yang dibangun, sehingga dapat dilakukan upaya perbaikan terhadap sistem agar menjadi lebih baik(Satriawan et al., 2019)

Penelitian terbaru mengenai keamanan sistem informasi yang dilakukan oleh Alwi dan rekan-rekannya pada tahun 2020 memiliki judul "Penganalisisan Keamanan Situs Web dengan Pendekatan *Footprinting* dan Pemindaian Kerentanan". Penelitian ini menerapkan dua metode analisis utama, yaitu tapak kaki (pencarian informasi terkait target) dan kerentanan pemindaian (*vulnerability scanning*). Target dari penelitian ini adalah salah satu situs web universitas di Indonesia. Penelitian ini didukung oleh berbagai alat seperti Zenmap, Nmap, Nikto, dan OWASP-ZAP. Hasil penelitian mengungkapkan adanya beberapa kerentanan pada situs web tersebut, masing-masing memiliki tingkat risiko yang bervariasi, mulai dari risiko rendah hingga tinggi(Irawadi Alwi & Budi Ilmawan, 2021). Permasalahan yang ada pada web sakupos.com adalah masih rentannya terhadap serangan *cyber* untuk disusupi oleh hacker, pergerakan pola kejadian *cyber* sangat cepat dan sangat sulit ditangani

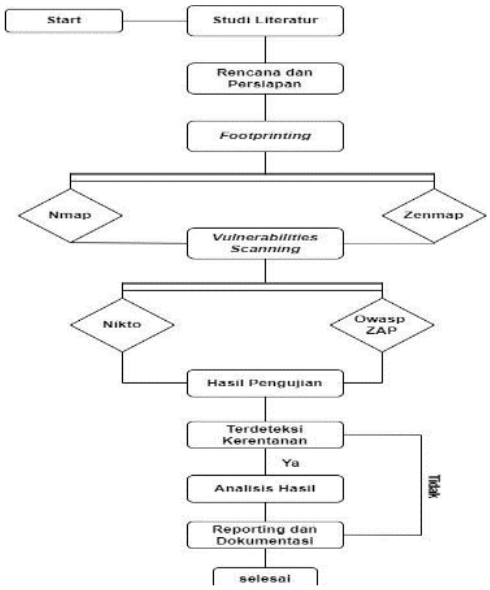
dikarenakan masih rendahnya kesadaran akan adanya serangan *cyber*. Maka dari itu perlu dilakukan pengetesan kerentanan celah pada web tersebut.

Adapun *tools* yang digunakan diantaranya adalah Nmap, Zenmap, Nikto, dan juga OwaspZAP. OWASP (*Open Web Application Security Project*) adalah sebuah komunitas penelitian independen yang terdiri dari ilmuwan, peneliti, dan perusahaan swasta. Mereka merilis laporan, artikel, perangkat, dan dokumen yang bersifat open source(Darojat et al., 2022). Zenmap merupakan aplikasi multi platform sebagai interface sederhana untuk apikasi Nmap. Nmap (*Network Mapper*) tetap menjadi perangkat lunak yang populer dan digunakan secara luas. Nmap berfungsi untuk melakukan pemindaian port dan memantau jaringan komputer. Dengan Nmap, kita dapat mengidentifikasi potensi kerentanan dalam jaringan yang memiliki tingkat keamanan yang rendah, sehingga dapat membuka peluang bagi penyusupan(Fahlevi & Putri, 2021). *Nikto which runs on a Kali-linux was used to identify the server and to test for Secured Sockets Layer (SSL) and Web Application Firewall (WAF). To demonstrate how to exploit web applications using SQL injection commands*(Evwiekpaefe et al., 2021).

Dengan adanya penelitian ini, perusahaan yang mengoperasikan website sakupos.com dapat mengetahui kelemahan atau kerentanan yang ada pada website mereka dan dapat mengambil tindakan yang tepat untuk meningkatkan keamanan website tersebut. Selain itu, hasil penenlitian ini juga dapat menjadi referensi atau panduan bagi organisasi atau individu lain yang memiliki website untuk meningkatkan tingkat keamanan website mereka. Penelitian ini juga menunjukkan bahwa metode *Vulnerability Assessment* adalah salah satu cara yang efektif untuk mengidentifikasi kelemahan-kelemahan dalam aplikasi. Metode ini dapat membantu pengembang dan organisasi untuk mengambil langkah-langkah proaktif dalam memperbaiki kelemahan-kelemahan dalam aplikasi sebelum terjadi serangan cyber yang merugikan dan sebagai rekomendasi kedepannya.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif. Penelitian ini berfokus pada server web sakupos.com yang dilakukan dengan melakukan identifikasi dan kemudian mendefinisikan permasalahan, lalu selanjutnya melakukan uji coba dan menganalisis hasil dari pengujian yang telah dilakukan. Adapun langkah-langkahnya yaitu antara lain studi literatur, Rencana dan Persiapan, footprinting, Vulnerabilities Scanning, menganalisis hasil dan reporting.



Sumber : Hasil Penelitian (2023)

Gambar 1. Alur Proses Prosedur Penelitian

Analisis penelitian

1. Identifikasi Kerentanan

Tinjauan penilaian kerentanan harus memahami toleransi resiko perusahaan serta model dan kelemahan bisnis perusahaan tersebut. Selanjutnya daftar lengkap dari kerentanan dalam sistem informasi dan sistem keamanan infrastruktur perusahaan kemudian disusun.

2. Menentukan Titik Kerentanan

Setelah pemindaian, langkah selanjutnya adalah menentukan jenis kerentanan seperti kerentanan injection(SQL Injection), kerentanan authentication dan access control. Tujuan lainnya adalah untuk mencari penyebab kerentanan tersebut.

3. Menilai Resiko

Penilaian risiko bertujuan untuk mengetahui kerentanan utama. Semua kerentanan kemudian dipisahkan dan dikategorikan menurut tingkat keparahannya, agar dapat menentukan kerentanan mana yang harus diperbaiki terlebih dahulu, dari *high, medium,* dan *low*.

4. Remediasi

Remediasi merupakan perbaikan atau tindakan untuk menghilangkan kerentanan dalam sistem keamanan. Jika kerentanan yang terdeteksi tidak segera diremediasi, kerentanan tersebut dapat menjadi lebih buruk dan meningkatkan potensi serangan siber.

5. Mitigasi

Tujuan mitigasi adalah untuk meminimalkan peluang buruk atau kerentanan yang akan muncul di kemudian hari. Ada beberapa hal yang dapat dilakukan seperti penggantian perangkat lunak atau perangkat keras yang tidak lagi dapat menjamin keamanan, penerapan enkripsi, pembuatan dan penyediaan kontrol keamanan baru, dan penerapan pemantauan keamanan berkelanjutan.

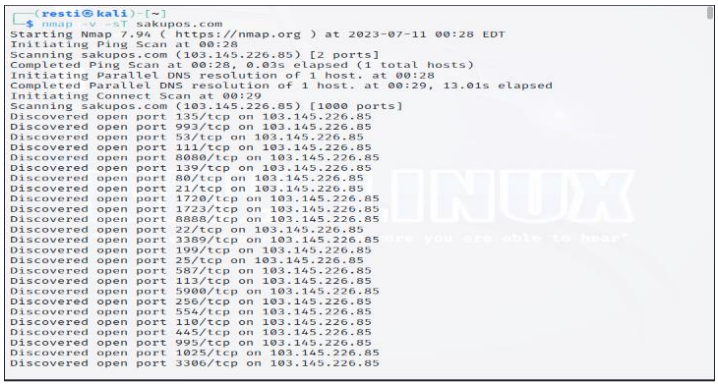
HASIL DAN PEMBAHASAN

Proses yang dilakukan untuk menemukan celah kerentanan pada website sakupos.com meliputi Footprinting, Vulnerability Scanning, dan terakhir melakukan Analisis hasil dan Rekomendasi.

1. Footprinting

a. Nmap

Pengujian dilakukan dengan memanfaatkan alat pemindaian NMAP versi 7.94, dan dalam hal ini, domain yang diperiksa adalah sakupos.com. Untuk menjalankan pengujian, perintah yang digunakan adalah sebagai berikut: nmap -v -sT sakupos.com, dapat dilihat pada gambar dibawah.



Sumber : Hasil Penelitian (2023)

Gambar 2. Pengujian Nmap Pada web Sakupos.com

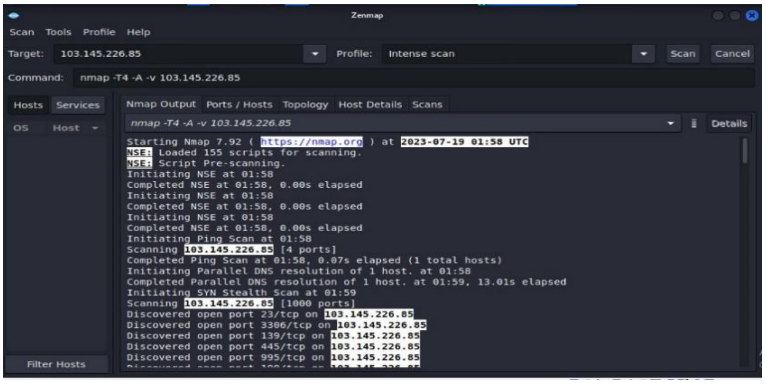
Berdasarkan scanning yang telah dilakukan dengan menggunakan tools Nmap, seperti pada gambar 3 maka didapatkan beberapa informasi yang telah di rangkum diantaranya yaitu sebagai berikut:

1). IP (Internet Protocol) Address: IP yang digunakan oleh Website sakupos.com adalah 103.145.226.85.

2). Dari hasil scanning yang telah dilakukan menunjukkan ada banyak port yang terbuka dan Service yang berjalan pada website sakupos.com. Identifikasi terhadap port dan service yang terbuka dapat memberikan penyerang informasi tentang kerentanan potensial yang dapat dieksploitasi. Dengan menyembunyikan informasi ini, maka dapat mengurangi risiko serangan.

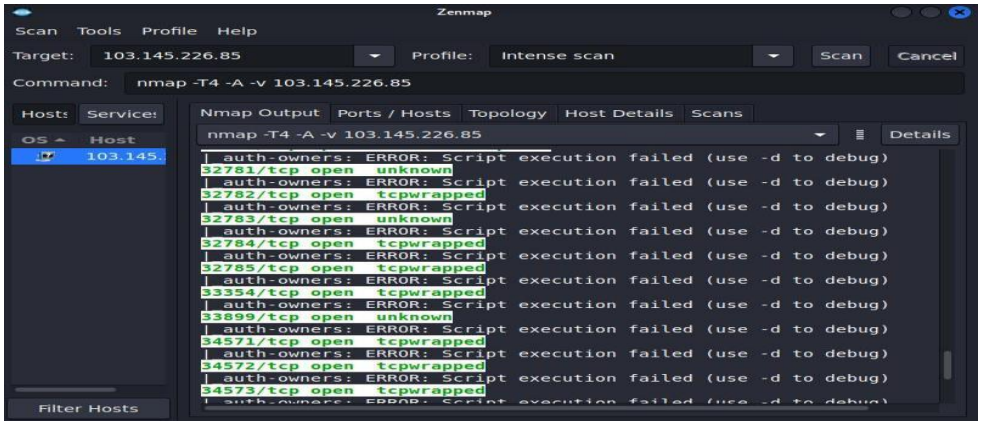
b. Zenmap

Pengujian dengan menggunakan tool Zenmap dengan memasukkan alamat Domain/IP address dari website sakupos.com di kolom Target: 103.145.226.85 lalu menuliskan perintah pada Command: nmap –T4 –A –v 103.145.226.85.



Sumber : Hasil Penelitian (2023)
Gambar 3. Hasil Pengujian tools Zenmap

Berdasarkan pengujian dengan menggunakan tools Zenmap, hasil scanning seperti pada gambar 4 maka diperoleh beberapa informasi yang terdapat pada website sakupos.com diantaranya:
Proses scanning dengan zenmap maka didapat bahwa masih ada banyak port-port yang terbuka pada website sakupos.com ini bisa dilihat di gambar 4. Berikut penjelasan dari port yang terbuka di website sakupos.com :
ini berarti bahwa Nmap telah menemukan port TCP dengan nomor 32781 dan menetapkan status "open". Status "open" menunjukkan bahwa port tersebut aktif dan dapat menerima koneksi dari perangkat lain.
Jika Anda menemukan port yang terbuka dan tidak diharapkan, Anda perlu memeriksanya lebih lanjut untuk memastikan keamanan sistem



Sumber : Hasil Penelitian (2023)
Gambar 4. Ports yang terbuka

. Dapat dilihat pada gambar 5 bahwa *Operating system* yang digunakan oleh website sakupos.com adalah menggunakan OS *Fingerprint, serta menggunakan Traceroute (using port 80/tcp).*

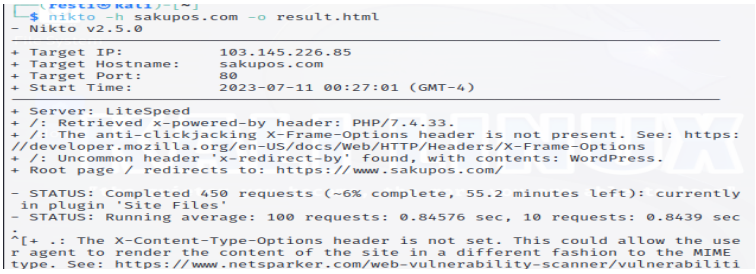
HOP	RRT	ADDRESS
1	5.1o ms	192.168.43.1
2	...3	-
4	63.54 ms	103.145.226.85

Sumber : Hasil Penelitian (2023)
Gambar 5. Hasil Traceroute sakupos.com

2. Vulnerabilities Scanning

a. Nikto

Berdasarkan hasil scanning yang telah dilakukan dengan menggunakan tools Nikto yang dijalankan melalui OS/system Kali Linux dengan tujuan untuk mencari informasi mengenai laman domain/website sakupos.com dengan IP Address 103.145.226.85. Pengujian dilakukan dengan cara menuliskan perintah: nikto –h sakupos.com –o result.html.



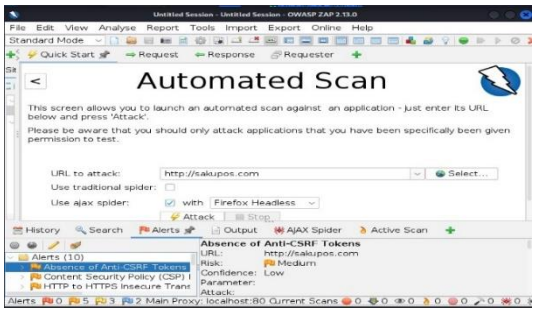
Sumber : Hasil Penelitian (2023)
Gambar 6. Hasil Pengujian Nikto

berikut adalah kerentanan yang ditemukan dengan perintah tersebut yaitu sebagai berikut:

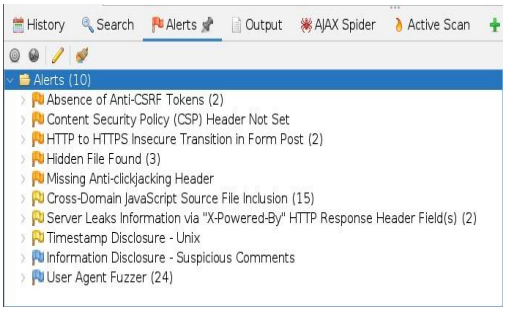
1) *The anti-iclickjacking X-Frame-Options header is not present dengan Risk Assessment* di level Medium. Berarti Header HTTP X-Frame-Options digunakan untuk mengontrol apakah halaman web dapat dimuat dalam suatu frame atau iframe. Keberadaan header ini membantu melindungi situs web dari serangan clickjacking. Rekomendasi solusi yaitu dengan Mengaktifkan *Header X-Frame-Options*. Yaitu menambahkan perintah berikut Header always append X-Frame-Options SAMEORIGIN. Atur SAMEORIGIN untuk membatasi halaman web agar hanya dapat dimuat dalam frame yang berasal dari domain yang sama.
2) The X-Content-Type-Options header is not set dengan Risk Assessment di level Low. Berarti Header HTTP X-Content-Type-Options digunakan untuk mencegah serangan MIME sniffing, yang dapat menyebabkan interpretasi jenis konten yang tidak diinginkan. Rekomendasi untuk mengatasi nya yaitu Tambahkan baris berikut untuk mengaktifkan header X-Content-Type-Options. Contoh untuk Apache: Header always set X-Content-Type-Options "nosniff". Nilai "nosniff" mencegah browser untuk melakukan sniffing terhadap tipe konten dan mematuhi tipe konten yang disediakan oleh server

b. Owasp ZAP

Pengujian dilakakukan dengan menuliskan alamat Domain atau IP Address dari website yang ingin kita uji pada kolom "*URL to Attack*" kemudian klik "*Attack*". Setelah itu akan muncul hasil daftar kerentanan yang ada pada website yang kita uji seperti gambar 7.



Sumber : Hasil Penelitian (2023)
Gambar 7. Laman Tampilan ZAP



Sumber : Hasil Penelitian (2023)
Gambar 8. Hasil Pengujian Owasp ZAP

Berdasarkan hasil pengujian yang telah dilakukan pada alamat domain sakupos.com dengan IP Address 103.145.226.85 dengan menggunakan *tools* Owasp ZAP, gambar 8 menunjukkkan kerentanan yang terdapat website tersebut. Pada tahap identifikasi, berbagai tingkat kerentanan keamanan dalam Sistem Informasi Laporan Keamanan Aplikasi Web diidentifikasi dengan tingkat tinggi dan menengah. Tiap kerentanan memiliki

konsekuensi yang bervariasi, oleh karena itu, tujuan dari laporan ini adalah untuk mencatat setiap kerentanan yang terdeteksi dan menyusun rekomendasi berdasarkan jenis kerentanan yang telah diidentifikasi. Beberapa temuan celah keamanan yang ditemukan diantaranya adalah sebagai berikut:

Tabel 1. Daftar Kerentanan

No	Jenis Kerentanan	Risk Assesment	Keterangan	Solusi
1.	Absence of Anti – CRSF Tokens	Medium	Kerentanan ini dapat memungkinkan serangan Cross-Site Request Forgery (CSRF) yang berpotensi mengakibatkan pelaksanaan tindakan tertentu dalam aplikasi atas nama pengguna yang telah masuk, seperti pencurian akun atau perubahan informasi akun.	Gunakan kata sandi yang unik untuk setiap halaman, serta pastikan kode tidak dapat dengan mudah ditebak.
2.	Content Security Police (CSP)	Medium	Content Security Policy (CSP) adalah pengaturan ekstra yang di implementasikan melalui header respons HTTP. Ini bertujuan untuk mengatasi potensi serangan Cross-Site Scripting (XSS).	Penting untuk memastikan bahwa server web, server aplikasi, dan komponen lainnya dikonfigurasi untuk mengatur header Content Security Policy (CSP).
3.	HTTP to HTTPS Insecure Transition In From Post	Medium	Pemeriksaan ini bertujuan untuk mendeteksi halaman HTTP yang tidak aman yang mengandung formulir HTTPS. Isu utamanya adalah formulir HTTPS yang berada dalam lingkungan yang tidak aman, yang dapat mengakibatkan risiko penggantian atau pemalsuan data.	Pastikan halaman pengarah yang menyelenggarakan formulir aman menggunakan protokol HTTPS. Dengan demikian, Anda dapat meminimalkan potensi risiko yang mungkin timbul akibat kehadiran formulir aman dalam lingkungan yang tidak terlindungi secara memadai.
4.	Hidden File Found	Medium	Celah ini dapat mengungkapkan informasi administratif, konfigurasi, atau data kredensial yang dapat dimanfaatkan oleh pihak jahat untuk melancarkan serangan lebih lanjut atau untuk melakukan taktik rekayasa sosial.	Evaluasi apakah komponen tersebut benar-benar diperlukan dalam lingkungan produksi. Jika tidak, pertimbangkan untuk menonaktifkannya.
5.	Missing anti-clickjacking Header	Medium	Dalam halaman tersebut, terdapat inklusi satu atau beberapa file skrip dari domain yang tidak terkait dengan aplikasi itu sendiri.	Penting untuk memastikan bahwa file sumber *JavaScript* hanya dimuat dari sumber yang dapat dipercayai seperti MDN Javascript, javascript.info dan tidak dikendalikan oleh pengguna akhir dari aplikasi.
6.	Server Leaks Information via “X-Powered-By”HTTP Response Header Fields	Low	Server web atau aplikasi mengungkapkan informasi melalui header respons HTTP "X-Powered-By". Akses terhadap informasi ini dapat membantu penyerang dalam mengidentifikasi kerangka kerja atau komponen lain yang digunakan oleh aplikasi web dan potensi kerentanan yang mungkin ada dalam komponen tersebut.	Pastikan bahwa konfigurasi server web, server aplikasi, penyeimbang beban, dan lainnya telah disesuaikan untuk menghilangkan atau menyembunyikan header "*X-Powered-By*".

7.	Cross-Domain JavaScript Source File Inclusion	Medium	Dalam halaman tersebut, terdapat inklusi satu atau beberapa file skrip dari domain yang tidak terkait dengan aplikasi itu sendiri.	Penting untuk memastikan bahwa file sumber *JavaScript* hanya dimuat dari sumber yang dapat dipercayai seperti MDN Javascript, javascript.info dan tidak dikendalikan oleh pengguna akhir dari aplikasi.

Sumber : Hasil Penelitian (2023)

3. Analisis Hasil

Berdasarkan proses pengujian yang telah dilakukan dengan menggunakan *tools-tools* yang terdapat pada Kali Linux. Pengujian dengan menggunakan *tool* NMap, Zenmap, Nikto dan Owasp ZAP, hasil pengujian pada website sakupos.com dengan metode *scanning* maka diketahui bahwa IP *Address* yang digunakan oleh sakupos.com adalah 103.145.226.85, dan terdapat ada banyak sekali *ports* yang terbuka serta *service* yang berjalan, dimana *ports-ports* yang terbuka tersebut mempunyai fungsi dan peran yang berbeda. Dari proses pengujian juga diketahui Level Kerentanan (*Risk Assessment*) dari website sakupos.com. dari masing-masing tools diatas tidak ada tools yang paling handal namun masing-masing tools saling melengkapi untuk menjelaskan kerentanan dalam suatu website. selanjutnya memberikan rekomendasi solusi yang bisa digunakan untuk mencegahnya. Tiap kerentanan memiliki konsekuensi yang bervariasi, oleh karena itu, tujuan dari laporan ini adalah untuk mencatat setiap kerentanan yang terdeteksi dan menyusun rekomendasi berdasarkan jenis kerentanan yang telah teridentifikasi. Terdapat ada 10 kerentanan yang terdeteksi, ditemukan 7 kerentanan dengan level/tingkat resiko *Medium* yaitu :

a) *Absence of Anti – CSRF Tokens* yaitu berarti situs web tidak menerapkan perlindungan CSRF yang memadai, Cross-Site Request Forgery (CSRF) adalah serangan di mana penyerang mencoba membuat pengguna melakukan tindakan yang tidak disadari tanpa persetujuannya,

b) *Content Security Policy (CSP) Header Not Set* ini menunjukkan bahwa situs web tidak mengimplementasikan *Content Security Policy (CSP). Content Security Policy* adalah langkah keamanan yang bertujuan untuk melindungi situs web dari serangan berbasis client-side seperti XSS (*Cross-Site Scripting*) dengan membatasi sumber-sumber yang diizinkan untuk ditampilkan atau dieksekusi oleh browser.

c) *HTTP to HTTPS Insecure Transition in Form Post,* Menjelaskan ada formulir pada situs web yang diakses melalui protokol HTTP, tetapi formulir tersebut mengarahkan permintaan POST ke URL yang menggunakan protokol HTTPS. Ini dapat meningkatkan risiko keamanan karena data yang dipostkan melalui formulir tidak terenkripsi saat berpindah dari HTTP ke HTTPS, menyebabkan potensi kebocoran informasi sensitif

d) *Hidden File Found,* menemukan file yang tidak terlihat secara umum, atau file yang mungkin tidak diinginkan atau diketahui oleh administrator atau pengguna biasa. Jika file tersembunyi tidak dibutuhkan atau merupakan potensi risiko, pertimbangkan untuk menghapus atau membatasi akses ke file tersebut.

e) *Missing Anti-clickjacking Header,* menunjukkan bahwa situs web yang diuji tidak mengimplementasikan atau tidak menyertakan header yang diperlukan untuk melawan serangan clickjacking.

f) *Cross-Domain JavaScript Source File Inclusion,* serangan keamanan yang terjadi ketika penyerang mencoba menyisipkan dan mengeksekusi skrip JavaScript dari domain yang berbeda ke dalam halaman web target. Serangan ini memanfaatkan kelemahan dalam kebijakan keamanan penyisipan sumber daya lintas domain yang diimplementasikan oleh browser, yang biasanya disebut sebagai kebijakan Same-Origin Policy (SOP).

2 kerentanan dengan tingkat resiko Low yaitu

a) *Server Leaks Information via "X-Powered-By" HTTP Response Header Fields, respons HTTP "X-Powered-By",* itu berarti bahwa server memberikan detail tentang teknologi atau perangkat lunak yang digunakan untuk menangani permintaan web, Mengungkapkan informasi rinci tentang teknologi server dapat menimbulkan risiko keamanan. Penyerang dapat memanfaatkan informasi ini untuk mengidentifikasi kerentanan yang terkait dengan versi perangkat lunak yang diungkapkan.

b) *Timestamp Disclosure – Unix* pada sistem operasi Unix terjadi ketika informasi terkait waktu eksekusi atau modifikasi suatu file atau direktori diungkapkan kepada pengguna yang tidak berwenang. Hal ini dapat terjadi jika aplikasi atau server mengembalikan informasi timestamp yang seharusnya bersifat rahasia, seperti waktu pembuatan atau modifikasi suatu file.

Serta 1 kerentanan lainnya di tingkat resiko *Informational* yakni *Information Disclosure - Suspicious Comments* yaitu *Information Disclosure* melalui *Suspicious Comments* terjadi ketika komentar-komentar yang tidak

semestinya atau mencurigakan disertakan dalam kode sumber aplikasi, skrip, atau halaman web. Komentar-komentar ini mungkin berisi informasi sensitif atau rincian tentang implementasi aplikasi yang seharusnya tidak diketahui oleh pengguna atau pihak yang tidak berwenang. Hal ini dapat memberikan peluang bagi penyerang untuk memperoleh wawasan tentang sistem atau memanfaatkan celah keamanan yang mungkin ada.

KESIMPULAN

Berdasarkan hasil analisa hasil screnning port yang telah dilakukan pada Website sakupos.com, dapat disimpulkan bahwa di website tersebut masih ditemukan adanya celah kerentananan namun tidak ditingkat resiko yang tinggi, karena tidak ditemukan celah kerentanan dengan tingkat resiko (Risk Assessment) di level High.

Penelitian ini dilakukan dengan tujuan untuk mencari celah/kerentanan keamanan dari website sakupos.com untuk kemudian di Analisis, pada tahap Vulnerabilies Scanning dilakukan dengan menggunakan tools Vulnerability Assessment yaitu Owasp ZAP ditemukan 6 kerentanan dengan vulnerability Risk Medium, 2 risk Low, 2 risk Informational dan di tools Nikto ditemukan 1 vulnerability risk Medium, dan 1 risk di tingkat Low.

Setelah diketahui celah kerentanan yang ada pada website sakupos.com Penulis lalu memberikan Rekomendasi/solusi yang bisa digunakan untuk mencegah serangan dan mungkin bisa membantu perbaikan kerentanan tersebut.

REFERENSI

Aziz, M. (2021). Vulnerability assesment untuk mencari celah keamanan web aplikasi e-learning pada Universitas XYZ. *JECSIT*, *1*(1).

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. *Jurnal Komputasi*, *9*(2), 1–10.

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. *Jurnal Sistem Informasi Bisnis*, *12*(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44

Evwiekpaefe, A., Evwiekpaefe, A. E., & Habila, I. (2021). Implementing SQL Injection Vulnerability Assessment of an E-commerce Web Application using Vega and Nikto Tools. *Afr. J. Comp. & ICT*, *14*(1), 1–8. https://afrjcict.net

Fahlevi, M. R., & Putri, D. R. D. (2021). Analisis Monitoring & Kinerja Sistem Keamanan Jaringan Komputer Menggunakan Nmap (Studi Kasus: Raz Hotel & Convention Medan). *It (Informatic Technique) Journal*, *9*(1), 35. https://doi.org/10.22303/it.9.1.2021.35-43

Irawadi Alwi, E., & Budi Ilmawan, L. (2021). Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *Informatics Journal*, *6*(3), 131–135.

Khera, Y., Kumar, D., Sujay, S., & Garg, N. (2019). Analysis and Impact of Vulnerability Assessment and Penetration Testing. *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019, February 2019*, 525–530. https://doi.org/10.1109/COMITCon.2019.8862224

Kumar, S. G. V. P. (2021). Vulnerability Assesment in Web based Applications. *International Journal for Research in Applied Science and Engineering Technology*, *9*(5). https://doi.org/10.22214/ijraset.2021.34604

Kusbandono, D., & Rosyad, S. (2019). Upaya Pengembangan Usaha Kecil Dan Menengah (Ukm) Dengan Memanfaatkan E-Commerce Untuk Meningkatkan Minat Pembelian Konsumen Terhadap Penjualan Bibit Ikan Di Desa Plosobuden Kec. Deket. *E-Prosiding SNasTekS*, *1*(1), 381–390.

Mantra, I. G. N., Hartawan, M. S., Saragih, H., & Rahman, A. A. (2019). Web vulnerability assessment and maturity model analysis on Indonesia higher education. *Procedia Computer Science*, *161*. https://doi.org/10.1016/j.procs.2019.11.229

Mira Orisa and M. Ardita. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web. *Jurnal Mnemonic*, *4*(1), 16–19.

Raazi Irfan Murti, Dwitawati Ima, & Putri, N. (2023). Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh. *JINTECH: Journal Of Information Technology*, *4*(1), 1–15.

S. Ghobadi. (2020). Sejarah dan Perkembangan Internet Di Indonesia. *Jurnal Mitra Manajemen*, *5*, 68–71.

Satriawan, E., Azhar, R., & Hariyadi, I. P. (2019). Implementasi IPS Berbasis Portsentry Dan Vulnerability Assesment Berbasis Openvas Untuk Pengamanan Web Server. *Jurnal BITE*, *1*(1).

ukmindonesia.id. (2024). *Inilah Aplikasi-Aplikasi POS yang Membantu UMKM*. Https://Ukmindonesia.Id. https://ukmindonesia.id/baca-deskripsi-posts/inilah-aplikasiaplikasi-pos-yang-membantu-umkm

Wibowo, F., Harjono, H., & Wicaksono, A. P. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. *Jurnal Informatika*, *6*(2), 212–217. https://doi.org/10.31311/ji.v6i2.5925