Analisis Kerentanan Pada *Website* Sdn 50 Bengkalis Menggunakan Metode *Vulnerability Assesment*

(Studi Kasus :SDN 50 Bengkalis)

M.Febrian Andhika M[1],M. Asep Subandri[2]
Politeknik Negeri Bengkalis
Febrian0479@gmail.com[1], msubandri@polbeng.ac.id[2]

Abstract

This research aims to analyze vulnerabilities and carry out mitigation on the SDN 50 Bengkalis Website using the Vulnerability Assessment method. In today's digital era, information security has become very important, especially for educational institutions that store sensitive data. This study identified various vulnerabilities found on school websites, such as SQL Injection, Cross-Site Scripting (XSS), and insecure configurations. Methods used include security scanning with tools such as OWASP ZAP, Nmap, and Nikto. It is hoped that the results of this research will show that website security is very important, and can improve the security of the website, to protect the personal data of students and staff, and maintain the school's reputation. Thus, this research not only contributes to improving the security of the SDN 50 Bengkalis website, but also provides insight for other institutions in dealing with increasingly complex cyber threats..

Keywords : Website, Vulnerability Assesment, Analisis

1. PENDAHULUAN

Saat ini, teknologi informasi memainkan peran yang sangat penting dalam semua lapisan masyarakat dan bidang kehidupan, dan dalam kehidupan bisnis, ekonomi dan politik. Sebab, teknologi sistem informasi saat ini dapat segera menjawab kebutuhan masyarakat. Sehingga membuat pengolahan data dan menghasilkan informasi yang diperlukan menjadi lebih sederhana, lebih akurat, lebih efisien dan efektif. Namun banyak pihak yang mengambil keuntungan dari perkembangan teknologi secara tidak bertanggung jawab. Mulai dari kasus peretasan, penipuan, bahkan kejahatan siber yang tidak hanya menyerang perorangan namun juga perusahaan/perusahaan dan instansi pemerintah.

Di Indonesia, kejahatan yang umum terjadi di dunia komputer melalui Internet adalah serangan virus, worm, dorm, korupsi cyber dan pencurian informasi pribadi, pinjaman online dan kartu kredit. Kejahatan dunia maya biasanya merupakan kejahatan dunia maya yang menggunakan jaringan komputer sebagai alatnya dan Internet sebagai alatnya. Kejahatan siber dalam arti luas adalah setiap aktivitas ilegal yang dilakukan melalui jaringan komputer dan Internet dengan tujuan memperoleh keuntungan dengan menimbulkan kerugian bagi pihak lain, sedangkan kejahatan siber dalam arti sempit adalah setiap aktivitas ilegal yang bertujuan untuk menyerang. sistem keamanan informasi dan data. mereka memprosesnya dengan sistem computer (Ayu Rifka Sitoresmi. 2023).

Di Indonesia, pemahaman dan penerapan metode penetration testing masih terbatas. Banyak orang belum mengenal berbagai metode penetration testing dan seringkali hanya menggunakan satu metode saja. Penggunaan satu metode ini kurang efektif karena pengujiannya tidak menyeluruh dan cakupannya terbatas. Setiap metode penetration testing memiliki fokus dan keahlian tertentu, sehingga menggunakan hanya satu metode tidak mampu mengidentifikasi semua potensi kerentanan yang ada dalam suatu sistem atau aplikasi. Penelitian lebih lanjut sangat penting karena aplikasi web sering digunakan oleh lembaga

swasta dan pemerintah. Banyak kasus pembobolan situs web dan kebocoran data pada lembaga pemerintahan yang disebabkan oleh berbagai serangan, seperti SQL injection, broken authentication, dan web defacement. Oleh karena itu, pemahaman yang mendalam tentang berbagai metode penetration testing sangat diperlukan untuk meningkatkan keamanan aplikasi web.(Bastian dkk, 2020) (D. N. Cunong dkk, 2020).

Pada Penelitian, ini di analisis beberapa celah keamanan pada Website SDN 50 Bengkalis yang di ambilkan dari domain *.sch.id. bertujuan untuk menganalisis dan melakukan pengujian keamanan menggunakan metode Vulnerability Assesment dan Website Vulnerability Assesment scanning yang di gunakan adalah Owasp ZAP, Nmap dan Nikto. Hasil dari penelitian ini diharapkan menjadi informasi sekaligus evaluasi bagi Website SDN 50 Bengkalis dalam menjaga dan mengembangkan Website sekolah.

2. TINJAUAN PUSTAKA

Beberapa penelitian yang melandasi yaitu penelitian dengan judul "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assesment" permasalahannya Teknologi informasi memainkan peran krusial dalam kehidupan sehari-hari, namun semakin banyak kasus penyalahgunaan seperti peretasan, penipuan, dan kejahatan cyber. Di Indonesia, serangan virus, pencurian data pribadi, deface Website, dan penyalahgunaan kartu kredit sering terjadi melalui Internet. Penelitian ini bertujuan untuk melakukan evaluasi keamanan Website Universitas Singaperbangsa Karawang dengan menggunakan metode Vulnerability Assesment dan alat seperti OWASP ZAP, Nmap, Nikto, dan Acunetix. Fokus utama adalah mengidentifikasi dan menguji kerentanan Website ini terhadap serangan siber (Akmal dkk, 2022).

Penelitian lainnya dengan judul "Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Assesment permasalahannya Keamanan Website SMAN 1 Sumbawa" sangat penting untuk diprioritaskan karena bisa diakses oleh banyak orang secara online. Beberapa waktu yang lalu, Website ini pernah disusupi oleh pihak yang tidak bertanggung jawab, mengubah tampilannya. Kejadian ini menunjukkan bahwa ada celah keamanan yang perlu segera diatasi. Oleh karena itu, penelitian ini akan menggunakan metode Vulnerability Assesment untuk mengidentifikasi, menganalisis, dan menutup celah keamanan yang ada pada Website SMAN 1 Sumbawa (Alwi dkk, 2021).

Penelitinan dengan judul Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assesment permasalahannya Website sangat penting dalam konteks pendidikan seperti pengelolaan sistem akademik dan penerimaan mahasiswa baru di Universitas Muhammadiyah Purwokerto. Namun, keamanan informasi adalah hal yang sangat penting mengingat potensi kerugian jika informasi jatuh ke pihak yang tidak berwenang. Oleh karena itu, perlu adanya sistem informasi yang dapat mengatasi dan mencegah langkah-langkah buruk yang tidak diinginkan. Untuk mengatasi masalah ini, penelitian ini menggunakan metode Vulnerability Assesment dengan tujuan untuk mengidentifikasi dan menutup celah keamanan serta kerentanan pada Website pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto, sehingga meningkatkan keamanan informasi secara keseluruhan (Hafsari dkk, 2024).

2.1 Owasp ZAP

OWASP ZAP adalah alat pemindai kerentanan web yang umum digunakan untuk mendeteksi kerentanan dengan menemukan dan menyerang bidang input yang rentan. Alat ini membantu mengidentifikasi kerentanan seperti *SQL Injection* dan *Cross-Site Scripting (XSS)* dengan melakukan serangan otomatis pada titik-titik rentan dalam aplikasi web. Tesis dengan judul *Study of the techniques used by owasp zap for analysis of vulnerabilities in web applications* mengevaluasi teknik *owasp zap* dan pemindai kerentanan lainnya, menguji aplikasi web dengan kerentanan disengaja, membandingkan kinerja, dan

mengimplementasikan teknik yang lebih baik untuk meningkatkan kemampuan deteksi owasp zap (A. Jakobsson and I. Häggström, 2022).

2.2 Nikto

Nikto adalah alat keamanan *web* yang berguna untuk mendeteksi kerentanan dan masalah keamanan pada *server web*. Alat ini berjalan pada sistem operasi *Kali Linux*. Dengan Nikto, kamu dapat mengidentifikasi jenis *server web* yang digunakan, menguji keamanan SSL, dan mendeteksi keberadaan *firewall* aplikasi web (WAF). Nikto membantu menemukan kerentanan yang bisa dieksploitasi oleh penyerang, serta digunakan oleh peneliti keamanan dan administrator sistem untuk memastikan server web mereka aman dari ancaman yang umum (A. E. Evwiekpaefe and I. Habila, 2021).

2.3 Nmap

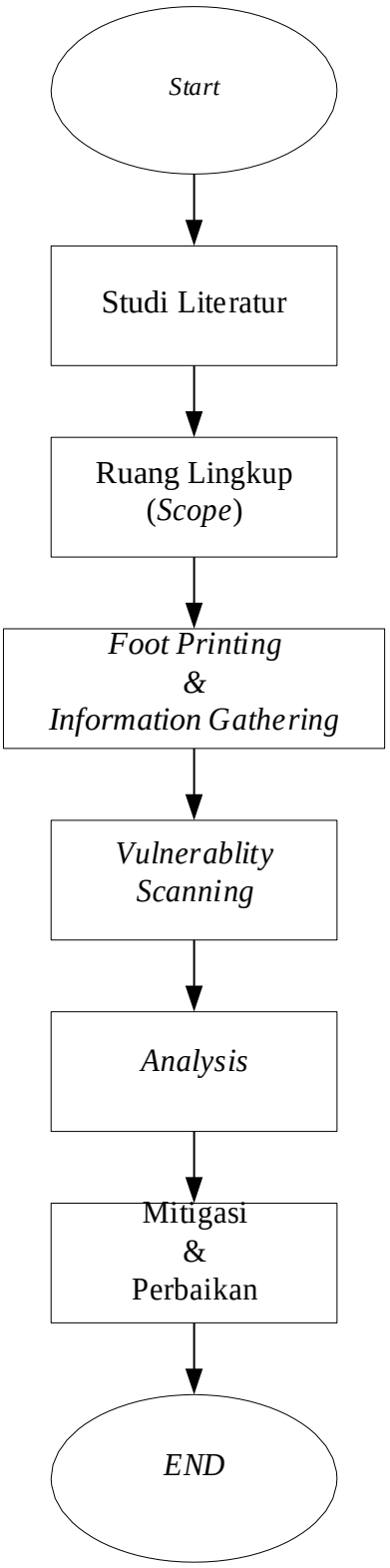
Nmap adalah sebuah alat atau software untuk melakukan pemindaian jaringan. Nmap, singkatan dari Network Mapper, adalah alat opensource yang digunakan untuk mengeksplorasi jaringan dan mendeteksi informasi tentang perangkat yang terhubung di dalamnya. Alat ini sangat berguna untuk mengidentifikasi perangkat aktif, membuka port, layanan yang berjalan, dan sistem operasi yang digunakan oleh perangkat-perangkat tersebut. Dengan Nmap, pengguna dapat dengan mudah melakukan audit keamanan jaringan dan mengidentifikasi potensi kerentanan (Orebaugh, A., Pinkard, B. 2021).

2.4 Kali Linux

Kali Linux adalah sebuah distribusi Linux yang dirancang khusus untuk penetration testing dan keamanan siber, dikembangkan dan didukung oleh Offensive Security. Sebagai penerus BackTrack Linux, Kali Linux ditujukan untuk profesional keamanan siber, penguji penetrasi, dan pengguna yang tertarik dengan isu-isu keamanan komputer. Distribusi ini menyediakan berbagai tool dan utilitas untuk analisis keamanan, pengujian penetrasi, forensik digital, dan aktivitas keamanan siber lainnya. Fitur utama Kali Linux meliputi sistem operasi live yang dapat dijalankan tanpa instalasi, mode forensik untuk analisis digital tanpa jejak, kernel Linux yang disesuaikan, serta kemampuan untuk dikustomisasi sepenuhnya. Kali Linux juga diakui sebagai sistem operasi terpercaya di industri keamanan siber dan dapat digunakan pada berbagai perangkat ARM. Kebijakan penggunaan Kali Linux meliputi penggunaan satu pengguna root secara default, layanan jaringan yang dinonaktifkan secara default, serta koleksi aplikasi yang dipilih khusus untuk kebutuhan keamanan dan pengujian. (R. Hertzog dkk, 2017).

3. METODE PENELITIAN

Penelitian ini untuk melakukan pengecekkan dan mitigasi terhadap Website SDN 50 Bengkalis dengan menggunakan Metode Vulnerability Assesment, Objek dari penelitian ini adalah Website, Bentuk kerangka kerja dari metode Vulnerability Assesment:



Gambar 1. Kerangka Kerja

1. Studi Literatur

   Tahap ini melibatkan pengumpulan dan pembelajaran informasi tentang topik atau subjek yang sedang diteliti.
2. Ruang Lingkup (Scope)
   Tahap ini menetapkan batasan dan fokus dari penelitian yang akan dilakukan.
3. Foot Printing & Information Gathering

Tahap ini melibatkan pengumpulan informasi dan data yang relevan dengan topik penelitian.

4. Vulnerability Scanning
   Pada tahap ini, dilakukan pemindaian atau scanning untuk mengidentifikasi celah keamanan (Vulnerability) pada Website yang akan diteliti.
5. Analysis
   Tahap ini melibatkan analisis mendalam terhadap hasil pemindaian untuk mengidentifikasi dan memahami kelemahan keamanan yang ditemukan.
6. Mitigasu dan Perbaikan
   Di tahapan ini peneliti melakukan mitigasi untuk mengurangi resiko ancaman keamanan website tersebut, mengcegah seerangan siber, dan melakukan perbaikan semisalnya ada kerentanan yang beresiko yang dapat merusak website tersebut.

4. HASIL PENELITIAN DAN PEMBAHASAN

Analisis kerentanan pada website SDN 50 Bengkalis menggunakan metode Vulnerability Assesment dengan tahapan sebagai berikut:

4.1 Studi Literatur

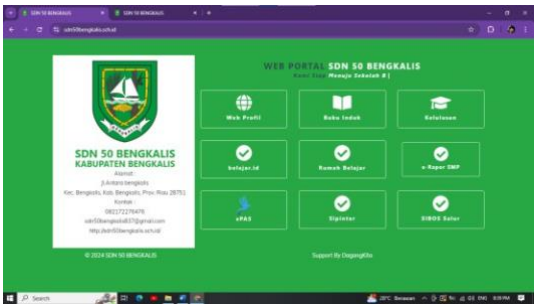
Tahap ini melibatkan pengumpulan dan pembelajaran informasi tentang topik atau subjek yang sedang diteliti. Informasi ini dapat diperoleh dari berbagai sumber referensi seperti buku, jurnal, artikel, situs web, laporan penelitian, dan lain-lain. Tujuan dari tahap ini adalah untuk mendapatkan pemahaman yang mendalam dan komprehensif tentang topik tersebut.

4.2 Ruang Lingkup (Scope)

Tahap ini menetapkan batasan dan fokus dari penelitian yang akan dilakukan. Pada tahap ini, kita menentukan apa saja yang akan menjadi objek penelitian, tujuan yang ingin dicapai, dan ruang lingkup penelitian. Selain itu, kita juga mengidentifikasi masalah yang akan diteliti, merumuskan pertanyaan penelitian, dan menentukan metode yang akan digunakan. Dengan demikian, penelitian menjadi terarah dan sesuai dengan tujuan yang diinginkan.

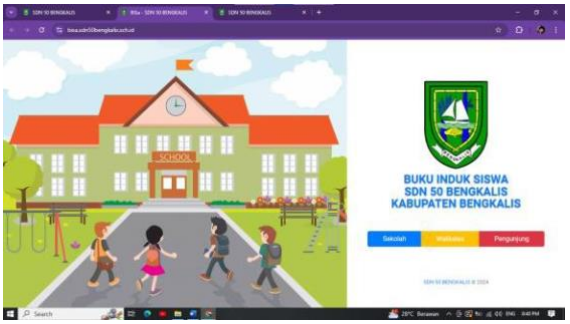
4.3 Foot Printing dan Information Gathering

Pada fase ini untuk memperoleh data informasi website sekolah SDN 50 Bengkalis, melalui websitenya sendiri ada apa saja fitur di website tersebut

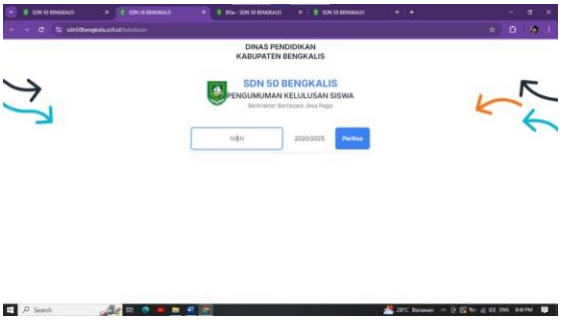


Gambar 2. Portal Website

Gambar 3. Beranda Website



Gambar 4. Buku Induk

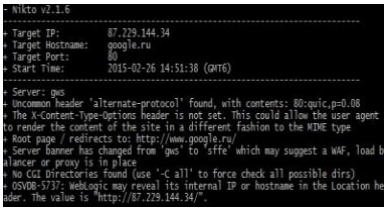


Gambar 5. Kelulusan

4.4 Vulnerability Scanning

Pada fase ini, dilakukan pemindaian atau scanning untuk mengidentifikasi celah keamanan (Vulnerability) pada Website SDN 50 Bengkalis, dengan tools OWASP ZAP, Nikto, Nmp dkk.

Gambar 6. OWASP ZAP



Gambar 7. Nikto

Gambar 8. Nmap

4.5 Analysis

Pada fase ini dilakukan analysis pada website SDN 50 Bengkalis, untuk mencari resiko kerntanan pada website sekolah tersebut

4.6 Mitigasi dan Perbaikan

Pada fase terakhir ini setelah menemukan celah keamanan di website sekolah, Langkah selanjutnya adalah mitigasi dan perbaikan terhadap keamanan website tersebut sebisa mungkin mengurangi resiko terhadap serangan siber.

5. KESIMPULAN DAN SARAN

Penelitian ini menganalisis kerentanan website SDN 50 Bengkalis menggunakan metode Vulnerability Assessment, mengidentifikasi berbagai kerentanan seperti SQL Injection dan Cross-Site Scripting (XSS). Hasil penelitian menunjukkan bahwa website sekolah rentan terhadap serangan siber. Penting untuk segera melakukan langkah mitigasi dan perbaikan. Demi meningkatkan keamanan data sensitif dan website secara keseluruhan, disarankan agar pihak sekolah meningkatkan pengetahuan teknologi informasi melalui pelatihan, menerapkan prosedur keamanan yang ketat, melakukan audit keamanan secara berkala, dan berkolaborasi dengan ahli keamanan siber.

6. DAFTAR PUSTAKA

Ayu Rifka Sitoresmi. (2023). Cyber Crime adalah Kejahatan Dunia Maya, Pahami Jenis-jenis dan Kerugiannya, https://www.liputan6.com/hot/read/5308185/cyber-crime-adalah-kejahatan-dunia-maya-pahami-jenis-jenis-dan-kerugiannya?page=5 pada tanggal 14 Jun 2023

A. Bastian, H. Sujadi, and L. Abror, 2020, “Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan Sql Injection,” INFOTECH J., vol. 6, no. 2, pp. 65–70,

D. N. Cunong, M. Saputra, and W. Puspitasari, 2020, “Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modan Dan Pelayanan Terpadu Satu Pintu Pemerintahan Xyzyz Menggunakan Standar Penetration Testing Executionstandard (Ptes),” e-Proceeding Eng., vol. 7, no. 1, pp. 2090–2095.

Akmal, A. Muhammad, N. Heryana, and A. Solehudin. 2022, "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment." Jurnal Pendidikan dan Konseling (JPDK) vol. 4, no.4. pp 6298-6308.

Alwi, E. Irawadi, and L. B. Ilmawan. 2021, "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment." INFORMAL: Informatics Journal, vol. 6, no.3, pp. 131-135.

Hafsari, S. Ameilia, and H. Harjono. 2024, "Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assessment." TIN: Terapan Informatika Nusantara, vol. 4, no. 11, pp. 698-708.

A. Jakobsson and I. Häggström, 2022, "Study of the techniques used by OWASP ZAP for analysis of vulnerabilities in web applications," Master's thesis, Linköping University.

A. E. Evwiekpaefe and I. Habila, 2021, "Implementing SQL Injection Vulnerability Assesment of an E-commerce Web Application using Vega and Nikto Tools," Afr. J. Comp. & ICT, vol. 14, no. 1, pp. 1–8.

Orebaugh, A., Pinkard, B. 2021, Nmap in the Enterprise: Your Guide to Network Scanning. Ukraina: Elsevier Science.

R. Hertzog, J. O'Gorman, dan M. Aharoni, 2017, Kali Linux Revealed: Mastering the Penetration Testing Distribution. Cornelius, USA, NC: Offsec Press.