Analisis Keamanan Website SMP Negeri 2 Bagan Sinembah Dengan Framework ISSAF (Studi Kasus : SMP Negeri 2 Bagan Sinembah)

Elpi Aprianti Br Saragih[1], Rezki Kurniati[2], Nurmi Hidayasari[3]
Politeknik Negeri Bengkalis
elpiaprianti@gmail.com[1], rezki@polbeng.ac.id[2], nurmihidayasari@polbeng.ac.id[3]

Abstract

Website security is a crucial aspect in the digital era, especially for educational institutions. This research aims to analyze the website security of SMP Negeri 2 Bagan Sinembah using the ISSAF (Information Systems Security Assessment Framework) framework. The method used is penetration testing to identify website vulnerabilities, such as SQL Injection attacks, Cross-Site Scripting (XSS), and others. After vulnerabilities are identified, fixes are made to improve website security. The main focus of this research is to ensure website protection, especially in the context of online new student enrollment. This research emphasizes the importance of regular security evaluation to maintain the availability of information on the website. The results of the research are expected to help schools prevent cyberattacks and keep websites safe from potential hacking.

Keywords : Website Security, ISSAF, Penetration Testing

1. PENDAHULUAN

Keamanan *website* sangat penting mengingat semakin meningkatnya volume data yang dipertukarkan di internet. Organisasi harus menjaga kerahasiaan, integritas, dan otentikasi data sesuai dengan standar keamanan (F. Fachri dkk, 2021). Kurangnya keamanan pada sistem website memungkinkan *hacker* untuk mengakses data pribadi serta data penting (Riadi dkk, 2020). Ancaman ini sering kali muncul karena kesalahan dalam desain sistem yang dieksploitasi untuk serangan seperti *defacing, phising*, dan *brute force* (Harahap & Baginda, 2021). Perubahan cepat seringkali membuat pengembang lalai dalam pengujian keamanan, yang bisa menjadi celah bagi penyerang (Zirwan & Afif, 2022). *Penetration testing* digunakan untuk mengidentifikasi kerentanan pada aplikasi dan jaringan melalui simulasi serangan (Utoro dkk, 2020).

Website sekolah dengan domain https://smpn2bagansinembah.sch.id sebagai lembaga pendidikan digunakan untuk menyampaikan informasi tentang sekolah termasuk layanan pendaftaran siswa baru secara *online*. Proses pendaftaran ini mengharuskan siswa memasukkan data pribadi, sehingga sangat penting untuk menjaga keamanan data tersebut. Namun, hingga saat ini, pihak sekolah belum pernah melakukan analisis keamanan atau pengujian pada *website* mereka, sehingga terdapat potensi adanya celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Selain itu, tantangan lainnya adalah bahwa serangan siber yang dapat terjadi tidak hanya akan mengancam keamanan, tetapi juga dapat merusak reputasi sekolah dan mengganggu kelangsungan operasionalnya. Serangan siber dapat mengakibatkan kerusakan pada sistem informasi sekolah, serta akses yang tidak sah ke dalam sistem. Oleh karena itu, keamanan sistem *website* ini menjadi prioritas yang harus segera diatasi, terutama karena *website* sekolah menyediakan layanan yang berkaitan langsung dengan data pribadi siswa baru.

Penelitian ini bertujuan untuk melakukan analisis keamanan dan *penetration testing* pada *website* SMP Negeri 2 Bagan Sinembah dengan menggunakan kerangka *kerja ISSAF (Information Systems Security Assessment Framework)*. Dengan analisis ini, diharapkan dapat

teridentifikasi celah keamanan yang ada, serta memberikan perbaikan untuk meningkatkan keamanan *website* tersebut. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam memastikan kelancaran operasional *website* sekolah.

2. TINJAUAN PUSTAKA

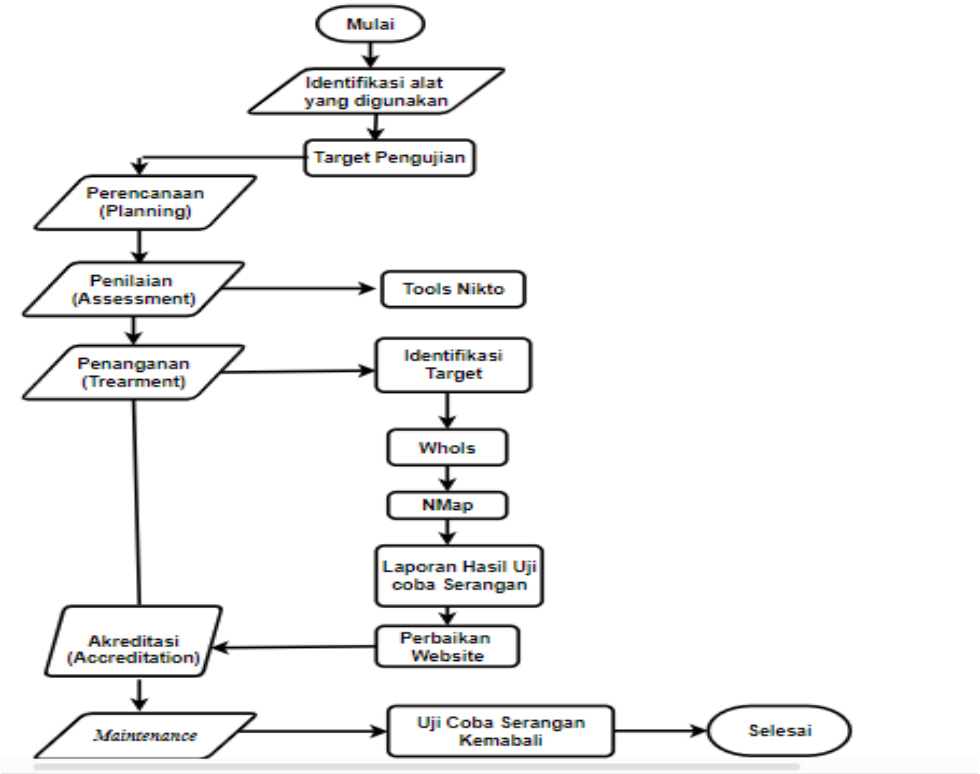
Beberapa penelitian yaitu dengan judul "Analisis Keamanan *Website* SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing (Pentest)",* dalam penelitian tersebut Sekolah Menengah Atas (SMA) Negeri 2 Sumbawa Besar menghadapi permasalahan keamanan *website* yang lemah sehingga rentan terhadap penyerangan oleh peretas. Penelitian ini menggunakan metode *penetration testing (Pentest)* yang meliputi tahapan *footprinting, scanning, fingerprinting, exploit, dan reporting*, serta menggunakan alat *Zed Attack Proxy (ZAP).* Hasil penelitian mengungkapkan 13 *sub-file vulnerability* dengan status *low* dan *medium*, rekomendasi perbaikan keamanan *website* disusun sebagai solusi untuk meningkatkan keamanan dan mencegah serangan *cyber criminal* di masa depan (Mulyanto dkk, 2022).

Berikutnya ada penelitian dengan judul *"*Analisis Keamanan *Open Website* Menggunakan Metode OWASP dan *ISSAF",* yang membahas permasalahan keamanan pada *website* Diskominfo Kabupaten Kerinci. Penelitian ini menggunakan metode OWASP dan *ISSAF* untuk mengidentifikasi kerentanan. Hasil penelitian menemukan beberapa celah keamanan seperti *Cross-Site Scripting* dan *SQL Injection*, yang kemudian diberikan rekomendasi perbaikan untuk meningkatkan keamanan *website*. Hasil akhir menunjukkan bahwa penerapan solusi berdasarkan metode tersebut berhasil menurunkan tingkat risiko dari "*Hign*" menjadi "*Low*" (Ashar & Rahmad, 2022).

Penelitian selanjutnya dengan judul "Analisis Celah Keamanan Pada *Website* Dengan Menggunakan Metode *Penetration Testing* Dan *Framework ISSAF* Pada *Website* SMK Al-Kautsar", dalam penelitian tersebut permasalahannya bahwa *website* SMK Al-Kautsar sebagai sistem informasi dapat memiliki celah keamanan seperti *SQL injection, clickjacking, brute force,* dan *XSS* sehingga penelitian ini menggunakan metode *penetration testing* dengan *Information Sistem Security Assessment Framework (ISSAF)* yang memiliki 3 *fase: planning and preparation, assessment, dan reporting,* dan hasil penelitian menunjukkan bahwa *website* SMK Al-Kautsar rentan terhadap serangan *Denial of Service (DdoS),* namun terhindar dari serangan *XSS* dan serangan melalui *port* terbuka (Andriyani dkk, 2023).

3. METODE PENELITIAN

Metode yang digunakan pada penelitian adalah analisis keamanan dengan menggunakan *Information Systems Security Assessment Framework (ISSAF)* dan *Penetration testing*. *Information Security Assessment Framework (ISSAF)* adalah kerangka kerja terstruktur yang digunakan untuk menilai keamanan sistem informasi. ISSAF mengelompokkan penilaian keamanan ke dalam berbagai domain dan menyediakan kriteria evaluasi untuk setiap domain. Tujuannya adalah memberikan panduan praktis dalam penilaian keamanan yang relevan dengan situasi nyata, serta membantu organisasi dalam memenuhi persyaratan keamanan informasi dan mengidentifikasi potensi kerentanan. (*Information Systems Security Assessment Framework* (ISSAF) draft 0.2, 2005). *Penetration testing* merupakan metode penilaian yang dilakukan dengan menguji kelemahan dari keamanan sistem, jaringan komputer, atau program aplikasi web (Delsi Samsumar dkk, 2017).



Gambar 1. Tahapan Penelitian

3.1 Identifikasi alat yang Digunakan

Dalam proses penelitian digunakannya alat sebagai alat bantu dalam proses penelitian. Alat yang digunakan adalah seperti *tools* yang bisa mendeteksi kerentanan.

3.2 Target Pengujian

Peneliti harus menentukan target atau objek yang akan dianalisis. Dalam konteks ini, target penelitian adalah pada *website* SMP Negeri 2 Bagan Sinembah.

3.3 Perencanaan *(Planning)*

Tahapan ini termasuk menetapkan tujuan penelitian, menyusun rencana kerja, dan mengumpulkan informasi yang diperlukan. Peneliti juga harus memastikan bahwa semua izin dan persetujuan yang diperlukan telah diperoleh, terutama jika penelitian melibatkan pengujian sistem yang bukan milik peneliti.

3.4 Penilaian *(Assessment)*

Pada tahap evaluasi, peneliti menganalisis informasi yang telah dikumpulkan untuk menentukan potensi kerentanan. Proses ini meliputi:
Pemindaian dengan Nikto: Melakukan pemindaian untuk menemukan kerentanan.

3.5 Penanganan *(Treatment)*

Tahapan ini melibatkan pelaksanaan pengujian berdasarkan analisis kerentanan yang telah dilakukan.
Penetration Testing: Melakukan Uji coba serangan dari hasil kerentanan setelah itu diberikan rekomendasi perbaikan dan membantu memperbaiki *website* setelah kerentanan teridentifikasi.

3.6 Akreditasi *(Accreditation)*

Setelah melakukan analisis dan *penetrasion testing*, peneliti menyusun laporan yang merangkum hasil uji coba serangan dan rekomendasi perbaikan. Laporan ini memberi bukti dokumentasi proses dalam uji coba serangan.

3.7 *Maintenance*

Tahapan ini bertujuan untuk menjaga keamanan *website* setelah membantu pihak sekolah untuk pada saat perbaikan *website* dilakukan. Penulis akan:

Melakukan Uji Coba Serangan Kembali: Mengulangi proses pengujian untuk memastikan bahwa perbaikan yang dilakukan efektif.

4. HASIL PENELITIAN DAN PEMBAHASAN

Hasil analisis penelitian dengan metode *Information Security Assessment Framework (ISSAF)* dengan tahapan sebagai berikut:

4.1 Identifikasi alat yang Digunakan

Table 1. Alat Yang Digunakan

Software	***Hardware***
Kali Linux	Laptop acer
Processor	11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz 3.00 GHz
Sistem Operasi *Windows* 11	Ram 8 GB
Tools Nikto, *Nmap*, dan lain-lain	

4.2 Penilaian *(Assessment)*



Gambar 2. Hasil *Scanning* Menggunakan Nikto

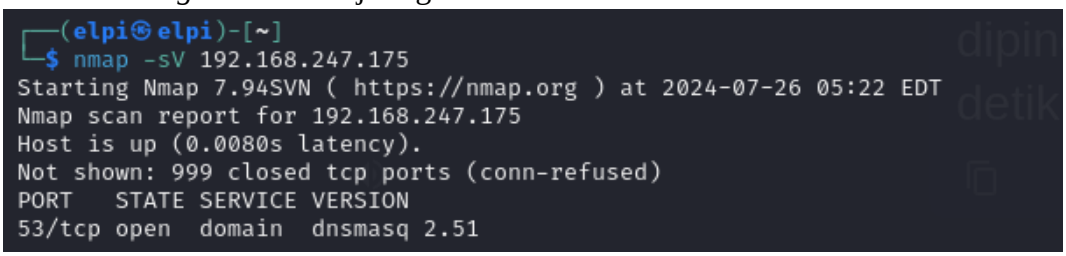
4.3 Penanganan *(Treatment)*

Hasil *Information Gathering*



Gambar 3. Hasil Whols

Hasil *scanning* Kerentanan jaringan



Gambar 4. Hasil *Port Scanning* dengan *Tools Nmap*

5. KESIMPULAN DAN SARAN

Berdasarkan analisis keamanan yang dilakukan pada *website* SMP Negeri 2 Bagan Sinembah, dapat disimpulkan bahwa keamanan *website* merupakan hal yang perlu dilakukan. Penelitian ini menunjukkan bahwa *website* tersebut belum pernah dilakukan analisis keamanan sebelumnya, sehingga berpotensi menghadapi berbagai ancaman *seperti SQL Injection* dan *Cross-Site Scripting* dan serangan lainnya. Melalui metode *penetration testing* dengan menggunakan *framework ISSAF*, identifikasi celah keamanan dapat dilakukan, dan langkah-langkah perbaikan untuk meningkatkan keamanan *website*. Oleh karena itu, disarankan agar sekolah melakukan audit keamanan secara berkala, meningkatkan kesadaran staf mengenai pentingnya keamanan siber, menerapkan kebijakan keamanan yang lebih ketat, menggunakan alat pemindai keamanan secara rutin, dan memperbarui infrastruktur TI secara berkala. Dengan menerapkan saran-saran ini, diharapkan keamanan *website* SMP Negeri 2 Bagan Sinembah dapat meningkat, sehingga informasi lainnya dapat terlindungi dengan lebih baik.

6. DAFTAR PUSTAKA

"Information Systems Security Assessment Framework (ISSAF) draft 0.2," 2005.

A. Zirwan, 2022, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, pp. 70–75, doi: 10.37034/jidt.v4i1.190.

B. Harahap, 2021, "Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta," Jurnal Informatika dan Teknologi Pendidikan, vol. 1, no. 2, pp. 80–86, doi: 10.25008/jitp.v1i2.15.

F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, 2021, "Analisis Keamanan Webserver Menggunakan Penetration Test," JURNAL INFORMATIKA, vol. 8, no. 2. [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji

I. Riadi, A. Yudhana, and P. Korspondensi, 2020, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," vol. 7, no. 4, doi: 10.25126/jtiik.202071928.

L. Delsi Samsumar and K. Gunawan, 2017, "Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram."

R. Ashar, 2022, "Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," Jurnal Informasi dan Teknologi, vol. 4, no. 4, doi: 10.37034/jsisfotek.v4i4.233.

S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, 2023, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework ISSAF Pada Website SMK Al-Kautsar."

S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, 2020, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," MULTINETICS, vol. 6, no. 2, pp. 169–178, doi: 10.32722/multinetics.v6i2.3432.

Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, 2022, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," Journal of Information System Research (JOSH), vol. 4, no. 1, pp. 202–209, doi: 10.47065/josh.v4i1.2335.