STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 4 No. 1, Februari 2025, 1 - 7
e-ISSN: 2828-5344 | DOI: 10.55123

Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma

[1)] Tamsir Ariyadi, [2)]Hidayatul Fadli, [3)]Taufik Akbar, [4)]Muhammad Bimo Prihandoko

[1,2,3,4)]Jurusan Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma Palembang Indonesia

Email:[1)] tamsirariyadi@binadarma.ac.id,[2)] hidayatulfadli1410@gmail.com,[3)] taufikakbar0125@gmail.com, [4)] mhmmdbimoo13@gmail.com

INFO ARTIKEL

Riwayat Artikel :
Diterima : 30 Desember 2024
Disetujui : 20 Januari 2025

Kata Kunci :

Teknologi informasi, Keamanan, Kerentanan.

ABSTRAK

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam cara proses belajar dan mengajar di perguruan tinggi, salah satunya melalui penerapan Sistem Informasi Akademik Terintegrasi (Siska) Meskipun sistem ini memberikan berbagai manfaat, ia juga menghadirkan potensi ancaman terhadap keamanan yang dapat membahayakan data dan kelancaran proses pembelajaran. Penelitian ini bertujuan untuk menganalisis kerentanannya pada Website https://siska.binadarma.ac.id/ Universitas Bina Darma dengan menggunakan kerangka kerja OWASP (Open Web Application Security Project). Metode ini membantu mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Penelitian ini mengkaji potensi kerentanannya berdasarkan sepuluh kategori utama yang diusulkan dalam OWASP Top 10. Hasil dari analisis ini diharapkan dapat memberikan rekomendasi yang berguna untuk meningkatkan tingkat keamanan sistem Siska(Sistem Informasi Akademik Terintegrasi) di Universitas Bina Darma, sehingga melindungi data pengguna dan memastikan proses pembelajaran tetap berlangsung dengan aman.

ARTICLE INFO

Article History :
Received : Dec 30, 2024
Accepted : Jan 20, 2025

***Keywords**:*
Information technology, Security, Vulnerability.

ABSTRACT

The advancement of information technology has brought significant changes to the way teaching and learning processes are carried out in higher education, one of which is through the implementation of the Siska (Integrated Academic Information System). While this system provides many benefits, it also introduces potential security risks that could threaten data integrity and disrupt the learning process. This study aims to analyze the vulnerabilities on the website https://siska.binadarma.ac.id/ of Universitas Bina Darma using the OWASP (Open Web Application Security Project) framework. This method assists in identifying potential security loopholes that could be exploited by unauthorized parties. The research examines these vulnerabilities based on the ten key categories proposed in the OWASP Top 10. The results of this analysis are expected to offer valuable recommendations to enhance the security of the Siska system at Universitas Bina Darma, ultimately protecting user

data and ensuring that the learning process continues safely and smoothly.

.

1. PENDAHULUAN

Sistem Informasi Akademik Terintegrasi (Siska) di Universitas Bina Darma merupakan platform digital yang dirancang untuk memper mudah dan mengoptimalkan proses administrasi akademik secara menyeluruh. Siska menghubun gkan berbagai fungsi penting di lingkungan kampus, mulai dari pendaftaran mahasiswa, pengelolaan data akademik, penjadwalan kuliah, hingga penyimpanan nilai dan transkrip akademik. Dengan adanya sistem ini, mahasiswa dan dosen dapat mengakses informasi akademik dengan lebih cepat dan mudah, sekaligus mempermudah pihak universitas dalam mengelola administrasi. Meskipun sistem ini menawarkan banyak kemudahan di tengah kemajuan teknologi, penggunaannya juga menghadirkan tantangan, terutama terkait dengan keamanan data. Mengingat sistem ini mengelola informasi yang sangat sensitif, seperti data pribadi mahasiswa, nilai akademik, dan informasi terkait kegiatan perkuliahan, isu keamanan informasi menjadi sangat penting. Karena itu, Universitas Bina Darma perlu terus mengevaluasi dan meningkatkan sistem Siska agar tetap aman, mampu melindungi data pengguna, dan mengurangi potensi ancaman yang bisa muncul. Dengan mengidentifikasi kerentanannya, diharapkan Siska dapat terus berfungsi dengan baik, mendukung kelancaran proses pembelajaran, serta menjaga privasi dan keamanan data mahasiswa dan staf akademik. (Ariyadi et al.).

Keamanan sistem informasi merupakan hal yang sangat penting dalam pengelolaan data akademik di perguruan tinggi, termasuk di Universitas Bina Darma melalui penerapan Sistem Informasi Akademik Terintegrasi (Siska). Siska mengelola data penting seperti informasi pribadi mahasiswa, nilai, jadwal kuliah, dan data akademik lainnya yang sangat sensitif.(Nugroho and Rochmadi) Oleh karena itu, menjaga keamanan sistem ini sangatlah krusial agar data tetap aman dari ancaman atau serangan yang bisa merusak integritas dan keberlanjutan sistem. Keamanan Siska bukan hanya soal melindungi data mahasiswa, tetapi juga melindungi informasi dosen, staf akademik, dan berbagai proses administrasi lainnya. Serangan terhadap sistem ini bisa mengakibatkan pencurian, kerusakan, atau manipulasi data yang sangat vital bagi kelancaran kegiatan perkuliahan dan operasional universitas. Karena itu, penting untuk memastikan bahwa sistem Siska dilengkapi dengan langkah-langkah keamanan yang tepat untuk menjaga perlindungan menyeluruh. Ancaman terhadap sistem Siska dapat berupa peretasan (hacking), eksploitasi celah keamanan (vulnerabilities), serangan DDoS (Distributed Denial of Service), hingga kebocoran data yang disebabkan oleh konfigurasi yang tidak aman atau akses yang tidak sah. Selain itu, perlindungan terhadap data pribadi mahasiswa dan dosen juga harus menjadi prioritas, mengingat adanya regulasi terkait perlindungan data pribadi yang harus diikuti oleh perguruan tinggi.

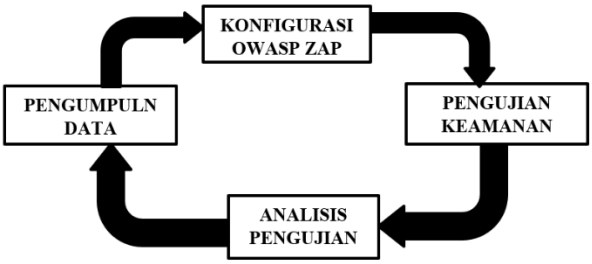
Untuk itu, Universitas Bina Darma perlu melakukan pengecekan dan evaluasi secara berkala terhadap sistem Siska, mengidentifikasi potensi kerentanannya, serta mengambil langkah-langkah untuk mengurangi risiko, seperti memperbarui perangkat lunak secara rutin, mengenkripsi data, menggunakan otentikasi multi-faktor, dan memberikan pelatihan keamanan kepada pengguna sistem. Dengan menjaga keamanan sistem Siska, Universitas Bina Darma dapat melindungi data penggunanya dan menciptakan lingkungan pembelajaran yang aman serta terpercaya. Ancaman terhadap keamanan Sistem Informasi Akademik Terintegrasi (Siska) ini menjadi semakin nyata seiring dengan semakin kompleksnya teknologi yang digunakan dan meningkatnya jumlah serangan siber yang menargetkan aplikasi web, termasuk platform Sistem Informasi Akademik Terintegrasi (Siska). Berdasarkan laporan-laporan keamanan yang ada, serangan terhadap aplikasi web, seperti **SQL Injection**, **Cross-Site Scripting (XSS)**, **Cross-Site Request Forgery (CSRF)**, dan **Remote Code Execution** (RCE), merupakan masalah umum yang dapat merusak integritas dan kerahasiaan data dalam Web Sistem Informasi Akademik Terintegrasi

(Siska).(Fredj et al.) Untuk itu, diperlukan pendekatan yang sistematis dan terstruktur dalam menganalisis kerentanannya keamanan pada Sistem Informasi Akademik Terintegrasi (Siska). Salah satu metodologi yang telah terbukti efektif dalam melakukan evaluasi keamanan aplikasi web adalah dengan menggunakan **OWASP (Open Web Application Security Project)**. OWASP adalah sebuah proyek internasional yang berfokus pada peningkatan keamanan aplikasi web dengan memberikan panduan, alat, dan rekomendasi untuk mengidentifikasi dan mengurangi risiko keamanan. Salah satu kontribusi terbesar dari OWASP adalah dokumen yang dikenal dengan **OWASP Top 10**, yang merangkum sepuluh kerentanannya paling kritis yang sering ditemukan pada aplikasi web.(Lala et al.) Kerangka kerja ini mencakup berbagai celah keamanan yang berpotensi mengekspos aplikasi terhadap ancaman seperti injeksi kode, pengelolaan sesi yang buruk, dan masalah autentikasi. (Kuncoro and Rahma).

Penggunaan OWASP dalam analisis kerentanannya pada Sistem Informasi Akademik Terintegrasi (Siska) Universitas Bina Darma dapat membantu pihak pengelola sistem untuk mengidentifikasi dan mengatasi celah-celah keamanan yang mungkin ada, serta memberikan rekomendasi yang tepat untuk meningkatkan keamanan sistem secara keseluruhan. Analisis ini juga memberikan gambaran yang lebih jelas tentang potensi ancaman yang dapat dihadapi oleh sistem, serta langkah-langkah mitigasi yang perlu diambil untuk mencegah kerusakan atau kebocoran data yang dapat merugikan mahasiswa, pengajar, maupun institusi. (Kusuma).

2. METODE

Penelitian ini menggunakan metode kualitatif deskriptif yang bertujuan untuk menganalisis kerentanannya keamanan pada sistem E-Learning Universitas Bina Darma dengan menggunakan kerangka kerja OWASP. Penelitian ini dilakukan dengan pendekatan studi kasus yang akan mengeksplorasi celah-celah keamanan Sistem Informasi Akademik Terintegrasi (Siska) secara mendalam dan memberikan rekomendasi untuk perbaikan. Adapun tahapan-tahapan yang dilakukan dalam penelitian ini meliputi Pengumpulan Data,Konfigurasi OWASP ZAP,Pengujian Keamanan,Analisis Pengujian.



Gambar 1. Metode Penelitian

2.1.Pengumpulan Data

Pada tahap pertama, dilakukan pengumpulan informasi dasar terkait dengan website Sistem Informasi Akademik Terintegrasi (Siska) Universitas Bina Darma. Proses ini mencakup pengumpulan data mengenai struktur dan desain website, teknologi yang digunakan dalam pengembangannya, serta jenis data yang dikelola dan diproses oleh sistem tersebut. Informasi-informasi yang diperoleh akan menjadi dasar yang penting dalam melakukan analisis terhadap aspek-aspek keamanan dari sistem, guna memastikan perlindungan yang optimal terhadap data dan informasi yang ada. (Febriani et al.)

2.2.Konfigurasi OWASP ZAP

Pada tahap ini, dilakukan instalasi dan konfigurasi OWASP ZAP (Zed Attack Proxy) sesuai dengan kebutuhan untuk pengujian keamanan yang lebih mendalam. Proses konfigurasi melibatkan beberapa langkah, di antaranya pengaturan proxy agar alat ini dapat berfungsi sebagai perantara antara pengguna dan website yang diuji. Selain itu, dilakukan pula spidering, yaitu proses pemetaan secara otomatis terhadap struktur website untuk mengidentifikasi berbagai elemen dan halaman yang ada di dalamnya.(Idris et al.) Selain itu, parameter uji juga disesuaikan dengan cermat agar analisis yang dilakukan dapat berjalan dengan efektif dan efisien, serta memastikan bahwa pengujian sesuai dengan tujuan yang telah ditetapkan.

2.3.Penngujian Keamanan

Pada tahap pengujian keamanan, dilakukan serangkaian uji yang memanfaatkan berbagai fitur yang disediakan oleh OWASP ZAP. Salah satu fitur yang digunakan adalah *Passive Scanning*, yang berfungsi untuk mendeteksi potensi kerentanannya tanpa mempengaruhi atau mengubah data yang ada pada sistem. Metode ini memungkinkan identifikasi masalah keamanan secara pasif, tanpa menimbulkan gangguan pada operasional sistem. Selain itu, pengujian juga dilakukan dengan menggunakan *Active Scanning*, yang memungkinkan sistem untuk secara aktif mengeksplorasi dan menguji lebih dalam terhadap potensi kerentanannya. Dengan pendekatan ini, pengujian dapat mengungkapkan masalah yang lebih kompleks, seperti injeksi SQL, kerentanannya terhadap serangan XSS, serta kelemahan dalam mekanisme autentikasi yang ada pada sistem, sehingga memberikan gambaran yang lebih menyeluruh mengenai tingkat keamanan dari website tersebut. (Dewangkara et al.).

2.4.Analisis hasil Pengujian

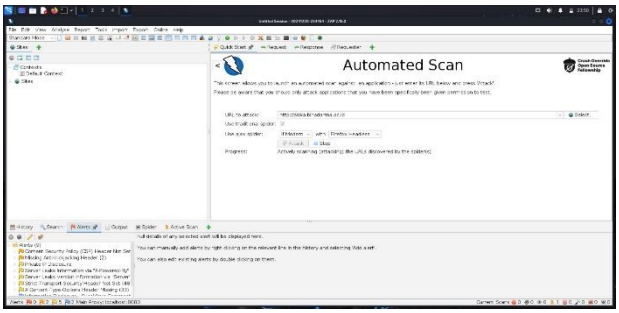
Setelah proses pengujian dilakukan menggun akan OWASP ZAP, langkah selanjutnya adalah menganalisis hasil pengujian untuk mengidentifikasi kelemahan- kelemahan yang mungkin ada pada situs web yang diuji. Dalam tahap analisis ini, setiap kerentanannya yang ditemukan akan diteliti secara mendalam, dengan menguraikan secara rinci mengenai tingkat keparahan dari masing-masing masalah keamanan yang terdeteksi.(Tamsir et al.) Selain itu, akan dilakukan penilaian terhada p potensi dampak yang dapat ditimbulkan jika k erentanannya dieksploitasi oleh pihak yang tidak bertanggung jawab. Proses ini juga mencakup pemahaman mengenai mekanisme eksploitasi yang dapat digunakan untuk memanfaatkan kerentanannya, sehingga langkah-langkah perbaikan yang lebih tepat dan efektif dapat diambil untuk meningkatkan keamanan situs web tersebut. (Nisa et al.)

3. HASIL DAN PEMBAHASAN

3.1. Analisa Web menggunakan OWASP ZAP

Bagian Website Sistem Informasi Akademik Terintegrasi (Siska) Universitas Bina Darma memiliki peran yang sangat penting dalam mendukung berbagai aktivitas akademik di kampus. Oleh karena itu, menjaga keamanan platform ini menjadi hal yang sangat krusial. Untuk memastikan keamanannya, digunakan alat OWASP ZAP yang membantu mendeteksi potensi kerentanannya, sehingga dapat melindu ngi system dari ancaman yang berisiko merusak integritas dan kerahasiaan data yang ada.(Wahidin et al.)

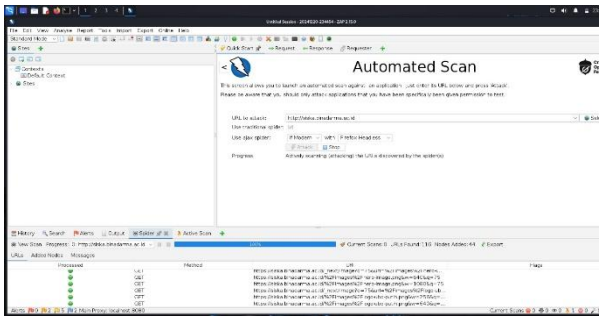
- Mulailah dengan menjelajahi Web Sistem Informasi Akademik Terintegrasi (Siska) menggunakan browser Anda, sambil memastikan bahwa lalu lintas web Anda diarahkan melalui proxy ZAP. Ini akan memungkinkan ZAP untuk menangkap setiap permintaan HTTP/HTTPS yang terjadi, dan secara otomatis mendeteksi jika ada potensi kerentanannya.(Adinugroho et al.)



Gambar 2. Menganalisa Web Menggunakan OWASP ZAP

Disini kami Web yang akan di Analisis disini kami memasukan Web https://siska.binadarma.ac.id/

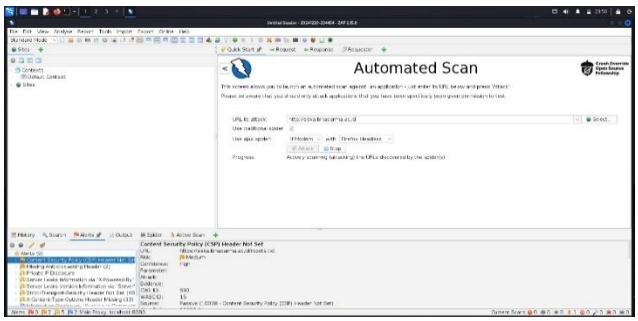
- Lalu Scan dengan cara klik attack untuk mengetahui kerentanan Web tersebut.



Gambar 3. Proses Pemindai Website

- Kemudian cek Alerts untuk mengetahui Keamanan system. Disini terlihat bermacam warna bendera yang menandakan keamanan system dari Sistem Informasi Akademik Terintegrasi (Siska).

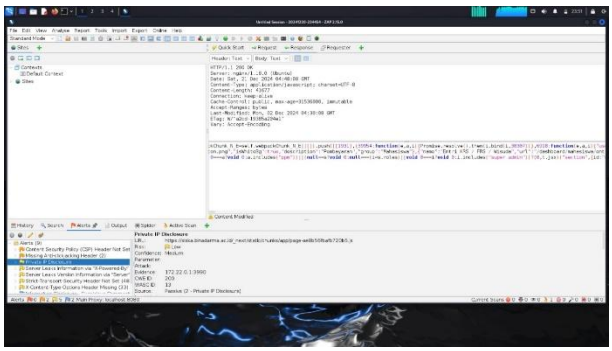
  Merah :
  critical yaitu menunjukan kerentanan yang sangat serius yang berpotensi mengekspos data sensitif.
  Oranye :
  Menunjukkan masalah keamanan yang cukup serius yang dapat menyebabkan akses tidak sah ataupun kebocoran data.
  Kuning :
  Menunjukkan kerentanan yang kurang berbahaya tetapi masih memerlukan perbaikan.
  Hijau :
  Yang menunjukkan bahwa jaringan tersebut mempunyai Tingkat keamanan yang bagus.



Gambar 4. Tingkat Kerentanan Medium

Kerentanan **Medium** dalam OWASP ZAP merujuk pada masalah keamanan yang memiliki tingkat risiko sedang terhadap aplikasi atau sistem yang diuji. Meskipun tidak sebesar kerentanannya yang dikategorikan sebagai "High", jika tidak segera ditangani, masalah ini dapat menjadi celah yang dimanfaatkan oleh penyerang. Kerentanan Medium sering kali tidak langsung mengancam sistem, namun bisa menjadi langkah awal bagi penyerang untuk melanjutkan serangan, terutama jika digabungkan dengan kerentanannya lain.(Gordon)

Dengan kata lain, meskipun dampaknya tidak sebesar kerentanannya yang lebih parah, kerentanannya Medium tetap perlu diperbaiki agar mencegah potensi risiko yang lebih besar di kemudian hari.(Wijayanto and Firdonsyah)



Gambar 5 .Tingkat Kerentanan Low

Dalam konteks OWASP ZAP (Zed Attack Proxy), "Tingkat Kerentanan Low" merujuk pada masalah keamanan yang ditemukan dalam aplikasi atau sistem yang diuji, dengan tingkat keparahan yang rendah. OWASP ZAP adalah alat sumber terbuka yang digunakan untuk mendeteksi dan menguji kerentanannya di aplikasi web. Kerentanan yang ditemukan biasanya dibagi menjadi beberapa kategori, seperti "High", "Medium", dan "Low", berdasarkan seberapa besar potensi risikonya jika dieksploitasi oleh pihak yang tidak bertanggung jawab. Kerentanan dengan tingkat "Low" umumnya memiliki dampak yang lebih kecil, meskipun tetap perlu diperbaiki untuk menjaga keamanan aplikasi secara keseluruhan.(Nurjannah and Abdul Muni)

3.2.UCAPAN TERIMA KASIH

Jika Peneliti ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dalam proses penyelesaian penelitian ini. Secara khusus, peneliti menyampaikan penghargaan yang mendalam kepada dosen kami, Tamsir Ariyadi, M.Kom, selaku pengampu Mata Kuliah

Keamanan Sistem Informasi, yang telah memberikan bimbingan, dukungan, dan bantuan yang sangat berharga sepanjang berlangsungnya penelitian ini, yang berjudul "Implementasi OWASP untuk Analisis Kerentanannya Keamanan pada Sistem Informasi Akademik Terintegrasi (Siska) Universitas Bina Darma".

4. PENUTUP

4.1. Kesimpulan

Proses analisis keamanan pada Sistem Informasi Akademik Terintegrasi (Siska) Universitas Bina Darma menggunakan OWASP ZAP berhasil mengungkap berbagai potensi kerentanannya yang dapat mengancam keamanan data dan kelancaran operasional sistem. Beberapa masalah utama yang ditemukan antara lain kerentanannya terhadap SQL Injection, Cross-Site Scripting (XSS), serta kekurangan dalam penerapan header keamanan. Namun, di sisi lain, terdapat juga beberapa aspek yang sudah menerapkan langkah-langkah keamanan yang baik, seperti validasi input pada formulir tertentu dan penggunaan autentikasi dua faktor.

OWASP ZAP terbukti menjadi alat yang sangat berguna dalam mendeteksi kerentanannya dan memberikan rekomendasi perbaikan sesuai dengan standar keamanan OWASP Top 10. Dengan mengikuti rekomendasi yang diberikan, keamanan Sistem Informasi Akademik Terintegrasi (Siska) dapat ditingkatkan, sehingga data pengguna lebih terlindungi dan sistem dapat beroperasi dengan lebih aman dan stabil.

DAFTAR PUSTAKA

Adinugroho, N. Bagas, et al. “Analisis Keamanan E-Learning Menggunakan Open Web Application Security Project (Owasp) (Studi Kasus Moca Unimma).” *Jurnal Informatika*, vol. 22, no. 2, 2022, pp. 132–38, https://doi.org/10.30873/ji.v22i2.3327.

Ariyadi, Tamsir, et al. “Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP.” *Techno.COM*, vol. 22, no. 2, 2023, pp. 418–29.

Dewangkara, Bagus Indra, et al. “Penerapan Analisis Kerentanan XSS Dan Rate Limiting Pada Situs Web MTsN 3 Negara Menggunakan OWASP ZAP.” *Jurnal Informatika Upgris*, vol. 8, no. 1, 2022, pp. 92–97, https://doi.org/10.26877/jiu.v8i1.10266.

Febriani, Sabrina Asiah, et al. “Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Owasp-Zap Di Universitas Islam Indragiri.” *Jurnal Sistem Informasi (TEKNOFILE)*, vol. 2, no. 6, 2024, pp. 409–20.

Fredj, Ouissem Ben, et al. “An OWASP Top Ten Driven Survey on Web Application Protection Methods.” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12528 LNCS, 2021, pp. 235–52, https://doi.org/10.1007/978-3-030-68887-5_14.

Gordon. “ﻯBAB 2 Tinjauan Pustaka.” *Pontificia Universidad Catolica Del Peru*, vol. 8, no. 33, 2019, p. 44.

Idris, Muhammad, et al. “Web Application Security Education Platform Based on OWASP API Security Project.” *EMITTER International Journal of Engineering Technology*, vol. 10, no. 2, 2022, pp. 246–61, https://doi.org/10.24003/emitter.v10i2.705.

Kuncoro, Aditya Wibisono, and Fayruz Rahma. “Analisis Metode Open Web Application Security Project (OWASP) Pada Pengujian Keamanan Website: Literature Review.” *Automata*, vol. 3, no. 1, 2021, pp. 1–5, https://www.sciencedirect.com.

Kusuma, Gregorius. “Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik.” *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, vol. 16, no. 2, 2022, pp. 178–86, https://doi.org/10.47111/jti.v16i2.3995.

Lala, Shubham Kumar, et al. “Secure Web Development Using OWASP Guidelines.” *Proceedings - 5th International Conference on Intelligent Computing and Control*

Systems, ICICCS 2021, no. Iciccs, 2021, pp. 323–32, https://doi.org/10.1109/ICICCS51141.2021.9432179.

Nisa, Khairrun, et al. "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)." *Bulletin of Information Technology (BIT)*, vol. 3, no. 4, 2022, pp. 308–216, https://doi.org/10.47065/bit.v3i4.389.

Nugroho, Saerozi Alfan, and Tri Rochmadi. *Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) Dan Information Systems Security Assessment Framework (ISSAF) Security Analysis Of Magelang Pusaka Information System Using Open Web Application Security Project (OWASP) And Information Systems Security Assessment Framework (ISSAF)*. no. 1, 2024, pp. 56–61.

Nurjannah, and Abdul Muni. "Analisis Keamanan Website Sekolah Sman 1 Tempuling Dengan Menggunakan Open Web Application Security Project (Owasp)." *Jurnal Perangkat Lunak*, vol. 6, no. 2, 2024, pp. 351–61, https://doi.org/10.32520/jupel.v6i2.3442.

Tamsir, Tamsir Ariyadi, et al. "Analisis Paket Icmp Website Universitas Binadarma Menggunakan Wireshark." *STORAGE: Jurnal Ilmiah Teknik Dan Ilmu Komputer*, vol. 2, no. 2, 2023, pp. 55–60, https://doi.org/10.55123/storage.v2i2.1956.

Wahidin, M., et al. "Analisis Kerentanan Situs Web KopKar Syariah PT BSIN Menggunakan OWASP Zed Attack Proxy." *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, vol. 18, no. 4, 2024, pp. 25–31, https://doi.org/10.35969/interkom.v18i4.321.

Wijayanto, Danur, and Arizona Firdonsyah. "Analisis Tingkat Resiko Pada Website Xyz Menggunakan Metode Owasp." *Digital Transformation Technology*, vol. 4, no. 1, 2024, pp. 644–51, https://doi.org/10.47709/digitech.v4i1.448

5.