EVALUASI KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP: PENILAIAN TERHADAP SERANGAN INJEKSI SQL DAN CROSS-SITE SCRIPTING (XSS)

Dede Ending Narhudin [1], Bambang Irawan [2], Agus Bahtiar [3]
[1,2] Teknik Informatika, STMIK IKMI Cirebon
[3] Sistem Informasi, STMIK IKMI Cirebon
Jalan Perjuangan No.10B, Karyamulya, Kota Cirebon, Jawa Barat, Indonesia
ddending@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk melakukan evaluasi keamanan terhadap aplikasi web milik PT Rachma Perkasa Utama dengan menggunakan metodologi Open Web Application Security Project (OWASP), dengan fokus khusus pada serangan Injeksi SQL dan Cross-Site Scripting (XSS). Proses penelitian melibatkan serangkaian langkah evaluasi keamanan sesuai pedoman OWASP, yang mencakup identifikasi aplikasi web, deteksi potensi kerentanan, analisis mendalam, penilaian risiko, dan dokumentasi. Hasil penelitian menunjukkan bahwa terdapat beberapa kerentanan keamanan dalam aplikasi web PT Rachma Perkasa Utama. Meskipun tidak ada kerentanan yang dapat diklasifikasikan sebagai risiko tinggi, 1 (satu) temuan menunjukkan adanya risiko sedang terkait ketidakpatuhan terhadap kebijakan keamanan. Selain itu, 4 (empat) temuan dengan risiko rendah mengungkapkan ketidakpatuhan terhadap praktik keamanan tertentu, sedangkan 8 (delapan) temuan dengan risiko informasional melibatkan informasi yang tidak langsung mengancam keamanan. Rekomendasi perbaikan diajukan untuk mengatasi temuan-temuan tersebut, antara lain penerapan validasi input yang lebih ketat, pembaruan rutin, dan peningkatan manajemen sesi. Penelitian ini memberikan wawasan mendalam tentang keamanan aplikasi web PT Rachma Perkasa Utama, sambil memberikan panduan praktis untuk memperkuat tingkat keamanan secara menyeluruh. Implikasi praktis dari penelitian ini mencakup pemahaman yang lebih jelas tentang risiko keamanan dan tindakan yang dapat diambil untuk mengurangi potensi ancaman..

Kata kunci : Keamanan Aplikasi Web, Injeksi SQL, Cross-Site Scripting, Evaluasi Keamanan.

1. PENDAHULUAN

Bidang Informatika mengalami perkembangan yang signifikan seiring dengan kemunculan revolusi digital yang telah mengubah paradigma interaksi, pola kerja, dan gaya hidup masyarakat. Teknologi informasi meresap ke berbagai sektor, melibatkan transformasi dalam aspek bisnis, pendidikan, kesehatan, hiburan, dan komunikasi. Fenomena perubahan ini berdampak besar terhadap cara kerja, pembelajaran, dan interaksi dengan lingkungan sekitar dalam konteks penelitian ini. [1]. Namun, perkembangan ini juga membawa tantangan besar, terutama dalam keamanan aplikasi web yang perlu ditangani [2] .

Dalam era digital, aplikasi web berperan penting namun rentan terhadap serangan siber seperti Injeksi SQL dan Cross-Site Scripting (XSS) [3]. Serangan-serangan ini bisa merusak keamanan data dan privasi pengguna. Injeksi SQL melibatkan penyisipan pernyataan SQL berbahaya pada input aplikasi, sementara XSS menyisipkan skrip berbahaya pada halaman web [4]. Kedua serangan ini menjadi fokus utama penyerang dalam mencari celah pada aplikasi web [5].

Penelitian sebelumnya membahas serangan seperti Injeksi SQL dan Cross-Site Scripting (XSS) serta cara mengatasinya pada aplikasi web. Namun, diperlukan penelitian lebih lanjut, terutama untuk memahami karakteristik unik aplikasi web PT Rachma Perkasa Utama dan memberikan solusi spesifik untuk mengatasi kerentanan keamanan dalam konteks tersebut [6].

Penelitian ini bertujuan mengevaluasi keamanan aplikasi web PT Rachma Perkasa Utama dengan metode OWASP [7], fokus pada Injeksi SQL dan Cross-Site Scripting (XSS). Tujuannya adalah mengidentifikasi kerentanan, menilai tingkat keamanan, serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan aplikasi web perusahaan [8].

Penelitian ini penting dalam mengisi kekosongan pengetahuan tentang aplikasi web PT Rachma Perkasa Utama, memberikan panduan penting bagi perusahaan dalam melindungi data dan privasi pengguna [9]. Hasilnya juga dapat memberi manfaat pada organisasi serupa untuk memahami dan meningkatkan keamanan aplikasi web mereka [10]. Penelitian ini akan menggunakan metodologi berdasarkan pedoman OWASP untuk mengevaluasi keamanan aplikasi web, melalui langkah-langkah identifikasi, penemuan kerentanan, analisis mendalam, penilaian, dan dokumentasi hasil dengan melibatkan pengujian aplikasi, pemindaian keamanan, dan analisis kode sumber [11].

Penelitian ini diharapkan memberikan wawasan lebih mendalam mengenai keamanan aplikasi web di PT Rachma Perkasa Utama dan panduan konkret untuk peningkatannya. Implikasi hasilnya termasuk

rekomendasi perbaikan yang melindungi aplikasi dari serangan Injeksi SQL dan XSS [12]. Hasilnya juga dapat memberikan pemahaman praktik terbaik dalam mengamankan aplikasi web bagi organisasi serupa.

2. TINJAUAN PUSTAKA

Tinjauan pustaka dalam penelitian keamanan aplikasi web di PT Rachma Perkasa Utama melibatkan sejumlah aspek penting yang mendukung pemahaman mendalam tentang konteks keamanan aplikasi web. [13]Beberapa fokus utama dalam tinjauan pustaka ini termasuk.

2.1. Metode Evaluasi Keamanan Aplikasi Web (OWASP)

Metode evaluasi keamanan aplikasi web yang didefinisikan oleh Open Web Application Security Project (OWASP) membentuk landasan krusial dalam penelitian ini. Melalui tinjauan mendalam tentang metodologi ini, termasuk tahapan identifikasi kerentanan, penilaian risiko, dan strategi perbaikan, penelitian ini dapat membangun dasar yang kokoh untuk menyelidiki dan meningkatkan keamanan aplikasi web. Tinjauan yang cermat terhadap setiap langkah metodologi ini memberikan wawasan mendalam tentang bagaimana serangan mungkin terjadi, bagaimana risiko dinilai, dan cara-cara optimal untuk memperbaiki kerentanan yang teridentifikasi. Dengan memahami metode ini secara holistik, penelitian dapat menghadirkan rekomendasi yang lebih kuat dan solusi yang tepat guna dalam melindungi aplikasi web dari ancaman keamanan.[14] [11].

2.2. Serangan Injeksi SQL dan Cross-Site Scripting (XSS)

Studi literatur mengenai serangan Injeksi SQL dan Cross-Site Scripting (XSS) memberikan wawasan yang vital tentang serangan paling umum pada aplikasi web. Penelusuran mendalam tentang mekanisme serangan, titik kerentanan yang dieksploitasi, dan strategi mitigasi yang efektif menjadi kunci utama dalam melindungi aplikasi dari ancaman berbahaya ini. Memahami secara terperinci cara serangan-serangan ini terjadi membantu mengidentifikasi lapisan kelemahan dalam aplikasi, sementara pemahaman tentang teknik mitigasi yang efektif menjadi landasan kuat dalam merancang pertahanan yang solid terhadap serangan-serangan ini. Dengan mendasarkan perbaikan keamanan pada wawasan dari studi literatur ini, aplikasi web menjadi lebih tahan terhadap potensi ancaman yang serius. [15].

2.3. Praktik Terbaik dalam Keamanan Aplikasi Web

Tinjauan praktik terbaik dalam keamanan aplikasi web melibatkan beberapa strategi kunci yang secara signifikan mempengaruhi tingkat keamanan. Di antaranya termasuk validasi input yang cermat untuk mencegah penyisipan kode berbahaya atau perintah SQL yang merugikan sistem. Manajemen database yang aman juga menjadi perhatian utama; langkah-langkah seperti penggunaan hak akses terbatas dan pemantauan aktif terhadap aktivitas database membantu mencegah akses tidak sah atau manipulasi data. Penggunaan teknik enkripsi data, terutama untuk data sensitif, memastikan bahwa informasi penting terlindungi bahkan jika diakses oleh pihak yang tidak berwenang. Selain itu, praktik mitigasi risiko lainnya, seperti penerapan kebijakan keamanan yang ketat dan pembaruan rutin perangkat lunak, juga menjadi bagian integral dari strategi keseluruhan untuk mengurangi risiko dan melindungi aplikasi dari serangan yang berpotensi merusak. Integrasi praktik-praktik ini memberikan panduan yang kokoh dalam merancang perbaikan yang mampu secara signifikan meningkatkan tingkat keamanan aplikasi.[16] [17] [18].

2.4. Karakteristik Unik PT Rachma Perkasa Utama

Tinjauan ini juga akan melibatkan aspek-aspek khusus dari PT Rachma Perkasa Utama yang dapat memiliki dampak signifikan pada keamanan aplikasi web. Ini termasuk lingkungan industri di mana perusahaan beroperasi, jenis data sensitif yang diolah dalam aplikasi, serta infrastruktur teknologi yang menjadi landasan dari sistem aplikasi tersebut. Memahami karakteristik unik ini menjadi kunci dalam mengidentifikasi titik-titik kritis yang mempengaruhi keamanan aplikasi web, karena memahami konteks di mana aplikasi tersebut beroperasi membantu merancang solusi keamanan yang lebih relevan dan efektif. [19] [20].

3. METODE PENELITIAN

Tim peneliti gabungan dari ahli keamanan TI dan pengembang aplikasi melakukan evaluasi keamanan aplikasi web PT Rachma Perkasa Utama. Pendekatan mereka terdiri dari langkah-langkah:

Gambar 1. Langkah evaluasi keamanan

3.1. Pengenalan dan Persiapan

Tim bertemu dengan internal perusahaan, memahami tujuan aplikasi, dan mendapatkan akses yang diperlukan.

3.2. Pengumpulan Informasi

Mereka menggali dokumentasi teknis, menganalisis kode sumber, dan kebijakan keamanan untuk mengidentifikasi potensi kerentanan, khususnya Injeksi SQL dan XSS.

3.3. Evaluasi dan Analisis Mendalam

Melalui pengujian, tim mencari kerentanan keamanan. Mereka memvalidasi celah keamanan dengan alat bantu dan teknik manual, fokus pada Injeksi SQL dan XSS, serta menganalisis dampak potensial.

3.4. Rekomendasi dan Laporan

Berdasarkan hasil, mereka merumuskan rekomendasi seperti validasi input yang lebih kuat dan pembaruan sistem. Laporan mereka mencakup ringkasan temuan, analisis kerentanan, dan rekomendasi perbaikan.

3.5. Validasi dan Implementasi

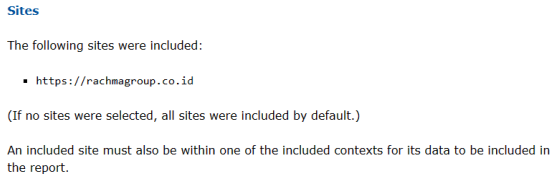
Tim memverifikasi kembali rekomendasi sebelum bekerja sama dengan PT Rachma Perkasa Utama dalam menerapkan perbaikan yang direkomendasikan.

4. HASIL DAN PENGUJIAN

Dalam tahapan ini, penelitian menggunakan Zed Attack Proxy (ZAP) untuk melakukan pemindaian keamanan pada aplikasi web PT Rachma Perkasa Utama. Pemindaian dilakukan dengan fokus pada identifikasi dan evaluasi potensi kerentanan keamanan, khususnya terhadap serangan Injeksi SQL dan Cross-Site Scripting (XSS).

4.1. Parameter Pemindaian

Pemindaian dilakukan pada situs web https://rachmagroup.co.id dengan memperhitungkan semua konteks yang relevan dalam evaluasi keamanan aplikasi web. Pemilihan situs ini sangat dipertimbangkan untuk memastikan bahwa seluruh aspek terkait keamanan aplikasi web dievaluasi secara komprehensif. Dengan memilih situs web ini, penelitian ini dapat menyelidiki setiap elemen yang memengaruhi keamanan aplikasi, termasuk infrastruktur, aliran data sensitif, interaksi pengguna, dan lingkungan di mana aplikasi beroperasi secara menyeluruh.



Gambar 2. Parameter Pemindaian

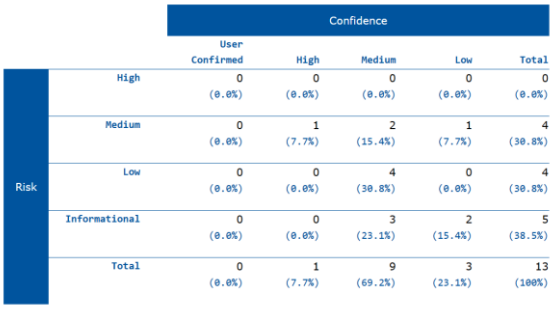
4.2. Tingkat Risiko dan Kepercayaan

Dalam pemindaian ini, evaluasi risiko mencakup klasifikasi risiko dari tingkat tinggi hingga rendah, serta kategori informasional. Begitu juga dengan evaluasi tingkat kepercayaan, yang mencakup tingkat kepercayaan pengguna yang telah terkonfirmasi, tinggi, sedang, dan rendah. Dengan pendekatan yang komprehensif ini, setiap potensi risiko dievaluasi dari berbagai tingkatan keparahan, memungkinkan identifikasi dan prioritisasi yang tepat terhadap masalah keamanan aplikasi web. Evaluasi tingkat risiko yang komprehensif memberikan pemahaman yang lebih mendalam tentang rentang potensi ancaman yang mungkin terjadi, sedangkan evaluasi tingkat kepercayaan membantu menilai sejauh mana keandalan serta kredibilitas pengguna yang terlibat dalam penggunaan aplikasi.

Gambar 3. Hasil tingkat resiko kepercayaan

4.3. Ringkasan Hasil Pemindaian

Berikut adalah ringkasan hasil pemindaian berdasarkan tingkat risiko dan kepercayaan:



		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Low	0 (0.0%)	0 (0.0%)	4 (30.8%)	0 (0.0%)	4 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	3 (23.1%)	2 (15.4%)	5 (38.5%)
	Total	0 (0.0%)	1 (7.7%)	9 (69.2%)	3 (23.1%)	13 (100%)

Gambar 4. Hasil pemindaian

a. Risiko Tinggi
   Tidak ada temuan kerentanan tingkat risiko tinggi.
b. Risiko Sedang
   1 temuan dengan tingkat risiko sedang, melibatkan ketidaksetujuan terhadap kebijakan pengamanan.
c. Risiko Rendah
   4 temuan dengan tingkat risiko rendah, termasuk ketidakpatuhan terhadap praktik keamanan tertentu.
d. Risiko Informasional
   8 temuan dengan tingkat risiko informasional, termasuk informasi yang ditemukan yang tidak secara langsung mengancam keamanan.

4.4. Analisis Keseluruhan Temuan Pemindaian

Dalam mengevaluasi hasil pemindaian dari ZAP, analisis dilakukan dengan mengacu pada pengetahuan yang terdokumentasi dalam literatur terkait. Referensi literatur seperti "Analisis Kerentanan Website Dengan Aplikasi Owasp Zap" (Hasibuan & Handoko, 2023) dan "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta" (Hariyadi & Nastiti, 2021) menjadi acuan utama. Dengan mengintegrasikan temuan dari penelitian terdahulu, penafsiran terhadap hasil pemindaian ZAP menjadi lebih kontekstual dan terperinci. Melalui pendekatan ini, penelitian ini dapat menggabungkan wawasan praktis yang terkait dengan aplikasi ZAP dari penelitian terdahulu, memungkinkan identifikasi yang lebih baik terhadap potensi kerentanan dan solusi yang mungkin lebih efektif untuk memperbaiki keamanan aplikasi web PT Rachma Perkasa Utama.

a. Kesamaan dengan Hasil Literatur
   Pemindaian dengan ZAP sejalan dengan praktik keamanan yang diidentifikasi dalam literatur, seperti penggunaan ZAP untuk mengidentifikasi kerentanan keamanan.
b. Analisis Keseluruhan
   - Temuan kerentanan risiko sedang dan rendah menunjukkan bahwa ada beberapa aspek yang perlu diperbaiki dalam hal keamanan aplikasi web PT Rachma Perkasa Utama.
   - Ketidaksetujuan terhadap kebijakan keamanan perlu mendapat perhatian khusus untuk memastikan kepatuhan terhadap praktik keamanan terbaik.

4.5. Hubungan dengan Literatur Terdahulu

Temuan dari hasil pemindaian menggunakan ZAP dapat dihubungkan dengan informasi yang terdokumentasi dalam literatur terdahulu. Misalnya, studi-studi sebelumnya seperti "Analisis Kerentanan Website Dengan Aplikasi Owasp Zap" dan "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta" menyoroti berbagai kerentanan yang mungkin ditemukan dalam aplikasi web menggunakan ZAP.

Pemindaian dengan ZAP mungkin memvalidasi temuan-temuan ini atau memberikan wawasan tambahan tentang kerentanan yang serupa atau berbeda. Temuan pemindaian bisa mendukung temuan dari literatur, menegaskan praktik terbaik yang telah diidentifikasi sebelumnya. Selain itu, pemindaian juga mungkin menantang sebagian temuan yang ada dalam literatur dengan menyoroti kerentanan yang tidak dijelaskan atau menghadirkan aspek keamanan yang belum diperhatikan sebelumnya dalam literatur.

Pentingnya adalah untuk melihat bagaimana hasil pemindaian, baik menegaskan maupun menantang, berkontribusi pada pemahaman peneliti tentang praktik terbaik keamanan aplikasi web. Apakah itu memperkuat temuan yang sudah ada, menambah dimensi baru pada pemahaman, atau bahkan memunculkan elemen keamanan yang belum teridentifikasi sebelumnya, semuanya penting untuk mengembangkan pemahaman yang lebih dalam dan solusi yang lebih kokoh dalam melindungi aplikasi web.

1. Dukungan terhadap Praktik Terbaik
   Temuan pemindaian mendukung praktik keamanan terbaik yang diidentifikasi dalam literatur-literatur sebelumnya, seperti penggunaan ZAP untuk mengidentifikasi kerentanan keamanan.
2. Pertimbangan Lanjutan
   Dalam merespon temuan, pertimbangkan langkah-langkah yang telah diusulkan dalam literatur untuk memperbaiki kerentanan serupa.

4.6. Rekomendasi Perbaikan

Berikan rekomendasi perbaikan berdasarkan temuan dari pemindaian ZAP dan literatur-literatur terdahulu. Rekomendasikan langkah-langkah konkret untuk memitigasi kerentanan yang teridentifikasi, dan sertakan saran tentang praktik terbaik yang dapat diimplementasikan untuk meningkatkan keamanan aplikasi web PT Rachma Perkasa Utama.

1. Validasi Input yang Lebih Ketat
   Implementasikan validasi input yang ketat untuk mencegah serangan Injeksi SQL. Gunakan metode parameterized queries atau prepared statements untuk mengolah data dari pengguna, sehingga data pengguna tidak dieksekusi sebagai perintah SQL.
2. Pembaruan Rutin dan Pengelolaan Patch
   Lakukan pembaruan rutin pada seluruh komponen aplikasi web, termasuk sistem operasi, server web, basis data, dan framework yang digunakan. Pemeliharaan rutin membantu meminimalkan risiko karena kerentanan yang diperbaiki dalam pembaruan.
3. Manajemen Sesi yang Diperbarui
   Perbarui manajemen sesi untuk mencegah serangan Cross-Site Scripting (XSS). Gunakan teknik seperti penggunaan token keamanan, header HTTP yang sesuai, dan sanitasi input pengguna untuk mencegah injeksi skrip berbahaya.
4. Implementasi Enkripsi Data
   Lindungi data sensitif dengan menerapkan enkripsi baik saat penyimpanan maupun saat berpindah melalui jaringan. Hal ini membantu melindungi informasi sensitif dari akses yang tidak sah.
5. Peningkatan Kesadaran Keamanan
   Lakukan pelatihan terjadwal dan upaya peningkatan kesadaran keamanan untuk tim pengembang dan administrator aplikasi web. Fokuskan pada pemahaman mendalam tentang risiko keamanan, kebijakan terbaru, dan teknik mitigasi yang efektif.

6. Pengujian Keamanan Berkala
   Lakukan pengujian keamanan berkala menggunakan alat seperti ZAP atau alat serupa untuk mendeteksi kerentanan dan memperbaikinya sesuai kebutuhan.
7. Implementasi Praktik Terbaik dari OWASP
   Terapkan praktik terbaik dari Open Web Application Security Project (OWASP) untuk memastikan kepatuhan dan kesiapan aplikasi terhadap serangan yang berpotensi.

Integrasi langkah-langkah ini secara menyeluruh dapat membantu meminimalkan kerentanan keamanan aplikasi web PT Rachma Perkasa Utama dan meningkatkan ketahanannya terhadap berbagai ancaman siber. Dengan terus memperbarui dan meningkatkan strategi keamanan, aplikasi dapat tetap aman dan terlindungi dari serangan yang mungkin terjadi di masa mendatang.

5. KESIMPULAN DAN SARAN

Penelitian ini meneliti keamanan aplikasi web di PT Rachma Perkasa Utama dengan fokus pada serangan Injeksi SQL dan XSS menggunakan metode OWASP. Hasil analisis menunjukkan temuan penting, termasuk identifikasi kerentanan dengan risiko sedang hingga rendah dan ketidakpatuhan pada kebijakan keamanan. Kesimpulan menegaskan perlunya perbaikan untuk meningkatkan keamanan aplikasi web, sejalan dengan praktik keamanan sebelumnya. Rekomendasi termasuk penerapan validasi input yang lebih ketat, pembaruan manajemen sesi, dan pelatihan keamanan bagi pengembang dan administrator aplikasi web.

DAFTAR PUSTAKA

[1] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. …*, 2021, [Online]. Available: https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/24777

[2] B. Wicaksono, R. Y. R. Kusumaningsih, and ..., "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing Dan Dast (Dynamic Application Security Testing)," *J. …*, 2020, [Online]. Available: https://journal.akprind.ac.id/index.php/jarkom/article/view/2755

[3] B. Ghozali, K. Kusrini, and ..., "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. …*, 2019, [Online]. Available: http://citec.amikom.ac.id/main/index.php/citec/article/view/119

[4] S. LIKMI, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *pdfs.semanticscholar.org*. [Online]. Available: https://pdfs.semanticscholar.org/c286/de02c7c5a134b62e02899cfdf060c20eb014.pdf

[5] A. Fajarino, Y. N. Kunang, H. M. Yudha, and ..., "Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang," *J-SAKTI (Jurnal …*, 2023, [Online]. Available: http://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/702

[6] D. Aryanti and J. N. Utamajaya, "Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja," *J. Fusion*, 2021, [Online]. Available: http://fusion.rifainstitute.com/index.php/fusion/article/view/53

[7] B. Kurniawan and I. Ruslianto, "Implementation of Penetration Testing on the Website Using the Penetration Testing Execution Standard (PTES) Method," *CESS (Journal Comput. Eng. …*, [Online]. Available: https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/47096

[8] S. F. Sijabat, *ANALISIS PERBANDINGAN KEAMANAN WEBSITE REKRUTMEN BUMN DAN KOLABJAR-ASNPINTAR DENGAN ACUNETIX DAN OWASP ZAP*. repositori.unsil.ac.id, 2023. [Online]. Available: http://repositori.unsil.ac.id/id/eprint/10719

[9] R. Umar, I. Riadi, and M. I. A. Elfatiha, "Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF," *Jutisi J. Ilm. …*, 2023, [Online]. Available: http://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/article/view/1191

[10] S. Alhidamkara, I. L. Kharisma, and ..., "Analisis Keamanan Website Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan Comprehensive Website Security Assessment," *… (Seminar Nas. Has. …*, 2023, [Online]. Available: http://prosiding.unipma.ac.id/index.php/sendiko/article/view/3699

[11] D. F. Syech, *ANALISIS KEAMANAN WEBSITE PEMERINTAH KOTA TIDORE KEPULAUAN MENGGUNAKAN METODE VULNERABILITY ASSESSMENT*. eprints.ipdn.ac.id, 2023. [Online]. Available: http://eprints.ipdn.ac.id/15861/

[12] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, 2022, [Online]. Available: https://jidt.org/jidt/article/view/190

[13] H. Hendra and E. B. Prasetya, "Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang

WFH," *Pros. Semnastek*, 2021, [Online]. Available: https://jurnal.umj.ac.id/index.php/semnastek/article/view/11483

[14] R. Farismana and D. Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," *J. Tek. ...*, 2023, [Online]. Available: https://ejurnal.politeknikpratama.ac.id/index.php/jutiti/article/view/2853

[15] B. P. Zen, R. A. G. Gultom, and ..., "Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," *Teknol. ...*, 2020, [Online]. Available: http://jurnalprodi.idu.ac.id/index.php/TP/article/view/574

[16] S. A. Robbani, *Analisa Kerentanan Keamanan Aplikasi Manajemen Aset Berbasis Web Menggunakan Metode OWASP (Open Web Application Security Project) Studi Kasus PT. XYZ*. repository.nurulfikri.ac.id, 2023. [Online]. Available: https://repository.nurulfikri.ac.id/id/eprint/254/

[17] B. T. K. Dewi and M. A. Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web," *AUTOMATA*, 2022, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/21883

[18] I. M. E. Listartha, G. A. J. Saskara, and ..., "Pengujian Kerentanan dan Penetrasi Keamanan pada Aplikasi Web Manajemen Skripsi Prodi XYZ," *... Comput. Sci. ...*, 2021, [Online]. Available: http://jurnal.untad.ac.id/jurnal/index.php/scientico/article/view/18178

[19] A. Z. Abidin, *Penetration Testing pada Wesite Mail Server dengan menggunakan Metode Owasp*. dspace.umkt.ac.id, 2023. [Online]. Available: https://dspace.umkt.ac.id/handle/463.2017/3528

[20] I. Dharmawangsa, G. M. A. Sasmita, and I. Pratama, "Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website)," *download.garuda.kemdikbud.go.id*. [Online]. Available: http://download.garuda.kemdikbud.go.id/article.php?article=3457857&val=30165&title=Penetration Testing Berbasis OWASP Testing Guide Versi 42 Studi Kasus X Website