

KAJIAN LITERATUR ANALISIS KEAMANAN WEBSITE

Jecksen Imada Nicholas Saputra Marbun, Cakra Trinata, Mila Rosmaya

Politeknik Imigrasi

Jalan Raya Gandul No. 4, RT.07 / RW.08, RT.5/RW.6, Gandul,

Kec. Cinere, Kota Depok, Jawa Barat 16514

jecksennicho@gmail.com

ABSTRAK

Era digitalisasi telah membawa banyak perubahan ke dalam kehidupan manusia. Digitalisasi telah banyak membantu manusia memudahkan hidupnya, salah satunya adalah penggunaan *website* sebagai wadah penyebaran informasi. Namun dari manfaat yang diberikan terdapat sebuah celah yang bisa membahayakan para penggunanya. Penelitian ini bertujuan untuk memberikan kajian analisa terhadap keamanan *website* untuk mencegah terjadinya kejahatan siber. Studi ini menggunakan metodologi PRISMA untuk menganalisis literatur yang mengkaji metode yang umum digunakan untuk menganalisis keamanan *website*. Pada penelitian ini dilakukan penetapan kriteria kelayakan artikel, seleksi literatur, pengumpulan data, dan seleksi data. Hasil penelitian menunjukkan variasi metode analisa *website*, termasuk OWASP, *Penetration Test*, ISSAF, *Vulnerability Testing*, *Vulnerability Scanning*, *Footprinting*, dan *Brute Force*. Penelitian yang dilakukan menunjukkan bahwa metode OWASP menjadi metode yang paling umum digunakan. Penelitian ini memberikan landasan untuk penelitian lebih lanjut dalam bidang keamanan *website*.

Kata Kunci : Keamanan Website; Metode Analisa Keamanan Website, OWASP, *Penetration Testing*

1. PENDAHULUAN

Perkembangan zaman telah membawa banyak perubahan yang berdampak pada kehidupan manusia. Salah satunya adalah digitalisasi. Hampir seluruh aspek kehidupan manusia di masa sekarang sudah mengalami digitalisasi dan mulai meninggalkan cara-cara kuno. Kemudahan mencari dan mendapatkan informasi serta melakukan komunikasi menjadi awal baru dari era digitalisasi. Kemudahan akses informasi seperti adanya internet, media sosial, berita digital, dan produk digital lainnya memberikan kemudahan akses informasi bagi setiap manusia. Hal ini turut mempercepat persebaran informasi dari satu individu ke individu lainnya.

Salah satu bentuk konkret dari adanya perkembangan zaman adalah pemanfaatan *website* sebagai media penyebaran informasi. *Website* memberikan dampak positif dengan menyebarkan informasi secara luas, dengan cepat dan mudah [1].

Website sudah banyak digunakan baik oleh sebuah instansi pemerintah, organisasi, bisnis, bahkan pribadi untuk melakukan penyebaran informasi. Kemudahan penyebaran dan akses bagi setiap orang membuat *website* menjadi salah satu pilihan terbaik untuk menjadi wadah informasi yang efektif dalam penyebaran informasi. *Website* turut menjadi sebuah *branding* atau profil bagi suatu badan ataupun organisasi untuk membangun citra di masyarakat.

Keamanan *website* sebagai sarana penyebaran informasi turut menjadi hal yang wajib diperhatikan untuk menghindari adanya pencurian data, peretasan, penyalahgunaan data dan kejahatan siber lainnya. Tingginya tingkat pemakaian *website* turut menjadi sebuah faktor yang menimbulkan kerentanan pada *website* dan menimbulkan risiko terjadinya peretasan [1].

Kerentanan *website* dapat dipengaruhi oleh faktor internal maupun eksternal. *Website* mudah rentan pada serangan seperti *SQL Injection*, *Cross Site Scripting*, *Brute Force*, dan *Malware* [2].

Kerentanan ini turut menjadi ancaman bagi para pengguna dalam penggunaannya, ancaman peretasan dan penyalahgunaan data menjadi ancaman yang cukup berbahaya.

Pengujian dan analisa keamanan *website* menjadi faktor penting dalam penggunaannya sebagai sarana penyebaran informasi di masa sekarang. Analisa keamanan yang dilakukan harus mencakup seluruh aspek sistem informasi seperti perlindungan terhadap integritas, kerahasiaan, ketersediaan data, serta keamanan pertukaran informasi dan komunikasi yang terjadi[3].

Analisa keamanan *website* harus bisa memastikan keamanan baik dari segi peraturan, prosedur, pedoman prinsip, dalam melindungi data yang ada[1].

Dalam melakukan analisa keamanan *website* tersedia berbagai metode yang dapat digunakan. Metode yang dapat digunakan seperti *Information Systems Security Assessment Framework* (ISSAF), *Open Web Application Security Project* (OWASP), *Open Source Security Testing Methodology Manual* (OSSTMM), *Penetration Testing* (PTES), dan beberapa metode lainnya [4].

Berbagai macam metode analisa keamanan *website* yang dapat digunakan memiliki ciri khasnya masing-masing, sebagai contoh PTES adalah metode yang runtut dalam menganalisis keamanan *website* [5] atau OWASP yang merupakan daftar kerentanan yang harus diuji pada sebuah *website* [6].

Pemilihan metode yang tepat dalam analisa keamanan *website* menjadi hal yang penting untuk

melihat risiko pada *website* dan memudahkan individu atau organisasi dalam mencegah terjadinya kejahatan siber pada *website*.

2. TINJAUAN PUSTAKA

Analisis adalah proses sistematis yang digunakan untuk menemukan pola atau cara berpikir melalui pengujian terhadap suatu hal dengan menganalisis bagian-bagian, hubungan antar bagian, dan kaitannya dengan keseluruhan. Proses melakukan penguraian masalah menjadi bagian-bagian kecil (dekomposisi) membuat struktur dan bentuknya menjadi lebih jelas dan mudah dipahami. Pada analisis data, langkah yang dilaksanakan adalah pengorganisasian data yang diperoleh, memecah menjadi bagian-bagian kecil, pengelompokan, penyaringan pada bagian yang relevan, dan menyusun kesimpulan agar informasi tersebut dapat dipahami [7].

Website adalah kumpulan dari beberapa halaman web dimana informasi dalam bentuk teks, gambar, suara, dan lain-lain dipresentasikan dalam bentuk *hypertext* dan dapat diakses oleh perangkat lunak yang disebut dengan browser [8].

Website adalah fitur internet yang menghubungkan dokumen baik secara lokal maupun jarak jauh. Pada website dokumen disebut dengan *web page* dan *link* memberikan pengalaman pengguna website yang memungkinkan berpindah dari satu *page* ke *page* lain [8].

Keamanan website adalah sebuah prioritas yang sangat utama bagi seorang pengelola atau pengguna *website*. Mengabaikan keamanan suatu website dapat menyebabkan kerugian pada pengguna itu sendiri karena rentan terjadi pencurian dan penyalahgunaan data-data penting pada suatu website. Hal yang paling utama dalam keamanan website adalah melindungi perangkat keras dan perangkat lunak, serta jaringan guna mengamankan informasi yang berada didalamnya [7].

Pada penelitian terdahulu, terdapat beberapa cara untuk menganalisis keamanan sebuah *website*. Seperti pada penelitian yang dilakukan untuk menganalisis keamanan *website* Kecamatan Cibodas [9], peneliti memilih untuk menggunakan metode *Open Web Application Security Project* (OWASP).

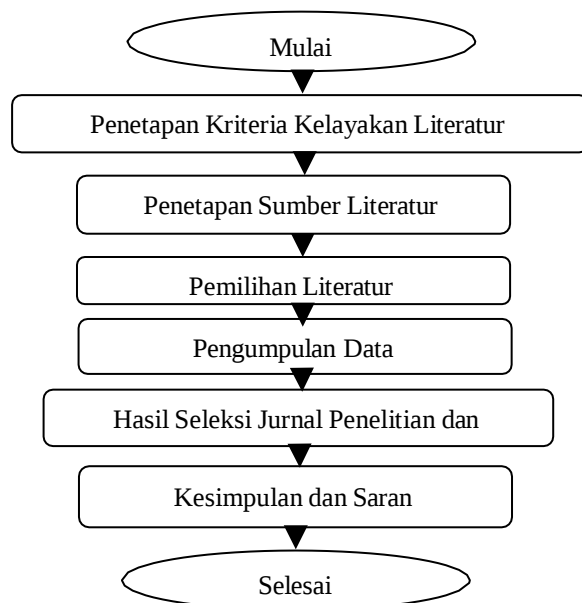
Berbeda dengan penelitian pada analisis keamanan *website* Universitas Internasional Batam [10], metode *Information Systems Security Assessment Framework* (ISSAF) menjadi pilihan yang diambil oleh peneliti. Penelitian ini dilakukan guna menemukan metode yang paling umum serta paling baik yang ditinjau dari penelitian-penelitian terdahulu, untuk membantu memberikan rekomendasi metode untuk penelitian berikutnya.

3. METODE PENELITIAN

Pada penelitian ini dilakukan survei menyeluruh terhadap penelitian yang membahas terkait dengan analisis keamanan *website*, berfokus

pada metode yang digunakan untuk menganalisis keamanan *website*. Kajian literatur ini disusun dengan metode PRISMA (*Preferred Reporting Items for Systematic Review and Meta-analysis*). Proses ini dibagi menjadi 4 (empat) tahap, yaitu: Penetapan Kriteria Kelayakan, Penetapan Sumber Informasi, Seleksi Literatur, dan Pengumpulan Data [11].

Kajian literatur dilakukan pada artikel yang dipublikasikan antara tahun 2017 sampai tahun 2025 yang membahas mengenai sebuah analisa dan uji penetrasi untuk memastikan keamanan dari sebuah *website*. Pencarian Artikel dilakukan dengan menggunakan kata kunci “Keamanan *Website*” menggunakan aplikasi *Harzing publish or perish*.



Gambar 1. Flowchart penelitian

Tahap 1 : Kriteria kelayakan artikel. Ditentukan *Inclusion Criteria* (IC), yaitu:

- a. IC1: artikel harus merupakan penelitian asli yang telah dipelajari dan ditulis dalam bahasa Indonesia.
- b. IC2: artikel diterbitkan antara tahun 2017 hingga 2025.
- c. IC3: artikel bertujuan untuk menganalisis keamanan sebuah *website* dengan metode penelitian atau cara yang sudah ada dan dapat diakses oleh semua orang.

Tahap 2 : Penetapan sumber literatur

- a. Literatur dicari pada basis data daring dengan repositori signifikan untuk studi akademis seperti *Crossref*, *Google Scholar*, dan *Semantic Scholar*
- b. Pada artikel-artikel yang memenuhi syarat untuk IC, dicari juga penelitian lain yang berhubungan dengan penelitian ini.

Tahap 3 : Pemilihan Literatur

- a. Kata Kunci penentuan pertama adalah “Keamanan *Website*”. Untuk mengeksplorasi dan

memilih judul, abstrak dan artikel kata kunci diperoleh dari hasil pencarian kelayakan kriteria yang telah ditentukan sebelumnya.

- b. Baca artikel yang tidak dihilangkan dari sebelumnya tahap, penuh atau sebagian, untuk menentukan item tersebut memenuhi syarat untuk peninjauan berikutnya
- c. Artikel terpilih dinilai kembali untuk menemukan penelitian terkait

Tahap 4 : Pengumpulan Data

Data dikumpulkan secara manual dengan membuat formulir ekstraksi data. Penelitian ini memfilter 651.433 jurnal dari seluruh sumber dan kriteria yang dicari. Terdapat 71 jurnal ilmiah yang dirasa dapat menjadi calon referensi menurut judul dan abstrak untuk menjawab pertanyaan penelitian atau *research question*. Setelah dipelajari lebih lanjut hanya 35 artikel yang terpilih dan dapat memenuhi syarat dalam penelitian ini. Tabel 1 menunjukkan data yang telah dikumpulkan.

Tabel 1. Hasil Seleksi Jurnal Penelitian

Sumber	Keamanan Website	Kandidat	Terpilih
Crossref	32.443	47	27
Google Scholar	134.000	16	5
Semantic Scholar	485.000	8	3
Total	651.443	71	35

Kajian literatur ini menjawab satu *Research Question* yang sudah dibuat sebagai berikut :

Tabel 2. Pertanyaan Penelitian

ID	Pertanyaan Penelitian	Latar Belakang
RQ	Metode apa yang sering digunakan dalam menganalisa keamanan website?	Mengidentifikasi metode yang sering digunakan pada penelitian yang sudah ada.

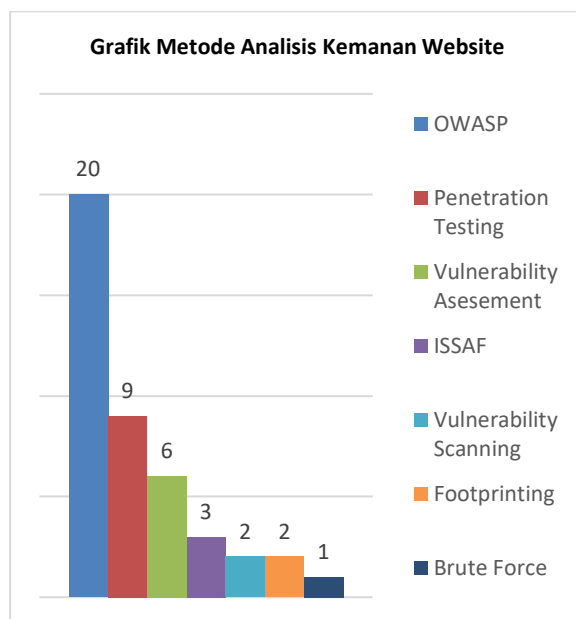
4. HASIL DAN PENELITIAN

Tabel 3. Hasil Tinjauan Literatur

No	Penulis	Judul	Tahun	Metode
1	SE Prasetyo, N Hassanah[10]	Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF	2021	ISSAF
2	D Aryanti, JN Utamajaya[12]	Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja	2021	OWASP
3	M Fatkhurozzi[13]	Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus	2021	Footprinting dan Vulnerability Scanning
4	E Nurelasari, DG Al Farabi[14]	Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (OWASP) Pada Simantep. Id	2024	OWASP
5	Y Mulyanto, E Haryanti, J Jumirah[7]	Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement: Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement	2021	Vulnerability Asesement
6	B Ghazali, K Kusriani...[15]	Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode OWASP (Open Web Application Security Project) Untuk Penilaian Risk Rating	2019	OWASP
7	Y Mulyanto, MTA Zaen, Y Yuliadi...[16]	Analisis Keamanan Website Sma Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)	2022	Penetration Testing
8	YTA Rosaliah, J Jayanta...[17]	Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing Dan Metode OWASP TOP 10 Pada Website SIM Xxx	2021	Penetration Testing dan OWASP
9	IO Riandhanu [18]	Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing Pada Keamanan Website Absensi	2022	Penetration Testing dan OWASP
10	VI Sugara, IW Sriyasa[19]	Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP)	2024	OWASP
11	S Andriyani, MF Sidiq, BP Zen[20]	Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website Smk Al-Kautsar	2023	Penetration Testing dan ISSAF
12	M Fronita[21]	Analisis Celah Keamanan Website Sitasi Menggunakan Vulnerability Assessment	2023	Vulnerability Asesement
13	A Syafaat[22]	Identifikasi Kerentanan Keamanan Pada Website Fakultas Ilmu Komputer Universitas Subang Menggunakan Metodologi OWASP	2024	OWASP
14	AM Akmal, N Heryana...[23]	Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment	2022	Vulnerability Asesement
15	M Tahir, MR Ardiansyah[3]	Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)	2024	Penetration Testing

No	Penulis	Judul	Tahun	Metode
16	S Hidayatulloh, D Saptadijaji[24]	<i>Penetration Testing</i> Pada Website Universitas ARS Menggunakan <i>Open Web Application Security Project</i> (OWASP)	2021	OWASP
17	VS Nugroho, FW Christanto[25]	Analisis Keamanan Website Dengan Information System Security Assessment Framework (ISSAF) Dan <i>Open Web Application Security Project</i> (OWASP)	2023	ISSAF dan OWASP
18	A Hardiansyah[26]	Analisis Keamanan Website SIAKAD Untirta Menggunakan Teknik Footprinting Dan Vulnerability Scanning	2024	Footprinting dan Vulnerability Scanning
19	M Akil, EI Alwi, SM Abdullah[27]	Analisa Keamanan Website Terhadap Serangan Html Injection Menggunakan Metode Penetration Testing	2024	<i>Penetration Testing</i>
20	IME Listartha, IMAP Mitha, MWA Arta...[28]	Analisis Kerentanan Website Sma Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project)	2022	OWASP
21	P Harahap, I Zufria[6]	Analisis Keamanan Pada Website Upm Saintek Uin-Su Medan Menggunakan Metode Vulnerability Assesment	2024	Vulnerability Asesement dan OWASP
22	NA Zahra, FH Zidane...[29]	Analisis Keamanan Sistem Informasi Pada Website Pt Sentra Vidya Utama (Sevima) Menggunakan Metode OWASP	2023	OWASP
23	TL Widodo[30]	Analisa Kerentanan Keamanan Website Tiketkai. Com Menggunakan OWASP Zap Dengan Metode PTES (Studi Kasus Pt. Kai Divre 3 Palembang)	2023	<i>Penetration Testing</i> dan OWASP
24	N Cholis, EIH Ujianto [31]	Analisis Keamanan Website Smk Taman Karya Kebumen Menggunakan Metode Vulnerability Asesement	2024	Vulnerability Asesement
25	I Riadi, Y Kurniawan, IA Rafiq[2]	Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (Issaf)	2023	ISSAF
26	A Zandra, M Hardjianto[32]	Deteksi Celah Keamanan Xss Pada Website Dengan Metode Brute Force	2024	Brute Force
27	T Ariyadi, H Fadli, T Akbar, ...[33]	Implementasi OWASP Untuk Analisis Kerentanan Dan Keamanan Pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma	2025	OWASP
28	Muhammad Arifai Nurrizki[1]	Analisis Keamanan Website Desa Budaya DIY Dengan Metode <i>Penetration Testing</i> (Pentest) Dan OWASP ZAP	2024	<i>Penetration Testing</i> dan OWASP
29	Nurjannah, Abdul Muni[34]	Analisis Keamanan Website Sekolah Sman 1 Tempuling Dengan Menggunakan <i>Open Web Application Security Project</i> (OWASP)	2024	OWASP
30	Tamsir Ariyadi, Tantri Langgeng Widodo, Nely Apriyanti, Febriani Sasti Kirana[35]	Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP	2023	OWASP
31	Fidyatun Nisa, Nanda Sitti Nurfebruary, Muhammad Ikhwani[36]	Analisis Keamanan Sistem Informasi Website Portal Akademik Universitas Malikussaleh Menggunakan OWASP ZAP	2024	OWASP
32	Muhammad Nur Fikri, Biti Parga Zen, Rifki Adhitama, Eryan Ahmad Firdaus[5]	Analisis Keamanan Sistem Informasi Website Sma Negeri 1 Sokaraja Menggunakan Metode <i>Penetration Testing</i> Execution Standard (PTES)	2023	<i>Penetration Testing</i>
33	Wahyudin Wahyudin, Heri Kuswara, R. Resti, Sopiyan Dalis[37]	Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points Of Sales	2024	Vulnerability Asesement
34	Janstipen Roy Mansen Sagala, Yusnia Budiarti, Rosi Kusuma Serli[9]	Analisis Keamanan Website Kecamatan Cibodas Tangerang Dengan Metode Open Web Application Security Project	2024	OWASP
35	M. A. Mu'min, Abdul Fadli, Imam Riadi[38]	Analisis Keamanan Sistem Informasi Akademik Menggunakan <i>Open Web Application Security Project</i> Framework	2022	OWASP

Pada hasil tinjauan literatur yang sudah dilakukan, peneliti telah mengambil 35 literatur yang dapat dijadikan referensi untuk melakukan penelitian ‘Analisis Keamanan Website’. Sesuai dengan *Research Question* yang sudah ditentukan diawal, pada tinjauan literatur yang dilakukan peneliti mengambil data berupa metode apa saja yang digunakan oleh penelitian terdahulu dalam melakukan analisis keamanan *website*. Hasil analisa di uraikan dalam grafik pada gambar 2.



Gambar 2. Grafik Jumlah Metode Analisis Keamanan Website

Dari grafik yang sudah dibuat, terdapat tujuh metode yang digunakan pada penelitian terdahulu untuk menganalisis keamanan *website*. Dari tujuh metode yang ada, OWASP menjadi metode yang paling sering digunakan pada penelitian terdahulu. OWASP adalah metode pengujian keamanan *website* dengan parameter yang disusun oleh organisasi OWASP [24].

OWASP membentuk 10 daftar kerentanan yang sering mengancam keamanan sebuah *website* dengan sebutan ‘OWASP TOP 10’. Daftar ini dibuat untuk membantu baik individu dan organisasi mudah melihat keamanan *website* sehingga membantu pengambilan keputusan yang tepat dalam menanggulangi risiko keamanan *website* mereka. [24].

Metode OWASP memberikan kemudahan dalam menganalisis keamanan *website* dengan adanya daftar yang ada. Peneliti diberikan sebuah panduan dari daftar yang ada guna memudahkan analisa kerentanan *website* yang diteliti.

Pada tinjauan literatur yang dilakukan, metode *Penetration Testing* (PTES) menjadi metode kedua yang paling banyak digunakan. PTES merupakan metode analisa keamanan *website* dengan melakukan tujuh tahapan yang ada berupa *Pre- engagement Interaction, Intelligence Gathering, Threat Modeling,*

Vulnerability Analysis, Exploitation, Post Exploitation, Reporting [5].

PTES merupakan metode yang terstruktur dalam menganalisis keamanan *website*. Metode ini menawarkan runtutan penelitian yang jelas mulai dari identifikasi awal masalah, proses analisis, hasil analisa, dan juga pelaporan hasil dari jawab atas identifikasi masalah yang sudah dibuat. PTES memudahkan peneliti untuk melakukan analisa keamanan *website* yang lebih runtut dan terstruktur.

Tidak hanya OWASP dan PTES, terdapat metode lain seperti *Vulnerability Asesement, ISSAF, Vunerability Scanning, Footprinting*, dan juga *Brute Force* turut digunakan pada penelitian terlebih dahulu. Namun tidak sedikit ditemukan bahwa terdapat penelitian yang menggunakan metode campuran pada tinjauan literatur yang telah dilakukan. Metode OWASP dan PTES menjadi metode yang paling banyak digunakan secara bersamaan pada penelitian terdahulu [17],[18], [35],[1].

Beberapa penelitian yang menggunakan lebih dari satu metode mempunyai tujuan untuk mendapatkan hasil analisa yang lebih rinci guna mendapat hasil analisa yang memuaskan. Tidak hanya itu, penggunaan metode campuran pada penelitian terdahulu disesuaikan dengan kebutuhan peneliti, kerentanan lebih pada *website* yang diteliti, dan proses pengujian yang lebih mendetail terhadap analisa keamanan *website*.

5. KESIMPULAN

Penelitian ini dilakukan kegiatan meninjau literatur yang ada atau pada penelitian terdahulu mengenai analisa keamanan *website*, dengan berfokus pada metode yang digunakan untuk menganalisis keamanan *website*. Hasil dari kajian literatur yang sudah dibuat menunjukkan bahwa metode OWASP menjadi metode yang paling umum digunakan pada penelitian terdahulu. Metode OWASP menjadi metode yang paling umum karena memberikan kemudahan bagi peneliti untuk menganalisis keamanan *website* berdasar dengan daftar yang sudah dibuat oleh organisasi OWASP. Dengan daftar yang sudah metode OWASP menawarkan kemudahan bagi peneliti dengan daftar kerentanan yang dirasa penting untuk ditinjau demi keamanan sebuah *website*.

Tidak hanya itu, pada tinjauan literatur yang telah dilakukan, ditemukan beberapa penelitian yang menggunakan metode campuran dalam menganalisis keamanan *website*. Menggabungkan metode yang ada dirasa mampu memberikan analisa yang lebih rinci dan memuaskan. Penggabungan metode mampu memberikan analisa yang lebih detail terhadap kerentanan sebuah *website*. Penggabungan metode disesuaikan dengan kebutuhan peneliti, kerentanan *website*, dan proses yang lebih detail guna mendapat hasil yang maksimal. OWASP dan PTES merupakan penggabungan metode yang cukup sering ditemukan pada penelitian terdahulu.

DAFTAR PUSTAKA

- [1] M. A. Nurriszki, "Analisis Keamanan Website Desa Budaya DIY Dengan Metode Penetration Testing (Pentest) dan OWASP ZAP," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 5, no. 1, pp. 22–27, 2024, doi: 10.31102/jatim.v5i1.2620.
- [2] H. Herman, I. Riadi, Y. Kurniawan, and I. A. Rafiq, "Analisis Keamanan Website Menggunakan Information System Security Assessment Framework(ISSAF)," *J. Teknol. Inform. dan Komput.*, vol. 9, no. 1, pp. 126–136, 2023, doi: 10.37012/jtik.v9i1.1439.
- [3] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," vol. 09, pp. 118–125, 2024.
- [4] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.
- [5] M. Nur Fikri, B. Parga Zen, R. Adhitama, and E. Ahmad Firdaus, "Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Inform.*, vol. 2, no. 2, pp. 19–27, 2023, doi: 10.57094/ji.v2i2.1046.
- [6] P. Harahap and I. Zufria, "Analisis Keamanan Pada Website UPM SAINTEK UIN-SU Medan Menggunakan Metode Vulnerability Assesment," *Februari*, vol. 2, no. 1, pp. 10–20, 2024, [Online]. Available: <http://creativecommons.org/licenses/by-sa/4.0/>
- [7] Y. Mulyanto, E. Haryanti, and J. Jumirah, "Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement," *J. Inform. Teknol. dan Sains*, vol. 3, no. 3, pp. 394–400, 2021, doi: 10.51401/jinteks.v3i3.1260.
- [8] Yumarlin MZ, "Evaluasi Penggunaan Website Universitas Janabadra Dengan Menggunakan Metode Usability Testing," *Inf. Interaktif*, vol. 1, no. 1, pp. 34–43, 2016, [Online]. Available: <http://www.e-journal.janabadra.ac.id/index.php/informasiinteraktif/article/view/345>
- [9] J. R. Mansen Sagala, Y. Budiarti, and R. K. Serli, "Analisis Keamanan Website Kecamatan Cibodas Tangerang Dengan Metode Open Web Application Security Project," *INFORMATIKA*, vol. 12, no. 2, pp. 341–347, Jul. 2024, doi: 10.36987/informatika.v12i2.5948.
- [10] S. Eko Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *J. Ilm. Inform.*, vol. 9, no. 02, pp. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.
- [11] F. Samuel Karunia, P. Assiroj, I. Anung Prabadhi, F. Gunawan, and K. Ananda Mustari, "Systematic Literature Review Peta Kerawanan Keimigrasian Berbasis Sistem Informasi Geografis," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 8, no. 3, pp. 3593–3602, 2024, doi: 10.36040/jati.v8i3.9744.
- [12] D. Aryanti, Nurholis, and J. Nashar Utamajaya, "ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA," *J. Syntax Fusion*, vol. 1, no. 03, pp. 15–25, Sep. 2021, doi: 10.54543/fusion.v1i03.53.
- [13] M. Fatkhurozzi, "Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus," *Pros. Semin. Nas. Inform. Bela Negara*, vol. 2, pp. 144–148, 2021, doi: 10.33005/santika.v2i0.74.
- [14] E. Nurelasari and D. Gumilang Al Farabi, "Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) Pada Simantep.Id," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 8, no. 3, pp. 3049–3054, 2024, doi: 10.36040/jati.v8i3.9314.
- [15] B. Ghozali, K. Kusri, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.
- [16] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 202–209, 2022, doi: 10.47065/josh.v4i1.2335.
- [17] J. J. B. H. Yum Thurfah Afifa Rosaliah, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM," *Senamika*, vol. 2, no. September, pp. 752–761, 2021.
- [18] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.
- [19] Victor Ilyas Sugara and I Wayan Sriyasa, "Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP)," *Indones. J. Comput. Sci.*, vol. 13, no. 2, pp. 3315–3327, 2024, doi: 10.33022/ijcs.v13i2.3736.
- [20] S. Andriyani, M. F. Sidiq, and B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website

- SMK Al-Kautsar,” *J. Inform. Inf. Technol.*, vol. 8798, pp. 1–13, 2023.
- [21] M. Fronita, “ANALISIS CELAH KEAMANAN WEBSITE SITASI MENGGUNAKAN VULNERABILITY ASSESSMENT,” *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 9, no. 1, p. 1, Mar. 2023, doi: 10.24014/rmsi.v9i1.21823.
- [22] A. Syafaat, “Identifikasi Kerentanan Keamanan Pada Website Fakultas Ilmu Komputer Universitas Subang Menggunakan Metodologi Owasp,” *E-Journal*, vol. 11, no. 1, pp. 84–99, 2024, [Online]. Available: <http://ejournal.unsub.ac.id/index.php/Fasilkom>
- [23] A. M. Akmal, N. Heryana, and Arip Solehudin, “Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment,” *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 6298–6309, 2022.
- [24] S. Hidayatulloh and D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP),” *J. Algoritma*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.
- [25] V. Setyo Nugroho and F. Wahyu Christanto, “Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project (Owasp) Website Security Analysis With Information System Security Assessment Framework (Issaf) and Open Web Application Se,” *J. Ilm. NERO*, vol. 8, no. 2, p. 2023, 2023.
- [26] A. Hardiansyah, M. Rahmalia, and E. Putri, “ANALISIS KEAMANAN WEBSITE SIAKAD UNTIRTA MENGGUNAKAN TEKNIK FOOT PRINTING DAN VULNERABILITY SCANNING,” vol. 4, no. 1, pp. 26–35, 2024.
- [27] M. Akil *et al.*, “Open Access ANALISA KEAMANAN WEBSITE TERHADAP SERANGAN HTML INJECTION MENGGUNAKAN METODE PENETRASIION TESTING WEBSITE SECURITY ANALYSIS AGAINST HTML INJECTION USING THE METHOD PENETRASIION TESTING,” vol. 01, no. 01, pp. 42–50, 2024.
- [28] I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, and I. K. W. Yuda Arimika, “Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project),” *Simkom*, vol. 7, no. 1, pp. 23–27, 2022, doi: 10.51717/simkom.v7i1.63.
- [29] N. A. Zahra, F. H. Zidane, and N. R. Kuslaila, “Analisis Keamanan Sistem Informasi Pada Website Pt Sentra Vidya Utama (Sevima) Menggunakan Metode Owasp,” *Pros. Semin. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 1, pp. 384–393, 2023, doi: 10.33005/sitasi.v3i1.564.
- [30] T. L. Widodo and A. Putra, “ANALISA KERENTANAN KEAMANAN WEBSITE TIKETKAI . COM MENGGUNAKAN OWASP ZAP DENGAN METODE PTES (STUDI KASUS PT.KAI DIVRE 3 PALEMBANG),” pp. 1–8, 2024.
- [31] N. Cholis and E. I. H. Ujianto, “ANALISIS KEAMANAN WEBSITE SMK TAMAN KARYA KEBUMEN MENGGUNAKAN METODE VULNERABILITY ASESEMENT,” vol. 8, no. 6, pp. 828–834, 2024.
- [32] A. Zandra and M. Hardjianto, “DETEKSI CELAH KEAMANAN XSS PADA WEBSITE DENGAN DETECTION OF XSS VULNERABILITIES ON WEBSITES USING,” vol. 3, no. September, pp. 66–73, 2024.
- [33] T. Ariyadi, H. Fadli, T. Akbar, and M. B. Prihandoko, “Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma,” vol. 4, no. 1, pp. 1–7, 2025, doi: <https://doi.org/10.55123/storage.v4i1.4737>.
- [34] Nurjannah and Abdul Muni, “Analisis Keamanan Website Sekolah Sman 1 Tempuling Dengan Menggunakan Open Web Application Security Project (Owasp),” *J. Perangkat Lunak*, vol. 6, no. 2, pp. 351–361, 2024, doi: 10.32520/jupel.v6i2.3442.
- [35] T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, “Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP,” *Techno.Com*, vol. 22, no. 2, pp. 418–429, 2023, doi: 10.33633/tc.v22i2.7562.
- [36] F. Nisa, N. S. Nurfebruary, and M. Ikhwan, “Analisis Keamanan Sistem Informasi Website Portal Akademik Universitas Malikussaleh Menggunakan OWASP ZAP,” *J. Nas. Komputasi dan Teknol. Inf.*, vol. 7, no. 6, pp. 2003–2013, Dec. 2024, doi: 10.32672/jnkti.v7i6.8345.
- [37] W. Wahyudin, H. Kuswara, R. Resti, and S. Dalis, “Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales,” *Comput. Sci.*, vol. 4, no. 1, pp. 44–52, 2024, doi: 10.31294/coscience.v4i1.2978.
- [38] M. A. Mu’min, A. Fadlil, and I. Riadi, “Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework,” *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.